Linear Algebra II (MAT 3141)

Course notes written by Damien Roy

with the assistance of Pierre Bel

and financial support from the University of Ottawa

for the development of pedagogical material in French

(Translated into English by Alistair Savage)

Fall 2012

Department of Mathematics and Statistics

University of Ottawa

Contents

Preface

These notes are aimed at students in the course *Linear Algebra II* (MAT 3141) at the University of Ottawa. The first three chapters contain a revision of basic notions covered in the prerequisite course *Linear Algebra I* (MAT 2141): vector spaces, linear maps and diagonalization. The rest of the course is divided into three parts. Chapters 4 to 8 make up the main part of the course. They culminate in the structure theorem for finite type modules over a euclidean ring, a result which leads to the Jordan canonical form of operators on a finite dimensional complex vector space, as well as to the structure theorem for abelian groups of finite type. Chapter 9 involves duality and the tensor product. Then Chapter 10 treats the spectral theorems for operators on an inner product space (after a review of some notions seen in the prerequisite course MAT 2141). With respect to the initial plan, they still lack an eleventh chapter on hermitian spaces, which will be added later. The notes are completed by two appendices. Appendix A provides a review of basic algebra that are used in the course: groups, rings and fields (and the morphisms betwen these objects). Appendix B covers the determinants of matrices with entries in an arbitrary commutative ring and their properties. Often the determinant is simply defined over a field and the goal of this appendix is to show that this notion easily generalizes to an arbitrary commutative ring.

This course provides students the chance to learn the theory of modules that is not covered, due to lack of time, in other undergraduate algebra courses. To simplify matters and make the course easier to follow, I have avoided introducing quotient modules. This topic could be added through exercises (for more motivated students). According to comments I have received, students appreciate the richness of the concepts presented in this course and that they open new horizons to them.

I thank Pierre Bel who greatly helped with the typing and updating of these notes. I also thank the Rectorat aux Études of the University of Ottawa for its financial support of this project via the funds for the development of French teaching materials. This project would not have been possible without their help. Finally, I thank my wife Laura Dutto for her help in the revision of preliminary versions of these notes and the students who took this course with me in the Winter and Fall of 2009 for their participation and their comments.

Damien Roy (as translated by Alistair Savage) Ottawa, January 2010.

Chapter 1

Review of vector spaces

This chapter, like the two that follow it, is devoted to a review of fundamental concepts of linear algebra from the prerequisite course MAT 2141. This first chapter concerns the main object of study in linear algebra: vector spaces. We recall here the notions of a vector space, vector subspace, basis, dimension, coordinates, and direct sum. The reader should pay special attention to the notion of direct sum, since it will play a vital role later in the course.

1.1 Vector spaces

Definition 1.1.1 (Vector space). A *vector space* over a field K is a set V with operations of addition and scalar multiplication:

$$\begin{array}{ccc} V \times V & \longrightarrow & V \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} + \mathbf{v} \end{array} \quad \text{and} \quad \begin{array}{ccc} K \times V & \longrightarrow & V \\ (a, \mathbf{v}) & \longmapsto & a\mathbf{v} \end{array}$$

that satisfies the following axioms:

$$\left.\begin{array}{ll} \textbf{VS1}. & \mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w} \\ \textbf{VS2}. & \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} \end{array}\right\} \text{for all } \mathbf{u}, \mathbf{v}, \mathbf{w} \in V.$$

VS3. There exists $\mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v} \in V$.
VS4. For all $\mathbf{v} \in V$, there exists $-\mathbf{v} \in V$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.

$$\left.\begin{array}{ll} \textbf{VS5}. & 1\mathbf{v} = \mathbf{v} \\ \textbf{VS6}. & a(b\mathbf{v}) = (ab)\mathbf{v} \\ \textbf{VS7}. & (a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v} \\ \textbf{VS8}. & a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v} \end{array}\right\} \text{for all } a, b \in K \text{ and } \mathbf{u}, \mathbf{v} \in V.$$

These eight axioms can be easily interpreted. The first four imply that $(V, +)$ is an *abelian group* (cf. Appendix **A**). In particular, **VS1** and **VS2** imply that the order in which

we add the elements $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of V does not affect their sum, denoted

$$\mathbf{v}_1 + \cdots + \mathbf{v}_n \quad \text{or} \quad \sum_{i=1}^{n} \mathbf{v}_i.$$

Condition **VS3** uniquely determines the element $\mathbf{0}$ of V. We call it the *zero!vector* of V, the term *vector* being the generic name used to designate an element of a vector space. For each $\mathbf{v} \in V$, there exists one and only one vector $-\mathbf{v} \in V$ that satisfies **VS4**. We call it the *additive inverse* of $\mathbf{v}$. The existence of the additive inverse allows us to define subtraction in V by

$$\mathbf{u} - \mathbf{v} := \mathbf{u} + (-\mathbf{v}).$$

Axioms **VS5** and **VS6** involve only scalar multiplication, while the Axioms **VS7** and **VS8** link the two operations. These last axioms require that multiplication by a scalar be distributive over addition on the right and on the left (i.e. over addition in K and in V). They imply general distributivity formulas:

$$\left(\sum_{i=1}^{n} a_i\right)\mathbf{v} = \sum_{i=1}^{n} a_i\mathbf{v} \quad \text{and} \quad a\sum_{i=1}^{n} \mathbf{v}_i = \sum_{i=1}^{n} a\mathbf{v}_i$$

for all $a, a_1, \ldots, a_n \in K$ and $\mathbf{v}, \mathbf{v}_1, \ldots, \mathbf{v}_n \in V$.

We will return to these axioms later when we study the notion of a module over a commutative ring, which generalizes the idea of a vector space over a field.

Example 1.1.2. Let $n \in \mathbb{N}_{>0}$. The set

$$K^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} ; a_1, a_2, \ldots, a_n \in K \right\}$$

of n-tuples of elements of K is a vector space over K for the operations:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad \text{and} \quad c\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} c\,a_1 \\ c\,a_2 \\ \vdots \\ c\,a_n \end{pmatrix}.$$

In particular, $K^1 = K$ is a vector space over K.

Example 1.1.3. More generally, let $m, n \in \mathbb{N}_{>0}$. The set

$$\mathrm{Mat}_{m\times n}(K) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} ; a_{11}, \ldots, a_{mn} \in K \right\}$$

of $m \times n$ matrices with entries in K is a vector space over K for the usual operations:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

$$\text{and} \quad c \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} c\,a_{11} & \cdots & c\,a_{1n} \\ \vdots & & \vdots \\ c\,a_{m1} & \dots & c\,a_{mn} \end{pmatrix}.$$

Example 1.1.4. Let X be an arbitrary set. The set $\mathcal{F}(X, K)$ of functions from X to K is a vector space over K when we define the sum of two functions $f\colon X \to K$ and $g\colon X \to K$ to be the function $f + g\colon X \to K$ given by

$$(f+g)(x) = f(x) + g(x) \quad \text{for all } x \in X,$$

and the product of $f\colon X \to K$ and a scalar $c \in K$ to be the function $c\,f\colon X \to K$ given by

$$(c\,f)(x) = c\,f(x) \quad \text{for all } x \in X.$$

Example 1.1.5. Finally, if $V_1, \dots, V_n$ are vector spaces over K, their *cartesian product*

$$V_1 \times \cdots \times V_n = \{(\mathbf{v}_1, \dots, \mathbf{v}_n)\,;\, \mathbf{v}_1 \in V_1, \dots, \mathbf{v}_n \in V_n\}$$

is a vector space over K for the operations

$$(\mathbf{v}_1, \dots, \mathbf{v}_n) + (\mathbf{w}_1, \dots, \mathbf{w}_n) = (\mathbf{v}_1 + \mathbf{w}_1, \dots, \mathbf{v}_n + \mathbf{w}_n),$$
$$c(\mathbf{v}_1, \dots, \mathbf{v}_n) = (c\mathbf{v}_1, \dots, c\mathbf{v}_n).$$

1.2 Vector subspaces

Fix a vector space V over a field K.

Definition 1.2.1 (Vector subspace). A *vector subspace* of V is a subset U of V satisfying the following conditions:

SUB1. $\mathbf{0} \in U$.
SUB2. If $\mathbf{u}, \mathbf{v} \in U$, then $\mathbf{u} + \mathbf{v} \in U$.
SUB3. If $\mathbf{u} \in U$ and $c \in K$, then $c\mathbf{u} \in U$.

Conditions **SUB2** and **SUB3** imply that U is stable under the addition in V and stable under scalar multiplication by elements of K. We thus obtain the operations

$$\begin{array}{ccc} U \times U & \longrightarrow & U \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} + \mathbf{v} \end{array} \quad \text{and} \quad \begin{array}{ccc} K \times U & \longrightarrow & U \\ (a, \mathbf{v}) & \longmapsto & a\mathbf{v} \end{array}$$

on U and we see that, with these operations, U is itself a vector space. Condition **SUB1** can be replaced by $U \neq \varnothing$ because, if U contains an element $\mathbf{u}$, then **SUB3** implies that $0\,\mathbf{u} = \mathbf{0} \in U$. Nevertheless, it is generally just as easy to verify **SUB1**. We therefore have the following proposition.

Proposition 1.2.2. *A vector subspace U of V is a vector space over K for the addition and scalar multiplication restricted from V to U.*

We therefore see that all vector subspaces of V give new examples of vector spaces. If U is a subspace of V, we can also consider subspaces of U. However, we see that these are simply subspaces of V contained in U. Thus, this does not give new examples. In particular, the notion of being a subspace is transitive.

Proposition 1.2.3. *If U is a subspace of V and W is a subspace of U, then W is a subspace of V.*

We can also form the sum and intersection of subspaces of V:

Proposition 1.2.4. *Let $U_1, \dots, U_n$ be subspaces of V. The sets*

$$U_1 + \cdots + U_n = \{\mathbf{u}_1 + \cdots + \mathbf{u}_n \,;\, \mathbf{u}_1 \in U_1, \dots, \mathbf{u}_n \in U_n\} \quad \textit{and}$$
$$U_1 \cap \cdots \cap U_n = \{\mathbf{u} \,;\, \mathbf{u} \in U_1, \dots, \mathbf{u} \in U_n\},$$

called, respectively, the sum *and* intersection *of $U_1, \dots, U_n$, are subspaces of V.*

Example 1.2.5. Let V_1 and V_2 be vector spaces over K. Then

$$U_1 = V_1 \times \{\mathbf{0}\} = \{(\mathbf{v}_1, \mathbf{0}) \,;\, \mathbf{v}_1 \in V_1\} \quad \text{and} \quad U_2 = \{\mathbf{0}\} \times V_2 = \{(\mathbf{0}, \mathbf{v}_2) \,;\, \mathbf{v}_2 \in V_2\}$$

are subspaces of $V_1 \times V_2$. We see that

$$U_1 + U_2 = V_1 \times V_2 \quad \text{and} \quad U_1 \cap U_2 = \{(\mathbf{0}, \mathbf{0})\}.$$

1.3 Bases

In this section, we fix a vector space V over a field K and elements $\mathbf{v}_1, \dots, \mathbf{v}_n$ of V.

Definition 1.3.1 (Linear combination). We say that an element $\mathbf{v}$ of V is a *linear combination* of $\mathbf{v}_1, \dots, \mathbf{v}_n$ if there exist $a_1, \dots, a_n \in K$ such that

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

We denote by

$$\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n \,;\, a_1, \dots, a_n \in K\}$$

the set of linear combinations of $\mathbf{v}_1, \dots, \mathbf{v}_n$. This is also sometimes denoted $\mathrm{Span}_K\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$.

The identities

$$0\mathbf{v}_1 + \cdots + 0\mathbf{v}_n = \mathbf{0}$$
$$\sum_{i=1}^{n} a_i\mathbf{v}_i + \sum_{i=1}^{n} b_i\mathbf{v}_i = \sum_{i=1}^{n} (a_i + b_i)\mathbf{v}_i$$
$$c \sum_{i=1}^{n} a_i\mathbf{v}_i = \sum_{i=1}^{n} (c\, a_i)\mathbf{v}_i$$

show that $\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K$ is a subspace of V. This subspaces contains $\mathbf{v}_1, \dots, \mathbf{v}_n$ since we have

$$\mathbf{v}_j = \sum_{i=1}^{n} \delta_{i,j} \mathbf{v}_i \quad \text{where} \quad \delta_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, every subspace of V that contains $\mathbf{v}_1, \dots, \mathbf{v}_n$ also contains all linear combinations of $\mathbf{v}_1, \dots, \mathbf{v}_n$, that is, it contains $\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K$. Therefore:

Proposition 1.3.2. *The set $\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K$ of linear combinations of $\mathbf{v}_1, \dots, \mathbf{v}_n$ is a subspace of V that contains $\mathbf{v}_1, \dots, \mathbf{v}_n$ and that is contained in all subspaces of V containing $\mathbf{v}_1, \dots, \mathbf{v}_n$.*

We express this property by saying that $\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K$ is the smallest subspace of V that contains $\mathbf{v}_1, \dots, \mathbf{v}_n$ (with respect to inclusion). We call it the subspace of V *generated* by $\mathbf{v}_1, \dots, \mathbf{v}_n$.

Definition 1.3.3 (Generators). We say that $\mathbf{v}_1, \dots, \mathbf{v}_n$ *generates* V or that $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a *system of generators* (or *generating set*) of V if

$$\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K = V$$

We say that V is a subspace of *finite type* (or is *finite dimensional*) if it admits a finite system of generators.

It is important to distinguish the finite set $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ consisting of n elements (counting possible repetitions) from the set $\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_K$ of their linear combinations, which is generally infinite.

Definition 1.3.4 (Linear dependence and independence). We say that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are *linearly independent*, or that the set $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is *linearly independent* if the only choice of $a_1, \dots, a_n \in K$ such that

$$a_1 \mathbf{v}_1 + \cdots + a_n \mathbf{v}_n = \mathbf{0} \tag{1.1}$$

is $a_1 = \cdots = a_n = 0$. Otherwise, we say that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are *linearly dependent*.

In other words, $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly dependent if there exist $a_1, \dots, a_n$, not all zero, that satisfy Condition (1.1). A relation of the form (1.1) with $a_1, \dots, a_n$ not all zero is called a *linear dependence relation* among $\mathbf{v}_1, \dots, \mathbf{v}_n$.

Definition 1.3.5 (Basis). We say that $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a *basis* of V if $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a system of linearly independent generators for V.

The importance of the notion of basis comes from the following result:

Proposition 1.3.6. *Suppose that $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for V. For all $\mathbf{v} \in V$, there exists a unique choice of scalars $a_1, \dots, a_n \in K$ such that*

$$\mathbf{v} = a_1 \mathbf{v}_1 + \cdots + a_n \mathbf{v}_n \,. \tag{1.2}$$

Proof. Suppose $\mathbf{v} \in V$. Since the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ generate V, there exist $a_1, \dots, a_n \in K$ satisfying (1.2). If $a'_1, \dots, a'_n \in K$ also satisfy $\mathbf{v} = a'_1\mathbf{v}_1 + \cdots + a'_n\mathbf{v}_n$, then we have

$$\begin{aligned}\mathbf{0} &= (a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) - (a'_1\mathbf{v}_1 + \cdots + a'_n\mathbf{v}_n)\\ &= (a_1 - a'_1)\mathbf{v}_1 + \cdots + (a_n - a'_n)\mathbf{v}_n.\end{aligned}$$

Since the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independents, this implies that $a_1 - a'_1 = \cdots = a_n - a'_n = 0$, and so $a_1 = a'_1, \dots, a_n = a'_n$. □

If $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis of V, the scalars $a_1, \dots, a_n$ that satisfy (1.2) are called the *coordinates* of $\mathbf{v}$ in the basis $\mathcal{B}$. We denote by

$$[\mathbf{v}]_{\mathcal{B}} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$

the column vector formed by these coordinates. Note that this supposes that we have fixed an order on the elements of $\mathcal{B}$, in other words that $\mathcal{B}$ is an ordered set of elements of V. Really, we should write $\mathcal{B}$ as an n-tuple $(\mathbf{v}_1, \dots, \mathbf{v}_n)$, but we stick with the traditional set notation.

Example 1.3.7. Let $n \in \mathbb{N}_{>0}$. The vectors

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ \dots, \ \mathbf{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

form a basis $\mathcal{E} = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ of K^n called the *standard basis* (or *canonical basis*) of K^n. We have

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

therefore

$$\left[\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}\right]_{\mathcal{E}} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \text{ for all } \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n.$$

The following result is fundamental:

Proposition 1.3.8. *Suppose V is a vector space of finite type. Then*

(i) V has a basis and all bases of V have the same cardinality.

(ii) *Every generating set of V contains a basis of V.*

(iii) *Every linearly independent set of elements of V is contained in a basis of V.*

(iv) *Every subspace of V has a basis.*

The common cardinality of the bases of V is called the *dimension* of V and is denoted $\dim_K V$. Recall that, by convention, if $V = \{\mathbf{0}\}$, then $\varnothing$ is a basis of V and $\dim_K V = 0$. If V is of dimension n, then it follows from statements (ii)) and (iii) of Proposition 1.3.8 that every generating set of V contains at least n elements and that every linearly independent set in V contains at most n elements. From this we can also deduce that if U_1 and U_2 are subspaces of V of the same finite dimension, with $U_1 \subseteq U_2$, then $U_1 = U_2$.

We also recall the following fact.

Proposition 1.3.9. *If U_1 and U_2 are finite dimensional subspaces of V, then*

$$\dim_K(U_1 + U_2) + \dim_K(U_1 \cap U_2) = \dim_K(U_1) + \dim_K(U_2).$$

1.4 Direct sum

In this section, we fix a vector space V over a field K and subspaces $V_1, \ldots, V_s$ of V.

Definition 1.4.1 (Direct sum). We say that the sum $V_1 + \cdots + V_s$ is *direct* if the only choice of vectors $\mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_s \in V_s$ such that

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

is $\mathbf{v}_1 = \cdots \mathbf{v}_s = \mathbf{0}$. We express this condition by writing the sum of the subspaces $V_1, \ldots, V_s$ as $V_1 \oplus \cdots \oplus V_s$ with circles around the addition signs.

We say that V is the *direct sum* of $V_1, \ldots, V_s$ if $V = V_1 \oplus \cdots \oplus V_s$.

Example 1.4.2. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of a vector space V over K. Proposition 1.3.6 shows that $V = \langle \mathbf{v}_1 \rangle_K \oplus \cdots \oplus \langle \mathbf{v}_n \rangle_K$.

Example 1.4.3. We always have $V = V \oplus \{\mathbf{0}\} = V \oplus \{\mathbf{0}\} \oplus \{\mathbf{0}\}$.

This last example shows that, in a direct sum, we can have one or more summands equal to $\{\mathbf{0}\}$.

Proposition 1.4.4. *The vector space V is the direct sum of the subspaces $V_1, \ldots, V_s$ if and only if, for every $\mathbf{v} \in V$, there exists a unique choice of vectors $\mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_s \in V_s$ such that*

$$\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_s.$$

The proof is similar to that of Proposition 1.3.6 and is left to the reader. We also have the following criterion (compare to Exercise 1.4.2).

Proposition 1.4.5. *The sum $V_1 + \cdots + V_s$ is direct if and only if*

$$V_i \cap \big(V_1 + \cdots + \widehat{V_i} + \cdots + V_s\big) = \{\mathbf{0}\} \text{ for } i = 1, \ldots, s. \tag{1.3}$$

In the above condition, the hat over the V_i indicates that V_i is omitted from the sum.

Proof. First suppose that Condition (1.3) is satisfied. If $\mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_s \in V_s$ satisfy $\mathbf{v}_1 + \cdots + \mathbf{v}_s = 0$, then, for $i = 1, \ldots, s$, we have

$$-\mathbf{v}_i = \mathbf{v}_1 + \cdots + \widehat{\mathbf{v}_i} + \cdots + \mathbf{v}_s \in V_i \cap \big(V_1 + \cdots + \widehat{V_i} + \cdots + V_s\big).$$

Therefore $-\mathbf{v}_i = \mathbf{0}$ and so $\mathbf{v}_i = \mathbf{0}$. Thus the sum $V_1 + \cdots + V_s$ is direct.

Conversely, suppose that the sum is direct, and fix $i \in \{1, \ldots, s\}$. If

$$\mathbf{v} \in V_i \cap \big(V_1 + \cdots + \widehat{V_i} + \cdots + V_s\big),$$

then there exists $\mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_s \in V_s$ such that

$$\mathbf{v} = -\mathbf{v}_i \quad \text{and} \quad \mathbf{v} = \mathbf{v}_1 + \cdots + \widehat{\mathbf{v}_i} + \cdots + \mathbf{v}_s.$$

Eliminating $\mathbf{v}$, we see that $-\mathbf{v}_i = \mathbf{v}_1 + \cdots + \widehat{\mathbf{v}_i} + \cdots + \mathbf{v}_s$, thus $\mathbf{v}_1 + \cdots + \mathbf{v}_s = \mathbf{0}$ and so $\mathbf{v}_1 = \cdots = \mathbf{v}_s = \mathbf{0}$. In particular, we see that $\mathbf{v} = 0$. Since the choice of $\mathbf{v}$ was arbitrary, this shows that Condition (1.3) is satisfied for all i. □

In particular, for $s = 2$, Proposition 1.4.5 implies that $V = V_1 \oplus V_2$ if and only if $V = V_1 + V_2$ and $V_1 \cap V_2 = \{\mathbf{0}\}$. Applying this result to Proposition 1.3.9, we see that:

Proposition 1.4.6. *Suppose V_1 and V_2 are subspaces of a vector space V of finite dimension. Then $V = V_1 \oplus V_2$ if and only if*

(i) $\dim_K V = \dim_K V_1 + \dim_K V_2$, *and*

(ii) $V_1 \cap V_2 = \{\mathbf{0}\}$.

Example 1.4.7. Let $V = \mathbb{R}^3$,

$$V_1 = \left\langle \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}} = \left\{ \begin{pmatrix} 2a \\ 0 \\ a \end{pmatrix} ; a \in \mathbb{R} \right\} \quad \text{and} \quad V_2 = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 ; x + y + z = 0 \right\}.$$

Proposition 1.3.2 implies that V_1 is a subspace of $\mathbb{R}^3$. Since $\left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\}$ is a basis of V_1, we have $\dim_{\mathbb{R}}(V_1) = 1$. On the other hand, since V_2 is the set of solutions to a homogeneous system

of linear equations of rank 1 (with a single equation), V_2 is a subsapce of $\mathbb{R}^3$ of dimension $\dim_{\mathbb{R}}(V_2) = 3 - (\text{rank of the system}) = 2$. We also see that

$$\begin{pmatrix} 2a \\ 0 \\ a \end{pmatrix} \in V_2 \Longleftrightarrow 2a + 0 + a = 0 \Longleftrightarrow a = 0,$$

and so $V_1 \cap V_2 = \{\mathbf{0}\}$. Since $\dim_{\mathbb{R}} V_1 + \dim_{\mathbb{R}} V_2 = 3 = \dim_{\mathbb{R}} \mathbb{R}^3$, Proposition 1.4.6 implies that $\mathbb{R}^3 = V_1 \oplus V_2$.

Geometric interpretation: The set V_1 represents a straight line passing through the origin in $\mathbb{R}^3$, while V_2 represents a plane passing through the origin with normal vector $\mathbf{n} := (1,1,1)^t$. The line V_1 is not parallel to the plane V_2 because its direction vector $(2,0,1)^t$ is not perpendicular to $\mathbf{n}$. In this situation, we see that every vector in the space can be written in a unique way as the sum of a vector of the line and a vector in the plane.

The following result will play a key role later in the course.

Proposition 1.4.8. *Suppose that $V = V_1 \oplus \cdots \oplus V_s$ is of finite dimension and that $\mathcal{B}_i = \{\mathbf{v}_{i,1}, \mathbf{v}_{i,2}, \ldots, \mathbf{v}_{i,n_i}\}$ is a basis of V_i for $i = 1, \ldots, s$. Then the ordered set*

$$\mathcal{B} = \{\mathbf{v}_{1,1}, \ldots, \mathbf{v}_{1,n_1}, \mathbf{v}_{2,1}, \ldots, \mathbf{v}_{2,n_2}, \ldots\ldots, \mathbf{v}_{s,1}, \ldots, \mathbf{v}_{s,n_s}\}$$

obtained by concatenation from $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_s$ is a basis of V.

From now on, we will denote this basis by $\mathcal{B}_1 \amalg \mathcal{B}_2 \amalg \cdots \amalg \mathcal{B}_s$. The symbol $\amalg$ represents "disjoint union".

Proof. 1st **We show that $\mathcal{B}$ is a generating set for V.**

Let $\mathbf{v} \in V$. Since $V = V_1 \oplus \cdots \oplus V_s$, we can write $\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_s$ with $\mathbf{v}_i \in V_i$ for $i = 1, \ldots, s$. Since $\mathcal{B}_i$ is a basis for V_i, we can also write

$$\mathbf{v}_i = a_{i,1}\mathbf{v}_{i,1} + \cdots + a_{i,n_i}\mathbf{v}_{i,n_i}$$

with $a_{i,1}, \ldots, a_{i,n_i} \in K$. From this, we conclude that

$$\mathbf{v} = a_{1,1}\mathbf{v}_{1,1} + \cdots + a_{1,n_1}\mathbf{v}_{1,n_i} + \cdots\cdots + a_{s,1}\mathbf{v}_{s,1} + \cdots + a_{s,n_s}\mathbf{v}_{s,n_s}.$$

So $\mathcal{B}$ generates V.

2nd **We show that $\mathcal{B}$ is linearly independent.**

Suppose that

$$a_{1,1}\mathbf{v}_{1,1} + \cdots + a_{1,n_1}\mathbf{v}_{1,n_i} + \cdots + a_{s,1}\mathbf{v}_{s,1} + \cdots + a_{s,n_s}\mathbf{v}_{s,n_s} = \mathbf{0}$$

for some elements $a_{1,1}, \ldots, a_{s,n_s} \in K$. Setting $\mathbf{v}_i = a_{i,1}\mathbf{v}_{i,1} + \cdots + a_{i,n_i}\mathbf{v}_{i,n_i}$ for $i = 1, \ldots, s$, we see that $\mathbf{v}_1 + \cdots + \mathbf{v}_s = \mathbf{0}$. Since $\mathbf{v}_i \in V_i$ for $i = 1, \ldots, s$ and V is the direct sum of $V_1, \ldots, V_s$, this implies $\mathbf{v}_i = \mathbf{0}$ for $i = 1, \ldots, s$. We deduce that $a_{i,1} = \cdots = a_{i,n_i} = 0$, because $\mathcal{B}_i$ is a basis of V_i. So we have $a_{1,1} = \cdots = a_{s,n_s} = 0$. This shows that $\mathcal{B}$ is linearly independent. $\square$

Corollary 1.4.9. *If $V = V_1 \oplus \cdots \oplus V_s$ is finite dimensional, then*

$$\dim_K V = \dim_K(V_1) + \cdots + \dim_K(V_s).$$

Proof. Using Proposition 1.4.8 and using the same notation, we have

$$\dim_K V = |\mathcal{B}| = \sum_{i=1}^{s} |\mathcal{B}_i| = \sum_{i=1}^{s} \dim_K(V_i).$$

□

Example 1.4.10. In Example 1.4.7, we have $\mathbb{R}^3 = V_1 \oplus V_2$. We see that

$$\mathcal{B}_1 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\} \quad \text{and} \quad \mathcal{B}_2 = \left\{ \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\}$$

are bases for V_1 and V_2 respectively (indeed, $\mathcal{B}_2$ is a linearly independent subset of V_2 consisting of two elements, and $\dim_{\mathbb{R}}(V_2) = 2$, thus it is a basis V_2). We conclude that

$$\mathcal{B} = \mathcal{B}_1 \amalg \mathcal{B}_2 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\}$$

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

Exercises.

1.4.1. Prove Proposition 1.4.4.

1.4.2. Let $V_1, \ldots, V_s$ be subspaces of a vector space V over a field K. Show that their sum is direct if and only if

$$V_i \cap (V_{i+1} + \cdots + V_s) = \{\mathbf{0}\}$$

for $i = 1, \ldots, s-1$.

1.4.3. Let $V_1, \ldots, V_s$ be subspaces of a vector space V over a field K. Suppose that their sum is direct.

(i) Show that, if U_i is a subspace of V_i for $i = 1, \ldots, s$, then the sum $U_1 + \cdots + U_s$ is direct.

(ii) Show that, if $\mathbf{v}_i$ is a nonzero element of V_i for $i = 1, \ldots, s$, then $\mathbf{v}_1, \ldots, \mathbf{v}_s$ are linearly independent over K.

1.4.4. Consider the subspaces of $\mathbb{R}^4$ given by

$$V_1 = \left\langle \begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\end{pmatrix} \right\rangle_{\mathbb{R}} \quad \text{and} \quad V_2 = \left\langle \begin{pmatrix}1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\2\\2\end{pmatrix} \right\rangle_{\mathbb{R}}.$$

Show that $\mathbb{R}^4 = V_1 \oplus V_2$.

1.4.5. Let

$$\begin{aligned} V_1 &= \{\, f\colon \mathbb{Z} \to \mathbb{R}\,;\ \ f(-x) = f(x) \text{ for all } x \in \mathbb{Z}\,\} \\ \text{and} \quad V_2 &= \{\, f\colon \mathbb{Z} \to \mathbb{R}\,;\ \ f(-x) = -f(x) \text{ for all } x \in \mathbb{Z}\,\}. \end{aligned}$$

Show that V_1 and V_2 are subspaces of $\mathcal{F}(\mathbb{Z}, \mathbb{R})$ and that $\mathcal{F}(\mathbb{Z}, \mathbb{R}) = V_1 \oplus V_2$.

1.4.6. Let $V_1, V_2, \ldots, V_s$ be vector subspaces over the same field K. Show that

$$\begin{aligned} &V_1 \times V_2 \times \cdots \times V_s \\ &\quad = \big(V_1 \times \{\mathbf{0}\} \times \cdots \times \{\mathbf{0}\}\big) \oplus \big(\{\mathbf{0}\} \times V_2 \times \cdots \times \{\mathbf{0}\}\big) \oplus \cdots \oplus \big(\{\mathbf{0}\} \times \cdots \times \{\mathbf{0}\} \times V_s\big). \end{aligned}$$

Chapter 2

Review of linear maps

Fixing a field K of scalars, a linear map from a vector space V to a vector space W is a function that "commutes" with addition and scalar multiplication. This second preliminary chapter review the notions of linear maps, kernel and image, and the operations we can perform on linear maps (addition, scalar multiplication and composition). We then review matrices of linear maps relative to a choice of bases, how they behave under the above-mentioned operations and also under a change of basis. We examine the particular case of linear operators on a vector space V, that is, linear maps from V to itself. We pay special attention to the notion of invariant subspace of a linear operator, which will play a fundamental role later in the course.

2.1 Linear maps

Definition 2.1.1 (Linear map). Let V and W be vector spaces over K. A *linear map* from V to W is a function $T\colon V \to W$ such that

LM1. $T(\mathbf{v}+\mathbf{v}') = T(\mathbf{v}) + T(\mathbf{v}')$ for all $\mathbf{v}, \mathbf{v}' \in V$,

LM2. $T(c\mathbf{v}) = c\,T(\mathbf{v})$ for all $c \in K$ and all $\mathbf{v} \in V$.

We recall the following results:

Proposition 2.1.2. *Let $T\colon V \to W$ be a linear map.*

(i) The set $\ker(T) := \{\mathbf{v}\,;\, T(\mathbf{v}) = \mathbf{0}\}$*, called the* kernel *of T, is a subspace of V.*

(ii) The set $\mathrm{Im}(T) := \{T(\mathbf{v})\,;\, \mathbf{v} \in V\}$*, called the* image *of T, is a subspace of W.*

(iii) The linear map T is injective if and only if $\ker(T) = \{\mathbf{0}\}$*. It is surjective if and only if* $\mathrm{Im}(T) = W$*.*

(iv) If V is finite dimensional, then

$$\dim_K V = \dim_K(\ker(T)) + \dim_K(\mathrm{Im}(T)).$$

Example 2.1.3 (Linear map associated to a matrix). Let $M \in \mathrm{Mat}_{m\times n}(K)$. The function

$$\begin{array}{rccc} T_M : & K^n & \longrightarrow & K^m \\ & X & \longmapsto & MX \end{array}$$

is linear (this follows immediately from the properties of matrix multiplication). Its kernel is

$$\ker(T_M) := \{X \in K^n \,;\, MX = \mathbf{0}\}$$

and is thus the solution set of the homogeneous system $MX = 0$. If $C_1, \ldots, C_n$ denote the columns of M, we see that

$$\begin{aligned} \mathrm{Im}(T_M) &= \{MX \,;\, X \in K^n\} \\ &= \left\{ (C_1 \cdots C_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \,;\; x_1, \ldots, x_n \in K \right\} \\ &= \{x_1 C_1 + \cdots + x_n C_n \,;\; x_1, \ldots, x_n \in K\} \\ &= \langle C_1, \ldots, C_n \rangle_K. \end{aligned}$$

Thus the image of T_M is the column space of M. Since the dimension of the latter is the rank of M, formula (iv) of Proposition 2.1.2 recovers the following known result:

$$\dim\{X \in K^n \,;\, MX = \mathbf{0}\} = n - \mathrm{rank}(M).$$

Example 2.1.4. Let V_1 and V_2 be vector spaces over K. The function

$$\begin{array}{rccc} \pi_1 : & V_1 \times V_2 & \longrightarrow & V_1 \\ & (\mathbf{v}_1, \mathbf{v}_2) & \longmapsto & \mathbf{v}_1 \end{array}$$

is a linear map since if $(\mathbf{v}_1, \mathbf{v}_2)$ and $(\mathbf{v}_1', \mathbf{v}_2')$ are elements of $V_1 \times V_2$ and $c \in K$, we have

$$\begin{aligned} \pi_1((\mathbf{v}_1, \mathbf{v}_2) + (\mathbf{v}_1', \mathbf{v}_2')) &= \pi_1(\mathbf{v}_1 + \mathbf{v}_1', \mathbf{v}_2 + \mathbf{v}_2') \\ &= \mathbf{v}_1 + \mathbf{v}_1' \\ &= \pi_1(\mathbf{v}_1, \mathbf{v}_2) + \pi_1(\mathbf{v}_1', \mathbf{v}_2') \end{aligned}$$

and

$$\pi_1(c\,(\mathbf{v}_1, \mathbf{v}_2)) = \pi_1(c\,\mathbf{v}_1, c\,\mathbf{v}_2) = c\,\mathbf{v}_1 = c\,\pi_1(\mathbf{v}_1, \mathbf{v}_2).$$

We also see that

$$\ker(\pi_1) = \{(\mathbf{v}_1, \mathbf{v}_2) \in V_1 \times V_2 \,;\, \mathbf{v}_1 = 0\} = \{(0, \mathbf{v}_2) \,;\, \mathbf{v}_2 \in V_2\} = \{\mathbf{0}\} \times V_2,$$

and $\mathrm{Im}(\pi_1) = V_1$ since $\mathbf{v}_1 = \pi_1(\mathbf{v}_1, \mathbf{0}) \in \mathrm{Im}(\pi_1)$ for all $\mathbf{v}_1 \in V_1$. Thus π_1 is surjective.

The map $\pi_1 \colon V_1 \times V_2 \to V_1$ is called the *projection onto the first factor*. Similarly, we see that

$$\begin{array}{rccc} \pi_2 : & V_1 \times V_2 & \longrightarrow & V_2 \\ & (\mathbf{v}_1, \mathbf{v}_2) & \longmapsto & \mathbf{v}_2 \end{array},$$

called *projection onto the second factor* is linear and surjective with kernel $V_1 \times \{\mathbf{0}\}$. In a similar manner, we see that the maps

$$\begin{array}{rccc} i_1 : & V_1 & \longrightarrow & V_1 \times V_2 \\ & \mathbf{v}_1 & \longmapsto & (\mathbf{v}_1, \mathbf{0}) \end{array} \quad \text{and} \quad \begin{array}{rccc} i_2 : & V_2 & \longrightarrow & V_1 \times V_2 \\ & \mathbf{v}_2 & \longmapsto & (\mathbf{0}, \mathbf{v}_2) \end{array}$$

are linear and injective, with images $V_1 \times \{\mathbf{0}\}$ and $\{\mathbf{0}\} \times V_2$ respectively.

We conclude this section with the following result which will be crucial in what follows. In particular, we will see in Chapter 9 that it can be generalized to "bilinear" maps (see also Appendix B for the even more general case of multilinear maps).

Theorem 2.1.5. *Let V and W be vector spaces over K, with $\dim_K(V) = n$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V, and $\mathbf{w}_1, \ldots, \mathbf{w}_n$ a sequence of n arbitrary elements of W (not necessarily distinct). Then there exists a unique linear map $T \colon V \to W$ satisfying $T(\mathbf{v}_i) = \mathbf{w}_i$ for all $i = 1, \ldots, n$.*

Proof. 1$^{\mathbf{st}}$ **Uniqueness.** If such a linear map T exists, then

$$T\Big(\sum_{i=1}^{n} a_i \mathbf{v}_i\Big) = \sum_{i=1}^{n} a_i T(\mathbf{v}_i) = \sum_{i=1}^{n} a_i \mathbf{w}_i$$

for all $a_1, \ldots, a_n \in K$. This uniquely determines T.

2$^{\mathbf{nd}}$ **Existence.** Consider the function $T \colon V \to W$ defined by

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

It satisfies $T(\mathbf{v}_i) = \mathbf{w}_i$ for all $i = 1, \ldots, n$. It remains to show that this map is linear. We have

$$\begin{aligned} T\Big(\sum_{i=1}^{n} a_i \mathbf{v}_i + \sum_{j=1}^{n} a_i' \mathbf{v}_i\Big) &= T\Big(\sum_{i=1}^{n} (a_i + a_i') \mathbf{v}_i\Big) \\ &= \sum_{i=1}^{n} (a_i + a_i') \mathbf{w}_i \\ &= \sum_{i=1}^{n} a_i \mathbf{w}_i + \sum_{i=1}^{n} a_i' \mathbf{w}_i \\ &= T\Big(\sum_{i=1}^{n} a_i \mathbf{v}_i\Big) + T\Big(\sum_{j=1}^{n} a_i' \mathbf{v}_i\Big), \end{aligned}$$

for all $a_1, \ldots, a_n, a'_1, \ldots, a'_n \in K$. We also see that

$$T\Big(c\sum_{i=1}^{n} a_i \mathbf{v}_i\Big) = c\,T\Big(\sum_{i=1}^{n} a_i \mathbf{v}_i\Big),$$

for all $c \in K$. Thus T is indeed a linear map. □

2.2 The vector space $\mathcal{L}_K(V, W)$

Let V and W be vector spaces over K. We denote by $\mathcal{L}_K(V, W)$ the set of linear maps from V to W. We first recall that this set is naturally endowed with the operations of addition and scalar multiplication.

Proposition 2.2.1. *Let $T_1 \colon V \to W$ and $T_2 \colon V \to W$ be linear maps, and let $c \in K$.*

(i) The function $T_1 + T_2 \colon V \to W$ given by

$$(T_1 + T_2)(\mathbf{v}) = T_1(\mathbf{v}) + T_2(\mathbf{v}) \quad \textit{for all } \mathbf{v} \in V$$

is a linear map.

(ii) The function $c\,T_1 \colon V \to W$ given by

$$(c\,T_1)(\mathbf{v}) = c\,T_1(\mathbf{v}) \quad \textit{for all } \mathbf{v} \in V$$

is also a linear map.

Proof of (i). For all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $a \in K$, we have:

$$\begin{aligned}
(T_1 + T_2)(\mathbf{v}_1 + \mathbf{v}_2) &= T_1(\mathbf{v}_1 + \mathbf{v}_2) + T_2(\mathbf{v}_1 + \mathbf{v}_2) && \text{(definition of } T_1 + T_2\text{)}\\
&= (T_1(\mathbf{v}_1) + T_1(\mathbf{v}_2)) + (T_2(\mathbf{v}_1) + T_2(\mathbf{v}_2)) && \text{(since } T_1 \text{ and } T_2 \text{ are linear)}\\
&= (T_1(\mathbf{v}_1) + T_2(\mathbf{v}_1)) + (T_1(\mathbf{v}_2) + T_2(\mathbf{v}_2))\\
&= (T_1 + T_2)(\mathbf{v}_1) + (T_1 + T_2)(\mathbf{v}_2), && \text{(definition of } T_1 + T_2\text{)}\\
(T_1 + T_2)(a\,\mathbf{v}_1) &= T_1(a\,\mathbf{v}_1) + T_2(a\,\mathbf{v}_1) && \text{(definition of } T_1 + T_2\text{)}\\
&= a\,T_1(\mathbf{v}_1) + a\,T_2(\mathbf{v}_1) && \text{(since } T_1 \text{ and } T_2 \text{ are linear)}\\
&= a\,(T_1(\mathbf{v}_1) + T_2(\mathbf{v}_1))\\
&= a\,(T_1 + T_2)(\mathbf{v}_1). && \text{(definition of } T_1 + T_2\text{)}
\end{aligned}$$

Thus $T_1 + T_2$ is linear. The proof that $c\,T_1$ is linear is analogous. □

Example 2.2.2. Let V be a vector space over $\mathbb{Q}$, and let $\pi_1 \colon V \times V \to V$ and $\pi_2 \colon V \times V \to V$ be the maps defined, as in Example 2.1.4, by

$$\pi_1(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{v}_1 \quad \text{and} \quad \pi_2(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{v}_2$$

for all $(\mathbf{v}_1, \mathbf{v}_2) \in V \times V$. Then

1) $\pi_1 + \pi_2 \colon V \times V \to V$ is the linear map given by

$$(\pi_1 + \pi_2)(\mathbf{v}_1, \mathbf{v}_2) = \pi_1(\mathbf{v}_1, \mathbf{v}_2) + \pi_2(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{v}_1 + \mathbf{v}_2,$$

2) $3\pi_1 \colon V \times V \to V$ is the linear map given by

$$(3\pi_1)(\mathbf{v}_1, \mathbf{v}_2) = 3\pi_1(\mathbf{v}_1, \mathbf{v}_2) = 3\mathbf{v}_1.$$

Combining addition and scalar multiplication, we can, for example, form

$$\begin{array}{rccl} 3\pi_1 + 5\pi_5 : & V \times V & \longrightarrow & V \\ & (\mathbf{v}_1, \mathbf{v}_2) & \longmapsto & 3\mathbf{v}_1 + 5\mathbf{v}_2. \end{array}$$

Theorem 2.2.3. *The set $\mathcal{L}_K(V,W)$ is a vector space over K for the addition and scalar multiplication defined in Proposition 2.2.1.*

Proof. To show that $\mathcal{L}_K(V,W)$ is a vector space over K, it suffices to proof that the operations satisfy the 8 required axioms.

We first note that the map $\mathcal{O} \colon V \to W$ given by

$$\mathcal{O}(\mathbf{v}) = \mathbf{0} \quad \text{for all } \mathbf{v} \in V$$

is a linear map (hence an element of $\mathcal{L}_K(V,W)$). We also note that, if $T \in \mathcal{L}_K(V,W)$, then the function $-T \colon V \to W$ defined by

$$(-T)(\mathbf{v}) = -T(\mathbf{v}) \quad \text{for all } \mathbf{v} \in V$$

is also a linear map (it is $(-1)T$). Therefore, it suffices to show that, for all $a, b \in K$ and $T_1, T_2, T_3 \in \mathcal{L}_K(V,W)$, we have

1) $T_1 + (T_2 + T_3) = (T_1 + T_2) + T_3$

2) $T_1 + T_2 = T_2 + T_1$

3) $\mathcal{O} + T_1 = T_1$

4) $T_1 + (-T_1) = \mathcal{O}$

5) $1 \cdot T_1 = T_1$

6) $a(b\,T_1) = (ab)\,T_1$

7) $(a+b)\,T_1 = a\,T_1 + b\,T_1$

8) $a\,(T_1 + T_2) = a\,T_1 + a\,T_2$.

We show, for example, Condition 8). To verify that two elements of $\mathcal{L}_K(V, W)$ are equal, we must show that they take the same values at each point of their domain V. In the case of 8), this amounts to checking that $(a\,(T_1 + T_2))(\mathbf{v}) = (a\,T_1 + a\,T_2)(\mathbf{v})$ for all $\mathbf{v} \in V$.

Suppose $\mathbf{v} \in V$. Then

$$\begin{aligned}(a\,(T_1 + T_2))(\mathbf{v}) &= a(T_1 + T_2)(\mathbf{v}) \\ &= a(T_1(\mathbf{v}) + T_2(\mathbf{v})) \\ &= aT_1(\mathbf{v}) + aT_2(\mathbf{v}) \\ &= (aT_1)(\mathbf{v}) + (aT_2)(\mathbf{v}) \\ &= (aT_1 + aT_2)(\mathbf{v}).\end{aligned}$$

Therefore, we have $a(T_1 + T_2) = a\,T_1 + a\,T_2$ as desired. The other conditions are left as an exercise. □

Example 2.2.4 (Duals and linear forms). We know that K is a vector space over K Therefore, for any vector space V, the set $\mathcal{L}_K(V, K)$ of linear maps from V to K is a vector space over K. We call in the *dual* of V and denote it V^*. An element of V^* is called a *linear form* on V.

Exercises.

2.2.1. Complete the proof of Proposition 2.2.1 by showing that cT_1 is a linear map.

2.2.2. Complete (more of) the proof of Theorem 2.2.3 by showing that conditions 3), 6) and 7) are satisfied.

2.2.3. Let n be a positive integer. Show that, for $i = 1, \ldots, n$, the function

$$\begin{array}{rccc} f_i : & K^n & \longrightarrow & K \\ & \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto & x_i \end{array}$$

is an element of the dual $(K^n)^*$ of K, and that $\{f_1, \ldots, f_n\}$ is a basis of $(K^n)^*$.

2.3 Composition

Let U, V and W be vector spaces over a field K. Recall that if $S\colon U \to V$ and $T\colon V \to W$ are linear maps, then their composition $T \circ S\colon U \to W$, given by

$$(T \circ S)(\mathbf{u}) = T(S(\mathbf{u})) \quad \text{for all } \mathbf{u} \in U,$$

is also a linear map. In what follows, we will use the fact that composition is distributive over addition and that it "commutes" with scalar multiplication as the following proposition indicates.

Proposition 2.3.1. *Suppose* $S, S_1, S_2 \in \mathcal{L}_K(U, V)$ *and* $T, T_1, T_2 \in \mathcal{L}_K(V, W)$*, and* $c \in K$*. We have*

(i) $(T_1 + T_2) \circ S = T_1 \circ S + T_2 \circ S$,

(ii) $T \circ (S_1 + S_2) = T \circ S_1 + T \circ S_2$,

(iii) $(cT) \circ S = T \circ (cS) = cT \circ S$.

Proof of (i). For all $\mathbf{u} \in U$, we have

$$\begin{aligned}((T_1 + T_2) \circ S)(\mathbf{u}) &= (T_1 + T_2)(S(\mathbf{u})) \\ &= T_1(S(\mathbf{u})) + T_2(S(\mathbf{u})) \\ &= (T_1 \circ S)(\mathbf{u}) + (T_2 \circ S)(\mathbf{u}) \\ &= (T_1 \circ S + T_2 \circ S)(\mathbf{u}) \,.\end{aligned}$$

The proofs of *(ii)* and *(iii)* are similar. □

Let $T\colon V \to W$ be a linear map. Recall that, if T is bijective, then the inverse function $T^{-1}\colon W \to V$ defined by

$$T^{-1}(\mathbf{w}) = \mathbf{u} \quad \Longleftrightarrow \quad T(\mathbf{u}) = \mathbf{w}$$

is also a linear map. It satisfies

$$T^{-1} \circ T = I_V \quad \text{and} \quad T \circ T^{-1} = I_W$$

where $I_V : \begin{array}{ccc} V & \to & V \\ \mathbf{v} & \mapsto & \mathbf{v} \end{array}$ and $I_W : \begin{array}{ccc} W & \to & W \\ \mathbf{w} & \mapsto & \mathbf{w} \end{array}$ denote the identity maps on V and W respectively.

Definition 2.3.2 (Invertible). We say that a linear map $T\colon V \to W$ is *invertible* if there exists a linear map $S\colon W \to V$ such that

$$S \circ T = I_V \quad \text{and} \quad T \circ S = I_W \,. \tag{2.1}$$

The preceding observations show that if T is bijective, then it is invertible. On the other hand, if T is invertible and $S\colon W \to V$ satisfies (2.1), then T is bijective and $S = T^{-1}$. An invertible linear map is thus nothing more than a bijective linear map. We recall the following fact:

Proposition 2.3.3. *Suppose that* $S\colon U \to V$ *and* $T\colon V \to W$ *are invertible linear maps. Then* U, V, W *have the same dimension (finite or infinite). Furthermore,*

(i) $T^{-1}\colon W \to V$ *is invertible and* $(T^{-1})^{-1} = T$*, and*

(ii) $T \circ S : U \to W$ *is invertible and* $(T \circ S)^{-1} = S^{-1} \circ T^{-1}$.

An invertible linear map is also called an *isomorphism*. We say that V is *isomorphic* to W and we write $V \simeq W$, if there exists an isomorphism from V to W. We can easily verify that

(i) $V \simeq V$,

(ii) $V \simeq W \iff W \simeq V$,

(iii) if $U \simeq V$ and $V \simeq W$, then $U \simeq W$.

Thus isomorphism is an equivalence relation on the class of vector spaces over K.

The following result shows that, for each integer $n \geq 1$, every vector space of dimension n over K is isomorphic to K^n.

Proposition 2.3.4. *Let* $n \in \mathbb{N}_{>0}$*, let* V *be a vector space over* K *of dimension* n*, and let* $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *be a basis of* V*. The map*

$$\begin{array}{rccc} \varphi : & V & \longrightarrow & K^n \\ & \mathbf{v} & \longmapsto & [\mathbf{v}]_{\mathcal{B}} \end{array}$$

is an isomorphism of vector spaces over K*.*

Proof. To prove this, we first show that φ is linear (exercise). The fact that φ is bijective follows directly from Proposition 1.3.6. □

Exercises.

2.3.1. Prove Part (iii) of Proposition 2.3.1.

2.3.2. Let V and W be vector spaces over a field K and let $T\colon V \to W$ be a linear map. Show that the function $T^*\colon W^* \to V^*$ defined by $T^*(f) = f \circ T$ for all $f \in W^*$ is a linear map (see Example 2.2.4 for the definitions of V^* and W^*). We say that T^* is the *linear map dual to* T.

2.4 Matrices associated to linear maps

In this section, U, V and W denote vector spaces over the same field K.

Proposition 2.4.1. *Let $T\colon V \to W$ be a linear map. Suppose that $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis of V and that $\mathcal{D} = \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ is a basis of W. Then there exists a unique matrix in $\mathrm{Mat}_{m\times n}(K)$, denoted $[\,T\,]_{\mathcal{D}}^{\mathcal{B}}$, such that*

$$[T(\mathbf{v})]_{\mathcal{D}} = [\,T\,]_{\mathcal{D}}^{\mathcal{B}}\,[\mathbf{v}]_{\mathcal{B}} \quad \textit{for all} \quad \mathbf{v} \in V.$$

This matrix is given by

$$[\,T\,]_{\mathcal{D}}^{\mathcal{B}} = \Big([T(\mathbf{v}_1)]_{\mathcal{D}} \cdots [T(\mathbf{v}_n)]_{\mathcal{D}}\Big),$$

that is, the j-th column of $[\,T\,]_{\mathcal{D}}^{\mathcal{B}}$ is $[T(\mathbf{v}_j)]_{\mathcal{D}}$.

Try to prove this without looking at the argument below. It's a good exercise!

Proof. 1$^{\mathbf{st}}$ **Existence:** Let $\mathbf{v} \in V$. Write

$$[\mathbf{v}]_{\mathcal{B}} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

By definition, this means that $\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$, thus

$$T(\mathbf{v}) = a_1T(\mathbf{v}_1) + \cdots + a_nT(\mathbf{v}_n).$$

Since the map $\begin{array}{ccc} W & \to & K^n \\ \mathbf{w} & \mapsto & [\mathbf{w}]_{\mathcal{D}} \end{array}$ is linear (see Proposition 2.3.4), we see that

$$\begin{aligned} [T(\mathbf{v})]_{\mathcal{D}} &= a_1[T(\mathbf{v}_1)]_{\mathcal{D}} + \cdots + a_n[T(\mathbf{v}_n)]_{\mathcal{D}} \\ &= \Big([T(\mathbf{v}_1)]_{\mathcal{D}} \cdots [T(\mathbf{v}_n)]_{\mathcal{D}}\Big) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \\ &= [\,T\,]_{\mathcal{D}}^{\mathcal{B}}[\mathbf{v}]_{\mathcal{B}}. \end{aligned}$$

2$^{\mathbf{nd}}$ **Uniqueness:** If a matrix $M \in \mathrm{Mat}_{m\times n}(K)$ satisfies $[T(\mathbf{v})]_{\mathcal{D}} = M[\mathbf{v}]_{\mathcal{B}}$ for all $\mathbf{v} \in V$, then, for $j = 1, \dots, n$, we have

$$\begin{aligned} [T(\mathbf{v}_j)]_{\mathcal{D}} = M[\mathbf{v}_j]_{\mathcal{B}} = M \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} &\leftarrow j\text{-th row} \\ = j\text{-th column of } M. \end{aligned}$$

Therefore $M = [\,T\,]_{\mathcal{D}}^{\mathcal{B}}$. $\square$

Example 2.4.2. Let $M \in \mathrm{Mat}_{m\times n}(K)$ and let

$$\begin{array}{rccc} T_M : & K^n & \longrightarrow & K^n \\ & X & \longmapsto & M\,X \end{array}$$

be the linear map associated to the matrix M (see Example 2.1.3). Let $\mathcal{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be the standard basis of K^n and $\mathcal{F} = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ the standard basis of K^m. For all $X \in K^n$ and $Y \in K^m$, we have

$$[X]_{\mathcal{E}} = X \quad \text{and} \quad [Y]_{\mathcal{F}} = Y$$

(see Example 1.3.7), thus

$$[T_M(X)]_{\mathcal{F}} = [MX]_{\mathcal{F}} = MX = M[X]_{\mathcal{E}}.$$

From this we conclude that

$$[T_M]_{\mathcal{F}}^{\mathcal{E}} = M,$$

that is, M is the matrix of T_M relative to the standard bases of K^n and K^m.

Theorem 2.4.3. *In the notation of Proposition 2.4.1, the function*

$$\begin{array}{rcl} \mathcal{L}_K(V,W) & \longrightarrow & \mathrm{Mat}_{m\times n}(K) \\ T & \longmapsto & [\,T\,]_{\mathcal{D}}^{\mathcal{B}} \end{array}$$

is an isomorphism of vector spaces over K.

Proof. $1^{\mathbf{st}}$ We show that this map in linear. For this, we choose arbitrary $T_1, T_2 \in \mathcal{L}_K(V,W)$ and $c \in K$. We need to check that

1) $[T_1 + T_2]_{\mathcal{D}}^{\mathcal{B}} = [T_1]_{\mathcal{D}}^{\mathcal{B}} + [T_2]_{\mathcal{D}}^{\mathcal{B}}$,
2) $[cT_1]_{\mathcal{D}}^{\mathcal{B}} = c\,[T_1]_{\mathcal{D}}^{\mathcal{B}}$.

To show 1), we note that, for all $\mathbf{v} \in V$, we have

$$\begin{aligned} [(T_1 + T_2)(\mathbf{v})]_{\mathcal{D}} &= [T_1(\mathbf{v}) + T_2(\mathbf{v})]_{\mathcal{D}} \\ &= [T_1(\mathbf{v})]_{\mathcal{D}} + [T_2(\mathbf{v})]_{\mathcal{D}} \\ &= [T_1]_{\mathcal{D}}^{\mathcal{B}}[\mathbf{v}]_{\mathcal{B}} + [T_1]_{\mathcal{D}}^{\mathcal{B}}[\mathbf{v}]_{\mathcal{B}} \\ &= ([T_1]_{\mathcal{D}}^{\mathcal{B}} + [T_2]_{\mathcal{D}}^{\mathcal{B}})[\mathbf{v}]_{\mathcal{B}}. \end{aligned}$$

Then 1) follows from the uniqueness of the matrix associated to $T_1 + T_2$. The proof of 2) is similar.

$2^{\mathbf{nd}}$ It remains to show that the function is bijective. Proposition 2.4.1 implies that it is injective. To show that it is surjective, we choose an arbitrary matrix $M \in \mathrm{Mat}_{m\times n}(K)$. We need to show that there exists $T \in \mathcal{L}_K(V,W)$ such that $[\,T\,]_{\mathcal{D}}^{\mathcal{B}} = M$. To do this, we consider the linear map

$$\begin{array}{rccc} T_M : & K^n & \longrightarrow & K^n \\ & X & \longmapsto & M\,X \end{array}$$

associated to M. Proposition 2.3.4 implies that the maps

$$\begin{array}{rccc} \varphi : & V & \longrightarrow & K^n \\ & \mathbf{v} & \longmapsto & [\mathbf{v}]_{\mathcal{B}} \end{array} \qquad \text{and} \qquad \begin{array}{rccc} \psi : & W & \longrightarrow & K^m \\ & \mathbf{w} & \longmapsto & [\mathbf{w}]_{\mathcal{D}} \end{array}$$

are isomorphisms. Thus the composition

$$T = \psi^{-1} \circ T_M \circ \varphi \colon V \longrightarrow W$$

is a linear map, that is, an element of $\mathcal{L}_K(V, W)$. For all $\mathbf{v} \in V$, we have

$$[T(\mathbf{v})]_{\mathcal{D}} = \psi(T(\mathbf{v})) = (\psi \circ T)(\mathbf{v}) = (T_M \circ \varphi)(\mathbf{v}) = T_M(\varphi(\mathbf{v})) = T_M([\mathbf{v}]_{\mathcal{B}}) = M[\mathbf{v}]_{\mathcal{B}},$$

and so $M = [\,T\,]_{\mathcal{D}}^{\mathcal{B}}$, as desired. □

Corollary 2.4.4. *If* $\dim_K(V) = n$ *and* $\dim_K(W) = m$*, then* $\dim_K \mathcal{L}_K(V, W) = mn$*.*

Proof. Since $\mathcal{L}_K(V, W) \simeq \mathrm{Mat}_{m\times n}(K)$, we have

$$\dim_K \mathcal{L}_K(V, W) = \dim_K \mathrm{Mat}_{m\times n}(K) = mn.$$ □

Example 2.4.5. If V is a vector space of dimension n, it follows from Corollary 2.4.4 that its dual $V^* = \mathcal{L}_K(V, K)$ has dimension $n \cdot 1 = n$ (see Example 2.2.4 for the notion of the dual of V). Also, the vector space $\mathcal{L}_K(V, V)$ of maps from V to itself has dimension $n \cdot n = n^2$.

Proposition 2.4.6. *Let* $S \colon U \to V$ *and* $T \colon V \to W$ *be linear maps. Suppose that* U*,* V*,* W *are finite dimensional, and that* $\mathcal{A}$*,* $\mathcal{B}$ *and* $\mathcal{D}$ *are bases of* U*,* V *and* W *respectively. Then we have*

$$[T \circ S]_{\mathcal{D}}^{\mathcal{A}} = [T]_{\mathcal{D}}^{\mathcal{B}}\, [S]_{\mathcal{B}}^{\mathcal{A}}\,.$$

Proof. For all $\mathbf{u} \in U$, we have

$$[T \circ S(\mathbf{u})]_{\mathcal{D}} = [T(S(\mathbf{u}))]_{\mathcal{D}} = [\,T\,]_{\mathcal{D}}^{\mathcal{B}}[S(\mathbf{u})]_{\mathcal{B}} = [\,T\,]_{\mathcal{D}}^{\mathcal{B}} \left([S]_{\mathcal{B}}^{\mathcal{A}}\, [\mathbf{u}]_{\mathcal{A}}\right) = \left([\,T\,]_{\mathcal{D}}^{\mathcal{B}}\, [S]_{\mathcal{B}}^{\mathcal{A}}\right) [\mathbf{u}]_{\mathcal{A}}.$$

□

Corollary 2.4.7. *Let* $T \colon V \to W$ *be a linear map. Suppose that* V *and* W *are of finite dimension* n *and that* $\mathcal{B}$ *and* $\mathcal{D}$ *are bases of* V *and* W *respectively. Then* T *is invertible if and only if the matrix* $[\,T\,]_{\mathcal{D}}^{\mathcal{B}} \in \mathrm{Mat}_{n\times n}(K)$ *is invertible, in which case we have*

$$[T^{-1}]_{\mathcal{B}}^{\mathcal{D}} = \left([\,T\,]_{\mathcal{D}}^{\mathcal{B}}\right)^{-1}.$$

Proof. If T is invertible, we have

$$T \circ T^{-1} = I_W \quad \text{and} \quad T^{-1} \circ T = I_V,$$

and so

$$\begin{array}{rrcccccc} & I_n & = & [\,I_W\,]_{\mathcal{D}}^{\mathcal{D}} & = & [T \circ T^{-1}]_{\mathcal{D}}^{\mathcal{D}} & = & [\,T\,]_{\mathcal{D}}^{\mathcal{B}}[T^{-1}]_{\mathcal{B}}^{\mathcal{D}} \\ \text{and} & I_n & = & [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}} & = & [T^{-1} \circ T]_{\mathcal{B}}^{\mathcal{B}} & = & [T^{-1}]_{\mathcal{B}}^{\mathcal{D}}[\,T\,]_{\mathcal{D}}^{\mathcal{B}}. \end{array}$$

Thus $[\,T\,]_{\mathcal{D}}^{\mathcal{B}}$ is invertible and its inverse is $[T^{-1}]_{\mathcal{B}}^{\mathcal{D}}$.

Conversely, if $[\,T\,]_{\mathcal{D}}^{\mathcal{B}}$ is invertible, there exists a linear map $S\colon W \to V$ such that $[S]_{\mathcal{B}}^{\mathcal{D}} = \left([\,T\,]_{\mathcal{D}}^{\mathcal{B}}\right)^{-1}$. We have

$$\begin{array}{rrclclcl} & [T \circ S]_{\mathcal{D}}^{\mathcal{D}} & = & [\,T\,]_{\mathcal{D}}^{\mathcal{B}}\,[\,S\,]_{\mathcal{B}}^{\mathcal{D}} & = & I_n & = & [\,I_W\,]_{\mathcal{D}}^{\mathcal{D}} \\ \text{and} & [S \circ T]_{\mathcal{B}}^{\mathcal{B}} & = & [\,S\,]_{\mathcal{B}}^{\mathcal{D}}\,[\,T\,]_{\mathcal{D}}^{\mathcal{B}} & = & I_n & = & [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}}, \end{array}$$

thus $T \circ S = I_W$ and $S \circ T = I_V$. Therefore T is invertible and its inverse is $T^{-1} = S$. □

2.5 Change of coordinates

We first recall the notion of a change of coordinates matrix.

Proposition 2.5.1. *Let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $\mathcal{B}' = \{\mathbf{v}'_1, \ldots, \mathbf{v}'_n\}$ be two bases of the same vector space V of dimension n over K. There exists a unique invertible matrix $P \in \mathrm{Mat}_{n\times n}(K)$ such that*

$$[\mathbf{v}]_{\mathcal{B}'} = P[\mathbf{v}]_{\mathcal{B}}$$

for all $\mathbf{v} \in V$. This matrix is given by

$$P = [\,I_V\,]_{\mathcal{B}'}^{\mathcal{B}} = \Big([\mathbf{v}_1]_{\mathcal{B}'} \cdots [\mathbf{v}_n]_{\mathcal{B}'}\Big)$$

that is, the j-th column of P is $[\mathbf{v}_j]_{\mathcal{B}'}$ for $j = 1, \ldots, n$. Its inverse is

$$P^{-1} = [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}'} = \Big([\mathbf{v}'_1]_{\mathcal{B}} \cdots [\mathbf{v}'_n]_{\mathcal{B}}\Big).$$

Proof. Since the identity map I_V on V is linear, Proposition 2.4.1 implies that there exists a unique matrix $P \in \mathrm{Mat}_{n\times n}(K)$ such that

$$[\mathbf{v}]_{\mathcal{B}'} = [\,I_V(\mathbf{v})\,]_{\mathcal{B}'} = P\,[\mathbf{v}]_{\mathcal{B}}$$

for all $\mathbf{v} \in V$. This matrix is

$$P = [\,I_V\,]_{\mathcal{B}'}^{\mathcal{B}} = \Big([\,I_V(\mathbf{v}_1)]_{\mathcal{B}'} \cdots [\,I_V(\mathbf{v}_n)]_{\mathcal{B}'}\Big) = \Big([\mathbf{v}_1]_{\mathcal{B}'} \cdots [\mathbf{v}_n]_{\mathcal{B}'}\Big).$$

Also, since I_V is invertible, equal to its own inverse, Corollary 2.4.7 gives

$$P^{-1} = [\,I_V^{-1}\,]_{\mathcal{B}}^{\mathcal{B}'} = [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}'}.$$ □

The matrix P is called the *change of coordinates matrix from basis $\mathcal{B}$ to basis $\mathcal{B}'$*..

Example 2.5.2. The set $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right\}$ is a basis of $\mathbb{R}^2$ since its cardinality is $|\mathcal{B}| = 2 = \dim_{\mathbb{R}} \mathbb{R}^2$ and $\mathcal{B}$ consists of linearly independent vectors. For the same reason, $\mathcal{B}' = \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$ is also a basis of $\mathbb{R}^2$. We see that

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} = -2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + 3 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ 3 \end{pmatrix} = -3 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + 4 \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

thus

$$[\, I_{\mathbb{R}^2}]_{\mathcal{B}'}^{\mathcal{B}} = \left(\left[\begin{pmatrix} 1 \\ 2 \end{pmatrix} \right]_{\mathcal{B}'}, \left[\begin{pmatrix} 1 \\ 3 \end{pmatrix} \right]_{\mathcal{B}'} \right) = \begin{pmatrix} -2 & -3 \\ 3 & 4 \end{pmatrix}$$

and so

$$[\mathbf{v}]_{\mathcal{B}'} = \begin{pmatrix} -2 & -3 \\ 3 & 4 \end{pmatrix} [\mathbf{v}]_{\mathcal{B}}$$

for all $\mathbf{v} \in \mathbb{R}^2$.

We can also do this calculation using the standard basis $\mathcal{E} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ of $\mathbb{R}^2$ as an intermediary. Since $I_{\mathbb{R}^2} = I_{\mathbb{R}^2} \circ I_{\mathbb{R}^2}$, we see that

$$\begin{aligned} [\, I_{\mathbb{R}^2}]_{\mathcal{B}'}^{\mathcal{B}} &= [\, I_{\mathbb{R}^2}]_{\mathcal{B}'}^{\mathcal{E}} \, [\, I_{\mathbb{R}^2}]_{\mathcal{E}}^{\mathcal{B}} \\ &= \left([\, I_{\mathbb{R}^2}]_{\mathcal{E}}^{\mathcal{B}'} \right)^{-1} \left([\, I_{\mathbb{R}^2}]_{\mathcal{E}}^{\mathcal{B}} \right) \\ &= \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} -2 & -3 \\ 3 & 4 \end{pmatrix}. \end{aligned}$$

The second method used in the above example can be generalized as follows:

Proposition 2.5.3. *If $\mathcal{B}, \mathcal{B}'$ and $\mathcal{B}''$ are three bases of the same vector space V, we have*

$$[\, I_V]_{\mathcal{B}''}^{\mathcal{B}} = [\, I_V]_{\mathcal{B}''}^{\mathcal{B}'} \, [\, I_V]_{\mathcal{B}'}^{\mathcal{B}}.$$

Change of basis matrices also allow us to relate the matrices of a linear map $T \colon V \to W$ with respect to different choices of bases for V and W.

Proposition 2.5.4. *Let $T \colon V \to W$ be a linear map. Suppose that $\mathcal{B}$ and $\mathcal{B}'$ are bases of V and that $\mathcal{D}$ and $\mathcal{D}'$ are bases of W. Then we have*

$$[\, T]_{\mathcal{D}'}^{\mathcal{B}'} = [\, I_W]_{\mathcal{D}'}^{\mathcal{D}} \, [\, T]_{\mathcal{D}}^{\mathcal{B}} \, [\, I_V]_{\mathcal{B}}^{\mathcal{B}'}.$$

Proof. To see this, it suffices to write $T = I_W \circ T \circ I_V$ and apply Proposition 2.4.6. □

We conclude by recalling the following result whose proof is left as an exercise, and which provides a useful complement to Proposition 2.5.1.

Proposition 2.5.5. *Let V be a vector space over K of finite dimension n, let $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V, and let $\mathcal{B}' = \{\mathbf{v}'_1, \dots, \mathbf{v}'_n\}$ be a set of n elements of V. Then $\mathcal{B}'$ is a basis of V if and only if the matrix*

$$P = \Big([\mathbf{v}'_1]_{\mathcal{B}} \cdots [\mathbf{v}'_n]_{\mathcal{B}} \Big)$$

is invertible.

2.6 Endomorphisms and invariant subspaces

A linear map $T\colon V \to V$ from a vector space V to itself is called an *endomorphism* of V, or a *linear operator* on V. We denote by

$$\mathrm{End}_K(V) := \mathcal{L}_K(V, V)$$

the set of endomorphisms of V. By Theorem 2.2.3, this is a vector space over K.

Suppose that V has finite dimension n and that $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis of V. For every linear operator $T\colon V \to V$, we simply write $[\,T\,]_{\mathcal{B}}$ for the matrix $[\,T\,]_{\mathcal{B}}^{\mathcal{B}}$. With this convention, we have

$$[T(\mathbf{v})]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}}\,[\mathbf{v}]_{\mathcal{B}} \quad \text{for all } \mathbf{v} \in V.$$

Theorem 2.4.3 tells us that we have an isomorphism of vector spaces

$$\begin{array}{rcl} \mathrm{End}_K(V) & \longrightarrow & \mathrm{Mat}_{n\times n}(K)\,. \\ T & \longmapsto & [\,T\,]_{\mathcal{B}} \end{array}$$

This implies:

$$\dim_K(\mathrm{End}_K(V)) = \dim_K(\mathrm{Mat}_{n\times n}(K)) = n^2.$$

Furthermore, if T_1 and T_2 are two linear operators on V and if $c \in K$, then we have:

$$[T_1 + T_2]_{\mathcal{B}} = [T_1]_{\mathcal{B}} + [T_2]_{\mathcal{B}} \quad \text{and} \quad [c\,T_1]_{\mathcal{B}} = c\,[T_1]_{\mathcal{B}}.$$

The composite $T_1 \circ T_2\colon V \to V$ is also a linear operator on V and Proposition 2.4.6 gives

$$[T_1 \circ T_2]_{\mathcal{B}} = [T_1]_{\mathcal{B}}\,[T_2]_{\mathcal{B}}.$$

Finally, Propositions 2.5.1 and 2.5.4 tell us that, if $\mathcal{B}'$ is another basis of V, then, for all $T \in \mathrm{End}_K(V)$, we have

$$[\,T\,]_{\mathcal{B}'} = P^{-1}\,[\,T\,]_{\mathcal{B}}\,P$$

where $P = [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}'}$.

As explained in the introduction, one of the principal goals of this course is to give the simplest possible description of an endomorphism of a vector space. This description involves the following notion:

Definition 2.6.1 (Invariant subspace). Let $T \in \mathrm{End}_K(V)$. We say that a subspace U of V is *T-invariant* if

$$T(\mathbf{u}) \in U \quad \text{for all } \mathbf{u} \in U.$$

The proof of the following result is left as an exercise:

Proposition 2.6.2. *Let $T \in \mathrm{End}_K(V)$ and let $U_1, \ldots, U_s$ be T-invariant subspaces of V. Then $U_1 + \cdots + U_s$ and $U_1 \cap \cdots \cap U_s$ are also T-invariant.*

We will now show the following:

Proposition 2.6.3. *Let $T \in \mathrm{End}_K(V)$ and let U be a T-invariant subspace of V. The function*

$$\begin{array}{rccc} T|_U : & U & \longrightarrow & U \\ & \mathbf{u} & \longmapsto & T(\mathbf{u}) \end{array}$$

is a linear map.

We say that $T|_U$ is the *restriction of T to U*. Proposition 2.6.3 tells us that this is a linear operator on U.

Proof. For all $\mathbf{u}_1, \mathbf{u}_2 \in U$ and $c \in K$, we have

$$T|_U(\mathbf{u}_1 + \mathbf{u}_2) = T(\mathbf{u}_1 + \mathbf{u}_2) = T(\mathbf{u}_1) + T(\mathbf{u}_2) = T|_U(\mathbf{u}_1) + T|_U(\mathbf{u}_2),$$

$$T|_U(c\,\mathbf{u}_1) = T(c\,\mathbf{u}_1) = cT(\mathbf{u}_1) = c\,T|_U(\mathbf{u}_1).$$

Thus $T|_U : U \to U$ is indeed linear. □

Finally, the following criterion is useful for determining if a subspace U of V is invariant under an endomorphism of V.

Proposition 2.6.4. *Let $T \in \mathrm{End}_K(V)$ and let $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ be a generating set of a subspace U of V. Then U is T-invariant if and only if $T(\mathbf{u}_i) \in U$ for all $i = 1, \ldots, m$.*

Proof. By definition, if U is T-invariant, we have $T(\mathbf{u}_1), \ldots, T(\mathbf{u}_m) \in U$. Conversely, suppose that $T(\mathbf{u}_i) \in U$ for all $i = 1, \ldots, m$ and choose an arbitrary element $\mathbf{u}$ of U. Since $U = \langle \mathbf{u}_1, \ldots, \mathbf{u}_m \rangle_K$, there exists $a_1, \ldots, a_m \in K$ such that $\mathbf{u} = a_1\,\mathbf{u}_1 + \cdots + a_m\mathbf{u}_m$. Therefore

$$T(\mathbf{u}) = a_1\,T(\mathbf{u}_1) + \cdots + a_m T(\mathbf{u}_m) \in U.$$

Thus U is T-invariant. □

Example 2.6.5. Let $\mathcal{C}_\infty(\mathbb{R})$ be the set of infinitely differentiable functions $f\colon \mathbb{R} \to \mathbb{R}$. The derivative

$$\begin{array}{rccc} D: & \mathcal{C}_\infty(\mathbb{R}) & \longrightarrow & \mathcal{C}_\infty(\mathbb{R}) \\ & f & \longmapsto & f' \end{array}$$

is an $\mathbb{R}$-linear operator on $\mathcal{C}_\infty(\mathbb{R})$. Let U be the subspace of $\mathcal{C}_\infty(\mathbb{R})$ generated by the functions f_1, f_2 and f_3 given by

$$f_1(x) = e^{2x}, \quad f_2(x) = x\, e^{2x}, \quad f_3(x) = x^2\, e^{2x}.$$

For all $x \in \mathbb{R}$, we have

$$\begin{aligned} f_1'(x) &= 2e^x = 2f_1(x), \\ f_2'(x) &= e^{2x} + 2x\, e^{2x} = f_1(x) + 2f_2(x), \\ f_3'(x) &= 2x\, e^{2x} + 2x^2\, e^{2x} = 2f_2(x) + 2f_3(x). \end{aligned}$$

Thus

$$D(f_1) = 2\, f_1, \quad D(f_2) = f_1 + 2\, f_2, \quad D(f_3) = 2\, f_2 + 2\, f_3 \tag{2.2}$$

belong to U and so U is a D-invariant subspace of $\mathcal{C}_\infty(\mathbb{R})$.

The functions f_1, f_2 and f_3 are linearly independent, since if $a_1, a_2, a_3 \in \mathbb{R}$ satisfy $a_1\, f_1 + a_2\, f_2 + a_3\, f_3 = 0$, then we have

$$a_1\, e^{2x} + a_2 x\, e^{2x} + a_3 x^2\, e^{2x} = 0 \quad \text{for all } x \in \mathbb{R}.$$

Since $e^{2x} \neq 0$ for any $x \in \mathbb{R}$, we conclude (by dividing by e^{2x})

$$a_1 + a_2 x + a_3 x^2 = 0 \quad \text{for all } x \in \mathbb{R}$$

and so $a_1 = a_2 = a_3 = 0$ (a nonzero degree 2 polynomial has at most 2 roots). Therefore $\mathcal{B} = \{f_1, f_2, f_3\}$ is a basis of U and the formulas (2.2) yield

$$[D|_U]_{\mathcal{B}} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix}.$$

Combining the above ideas with those of Section 1.4, we obtain:

Theorem 2.6.6. *Let $T\colon V \longrightarrow V$ be a linear operator on a finite dimensional vector space V. Suppose that V is the direct sum of T-invariant subspaces $V_1, \ldots, V_s$. Let $\mathcal{B}_i = \{\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,n_i}\}$ be a basis of V_i for $i = 1, \ldots, s$. Then*

$$\mathcal{B} = \mathcal{B}_1 \amalg \cdots \amalg \mathcal{B}_s = \{\mathbf{v}_{1,1}, \ldots, \mathbf{v}_{1,n_1}, \ \ldots\ldots, \ \mathbf{v}_{s,1}, \ldots, \mathbf{v}_{s,n_s}\}$$

is a basis of V and we have

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} [T|_{V_1}]_{\mathcal{B}_1} & 0 & \cdots & 0 \\ 0 & [T|_{V_2}]_{\mathcal{B}_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & [T|_{V_s}]_{\mathcal{B}_s} \end{pmatrix}, \tag{2.3}$$

that is, the matrix of T relative to the basis $\mathcal{B}$ is block diagonal, the i-th block on the diagonal being the matrix $[T|_{V_i}]_{\mathcal{B}_i}$ of the restriction of T to V_i relative to the basis $\mathcal{B}_i$.

The fact that $\mathcal{B}$ is a basis of V follows from Proposition 1.4.8. We prove Equation (2.3) by induction on s. For $s = 1$, there is nothing to prove. For $s = 2$, it is easier to change notation. It suffices to prove:

Lemma 2.6.7. *Let $T\colon V \to V$ be a linear operator on a finite dimensional vector space V. Suppose that $V = U \oplus W$ where U and W are T-invariant subspaces. Let $\mathcal{A} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ be a basis of U and $\mathcal{D} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ a basis of W. Then*

$$\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n\}$$

is a basis of V and

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} [T|_U]_{\mathcal{A}} & 0 \\ 0 & [T|_W]_{\mathcal{D}} \end{pmatrix}.$$

Proof. Write $[T|_U]_{\mathcal{A}} = (a_{ij})$ and $[T|_W]_{\mathcal{D}} = (b_{ij})$. Then, for $j = 1, \ldots, m$, we have:

$$T(\mathbf{u}_j) = T|_U(\mathbf{u}_j) = a_{1j}\mathbf{u}_1 + \cdots + a_{mj}\mathbf{u}_m \quad \Longrightarrow \quad [T(\mathbf{u}_j)]_{\mathcal{B}} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Similarly, for $j = 1, \ldots, n$, we have:

$$T(\mathbf{w}_j) = T|_W(\mathbf{w}_j) = b_{1j}\mathbf{w}_1 + \cdots + b_{nj}\mathbf{w}_n \quad \Longrightarrow \quad [T(\mathbf{w}_j)]_{\mathcal{B}} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix}.$$

Thus,

$$\begin{aligned} [\,T\,]_{\mathcal{B}} &= \Big([T(\mathbf{u}_1)]_{\mathcal{B}}, \ldots, [T(\mathbf{u}_m)]_{\mathcal{B}}, [T(\mathbf{w}_1)]_{\mathcal{B}}, \ldots, [T(\mathbf{w}_n)]_{\mathcal{B}}\Big) \\ &= \begin{pmatrix} a_{11} & \cdots & a_{1m} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & b_{n1} & \cdots & b_{nn} \end{pmatrix} \\ &= \begin{pmatrix} [T|_U]_{\mathcal{A}} & 0 \\ 0 & [T|_W]_{\mathcal{D}} \end{pmatrix} \end{aligned}$$

□

Proof of Theorem 2.6.6. As explained above, it suffices to prove (2.3). The case where $s = 1$ is clear. Now suppose that $s \leq 2$ and that the result holds for all values less than s. The hypotheses of Lemma 2.6.7 are fulfilled for the choices

$$U := V_1, \quad \mathcal{A} := \mathcal{B}_1, \quad W := V_2 \oplus \cdots \oplus V_s \quad \text{and} \quad \mathcal{D} := \mathcal{B}_2 \amalg \cdots \amalg \mathcal{B}_s.$$

Thus we have

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} [T|_{V_1}]_{\mathcal{B}_1} & 0 \\ 0 & [T|_W]_{\mathcal{D}} \end{pmatrix}.$$

Since $W = V_2 \oplus \cdots \oplus V_s$ is a direct sum of $s-1$ $T|_W$-invariant subspaces, the induction hypothesis gives

$$[\,T|_W\,]_{\mathcal{D}} = \begin{pmatrix} [T|_{V_2}]_{\mathcal{B}_2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [T|_{V_s}]_{\mathcal{B}_s} \end{pmatrix},$$

since $(T|_W)|_{V_i} = T|_{V_i}$ for $i = 2, \ldots, s$. The result follows. □

Exercises.

2.6.1. Prove Proposition 2.6.2.

2.6.2. Let V be a vector space over a field K and let S and T be commuting linear operators on V (i.e. such that $S \circ T = T \circ S$). Show that $\ker(S)$ and $\operatorname{Im}(S)$ are T-invariant subspaces of V.

2.6.3. Let D be the linear operator of differentiation on the space $C_\infty(\mathbb{R})$ of infinitely differentiable functions $f\colon \mathbb{R} \to \mathbb{R}$. Consider the vector subspace $U = \langle\, 1, x, \ldots, x^m \,\rangle_{\mathbb{R}}$ of $C_\infty(\mathbb{R})$ for an integer $m \geq 0$.

(i) Show that U is D-invariant.

(ii) Show that $\mathcal{B} = \{1, x, \ldots, x^m\}$ is a basis of U.

(iii) Calculate $[\,D|_U\,]_{\mathcal{B}}$.

2.6.4. Let D be as in Exercise 2.6.3, and let $U = \langle\, \cos(3x), \sin(3x), x\cos(3x), x\sin(3x) \,\rangle_{\mathbb{R}}$.

(i) Show that U is D-invariant.

(ii) Show that $\mathcal{B} = \{\cos(3x), \sin(3x), x\cos(3x), x\sin(3x)\}$ is a basis of U.

(iii) Calculate $[\,D|_U\,]_{\mathcal{B}}$.

2.6.5. Let V be a vector space of dimension 4 over $\mathbb{Q}$, let $\mathcal{A} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ be a basis of V, and let $T\colon V \to V$ be the linear map determined by the conditions

$$\begin{aligned} T(\mathbf{v}_1) &= \mathbf{v}_1 + \mathbf{v}_2 + 2\mathbf{v}_3, & T(\mathbf{v}_2) &= \mathbf{v}_1 + \mathbf{v}_2 + 2\mathbf{v}_4, \\ T(\mathbf{v}_3) &= \mathbf{v}_1 - 3\mathbf{v}_2 + \mathbf{v}_3 - \mathbf{v}_4, & T(\mathbf{v}_4) &= -3\mathbf{v}_1 + \mathbf{v}_2 - \mathbf{v}_3 + \mathbf{v}_4. \end{aligned}$$

(i) Show that $\mathcal{B}_1 = \{\mathbf{v}_1 + \mathbf{v}_2,\ \mathbf{v}_3 + \mathbf{v}_4\}$ and $\mathcal{B}_2 = \{\mathbf{v}_1 - \mathbf{v}_2,\ \mathbf{v}_3 - \mathbf{v}_4\}$ are bases (respectively) of T-invariant subspaces V_1 and V_2 of V such that $V = V_1 \oplus V_2$.

(ii) Calculate $[\,T|_{V_1}\,]_{\mathcal{B}_1}$ and $[\,T|_{V_2}\,]_{\mathcal{B}_2}$. Then find $[\,T\,]_{\mathcal{B}}$, where $\mathcal{B} = \mathcal{B}_1 \coprod \mathcal{B}_2$.

2.6.6. Let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the linear map whose matrix relative to the standard basis $\mathcal{E}$ of $\mathbb{R}^3$ is

$$[\,T\,]_{\mathcal{E}} = \begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}.$$

(i) Show that $\mathcal{B}_1 = \{(1,1,1)^t\}$ and $\mathcal{B}_2 = \{(1,-1,0)^t,\ (0,1,-1)^t\}$ are bases (respectively) of T-invariant subspaces V_1 and V_2 of $\mathbb{R}^3$ such that $\mathbb{R}^3 = V_1 \oplus V_2$.

(ii) Calculate $[\,T|_{V_1}\,]_{\mathcal{B}_1}$ and $[\,T|_{V_2}\,]_{\mathcal{B}_2}$, and deduce $[\,T\,]_{\mathcal{B}}$, where $\mathcal{B} = \mathcal{B}_1 \coprod \mathcal{B}_2$.

2.6.7. Let V be a finite dimensional vector space over a field K, let $T\colon V \to V$ be an endomorphism of V, and let $n = \dim_K(V)$. Suppose that there exists an integer $m \geq 0$ and a vector $\mathbf{v} \in V$ such that $V = \langle\, \mathbf{v}, T(\mathbf{v}), T^2(\mathbf{v}), \ldots, T^m(\mathbf{v})\,\rangle_K$. Show that $\mathcal{B} = \{\mathbf{v}, T(\mathbf{v}), \ldots, T^{n-1}(\mathbf{v})\}$ is a basis of V and that there exist $a_0, \ldots, a_{n-1} \in K$ such that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}.$$

Note. We say that a vector spacel V with the above property is T-*cyclic*, or simply *cyclic*.

The last three exercises give examples of the general situation discussed in Exercise 2.6.7.

2.6.8. Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map whose matrix in the standard basis $\mathcal{E}$ is

$$[\,T\,]_{\mathcal{E}} = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}.$$

(i) Let $\mathbf{v} = (1,1)^t$. Show that $\mathcal{B} = \{\mathbf{v}, T(\mathbf{v})\}$ is a basis of $\mathbb{R}^2$.

(ii) Determine $[T^2(\mathbf{v})]_{\mathcal{B}}$.

(iii) Calculate $[\,T\,]_{\mathcal{B}}$.

2.6.9. Let V be a vector space of dimension 3 over $\mathbb{Q}$, let $\mathcal{A} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ be a basis of V, and let $T\colon V \to V$ be the linear map determined by the conditions

$$T(\mathbf{v}_1) = \mathbf{v}_1 + \mathbf{v}_3, \quad T(\mathbf{v}_2) = \mathbf{v}_1 - \mathbf{v}_2 \quad \text{and} \quad T(\mathbf{v}_3) = \mathbf{v}_2.$$

(i) Find $[\,T\,]_{\mathcal{A}}$.

(ii) Show that $\mathcal{B} = \{\mathbf{v}_1, T(\mathbf{v}_1), T^2(\mathbf{v}_1)\}$ is a basis of V.

(iii) Calculate $[\,T\,]_{\mathcal{B}}$.

2.6.10. Let $V = \langle\, 1, e^x, e^{2x} \,\rangle_{\mathbb{R}} \subset \mathcal{C}_\infty(\mathbb{R})$ and let D be the restriction to V of the operator of derivation on $\mathcal{C}_\infty(\mathbb{R})$. Then $\mathcal{A} = \{1, e^x, e^{2x}\}$ is a basis of V (you do not need to show this).

(i) Let $f(x) = 1 + e^x + e^{2x}$. Show that $\mathcal{B} = \{\, f,\ D(f),\ D^2(f)\,\}$ is a basis of V.

(ii) Calculate $[\,D\,]_{\mathcal{B}}$.

Chapter 3

Review of diagonalization

In this chapter, we recall how to determine if a linear operator or a square matrix is diagonalizable and, if so, how to diagonalize it.

3.1 Determinants and similar matrices

Let K be a field. We define the *determinant* of a square matrix $A = (a_{ij}) \in \mathrm{Mat}_{n\times n}(K)$ by

$$\det(A) = \sum_{(j_1,\ldots,j_n)\in S_n} \epsilon(j_1,\ldots,j_n) a_{1j_1}\cdots a_{nj_n}$$

where S_n denotes the set of permutations of $(1,2,\ldots,n)$ and where, for a permutation $(j_1,\ldots,j_n) \in S_n$, the expression $\epsilon(j_1,\ldots,j_n)$ represents the *signature* of $(j_1,\ldots,j_n)$, given by

$$\epsilon(j_1,\ldots,j_n) = (-1)^{N(j_1,\ldots,j_n)}$$

where $N(j_1,\ldots,j_n)$ denotes the number of pairs of indices (k,l) with $1 \leq k < l \leq n$ and $j_k > j_l$ (called the *number of inversions* of $(j_1,\ldots,j_n)$).

Recall that the determinant satisfies the following properties:

Theorem 3.1.1. *Let $n \in \mathbb{N}_{>0}$ and let $A, B \in \mathrm{Mat}_{n\times n}(K)$. Then we have:*

(i) $\det(I) = 1$,

(ii) $\det(A^t) = \det(A)$,

(iii) $\det(AB) = \det(A)\det(B)$,

where I denotes the $n \times n$ identity matrix and A^t denotes the transpose of A. Moreover, the matrix A is invertible if and only if $\det(A) \neq 0$, *in which case*

(iv) $\det(A^{-1}) = \det(A)^{-1}$.

In fact, the above formula for the determinant applies to any square matrix with coefficients in a commutative ring. A proof of Theorem 3.1.1 in the general case, with K replaced by an arbitrary commutative ring, can be found in Appendix B.

The "multiplicative" properties (iii) and (iv) of the determinant imply the following result.

Proposition 3.1.2. *Let T be an endomorphism of a finite dimensional vector space V, and let $\mathcal{B}$, $\mathcal{B}'$ be two bases of V. Then we have*

$$\det[\,T\,]_{\mathcal{B}} = \det[\,T\,]_{\mathcal{B}'}.$$

Proof. We have $[\,T\,]_{\mathcal{B}'} = P^{-1}[\,T\,]_{\mathcal{B}}P$ where $P = [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}'}$, and so

$$\begin{aligned}
\det[\,T\,]_{\mathcal{B}'} &= \det(P^{-1}[\,T\,]_{\mathcal{B}}P) \\
&= \det(P^{-1})\det[\,T\,]_{\mathcal{B}}\det(P) \\
&= \det(P)^{-1}\det[\,T\,]_{\mathcal{B}}\det(P) \\
&= \det[\,T\,]_{\mathcal{B}}.
\end{aligned}$$

□

This allows us to formulate the following:

Definition 3.1.3 (Determinant). Let $T\colon V \to V$ be a linear operator on a finite dimensional vector space V. We define the *determinant* of T by

$$\det(T) = \det[\,T\,]_{\mathcal{B}}$$

where $\mathcal{B}$ denotes an arbitrary basis of V.

Theorem 3.1.1 allows us to study the behavior of the determinant under the composition of linear operators:

Theorem 3.1.4. *Let S and T be linear operators on a finite dimensional vector space V. We have:*

(i) $\det(I_V) = 1$,

(ii) $\det(S \circ T) = \det(S)\det(T)$.

Moreover, T is invertible if and only if $\det(T) \neq 0$, *in which case we have*

(iii) $\det(T^{-1}) = \det(T)^{-1}$.

Proof. Let $\mathcal{B}$ be a basis of V. Since $[\,I_V\,]_{\mathcal{B}} = I$ is the $n \times n$ identity matrix, we have $\det(I_V) = \det(I) = 1$. This proves (i). For (iii), we note, by Corollary 2.4.7, that T is invertible if and only if the matrix $[\,T\,]_{\mathcal{B}}$ is invertible and that, in this case,

$$[\,T^{-1}]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}}^{-1}.$$

This proves (iii). Relation (ii) is left as an exercise. □

Theorem 3.1.4 illustrates the phenomenon mentioned in the introduction that, most of the time in this course, a result about matrices implies a corresponding result about linear operators and vice-versa. We conclude with the following notion:

Definition 3.1.5 (Similarity). Let $n \in \mathbb{N}_{>0}$ and let $A, B \in \mathrm{Mat}_{n\times n}(K)$ be square matrices of the same size $n \times n$. We say that A is *similar* to B (or *conjugate* to B), if there exists an invertible matrix $P \in \mathrm{Mat}_{n\times n}(K)$, such that $B = P^{-1}\,A\,P$. We then write $A \sim B$.

Example 3.1.6. If $T\colon V \to V$ is a linear operator on a finite dimensional vector space V and if $\mathcal{B}$ and $\mathcal{B}'$ are two bases of V, then we have

$$[\,T\,]_{\mathcal{B}'} = P^{-1}\,[\,T\,]_{\mathcal{B}} P$$

where $P = [\,I_V\,]_{\mathcal{B}}^{\mathcal{B}'}$, and so $[\,T\,]_{\mathcal{B}'}$ and $[\,T\,]_{\mathcal{B}}$ are similar.

More precisely, we can show:

Proposition 3.1.7. *Let $T\colon V \to V$ be a linear operator on a finite dimensional vector space V, and let $\mathcal{B}$ be a basis of V. A matrix M is similar to $[\,T\,]_{\mathcal{B}}$ if and only if there exists a basis $\mathcal{B}'$ of V such that $M = [\,T\,]_{\mathcal{B}'}$.*

Finally, Theorem 3.1.1 provides a necessary condition for two matrices to be similar:

Proposition 3.1.8. *If A and B are two similar matrices, then* $\det(A) = \det(B)$.

The proof is left as an exercise. Proposition 3.1.2 can be viewed as a corollary to this result, together with Example 3.1.6.

Exercises.

3.1.1. Show that similarity $\sim$ is an equivalence relation on $\mathrm{Mat}_{n\times n}(K)$.

3.1.2. Prove Proposition 3.1.7.

3.1.3. Prove Proposition 3.1.8.

3.2 Diagonalization of operators

In this section, we fix a vector space V of finite dimension n over a field K and a linear operator $T\colon V \to V$. We say that:

- T is *diagonalizable* if there exists a basis $\mathcal{B}$ of V such that $[\,T\,]_{\mathcal{B}}$ is a diagonal matrix,
- an element λ of K is an *eigenvalue* of T if there exists a *nonzero* vector $\mathbf{v}$ of V such that
$$T(\mathbf{v}) = \lambda\mathbf{v}\,,$$
- a nonzero vector $\mathbf{v}$ that satisfies the above relation for an element λ of K is called an *eigenvector* of T or, more precisely, an *eigenvector of T for the eigenvalue λ*.

We also recall that if $\lambda \in K$ is an eigenvalue of T then the set

$$E_\lambda := \{\mathbf{v} \in V\,;\, T(\mathbf{v}) = \lambda\mathbf{v}\}$$

(also denoted $E_\lambda(T)$) is a subspace of V since, for $\mathbf{v} \in V$, we have

$$T(\mathbf{v}) = \lambda\mathbf{v} \quad\Longleftrightarrow\quad (T - \lambda I)(\mathbf{v}) = \mathbf{0}$$

and so

$$E_\lambda = \ker(T - \lambda I).$$

We way that E_λ is the *eigenspace of T for the eigenvalue λ*. The eigenvectors of T for this eigenvalue are the nonzero elements of E_λ.

For each eigenvalue $\lambda \in K$, the eigenspace E_λ is a T-invariant subspace of V since, if $\mathbf{v} \in E_\lambda$, we have $T(\mathbf{v}) = \lambda\mathbf{v} \in E_\lambda$. Also note that an element $\mathbf{v}$ of V is an eigenvector of T if and only if $\langle\mathbf{v}\rangle_K$ is a T-invariant subspace of V of dimension 1 (exercise).

Proposition 3.2.1. *The operator T is diagonalizable if and only if V admits a basis consisting of eigenvectors of T.*

Proof. Let $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V, and let $\lambda_1, \dots, \lambda_n \in K$. We have

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad\Longleftrightarrow\quad T(\mathbf{v}_1) = \lambda_1\mathbf{v}_1\,,\ \dots\,,\ T(\mathbf{v}_n) = \lambda_n\mathbf{v}_n.$$

The conclusion follows. □

The crucial point is the following result:

Proposition 3.2.2. *Let $\lambda_1, \ldots, \lambda_s \in K$ be distinct eigenvalues of T. The sum $E_{\lambda_1} + \cdots + E_{\lambda_s}$ is direct.*

Proof. In light of Definition 1.4.1, we need to show that the only possible choice of vectors $\mathbf{v}_1 \in E_{\lambda_1}, \ldots, \mathbf{v}_s \in E_{\lambda_s}$ such that

$$\mathbf{v}_1 + \cdots + \mathbf{v}_s = \mathbf{0} \tag{3.1}$$

is $\mathbf{v}_1 = \cdots = \mathbf{v}_s = \mathbf{0}$. We show this by induction on s, noting first that, for $s = 1$, the result is immediate.

Suppose that $s \geq 2$ and that the sum $E_{\lambda_1} + \cdots + E_{\lambda_{s-1}}$ is direct. Choose vectors $\mathbf{v}_1 \in E_{\lambda_1}, \ldots, \mathbf{v}_s \in E_{\lambda_s}$ satisfying (3.1) and apply T to both sides of this equality. Since $T(\mathbf{v}_i) = \lambda_i \mathbf{v}_i$ for $i = 1, \ldots, s$ and $T(\mathbf{0}) = \mathbf{0}$, we get

$$\lambda_1 \mathbf{v}_1 + \cdots + \lambda_s \mathbf{v}_s = \mathbf{0}. \tag{3.2}$$

Subtracting from (3.2) the equality (3.1) multiplied by λ_s, we have

$$(\lambda_1 - \lambda_s)\mathbf{v}_1 + \cdots + (\lambda_{s-1} - \lambda_s)\mathbf{v}_{s-1} = \mathbf{0}.$$

Since $(\lambda_i - \lambda_s)\mathbf{v}_i \in E_{\lambda_i}$ for $i = 1, \ldots, s-1$ and, by hypothesis, the sum $E_{\lambda_1} + \cdots + E_{\lambda_{s-1}}$ is direct, we see that

$$(\lambda_1 - \lambda_s)\mathbf{v}_1 = \cdots = (\lambda_{s-1} - \lambda_s)\mathbf{v}_{s-1} = \mathbf{0}.$$

Finally, since $\lambda_s \neq \lambda_i$ for $i = 1, \ldots, s-1$, we conclude that $\mathbf{v}_1 = \cdots = \mathbf{v}_{s-1} = \mathbf{0}$, hence, by (3.1), that $\mathbf{v}_s = \mathbf{0}$. Therefore the sum $E_{\lambda_1} + \cdots + E_{\lambda_s}$ is direct. □

From this we conclude the following:

Theorem 3.2.3. *The operator T has at most $n = \dim_K(V)$ eigenvalues. Let $\lambda_1, \ldots, \lambda_s$ be the distinct eigenvalues of T in K. Then T is diagonalizable if and only if*

$$\dim_K(V) = \dim_K(E_{\lambda_1}) + \cdots + \dim_K(E_{\lambda_s}).$$

If this is the case, we obtain a basis $\mathcal{B}$ of V consisting of eigenvectors of T by concatenating bases of $E_{\lambda_1}, \ldots, E_{\lambda_s}$ and

$$[T]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & 0 & \\ & & \lambda_1 & & & & \\ & & & \ddots & & & \\ & & & & \lambda_s & & \\ & 0 & & & & \ddots & \\ & & & & & & \lambda_s \end{pmatrix}$$

with each λ_i repeated a number of times equal to $\dim_K(E_{\lambda_i})$.

Proof. First suppose that $\lambda_1, \dots, \lambda_s$ are distinct eigenvalues of T (not necessarily all of them). Then, since the sum $E_{\lambda_1} + \cdots + E_{\lambda_s}$ is direct, we find that

$$\dim_K(E_{\lambda_1} + \cdots + E_{\lambda_s}) = \dim_K(E_{\lambda_1}) + \cdots + \dim_K(E_{\lambda_s}).$$

Since $E_{\lambda_1} + \cdots + E_{\lambda_s} \subseteq V$ and $\dim_K(E_{\lambda_i}) \geq 1$ for $i = 1, \dots, s$, we deduce that

$$n = \dim_K(V) \geq \dim_K(E_{\lambda_1}) + \cdots + \dim_K(E_{\lambda_s}) \geq s.$$

This proves the first statement of the theorem: T has at most n eigenvalues.

Now suppose that $\lambda_1, \dots, \lambda_s$ are all the distinct eigenvalues of T. By propositions 3.2.1, 3.2.2 and Corollary 1.4.9, we see that

$$\begin{aligned} T \text{ is diagonalizable} &\iff V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_s} \\ &\iff n = \dim_K(E_{\lambda_1}) + \cdots + \dim_K(E_{\lambda_s}). \end{aligned}$$

This proves the second assertion of the theorem. The last two follow from Theorem 2.6.6. □

To be able to *diagonalize* T in practice, that is, find a basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}}$ is diagonal, if such a basis exists, it suffices to be able to determine the eigenvalues of T and the corresponding eigenvspaces. Since $E_\lambda = \ker(T - \lambda I)$ for each eigenvalue λ, the problem is reduced to the determination of the eigenvalues of T. To do this, we rely on the following result:

Proposition 3.2.4. *Let $\mathcal{B}$ be a basis of V. The polynomial*

$$\mathrm{char}_T(x) := \det(x\,I - [T]_{\mathcal{B}}) \in K[x]$$

does not depend on the choice of $\mathcal{B}$. The eigenvalues of T are the roots of this polynomial in K.

Before proving this result, we first note that the expression $\det(x\,I - [T]_{\mathcal{B}})$ really is an element of $K[x]$, that is, a polynomial in x with coefficients in K. To see this, write $[T]_{\mathcal{B}} = (a_{ij})$. Then we have

$$\begin{aligned} \det(x\,I - [T]_{\mathcal{B}}) &= \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} \\ &= (x - a_{11})(x - a_{22}) \cdots (x - a_{nn}) + (\text{terms of degree} \leq n - 2) \\ &= x^n - (a_{11} + \cdots + a_{nn})x^{n-1} + \cdots . \end{aligned} \tag{3.3}$$

as can be seen from the formula for the expansion of the determinant reviewed in Section 3.1. This polynomial is called the *characteristic polynomial of T* and is denoted $\mathrm{char}_T(X)$.

Proof of Proposition 3.2.4. Let $\mathcal{B}'$ be another basis of V. We know that

$$[\,T\,]_{\mathcal{B}'} = P^{-1}[\,T\,]_{\mathcal{B}}\,P$$

where $P = [\,I\,]_{\mathcal{B}}^{\mathcal{B}'}$. We thus have

$$xI - [\,T\,]_{\mathcal{B}'} = xI - P^{-1}[\,T\,]_{\mathcal{B}}\,P = P^{-1}(xI - [\,T\,]_{\mathcal{B}})\,P,$$

and so

$$\begin{aligned}\det(xI - [\,T\,]_{\mathcal{B}'}) &= \det\left(P^{-1}(xI - [\,T\,]_{\mathcal{B}})\,P\right)\\ &= \det(P)^{-1}\det(xI - [\,T\,]_{\mathcal{B}})\det(P)\\ &= \det(xI - [\,T\,]_{\mathcal{B}}).\end{aligned} \tag{3.4}$$

This shows that the polynomial $\det(xI - [\,T\,]_{\mathcal{B}})$ is independent of the choice of $\mathcal{B}$. Note that the calculations (3.4) involve matrices with polynomial coefficients in $K[x]$, and the multiplicativity of the determinant for a product of such matrices. This is justified in Appendix B. If the field K if infinite, we can avoid this difficulty by identifying the polynomials in $K[x]$ with polynomial functions from K to K (see Section 4.2).

Finally, let $\lambda \in K$. Be definition, λ is an eigenvalue of T if and only if

$$\begin{aligned}\ker(T - \lambda I) \neq \{\mathbf{0}\} \quad &\Longleftrightarrow \quad \text{there exists } \mathbf{v} \in V \setminus \{\mathbf{0}\} \text{ such that } (T - \lambda\, I)\mathbf{v} = \mathbf{0}\,,\\ &\Longleftrightarrow \quad \text{there exists } X \in K^n \setminus \{\mathbf{0}\} \text{ such that } [\,T - \lambda\, I\,]_{\mathcal{B}}X = \mathbf{0}\,,\\ &\Longleftrightarrow \quad \det([\,T - \lambda\, I\,]_{\mathcal{B}}) = 0\,.\end{aligned}$$

Since $[\,T - \lambda I\,]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}} - \lambda[\,I\,]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}} - \lambda I = -(\lambda I - [\,T\,]_{\mathcal{B}})$, we also have

$$\det([\,T - \lambda I\,]_{\mathcal{B}}) = (-1)^n \mathrm{char}_T(\lambda)\,.$$

Thus the eigenvalues of T are the roots of $\mathrm{char}_T(x)$. □

Corollary 3.2.5. *Let $\mathcal{B}$ be a basis of V. Writes $[\,T\,]_{\mathcal{B}} = (a_{ij})$. Then the number*

$$\mathrm{trace}(T) := a_{11} + a_{22} + \cdots + a_{nn},$$

called the trace *of T, does not depend on the choice of $\mathcal{B}$. We have*

$$\mathrm{char}_T(x) = x^n - \mathrm{trace}(T)\,x^{n-1} + \cdots + (-1)^n\det(T).$$

Proof. The calculations (3.3) show that the coefficient of x^{n-1} in $\det(x\,I - [\,T\,]_{\mathcal{B}})$ is equal to $-(a_{11} + \cdots + a_{nn})$. Since $\mathrm{char}_T(x) = \det(xI - [\,T\,]_{\mathcal{B}})$ does not depend on the choice of $\mathcal{B}$, the sum $a_{11} + \cdots + a_{nn}$ does not depend on it either. This proves the first assertion of the corollary. For the second, it suffices to show that the constant term of $\mathrm{char}_T(x)$ is $(-1)^n\det(T)$. But this coefficient is

$$\mathrm{char}_T(0) = \det(-[\,T\,]_{\mathcal{B}}) = (-1)^n\det([\,T\,]_{\mathcal{B}}) = (-1)^n\det(T).$$

□

Example 3.2.6. With the notation of Example 2.6.5, we set $T = D|_U$ where U is the subspace of $\mathcal{C}_\infty(\mathbb{R})$ generated by the functions $f_1(x) = e^{2x}$, $f_2(x) = x\,e^{2x}$ and $f_3(x) = x^2 e^{2x}$, and where D is the derivative operator on $\mathcal{C}_\infty(\mathbb{R})$. We have seen that $\mathcal{B} = \{f_1, f_2, f_3\}$ is a basis for U and that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix}.$$

The characteristic polynomial of T is therefore

$$\mathrm{char}_T(x) = \det(xI - [\,T\,]_{\mathcal{B}}) = \begin{vmatrix} x-2 & -1 & 0 \\ 0 & x-2 & -2 \\ 0 & 0 & x-2 \end{vmatrix} = (x-2)^3.$$

Since $x = 2$ is the only root of $(x-2)^3$ in $\mathbb{R}$, we see that 2 is the only eigenvalue of T. The eigenspace of T for this eigenvalue is

$$E_2 = \ker(T - 2I).$$

Let $f \in U$. We have

$$\begin{aligned} f \in E_2 &\iff (T-2I)(f) = 0 \iff [\,T-2I\,]_{\mathcal{B}}[f]_{\mathcal{B}} = 0 \iff ([\,T\,]_{\mathcal{B}} - 2I)[f]_{\mathcal{B}} = 0 \\ &\iff \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} [f]_{\mathcal{B}} = 0 \iff [f]_{\mathcal{B}} = \begin{pmatrix} t \\ 0 \\ 0 \end{pmatrix} \text{ with } t \in \mathbb{R} \\ &\iff f = t\,f_1 \quad \text{with } t \in \mathbb{R}\,. \end{aligned}$$

Thus $E_2 = \langle f_1 \rangle_{\mathbb{R}}$ has dimension 1. Since

$$\dim_{\mathbb{R}}(E_2) = 1 \neq 3 = \dim_{\mathbb{R}}(U),$$

Theorem 3.2.3 tells us that T is not diagonalizable.

Exercises.

3.2.1. Let V be a vector space over a field K, let $T\colon V \to V$ be a linear operator on V, and let $\mathbf{v}_1, \ldots, \mathbf{v}_s$ be eigenvectors of T for the distinct eigenvalues $\lambda_1, \ldots, \lambda_s \in K$. Show that $\mathbf{v}_1, \ldots, \mathbf{v}_s$ are linearly independent over K.

Hint. You can, for example, combine Proposition 3.2.2 with Exercise 1.4.3(ii).

3.2.2. Let $V = \langle\, f_0, f_1, \ldots, f_n \,\rangle_{\mathbb{R}}$ be the subspace of $\mathcal{C}_\infty(\mathbb{R})$ generated by the functions $f_i(x) = e^{ix}$ for $i = 0, \ldots, n$.

(i) Show that V is invariant under the operator D of derivation on $\mathcal{C}_\infty(\mathbb{R})$ and that, for $i = 0, \ldots, n$, the function f_i is an eigenvector of D with eigenvalue i.

(ii) Using Exercise 3.2.1, deduce that $\mathcal{B} = \{f_0, f_1, \ldots, f_n\}$ is a basis of V.

(iii) Calculate $[\, D|_V \,]_{\mathcal{B}}$.

3.2.3. Consider the subspace $\mathcal{P}_2(\mathbb{R})$ of $\mathcal{C}_\infty(\mathbb{R})$ given by $\mathcal{P}_2(\mathbb{R}) = \langle\, 1, x, x^2 \,\rangle_{\mathbb{R}}$. In each case, determine whether or not the given linear map is diagonalizable and, if it is, find a basis with respect to which its matrix is diagonal.

(i) $T\colon \mathcal{P}_2(\mathbb{R}) \to \mathcal{P}_2(\mathbb{R})$ given by $T(p(x)) = p'(x)$.

(ii) $T\colon \mathcal{P}_2(\mathbb{R}) \to \mathcal{P}_2(\mathbb{R})$ given by $T(p(x)) = p(2x)$.

3.2.4. Let $T\colon \mathrm{Mat}_{2\times 2}(\mathbb{R}) \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$ be the linear map given by $T(A) = A^t$.

(i) Find a basis of the eigenspaces of T for the eigenvalues 1 and -1.

(ii) Find a basis $\mathcal{B}$ of $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ such that $[\, T \,]_{\mathcal{B}}$ is diagonal, and write $[\, T \,]_{\mathcal{B}}$.

3.2.5. Let $S\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the reflection in the plane with equation $x + y + z = 0$.

(i) Describe geometrically the eigenspaces of S and give a basis of each.

(ii) Find a basis $\mathcal{B}$ of $\mathbb{R}^3$ relative to which the matrix of S is diagonal and give $[\, S \,]_{\mathcal{B}}$.

(iii) Using the above, find the matrix of T in the standard basis.

3.3 Diagonalization of matrices

As we have already mentioned, results on linear operators translate into results on matrices and vice versa. The problem of diagonalization is a good example of this.

In this section, we fix an integer $n \geq 1$.

- We say that a matrix $A \in \mathrm{Mat}_{n\times n}(K)$ is *diagonalizable* if there exists an invertible matrix $P \in \mathrm{Mat}_{n\times n}(K)$ such that $P^{-1}\, A\, P$ is a diagonal matrix.

- We say that an element λ of K is an *eigenvalue* of A if there exists a nonzero column vector $X \in K^n$ such that $AX = \lambda X$.

- A nonzero column vector $X \in K^n$ that satisfies the relation $AX = \lambda X$ for a scalar $\lambda \in K$ is called an *eigenvector of A for the eigenvalue λ*.

- If λ is an eigenvalue of A, then the set

$$\begin{aligned} E_\lambda(A) &:= \{X \in K^n\,;\, A\,X = \lambda\,X\} \\ &= \{X \in K^n\,;\, (A - \lambda I)\,X = \mathbf{0}\} \end{aligned}$$

  is a subspace of K^n called the *eigenspace of A for the eigenvalue λ*.

- The polynomial

$$\mathrm{char}_A(x) := \det(x\,I - A) \in K[x]$$

  is called the *characteristic polynomial* of A.

Recall that to every $A \in \mathrm{Mat}_{n\times n}(K)$, we associate a linear operator $T_A\colon K^n \to K^n$ given by

$$T_A(X) = A\,X \quad \text{for all} \quad X \in K^n.$$

Then we see that the above definitions coincide with the corresponding notions for the operator T_A. More precisely, we note that:

Proposition 3.3.1. *Let $A \in \mathrm{Mat}_{n\times n}(K)$.*

(i) The eigenvalues of T_A coincide with those of A.

(ii) If λ is an eigenvalue T_A, then the eigenvectors of T_A for this eigenvalue are the same as those of A and we have $E_\lambda(T_A) = E_\lambda(A)$.

(iii) $\mathrm{char}_{T_A}(x) = \mathrm{char}_A(x)$.

Proof. Assertions (i) and (ii) follow directly from the definitions, while (iii) follows from the fact that $[\,T_A\,]_{\mathcal{E}} = A$, where $\mathcal{E}$ is the standard basis of K^n. □

We also note that:

Proposition 3.3.2. *Let $A \in \mathrm{Mat}_{n\times n}(K)$. The following conditions are equvalent:*

(i) T_A is diagonalizable,

(ii) there exists a basis of K^n consisting of eigenvectors of A,

(iii) A is diagonalizable.

Furthermore, if these conditions are satisfied and if $\mathcal{B} = \{X_1, \dots, X_n\}$ is a basis of K^n consisting of eigenvectors of A, then the matrix $P = (X_1 \cdots X_n)$ is invertible and

$$P^{-1}\,A\,P = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

where λ_i is the eigenvalue of A corresponding to X_i for $i = 1, \dots, n$.

Proof. If T_A is diagonalizable, Proposition 3.2.1 shows that there exists a basis $\mathcal{B} = \{X_1, \dots, X_n\}$ of K^n consisting of eigenvectors of T_A or, equivalently, of A. For such a basis, the change of basis matrix $P = [\,I\,]_{\mathcal{E}}^{\mathcal{B}} = (X_1 \cdots X_n)$ from the basis $\mathcal{B}$ to the standard basis $\mathcal{E}$ is invertible and we find that

$$P^{-1}\,A\,P = P^{-1}[\,T_A\,]_{\mathcal{E}}P = [\,T_A\,]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

where λ_i is the eigenvalue of A corresponding to X_i for $i = 1, \dots, n$. This proves the implication (i)⇒(ii)⇒(iii) as well as the last assertion of the proposition. It remains to prove the implication (iii)⇒(i).

Suppose therefore that A is diagonalizable and that $P \in \mathrm{Mat}_{n\times n}(K)$ is an invertible matrix such that $P^{-1}\,A\,P$ is diagonal. Since P is invertible, its columns form a basis $\mathcal{B}$ of K^n and, with this choice of basis, we have $P = [\,I\,]_{\mathcal{E}}^{\mathcal{B}}$. Then $[\,T_A\,]_{\mathcal{B}} = P^{-1}[\,T_A\,]_{\mathcal{E}}P = P^{-1}A\,P$ is diagonal, which proves that T_A is diagonalizable. □

Combining Theorem 3.2.3 with the two preceding propositions, we have the following:

Theorem 3.3.3. *Let $A \in \mathrm{Mat}_{n\times n}(K)$. Then A has an most n eigenvalues in K. Let $\lambda_1, \dots, \lambda_s$ be the distinct eigenvalues of A in K. Then A is diagonalizable if and only if*

$$n = \dim_K(E_{\lambda_1}(A)) + \cdots + \dim_K(E_{\lambda_s}(A))\,.$$

If this is the case, we obtain a basis $\mathcal{B} = \{X_1, \dots, X_n\}$ of K^n consisting of eigenvectors of A by concatenating the bases $E_{\lambda_1}(A), \dots, E_{\lambda_s}(A)$. Then the matrix $P = (X_1 \cdots X_n)$ with columns $X_1, \dots, X_n$ is invertible and

$$P^{-1}A\,P = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & 0 & \\ & & \lambda_1 & & & & \\ & & & \ddots & & & \\ & & & & \lambda_s & & \\ & 0 & & & & \ddots & \\ & & & & & & \lambda_s \end{pmatrix}$$

with each λ_i repeated a number of times equal to $\dim_K(E_{\lambda_i}(A))$.

Example 3.3.4. Let $A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{2} & \bar{1} \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{F}_3)$, were $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ is the finite field with 3 elements. Do the following:

1° Find the eigenvalues of A in $\mathbb{F}_3$.

2° For each eigenvalue, find a basis of the corresponding eigenspace.

3° Determine whether or not A is diagonalizable. If it is, find an invertible matrix P such that $P^{-1}A\,P$ is diagonal and give this diagonal matrix.

Solution: 1st We find

$$\begin{aligned} \mathrm{char}_A(x) &= \begin{vmatrix} x-\bar{1} & -\bar{2} & -\bar{1} \\ \bar{0} & x & \bar{0} \\ -\bar{1} & -\bar{2} & x-\bar{1} \end{vmatrix} = x \begin{vmatrix} x-\bar{1} & -\bar{1} \\ -\bar{1} & x-\bar{1} \end{vmatrix} \quad \text{(expansion along the second row)} \\ &= x(x^2+x) = x^2(x+\bar{1}), \end{aligned}$$

and so the eigenvalues of A are $\bar{0}$ and $-\bar{1} = \bar{2}$.

2nd We have

$$E_{\bar{0}}(A) = \{X \in \mathbb{F}_3^3\,;\, (A-\bar{0}I)X = \mathbf{0}\} = \{X \in \mathbb{F}_3^3\,;\, A\,X = \mathbf{0}\}.$$

In other words $E_{\bar{0}}(A)$ is the solution set in $\mathbb{F}_3^3$ to the homogeneous system of linear equations $A\,X = \mathbf{0}$. The latter does not change if we apply to the matrix A of the system a series of elementary row operations:

$$A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{2} & \bar{1} \end{pmatrix} \sim \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow L_3 - L_1 \end{matrix}$$

Therefore, $E_{\bar{0}}(A)$ is the solution set of the equation

$$x + \bar{2}y + z = \bar{0}\,.$$

Setting $y = s$ and $z = t$, we see that $x = s - t$, and so

$$E_{\bar{0}}(A) = \left\{ \begin{pmatrix} s-t \\ s \\ t \end{pmatrix} ;\, s,t \in \mathbb{F}_3^3 \right\} = \left\langle \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\rangle_{\mathbb{F}_3}.$$

Thus $\mathcal{B}_1 = \left\{ \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\}$ is a basis of $E_0(A)$ (it is clear that the two column ectors are linearly independent).

Similarly, we have:

$$E_{\bar{2}}(A) = \{X \in \mathbb{F}_3^3\,;\, (A - \bar{2}I)X = \mathbf{0}\} = \{X \in \mathbb{F}_3^3\,;\, (A + I)X = \mathbf{0}\}\,.$$

We find

$$\begin{aligned} A + I &= \begin{pmatrix} \bar{2} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{1} & \bar{2} & \bar{2} \end{pmatrix} \sim \begin{pmatrix} \bar{1} & \bar{1} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{1} & \bar{2} & \bar{2} \end{pmatrix} \begin{matrix} \leftarrow \bar{2}L_1 \\ \\ \\ \end{matrix} \sim \begin{pmatrix} \bar{1} & \bar{1} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow L_3 - L_1 \end{matrix} \\ &\sim \begin{pmatrix} \bar{1} & \bar{0} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix} \begin{matrix} \leftarrow L_1 - L_2 \\ \\ \leftarrow L_3 - L_2 \end{matrix} \end{aligned}$$

Therefore, $E_{\bar{2}}(A)$ is the solution set to the system

$$\begin{cases} x \qquad + \bar{2}z &= \bar{0} \\ \qquad y \qquad &= \bar{0}. \end{cases}$$

Here, z is the only independent variable. Let $z = t$. Then $x = -\bar{2}t = t$ and $y = \bar{0}$, and so

$$E_{\bar{2}}(A) = \left\{ \begin{pmatrix} t \\ \bar{0} \\ t \end{pmatrix} \,;\, t \in \mathbb{F}_3 \right\} = \left\langle \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\rangle_{\mathbb{F}_3}$$

and it follows that $\mathcal{B}_2 = \left\{ \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\}$ is a basis of $E_{\bar{2}}(A)$.

3rd Since A is a 3×3 matrix and

$$\dim_{\mathbb{F}_3} E_{\bar{0}}(A) + \dim_{\mathbb{F}_3} E_{\bar{2}}(A) = 3,$$

we conclude that A is diagonalizable, and that

$$\mathcal{B} = \mathcal{B}_1 \amalg \mathcal{B}_2 = \left\{ \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\}$$

is a basis of $\mathbb{F}_3^3$ consisting of eigenvectors of A for the respective eigenvalues $\bar{0}, \bar{0}, \bar{2}$. Then the matrix

$$P = \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \end{pmatrix}$$

is invertible and the product $P^{-1}A\,P$ is a diagonal matrix with diagonal $(\bar{0}, \bar{0}, \bar{2})$:

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

Exercises.

3.3.1. In each case, find the real eigenvalues of the given matrix $A \in \mathrm{Mat}_{3\times 3}(\mathbb{R})$ and, for each of the eigenvalues, give a basis of the corresponding eigenspace. If A is diagonalizable, find an invertible matrix $P \in \mathrm{Mat}_{3\times 3}(\mathbb{R})$ such that $P^{-1}AP$ is diagonal, and give $P^{-1}AP$.

$$\text{(i)} \quad A = \begin{pmatrix} -2 & 0 & 5 \\ 0 & 5 & 0 \\ -4 & 0 & 7 \end{pmatrix}, \qquad \text{(ii)} \quad A = \begin{pmatrix} 1 & -2 & 3 \\ 2 & 6 & -6 \\ 1 & 2 & -1 \end{pmatrix}.$$

3.3.2. The matrix $A = \begin{pmatrix} 1 & -2 \\ 4 & -3 \end{pmatrix}$ is not diagonalizable over the real numbers. However, it is over the complex numbers. Find an invertible matrix P with complex entries such that $P^{-1}AP$ is diagonal, and give $P^{-1}AP$.

3.3.3. Let $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ be the field with 2 elements and let $A = \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{F}_2)$. Find the eigenvalues of A in $\mathbb{F}_2$ and, for each one, give a basis of the corresponding eigenspace. If A is diagonalizable, find an invertible matrix $P \in \mathrm{Mat}_{3\times 3}(\mathbb{F}_2)$ such that $P^{-1}AP$ is diagonal, and give $P^{-1}AP$.

Chapter 4

Polynomials, linear operators and matrices

Let V be a vector space of finite dimension n over a field K. In this chapter, we show that the set $\mathrm{End}_K(V)$ of linear operators on V is a ring under addition and composition, isomorphic to the ring $\mathrm{Mat}_{n\times n}(K)$ of $n \times n$ matrices with coefficients in K. We then construct the ring $K[x]$ of polynomials in one indeterminate x over the field K. For each linear operator $T \in \mathrm{End}_K(V)$ and each matrix $A \in \mathrm{Mat}_{n\times n}(K)$, we define ring homomorphisms

$$\begin{array}{rcl} K[x] & \longrightarrow & \mathrm{End}_K(V) \\ P(x) & \longmapsto & P(T) \end{array} \qquad \text{and} \qquad \begin{array}{rcl} K[x] & \longrightarrow & \mathrm{Mat}_{n\times n}(K) \\ P(x) & \longmapsto & P(A) \end{array}$$

that send x to T and x to A respectively. The link between them is that, if $\mathcal{B}$ is a basis of V, then $[P(T)]_{\mathcal{B}} = P([\,T\,]_{\mathcal{B}})$.

4.1 The ring of linear operators

We refer the reader to Appendix A for a review of the basic notions related to rings. We first show:

Theorem 4.1.1. *Let V be a vector space of dimension n over a field K and let $\mathcal{B}$ be a basis of V. The set $\mathrm{End}_K(V)$ of linear operators on V is a ring under addition and composition. Furthermore, the function*

$$\begin{array}{rrcl} \varphi : & \mathrm{End}_K(V) & \longrightarrow & \mathrm{Mat}_{n\times n}(K) \\ & T & \longmapsto & [\,T\,]_{\mathcal{B}} \end{array}$$

is a ring isomorphism.

Proof. We already know, by Theorem 2.2.3, that the set $\mathrm{End}_K(V) = \mathcal{L}_K(V, V)$ is a vector space over K. In particular, it is an abelian group under addition. We also know that the

composite of two linear operators $S\colon V \to V$ and $T\colon V \to V$ is a linear operator $S \circ T\colon V \to V$, hence an element of $\mathrm{End}_K(V)$. Since the composition is associative and the identity map $I_V \in \mathrm{End}_K(V)$ is an identity element for this operation, we conclude that $\mathrm{End}_K(V)$ is a monoid under composition. Finally, Proposition 2.3.1 gives that if $R, S, T \in \mathrm{End}_K(V)$, then

$$(R + S) \circ T = R \circ T + S \circ T \quad \text{and} \quad R \circ (S + T) = R \circ S + R \circ T.$$

Therefore composition is distributive over addition in $\mathrm{End}_K(V)$ and so $\mathrm{End}_K(V)$ is a ring.

In addition, Theorem 2.4.3 shows that the function φ is an isomorphism of vector spaces over K. In particular, it is an isomorphism of abelian groups under addition. Finally, Proposition 2.4.6 implies that if $S, T \in \mathrm{End}_K(V)$, then

$$\varphi(S \circ T) = [\, S \circ T \,]_{\mathcal{B}} = [\, S \,]_{\mathcal{B}} [\, T \,]_{\mathcal{B}} = \varphi(S)\varphi(T)\,.$$

Since $\varphi(I_V) = I$, we conclude that φ is also an isomorphism of rings. □

Exercises.

4.1.1. Let V be a vector space over a field K and let U be a subspace of V. Show that the set of linear maps $T\colon V \to V$ such that $T(\mathbf{u}) \in U$ for all $\mathbf{u} \in U$ is a subring of $\mathrm{End}_K(V)$.

4.1.2. Let $A = \{a + b\sqrt{2}\,;\, a, b \in \mathbb{Q}\}$.

(i) Show that A is a subring of $\mathbb{R}$ and that $\mathcal{B} = \{1, \sqrt{2}\}$ is a basis of A viewed as a vector space over $\mathbb{Q}$.

(ii) Let $\alpha = a + b\sqrt{2} \in A$. Show that the function $m_\alpha\colon A \to A$ defined by $m_\alpha(\beta) = \alpha\beta$ for all $\beta \in A$ is a $\mathbb{Q}$-linear map and calculate $[m_\alpha]_{\mathcal{B}}$.

(iii) Show that the function $\varphi\colon A \to \mathrm{Mat}_{2\times 2}(\mathbb{Q})$ given by $\varphi(\alpha) = [m_\alpha]_{\mathcal{B}}$ is an injective ring homomorphism, and describe its image.

4.2 Polynomial rings

Proposition 4.2.1. *Let A be a commutative ring and let x be a symbol not in A. There exists a commutative ring, denoted $A[x]$, containing A as a subring and x as an element such that*

(i) every element of $A[x]$ can be written as $a_0 + a_1\, x + \cdots + a_n\, x^n$ for some integer $n \geq 0$ and some elements $a_0, a_1, \ldots, a_n$ of A;

(ii) *if* $a_0 + a_1\,x + \cdots + a_n\,x^n = 0$ *for an integer* $n \geq 0$ *and elements* $a_0, a_1, \dots, a_n$ *of* A*, then* $a_0 = a_1 = \cdots = a_n = 0$.

This ring $A[x]$ is called the *polynomial ring in the indeterminate* x *over* A. The proof of this result is a bit technical. The student make skip it in a first reading. However, it is important to known how to manipulate the elements of this ring, called *polynomials in* x *with coefficients in* A.

Suppose the existence of this ring $A[x]$ and let

$$p = a_0 + a_1\,x + \cdots + a_m\,x^m \quad \text{and} \quad q = b_0 + b_1\,x + \cdots + b_n\,x^n$$

be two of its elements. We first note that condition (ii) implies

$$p = q \quad \Longleftrightarrow \quad \begin{cases} a_i = b_i & \text{for} \quad i = 0, 1, \dots, \min(m, n), \\ a_i = 0 & \text{for} \quad i > n, \\ b_i = 0 & \text{for} \quad i > m. \end{cases}$$

Defining $a_i = 0$ for each $i > m$ and $b_i = 0$ for each $i > n$, we also have

$$p + q = \sum_{i=0}^{\max(n,m)} a_i x^i + \sum_{i=0}^{\max(n,m)} b_i x^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i)\,x^i,$$

$$p \cdot q = \left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j\,x^{i+j} = \sum_{k=0}^{m+n}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

Example 4.2.2. Over the field $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ of 3 elements, we have

$$\begin{aligned} (\bar{1} + x^2 + \bar{2}x^3) + (x + \bar{2}x^2) &= \bar{1} + x + \bar{2}x^3, \\ (\bar{1} + x^2 + \bar{2}x^3)(x + \bar{2}x^2) &= x + \bar{2}x^2 + x^3 + x^4 + x^5. \end{aligned}$$

Proof of Proposition 4.2.1. Let S be the set of sequences $(a_0, a_1, a_2, \dots)$ of elements of A whose elements are all zero after a certain point. We define an "addition" on S by setting

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots).$$

The result is indeed an element of S, since if $a_i = b_i = 0$ for all $i > n$, then $a_i + b_i = 0$ for all $i > n$. It is easily verified that this operation is associative and commutative, that the element $(0, 0, 0, \dots)$ is an identity element, and that an arbitrary element $(a_0, a_1, a_2, \dots)$ of S has inverse $(-a_0, -a_1, -a_2, \dots)$. Thus S is an abelian group under this operation.

We also define a "multiplication" on S by defining

$$(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (t_0, t_1, t_2, \dots) \quad \text{where} \quad t_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

The result is an element of S, since if we suppose again that $a_i = b_i = 0$ for all $i > n$, then, for every integer $k > 2n$, each of the products $a_i b_{k-i}$ with $i = 0, \dots, k$ is zero (one of the indices i or $k - i$ being necessarily $> n$) and so $t_k = 0$. It is easy to see that the sequence $(1, 0, 0, \dots)$ is an identity element for this operation.

To conclude that S is a ring under these operations, it remains to show that the multiplication is associative and distributive over the addition. In other words, we must show that if

$$p = (a_0, a_1, a_2, \dots), \quad q = (b_0, b_1, b_2, \dots) \quad \text{and} \quad r = (c_0, c_1, c_2, \dots)$$

are three elements of S, then

1) $(pq)r = p(qr)$,

2) $(p + q)r = p\,r + q\,r$,

3) $p(q + r) = p\,q + p\,r$.

These three equalities are proved in the same manner: it suffices to show that the sequences on either side of the equality have the same element of index k for each $k \geq 0$. Equality 1) is the most delicate to verify since each term involves two products. We see that the element of index k of $(pq)r$ is

$$((pq)r)_k = \sum_{j=0}^{k} (pq)_j c_{k-j} = \sum_{j=0}^{k} \left(\sum_{i=0}^{j} a_i b_{j-i} \right) c_{k-j} = \sum_{j=0}^{k} \sum_{i=0}^{j} a_i b_{j-i} c_{k-j}$$

and that of $p(qr)$ is

$$(p(qr))_k = \sum_{i=0}^{k} a_i (qr)_{k-i} = \sum_{i=0}^{k} a_i \left(\sum_{j=0}^{k-i} b_j c_{k-i-j} \right) = \sum_{i=0}^{k} \sum_{j=0}^{k-i} a_i b_j c_{k-i-j}.$$

In both cases, we see that the result if the sum of all products $a_i b_j c_l$ with $i, j, l \geq 0$ and $i + j + l = k$, hence

$$((pq)r)_k = \sum_{i+j+l=k} a_i b_j c_l = (p(qr))_k.$$

This proves 1). The proofs of 2) and 3) are simpler and left as exercises.

For all $a, b \in A$, we see that

$$\begin{aligned} (a, 0, 0, \dots) + (b, 0, 0, \dots) &= (a + b, 0, 0, \dots), \\ (a, 0, 0, \dots)(b, 0, 0, \dots) &= (ab, 0, 0, \dots). \end{aligned}$$

Thus the map $\iota \colon A \to S$ given by

$$\iota(a) = (a, 0, 0, \dots)$$

is an injective ring homomorphism. From now on, we identify A with its image under ι. Then A becomes a subring of S and we have

$$a(b_0, b_1, \dots) = (a\, b_0, a\, b_1, a\, b_2, \dots)$$

for all $a \in A$ and every sequence $(b_0, b_1, b_2, \dots) \in S$.

Let $X = (0, 1, 0, 0, \dots)$. An easy induction shows that, for every integer $i \geq 1$, the i-th power X^i of X is the sequence whose elements are all zero except for the element of index i, which is equal to 1:

$$X^i = (0, \dots, 0, \overset{\overset{i}{\vee}}{1}, 0, \dots).$$

From this we deduce:

1st For every sequence $(a_0, a_1, a_2, \dots)$ of S, by choosing an integer $n \geq 0$ such that $a_i = 0$ for all $i > n$, we have:

$$(a_0, a_1, a_2, \dots) = \sum_{i=0}^{n} (0, \dots, 0, \overset{\overset{i}{\vee}}{a_i}, 0, \dots) = \sum_{i=0}^{n} a_i\, (0, \dots, 0, \overset{\overset{i}{\vee}}{1}, 0, \dots) = \sum_{i=0}^{n} a_i\, X^i.$$

2nd In addition, if n is an integer ≥ 0 and $a_0, a_1, \dots, a_n \in A$ satisfy

$$a_0 + a_1\, X + \cdots + a_n\, X^n = 0,$$

then

$$0 = \sum_{i=0}^{n} a_i\, (0, \dots, 0, \overset{\overset{i}{\vee}}{1}, 0, \dots) = \sum_{i=0}^{n} (0, \dots, 0, \overset{\overset{i}{\vee}}{a_i}, 0, \dots) = (a_0, a_1, \dots, a_n, 0, 0, \dots),$$

and so $a_0 = a_1 = \cdots = a_n = 0$.

These last two observations show that the ring S has the two properties required by the proposition except that instead of the element x, we have the sequence $X = (0, 1, 0, \dots)$. This is not really a problem: it suffices to replace X by x in S and in the addition and multiplication tables of S. □

Every polynomial $p \in A[x]$ induces a function from A to A. Before giving this construction, we first note the following fact whose proof is left as an exercise:

Proposition 4.2.3. *Let X be a set and let A be a commutative ring. The set $\mathcal{F}(X, A)$ of functions from X to A is a commutative ring under the addition and multiplication defined in the following manner. If $f, g \in \mathcal{F}(X, A)$ then $f + g$ and $f\, g$ are functions from X to A given by*

$$(f + g)(x) = f(x) + g(x) \quad \textit{and} \quad (f\, g)(x) = f(x)\, g(x)$$

for all $x \in X$.

We also show:

Proposition 4.2.4. *Let A be a subring of a commutative ring C and let $c \in C$. The function*

$$\begin{array}{rcl} A[x] & \longrightarrow & C \\ \displaystyle\sum_{i=0}^{n} a_i x^i & \longmapsto & \displaystyle\sum_{i=0}^{n} a_i c^i \end{array} \tag{4.1}$$

is a ring homomorphism.

This homomorphism is called *evaluation at c* and the image of a polynomial p under this homomorphism is denoted $p(c)$.

Proof of Proposition 4.2.4. Let

$$p = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad q = \sum_{i=0}^{m} b_i x^i$$

be elements of $A[x]$. Define $a_i = 0$ for all $i > n$ and $b_i = 0$ for all $i > m$. Then we have:

$$p + q = \sum_{i=0}^{\max(n,m)} (a_i + b_i)\, x^i \quad \text{and} \quad p\, q = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k.$$

We see that

$$p(c) + q(c) = \sum_{i=0}^{m} a_i c^i + \sum_{i=0}^{n} b_i c^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i)\, c^i = (p+q)(c)$$

and

$$p(c)q(c) = \left(\sum_{i=0}^{m} a_i c^i \right) \left(\sum_{i=0}^{n} b_i c^i \right) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j\, c^{i+j} = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) c^k = (pq)(c).$$

These last equalities, together with the fact that the image of $1 \in A[x]$ is 1 show that the function (4.1) is indeed a ring homomorphism. □

In particular, if we take $C = A[x]$ and $c = x$, the map 4.1 becomes the identity map:

$$\begin{array}{rcl} A[x] & \longrightarrow & A[x] \\ p = \displaystyle\sum_{i=0}^{n} a_i x^i & \longmapsto & p(x) = \displaystyle\sum_{i=0}^{n} a_i x^i. \end{array}$$

For this reason, we generally write $p(x)$ to denote a polynomial in $A[x]$. This is what we will generally do from now on.

Proposition 4.2.5. *Let A be a commutative ring. For each $p \in A[x]$, denote by $\Phi(p) : A \to A$ the function given by $\Phi(p)(a) = p(a)$ for all $a \in A$. The map $\Phi : A[x] \to \mathcal{F}(A, A)$ thus defined is a ring homomorphism with kernel*

$$\ker(\Phi) = \{p \in A[x]\,;\, p(a) = 0 \ \textit{for all}\ a \in A\}.$$

We say that $\Phi(p)$ is the *polynomial function from A to A induced by p*. The image of Φ in $\mathcal{F}(A, A)$ is called the *ring of polynomial functions from A to A*. More concisely, we can define Φ in the following manner:

$$\begin{array}{rcl} \Phi\ :\ A[x] & \longrightarrow & \mathcal{F}(A, A) \\ p & \longmapsto & \Phi(p)\colon A \longrightarrow A \\ & & \qquad\quad a \longmapsto p(a) \end{array}$$

Proof. Let $p, q \in A[x]$. For all $a \in A$, we have

$$\Phi(p + q)(a) = (p + q)(a) = p(a) + q(a) = \Phi(p)(a) + \Phi(q)(a),$$
$$\Phi(p\,q)(a) = (p\,q)(a) = p(a)\,q(a) = \Phi(p)(a) \cdot \Phi(q)(a),$$

hence $\Phi(p + q) = \Phi(p) + \Phi(q)$ and $\Phi(p\,q) = \Phi(p)\Phi(q)$. Since $\Phi(1)$ is the constant function equal to 1 (the identity element of $\mathcal{F}(A, A)$ for the product), we conclude that Φ is a ring homomorphism. The last assertion concerning its kernel follows from the definitions. □

Example 4.2.6. If $A = \mathbb{R}$, the function $\Phi\colon \mathbb{R}[x] \to \mathcal{F}(\mathbb{R}, \mathbb{R})$ defined by Proposition 4.2.5 is injective, since we know that a nonzero polynomial in $\mathbb{R}[x]$ has a finite number of real roots and thus $\ker \Phi = \{\mathbf{0}\}$. In this case, Φ induces an isomorphism between the ring $\mathbb{R}[x]$ of polynomials with coefficients in $\mathbb{R}$ and its image in $\mathcal{F}(\mathbb{R}, \mathbb{R})$, the ring of polynomials functions from $\mathbb{R}$ to $\mathbb{R}$.

Example 4.2.7. Let $A = \mathbb{F}_2 = \{\bar{0}, \bar{1}\}$, the field with two elements. The ring $\mathcal{F}(\mathbb{F}_2, \mathbb{F}_2)$ of functions from $\mathbb{F}_2$ to itself consists of 4 elements whereas $\mathbb{F}_2[x]$ contains an infinite number of polynomials. In this case, the map Φ is not injective. For example, the polynomial $p(x) = x^2 - x$ satisfies $p(\bar{0}) = \bar{0}$ and $p(\bar{1}) = \bar{0}$, hence $p(x) \in \ker \Phi$.

Exercises.

4.2.1. Prove Proposition 4.2.3.

4.2.2. Show that the map $\Phi\colon A[x] \to \mathcal{F}(A, A)$ of Proposition 4.2.5 is not injective if A is a finite ring.

4.3 Evaluation at a linear operator or matrix

Let V be a vector space over a field K and let $T\colon V \to V$ be a linear operator on V. For every polynomial

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x],$$

we set

$$P(T) = a_0 I + a_1 T + \cdots + a_n T^n \in \mathrm{End}_K(V),$$

where I denotes the identity map on V.

Proposition 4.3.1. *With the above notation, the map*

$$\begin{array}{ccc} K[x] & \longrightarrow & \mathrm{End}_K(V) \\ p(x) & \longmapsto & p(T) \end{array}$$

is a ring homomorphism. Its image, denoted $K[T]$, is the commutative subring of $\mathrm{End}_K(V)$ *given by*

$$K[T] = \{a_0 I + a_1 T + \cdots + a_n T^n \,;\, n \in \mathbb{N}_{>0}, a_0, \ldots, a_n \in K\}.$$

This homomorphism is called *evaluation at T*.

Proof. By definition, the image of the constant polynomial 1 is the identity element I of $\mathrm{End}_K(V)$. To conclude that evaluation at T is a ring homomorphism, it remains to show that if $p, q \in K[x]$ are arbitrary polynomials, then

$$(p+q)(T) = p(T) + q(T) \quad \text{and} \quad (pq)(T) = p(T) \circ q(T).$$

The proof for the sum is left as an exercise. The proof for the product uses the fact that, for all $a \in K$ and all $S \in \mathrm{End}_K(V)$, we have

$$(a\,I) \circ S = S \circ (a\,I) = a\,S.$$

Write

$$p = \sum_{i=0}^{n} a_i\, x^i \quad \text{and} \quad q = \sum_{j=0}^{m} b_j\, x^j.$$

We see that

$$\begin{aligned} p(T) \circ q(T) &= \Big(a_0 I + \sum_{i=1}^{n} a_i\, T^i\Big) \circ \Big(b_0 I + \sum_{j=1}^{m} b_j\, T^i\Big) \\ &= (a_0 I) \circ (b_0 I) + (a_0 I) \circ \Big(\sum_{j=1}^{m} b_j\, T^j\Big) + \Big(\sum_{i=1}^{n} a_i\, T^i\Big) \circ (b_0 I) + \Big(\sum_{i=1}^{n} a_i\, T^i\Big) \circ \Big(\sum_{j=1}^{m} b_j\, T^j\Big) \\ &= a_0 b_0 I + \sum_{j=1}^{m} a_0 b_j\, T^j + \sum_{i=1}^{n} a_i b_0\, T^i + \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j\, T^{i+j} \\ &= (a_0 b_0) I + \sum_{k=1}^{n+m} \Big(\sum_{i+j=k} a_i b_j\Big) T^k \\ &= (pq)(T). \end{aligned}$$

Thus evaluation at T is indeed a ring homomorphism. The fact that its image is a commutative subring of $\mathrm{End}_K(V)$ follows from the fact that $K[x]$ is commutative. $\square$

Example 4.3.2. Let D be the operator of derivation on the vector space $\mathcal{C}_\infty(\mathbb{R})$ of infinitely differentiable functions $f\colon \mathbb{R} \to \mathbb{R}$. Let

$$p(x) = x^2 - 1 \in \mathbb{R}[x] \quad \text{and} \quad q(x) = 2x + 1 \in \mathbb{R}[x].$$

For every function $f \in \mathcal{C}_\infty(\mathbb{R})$, we have

$$\begin{aligned} p(D)(f) &= (D^2 - I)(f) = f'' - f, \\ q(D)(f) &= (2D + I)(f) = 2f' + f. \end{aligned}$$

By the above, we have $p(D) \circ q(D) = (pq)(D)$ for all polynomials $p, q \in \mathbb{R}[X]$. We verify this for the above choices of p and q. This reduces to showing that

$$(p(D) \circ q(D))(f) = ((pq)(D))(f)$$

for all $f \in \mathcal{C}_\infty(\mathbb{R})$. We see that

$$\begin{aligned} \big(p(D) \circ q(D)\big)(f) &= p(D)\big(q(D)(f)\big) \\ &= p(D)(2f' + f) \\ &= (2f' + f)'' - (2f' + f) \\ &= 2f''' + f'' - 2f' - f. \end{aligned}$$

Since $pq = (x^2 - 1)(2x + 1) = 2x^3 + x^2 - 2x - 1$, we also have

$$((pq)(D))(f) = (2D^3 + D^2 - 2D - I)(f) = 2f''' + f'' - 2f' - f$$

as claimed.

Example 4.3.3. Let $\mathcal{F}(\mathbb{Z}, \mathbb{R})$ be the vector space of functions $f\colon \mathbb{Z} \to \mathbb{R}$. We define a linear operator T on this vector space in the following manner. If $f\colon \mathbb{Z} \to \mathbb{R}$ is an arbitrary function, then $T(f)\colon \mathbb{Z} \to \mathbb{R}$ is the function given by

$$\big(T(f)\big)(i) = f(i + 1) \quad \text{for all } i \in \mathbb{Z}.$$

We see that

$$\begin{aligned} \big(T^2(f)\big)(i) &= \big(T(T(f))\big)(i) = (T(f))(i + 1) = f(i + 2), \\ \big(T^3(f)\big)(i) &= \big(T(T^2(f))\big)(i) = (T^2(f))(i + 1) = f(i + 3), \end{aligned}$$

and so on. In general,

$$\big(T^k(f)\big)(i) = f(i + k) \quad \text{for} \quad k = 1, 2, 3, \ldots$$

From this, we deduce that if $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x]$, then $p(T)(f)$ is the function from $\mathbb{Z}$ to $\mathbb{R}$ given, for all $i \in \mathbb{Z}$, by

$$\begin{aligned} (p(T)(f))(i) &= ((a_0 I + a_1 T + \cdots + a_n T^n)(f))(i) \\ &= (a_0 f + a_1 T(f) + \cdots + a_n T^n(f))(i) \\ &= a_0 f(i) + a_1 T(f)(i) + \cdots + a_n T^n(f)(i) \\ &= a_0 f(i) + a_1 f(i + 1) + \cdots + a_n f(i + n)\,. \end{aligned}$$

Let $A \in \mathrm{Mat}_{n\times n}(K)$ be an $n \times n$ square matrix with coefficients in a field K. For every polynomial

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x],$$

we set

$$p(A) = a_0 I + a_1 A + \cdots + a_n A^n \in \mathrm{Mat}_{n\times n}(K),$$

where I denotes the $n \times n$ identity matrix.

Proposition 4.3.4. *With the above notation, the map*

$$\begin{array}{rcl} K[x] & \longrightarrow & \mathrm{Mat}_{n\times n}(K) \\ p(x) & \longmapsto & p(A) \end{array}$$

is a ring homomorphism. Its image, denoted $K[A]$, is the commutative subring of $\mathrm{Mat}_{n\times n}(K)$ *given by*

$$K[A] = \{a_0 I + a_1 A + \cdots + a_n A^n \,;\, n \in \mathbb{N},\, a_0, \ldots, a_n \in K\}.$$

This homomorphism is called *evaluation at A*. The proof of this proposition is similar to that of Proposition 4.3.1 and is left as an exercise.

Example 4.3.5. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Q})$ and let $p(x) = x^3 + 2x - 1 \in \mathbb{Q}[x]$. We have

$$p(A) = A^3 + 2A - I = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 0 & 2 \end{pmatrix}.$$

We conclude with the following result:

Theorem 4.3.6. *Let V be a vector space of finite dimension n, let $\mathcal{B}$ be a basis of V, and let $T\colon V \to V$ be a linear operator on V. For every polynomial $p(x) \in K[x]$, we have*

$$[p(T)]_{\mathcal{B}} = p([\,T\,]_{\mathcal{B}}).$$

Proof. Write $p(x) = a_0 + a_1\, x + \cdots + a_n\, x^n$. We have

$$\begin{aligned} [p(T)]_{\mathcal{B}} &= [a_0 I + a_1 T + \cdots + a_n T^n]_{\mathcal{B}} \\ &= a_0 I + a_1 [T]_{\mathcal{B}} + \cdots + a_n [T^n]_{\mathcal{B}} \\ &= a_0 I + a_1 [T]_{\mathcal{B}} + \cdots + a_n ([T]_{\mathcal{B}})^n \\ &= p([\,T\,]_{\mathcal{B}}). \end{aligned}$$

□

Example 4.3.7. Let $V = \langle \cos(2t), \sin(2t)\rangle_{\mathbb{R}} \subseteq \mathcal{C}_\infty(\mathbb{R})$ and let D be the operator of derivation on $\mathcal{C}_\infty(\mathbb{R})$. The subspace V is stable under D since

$$D(\cos(2t)) = -2\sin(2t) \in V \quad \text{and} \quad D(\sin(2t)) = 2\cos(2t) \in V. \tag{4.2}$$

For simplicity, denote by D the restriction $D|_V$ of D to V. We note that

$$\mathcal{B} = \{\cos(2t), \sin(2t)\}$$

is a basis of V (exercise). Then formulas (4.2) give

$$[\,D\,]_{\mathcal{B}} = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}.$$

Thus we have

$$[p(D)]_{\mathcal{B}} = p\left(\begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}\right)$$

for all $p(x) \in \mathbb{R}[x]$. In particular, for $p(x) = x^2 + 4$, we have $p([\,D\,]_{\mathcal{B}}) = 0$, hence $p(D) = 0$.

Exercises.

4.3.1. Prove the equality $(p+q)(T) = p(T) + q(T)$ left as an exercise in the proof of Proposition 4.3.1.

4.3.2. Let $R_{\pi/4}\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation through angle $\pi/4$ about the origin in $\mathbb{R}^2$, and let $p(x) = x^2 - 1 \in \mathbb{R}[x]$. Compute $p(R_{\pi/4})(1, 2)$.

4.3.3. Let $R_{2\pi/3}\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation through angle $2\pi/3$ about the origin in $\mathbb{R}^2$, and let $p(x) = x^2 + x + 1 \in \mathbb{R}[x]$. Show that $p(R_{2\pi/3}) = 0$.

4.3.4. Let D be the restriction to $V = \langle\, e^x, xe^x, x^2e^x \,\rangle_{\mathbb{R}}$ of the operator of differentiation in $\mathcal{C}_\infty(\mathbb{R})$.

(i) Show that $\mathcal{B} = \{e^x, xe^x, x^2e^x\}$ is a basis of V and determine $[\,D\,]_{\mathcal{B}}$.

(ii) Let $p(x) = x^2 - 1$ and $q(x) = x - 1$. Compute $[p(D)]_{\mathcal{B}}$ and $[q(D)]_{\mathcal{B}}$. Do these matrices commute? Why or why not?

4.3.5. Let V be a vector space over $\mathbb{C}$ of dimension 3, let $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ be a basis of V, and let $T\colon V \to V$ be the linear map determined by the conditions

$$T(\mathbf{v}_1) = i\mathbf{v}_2 + \mathbf{v}_3, \quad T(\mathbf{v}_2) = i\mathbf{v}_3 + \mathbf{v}_1 \quad \text{and} \quad T(\mathbf{v}_3) = i\mathbf{v}_1 + \mathbf{v}_2.$$

(i) Calculate $[p(T)]_{\mathcal{B}}$ where $p(x) = x^2 + (1+i)x + i$.

(ii) Calculate $p(T)(\mathbf{v}_1)$.

Chapter 5

Unique factorization in euclidean domains

The goal of this chapter is to show that every nonconstant polynomial with coefficients in a field K can be written as a product of *irreducible* polynomials in $K[x]$ and that this factorization is unique up to the ordering of the factors and multiplying each factor by a nonzero element of K. We will show that this property extends to a relatively large class of rings called *euclidean domains*. This class includes the polynomials rings $K[x]$ over a field K, the ring $\mathbb{Z}$ of ordinary integers and the ring of gaussian integers, just to mention a few. The key property of euclidean rings is that every ideal of such a ring is *principal*, that is, generated by a single element.

5.1 Divisibility in integral domains

Definition 5.1.1 (Integral domain). An *integral domain* (or *integral ring*) is a commutative ring A with $0 \neq 1$ satisfying the property that $ab \neq 0$ for all $a, b \in A$ with $a \neq 0$ and $b \neq 0$ (in other words, $ab = 0 \implies a = 0$ or $b = 0$).

Example 5.1.2. The ring $\mathbb{Z}$ is integral. Every subring of a field K is integral.

We will see later that the ring $K[x]$ is integral for all fields K.

Definition 5.1.3 (Division). Let A be an integral domain and let $a, b \in A$ with $a \neq 0$. We that that a *divides* b (in A) or that b is *divisible* by a if there exists $c \in A$ such that $b = c\,a$. We denote this condition by $a \mid b$. A *divisor* of b (in A) is a nonzero element of A that divides b.

Example 5.1.4. In $\mathbb{Z}$, we have $-2 \mid 6$, since $-6 = (-2)(-3)$. On the other hand, 5 does not divide 6 in $\mathbb{Z}$, but 5 divides 6 in $\mathbb{Q}$.

The following properties are left as exercises:

Proposition 5.1.5. *Let A be an integral domain and let $a, b, c \in A$ with $a \neq 0$.*

(i) $1 \mid b$

(ii) If $a \mid b$, then $a \mid bc$.

(iii) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

(iv) If $a \mid b$, $b \neq 0$ and $b \mid c$, then $a \mid c$.

(v) If $a \neq 0$ and $ab \mid ac$, then $b \mid c$.

Definition 5.1.6 (Associate). Let A be an integral domain and let $a, b \in A \setminus \{0\}$. We say that a and b are *associates* or that a is *associated to* b if $a \mid b$ and $b \mid a$. We denote this condition by $a \sim b$.

Example 5.1.7. In $\mathbb{Z}$, two nonzero integers a and b are associates if and only if $a = \pm b$. In particular, every nonzero integer a is associated to a unique positive integer, known as $|a|$.

Lemma 5.1.8. *Let A be a integral domain and let $a \in A \setminus \{0\}$. The following conditions are equivalent:*

(i) $a \sim 1$,

(ii) $a \mid 1$,

(iii) a is invertible.

Proof. Since $1 \mid a$, conditions (i) and (ii) are equivalent. Since A is commutative, conditions (ii) and (iii) are also equivalent. □

Definition 5.1.9 (Unit). The nonzero elements of an integral domain A that satisfy the equivalent conditions of Lemma 5.1.8 are called *units* of A. The set of all units of A is denoted $A^\times$.

Proposition 5.1.10. *The set $A^\times$ of units of an integral domain A is stable under the product in A and, for this operation, it is an abelian group.*

For the proof, see Appendix A.

Example 5.1.11. The group of units of $\mathbb{Z}$ is $\mathbb{Z}^\times = \{1, -1\}$. The group of units of a field K is $K^\times = K \setminus \{0\}$. We also call it the *multiplicative group of K*.

Proposition 5.1.12. *Let A be an integral domain and let $a, b \in A \setminus \{0\}$. Then $a \sim b$ if and only if $a = u\,b$ for some unit u of A.*

Proof. First suppose that $a \sim b$. Then there exists $u, v \in A$ such that $a = u\,b$ and $b = v\,a$. We thus have $a = u\,v\,a$, and so $(1 - u\,v)a = 0$. Since A is integral and $a \neq 0$, this implies $1 - u\,v = 0$, hence $u\,v = 1$ and so $u \in A^\times$.

Conversely, suppose that $a = u\,b$ with $u \in A^\times$. Since $u \in A^\times$, there exists $v \in A$ such that $v\,u = 1$. Therefore $b = v\,u\,b = v\,a$. By the equalities $a = u\,b$ and $b = v\,a$, we have $b \mid a$ and $a \mid b$, hence $a \sim b$. □

Definition 5.1.13 (Irreducible). We say that an element p in an integral domain A is *irreducible* (in A) if $p \neq 0$, $p \notin A^\times$ and the only divisors of p (in A) are the elements of A associated to 1 or to p.

Example 5.1.14. The irreducible elements of $\mathbb{Z}$ are of the form $\pm p$ where p is a prime number.

Definition 5.1.15 (Greatest common divisor). Let a, b be elements of an integral domain A, with $a \neq 0$ or $b \neq 0$. We say that a nonzero element d of A is a *greatest common divisor* (gcd) *of a and b* if

(i) $d \mid a$ and $d \mid b$,

(ii) for all $c \in A \setminus \{0\}$ such that $c \mid a$ and $c \mid b$, we have $c \mid d$.

We then write $d = \gcd(a, b)$.

Note that the gcd doesn't always exist and, if it exists, it is not unique in general. More precisely, if d is a gcd of a and b, than the gcds of a and b are the elements of A associated to d (see Exercise 5.1.3). For this reason, we often write $d \sim \gcd(a, b)$ to indicate that d is a gcd of a and b.

Example 5.1.16. We will soon see that $\mathbb{Z}[x]$ is an integral domain. Thus, so is the subring $\mathbb{Z}[x^2, x^3]$. However, the elements x^5 and x^6 do not have a gcd in $\mathbb{Z}[x^2, x^3]$ since x^2 and x^3 are both common divisors, but neither one divides the other.

Exercises.

5.1.1. Prove Proposition 5.1.5.

Note. Part (v) uses in a crucial way the fact that A is an integral domain.

5.1.2. Let A be an integral domain. Show that the relation $\sim$ of Definition 5.1.6 is an equivalence relation on $A \setminus \{0\}$.

5.1.3. Let A be an integral domain and let $a, b \in A \setminus \{0\}$. Suppose that d and d' are gcds of a and b. Show that $d \sim d'$.

5.1.4. Let A be an integral domain and let p and q be nonzero element of A with $p \sim q$. Show that p is irreducible if and only if q is irreducible.

5.1.5. Let A be an integral domain, and let p and q be irreducible elements of A with $p|q$. Show that $p \sim q$.

5.2 Divisibility in terms of ideals

Let A be a *commutative* ring. Recall that an *ideal* of A is a subsets I of A such that

(i) $0 \in I$,

(ii) if $r, s \in I$, then $r + s \in I$,

(iii) if $a \in A$ and $r \in I$, then $ar \in I$.

Example 5.2.1. The subsets $\{0\}$ and A are ideals of A.

The following result is left as an exercise.

Lemma 5.2.2. *Let $r_1, \ldots, r_m$ be elements of a commutative ring A. The set*

$$\{a_1 r_1 + \cdots + a_m r_m \,;\, a_1, \ldots, a_m \in A\}$$

is the smallest ideal of A containing $r_1, \ldots, r_m$.

Definition 5.2.3 (Ideal generated by elements, principal ideal). The ideal constructed in Lemma 5.2.2 is called the *ideal of A generated by $r_1, \ldots, r_m$* and is denoted $(r_1, \ldots, r_m)$. We say that an ideal of A is *principal* if it is generated by a single element. The principal ideal of A generated by r is

$$(r) = \{a\, r \,;\, a \in A\}.$$

Example 5.2.4. The ideal of $\mathbb{Z}$ generated by 2 is the set $(2) = \{2\, a \,;\, a \in \mathbb{Z}\}$ of even integers.

Example 5.2.5. In $\mathbb{Z}$, we have $1 \in (5, 18)$ since $1 = -7 \cdot 5 + 2 \cdot 18$, hence $\mathbb{Z} = (1) \subseteq (5, 18)$ and thus $(5, 18) = (1) = \mathbb{Z}$.

Let A be an integral domain and let $a \in A \setminus \{0\}$. By the definitions, for every element b of A, we have

$$\boxed{a \,|\, b \iff b \in (a) \iff (b) \subseteq (a).}$$

Therefore

$$a \sim b \iff (a) = (b) \qquad \text{and} \qquad a \in A^\times \iff (a) = A.$$

Exercises.

5.2.1. Prove Lemma 5.2.2.

5.2.2. Let I and J be ideals of a commutative ring A.

(i) Show that
$$I + J := \{r + s\,;\, r \in I,\, s \in J\}$$
is the smallest ideal of A containing I and J.

(ii) If $I = (a)$ and $J = (b)$, show that $I + J = (a, b)$.

5.2.3. Let $a_1, \ldots, a_s$ be nonzero elements of an integral domain A. Suppose that there exists $d \in A$ such that
$$(d) = (a_1, \ldots, a_s).$$
Show that

(i) d is nonzero and divides $a_1, \ldots, a_s$;

(ii) if a nonzero element c of A divides $a_1, \ldots, a_s$, then $c|d$.

Note. An element d of A satisfying conditions (i) and (ii) is called a *greatest common divisor of* $a_1, \ldots, a_s$ (we abbreviate *gcd*).

5.2.4. Let $a_1, \ldots, a_s$ be nonzero elements of an integral domain A. Suppose that there exists $m \in A$ such that
$$(m) = (a_1) \cap \cdots \cap (a_s).$$
Prove that

(i) m is nonzero and $a_1, \ldots, a_s$ divide m;

(ii) if a nonzero element c of A is divisible by $a_1, \ldots, a_s$, then $m|c$.

Note. An element m of A satisfying conditions (i) and (ii) is called a *least common multiple of* $a_1, \ldots, a_s$ (we abbreviate *lcm*).

5.3 Euclidean division of polynomials

Let K be a field. Every nonzero polynomial $p(x) \in K[x]$ can be written in the form

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

for an integer $n \geq 0$ and elements $a_0, a_1, \ldots, a_n$ of K with $a_n \neq 0$. This integer n is called the *degree* of $p(x)$ and is denoted $\deg(p(x))$. The coefficient a_n is called the *leading coefficient of* $p(x)$. We say that $p(x)$ is *monic* if its leading coefficient is 1.

The degree of the polynomial 0 is not defined (certain authors set $\deg(0) = -\infty$, but we will not adopt that convention in this course).

Proposition 5.3.1. *Let $p(x), q(x) \in K[x] \setminus \{0\}$. Then we have $p(x)q(x) \neq 0$ and*

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$

Proof. Write $p(x) = a_0 + \cdots + a_n x^n$ and $q(x) = b_0 + \cdots + b_m x^m$ with $a_n \neq 0$ and $b_m \neq 0$. Then the product

$$p(x)q(x) = a_0 b_0 + \cdots + a_n b_m x^{n+m}$$

has leading term $a_n b_m \neq 0$ and so

$$\deg(p(x)q(x)) = n + m = \deg(p(x)) + \deg(q(x)).$$

□

Corollary 5.3.2.

(i) $K[x]$ is an integral domain.

(ii) $K[x]^\times = K^\times = K \setminus \{0\}$.

(iii) Every polynomial $p(x) \in K[x] \setminus \{0\}$ is associated to a unique monic polynomial in $K[x]$.

Proof. Statement (i) follows directly from the preceding proposition. To prove (ii), we first note that if $p(x) \in K[x]^\times$, then there exists $q(x) \in K[x]$, such that $p(x)q(x) = 1$. Applying the proposition, we obtain

$$\deg(p(x)) + \deg(q(x)) = \deg(1) = 0,$$

hence $\deg(p(x)) = 0$ and thus $p(x) \in K \setminus \{0\} = K^\times$. This proves that $K[x]^\times \subseteq K^\times$. Since the inclusion $K^\times \subseteq K[x]^\times$ is immediate, we obtain $K[x]^\times = K^\times$. Statement (iii) is left as an exercise. □

The proof of the following result is also left as an exercise:

Proposition 5.3.3. *Let $p_1(x), p_2(x) \in K[x]$ with $p_2(x) \neq 0$. We can write*

$$p_1(x) = q(x)p_2(x) + r(x)$$

for a unique choice of polynomials $q(x) \in K[x]$ and $r(x) \in K[x]$ satisfying

$$r(x) = 0 \quad \text{or} \quad \deg(r(x)) < \deg(p_2(x)).$$

This fact is called *euclidean division*. We prove it, for fixed $p_2(x)$, by induction on the degree of $p_1(x)$ (supposing $p_1(x) \neq 0$). The polynomials $q(x)$ and $r(x)$ are called respectively the *quotient* and the *remainder* of the division of $p_1(x)$ by $p_2(x)$.

Example 5.3.4. For $K = \mathbb{Q}$, $p_1(x) = x^3 - 5x^2 + 8x - 4$ and $p_2(x) = x^2 - 2x + 1$, we see that

$$p_1(x) = (x-3)\,p_2(x) + (x-1)$$

with $\deg(x-1) = 1 < \deg(p_2(x)) = 2$.

Exercises.

5.3.1. Prove part (iii) of Corollary 5.3.2.

5.3.2. Let $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ be the field with 3 elements and let

$$p_1(x) = x^5 - x^2 + \bar{2}x + \bar{1},\ p_2(x) = x^3 - \bar{2}x + \bar{1}\ \in \mathbb{F}_3[x].$$

Determine the quotient and the remainder of the division of $p_1(x)$ by $p_2(x)$.

5.4 Euclidean domains

Definition 5.4.1 (Euclidean domain). A *euclidean domain* (or *euclidean ring*) is an integral domain A that admits a function

$$\varphi\ :\ A \setminus \{0\} \to \mathbb{N}$$

satisfying the following properties:

(i) for all $a, b \in A \setminus \{0\}$ with $a \mid b$, we have $\varphi(a) \leq \varphi(b)$,

(ii) for all $a, b \in A$ with $b \neq 0$, we can write

$$a = q\,b + r$$

with $q, r \in A$ satisfying $r = 0$ or $\varphi(r) < \varphi(b)$.

A function φ possessing these properties is called a *euclidean function*. Condition (i) is often omitted. (In fact, if A has a function satisfying Condition (ii) then it also has a function satisfying both conditions.) We have included it since it permits us to simplify certain arguments and because it is satisfied in the cases that are most important to us.

Example 5.4.2. The ring $\mathbb{Z}$ is euclidean for the absolute value function

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & \mathbb{N}\,. \\ & a & \longmapsto & |a| \end{array}$$

For any field K, the ring $K[x]$ is euclidean for the degree

$$\begin{array}{rccc} \deg : & K[x] \setminus \{0\} & \longrightarrow & \mathbb{N}\,. \\ & p(x) & \longmapsto & \deg(p(x)) \end{array}$$

For the remainder of this section, we fix a euclidean domain A and a function $\varphi\ A \setminus \{0\} \to \mathbb{N}$ as in Definition 5.4.1.

Theorem 5.4.3. *Every ideal of A is principal.*

Proof. If $I = \{0\}$, then $I = (0)$ is generated by 0. Now suppose that $I \neq \{0\}$. Then the set $I \setminus \{0\}$ is not empty and thus it contains an element a for which $\varphi(a)$ is minimal. We will show that $I = (a)$.

We first note that $(a) \subseteq I$ since $a \in I$. To show the reverse inclusion, choose $b \in I$. Since A is euclidean, we can write

$$b = q\,a + r$$

with $q, r \in A$ satisfying $r = 0$ or $\varphi(r) < \varphi(a)$. Since

$$r = b - q\,a = b + (-q)a \in I$$

(because $a, b \in I$), the choice of a implies $\varphi(r) \geq \varphi(a)$ if $r \neq 0$. So we must have $r = 0$ and so $b = q\,a \in (a)$. Since the choice of b is arbitrary, this shows that $I \subseteq (a)$. Thus $I = (a)$, as claimed. □

For an ideal generated by two elements, we can find a single generator by using the following algorithm:

Euclidean Algorithm 5.4.4. *Let $a_1, a_2 \in A$ with $a_2 \neq 0$. By repeated euclidean division, we write*

$$\begin{cases} a_1 = q_1 a_2 + a_3 & \textit{with } a_3 \neq 0 \textit{ and } \varphi(a_3) < \varphi(a_2), \\ a_2 = q_2 a_3 + a_4 & \textit{with } a_4 \neq 0 \textit{ and } \varphi(a_4) < \varphi(a_3), \\ \quad \cdots & \cdots \\ a_{k-2} = q_{k-2} a_{k-1} + a_k & \textit{with } a_k \neq 0 \textit{ and } \varphi(a_k) < \varphi(a_{k-1}), \\ a_{k-1} = q_{k-1} a_k. & \end{cases}$$

Then we have $(a_1, a_2) = (a_k)$.

An outline of a proof of this result is given in Exercise 5.4.1.

Corollary 5.4.5. *Let $a, b \in A$ with $a \neq 0$ or $b \neq 0$. Then a and b admit a gcd in A. More precisely, an element d of A is a gcd of a and b if and only if $(d) = (a, b)$.*

Proof. Let d be a generator of (a, b). Since $a \neq 0$ or $b \neq 0$, we have $(a, b) \neq (0)$ and so $d \neq 0$. Since $a, b \in (a, b) = (d)$, we first note that d divides a and b. Also, if $c \in A \setminus \{0\}$ divides a and b, then $a, b \in (c)$, hence $d \in (a, b) \subseteq (c)$ and so c divides d. This shows that d is a gcd of a and b.

If d' is another gcd of a and b, we have $d \sim d'$ (see Exercise 5.1.3), and so $(d') = (d) = (a, b)$. □

Corollary 5.4.5 implies in particular that every gcd of elements a and b of A with $a \neq 0$ or $b \neq 0$ can be written in the form

$$d = r\,a + s\,b$$

with $r, s \in A$ since such an element belongs to the ideal (a, b).

Example 5.4.6. Find the gcd of 15 and 39 and write it in the form $15r + 39s$ with $r, s \in \mathbb{Z}$.

Solution: We apply the euclidean algorithm 5.4.4 to determine the generator of $(15, 39)$. By repeated euclidean division, we find

$$39 = 2 \cdot 15 + 9 \tag{5.1}$$
$$15 = 9 + 6 \tag{5.2}$$
$$9 = 6 + 3 \tag{5.3}$$
$$6 = 2 \cdot 3 \tag{5.4}$$

hence $\gcd(15, 39) = 3$. To find r and s, we follow the chain of calculations (5.1) to (5.4) starting at the end. Doing this, we have

$$\begin{aligned} 3 &= 9 - 6 && \text{by (5.3)},\\ &= 9 - (15 - 9) = 2 \cdot 9 - 15 && \text{by (5.2)},\\ &= 2(39 - 2 \cdot 15) - 15 = 2 \cdot 39 - 5 \cdot 15 && \text{by (5.1)}. \end{aligned}$$

Therefore

$$\gcd(15, 39) = 3 = (-5) \cdot 15 + 2 \cdot 39.$$

Example 5.4.7. Find the gcd of

$$p_1(x) = x^4 + 3x^2 + x - 1 \quad \text{and} \quad p_2(x) = x^2 - 1$$

in $\mathbb{Q}[x]$ and write it in the form $a_1(x)\,p_1(x) + a_2(x)\,p_2(x)$ with $a_1(x), a_2(x) \in \mathbb{Q}[x]$.

Solution: By repeated repeated division, we have

$$p_1(x) = (x^2+4)p_2(x) + (x+3) \tag{5.5}$$
$$p_2(x) = (x-3)(x+3) + 8 \tag{5.6}$$
$$x+3 = (1/8)(x+3)\cdot 8 \tag{5.7}$$

hence $\gcd(p_1(x), p_2(x)) = 8$ (or 1). Retracing the calculation starting at the end, we find

$$\begin{aligned} 8 &= p_2(x) - (x-3)(x+3) && \text{by (5.6)}, \\ &= p_2(x) - (x-3)(p_1(x) - (x^2+4)p_2(x)) && \text{by (5.5)}, \\ &= (3-x)\,p_1(x) + (x^3 - 3\,x^2 + 4\,x - 11)\,p_2(x)\,. \end{aligned}$$

Another consequence of Theorem 5.4.3 is the following result which will play a key role later.

Theorem 5.4.8. *Let p be an irreducible element of A and let $a, b \in A$. Suppose that $p \mid ab$. Then we have $p \mid a$ or $p \mid b$.*

Proof. Suppose that $p \nmid a$. We have to show that $p \mid b$. To do this, we choose d such that $(p, a) = (d)$. Since $d \mid p$ and p is irreducible, we have $d \sim 1$ or $d \sim p$. Since we also have $d \mid a$ and $p \nmid a$, the possibility $d \sim p$ is excluded. Thus d is a unit of A and so

$$1 \in (d) = (p, a).$$

This implies that we can write $1 = r\,p + s\,a$ with $r, s \in A$. Then $b = (r\,p + s\,a)b = r\,b\,p + s\,a\,b$ is divisible by p, since $p \mid a\,b$. □

By induction, this result can be generalized to an arbitrary product of elements of A:

Corollary 5.4.9. *Let p be an irreducible element of A and let $a_1, \ldots, a_s \in A$. Suppose that $p \mid a_1 \cdots a_s$. Then p divides at least one of the elements $a_1, \ldots, a_s$.*

Exercises.

5.4.1. Let a_1 and a_2 be elements of a euclidean domain A, with $a_2 \neq 0$.

(i) Show that Algorithm 5.4.4 terminates after a finite number of steps.

(ii) In the notation of this algorithm, show that $(a_i, a_{i+1}) = (a_{i+1}, a_{i+2})$ for all $i = 1, \ldots, k-2$.

(iii) In the same notation, show that $(a_{k-1}, a_k) = (a_k)$.

(iv) Conclude that $(a_1, a_2) = (a_k)$.

5.4.2. Find the gcd of $f(x) = x^3 + x - 2$ and $g(x) = x^5 - x^4 + 2x^2 - x - 1$ in $\mathbb{Q}[x]$ and express it as a linear combination of $f(x)$ and $g(x)$.

5.4.3. Find the gcd of $f(x) = x^3 + \bar{1}$ and $g(x) = x^5 + x^4 + x + \bar{1}$ in $\mathbb{F}_2[x]$ and express it as a linear combination of $f(x)$ and $g(x)$.

5.4.4. Find the gcd of 114 and 45 in $\mathbb{Z}$ and express it as a linear combination of 114 and 45.

5.4.5. Let $a_1, \ldots, a_s$ be elements, not all zero, of a euclidean domain A.

(i) Show that $a_1, \ldots, a_s$ admit a gcd in A in the sense of Exercise 5.2.3.

(ii) If $s \geq 3$, show that $\gcd(a_1, \ldots, a_s) = \gcd(a_1, \gcd(a_2, \ldots, a_s))$.

5.4.6. Let $a_1, \ldots, a_s$ be nonzero elements of a euclidean domain A.

(i) Show that $a_1, \ldots, a_s$ admit an lcm in A in the sense of Exercise 5.2.4.

(ii) If $s \geq 3$, show that $\operatorname{lcm}(a_1, \ldots, a_s) = \operatorname{lcm}(a_1, \operatorname{lcm}(a_2, \ldots, a_s))$.

5.4.7. Find the gcd of 42, 63 and 140 in $\mathbb{Z}$, and express it as a linear combination of the three integers (see Exercise 5.4.5).

5.4.8. Find the gcd of $x^4 - 1$, $x^6 - 1$ and $x^3 + x^2 + x + 1$ in $\mathbb{Q}[x]$, and express it as a linear combination of the three polynomials (see Exercise 5.4.5).

5.5 The Unique Factorization Theorem

We again fix a euclidean domain A and a function $\varphi : A \setminus \{0\} \to \mathbb{N}$ as in Definition 5.4.1. The results of the preceding section only rely on the second property of φ required by Definition 5.4.1. The following result uses the first property.

Proposition 5.5.1. *Let $a, b \in A \setminus \{0\}$ with $a \mid b$. Then we have*

$$\varphi(a) \leq \varphi(b)$$

with equality if and only if $a \sim b$.

Proof. Since $a \mid b$, we have $\varphi(a) \leq \varphi(b)$ as required in Definition 5.4.1.

If $a \sim b$, we also have $b \mid a$, hence $\varphi(b) \leq \varphi(a)$ and so $\varphi(a) = \varphi(b)$.

Conversely, suppose that $\varphi(a) = \varphi(b)$. We can write

$$a = q\,b + r$$

with $q, r \in A$ satisfying $r = 0$ or $\varphi(r) < \varphi(b)$. Since $a \mid b$, we see that a divides $r = a - q\,b$, hence $r = 0$ or $\varphi(a) \leq \varphi(r)$. Since $\varphi(a) = \varphi(b)$, the only possibility is that $r = 0$. This implies that $a = q\,b$, hence $b \mid a$ and thus $a \sim b$. $\square$

Applying this result with $a = 1$, we deduce the following.

Corollary 5.5.2. *Let $b \in A \setminus \{0\}$. We have $\varphi(b) \geq \varphi(1)$ with equality if and only if $b \in A^\times$.*

We are now ready to prove the main result of this chapter.

Theorem 5.5.3 (Unique Factorization Theorem). *Let $a \in A \setminus \{0\}$. There exists a unit $u \in A^\times$, an integer $r \geq 0$ and irreducible elements $p_1, \ldots, p_r$ of A such that*

$$a = u\, p_1 \cdots p_r. \tag{5.8}$$

For every other factorization of a as a product

$$a = u'\, q_1 \cdots q_s \tag{5.9}$$

of a unit $u' \in A^\times$ and irreducible elements $q_1, \ldots, q_s$ of A, we have $s = r$ and there exists a permutation $(i_1, i_2, \ldots, i_r)$ of $(1, 2, \ldots, r)$ such that

$$q_1 \sim p_{i_1}\,,\ q_2 \sim p_{i_2}\,,\ \ldots\,,\ q_r \sim p_{i_r}.$$

Proof. **1st Existence:** We first show the existence of a factorization of the form (5.8) by induction on $\varphi(a)$.

If $\varphi(a) \leq \varphi(1)$, Corollary 5.5.2 tells us that $\varphi(a) = \varphi(1)$ and that $a \in A^\times$. In this case, Equality (5.8)) is satisfied for the choices $u = a$ and $r = 0$.

Now suppose that $\varphi(a) > \varphi(1)$. Among the divisors p of a with $\varphi(p) > \varphi(1)$, we choose one for which $\varphi(p)$ is minimal. If q is a divisor of this element p then $q \,|\, a$ and so we have $\varphi(q) = \varphi(1)$ or $\varphi(q) \geq \varphi(p)$. By Proposition 5.5.1, this implies that $q \sim 1$ or $q \sim p$. Since this is true for every divisor q of p, we conclude that p is irreducible. Write $a = b\,p$ with $b \in A$. Since $b \,|\, a$ and $b \not\sim a$, Proposition 5.5.1 gives $\varphi(b) < \varphi(a)$. By induction, we can assume that b admits a factorization of the type (5.8). Then $a = b\,p$ also admits such a factorization (with the additional factor p).

2nd Uniqueness: Suppose that a also admits the factorization (5.9). We we have

$$u\, p_1 \cdots p_r = u'\, q_1 \cdots q_s \tag{5.10}$$

where u, u' are units and $p_1, \ldots, p_r, q_1, \cdots, q_s$ are irreducible elements of A. If $r = 0$, the left side of this equality is simply u and since no irreducible element of A can divide a unit, this implies that $s = 0$ as required. Now suppose that $r \geq 1$. Since p_1 divides $u\, p_1 \cdots p_r$, it also divides $u'\, q_1 \cdots q_s$. Since p_1 is irreducible, this implies, by Corollary 5.4.9, that p_1 divides at least one of the factors $q_1, \ldots, q_s$ (since $p_1 \nmid u'$). Permuting $q_1, \ldots, q_s$ if necessary, we can assume that $p_1 \,|\, q_1$. Then we have $q_1 = u_1 p_1$ for a unit $u_1 \in A^\times$, and Equality (5.10) gives

$$u\, p_2 \cdots p_r = u''\, q_2 \cdots q_s$$

where $u'' = u' u_1 \in A^\times$. Since the left side of this new equality contains one less irreducible factor, we can assume, by induction, that this implies $r - 1 = s - 1$ and $q_2 \sim p_{i_2}, \ldots, q_r \sim p_{i_r}$ for some permutation $(i_2, \ldots, i_r)$ of $(2, \ldots, r)$. Then $r = s$ and $q_1 \sim p_1$, $q_2 \sim p_{i_2}$, $\ldots$, $q_r \sim p_{i_r}$ as desired. $\square$

Because the group of units of $\mathbb{Z}$ is $\mathbb{Z}^\times = \{1, -1\}$ and every irreducible element of $\mathbb{Z}$ is associated to a unique (positive) prime p, we conclude:

Corollary 5.5.4. *Every nonzero integer a can be written in the form*

$$a = \pm p_1 \cdots p_r$$

for a choice of sign $\pm$, an integer $r \geq 0$ and prime numbers $p_1, \ldots, p_r$. This expression is unique up to a permutation of $p_1, \ldots, p_r$.

If $r = 0$, we interpret the product $\pm p_1 \cdots p_r$ as being ± 1.

Since we can order the prime number by their size, we can deduce:

Corollary 5.5.5. *For every nonzero integer a, there exists a unique choice of sign $\pm$, an integer $s \geq 0$, prime numbers $p_1 < p_2 < \cdots < p_s$ and positive integers $e_1, e_2, \ldots, e_s$ such that*

$$a = \pm p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}.$$

Similarly, if K is a field, we know that $K[x]^\times = K^\times$ and that every irreducible polynomial of $K[x]$ is associated to a unique irreducible monic polynomial. However, there is no natural order on $K[x]$. Therefore we have:

Corollary 5.5.6. *Let K be a field and let $a(x) \in K[x] \setminus \{0\}$. There exists a constant $c \in K^\times$, an integer $s \geq 0$, irreducible* distinct *monic polynomials $p_1(x), \ldots, p_s(x)$ of $K[x]$ and positive integers $e_1, \ldots, e_s$ such that*

$$a(x) = c\, p_1(x)^{e_1} \cdots p_s(x)^{e_s}.$$

This factorization is unique up to permutation of the factors $p_1(x)^{e_1}, \ldots, p_s(x)^{e_s}$.

Exercises.

5.5.1. Let a be a nonzero element of a euclidean domain A. Write $a = up_1^{e_1} \cdots p_s^{e_s}$ where u is a unit of A, where $p_1, \ldots, p_s$ are irreducible elements of A, pairwise non-associated, and where $e_1, \ldots, e_s$ are integers ≥ 0 (we set $p^0 = 1$). Show that the divisors of a are the products $vp_1^{d_1} \cdots p_s^{d_s}$ where v is a unit of A and where $d_1, \ldots, d_s$ are integers with $0 \leq d_i \leq e_i$ for $i = 1, \ldots, s$.

5.5.2. Let a and b be nonzero elements of euclidean domain A and let $p_1, \ldots, p_s$ be a maximal system of irreducible divisors, pairwise non-associated, of ab.

(i) Show that we can write

$$a = up_1^{e_1} \cdots p_s^{e_s} \quad \text{and} \quad b = vp_1^{f_1} \cdots p_s^{f_s}$$

with $u, v \in A^\times$ and $e_1, \ldots, e_s, f_1, \ldots, f_s \in \mathbb{N}$.

(ii) Show that
$$\gcd(a,b) \sim p_1^{d_1} \cdots p_s^{d_s}$$
where $d_i = \min(e_i, f_i)$ for $i = 1, \ldots, s$.

(iii) Show that
$$\operatorname{lcm}(a,b) \sim p_1^{h_1} \cdots p_s^{h_s}$$
where $h_i = \max(e_i, f_i)$ for $i = 1, \ldots, s$ (see Exercise 5.2.4 for the notion of lcm).

Hint. For (ii), use the result of Exercise 5.5.1.

5.6 The Fundamental Theorem of Algebra

Fix a field K. We first note:

Proposition 5.6.1. *Let $a(x) \in K[x]$ and $r \in K$. The polynomial $x - r$ divides $a(x)$ if and only if $a(r) = 0$.*

Proof. Dividing $a(x)$ by $x - r$, we see that
$$a(x) = q(x)(x - r) + b$$
where $q(x) \in K[x]$ and $b \in K$ since the remainder in the division is zero or of degree $< \deg(x - r) = 1$. Evaluating the two sides of this equality at $x = r$, we obtain $a(r) = b$. The conclusion follows. □

Definition 5.6.2 (Root). Let $a(x) \in K[x]$. We say that an element r of K is a *root* of $a(x)$ if $a(r) = 0$.

The Alembert-Gauss Theorem, also called the *Fundamental Theorem of Algebra* is in fact a theorem in analysis which can be stated as follows:

Theorem 5.6.3 (Alembert-Gauss Theorem)**.** *Every polynomial $a(x) \in \mathbb{C}[x]$ of degree ≥ 1 has at least one root in $\mathbb{C}$.*

We will accept this result without proof. In light of Proposition 5.6.1, it implies that the irreducible monic polynomials of $\mathbb{C}[x]$ are of the form $x - r$ with $r \in \mathbb{C}$. By Corollary 5.5.6, we conclude:

Theorem 5.6.4. *Let $a(x) \in \mathbb{C}[x] \setminus \{0\}$, let $r_1, \ldots, r_s$ be the distinct roots of $a(x)$ in $\mathbb{C}$, and let c be the leading coefficient of $a(x)$. There exists a unique choice of integers $e_1, \ldots, e_s \geq 1$ such that*
$$a(x) = c(x - r_1)^{e_1} \cdots (x - r_s)^{e_s}.$$
The integer e_i is called the multiplicity *of the root r_i of $a(x)$.*

Theorem 5.6.3 also sheds light on the irreducible polynomials of $\mathbb{R}[x]$.

Theorem 5.6.5. *The monic irreducible polynomials of* $\mathbb{R}[x]$ *are of the form* $x-r$ *with* $r \in \mathbb{R}$ *or of the form* $x^2 + b\,x + c$ *with* $b, c \in \mathbb{R}$ *and* $b^2 - 4c < 0$.

Proof. Let $p(x)$ be a monic irreducible polynomial in $\mathbb{R}[x]$. By Theorem 5.6.3, it has at least one root r in $\mathbb{C}$. If $r \in \mathbb{R}$, then $x - r$ divides $p(x)$ in $\mathbb{R}[x]$ and so $p(x) = x - r$. If $r \notin \mathbb{R}$, then the complex conjugate $\bar{r}$ of r is different from r and, since

$$p(\bar{r}) = \overline{p(r)} = 0,$$

it is also a root of $p(x)$. Therefore, $p(x)$ is divisible by $(x - r)(x - \bar{r})$ in $\mathbb{C}[x]$. Since this product can be written as $x^2 + b\,x + c$ with $b = -(r + \bar{r}) \in \mathbb{R}$ and $c = r\bar{r} \in \mathbb{R}$, the quotient of $p(x)$ by $x^2 + b\,x + c$ is a polynomial in $\mathbb{R}[x]$ and so $p(x) = x^2 + b\,x + c$. Since the roots of $p(x)$ in $\mathbb{C}$ are not real, we must have $b^2 - 4c < 0$. □

Exercises.

5.6.1. Let K be a field and let $p(x)$ be a nonzero polynomial of $K[x]$.

(i) Suppose that $\deg(p(x)) = 1$. Show that $p(x)$ is irreducible.

(ii) Suppose that $2 \leq \deg(p(x)) \leq 3$. Show that $p(x)$ is irreducible if and only if it does not have a root in K.

(iii) In general, show that $p(x)$ is irreducible if and only if it does not have any irreducible factors of degree $\leq \deg(p(x))/2$ in $K[x]$.

5.6.2. Let $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ be the finite field with 3 elements.

(i) Find all the irreducible monic polynomials of $\mathbb{F}_3[x]$ of degree at most 2.

(ii) Show that $x^4 + x^3 + \bar{2}$ is an irreducible polynomial of $\mathbb{F}_3[x]$.

(iii) Factor $x^5 + \bar{2}x^4 + \bar{2}x^3 + x^2 + x + \bar{2}$ as a product of irreducible polynomials of $\mathbb{F}_3[x]$.

5.6.3. Find all the irreducible monic polynomials of $\mathbb{F}_2[x]$ of degree at most 4 where $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ is the finite field with 2 elements.

5.6.4. Factor $x^4 - 2$ as a product of irreducible polynomials (i) in $\mathbb{R}[x]$, (ii) in $\mathbb{C}[x]$.

5.6.5. Let V be a vector space of finite dimension $n \geq 1$ over $\mathbb{C}$ and let $T\colon V \to V$ be a linear operator. Show that T has an least one eigenvalue.

5.6.6. Let V be a vector space of finite dimension $n \geq 1$ over a field K, let $T\colon V \to V$ be a linear operator over V, and let $\lambda_1, \ldots, \lambda_s$ be the distinct eigenvalues of T in K. Show that T is diagonalizable if and only if

$$\operatorname{char}_T(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_s)^{e_s}$$

where $e_i = \dim_K E_{\lambda_i}(T)$ for $i = 1, \ldots, s$.

Hint. Use Theorem 3.2.3.

5.6.7. Let $A \in \operatorname{Mat}_{n\times n}(K)$ where n is a positive integer and K is a field. State and prove a necessary and sufficient condition, analogous to that of Exercise 5.6.6, for A to be diagonalizable over K.

Chapter 6

Modules

The notion of a module is a natural extension of that of a vector space. The difference is that the scalars no longer lie in a field but rather in a ring. This permits one to encompass more objects. For example, we will see that an abelian group is a module over the ring $\mathbb{Z}$ of integers. We will also see that if V is a vector space over a field K equipped with a linear operator, then V is naturally a module over the ring $K[x]$ of polynomials in one variable over K. In this chapter, we introduce in a general manner the theory of modules over a commutative ring and the notions of submodule, free module, direct sum, homomorphism and isomorphism of modules. We interpret these constructions in several contexts, the most important for us being the case of a vector space over a field K equipped with a linear operator.

6.1 The notion of a module

Definition 6.1.1 (Module). A *module* over a commutative ring A is a set M equipped with an addition and a multiplication by the elements of A:

$$\begin{array}{rcl} M \times M & \longrightarrow & M \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} + \mathbf{v} \end{array} \qquad \text{and} \qquad \begin{array}{rcl} A \times M & \longrightarrow & M \\ (a, \mathbf{u}) & \longmapsto & a\,\mathbf{u} \end{array}$$

that satisfies the following axioms:

$$\left.\begin{array}{ll} \textbf{Mod1}. & \mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w} \\ \textbf{Mod2}. & \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} \end{array}\right\} \text{for all } \mathbf{u}, \mathbf{v}, \mathbf{w} \in M.$$

Mod3. There exists $\mathbf{0} \in M$ such that $\mathbf{u} + \mathbf{0} = \mathbf{u}$ for all $\mathbf{u} \in M$.
Mod4. For all $\mathbf{u} \in M$, there exists $-\mathbf{u} \in M$ such that $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.

$$\left.\begin{array}{ll} \textbf{Mod5}. & 1\mathbf{u} = \mathbf{u} \\ \textbf{Mod6}. & a(b\mathbf{u}) = (ab)\mathbf{u} \\ \textbf{Mod7}. & (a+b)\mathbf{u} = a\,\mathbf{u} + b\,\mathbf{u} \\ \textbf{Mod8}. & a(\mathbf{u} + \mathbf{v}) = a\,\mathbf{u} + a\,\mathbf{v} \end{array}\right\} \text{for all } a, b \in A \text{ and } \mathbf{u}, \mathbf{v} \in M.$$

In what follows, we will speak of a *module over* A or of an A-*module* to designate such an object.

If we compare the definition of a module over a commutative ring A to that of a vector space over a field K (see Definition 1.1.1), we recognize the same axioms. Since a field is a particular type of commutative ring, we deduce:

Example 6.1.2. A module over a field K is simply a vector space over K.

Axioms **Mod1** to **Mod4** imply that a module M is an abelian group under addition (see Appendix A). From this we deduce that the order in which we add elements $\mathbf{u}_1, \dots, \mathbf{u}_n$ of M does not affect their sum, denoted

$$\mathbf{u}_1 + \cdots + \mathbf{u}_n \quad \text{or} \quad \sum_{i=1}^{n} \mathbf{u}_i.$$

The element $\mathbf{0}$ of M characterized by axiom **Mod3** is called the *zero* of M (it is the identity element for the addition). Finally, for each $\mathbf{u} \in M$, the element $-\mathbf{u}$ of M characterized by axiom **Mod 4** is called the *additive inverse* of $\mathbf{u}$. We define subtraction in M by

$$\mathbf{u} - \mathbf{v} := \mathbf{u} + (-\mathbf{v}).$$

We also verify, by induction on n, that the axioms of distributivity **Mod7** and **Mod8** imply in general

$$\left(\sum_{i=1}^{n} a_i\right)\mathbf{u} = \sum_{i=1}^{n} a_i\mathbf{u} \quad \text{and} \quad a\sum_{i=1}^{n} \mathbf{u}_i = \sum_{i=1}^{n} a\,\mathbf{u}_i \tag{6.1}$$

for all $a, a_1, \dots, a_n \in A$ and $\mathbf{u}, \mathbf{u}_1, \dots, \mathbf{u}_n \in M$.

We also show:

Lemma 6.1.3. *Let M be a module over a commutative ring A. For all $a \in A$ and all $\mathbf{u} \in M$, we have*

(i) $0\mathbf{u} = \mathbf{0}$ *and* $a\mathbf{0} = \mathbf{0}$

(ii) $(-a)\mathbf{u} = a(-\mathbf{u}) = -(a\,\mathbf{u})$.

Proof. In A, we have $0 + 0 = 0$. Then axiom **Mod7** gives

$$0\mathbf{u} = (0 + 0)\mathbf{u} = 0\mathbf{u} + 0\mathbf{u},$$

hence $0\mathbf{u} = \mathbf{0}$. More generally, since $a + (-a) = 0$, the same axiom gives

$$0\mathbf{u} = (a + (-a))\mathbf{u} = a\,\mathbf{u} + (-a)\mathbf{u}.$$

Since $0\mathbf{u} = \mathbf{0}$, this implies that $(-a)\mathbf{u} = -(a\,\mathbf{u})$.

The relations $a\mathbf{0} = \mathbf{0}$ and $a(-\mathbf{u}) = -(a\,\mathbf{u})$ are proven in a similar manner by applying instead axiom **Mod8**. $\square$

Suppose that M is an $\mathbb{Z}$-module, that is, a module over $\mathbb{Z}$. Then M is an abelian group under addition and, for every integer $n \geq 1$ and for all $\mathbf{u} \in M$, the general formulas for distributivity (6.1) give

$$n\,\mathbf{u} = (\underbrace{1 + \cdots + 1}_{n \text{ times}})\mathbf{u} = \underbrace{1\mathbf{u} + \cdots + 1\mathbf{u}}_{n \text{ times}} = \underbrace{\mathbf{u} + \cdots + \mathbf{u}}_{n \text{ times}}.$$

Thanks to Lemma 6.1.3, we also find that

$$(-n)\mathbf{u} = n(-\mathbf{u}) = \underbrace{(-\mathbf{u}) + \cdots + (-\mathbf{u})}_{n \text{ times}} \quad \text{and} \quad 0\mathbf{u} = \mathbf{0}.$$

In other words, multiplication by the integers in M is entirely determined by the addition law in M and corresponds to the natural notion of product by an integer in an abelian group. Conversely, if M is an abelian group, the rule of "exponents" (Proposition A.2.11 of Appendix A) implies that the product by an integer in M satisfies axioms **Mod6** to **Mod8**. Since it clearly satisfies axiom **Mod5**, we conclude:

Proposition 6.1.4. *A $\mathbb{Z}$-module is simply an abelian group equipped with the natural multiplication by the integers.*

The following proposition gives a third example of modules.

Proposition 6.1.5. *Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$ be a linear operator on V. Then V is a $K[x]$-module for the addition of V and the multiplication by polynomials given by*

$$p(x)\mathbf{v} := p(T)(\mathbf{v})$$

for all $p(x) \in K[x]$ and all $\mathbf{v} \in V$.

Proof. Since V is an abelian group under addition, it suffices to verify axioms **Mod5** to **Mod8**. Let $p(x), q(x) \in K[x]$ and $\mathbf{u}, \mathbf{v} \in V$. We must show:

1) $1\mathbf{v} = \mathbf{v}$,

2) $p(x)(q(x)\mathbf{v}) = (p(x)q(x))\mathbf{v}$,

3) $(p(x) + q(x))\mathbf{v} = p(x)\mathbf{v} + q(x)\mathbf{v}$,

4) $p(x)(\mathbf{u} + \mathbf{v}) = p(x)\mathbf{u} + p(x)\mathbf{v}$.

By the definition of the product by a polynomial, this reduces to showing

1′) $I_V(\mathbf{v}) = \mathbf{v}$,

2′) $p(T)(q(T)\mathbf{v}) = (p(T) \circ q(T))\mathbf{v}$,

3′) $(p(T) + q(T))\mathbf{v} = p(T)\mathbf{v} + q(T)\mathbf{v}$,

4′) $p(T)(\mathbf{u}+\mathbf{v}) = p(T)\mathbf{u} + p(T)\mathbf{v}$,

because the map

$$\begin{array}{ccc} K[x] & \longrightarrow & \mathrm{End}_K(V)\,, \\ r(x) & \longmapsto & r(T) \end{array}$$

of evaluation at T, being a ring homomorphism, maps 1 to I_V, $p(x)+q(x)$ to $p(T)+q(T)$ and $p(x)q(x)$ to $p(T)\circ q(T)$. Equalities 1′), 2′) and 3′) follow from the definitions of I_V, $p(T)\circ q(T)$ and $p(T)+q(T)$ respectively. Finally, 4′) follows from the fact that $p(T)$ is a linear map. □

In the context of Proposition 6.1.5, we also note that, for a constant polynomial $p(x) = a$ with $a \in K$, we have

$$p(x)\mathbf{v} = (a\,I)(\mathbf{v}) = a\,\mathbf{v}$$

for all $\mathbf{v} \in V$. Thus the notation $a\,\mathbf{v}$ has the same meaning if we consider a as a polynomial of $K[x]$ or as a scalar of the field K. We can then state the following complement to Proposition 6.1.5.

Proposition 6.1.6. *In the notation of Proposition 6.1.5, the external multiplication by the elements of $K[x]$ on V extends the scalar multiplication by the elements of K.*

Example 6.1.7. Let V be a vector space of dimension 2 over $\mathbb{Q}$ equipped with a basis $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$ and let $T\colon V \to V$ be the linear operator determined by the conditions

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

We equip V with the structure of a $\mathbb{Q}[x]$-module associated to the endomorphism T and calculate

$$(2x-1)\mathbf{v}_1 + (x^2+3x)\mathbf{v}_2.$$

By definition, we have

$$\begin{aligned} (2\,T - I)(\mathbf{v}_1) + (T^2 + 3\,T)(\mathbf{v}_2) &= 2\,T(\mathbf{v}_1) - \mathbf{v}_1 + T^2(\mathbf{v}_2) + 3\,T(\mathbf{v}_2) \\ &= 3\,T(\mathbf{v}_1) - \mathbf{v}_1 + 3\,T(\mathbf{v}_2) \quad (\text{car } T^2(\mathbf{v}_2) = T(T(\mathbf{v}_2)) = T(\mathbf{v}_1)) \\ &= 3(\mathbf{v}_1 - \mathbf{v}_2) - \mathbf{v}_1 + 3\mathbf{v}_1 \\ &= 5\mathbf{v}_1 - 3\mathbf{v}_2. \end{aligned}$$

Fix an arbitrary commutative ring A. We conclude with three general examples of A-modules. The details of the proofs are left as exercises.

Example 6.1.8. The ring A is an A-module for its addition law and the external multplication

$$\begin{array}{ccc} A \times A & \longrightarrow & A \\ (a, \mathbf{u}) & \longmapsto & a\,\mathbf{u} \end{array}$$

given by the product in A.

Example 6.1.9. Let $n \in \mathbb{N}_{>0}$. The set

$$A^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} ; a_1, a_2, \dots, a_n \in A \right\}$$

of n-tuples of elements of A is a module over A for the operations

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad \text{and} \quad c \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} c\, a_1 \\ c\, a_2 \\ \vdots \\ c\, a_n \end{pmatrix}.$$

For $n = 1$, we recover the natural structure of A-module on $A^1 = A$ described by Example 6.1.8.

Example 6.1.10. Let $M_1, \dots, M_n$ be A-modules. Their cartesian product

$$M_1 \times \cdots \times M_n = \{(\mathbf{u}_1, \dots, \mathbf{u}_n) ; \mathbf{u}_1 \in M_1, \dots, \mathbf{u}_n \in M_n\}$$

is an A-module for the operations

$$\begin{aligned} (\mathbf{u}_1, \dots, \mathbf{u}_n) + (\mathbf{v}_1, \dots, \mathbf{v}_n) &= (\mathbf{u}_1 + \mathbf{v}_1, \dots, \mathbf{u}_n + \mathbf{v}_n), \\ c\,(\mathbf{u}_1, \dots, \mathbf{u}_n) &= (c\,\mathbf{u}_1, \dots, c\,\mathbf{u}_n). \end{aligned}$$

Remark. If we apply the construction of Example 6.1.10 with $M_1 = \cdots = M_n = A$ for the natural A-module structure on A given by Example 6.1.8, we obtain the structure of an A-module on $A \times \cdots \times A = A^n$ that is essentially that of Example 6.1.9 except that the elements of A^n are presented in rows. For other applications, it is nevertheless more convenient to write the elements of A^n in columns.

Exercises.

6.1.1. Complete the proof of Lemma 6.1.3 by showing that $a\,\mathbf{0} = \mathbf{0}$ and $a(-\mathbf{u}) = -(a\,\mathbf{u})$.

6.1.2. Let V be a vector space of dimension 3 over $\mathbb{F}_5$ equipped with a basis $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ and let $T\colon V \to V$ be a linear operator determined by the conditions

$$T(\mathbf{v}_1) = \mathbf{v}_1 + \bar{2}\mathbf{v}_2 - \mathbf{v}_3, \quad T(\mathbf{v}_2) = \mathbf{v}_2 + \bar{4}\mathbf{v}_3, \quad T(\mathbf{v}_3) = \mathbf{v}_3.$$

For the corresponding structure of an $\mathbb{F}_5[x]$-module on V, calculate

(i) $x\,\mathbf{v}_1$,

(ii) $x^2\,\mathbf{v}_1 - (x+\bar{1})\mathbf{v}_2$,

(iii) $(\bar{2}x^2 - \bar{3})\mathbf{v}_1 + (\bar{3}x)\mathbf{v}_2 + (x^2+\bar{2})\mathbf{v}_3$.

6.1.3. Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be a linear operator whose matrix in the standard basis $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2\}$ is $[\,T\,]_{\mathcal{E}} = \begin{pmatrix} 2 & -1 \\ 3 & 0 \end{pmatrix}$. For the associated $\mathbb{R}[x]$-module structure on $\mathbb{R}^2$, calculate

(i) $x\,\mathbf{e}_1$,

(ii) $x^2\,\mathbf{e}_1 + \mathbf{e}_2$,

(iii) $(x^2+x+1)\mathbf{e}_1 + (2x-1)\mathbf{e}_2$.

6.1.4. Let $n \in \mathbb{N}_{>0}$ and let A be a commutative ring. Show that A^n is an A-module for the operations defined in Example 6.1.9.

6.1.5. Let $M_1, \ldots, M_n$ be modules over a commutative ring A. Show that their cartesian product $M_1 \times \cdots \times M_n$ is an A-module for the operations defined in Example 6.1.10.

6.1.6. Let M be a module over the commutative ring A and let X be a set. For all $a \in A$ and every pair of functions $f\colon X \to M$ and $g\colon X \to M$, we define $f+g\colon X \to M$ and $af\colon X \to M$ by setting

$$(f+g)(x) = f(x) + g(x) \quad \text{and} \quad (af)(x) = af(x)$$

for all $x \in X$. Show that the set $\mathcal{F}(X, M)$ of functions from X to M is an A-module for these operations.

6.2 Submodules

Fix an arbitrary module M over an arbitrary commutative ring A.

Definition 6.2.1 (Submodule). An A-*submodule* of M is a subset N of M satisfying the following conditions:

SM1. $\mathbf{0} \in N$.
SM2. If $\mathbf{u}, \mathbf{v} \in N$, then $\mathbf{u} + \mathbf{v} \in N$.
SM3. If $a \in A$ and $\mathbf{u} \in N$, then $a\,\mathbf{u} \in N$.

Note that condition **SM3** implies that $-\mathbf{u} = (-1)\mathbf{u} \in N$ for all $\mathbf{u} \in N$ which, together with conditions **SM1** and **SM2**, implies that an A-submodule of M is, in particular, a subgroup of M.

Conditions **SM2** and **SM3** require that an A-submodule N of M be stable under the addition in M and the multiplication by elements of A in M. By restriction, these operations therefore define an addition on N and a multiplication by elements of A on N. We leave it as an exercise to verify that these operations satisfy the 8 axioms required for N to be an A-module.

Proposition 6.2.2. *An A-submodule N of M is itself an A-module for the addition and multiplication by the elements of A restricted from M to N.*

Example 6.2.3. Let V be a vector space over a field K. A K-submodule of V is simply a vector subspace of V.

Example 6.2.4. Let M be an abelian group. A $\mathbb{Z}$-submodule of M is simply a subgroup of M.

Example 6.2.5. Let A be a commutative ring considered as a module for itself (see Example 6.1.8). An A-submodule of A is simply an ideal of A.

In the case of a vector space V equipped with an endomorphism, the concept of submodule translates as follows:

Proposition 6.2.6. *Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$. For the corresponding structure of a $K[x]$-module on V, a $K[x]$-submodule of V is simply a T-*invariant *vector subspace of V, that is a vector subspace U of V such that $T(\mathbf{u}) \in U$ for all $\mathbf{u} \in U$.*

Proof. Since the multiplication by elements of $K[x]$ on V extends the scalar multiplication by the elements of K (see Proposition 6.1.6), a $K[x]$-submodule U of B is necessarily a vector subspace of V. Since it also satisfies $x\mathbf{u} \in U$ for all $\mathbf{u} \in U$, and $x\mathbf{u} = T(\mathbf{u})$ (by definition), we also see that U must be T-invariant.

Conversely, if U is a T-invariant vector subspace of U, we have $T(\mathbf{u}) \in U$ for all $\mathbf{u} \in U$. By induction on n, we deduce that $T^n(\mathbf{u}) \in U$ for every integer $n \geq 1$ and all $\mathbf{u} \in U$. Therefore, for every polynomial $p(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ and $\mathbf{u} \in U$, we have

$$p(x)\mathbf{u} = (a_0I + a_1T + \cdots + a_nT^n)(\mathbf{u}) = a_0\mathbf{u} + a_1T(\mathbf{u}) + \cdots + a_nT^n(\mathbf{u}) \in U.$$

Thus U is a $K[x]$-submodule of V: we have just showed that it satisfies condition **SM3** and the other conditions **SM1** and **SM2** are satisfied by virtue of the fact that U is a subspace of V. □

We conclude this section with several valuable general constructions for an arbitrary A-module.

Proposition 6.2.7. *Let $\mathbf{u}_1, \ldots, \mathbf{u}_s$ be elements of an A-module M. The set*

$$\{a_1\,\mathbf{u}_1 + \cdots + a_s\,\mathbf{u}_s\,;\, a_1, \ldots, a_s \in A\}$$

is an A-submodule of M that contains $\mathbf{u}_1, \ldots, \mathbf{u}_s$ and it is the smallest A-submodule of M with this property.

This A-submodule is called the A-submodule of M *generated* by $\mathbf{u}_1, \ldots, \mathbf{u}_s$. It is denoted

$$\langle \mathbf{u}_1, \ldots, \mathbf{u}_s \rangle_A \quad \text{or} \quad A\,\mathbf{u}_1 + \cdots + A\,\mathbf{u}_s.$$

The proof of this result is left as an exercise.

Definition 6.2.8 (Cyclic module and finite type module). We say that an A-module M (or an A-submodule of M) is *cyclic* if it is generated by a single element. We say that it is of *finite type* (or is *finitely generated*) if it is generated by a finite number of elements of M.

Example 6.2.9. If $\mathbf{u}_1, \dots, \mathbf{u}_s$ are elements of an abelian group M, then $\langle \mathbf{u}_1, \dots, \mathbf{u}_s \rangle_{\mathbb{Z}}$ is simply the subgroup of M generated by $\mathbf{u}_1, \dots, \mathbf{u}_s$. In particular, M is cyclic as an abelian group if and only if it is cyclic as a $\mathbb{Z}$-module.

Example 6.2.10. Let V be a finite-dimensional vector space over a field K, let $\{\mathbf{v}_1, \dots, \mathbf{v}_s\}$ be a set of generators of V, and let $T \in \mathrm{End}_K(V)$. Since the structure of a $K[x]$-module on V associated to T extends that of a K-module, we have

$$V = \langle \mathbf{v}_1, \dots, \mathbf{v}_s \rangle_K \subseteq \langle \mathbf{v}_1, \dots, \mathbf{v}_s \rangle_{K[x]},$$

hence $V = \langle \mathbf{v}_1, \dots, \mathbf{v}_s \rangle_{K[x]}$ is also generated by $\mathbf{v}_1, \dots, \mathbf{v}_s$ as a $K[x]$-module. In particular, V is a $K[x]$-module of finite type.

Proposition 6.2.11. *Let $N_1, \dots, N_s$ be submodules of an A-module M. Their* intersection *$N_1 \cap \cdots \cap N_s$ and their* sum

$$N_1 + \cdots + N_s = \{\mathbf{u}_1 + \cdots + \mathbf{u}_s \,;\, \mathbf{u}_1 \in N_1, \dots, \mathbf{u}_s \in N_s\}$$

are also A-submodules of M.

Proof for the sum. We first note that, since $\mathbf{0} \in N_i$ for $i = 1, \dots, s$, we have

$$\mathbf{0} = \mathbf{0} + \cdots + \mathbf{0} \in N_1 + \cdots + N_s.$$

Let $\mathbf{u}, \mathbf{u}'$ be arbitrary elements of $N_1 + \cdots + N_s$, and let $a \in A$. We can write

$$\mathbf{u} = \mathbf{u}_1 + \cdots + \mathbf{u}_s \quad \text{and} \quad \mathbf{u}' = \mathbf{u}'_1 + \cdots + \mathbf{u}'_s$$

with $\mathbf{u}_1, \mathbf{u}'_1 \in N_1, \dots, \mathbf{u}_s, \mathbf{u}'_s \in N_s$. Thus we have

$$\begin{aligned} \mathbf{u} + \mathbf{u}' &= (\mathbf{u}_1 + \mathbf{u}'_1) + \cdots + (\mathbf{u}_s + \mathbf{u}'_s) \in N_1 + \cdots + N_s, \\ a\,\mathbf{u} &= (a\,\mathbf{u}_1) + \cdots + (a\,\mathbf{u}_s) \in N_1 + \cdots + N_s. \end{aligned}$$

This proves that $N_1 + \cdots + N_s$ is an A-submodule of M. □

In closing this section, we note that the notation $A\,\mathbf{u}_1 + \cdots + A\,\mathbf{u}_s$ for the A-submodule $\langle \mathbf{u}_1, \dots, \mathbf{u}_s \rangle_A$ generated by the elements $\mathbf{u}_1, \dots, \mathbf{u}_s$ of M is consistent with the notion of a sum of submodules since, for every element $\mathbf{u}$ of M, we have

$$A\,\mathbf{u} = \langle \mathbf{u} \rangle_A = \{a\,\mathbf{u} \,;\, a \in A\}.$$

When $A = K$ is a field, we recover the usual notions of the intersection and sum of subspaces of a vector space over K. When $A = \mathbb{Z}$, we instead recover the notions of the intersection and sum of subgroups of an abelian group.

Exercises.

6.2.1. Prove Proposition 6.2.2.

6.2.2. Let M be an abelian group. Explain why the $\mathbb{Z}$-submodules of M are simply the subgroups of M.

Hint. Show that every $\mathbb{Z}$-submodule of M is a subgroup of M and, conversely, that every subgroup of M is a $\mathbb{Z}$-submodule of M.

6.2.3. Prove Proposition 6.2.7.

6.2.4. Let M be a module over a commutative ring A, and let $u_1, \dots, u_s, v_1, \dots, v_t \in M$. Set $L = \langle u_1, \dots, u_s \rangle_A$ and $N = \langle v_1, \dots, v_t \rangle_A$. Show that $L + N = \langle u_1, \dots, u_s, v_1, \dots, v_t \rangle_A$.

6.2.5. Let M be a module over a commutative ring A. We say that an element $\mathbf{u}$ of M is *torsion* if there exits a nonzero element a of A such that $a\,\mathbf{u} = \mathbf{0}$. We say that M is a *torsion A-module* if all its elements are torsion. Suppose that A is an integral domain.

(i) Show that the set M_{tor} of torsion elements of M is an A-submodule of M.

(ii) Show that, if M is of finite type and if all its elements are torsion, then there exists a nonzero element a of A such that $a\,\mathbf{u} = \mathbf{0}$ for all $\mathbf{u} \in M$.

6.3 Free modules

Definition 6.3.1 (Linear independence, basis, free module). Let $\mathbf{u}_1, \dots, \mathbf{u}_n$ be elements of an A-module M.

(i) We say that $\mathbf{u}_1, \dots, \mathbf{u}_n$ are *linearly independent* over A if the only choice of elements $a_1, \dots, a_n$ of A such that
$$a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n = \mathbf{0}$$
is $a_1 = \cdots = a_n = 0$.

(ii) We say that $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is a *basis* of M if $\mathbf{u}_1, \dots, \mathbf{u}_n$ are linearly independent over A and generate M as an A-module.

(iii) We say that M is an *free* A-module if it admits a basis.

By convention, the module $\{\mathbf{0}\}$ consisting of a single element is a free A-module that admits the empty set as a basis.

In contrast to finite type vector spaces over a field K, which always admit a basis, A-modules of finite type do not always admit a basis (see the exercises).

Example 6.3.2. Let $n \in \mathbb{N}_{>0}$. The A-module A^n introduced in Example 6.1.9 admits the basis

$$\left\{ \mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \mathbf{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Indeed, we have

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{6.2}$$

for all $a_1, \ldots, a_n \in A$. Thus $\mathbf{e}_1, \ldots, \mathbf{e}_n$ generate A^n as an A-module. Furthermore, if $a_1, \ldots, a_n \in A$ satisfy $a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n = \mathbf{0}$, then equality (6.2) gives

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

and so $a_1 = a_2 = \cdots = a_n = 0$. Hence $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are also linearly independent over A.

Exercises.

6.3.1. Show that a finite abelian group M admits a basis as a $\mathbb{Z}$-module if and only if $M = \{0\}$ (in which case the empty set is, by convention, a basis of M).

6.3.2. In general, show that, if M is a finite module over an infinite commutative ring A, then M is a free A-module if and only if $M = \{0\}$.

6.3.3. Let V be a finite-dimensional vector space over a field K and let $T \in \mathrm{End}_K(V)$. Show that, for the corresponding structure of a $K[x]$-module, V admits a basis if and only if $V = \{0\}$.

6.3.4. Let m and n be positive integers and let A be a commutative ring. Show that $\mathrm{Mat}_{m\times n}(A)$ is a free A-module for the usual operations of addition and multiplication by elements of A.

6.4 Direct sum

Definition 6.4.1 (Direct sum). Let $M_1, \ldots, M_s$ be submodules of an A-module M. We say that their sum is *direct* if the only choice of $\mathbf{u}_1 \in M_1, \ldots, \mathbf{u}_s \in M_s$ such that

$$\mathbf{u}_1 + \cdots + \mathbf{u}_s = 0$$

is $\mathbf{u}_1 = \cdots = \mathbf{u}_s = 0$. When this condition is satisfied, we write the sum $M_1 + \cdots + M_s$ as $M_1 \oplus \cdots \oplus M_s$.

We say that M is the *direct sum* of $M_1, \ldots, M_s$ if $M = M_1 \oplus \cdots \oplus M_s$.

The following propositions, which generalize the analogous results of Section 1.4 are left as exercises. The first justifies the importance of the notion of direct sum.

Proposition 6.4.2. *Let $M_1, \ldots, M_s$ be submodules of an A-module M. Then we have $M = M_1 \oplus \cdots \oplus M_s$ if and only if, for all $\mathbf{u} \in M$, there exists a unique choice of $\mathbf{u}_1 \in M_1, \ldots, \mathbf{u}_s \in M_s$ such that $\mathbf{u} = \mathbf{u}_1 + \cdots + \mathbf{u}_s$.*

Proposition 6.4.3. *Let $M_1, \ldots, M_s$ be submodules of an A-module M. The following conditions are equivalent:*

1) the sum of $M_1, \ldots, M_s$ is direct,

2) $M_i \cap (M_1 + \cdots + \widehat{M_i} + \cdots + M_s) = \{\mathbf{0}\}$ for $i = 1, \ldots, s$,

3) $M_i \cap (M_{i+1} + \cdots + M_s) = \{\mathbf{0}\}$ for $i = 1, \ldots, s-1$.

(As usual, the notation $\widehat{M_i}$ means that we omit the term M_i from the sum.)

Example 6.4.4. Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$. For the corresponding structure of a $K[x]$-module on V, we know that the submodules of V are simply the T-invariants subspaces of V. Since the notion of direct sum only involves addition, to say that V, as a $K[x]$-module, is a direct sum of $K[x]$-submodules $V_1, \ldots, V_s$ is equivalent to saying that V, as a vector space over K, is a direct sum of T-invariant subspaces $V_1, \ldots, V_s$.

Exercises.

6.4.1. Prove Proposition 6.4.3.

6.4.2. Let M be a module over a commutative ring A and let $\mathbf{u}_1, \ldots, \mathbf{u}_n \in M$. Show that $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is a basis of M if and only if $M = A\mathbf{u}_1 \oplus \cdots \oplus A\mathbf{u}_n$ and none of the elements $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is torsion (see Exercise 6.2.5 for the definition of this term).

6.5 Homomorphisms of modules

Fix a commutative ring A.

Definition 6.5.1. Let M and N be A-modules. A *homomorphism* of A-modules from M to N is a function $\varphi\colon M \to N$ satisfying the following conditions:

HM1. $\varphi(\mathbf{u}_1 + \mathbf{u}_2) = \varphi(\mathbf{u}_1) + \varphi(\mathbf{u}_2)$ for all $\mathbf{u}_1, \mathbf{u}_2 \in M$,
HM2. $\varphi(a\,\mathbf{u}) = a\,\varphi(\mathbf{u})$ for all $a \in A$ and all $\mathbf{u} \in M$.

Condition **HM1** implies that a homomorphism of A-modules is, in particular, a homomorphism of groups under addition.

Example 6.5.2. If $A = K$ is a field, then K-modules M and N are simply vector spaces over K and a homomorphism of K-modules $\varphi\colon M \to N$ is nothing but a linear map from M to N.

Example 6.5.3. We recall that if $A = \mathbb{Z}$, then $\mathbb{Z}$-modules M and N are simply abelian groups equipped with the natural multiplication by the integers. If $\varphi\colon M \to N$ is a homomorphism of $\mathbb{Z}$-modules, condition **HM1** shows that it is a homomorphism of groups. Conversely, if $\varphi\colon M \to N$ is a homomorphism of abelian groups, we have

$$\varphi(n\,\mathbf{u}) = n\,\varphi(\mathbf{u})$$

for all $n \in \mathbb{Z}$ and all $\mathbf{u} \in M$ (exercise), hence φ satisfies conditions **HM1** and **HM2** of Definition 6.5.1. Thus, *a homomorphism of $\mathbb{Z}$-modules is simply a homomorphism of abelian groups.*

Example 6.5.4. Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$. For the corresponding structure of a $K[x]$-module on V, a homomorphism of $K[x]$-modules $S\colon V \to V$ is simply a linear map that commutes with T, i.e. such that $S \circ T = T \circ S$ (exercise).

Example 6.5.5. Let $m, n \in \mathbb{N}_{>0}$, and let $P \in \mathrm{Mat}_{m\times n}(A)$. For all $\mathbf{u}, \mathbf{u}' \in A^n$ and $a \in A$, we have:

$$P(\mathbf{u} + \mathbf{u}') = P\mathbf{u} + P\mathbf{u}' \quad \text{and} \quad P(a\,\mathbf{u}) = a\,P\mathbf{u}.$$

Thus the function

$$\begin{array}{rcl} A^n & \longrightarrow & A^m \\ \mathbf{u} & \longmapsto & P\mathbf{u} \end{array}$$

is a homomorphism of A-modules.

The following result shows that we obtain in this way all the homomorphism of A-modules from A^n to A^m.

Proposition 6.5.6. *Let $m, n \in \mathbb{N}_{>0}$ and let $\varphi\colon A^n \to A^m$ be a homomorphism of A-modules. There exists a unique matrix $P \in \mathrm{Mat}_{m\times n}(A)$ such that*

$$\varphi(\mathbf{u}) = P\,\mathbf{u} \quad \textit{for all } \mathbf{u} \in A^n. \tag{6.3}$$

Proof. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be the standard basis of A^n defined in Example 6.3.2 and let P be the $m \times n$ matrix whose columns are $C_1 := \varphi(\mathbf{e}_1)\,, \dots, C_n := \varphi(\mathbf{e}_n)$. For every n-tuple $\mathbf{u} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in A^n$, we have:

$$\varphi(\mathbf{u}) = \varphi(a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n) = a_1\, C_1 + \cdots + a_n\, C_n = \big(C_1 \cdots C_n\big) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = P\,\mathbf{u}\,.$$

Thus P satisfies Condition (6.3). It is the only matrix that satisfies this condition since if a matrix $P' \in \mathrm{Mat}_{m\times n}(A)$ also satisfies $\varphi(\mathbf{u}) = P'\mathbf{u}$ for all $\mathbf{u} \in A^n$, then its j-th column is $P'\mathbf{e}_j = \varphi(\mathbf{e}_j) = C_j$ for all $j = 1, \dots, n$. □

We continue the general theory with the following result.

Proposition 6.5.7. *Let $\varphi\colon M \to N$ and $\psi\colon N \to P$ be homomorphisms of A-modules.*

(i) The composite $\psi \circ \varphi\colon M \to P$ is also a homomorphism of A-modules.

(ii) If $\varphi\colon M \to N$ is bijective, its inverse $\varphi^{-1}\colon N \to M$ is a homomorphism of A-modules.

Part (i) is left as an exercise.

Proof of (ii). Suppose that φ is bijective. Let $\mathbf{v}, \mathbf{v}' \in N$ and $a \in A$. We set

$$\mathbf{u} := \varphi^{-1}(\mathbf{v}) \quad \text{and} \quad \mathbf{u}' := \varphi^{-1}(\mathbf{v}').$$

Since $\mathbf{u}, \mathbf{u}' \in M$ and φ is a homomorphism of A-modules, we have

$$\varphi(\mathbf{u} + \mathbf{u}') = \varphi(\mathbf{u}) + \varphi(\mathbf{u}') = \mathbf{v} + \mathbf{v}' \quad \text{and} \quad \varphi(a\,\mathbf{u}) = a\,\varphi(\mathbf{u}) = a\,\mathbf{v}.$$

Therefore,

$$\varphi^{-1}(\mathbf{v} + \mathbf{v}') = \mathbf{u} + \mathbf{u}' = \varphi^{-1}(\mathbf{v}) + \varphi^{-1}(\mathbf{v}') \quad \text{and} \quad \varphi^{-1}(a\,\mathbf{v}) = a\,\mathbf{u} = a\,\varphi^{-1}(\mathbf{v}).$$

This proves that $\varphi^{-1}\colon N \to M$ is indeed a homomorphism of A-modules. □

Definition 6.5.8 (Isomorphism). A bijective homomorphism of A-modules is called an *isomorphism* of A-modules. We say that an A-module M is *isomorphic* to an A-module N if there exists an isomorphism of A-modules $\varphi\colon M \to N$. We then write $M \simeq N$.

In light of these definitions, Proposition 6.5.7 has the following immediate consequence:

Corollary 6.5.9. *Let $\varphi\colon M \to N$ and $\psi\colon N \to P$ be isomorphisms of A-modules. Then $\psi \circ \varphi\colon M \to P$ and $\varphi^{-1}\colon N \to M$ are also isomorphisms of A-modules.*

We deduce from this that isomorphism is an equivalence relation on the class of A-modules. Furthermore, the set of isomorphisms of A-modules from an A-module M to itself, called *automorphisms* of M, form a subgroup of the group of bijections from M to itself. We call it the *group of automorphisms* of M.

Definition 6.5.10. Let $\varphi\colon M \to N$ be a homomorphism of A-modules. The *kernel* of φ is

$$\ker(\varphi) := \{\mathbf{u} \in M\,;\, \varphi(\mathbf{u}) = \mathbf{0}\}$$

and the *image* of φ is

$$\mathrm{Im}(\varphi) := \{\varphi(\mathbf{u})\,;\, \mathbf{u} \in M\}.$$

The kernel and image of a homomorphism of A-modules $\varphi\colon M \to N$ are therefore simply the kernel and image of φ considered as a homomorphism of abelian groups. The proof of the following result is left as an exercise.

Proposition 6.5.11. *Let $\varphi\colon M \to N$ be a homomorphism of A-modules.*

(i) $\ker(\varphi)$ *is an A-submodule of M.*

(ii) $\mathrm{Im}(\varphi)$ *is an A-submodule of N.*

(iii) The homomorphism φ is injective if and only if $\ker(\varphi) = \{\mathbf{0}\}$. *It is surjective if and only if* $\mathrm{Im}(\varphi) = N$.

Example 6.5.12. Let M be an A-module and let $a \in A$. The function

$$\begin{array}{rccc} \varphi: & M & \to & M \\ & \mathbf{u} & \to & a\mathbf{u} \end{array}$$

is a homomorphism of A-modules (exercise). Its kernel is

$$M_a := \{\mathbf{u} \in M\,;\, a\mathbf{u} = \mathbf{0}\}$$

and its image is

$$aM := \{a\mathbf{u}\,;\, \mathbf{u} \in M\}.$$

Thus, by Proposition 6.5.11, M_a and aM are both A-submodules of M.

We conclude this chapter with the following result.

Proposition 6.5.13. *Let $\varphi\colon M \to N$ be a homomorphism of A-modules. Suppose that M is free with basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$. Then φ is an isomorphism if and only if $\{\varphi(\mathbf{u}_1), \ldots, \varphi(\mathbf{u}_n)\}$ is a basis of N.*

Proof. We will show more precisely that

i) φ is injective if and only if $\varphi(\mathbf{u}_1), \ldots, \varphi(\mathbf{u}_n)$ are linearly independent over A, and

ii) φ is surjective if and only if $\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n)$ generate N.

Therefore, φ is bijective if and only if $\{\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n)\}$ is a basis of N.

To prove (i), we use the fact that φ is injective if and only if $\ker(\varphi) = \{\mathbf{0}\}$ (Proposition 6.5.11(iii)). We note that, for all $a_1, \dots, a_n \in A$, we have

$$\begin{aligned} a_1\varphi(\mathbf{u}_1) + \cdots + a_n\varphi(\mathbf{u}_n) = 0 &\iff \varphi(a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n) = 0 \\ &\iff a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n \in \ker(\varphi). \end{aligned} \tag{6.4}$$

If $\ker(\varphi) = \{\mathbf{0}\}$, the last condition becomes $a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n = \mathbf{0}$ which implies $a_1 = \cdots = a_n = 0$ since $\mathbf{u}_1, \dots, \mathbf{u}_n$ are linearly independent over A. In this case, we conclude that $\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n)$ are linearly independent over A. Conversely, if $\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n)$ are linearly independent, the equivalences (6.4) tell us that the only choice of $a_1, \dots, a_n \in A$ such that $a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n \in \ker(\varphi)$ is $a_1 = \cdots = a_n = 0$. Since $\mathbf{u}_1, \dots, \mathbf{u}_n$ generate M, this implies that $\ker(\varphi) = \{\mathbf{0}\}$. Thus $\ker(\varphi) = \{\mathbf{0}\}$ if and only if $\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n)$ are linearly independent. To prove (ii), we use the fact that φ is surjective if and only if $\mathrm{Im}(\varphi) = N$. Since $M = \langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle_A$, we have

$$\begin{aligned} \mathrm{Im}(\varphi) &= \{\varphi(a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n)\,;\, a_1, \dots, a_n \in A\} \\ &= \{a_1\varphi(\mathbf{u}_1) + \cdots + a_n\varphi(\mathbf{u}_n)\,;\, a_1, \dots, a_n \in A\} \\ &= \langle \varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n) \rangle_A. \end{aligned}$$

Thus $\mathrm{Im}(\varphi) = N$ if and only if $\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_n)$ generate N. □

Exercises.

6.5.1. Prove Proposition 6.5.7(i).

6.5.2. Prove Proposition 6.5.11.

6.5.3. Prove that the map φ of Example 6.5.12 is a homomorphism of A-modules.

6.5.4. Let $\varphi\colon M \to M'$ be a homomorphism of A-modules and let N be an A-submodule of M. We define the *image* of N under φ by

$$\varphi(N) := \{\varphi(\mathbf{u})\,;\, \mathbf{u} \in M\}.$$

Show that

(i) $\varphi(N)$ is an A-submodule of M';

(ii) if $N = \langle \mathbf{u}_1, \dots, \mathbf{u}_m \rangle_A$, then $\varphi(N) = \langle \varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_m) \rangle_A$;

(iii) if N admits a basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ and if φ is injective, then $\{\varphi(\mathbf{u}_1), \ldots, \varphi(\mathbf{u}_m)\}$ is a basis of $\varphi(N)$.

6.5.5. Let $\varphi\colon M \to M'$ be a homomorphism of A-modules and let N' be an A-submodule of M'. We define the *inverse image* of N' under φ by

$$\varphi^{-1}(N') := \{\mathbf{u} \in M\,;\, \varphi(\mathbf{u}) \in N'\}$$

(this notation does not imply that φ^{-1} exists). Show that $\varphi^{-1}(N')$ is an A-submodule of M.

6.5.6. Let M be a free A-module with basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, let N be an arbitrary A-module, and let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be arbitrary elements of N. Show that there exists a unique homomorphism of A-modules $\varphi\colon M \to N$ such that $\varphi(\mathbf{u}_i) = \mathbf{v}_i$ for $i = 1, \ldots, n$.

6.5.7. Let N be an A-module of finite type generated by n elements. Show that there exists a surjective homomorphism of A-modules $\varphi\colon A^n \to N$.

Hint. Use the result of Exercise 6.5.6.

Chapter 7

Structure of modules of finite type over a euclidean domain

In this chapter, we define the notions of the annihilator of a module and the annihilator of an element of a module. We study in detail the meaning of these notions for a finite abelian group considered as a $\mathbb{Z}$-module and then for a finite-dimensional vector space over a field K equipped with an endomorphism. We also cite without proof the structure theorem for modules of finite type over a euclidean domain and we analyze its consequences in the same situations. Finally, we prove a refinement of this result and we conclude with the Jordan canonical form for a linear operator on a finite-dimensional complex vector space.

7.1 Annihilators

Definition 7.1.1 (Annihilator). Let M be a module over a commutative ring A. The *annihilator* of an element $\mathbf{u}$ of M is

$$\mathrm{Ann}(\mathbf{u}) := \{a \in A\,;\, a\mathbf{u} = \mathbf{0}\}.$$

The *annihilator* of M is

$$\mathrm{Ann}(M) := \{a \in A\,;\, a\mathbf{u} = \mathbf{0} \text{ for all } \mathbf{u} \in M\}.$$

The following result is left as an exercise:

Proposition 7.1.2. *Let A and M be as in the above definition. The annihilator of M and the annihilator of any element of M are ideals of A. Furthermore, if $M = \langle \mathbf{u}_1, \ldots, \mathbf{u}_s \rangle_A$, then*

$$\mathrm{Ann}(M) = \mathrm{Ann}(\mathbf{u}_1) \cap \cdots \cap \mathrm{Ann}(\mathbf{u}_s).$$

Recall that an A-module is called *cylic* if it is generated by a single element (see Section 6.2). For such a module, the last assertion of Proposition 7.1.2 gives:

Corollary 7.1.3. *Let M be a cyclic module over a commutative ring A. We have* $\mathrm{Ann}(M) = \mathrm{Ann}(\mathbf{u})$ *for every generator* $\mathbf{u}$ *of M.*

In the case of an abelian group G written additively and considered as a $\mathbb{Z}$-module, these notions become the following:

- The annihilator of an element g of G is

$$\mathrm{Ann}(g) = \{m \in \mathbb{Z}\,;\, mg = 0\}.$$

  It is an ideal of $\mathbb{Z}$. By definition, if $\mathrm{Ann}(g) = \{0\}$, we say that g is of *infinite order*. Otherwise, we say that g is of *finite order* and its *order*, denoted $\mathrm{o}(g)$, is the smallest positive integer in $\mathrm{Ann}(g)$, hence it is also a generator of $\mathrm{Ann}(g)$.

- The annihilator of G is

$$\mathrm{Ann}(G) = \{m \in \mathbb{Z}\,;\, mg = 0 \text{ for all } g \in G\}.$$

  It is also an ideal of $\mathbb{Z}$. If $\mathrm{Ann}(G) \neq \{0\}$, then the smallest positive integer in $\mathrm{Ann}(G)$, that is, its positive generator, is called the *exponent* of G.

If G is a finite group, then the *order* $|G|$ of the group (its cardinality) is an element of $\mathrm{Ann}(G)$. This follows from Lagrange's Theorem which says that, in a finite group (commutative or not), the order of every element divides the order of the group. In this case, we have $\mathrm{Ann}(G) \neq \{0\}$ and the exponent of G is a divisor of $|G|$. More precisely, we prove:

Proposition 7.1.4. *Let G be a finite abelian group considered as a $\mathbb{Z}$-module. The exponent of G is the lcm of the orders of the elements of G and is a divisor of the order $|G|$ of G. If G is cyclic, generated by an element g, the exponent of G, the order of G and the order of g are equal.*

Recall that a *lowest common multiple* (lcm) of a finite family of nonzero integers $a_1, \ldots, a_s$ is any nonzero integer m divisible by each of $a_1, \ldots, a_s$ and that divides every other integer with this property (see Exercises 5.2.4 and 5.4.6 for the existence of the lcm).

Proof. Let m be the lcm of the orders of the elements of G. For all $g \in G$, we have $mg = 0$ since $\mathrm{o}(g) \mid m$, hence $m \in \mathrm{Ann}(G)$. Otherwise, if $n \in \mathrm{Ann}(G)$, then $ng = O$ for all $g \in G$, hence $\mathrm{o}(g) \mid n$ for all $g \in G$ and thus $m \mid n$. This shows that $\mathrm{Ann}(G) = m\mathbb{Z}$. Therefore the exponent of G is m. The remark preceding the proposition shows that it is a divisor of $|G|$.

If $G = \mathbb{Z}g$ is cyclic generated by g, we know that $|G| = \mathrm{o}(g)$, and Corollary 7.1.3 gives $\mathrm{Ann}(G) = \mathrm{Ann}(g)$. Thus the exponent of G is $\mathrm{o}(g) = |G|$. □

Example 7.1.5. Let $C_1 = \mathbb{Z}g_1$ and $C_2 = \mathbb{Z}g_2$ be cyclic groups generated respectively by an element g_1 of order 6 and an element g_2 of order 8. We form their cartesian product

$$C_1 \times C_2 = \{(k\, g_1,\, \ell\, g_2)\,;\, k, \ell \in \mathbb{Z}\} = \mathbb{Z}(g_1, 0) + \mathbb{Z}(0, g_2).$$

1st Find the order of $(2g_1, 3g_2)$.

For an integer $m \in \mathbb{Z}$, we have

$$\begin{aligned} m(2g_1, 3g_2) = (0,0) &\iff 2mg_1 = 0 \quad \text{and} \quad 3mg_2 = 0 \\ &\iff 6 \,|\, 2m \quad \text{and} \quad 8 \,|\, 3m \\ &\iff 3 \,|\, m \quad \text{and} \quad 8 \,|\, m \\ &\iff 24 \,|\, m\,. \end{aligned}$$

Thus the order of $(2g_1, 3g_2)$ is 24.

2nd Find the exponent of $C_1 \times C_2$.

For an integer $m \in \mathbb{Z}$, we have

$$\begin{aligned} m \in \mathrm{Ann}(C_1 \times C_2) &\iff m(kg_1, \ell g_2) = (0,0) \quad \forall k, \ell \in \mathbb{Z} \\ &\iff mk\, g_1 = 0 \quad \text{and} \quad m\ell\, g_2 = 0 \quad \forall k, \ell \in \mathbb{Z} \\ &\iff m\, g_1 = 0 \quad \text{and} \quad m\, g_2 = 0 \\ &\iff 6 \,|\, m \quad \text{and} \quad 8 \,|\, m \\ &\iff 24 \,|\, m\,. \end{aligned}$$

Thus the exponent of $C_1 \times C_2$ is 24.

Since $|C_1 \times C_2| = |C_1|\,|C_2| = 6 \cdot 8 = 48$ is a strict multiple of the exponent of $C_1 \times C_2$, the group $C_1 \times C_2$ is not cyclic (see the last part of Proposition 7.1.4).

In the case of a vector space equipped with an endomorphism, the notions of annihilators become the following:

Proposition 7.1.6. *Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$. For the corresponding structure of a $K[x]$-module on V, the annihilator of an element $\mathbf{v}$ of V is*

$$\mathrm{Ann}(\mathbf{v}) = \{p(x) \in K[x]\,;\, p(T)(\mathbf{v}) = \mathbf{0}\},$$

while the annihilator of V is

$$\mathrm{Ann}(V) = \{p(x) \in K[x]\,;\, p(T) = 0\}.$$

These are ideals of $K[x]$.

Proof. Multiplication by a polynomial $p(x) \in K[x]$ is defined by $p(x)\mathbf{v} = p(T)\mathbf{v}$ for all $\mathbf{v} \in V$. Thus, for fixed $\mathbf{v} \in V$ we have:

$$p(x) \in \mathrm{Ann}(\mathbf{v}) \iff p(T)(\mathbf{v}) = \mathbf{0}$$

and so

$$p(x) \in \mathrm{Ann}(V) \iff p(T)(\mathbf{v}) = \mathbf{0} \quad \forall \mathbf{v} \in V \iff p(T) = 0. \quad \square$$

We know that every *nonzero* ideal of $K[x]$ has a unique monic generator: the monic polynomial of smallest degree that belongs to this ideal. In the context of Proposition 7.1.6, the following result provides a means of calculating the monic generator of $\mathrm{Ann}(\mathbf{v})$ when V is finite-dimensional.

Proposition 7.1.7. *With the notation of Proposition 7.1.6, suppose that V is finite-dimensional. Let $\mathbf{v} \in V$ with $\mathbf{v} \neq \mathbf{0}$. Then:*

(i) there exists a greatest positive integer m such that $\mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})$ are linearly independent over K;

(ii) for this integer m, there exists a unique choice of element $a_0, a_1, \ldots, a_{m-1}$ of K such that
$$T^m(\mathbf{v}) = a_0\mathbf{v} + a_1T(\mathbf{v}) + \cdots + a_{m-1}T^{m-1}(\mathbf{v});$$

(iii) the polynomial $p(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0$ is the monic generator of $\mathrm{Ann}(\mathbf{v})$;

(iv) the $K[x]$-submodule U of V generated by $\mathbf{v}$ is a T-invariant vector subspace of V that admits $\mathcal{C} = \{\mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})\}$ as a basis;

(v) we have $[T|_U]_{\mathcal{C}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{pmatrix}.$

Before presenting the proof of this result, we give a name to the matrix appearing in the last assertion of the proposition.

Definition 7.1.8 (Companion matrix). Let $m \in \mathbb{N}_{>0}$ and let $a_0, \ldots, a_{m-1}$ be elements of a field K. The matrix
$$\begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{pmatrix}$$
is called the *companion matrix* of the monic polynomial $x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0 \in K[x]$.

Proof of Proposition 7.1.7. Let $n = \dim_K(V)$. We first note that, for every integer $m \geq 1$, the vectors $\mathbf{v}, T(\mathbf{v}), \ldots, T^m(\mathbf{v})$ are linearly dependent if and only if the annihilator $\mathrm{Ann}(\mathbf{v})$ of $\mathbf{v}$ contains a nonzero polynomial of degree at most m. Since $\dim_K(V) = n$, we know that $\mathbf{v}, T(\mathbf{v}), \ldots, T^n(\mathbf{v})$ are linearly dependent and thus $\mathrm{Ann}(\mathbf{v})$ contains a nonzero polynomial of degree $\leq n$. In particular, $\mathrm{Ann}(\mathbf{v})$ is a nonzero ideal of $K[x]$, and as such it possesses a unique monic generator $p(x)$, namely its monic element of least degree. Let m be the degree of $p(x)$. Since $\mathbf{v} \neq \mathbf{0}$, we have $m \geq 1$. Write
$$p(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0.$$

Then the integer m is the largest integer such that $\mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})$ are linearly independent and the elements $a_0, a_1, \ldots, a_{m-1}$ of A are the only ones for which

$$T^m(\mathbf{v}) - a_{m-1}T^{m-1}(\mathbf{v}) - \cdots - a_1T(\mathbf{v}) - a_0\mathbf{v} = \mathbf{0},$$

that is, such that

$$T^m(\mathbf{v}) = a_0\mathbf{v} + a_1T(\mathbf{v}) + \cdots + a_{m-1}T^{m-1}(\mathbf{v}). \tag{7.1}$$

This proves (i), (ii) and (iii) all at the same time. On the other hand, we clearly have

$$T(T^i(\mathbf{v})) \in \langle \mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})\rangle_K$$

for $i = 0, \ldots, m-2$ and equation (7.1) shows that this is again true for $i = m-1$. Then, by Proposition 2.6.4, the subspace $\langle \mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})\rangle_K$ is T-invariant. Therefore, it is a $K[x]$-submodule of V (see Proposition 6.2.6). Since it contains $\mathbf{v}$ and it is contained in $U := K[x]\mathbf{v}$, we deduce that this subspace is U. Finally, since $\mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})$ are linearly independent, we conclude that these m vectors form a basis of U. This proves (iv). The final assertion (v) follows directly from (iv) by using the relation (7.1). □

Example 7.1.9. Let V be a vector space of dimension 3 over $\mathbb{Q}$, let $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ be a basis of V, and let $T \in \mathrm{End}_{\mathbb{Q}}(V)$. Suppose that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 2 & -2 & -1 \\ 1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix},$$

and find the monic generator of $\mathrm{Ann}(\mathbf{v}_1)$.

We have

$$[T(\mathbf{v}_1)]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}}[\mathbf{v}_1]_{\mathcal{B}} = \begin{pmatrix} 2 & -2 & -1 \\ 1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix},$$

$$[T^2(\mathbf{v}_1)]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}}[T(\mathbf{v}_1)]_{\mathcal{B}} = \begin{pmatrix} 2 & -2 & -1 \\ 1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix},$$

$$[T^3(\mathbf{v}_1)]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}}[T^2(\mathbf{v}_1)]_{\mathcal{B}} = \begin{pmatrix} 2 & -2 & -1 \\ 1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 1 \end{pmatrix},$$

and so

$$T(\mathbf{v}_1) = 2\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3, \quad T^2(\mathbf{v}_1) = \mathbf{v}_1 + 3\mathbf{v}_3, \quad T^3(\mathbf{v}_1) = -\mathbf{v}_1 - 2\mathbf{v}_2 + \mathbf{v}_3.$$

Since

$$\det\Big([\mathbf{v}_1]_{\mathcal{B}}\,[T(\mathbf{v}_1)]_{\mathcal{B}}\,[T^2(\mathbf{v}_1)]_{\mathcal{B}}\Big) = \begin{vmatrix} 1 & 2 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 3 \end{vmatrix} = 3 \neq 0,$$

the vectors $\mathbf{v}_1, T(\mathbf{v}_1), T^2(\mathbf{v}_1)$ are linearly independent. Since $\dim_{\mathbb{Q}}(V) = 3$, the greatest integer m such that $\mathbf{v}_1, T(\mathbf{v}_1), \ldots, T^{m-1}(\mathbf{v}_1)$ are linearly independent is necessarily $m = 3$. By Proposition 7.1.7, this implies that the monic generator of $\mathrm{Ann}(\mathbf{v}_1)$ is of degree 3. We see that

$$\begin{aligned}
T^3(\mathbf{v}_1) = a_0\mathbf{v}_1 + a_1T(\mathbf{v}_1) + a_2T^2(\mathbf{v}_1) \quad &\Longleftrightarrow \quad [T^3(\mathbf{v}_1)]_{\mathcal{B}} = a_0[\mathbf{v}_1]_{\mathcal{B}} + a_1[T(\mathbf{v}_1)]_{\mathcal{B}} + a_2[T^2(\mathbf{v}_1)]_{\mathcal{B}} \\
&\Longleftrightarrow \quad \begin{pmatrix} -1 \\ -2 \\ 1 \end{pmatrix} = a_0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \\
&\Longleftrightarrow \quad \begin{cases} a_0 + 2a_1 + a_2 = -1 \\ a_1 = -2 \\ a_1 + 3a_2 = 1 \end{cases} \\
&\Longleftrightarrow \quad a_0 = 2, \quad a_1 = -2 \quad \text{and} \quad a_2 = 1.
\end{aligned}$$

Hence we have

$$T^3(\mathbf{v}_1) = 2\mathbf{v}_1 - 2T(\mathbf{v}_1) + T^2(\mathbf{v}_1).$$

By Proposition 7.1.7, we conclude that the polynomial

$$p(x) = x^3 - x^2 + 2x - 2$$

is the monic generator of $\mathrm{Ann}(\mathbf{v}_1)$.

Since $\dim_{\mathbb{Q}}(V) = 3$ and $\mathbf{v}_1, T(\mathbf{v}_1), T^2(\mathbf{v}_1)$ are linearly independent over $\mathbb{Q}$, the ordered set $\mathcal{C} = \{\mathbf{v}_1, T(\mathbf{v}_1), T^2(\mathbf{v}_1)\}$ forms a basis of V. Therefore,

$$V = \langle \mathbf{v}_1, T(\mathbf{v}_1), T^2(\mathbf{v}_1)\rangle_{\mathbb{Q}} = \langle \mathbf{v}_1\rangle_{\mathbb{Q}[x]}$$

is a cyclic $\mathbb{Q}[x]$-module generated by $\mathbf{v}_1$ and the last assertion of Proposition 7.1.7 gives

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -2 \\ 0 & 1 & 1 \end{pmatrix}.$$

From Proposition 7.1.7, we deduce:

Proposition 7.1.10. *Let V be a finite-dimensional vector space over a field K and let $T \in \mathrm{End}_K(V)$. For the corresponding structure of a $K[x]$-module on V, the ideal $\mathrm{Ann}(V)$ is nonzero.*

Proof. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V. We have

$$V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n\rangle_K = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n\rangle_{K[x]}.$$

Then Proposition 7.1.2 gives

$$\mathrm{Ann}(V) = \mathrm{Ann}(\mathbf{v}_1) \cap \cdots \cap \mathrm{Ann}(\mathbf{v}_n).$$

For each $i = 1, \ldots, n$, Proposition 7.1.7 shows that $\mathrm{Ann}(\mathbf{v}_i)$ is generated by a monic polynomial $p_i(x) \in K[x]$ of degree $\leq n$. The product $p_1(x) \cdots p_n(x)$ annihilates each $\mathbf{v}_i$, hence it annihilates all of V. This proves that $\mathrm{Ann}(V)$ contains a nonzero polynomial of degree $\leq n^2$. $\square$

We conclude this section with the following definition.

Definition 7.1.11 (Minimal polynomial). Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$. Suppose that $\mathrm{Ann}(V) \neq \{0\}$ for the corresponding structure of a $K[x]$-module on V. Then the monic generator of $\mathrm{Ann}(V)$ is called the *minimal polynomial* of T and is denoted $\min_T(x)$. By Proposition 7.1.6, it is the monic polynomial $p(x) \in K[x]$ of smallest degree such that $p(T) = 0$.

Example 7.1.12. In Example 7.1.9, V is a cyclic $\mathbb{Q}[x]$-module generated by $\mathbf{v}_1$. By Corollary 7.1.3, we therefore have

$$\mathrm{Ann}(V) = \mathrm{Ann}(\mathbf{v}_1),$$

and thus the minimal polynomial of T is the monic generator of $\mathrm{Ann}(\mathbf{v}_1)$, that is, $\min_T(x) = x^3 - x^2 + 2x - 2$.

Exercises.

7.1.1. Prove Proposition 7.1.2 and Corollary 7.1.3.

7.1.2. Let $C_1 = \mathbb{Z}g_1$, $C_2 = \mathbb{Z}g_2$ and $C_3 = \mathbb{Z}g_3$ be cyclic abelian groups of orders 6, 10 and 15 respectively.

(i) Find the order of $(3g_1, 5g_2) \in C_1 \times C_2$.

(ii) Find the order of $(g_1, g_2, g_3) \in C_1 \times C_2 \times C_3$.

(iii) Find the exponent of $C_1 \times C_2$.

(iv) Find the exponent of $C_1 \times C_2 \times C_3$.

7.1.3. Let V be a vector space of dimensions 3 over $\mathbb{R}$, let $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ be a basis of V, and let $T \in \mathrm{End}_{\mathbb{R}}(V)$. Suppose that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 2 \\ 1 & -1 & -2 \end{pmatrix}.$$

For the corresponding structure of a $\mathbb{R}[x]$-module on V:

(i) find the monic generator of $\mathrm{Ann}(\mathbf{v}_1)$;

(ii) find the monic generator of $\mathrm{Ann}(\mathbf{v}_2)$ and, from this, deduce the monic generator of $\mathrm{Ann}(V)$.

7.1.4. Let $T\colon \mathbb{Q}^3 \to \mathbb{Q}^3$ be the linear map whose matrix relative to the standard basis $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ of $\mathbb{Q}^3$ is

$$[\,T\,]_{\mathcal{E}} = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 2 & 2 \\ -2 & 2 & 3 \end{pmatrix}.$$

For the corresponding structure of a $\mathbb{Q}[x]$-module on $\mathbb{Q}^3$:

(i) find the monic generator of $\mathrm{Ann}(\mathbf{e}_1 + \mathbf{e}_3)$;

(ii) show that $\mathbb{Q}^3$ is cyclic and find $\min_T(x)$.

7.1.5. Let V be a vector space of dimension n over a field K and let $T \in \mathrm{End}_K(V)$.

(i) Show that $I, T, \ldots, T^{n^2}$ are linearly dependent over K.

(ii) Deduce that there exists a nonzero polynomial $p(x) \in K[x]$ of degree at most n^2 such that $p(T) = 0$.

(iii) State and prove the corresponding result for a matrix $A \in \mathrm{Mat}_{n\times n}(K)$.

7.1.6. Let V be a vector space of dimension n over a field K and let $T \in \mathrm{End}_K(V)$. Suppose that V is T-cyclic (i.e. cyclic as a $K[x]$-module for the corresponding $K[x]$-module structure). Show that there exists a nonzero polynomial $p(x) \in K[x]$ of degree at most n such that $p(T) = 0$.

7.2 Modules over a euclidean domain

We first state the structure theorem for a module of finite type over a euclidean domain, and then we examine its consequence for abelian groups and vector spaces equipped with an endomorphism. The proof of the theorem will be given in Chapter 8.

Theorem 7.2.1 (The structure theorem)**.** *Let M be a module of finite type over a euclidean domain A. Then M is a direct sum of cyclic submodules*

$$M = A\mathbf{u}_1 \oplus A\mathbf{u}_2 \oplus \cdots \oplus A\mathbf{u}_s$$

with $A \supsetneq \mathrm{Ann}(\mathbf{u}_1) \supseteq \mathrm{Ann}(\mathbf{u}_2) \supseteq \cdots \supseteq \mathrm{Ann}(\mathbf{u}_s)$.

Since A is euclidean, each of the ideals $\mathrm{Ann}(\mathbf{u}_i)$ is generated by an element d_i of A. The condition $\mathrm{Ann}(\mathbf{u}_i) \supseteq \mathrm{Ann}(\mathbf{u}_{i+1})$ implies in this case that $d_i \mid d_{i+1}$ if $d_i \neq 0$ and that $d_{i+1} = 0$ if $d_i = 0$. Therefore there exists an integer t such that $d_1, \ldots, d_t$ are nonzero with $d_1 \mid d_2 \mid \ldots \mid d_t$ and $d_{t+1} = \cdots = d_s = 0$. Moreover, the condition $A \neq \mathrm{Ann}(\mathbf{u}_1)$ implies that d_1 is not a unit. This is easy to fulfill since if $\mathrm{Ann}(\mathbf{u}_1) = A$, then $\mathbf{u}_1 = 0$ and so we can omit the factor $A\mathbf{u}_1$ in the direct sum.

While the decomposition of M given by Theorem 7.2.1 is not unique in general, one can show that the integer s and the ideals $\mathrm{Ann}(\mathbf{u}_1), \ldots, \mathrm{Ann}(\mathbf{u}_s)$ only depend on M and not on the choice of the $\mathbf{u}_i$. For example, we have the following characterization of $\mathrm{Ann}(\mathbf{u}_s)$, whose proof is left as an exercise:

Corollary 7.2.2. *With the notation of Theorem 7.2.1, we have* $\mathrm{Ann}(M) = \mathrm{Ann}(\mathbf{u}_s)$.

In the case where $A = \mathbb{Z}$, an A-module is simply an abelian group. For a finite abelian group, Theorem 7.2.1 and its corollary give:

Theorem 7.2.3. *Let G be a finite abelian group. Then G is a direct sum of cyclic subgroups*

$$G = \mathbb{Z}g_1 \oplus \mathbb{Z}g_2 \oplus \cdots \oplus \mathbb{Z}g_s$$

with $o(g_1) \neq 1$ and $o(g_1) \,|\, o(g_2) \,|\, \ldots \,|\, o(g_s)$. Furthermore, the exponent of G is $o(g_s)$.

For the situation in which we are particularly interested in this course, we obtain:

Theorem 7.2.4. *Let V be a finite-dimensional vector space over a field K and let $T \in \mathrm{End}_K(V)$. For the corresponding structure of a $K[x]$-module on V, we can write*

$$V = K[x]\mathbf{v}_1 \oplus K[x]\mathbf{v}_2 \oplus \cdots \oplus K[x]\mathbf{v}_s \tag{7.2}$$

such that, if we denote by $d_i(x)$ the monic generator of $\mathrm{Ann}(\mathbf{v}_i)$ for $i = 1, \ldots, s$, we have $\deg(d_1(x)) \neq 0$ and

$$d_1(x) \,|\, d_2(x) \,|\, \ldots \,|\, d_s(x).$$

The minimal polynomial of T is $d_s(x)$.

Combining this result with Proposition 7.1.7, we get:

Theorem 7.2.5. *With the notation of Theorem 7.2.4, set*

$$V_i = K[x]\mathbf{v}_i \quad \text{and} \quad n_i = \deg(d_i(x))$$

for $i = 1, \ldots, s$. Then the ordered set

$$\mathcal{C} = \{\mathbf{v}_1, T(\mathbf{v}_1), \ldots, T^{n_1-1}(\mathbf{v}_1), \ldots\ldots, \mathbf{v}_s, T(\mathbf{v}_s), \ldots, T^{n_s-1}(\mathbf{v}_s)\}$$

is a basis of V relative to which the matrix of T is block diagonal with s blocks on the diagonal:

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} D_1 & & & 0 \\ & D_2 & & \\ & & \ddots & \\ 0 & & & D_s \end{pmatrix}, \tag{7.3}$$

the i-th block D_i of the diagonal being the companion matrix of the polynomial $d_i(x)$.

Proof. By Proposition 7.1.7, each V_i is a T-cyclic subspace of V that admits a basis

$$\mathcal{C}_i = \{\mathbf{v}_i, T(\mathbf{v}_i), \dots, T^{n_i-1}(\mathbf{v}_i)\}$$

and we have

$$[\,T|_{V_i}\,]_{\mathcal{C}_i} = D_i.$$

Since $V = V_1 \oplus \cdots \oplus V_s$, Theorem 2.6.6 implies that $\mathcal{C} = \mathcal{C}_1 \amalg \cdots \amalg \mathcal{C}_s$ is a basis of V such that

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} [T|_{V_1}]_{\mathcal{C}_1} & & 0 \\ 0 & \ddots & \\ & & [T|_{V_s}]_{\mathcal{C}_s} \end{pmatrix} = \begin{pmatrix} D_1 & & 0 \\ 0 & \ddots & \\ & & D_s \end{pmatrix}.$$

□

The polynomials $d_1(x), \dots, d_s(x)$ appearing in Theorem 7.2.4 are called the *invariant factors* of T and the corresponding matrix (7.3) given by Theorem 7.2.5 is call the *rational canonical form* of T. It follows from Theorem 7.2.5 that the sum of the degree of the invariant factors of T is equal to the dimension of V.

Example 7.2.6. Let V be a vector space over $\mathbb{R}$ of dimension 5. Suppose that the invariant factors of T are

$$d_1(x) = x - 1, \quad d_2(x) = d_3(x) = x^2 - 2x + 1.$$

Then there exists a basis $\mathcal{C}$ of V such that

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} \boxed{1} & & & 0 \\ & \boxed{\begin{matrix} 0 & -1 \\ 1 & 2 \end{matrix}} & & \\ 0 & & \boxed{\begin{matrix} 0 & -1 \\ 1 & 2 \end{matrix}} \end{pmatrix}$$

since the companion matrix of $x - 1$ is $\begin{pmatrix} 1 \end{pmatrix}$ and that of $x^2 - 2x + 1$ is $\begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}$.

The proof of Theorem 7.2.5 does not use the divisibility relations relating the polynomials $d_1(x), \dots, d_s(x)$. In fact, it applies to any decomposition of the form (7.2).

Example 7.2.7. Let V be a vector space over $\mathbb{C}$ of dimension 5 and let $T\colon V \to V$ be a linear operator on $\mathbb{C}$. Suppose that, for the corresponding structure of a $\mathbb{C}[x]$-module on V, we have

$$V = \mathbb{C}[x]\mathbf{v}_1 \oplus \mathbb{C}[x]\mathbf{v}_2 \oplus \mathbb{C}[x]\mathbf{v}_3$$

and that the monic generators of the annihilators of $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{v}_3$ are respectively

$$x^2 - i\,x + 1 - i, \quad x - 1 + 2i, \quad x^2 + (2+i)x - 3.$$

Then $\mathcal{C} = \{\mathbf{v}_1, T(\mathbf{v}_1), \mathbf{v}_2, \mathbf{v}_3, T(\mathbf{v}_3)\}$ is a basis of V and

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} \boxed{\begin{matrix} 0 & -1+i \\ 1 & i \end{matrix}} & & 0 \\ & \boxed{1-2i} & \\ 0 & & \boxed{\begin{matrix} 0 & 3 \\ 1 & -2-i \end{matrix}} \end{pmatrix}.$$

Exercises.

7.2.1. Prove Corollary 7.2.2 using Theorem 7.2.1.

7.2.2. Prove Theorem 7.2.3 using Theorem 7.2.1 and Corollary 7.2.2.

7.2.3. Prove Theorem 7.2.4 using Theorem 7.2.1 and Corollary 7.2.2.

7.2.4. Let V be a finite-dimensional real vector space equipped with an endomorphism $T \in \mathrm{End}_{\mathbb{R}}(V)$. Suppose that, for the corresponding structure of an $\mathbb{R}[x]$-module on V, we have

$$V = \mathbb{R}[x]\mathbf{v}_1 \oplus \mathbb{R}[x]\mathbf{v}_2 \oplus \mathbb{R}[x]\mathbf{v}_3,$$

where $\mathbf{v}_1$, $\mathbf{v}_2$ and $\mathbf{v}_3$ are elements of V whose respective annihilators are generated by $x^2 - x + 1$, x^3 and $x - 2$. Determine the dimension of V, a basis $\mathcal{C}$ of V associated to this decomposition and, for this basis, determine $[\,T\,]_{\mathcal{C}}$.

7.2.5. Let $A \in \mathrm{Mat}_{n\times n}(K)$ where K is a field. Show that there exist nonconstant monic polynomials $d_1(x), \ldots, d_s(x) \in K[x]$ with $d_1(x) \mid \cdots \mid d_s(x)$ and an invertible matrix $P \in \mathrm{Mat}_{n\times n}(K)$ such that PAP^{-1} is block diagonal, with the companion matrices of $d_1(x), \ldots, d_s(x)$ on the diagonal.

7.3 Primary decomposition

Theorem 7.2.1 tells us that every module of finite type over a euclidean ring is a direct sum of cyclic submodules. To obtain a finer decomposition, it suffices to decompose cyclic modules. This is the subject of primary decomposition. Since it applies to every module with nonzero annihilator, we consider the more general case, which is no more complicated.

Before stating the principal result, recall that, if M is a module over a commutative ring A, then, for each $a \in A$, we define A-submodules of M by setting

$$M_a := \{\mathbf{u} \in M\,;\, a\mathbf{u} = \mathbf{0}\} \quad \text{and} \quad aM = \{a\mathbf{u}\,;\, \mathbf{u} \in M\}$$

(see Example 6.5.12).

Theorem 7.3.1. *Let M be a module over a euclidean ring A. Suppose that $M \neq \{\mathbf{0}\}$ and that $\mathrm{Ann}(M)$ contains a nonzero element a. Write*

$$a = \epsilon q_1 \ldots q_s$$

where ϵ is a unit in A, s is an integer ≥ 0, and $q_1, \ldots, q_s$ are nonzero elements of A which are pairwise relatively prime. Then the integer s is ≥ 1 and we have:

1) $M = M_{q_1} \oplus \cdots \oplus M_{q_s}$,

2) $M_{q_i} = q_1 \cdots \widehat{q_i} \cdots q_s M$ *for* $i = 1, \ldots, s$.

Furthermore, if $\mathrm{Ann}(M) = (a)$*, then* $\mathrm{Ann}(M_{q_i}) = (q_i)$ *for* $i = 1, \ldots, s$.

In formula 2), the hat on q_i indicates that q_i is omitted from the product. If $s = 1$, this product is empty and we adopt the convention that $q_1 \cdots \widehat{q_i} \cdots q_s = 1$.

Proof. Since $\mathrm{Ann}(M)$ is an ideal of A, it contains

$$\epsilon^{-1} a = q_1 \cdots q_s.$$

Furthermore, since $M \neq \{0\}$, it does not contain 1. Therefore, we must have $s \geq 1$.

If $s = 1$, we find that $M = M_{q_1} = \widehat{q_1} M$, and formulas 1) and 2) are verified. Suppose now that $s \geq 2$ and define

$$a_i := q_1 \cdots \widehat{q_i} \cdots q_s \quad \text{for } i = 1, \ldots, s.$$

Since $q_1, \ldots, q_s$ are pairwise relatively prime, the products $a_1, \ldots, a_s$ are relatively prime (i.e. their gcd is one), and so there exist $r_1, \ldots, r_s \in A$ such that

$$r_1 a_1 + \cdots + r_s a_s = 1$$

(see Exercise 7.3.1). Then, for all $u \in M$, we have:

$$u = (r_1 a_1 + \cdots + r_s a_s) u = r_1 a_1 u + \cdots + r_s a_s u. \tag{7.4}$$

Since $r_i a_i u = a_i (r_i u) \in a_i M$ for $i = 1, \ldots, s$, this shows that

$$M = a_1 M + \cdots + a_s M. \tag{7.5}$$

If $u \in M_{q_i}$, we have $a_j u = 0$ for every index j different from i since $q_i \mid a_j$. Thus formula (7.4) gives:

$$u = r_i a_i u \quad \text{for all } u \in M_{q_i}. \tag{7.6}$$

This shows that $M_{q_i} \subseteq a_i M$. Since

$$q_i a_i M = \epsilon^{-1} a M = \{0\},$$

we also have $a_i M \subseteq M_{q_i}$, hence $a_i M = M_{q_i}$. Then equality (7.5) becomes

$$M = M_{q_1} + \cdots + M_{q_s}. \tag{7.7}$$

To show that this sum is direct, choose $u_1 \in M_{q_1}, \ldots, u_s \in M_{q_s}$ such that

$$u_1 + \cdots + u_s = 0.$$

By multiplying the two sides of this equalities by $r_i a_i$ and noting that $r_i a_i u_j = 0$ for $j \neq i$ (since $q_j \mid a_i$ if $j \neq i$), we have

$$r_i a_i u_i = 0.$$

Since (7.6) gives $u_i = r_i a_i u_i$, we conclude that $u_i = 0$ for $i = 1, \ldots, s$. By Definition 6.4.1, this shows that the sum (7.7) is direct.

Finally, suppose that $\mathrm{Ann}(M) = (a)$. Since $M_{q_i} = a_i M$, we see that

$$\begin{aligned}
\mathrm{Ann}(M_{q_i}) &= \mathrm{Ann}(a_i M) \\
&= \{r \in A\,;\, r\, a_i M = \{0\}\} \\
&= \{r \in A\,;\, r\, a_i \in \mathrm{Ann}(M)\} \\
&= \{r \in A\,;\, a \,|\, r\, a_i\} \\
&= (q_i).
\end{aligned}$$

□

For a cyclic module, Theorem 7.3.1 implies the following:

Corollary 7.3.2. *Let A be a euclidean ring and let $M = A\,\mathbf{u}$ be a cylic A-module. Suppose that $\mathbf{u} \neq \mathbf{0}$ and that $\mathrm{Ann}(\mathbf{u}) \neq \{\mathbf{0}\}$. Choose a generator a of $\mathrm{Ann}(\mathbf{u})$ and factor it in the form*

$$a = \epsilon p_1^{e_1} \cdots p_s^{e_s}$$

where ϵ is a unit of A, s is an integer ≥ 1, $p_1, \ldots, p_s$ are pairwise non-associated irreducible elements of A, and $e_1, \ldots, e_s$ are positive integers. Then, for $i = 1, \ldots, s$, the product

$$\mathbf{u}_i = p_1^{e_1} \cdots \widehat{p_i^{e_i}} \cdots p_s^{e_s} \mathbf{u} \in M$$

satisfies $\mathrm{Ann}(\mathbf{u}_i) = (p_i^{e_i})$, and we have:

$$M = A\mathbf{u}_1 \oplus \cdots \oplus A\mathbf{u}_s. \tag{7.8}$$

Proof. Since $\mathrm{Ann}(M) = \mathrm{Ann}(\mathbf{u}) = (a)$, Theorem 7.3.1 applies with $q_1 = p_1^{e_1}, \ldots, q_s = p_s^{e_s}$. Since

$$q_1 \cdots \widehat{q_i} \cdots q_s\, M = A\mathbf{u}_i \quad (1 \leq i \leq s),$$

it gives the decomposition (7.8) and

$$\mathrm{Ann}(\mathbf{u}_i) = \mathrm{Ann}(A\mathbf{u}_i) = (q_i) = (p_i^{e_i}) \quad (1 \leq i \leq s).$$

□

Combining this result with Theorem 7.2.1, we obtain:

Theorem 7.3.3. *Let M be a module of finite type over a euclidean ring. Suppose that $M \neq \{\mathbf{0}\}$ and that $\mathrm{Ann}(M) \neq \{0\}$. Then M is a direct sum of cyclic submodules whose annihilator is generated by a power of an irreducible element of A.*

Proof. Corollary 7.3.2 shows that the result is true for a cylic module. The general case follows since, according to Theorem 7.2.1, the module M is a direct sum of cyclic submodules, and the annihilator of each of these submodules is nonzero since it contains $\mathrm{Ann}(M)$. □

Example 7.3.4. We use the notation of Example 7.1.9. The vector space V is a cyclic $\mathbb{Q}[x]$-module generated by the vector $\mathbf{v}_1$ and the ideal $\mathrm{Ann}(\mathbf{v}_1)$ is generated by

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

Since x^2+2 has no real root, it has no root in $\mathbb{Q}$, hence it is an irreducible polynomial in $\mathbb{Q}[x]$. The polynomial $x-1$ is also irreducible, since its degree is 1. Then Corollary 7.3.2 gives

$$V = \mathbb{Q}[x]\mathbf{u}_1 \oplus \mathbb{Q}[x]\mathbf{u}_2$$

where

$$\begin{array}{rclclcl} \mathbf{u}_1 & = & (x^2+2)\mathbf{v}_1 & = & T^2(\mathbf{v}_1) + 2\mathbf{v}_1 & = & 3\mathbf{v}_1 + 3\mathbf{v}_3, \\ \mathbf{u}_2 & = & (x-1)\mathbf{v}_1 & = & T(\mathbf{v}_1) - \mathbf{v}_1 & = & \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 \end{array}$$

satisfy

$$\mathrm{Ann}(\mathbf{u}_1) = (x-1) \quad \text{and} \quad \mathrm{Ann}(\mathbf{u}_2) = (x^2+2).$$

Reasoning as in the proof of Theorem 7.2.5, we deduce that

$$\mathcal{C} = \{\mathbf{u}_1, \mathbf{u}_2, T(\mathbf{u}_2)\} = \{3\mathbf{v}_1 + 3\mathbf{v}_3, \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3, -\mathbf{v}_1 - \mathbf{v}_2 + 2\mathbf{v}_3)\}$$

is a basis of V such that

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} \boxed{1} & 0 \\ 0 & \boxed{\begin{matrix} 0 & -2 \\ 1 & 0 \end{matrix}} \end{pmatrix}$$

are block diagonal with the companion matrices of $x-1$ and x^2+2 on the diagonal.

We leave it to the reader to analyze the meaning of Theorem 7.3.3 for abelian groups. For the situation that interests us the most, we have:

Theorem 7.3.5. *Let V be a finite-dimensional vector space over a field K and let $T\colon V \to V$ be a linear operator on V. There exists a basis of V relative to which the matrix of T is block diagonal with the companion matrices of powers of monic irreducible polynomials of $K[x]$ on the diagonal.*

This matrix is called a *primary rational canonical form* of T. We can show that it is unique up to a permutation of the blocks on the diagonal. The powers of monic irreducible polynomials whose companion matrices appear on its diagonal are called the *elementary divisors* of T.

We leave the proof of this result as an exercise and we give an example.

Example 7.3.6. Let V be a vector space of dimension 6 over $\mathbb{R}$ and let $T\colon V \to V$ be a linear operator. Suppose that, for the corresponding structure of an $\mathbb{R}[x]$-module on V, we have

$$V = \mathbb{R}[x]\mathbf{v}_1 \oplus \mathbb{R}[x]\mathbf{v}_2$$

with $\mathrm{Ann}(\mathbf{v}_1) = (x^3 - x^2)$ and $\mathrm{Ann}(\mathbf{v}_2) = (x^3 - 1)$.

1st We have $x^3 - x^2 = x^2(x-1)$ where x and $x-1$ are irreducible. Thus,

$$\mathbb{R}[x]\mathbf{v}_1 = \mathbb{R}[x]\mathbf{v}_1' \oplus \mathbb{R}[x]\mathbf{v}_1''$$

where $\mathbf{v}_1' = (x-1)\mathbf{v}_1 = T(\mathbf{v}_1) - \mathbf{v}_1$ and $\mathbf{v}_1'' = x^2\mathbf{v}_1 = T^2(\mathbf{v}_1)$ satisfy

$$\mathrm{Ann}(\mathbf{v}_1') = (x^2) \quad \text{and} \quad \mathrm{Ann}(\mathbf{v}_1'') = (x-1).$$

2nd Similarly, $x^3 - 1 = (x-1)(x^2+x+1)$ is the factorization of x^3-1 as a product of powers of irreducible polynomials of $\mathbb{R}[x]$. Therefore,

$$\mathbb{R}[x]\mathbf{v}_2 = \mathbb{R}[x]\mathbf{v}_2' \oplus \mathbb{R}[x]\mathbf{v}_2''$$

where $\mathbf{v}_2' = (x^2+x+1)\mathbf{v}_2 = T^2(\mathbf{v}_2) + T(\mathbf{v}_2) + \mathbf{v}_2$ and $\mathbf{v}_2'' = (x-1)\mathbf{v}_2 = T(\mathbf{v}_2) - \mathbf{v}_2$ satisfy

$$\mathrm{Ann}(\mathbf{v}_2') = (x-1) \quad \text{and} \quad \mathrm{Ann}(\mathbf{v}_2'') = (x^2+x+1).$$

3rd We conclude that

$$V = \mathbb{R}[x]\mathbf{v}_1' \oplus \mathbb{R}[x]\mathbf{v}_1'' \oplus \mathbb{R}[x]\mathbf{v}_2' \oplus \mathbb{R}[x]\mathbf{v}_2''$$

and that

$$\mathcal{C} = \{\mathbf{v}_1', T(\mathbf{v}_1'), \mathbf{v}_1'', \mathbf{v}_2', \mathbf{v}_2'', T(\mathbf{v}_2'')\}$$

is a basis of V for which

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} \boxed{\begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}} & & & \mathbf{0} \\ & \boxed{1} & & \\ & & \boxed{1} & \\ \mathbf{0} & & & \boxed{\begin{matrix} 0 & -1 \\ 1 & -1 \end{matrix}} \end{pmatrix},$$

with the companion matrices of x^2, $x-1$, $x-1$ and x^2+x+1 on the diagonal.

Exercises.

7.3.1. Let A be a euclidean domain, let $p_1, \ldots, p_s$ be non-associated irreducible elements of A and let $e_1, \ldots, e_s$ be positive integers. Set $q_i = p_i^{e_i}$ and $a_i = q_1 \cdots \widehat{q_i} \cdots q_s$ for $i = 1, \ldots, s$. Show that there exists $r_1, \ldots, r_s \in A$ such that $1 = r_1 a_1 + \cdots + r_s a_s$.

7.3.2. Let M be a module over a euclidean ring A. Suppose that $\mathrm{Ann}(M) = (a)$ with $a \neq 0$, and that $c \in A$ with $c \neq 0$. Show that $M_c = M_d$ where $d = \gcd(a, c)$.

7.3.3. Let V be a vector space over a field K and let $T \in \mathrm{End}_K(V)$. We consider V as a $K[x]$-module in the usual way. Show that, in this context, the notions of the submodules M_a and aM introduced in Example 6.5.12 and recalled before Theorem 7.3.1 become:

$$V_{p(x)} = \ker(p(T)) \quad \text{and} \quad p(x)V = \mathrm{Im}(p(T))$$

for all $p(x) \in k[x]$. Deduce that $\ker(p(T))$ and $\mathrm{Im}(p(T))$ are T-invariant subspaces of V.

7.3.4. Let V be a finite-dimensional vector space over a field K and let $T \in \mathrm{End}_K(V)$. Suppose that $p(x) \in K[x]$ is a monic polynomial such that $p(T) = 0$, and write $p(x) = p_1(x)^{e_1} \cdots p_s(x)^{e_s}$ where $p_1(x), \ldots, p_s(x)$ are distinct monic irreducible polynomials of $K[x]$ and $e_1, \ldots, e_s$ are positive integers. Combining Exercise 7.3.3 and Theorem 7.3.1, show that

(i) $V = (\ker p_1(T)^{e_1}) \oplus \cdots \oplus (\ker p_s(T)^{e_s})$,

(ii) $\ker p_i(T)^{e_i} = \mathrm{Im}\left(p_1(T)^{e_1} \ldots \widehat{p_i(T)^{e_i}} \ldots p_s(T)^{e_s}\right)$ for $i = 1, \ldots s$.

7.3.5. Let V be a vector space of dimension n over a field K, and let $T \in \mathrm{End}_K(V)$. Show that T is diagonalizable if and only if its minimal polynomial $\min_T(x)$ admits a factorization of the form

$$\min_T(x) = (x - \alpha_1) \cdots (x - \alpha_s)$$

where $\alpha_1, \ldots, \alpha_s$ are distinct elements of K.

7.3.6. Let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be a linear maps whose matrix relative to the standard basis $\mathcal{C}$ of $\mathbb{R}^3$ is

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} 2 & 2 & -1 \\ 1 & 3 & -1 \\ 2 & 4 & -1 \end{pmatrix}.$$

(i) Show that $p(T) = 0$ where $p(x) = (x-1)(x-2) \in \mathbb{R}[x]$.

(ii) Why can we assert that $\mathbb{R}^3 = \ker(T - I) \oplus \ker(T - 2I)$?

(iii) Find a basis $\mathcal{B}_1$ for $\ker(T - I)$ and a basis $\mathcal{B}_2$ for $\ker(T - 2I)$.

(iv) Give the matrix of T with respect to the basis $\mathcal{B} = \mathcal{B}_1 \coprod \mathcal{B}_2$ of $\mathbb{R}^3$.

7.3.7. Let V be a vector space over $\mathbb{Q}$ with basis $\mathcal{A} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, and let $T\colon V \to V$ be the linear map whose matrix relative to the basis $\mathcal{A}$ is

$$[\,T\,]_{\mathcal{A}} = \begin{pmatrix} 5 & 1 & 5 \\ -3 & -2 & -2 \\ -3 & -1 & -3 \end{pmatrix}.$$

(i) Show that $p(T) = 0$ where $p(x) = (x+1)^2(x-2) \in \mathbb{Q}[x]$.

(ii) Why can we assert that $V = \ker(T+I)^2 \oplus \ker(T-2I)$?

(iii) Find a basis $\mathcal{B}_1$ for $\ker(T+I)^2$ and a basis $\mathcal{B}_2$ for $\ker(T-2I)$.

(iv) Give the matrix of T with respect to the basis $\mathcal{B} = \mathcal{B}_1 \coprod \mathcal{B}_2$ of V.

7.3.8. Let V be a finite-dimensional vector space over $\mathbb{C}$ and let $T\colon V \to V$ be a $\mathbb{C}$-linear map. Suppose that the polynomial $p(x) = x^4 - 1$ satisfies $p(T) = 0$. Factor $p(x)$ as a product of powers of irreducible polynomials in $\mathbb{C}[x]$ and give a corresponding decomposition of V as a direct sum of T-invariant subspaces.

7.3.9. Let V be a finite-dimensional vector space over $\mathbb{R}$ and let $T\colon V \to V$ be an $\mathbb{R}$-linear map. Suppose that the polynomial $p(x) = x^3 + 2x^2 + 2x + 4$ satisfies $p(T) = 0$. Factor $p(x)$ as a product of powers of irreducible polynomials in $\mathbb{R}[x]$ and give a corresponding decomposition of V as a direct sum of T-invariant subspaces.

7.3.10 (Application to differential equations). Let D be the operator of derivation on the vector space $\mathcal{C}_\infty(\mathbb{R})$ of infinitely differentiable functions from $\mathbb{R}$ to $\mathbb{R}$. Rolle's Theorem tells us that if a function $f\colon \mathbb{R} \to \mathbb{R}$ is differentiable at each point $x \in \mathbb{R}$ with $f'(x) = 0$, then f is constant.

(i) Let $\lambda \in \mathbb{R}$. Suppose that a function satisfies $f'(x) = \lambda f(x)$ for all $x \in \mathbb{R}$. Applying Rolle's Theorem to the function $f(x)e^{-\lambda x}$, shows that there exists a constant $C \in \mathbb{R}$ such that $f(x) = Ce^{\lambda x}$ for all $x \in \mathbb{R}$. Deduce that $\ker(D - \lambda I) = \langle e^{\lambda x} \rangle_{\mathbb{R}}$.

(ii) Let $\lambda_1, \ldots, \lambda_s$ be distinct real numbers, and let $p(x) = (x - \lambda_1) \cdots (x - \lambda_s) \in \mathbb{R}[x]$. Combining the result of (i) with Theorem 7.3.1, show that $\ker p(D)$ is a subspace of $\mathcal{C}_\infty(\mathbb{R})$ of dimension s that admits the basis $\{e^{\lambda_1 x}, \ldots, e^{\lambda_s x}\}$.

(iii) Determine the general form of functions $f \in \mathcal{C}_\infty(\mathbb{R})$ such that $f''' - 2f'' - f' + 2f = 0$.

7.4 Jordan canonical form

In this section, we fix a finite-dimensional vector space V over $\mathbb{C}$ and a linear operator $T\colon V \to V$. We also equip V with the corresponding structure of a $\mathbb{C}[x]$-module.

Since the irreducible monic polynomials of $\mathbb{C}[x]$ are of the form $x - \lambda$ with $\lambda \in \mathbb{C}$, Theorem 7.3.3 gives

$$V = \mathbb{C}[x]\mathbf{v}_1 \oplus \cdots \oplus \mathbb{C}[x]\mathbf{v}_s$$

for the elements $\mathbf{v}_1, \ldots, \mathbf{v}_s$ of V whose annihilators are of the form

$$\mathrm{Ann}(\mathbf{v}_1) = \big((x - \lambda_1)^{e_1}\big), \ \ldots, \ \mathrm{Ann}(\mathbf{v}_s) = \big((x - \lambda_s)^{e_s}\big)$$

with $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ and $e_1, \ldots, e_s \in \mathbb{N}_{>0}$.

Set $U_i = \mathbb{C}[x]\mathbf{v}_i$ for $i = 1, \ldots, s$. For each i, Proposition 7.1.7 shows that $\mathcal{C}_i := \{\mathbf{v}_i, T(\mathbf{v}_i), \ldots, T^{e_i-1}(\mathbf{v}_i)\}$ is a basis of U_i and that $[\,T|_{U_i}\,]_{\mathcal{C}_i}$ is the companion matrix of $(x-\lambda_i)^{e_i}$. Then Theorem 2.6.6 tells us that $\mathcal{C} = \mathcal{C}_1 \amalg \cdots \amalg \mathcal{C}_s$ is a basis of V relative to which the matrix $[\,T\,]_{\mathcal{C}}$ of T is block diagonal with the companion matrices of the polynomials $(x-\lambda_1)^{e_1}, \ldots, (x-\lambda_s)^{e_s}$ on the diagonal. This is the rational canonical form of T. The following lemma proposes a different choice of basis for each of the subspaces U_i.

Lemma 7.4.1. *Let $\mathbf{v} \in V$ and let $U := \mathbb{C}[x]\mathbf{v}$. Suppose that $\mathrm{Ann}(\mathbf{v}) = ((x-\lambda)^e)$ with $\lambda \in \mathbb{C}$ and $e \in \mathbb{N}_{>0}$. Then*

$$\mathcal{B} = \{(T-\lambda I)^{e-1}(\mathbf{v}), \ldots, (T-\lambda I)(\mathbf{v}), \mathbf{v}\}$$

is a basis of U for which

$$[\,T|_U\,]_{\mathcal{B}} = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \tag{7.9}$$

Proof. Since $\mathrm{Ann}(\mathbf{v}) = ((x-\lambda)^e)$, Proposition 7.1.7 shows that

$$\mathcal{C} := \{\mathbf{v}, T(\mathbf{v}), \ldots, T^{e-1}(\mathbf{v})\}$$

is a basis of U and therefore $\dim_{\mathbb{C}}(U) = e$. Set

$$\mathbf{u}_i = (T-\lambda I)^{e-i}(\mathbf{v}) \quad \text{for } i = 1, \ldots, e,$$

so that $\mathcal{B}$ can be written as

$$\mathcal{B} = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_e\}$$

(we adopt the convention that $\mathbf{u}_e = (T-\lambda I)^0(\mathbf{v}) = \mathbf{v}$). We see that

$$T(\mathbf{u}_1) = (T-\lambda I)(\mathbf{u}_1) + \lambda\mathbf{u}_1 = (T-\lambda I)^e(\mathbf{v}) + \lambda\mathbf{u}_1 = \lambda\mathbf{u}_1 \tag{7.10}$$

since $(T-\lambda I)^e(\mathbf{v}) = (x-\lambda)^e\mathbf{v} = \mathbf{0}$. For $i = 2, \ldots, e$, we also have

$$T(\mathbf{u}_i) = (T-\lambda I)(\mathbf{u}_i) + \lambda\mathbf{u}_i = \mathbf{u}_{i-1} + \lambda\mathbf{u}_i\,. \tag{7.11}$$

Relation (7.10) and (7.11) show in particular that

$$T(\mathbf{u}_i) \in \langle \mathbf{u}_1, \ldots, \mathbf{u}_e \rangle_{\mathbb{C}} \quad \text{for } i = 1, \ldots, e.$$

Thus $\langle \mathbf{u}_1, \ldots, \mathbf{u}_e \rangle_{\mathbb{C}}$ is a T-invariant subspace of U. Since it contains $\mathbf{v} = \mathbf{u}_e$, it contains all elements of $\mathcal{C}$ and so

$$\langle \mathbf{u}_1, \ldots, \mathbf{u}_e \rangle_{\mathbb{C}} = U.$$

Since $\dim_{\mathbb{C}}(U) = e = |\mathcal{B}|$, we conclude that $\mathcal{B}$ is a basis of U. From (7.10) and (7.11), we deduce

$$[T(\mathbf{u}_1)]_{\mathcal{B}} = [\lambda\mathbf{u}_1]_{\mathcal{B}} = \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{and} \quad [T(\mathbf{u}_i)]_{\mathcal{B}} = [\mathbf{u}_{i-1} + \lambda\mathbf{u}_i]_{\mathcal{B}} = \begin{array}{cl} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \lambda \\ \vdots \\ 0 \end{pmatrix} & \begin{array}{l} \\ \\ \leftarrow i \\ \\ \\ \\ \end{array} \end{array} \quad \text{for } i = 2, \ldots, e,$$

and hence the form (7.9) for the matrix $[\,T|_U\,]_{\mathcal{B}}$. □

Definition 7.4.2 (Jordan block). For each $\lambda \in \mathbb{C}$ and each $e \in \mathbb{N}_{>0}$, we denote by $J_\lambda(e)$ the square matrix of size e with entries on the diagonal equal to λ, entries just above the diagonal equal to 1, and all other entries equal to 0:

$$J_\lambda(e) = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \in \mathrm{Mat}_{e\times e}(\mathbb{C}).$$

We call it the *Jordan block* of size $e \times e$ for λ.

Thanks to Lemma 7.4.1 and the discussion preceding it, we conclude:

Theorem 7.4.3. *There exists a basis $\mathcal{B}$ of V such that $[\,T\,]_{\mathcal{B}}$ is block diagonal with Jordan blocks on the diagonal.*

Proof. Lemma 7.4.1 shows that, for $i = 1, \ldots, s$, the subspace U_i admits the basis

$$\mathcal{B}_i = \{(T - \lambda_i I)^{e_i - 1}(\mathbf{v}_i), \ldots, (T - \lambda_i I)(\mathbf{v}_i), \mathbf{v}_i\}$$

and that

$$[\,T|_{U_i}\,]_{\mathcal{B}_i} = J_{\lambda_i}(e_i).$$

Then, according to Theorem 2.6.6, the ordered set $\mathcal{B} := \mathcal{B}_1 \amalg \cdots \amalg \mathcal{B}_s$ is a basis of V for which

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} J_{\lambda_1}(e_1) & & & 0 \\ & J_{\lambda_2}(e_2) & & \\ & & \ddots & \\ 0 & & & J_{\lambda_s}(e_s) \end{pmatrix}. \tag{7.12}$$

□

We say that (7.12)) is a *Jordan canonical form* (or *Jordan normal form*) of T. The following result shows that this form is essentially unique and gives a method for calculating it:

Theorem 7.4.4. *The Jordan canonical forms of T are obtained from one another by a permutation of the Jordan blocks on the diagonal. These blocks are of the form $J_\lambda(e)$ where λ is an eigenvalue of T and where e is an integer ≥ 1. For each $\lambda \in \mathbb{C}$ and each integer $k \geq 1$, we have*

$$\dim_{\mathbb{C}} \ker(T - \lambda I)^k = \sum_{e \geq 1} \min(k, e)\, n_\lambda(e) \tag{7.13}$$

where $n_\lambda(e)$ denotes the number of Jordan blocks equal to $J_\lambda(e)$ on the diagonal.

Before proceeding to the proof of this theorem, we first explain how formula (7.13) allows us to calculate the integers $n_\lambda(e)$ and hence to determine a Jordan canonical form of T. For this, we fix $\lambda \in \mathbb{C}$. We note that there exists an integer $r \geq 1$ such that $n_\lambda(e) = 0$ for all $e > r$ and we set

$$m_k = \dim_{\mathbb{C}} \ker(T - \lambda I)^k$$

for $k = 1, \ldots, r$. Then formula (7.13) gives

$$\begin{aligned}
m_1 &= n_\lambda(1) + \ \ n_\lambda(2) + \ \ n_\lambda(3) + \cdots + \ \ n_\lambda(r), \\
m_2 &= n_\lambda(1) + 2n_\lambda(2) + 2n_\lambda(3) + \cdots + 2n_\lambda(r), \\
m_3 &= n_\lambda(1) + 2n_\lambda(2) + 3n_\lambda(3) + \cdots + 3n_\lambda(r), \\
&\cdots \\
m_r &= n_\lambda(1) + 2n_\lambda(2) + 3n_\lambda(3) + \cdots + rn_\lambda(r).
\end{aligned} \tag{7.14}$$

From this we deduce

$$\begin{aligned}
m_1 &= n_\lambda(1) + n_\lambda(2) + n_\lambda(3) + \cdots + n_\lambda(r), \\
m_2 - m_1 &= n_\lambda(2) + n_\lambda(3) + \cdots + n_\lambda(r), \\
m_3 - m_2 &= n_\lambda(3) + \cdots + n_\lambda(r), \\
&\cdots \\
m_r - m_{r-1} &= n_\lambda(r).
\end{aligned}$$

Therefore, we can recover $n_\lambda(1), \ldots, n_\lambda(r)$ from the data $m_1, \ldots, m_r$. Explicitly, this gives

$$n_\lambda(e) = \begin{cases} 2m_1 - m_2 & \text{if } e = 1, \\ 2m_e - m_{e-1} - m_{e+1} & \text{if } 1 < e < r, \\ m_r - m_{r-1} & \text{if } e = r. \end{cases} \tag{7.15}$$

Proof of Theorem 7.4.4. Suppose that $[T]_{\mathcal{B}}$ is in Jordan canonical form 7.12 for a basis $\mathcal{B}$ of V.

Exercise 7.4.1 at the end of this section shows that, for every permuation $J_1', \ldots, J_s'$ of the blocks $J_{\lambda_1}(e_1), \ldots, J_{\lambda_s}(e_s)$, there exists a basis $\mathcal{B}'$ of V such that

$$[T]_{\mathcal{B}'} = \begin{pmatrix} J_1' & & 0 \\ & \ddots & \\ 0 & & J_s' \end{pmatrix}.$$

To prove the first statement of the theorem, it therefore suffices to verify formula (7.13) because, as the remark following the theorem shows, this formula allows us to calculate all the integers $n_\lambda(e)$ and thus determine a Jordan canonical form of T up to a permutation of the blocks on the diagonal.

Fix $\lambda \in \mathbb{C}$ and $k \in \mathbb{N}_{>0}$, and set $n = \dim_{\mathbb{C}}(V)$. We have

$$\begin{aligned}
\dim_{\mathbb{C}} \ker(T - \lambda I)^k &= n - \operatorname{rank}[(T - \lambda I)^k]_{\mathcal{B}} \\
&= n - \operatorname{rank}([T]_{\mathcal{B}} - \lambda I)^k \\
&= n - \operatorname{rank} \begin{pmatrix} J_{\lambda_1}(e_1) - \lambda I & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_s}(e_s) - \lambda I \end{pmatrix}^k \\
&= n - \operatorname{rank} \begin{pmatrix} (J_{\lambda_1}(e_1) - \lambda I)^k & & 0 \\ & \ddots & \\ 0 & & (J_{\lambda_s}(e_s) - \lambda I)^k \end{pmatrix} \\
&= n - \big(\operatorname{rank}(J_{\lambda_1}(e_1) - \lambda I)^k + \cdots + \operatorname{rank}(J_{\lambda_s}(e_s) - \lambda I)^k\big).
\end{aligned}$$

Since we also have $n = e_1 + \cdots + e_s$, we conclude that

$$\dim_{\mathbb{C}} \ker(T - \lambda I)^k = \sum_{i=1}^{s} \big(e_i - \operatorname{rank}(J_{\lambda_i}(e_i) - \lambda I)^k\big).$$

For $i = 1, \ldots, s$, we have

$$J_{\lambda_i}(e_i) - \lambda I = \begin{pmatrix} \lambda_i - \lambda & 1 & & 0 \\ & \lambda_i - \lambda & \ddots & \\ 0 & & \ddots & 1 \\ & & & \lambda_i - \lambda \end{pmatrix} = J_{\lambda_i - \lambda}(e_i)$$

and so the formula becomes

$$\dim_{\mathbb{C}} \ker(T - \lambda I)^k = \sum_{i=1}^{s} \big(e_i - \operatorname{rank}(J_{\lambda_i - \lambda}(e_i))^k\big). \tag{7.16}$$

If $\lambda_i \neq \lambda$, we have

$$\det(J_{\lambda_i - \lambda}(e_i)) = (\lambda_i - \lambda)^{e_i} \neq 0,$$

hence $J_{\lambda_i - \lambda}(e_i)$ is invertible. Then $J_{\lambda_i - \lambda}(e_i)^k$ is also invertible for each integer $k \geq 1$. Therefore, we have

$$\operatorname{rank}(J_{\lambda_i - \lambda}(e_i)^k) = e_i \quad \text{if } \lambda_i \neq \lambda. \tag{7.17}$$

If $\lambda_i = \lambda$, we have

$$J_{\lambda_i - \lambda}(e_i) = J_0(e_i) = \begin{pmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ 0 & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

and we easily check by induction on k that

$$J_0(e_i)^k = \left(\begin{array}{c|c} 0 & I_{e_i-k} \\ \hline 0_k & 0 \end{array}\right) \qquad \text{for } k = 1, \dots, e_i - 1 \tag{7.18}$$

and that $J_0(e_i)^k = 0$ if $k \geq e_i$ (in formula (7.18)), the symbol I_{e_i-k} represents the identity matrix of size $(e_i - k) \times (e_i - k)$, the symbol 0_k represents the zero matrix of size $k \times k$, and the symbols 0 on the diagonal are zero matrices of mixed size). From this we deduce that

$$\operatorname{rank}(J_0(e_i)^k) = \begin{cases} e_i - k & \text{if } 1 \leq k < e_i, \\ 0 & \text{if } k \geq e_i. \end{cases} \tag{7.19}$$

By (7.17) and (7.19), formula (7.16) becomes

$$\dim_{\mathbb{C}} \ker(T - \lambda I)^k = \sum_{\{i\,;\,\lambda_i = \lambda\}} \min(k, e_i) = \sum_{e \geq 1} \min(k, e) n_\lambda(e)$$

where, for each integer $e \geq 1$, the integer $n_\lambda(e)$ represents the number of indices $i \in \{1, \dots, s\}$ such that $(\lambda_i, e_i) = (\lambda, e)$, hence the number of blocks equal to $J_\lambda(e)$ on the diagonal of (7.12). This proves formula (7.13) and, at the same time, we complete the proof of the first assertion of the theorem. The exercises at the end of this section propose an alternative proof of (7.13).

Finally, we find that

$$\begin{aligned} \operatorname{char}_T(x) = \det(xI - [T]_{\mathcal{B}}) &= \begin{vmatrix} xI - J_{\lambda_1}(e_1) & & 0 \\ & \ddots & \\ 0 & & xI - J_{\lambda_s}(e_s) \end{vmatrix} \\ &= \det(xI - J_{\lambda_1}(e_1)) \cdots \det(xI - J_{\lambda_s}(e_s)) \\ &= (x - \lambda_1)^{e_1} \cdots (x - \lambda_s)^{e_s}. \end{aligned}$$

Thus, the numbers λ for which the Jordan canonical form (7.12) of T contains a block $J_\lambda(e)$ with $e \geq 1$ are the eigenvalues of T. This proves the second assertion of the theorem and completes the proof. □

To determine the integers $n_\lambda(e)$ using formulas (7.14), we must determine, for each eigenvalue λ of T, the largest integer r such that $n_\lambda(r) \geq 1$. The following corollary provides a method for calculating this integer.

Corollary 7.4.5. *Let λ be an eigenvalue of T. Let $m_k = \dim_{\mathbb{C}} \ker(T - \lambda I)^k$ for all $k \geq 1$. Then we have*

$$m_1 < m_2 < \cdots < m_r = m_{r+1} = m_{r+2} = \cdots$$

where r denotes the largest integer for which $n_\lambda(r) \geq 1$.

Proof. Let r be the largest integer for which $n_\lambda(r) \geq 1$. The equalities (7.14) show that $m_k - m_{k-1} \geq n_\lambda(r) \geq 1$ for $k = 2, \dots, r$ and so $m_1 < m_2 < \cdots < m_r$. For $k \geq r$, formula (7.13) gives $m_k = m_r$. □

Example 7.4.6. Let $T\colon \mathbb{C}^{10} \to \mathbb{C}^{10}$ be a linear map. Suppose that its eigenvalues are $1+i$ and 2, and that the integers

$$m_k = \dim_{\mathbb{C}} \ker(T-(1+i)I)^k \quad \text{and} \quad m'_k = \dim_{\mathbb{C}} \ker(T-2I)^k$$

satisfy

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 6, \quad m_4 = 6, \quad m'_1 = 2, \quad m'_2 = 4 \quad \text{and} \quad m'_3 = 4.$$

Since $m_1 < m_2 < m_3 = m_4$, Corollary 7.4.5 shows that the largest Jordan block of T for the eigenvalue $\lambda = 1+i$ is of size 3×3. Similarly, since $m'_1 < m'_2 = m'_3$, the largest Jordan block of T for the eigenvalue $\lambda = 2$ is of size 2×2.

Formulas (7.14) for $\lambda = 1+i$ give

$$\begin{aligned} m_1 &= 3 = n_{1+i}(1) + \ \ n_{1+i}(2) + \ \ n_{1+i}(3), \\ m_2 &= 5 = n_{1+i}(1) + 2n_{1+i}(2) + 2n_{1+i}(3), \\ m_3 &= 6 = n_{1+i}(1) + 2n_{1+i}(2) + 3n_{1+i}(3), \end{aligned}$$

hence $n_{1+i}(1) = n_{1+i}(2) = n_{1+i}(3) = 1$. For $\lambda = 2$, they are written as

$$\begin{aligned} m'_1 &= 2 = n_2(1) + \ \ n_2(2), \\ m'_2 &= 4 = n_2(1) + 2n_2(2), \end{aligned}$$

hence $n_2(1) = 0$ and $n_2(2) = 2$. We conclude that the Jordan canonical form of T is the block diagonal matrix with the blocks

$$(1+i), \begin{pmatrix} 1+i & 1 \\ 0 & 1+i \end{pmatrix}, \begin{pmatrix} 1+i & 1 & 0 \\ 0 & 1+i & 1 \\ 0 & 0 & 1+i \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

on the diagonal.

Example 7.4.7. Let $T\colon \mathbb{C}^4 \to \mathbb{C}^4$ be the linear map whose matrix relative to the standard basis $\mathcal{E}$ of $\mathbb{C}^4$ is

$$[\,T\,]_{\mathcal{E}} = \begin{pmatrix} 1 & 0 & -1 & 4 \\ 0 & 1 & -1 & 5 \\ 1 & 0 & -1 & 8 \\ 1 & -1 & 0 & 3 \end{pmatrix}.$$

We wish to determine a Jordan canonical form of T.

Solution: We calculate

$$\operatorname{char}_T(x) = \det(xI - [\,T\,]_{\mathcal{E}}) = x^2(x-2)^2.$$

Thus the eigenvalues of T are 0 and 2. We set

$$\begin{aligned} m_k &= \dim_{\mathbb{C}} \ker(T-0I)^k = 4 - \operatorname{rank}[\,T^k\,]_{\mathcal{E}} = 4 - \operatorname{rank}([\,T\,]_{\mathcal{E}})^k \\ m'_k &= \dim_{\mathbb{C}} \ker(T-2I)^k = 4 - \operatorname{rank}[(T-2I)^k]_{\mathcal{E}} = 4 - \operatorname{rank}([\,T\,]_{\mathcal{E}} - 2I)^k \end{aligned}$$

for every integer $k \geq 1$.

We find, after a series of elementary row operations, the following reduced echelon forms:

$$[T]_{\mathcal{E}} \sim \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$[T]_{\mathcal{E}}^2 = \begin{pmatrix} 4 & -4 & 0 & 8 \\ 4 & -4 & 0 & 12 \\ 8 & -8 & 0 & 20 \\ 4 & -4 & 0 & 8 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$[T]_{\mathcal{E}}^3 = \begin{pmatrix} 12 & -12 & 0 & 20 \\ 16 & -16 & 0 & 32 \\ 28 & -28 & 0 & 52 \\ 12 & -12 & 0 & 20 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$[T]_{\mathcal{E}} - 2I = \begin{pmatrix} -1 & 0 & -1 & 4 \\ 0 & -1 & -1 & 5 \\ 1 & 0 & -3 & 8 \\ 1 & -1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$([T]_{\mathcal{E}} - 2I)^2 = \begin{pmatrix} 4 & -4 & 4 & -8 \\ 4 & -4 & 4 & -8 \\ 4 & -8 & 8 & -12 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$([T]_{\mathcal{E}} - 2I)^3 = \begin{pmatrix} -8 & -12 & -12 & 20 \\ -8 & -12 & -12 & 20 \\ -8 & -20 & -20 & 28 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

hence $m_1 = 1$, $m_2 = m_3 = 2$, $m_1' = 1$ and $m_2' = m_3' = 2$. So the largest Jordan block of T for the eigenvalue 0 is of size 2×2 and the block for the eigenvalue 2 is also of size 2×2. Since the sum of the sizes of the block must be equal to 4, we conclude that the Jordan canonical form of T is

$$\begin{pmatrix} J_0(2) & 0 \\ 0 & J_2(2) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

However, this does not say how to find a basis $\mathcal{B}$ of $\mathbb{C}^4$ such that $[T]_{\mathcal{B}}$ is of this form. We will see in the following chapter how to do this in principle.

The matrix version of Theorem 7.4.3 is the following:

Theorem 7.4.8. *Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$. There exists an invertible matrix $P \in GL_n(\mathbb{C})$ such that $P^{-1}AP$ is block diagonal with Jordan blocks on the diagonal.*

Such a product $P^{-1}AP = \begin{pmatrix} J_{\lambda_1}(e_1) & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_s}(e_s) \end{pmatrix}$ is called a *Jordan canonical form of A* (or *Jordan normal form of A*).

The matrix version of Theorem 7.4.4 is stated as follows:

Theorem 7.4.9. *Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$. The Jordan canonical forms of A are obtained from one another by a permutation of the Jordan blocks on the diagonal. The blocks in question are of the form $J_\lambda(e)$ where λ is an eigenvalue of A and where e is an integer ≥ 1. For each $\lambda \in \mathbb{C}$ and each integer $k \geq 1$, we have*

$$n - \mathrm{rank}(A - \lambda I)^k = \sum_{e\geq 1} \min(k, e) n_\lambda(e)$$

where $n_\lambda(e)$ denotes the number of blocks on the diagonal equal to $J_\lambda(e)$.

This result provides the means to determine if two matrices with complex entries are similar or not:

Corollary 7.4.10. *Let $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{C})$. Then A and B are similar if and only if they admit the same Jordan canonical form.*

The proof of this statement is left as an exercise.

Exercises.

7.4.1. Let V be a finite-dimensional vector space over $\mathbb{C}$ and let $T\colon V \to V$ be a linear operator. Suppose that there exists a basis $\mathcal{B}$ of V such that

$$[T]_{\mathcal{B}} = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_s \end{pmatrix}$$

where $A_i \in \mathrm{Mat}_{e_i\times e_i}(\mathbb{C})$ for $i = 1, \ldots, s$. Write

$$\mathcal{B} = \mathcal{B}_1 \amalg \cdots \amalg \mathcal{B}_s$$

where $\mathcal{B}_i$ has e_i elements for $i = 1, \ldots, s$. Finally, for each i, denote by V_i the subspace of V generated by $\mathcal{B}_i$.

(a) Show that each subspace V_i is T-invariant, that it admits $\mathcal{B}_i$ as a basis and that

$$[\,T|_{V_i}\,]_{\mathcal{B}_i} = A_i.$$

(b) Show that if $(i_1, \ldots, i_s)$ is a permutation of $(1, \ldots, s)$, then $\mathcal{B}' = \mathcal{B}_{i_1} \amalg \cdots \amalg \mathcal{B}_{i_s}$ is a basis of V such that

$$[\,T\,]_{\mathcal{B}'} = \begin{pmatrix} A_{i_1} & & 0 \\ & \ddots & \\ 0 & & A_{i_s} \end{pmatrix}.$$

7.4.2. Let V be a vector space over $\mathbb{C}$ and let $T\colon V \to V$ be a linear operator. Suppose that

$$V = V_1 \oplus \cdots \oplus V_s$$

where V_i is a T-invariant subspace of V for $i = 1, \ldots, s$.

(a) Show that $\ker(T) = \ker(T|_{V_1}) \oplus \cdots \oplus \ker(T|_{V_s})$.

(b) Deduce that, for all $\lambda \in \mathbb{C}$ and all $k \in \mathbb{N}_{>0}$, we have

$$\ker(T - \lambda I_V)^k = \ker(T|_{V_1} - \lambda I_{V_1})^k \oplus \cdots \oplus \ker(T|_{V_s} - \lambda I_{V_s})^k.$$

7.4.3. Set $T\colon V \to V$ be a linear operator on a vector space V of dimension n over $\mathbb{C}$. Suppose that there exists a basis $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ of V and $\lambda \in \mathbb{C}$ such that

$$[\,T\,]_{\mathcal{B}} = J_\lambda(n).$$

(a) Show that, if $\lambda \neq 0$, then $\dim_{\mathbb{C}}(\ker T^k) = 0$ for every integer $k \geq 1$.

(b) Suppose that $\lambda = 0$. Show that

$$\ker(T^k) = \langle \mathbf{v}_1, \ldots, \mathbf{v}_k \rangle_{\mathbb{C}}$$

for $k = 1, \ldots, n$. Deduce that $\dim_{\mathbb{C}} \ker(T^k) = \min(k, n)$ for every integer $k \geq 1$.

7.4.4. Give an alternative proof of formula (7.13) of Theorem 7.4.4 by proceeding in the following manner. First suppose that $\mathcal{B}$ is a basis of V such that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} J_{\lambda_1}(e_1) & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_s}(e_s) \end{pmatrix}.$$

By Exercise 7.4.1, we can write $\mathcal{B} = \mathcal{B}_1 \amalg \cdots \amalg \mathcal{B}_s$ where, for each i, $\mathcal{B}_i$ is a basis of a T-invariant subspace V_i of V with

$$[\,T|_{V_i}\,]_{\mathcal{B}_i} = J_{\lambda_i}(e_i)$$

and we have $V = V_1 \oplus \cdots \oplus V_s$.

(a) Applying Exercise 7.4.2, show that

$$\dim_{\mathbb{C}} \ker(T - \lambda I)^k = \sum_{i=1}^{s} \dim_{\mathbb{C}} \ker(T|_{V_i} - \lambda I_{V_i})^k$$

for each $\lambda \in \mathbb{C}$ and each integer $k \geq 1$.

(b) Show that $[\,T|_{V_i} - \lambda I_{V_i}\,]_{\mathcal{B}_i} = J_{\lambda_i - \lambda}(e_i)$ and, using Exercise 7.4.3, deduce that

$$\dim_{\mathbb{C}} \ker(T|_{V_i} - \lambda I_{V_i})^k = \begin{cases} 0 & \text{if } \lambda \neq \lambda_i\,, \\ \min(e_i, k) & \text{if } \lambda = \lambda_i\,. \end{cases}$$

(c) Deduce formula (7.13).

7.4.5. Deduce Theorem 7.4.8 from Theorem 7.4.3 by applying the latter to the linear operator $T_A \colon \mathbb{C}^n \to \mathbb{C}^n$ associated to A. Similarly, deduce Theorem 7.4.9 from Theorem 7.4.4.

7.4.6. Prove Corollary 7.4.10.

7.4.7. Let $T \colon \mathbb{C}^7 \to \mathbb{C}^7$ be a linear map. Suppose that its eigenvalues are 0, 1 and $-i$ and that the integers

$$m_k = \dim_{\mathbb{C}} \ker T^k, \quad m'_k = \dim_{\mathbb{C}} \ker(T - I)^k, \quad m''_k = \dim_{\mathbb{C}} \ker(T + iI)^k$$

satisfy $m_1 = m_2 = 2$, $m'_1 = 1$, $m'_2 = 2$, $m'_3 = m'_4 = 3$, $m''_1 = 1$ and $m''_2 = m''_3 = 2$. Determine a Jordan canonical form of T.

7.4.8. Determine a Jordan canonical form of the matrix

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

Chapter 8

The proof of the structure theorem

This chapter concludes the first part of the course. We first state a theorem concerning submodules of free modules over a euclidean domain and then we show that it implies the structure theorem for modules of finite type over a euclidean domain. In Section 8.2, we prove the Cayley-Hamilton Theorem which says that, for every linear operator $T\colon V \to V$ on a finite-dimensional vector space V, we have $\mathrm{char}_T(T) = 0$. The rest of the chapter is dedicated to the proof of our submodule theorem. In Section 8.3, we show that, if A is a euclidean domian, then every submodule N of A^n has a basis. In Section 8.4, we give an algorithm for finding such a basis from a system of generators of N. In Section 8.5, we present a more complex algorithm that allows us to transform every matrix with coefficients in A into its "Smith normal form" and we deduce from this the theorem on submodules of free modules. Finally, given a linear operator $T\colon V \to V$ as above, Section 8.6 provides a method for determining a basis $\mathcal{B}$ of V such that $[\,T\,]_{\mathcal{B}}$ is in rational canonical form.

Throughout this chapter, A denotes a euclidean domain and n is a positive integer.

8.1 Submodules of free modules, Part I

We first state:

Theorem 8.1.1. *Let N be an A-submodule of A^n. Then there exists a basis $\{C_1, \dots, C_n\}$ of A^n, an integer r with $0 \le r \le n$ and nonzero elements $d_1, \dots, d_r$ of A with $d_1 \mid d_2 \mid \cdots \mid d_r$ such that $\{d_1C_1, \dots, d_rC_r\}$ is a basis of N.*

The proof of this result is given in Section 8.5. We will see that the elements $d_1, \dots, d_r$ are completely determined by N up to multiplication by units of A. We explain here how we can deduce the structure theorem for A-modules of finite type from Theorem 8.1.1.

Proof of Theorem 7.2.1. Let $M = \langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle_A$ be an A-module of finite type. The function

$$\begin{array}{rccc} \psi : & A^n & \longrightarrow & M \\ & \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} & \longmapsto & a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n \end{array} \tag{8.1}$$

is a surjective homomorphism of A-modules. Let

$$N = \ker \psi.$$

Then N is an A-submodule of A^n. By Theorem 8.1.1, there exists a basis $\{C_1, \ldots, C_n\}$ of A^n, an integer r with $0 \le r \le n$ and nonzero elements $d_1, \ldots, d_r$ of A with $d_1 \mid d_2 \mid \cdots \mid d_r$ such that $\{d_1C_1, \ldots, d_rC_r\}$ is a basis of N. Then let

$$\mathbf{u}_i = \psi(C_i) \quad (i = 1, \ldots, n).$$

Since $A^n = \langle C_1, \ldots, C_n\rangle_A$, we have

$$M = \mathrm{Im}(\psi) = \langle \mathbf{u}_1, \ldots, \mathbf{u}_n\rangle_A = A\mathbf{u}_1 + \cdots + A\mathbf{u}_n. \tag{8.2}$$

On the other hand, for $a_1, \ldots, a_n \in A$, we find

$$\begin{aligned} a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n = \mathbf{0} \quad &\Longleftrightarrow \quad a_1\psi(C_1) + \cdots + a_n\psi(C_n) = \mathbf{0} \\ &\Longleftrightarrow \quad \psi(a_1C_1 + \cdots + a_nC_n) = \mathbf{0} \\ &\Longleftrightarrow \quad a_1C_1 + \cdots + a_nC_n \in N. \end{aligned}$$

Recall that $\{d_1C_1, \ldots, d_rC_r\}$ is a basis of N. Thus the condition $a_1C_1 + \cdots + a_nC_n \in N$ is equivalent to the existence of $b_1, \ldots, b_r \in A$ such that

$$a_1C_1 + \cdots + a_nC_n = b_1(d_1C_1) + \cdots + b_r(d_rC_r).$$

Since $C_1, \ldots, C_n$ are linearly independent over A, this is not possible unless

$$a_1 = b_1d_1, \ \ldots, \ a_r = b_rd_r \quad \text{and} \quad a_{r+1} = \cdots = a_n = 0.$$

We conclude that

$$\begin{aligned} a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n = \mathbf{0} \quad &\Longleftrightarrow \quad a_1C_1 + \cdots + a_nC_n \in N \\ &\Longleftrightarrow \quad a_1 \in (d_1), \ \ldots, \ a_r \in (d_r) \quad \text{and} \quad a_{r+1} = \cdots = a_n = 0. \end{aligned} \tag{8.3}$$

In particular, this shows that

$$a_i\mathbf{u}_i = \mathbf{0} \quad \Longleftrightarrow \quad \begin{cases} a_i \in (d_i) & \text{if } 1 \le i \le r, \\ a_i = 0 & \text{if } r < i \le n. \end{cases} \tag{8.4}$$

Thus $\mathrm{Ann}(\mathbf{u}_i) = (d_i)$ for $i = 1, \ldots, r$ and $\mathrm{Ann}(\mathbf{u}_i) = (0)$ for $i = r+1, \ldots, n$. Since $d_1 \mid d_2 \mid \cdots \mid d_r$, we have

$$\mathrm{Ann}(\mathbf{u}_1) \supseteq \mathrm{Ann}(\mathbf{u}_2) \supseteq \cdots \supseteq \mathrm{Ann}(\mathbf{u}_n). \tag{8.5}$$

Formulas (8.3) and (8.4) also imply that

$$a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n = \mathbf{0} \quad \Longleftrightarrow \quad a_1\mathbf{u}_1 = \cdots = a_n\mathbf{u}_n = \mathbf{0}.$$

By (8.2), this property implies that

$$M = A\mathbf{u}_1 \oplus \cdots \oplus A\mathbf{u}_n \tag{8.6}$$

(see Definition 6.4.1). This completes the proof of Theorem 7.2.1 except for the condition that $\mathrm{Ann}(\mathbf{u}_1) \neq A$.

Starting with a decomposition (8.6) satisfying (8.5), it is easy to obtain another with $\mathrm{Ann}(\mathbf{u}_1) \neq A$. Indeed, for all $\mathbf{u} \in M$, we have

$$\mathrm{Ann}(\mathbf{u}) = A \quad \Longleftrightarrow \quad \mathbf{u} = \mathbf{0} \quad \Longleftrightarrow \quad A\mathbf{u} = \{\mathbf{0}\}.$$

Thus if $M \neq \{\mathbf{0}\}$ and k denotes the smallest integer such that $\mathbf{u}_k \neq 0$, we have

$$A \neq \mathrm{Ann}(\mathbf{u}_k) \supseteq \cdots \supseteq \mathrm{Ann}(\mathbf{u}_n)$$

and

$$M = \{\mathbf{0}\} \oplus \cdots \oplus \{\mathbf{0}\} \oplus A\mathbf{u}_k \oplus \cdots \oplus A\mathbf{u}_n = A\mathbf{u}_k \oplus \cdots \oplus A\mathbf{u}_n$$

as required. If $M = \{\mathbf{0}\}$, we obtain an empty direct sum. □

Section 8.6 provides an algorithm for determining $\{C_1, \ldots, C_n\}$ and $d_1, \ldots, d_r$ as in the statement of Theorem 8.1.1, provided that we know a system of generators of N. In the application of Theorem 7.2.1, this means knowing a system of generators of $\ker(\psi)$ where ψ is given by (8.1). The following result allows us to find such a system of generators in the situation most interesting to us.

Proposition 8.1.2. *Let V be a vector space of finite dimension $n > 0$ over a field K, let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V and let $T\colon V \to V$ be a linear operator. For the corresponding structure of a $K[x]$-module on V, the function*

$$\begin{array}{rccc} \psi : & K[x]^n & \longrightarrow & V \\ & \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} & \longmapsto & p_1(x)\mathbf{v}_1 + \cdots + p_n(x)\mathbf{v}_n \end{array}$$

is a surjective homomorphism of $K[x]$-modules, and its kernel is the $K[x]$-submodule of $K[x]^n$ generated by the columns of the matrix $xI - [\,T\,]_{\mathcal{B}}$.

Proof. Write $[\,T\,]_{\mathcal{B}} = (a_{ij})$. Let N be the $K[x]$-submodule of $K[x]^n$ generated by the columns $C_1, \ldots, C_n$ of $xI - [\,T\,]_{\mathcal{B}}$. For $j = 1, \ldots, n$, we have

$$C_j = \begin{pmatrix} -a_{1,j} \\ \vdots \\ x - a_{jj} \\ \vdots \\ -a_{nj} \end{pmatrix},$$

hence

$$\begin{aligned}\psi(C_j) &= (-a_{1j})\mathbf{v}_1 + \cdots + (x - a_{jj})\mathbf{v}_j + \cdots + (-a_{nj})\mathbf{v}_n \\ &= T(\mathbf{v}_j) - (a_{1j}\mathbf{v}_1 + \cdots + a_{nj}\mathbf{v}_n) \\ &= \mathbf{0}\end{aligned}$$

and so $C_j \in \ker(\psi)$. This proves that $N \subseteq \ker(\psi)$.

To prove the reverse inclusion, we first show that every n-tuple $(p_1(x), \ldots, p_n(x))^t$ of $K[x]^n$ can be written as a sum of an element of N and an element of K^n.

We prove this assertion by induction on the maximum m of the degree of the polynomials $p_1(x), \ldots, p_n(x)$ where, for the purpose of this argument, we say that the zero polynomial has degree 0. If $m = 0$, then $(p_1(x), \ldots, p_n(x))^t$ is an element of K^n and we are done. Suppose that $m \geq 1$ and that the result is true for an n-tuple of polynomials of degrees $\leq m - 1$. Denoting by b_i the coefficient of x^m in $p_i(x)$, we have:

$$\begin{aligned}\begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} &= \begin{pmatrix} b_1x^m + (\text{terms of degree } \leq m-1) \\ \cdots\cdots \\ b_nx^m + (\text{terms of degree } \leq m-1) \end{pmatrix} \\ &= \underbrace{b_1x^{m-1}C_1 + \cdots + b_nx^{m-1}C_n}_{\in N} + \begin{pmatrix} p_1^*(x) \\ \vdots \\ p_n^*(x) \end{pmatrix}\end{aligned}$$

for polynomials $p^*(x), \ldots, p_n^*(x)$ in $K[x]$ of degree $\leq m-1$. Applying the induction hypothesis to the n-tuple $(p_1^*(x), \ldots, p_n^*(x))^t$, we conclude that $(p_1(x), \ldots, p_n(x))^t$ is the sum of an element of N and an element of K^n.

Let $(p_1(x), \ldots, p_n(x))^t$ be an arbitrary element of $\ker(\psi)$. By the above observation, we can write

$$\begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} = \begin{pmatrix} q_1(x) \\ \vdots \\ q_n(x) \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \tag{8.7}$$

where $(q_1(x), \ldots, q_n(x))^t \in N$ and $(c_1, \ldots, c_n)^t \in K^n$. Since $N \subseteq \ker(\psi)$, we see that

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} - \begin{pmatrix} q_1(x) \\ \vdots \\ q_n(x) \end{pmatrix} \in \ker(\psi),$$

and so, applying ψ to the vector $(c_1, \ldots, c_n)^t$, we get

$$c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \mathbf{0}.$$

Since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent over K, this implies that $c_1 = \cdots = c_n = 0$ and equality (8.7) gives

$$\begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} = \begin{pmatrix} q_1(x) \\ \vdots \\ q_n(x) \end{pmatrix} \in N.$$

Since the choice of $(p_1(x), \ldots, p_n(x))^t \in \ker(\psi)$ is arbitrary, this shows that $\ker(\psi) \subseteq N$, and so $\ker(\psi) = N$. $\square$

Example 8.1.3. Let V be a vector space of dimension 2 over $\mathbb{R}$, let $\mathcal{A} = \{\mathbf{v}_1, \mathbf{v}_2\}$ be a basis of V, and let $T \in \mathrm{End}_{\mathbb{R}}(V)$ with $[\,T\,]_{\mathcal{A}} = \begin{pmatrix} -1 & 2 \\ 4 & 1 \end{pmatrix}$. For the corresponding structure of an $\mathbb{R}[x]$-module over V, we consider the homomorphism of $\mathbb{R}[x]$-modules $\psi\colon \mathbb{R}[x]^2 \to V$ given by

$$\psi \begin{pmatrix} p_1(x) \\ p_2(x) \end{pmatrix} = p_1(x)\mathbf{v}_1 + p_2(x)\mathbf{v}_2.$$

(i) By Proposition 8.1.2, $\ker(\psi)$ is the submodule of $\mathbb{R}[x]^2$ generated by the columns of

$$xI - [\,T\,]_{\mathcal{A}} = \begin{pmatrix} x+1 & -2 \\ -4 & x-1 \end{pmatrix},$$

that is,

$$\ker(\psi) = \left\langle \begin{pmatrix} x+1 \\ -4 \end{pmatrix}, \begin{pmatrix} -2 \\ x-1 \end{pmatrix} \right\rangle_{\mathbb{R}[x]}.$$

(ii) We see that $(x^2 - 9)\mathbf{v}_1 = \mathbf{0}$ since

$$(x^2 - 9)\mathbf{v}_1 = T^2(\mathbf{v}_1) - 9\mathbf{v}_1 = T(-\mathbf{v}_1 + 4\mathbf{v}_2) - 9\mathbf{v}_1 = \mathbf{0}.$$

So we have $\begin{pmatrix} x^2 - 9 \\ 0 \end{pmatrix} \in \ker(\psi)$. To write this element of $\ker(\psi)$ as a linear combination of the generators of $\ker(\psi)$ found in (i), we proceed as in the proof of Proposition 8.1.2. We obtain

$$\begin{pmatrix} x^2 - 9 \\ 0 \end{pmatrix} = x \begin{pmatrix} x+1 \\ -4 \end{pmatrix} + 0 \begin{pmatrix} -2 \\ x-1 \end{pmatrix} + \begin{pmatrix} -x-9 \\ 4x \end{pmatrix}$$

and

$$\begin{pmatrix} -x-9 \\ 4x \end{pmatrix} = (-1) \begin{pmatrix} x+1 \\ -4 \end{pmatrix} + 4 \begin{pmatrix} -2 \\ x-1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

thus

$$\begin{pmatrix} x^2 - 9 \\ 0 \end{pmatrix} = (x-1) \begin{pmatrix} x+1 \\ -4 \end{pmatrix} + 4 \begin{pmatrix} -2 \\ x-1 \end{pmatrix}.$$

Exercises.

8.1.1. Let V be a vector space over $\mathbb{Q}$ equipped with a basis $\mathcal{A} = \{\mathbf{v}_1, \mathbf{v}_2\}$, and let $T \in \mathrm{End}_{\mathbb{Q}}(V)$ with $[\,T\,]_{\mathcal{A}} = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$. We consider V as a $\mathbb{Q}[x]$-module and we denote by N the kernel of the homomorphism of $\mathbb{Q}[x]$-modules $\psi\colon \mathbb{Q}[x]^2 \longrightarrow V$ given by

$$\psi \begin{pmatrix} p_1(x) \\ p_2(x) \end{pmatrix} = p_1(x) \cdot \mathbf{v}_1 + p_2(x) \cdot \mathbf{v}_2.$$

(i) Find a system of generators of N as a $\mathbb{Q}[x]$-module.

(ii) Show that $\begin{pmatrix} x^2 - 3 \\ -2x - 5 \end{pmatrix} \in N$ and express this column vector as a linear combination of the generators of N found in (i).

8.1.2. Let V be a vector space over $\mathbb{R}$ equipped with a basis $\mathcal{A} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ an let $T \in \mathrm{End}_{\mathbb{R}}(V)$ with $[\,T\,]_{\mathcal{A}} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$. We consider V as a $\mathbb{R}[x]$-module and we denote by N the kernel of the homomorphism of $\mathbb{R}[x]$-modules $\psi\colon \mathbb{R}[x]^3 \longrightarrow V$ given by

$$\psi \begin{pmatrix} p_1(x) \\ p_2(x) \\ p_3(x) \end{pmatrix} = p_1(x) \cdot \mathbf{v}_1 + p_2(x) \cdot \mathbf{v}_2 + p_3(x) \cdot \mathbf{v}_3.$$

(i) Find a system of generators of N as a $\mathbb{R}[x]$-module.

(ii) Show that $\begin{pmatrix} x^2 - x - 6 \\ x - 1 \\ x^2 - 2x + 1 \end{pmatrix} \in N$ and express this column vector as a linear combination of the generators of N found in (i).

8.2 The Cayley-Hamilton Theorem

We begin with the following observation:

Proposition 8.2.1. *Let N be the A-submodule of A^n generated by the columns of a matrix $U \in \mathrm{Mat}_{n\times n}(A)$. Then N contains $\det(U)A^n$.*

Proof. We know that the adjugate $\mathrm{Adj}(U)$ of U is a matrix of $\mathrm{Mat}_{n\times n}(A)$ satisfying

$$U\mathrm{Adj}(U) = \det(U)I \tag{8.8}$$

(see Theorem B.3.4). Denote by $C_1, \dots, C_n$ the columns of U and by $\mathbf{e}_1, \dots, \mathbf{e}_n$ those of I (these are the elements of the standard basis of A^n). Also write $\mathrm{Adj}(U) = (a_{ij})$. Comparing the j-th columns of the matrices on each side of (8.8), we see that

$$a_{1j}C_1 + \cdots + a_{nj}C_n = \det(U)\mathbf{e}_j \quad (1 \le j \le n).$$

Since $N = \langle C_1, \dots, C_n\rangle_A$, we deduce that

$$\det(U)A^n = \langle \det(U)\mathbf{e}_1, \dots, \det(U)\mathbf{e}_n\rangle_A \subseteq N.$$

□

We can now prove the following fundamental result:

Theorem 8.2.2 (Cayley-Hamilton Theorem)**.** *Let V be a finite-dimensional vector space over a field K and let $T\colon V \to V$ be a linear operator on V. Then we have*

$$\mathrm{char}_T(T) = 0.$$

Proof. Let $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V over K. By Proposition 8.1.2, the kernel of the homomorphism of $K[x]$-modules

$$\begin{array}{rccl} \psi : & K[x]^n & \longrightarrow & V \\ & \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} & \longmapsto & p_1(x)\mathbf{v}_1 + \cdots + p_n(x)\mathbf{v}_n \end{array}$$

is the submodule of $K[x]^n$ generated by the columns of $xI - [\,T\,]_{\mathcal{B}} \in \mathrm{Mat}_{n\times n}(K[x])$. By the proceeding proposition (applied to $A = K[x]$), this implies that

$$\ker(\psi) \supseteq \det(xI - [\,T\,]_{\mathcal{B}}) \cdot K[x]^n = \mathrm{char}_T(x) \cdot K[x]^n.$$

In particular, for all $\mathbf{u} \in K[x]^n$, we have $\mathrm{char}_T(x)\mathbf{u} \in \ker(\psi)$ and so

$$\mathbf{0} = \psi(\mathrm{char}_T(x)\,\mathbf{u}) = \mathrm{char}_T(x)\,\psi(\mathbf{u}).$$

Since ψ is a surjective homomorphism, this implies that $\mathrm{char}_T(x) \in \mathrm{Ann}(V)$, that is, $\mathrm{char}_T(T) = 0$. □

The following consequence is left as an exercise.

Corollary 8.2.3. *For every matrix $M \in \mathrm{Mat}_{n\times n}(K)$, we have* $\mathrm{char}_M(M) = 0$.

Example 8.2.4. For $n = 2$, we can give a direct proof. Write $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We see that

$$\mathrm{char}_T(x) = \begin{vmatrix} x-a & -b \\ -c & x-d \end{vmatrix} = x^2 - (a+d)x + (ad-bc)$$

thus

$$\begin{aligned} \mathrm{char}_M(M) &= M^2 - (a+d)M + (ad-bc)I \\ &= \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Exercises.

8.2.1. Prove Corollary 8.2.3.

8.2.2. Let V be a finite-dimensional vector space over a field K and let $T\colon V \to V$ be a linear operator on V.

(i) Show that $\min_T(x)$ divides $\mathrm{char}_T(x)$.

(ii) If $K = \mathbb{Q}$ and $\mathrm{char}_T(x) = x^3 - 2x^2 + x$, what are the possibilities for $\min_T(x)$?

8.2.3 (Alternate proof of the Cayley-Hamilton Theorem). Let V be a vector space of finite dimension n over a field K and let $T\colon V \to V$ be a linear operator on V. The goal of this exercise is to give another proof of the Cayley-Hamilton Theorem. To do this, we equip V with the corresponding structure of a $K[x]$-module, and we choose an arbitrary element $\mathbf{v}$ of V. Let $p(x)$ be the monic generator of $\mathrm{Ann}(\mathbf{v})$, and let m be its degree.

(i) Show that there exists a basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}} = \left(\begin{array}{c|c} P & Q \\ \hline 0 & R \end{array}\right)$ where P denotes the companion matrix of $p(x)$ and where R is a square matrix of size $(n-m)\times(n-m)$.

(ii) Show that $\mathrm{char}_T(x) = p(x)\mathrm{char}_R(x) \in \mathrm{Ann}(\mathbf{v})$.

(iii) Why can we conclude that $\mathrm{char}_T(T) = 0$?

8.3 Submodules of free modules, Part II

The goal of this section is to prove the following weaker version of Theorem 8.1.1 as a first step towards the proof of this theorem.

Theorem 8.3.1. *Every A-submodule of A^n is free and possesses a basis with at most n elements.*

This result is false in general for an arbitrary commutative ring A (see Exercise 8.3.1).

Proof. We proceed by induction on n. For $n = 1$, an A-submodule N of $A^1 = A$ is simply an ideal of A. If $N = \{\mathbf{0}\}$, then by convention N is free and admits the basis $\varnothing$. Otherwise, we know that $N = (b) = A\,b$ for a nonzero element b of A since every ideal of A is principal (Theorem 5.4.3). We note that if $ab = 0$ with $a \in A$ then $a = 0$ since A is an integral domain. Therefore, in this case, $\{b\}$ is a basis of N.

Now suppose that $n \geq 2$ and that every A-submodule of A^{n-1} admits a basis with at most $n-1$ elements. Let N be an A-submodule of A^n. We define

$$I = \left\{ a \in A\,;\ \begin{pmatrix} a \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in N \text{ for some } a_2, \ldots, a_n \in A \right\},$$

$$N' = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in N\,;\ a_1 = 0 \right\} \quad \text{and} \quad N'' = \left\{ \begin{pmatrix} a_2 \\ \vdots \\ a_n \end{pmatrix} \in A^{n-1}\,;\ \begin{pmatrix} 0 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in N \right\}.$$

It is straightforward (exercise) to verify that I is an ideal of A, that N' is a submodule of N and that N'' is a submodule of A^{n-1}. Moreover, the function

$$\begin{array}{rccc} \varphi : & N'' & \longrightarrow & N' \\ & \begin{pmatrix} a_2 \\ \vdots \\ a_n \end{pmatrix} & \longmapsto & \begin{pmatrix} 0 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \end{array}$$

is an isomorphism of A-modules. By the induction hypothesis, N'' admits a basis with at most $n-1$ elements. The image of this basis under φ is therefore a basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ of N' with $0 \leq m \leq n-1$ (Proposition 6.5.13).

If $I = \{\mathbf{0}\}$, then we have $N = N'$. In this case, $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ is a basis of N and, since $0 \leq m \leq n$, we are finished.

Otherwise, Theorem 5.4.3 implies $I = (b_1) = Ab_1$ for a nonzero element b_1 of A. Since $b_1 \in I$, there exists $b_2, \ldots, b_n \in A$ such that

$$\mathbf{u}_{m+1} := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in N.$$

We will show that $N = N' \oplus A\mathbf{u}_{m+1}$. Assuming this result, we have that $\{\mathbf{u}_1, \ldots, \mathbf{u}_{m+1}\}$ is a basis of N and, since $m + 1 \leq n$, the induction step is complete.

Let $\mathbf{u} = (c_1, \ldots, c_n)^t \in N$. By the definition of I, we have $c_1 \in I$. Thus there exists $a \in A$ such that $c_1 = a\, b_1$. We see that

$$\mathbf{u} - a\mathbf{u}_{m+1} = \begin{pmatrix} 0 \\ c_2 - a\, b_2 \\ \vdots \\ c_n - a\, b_n \end{pmatrix} \in N',$$

and so

$$\mathbf{u} = (\mathbf{u} - a\mathbf{u}_{m+1}) + a\mathbf{u}_{m+1} \in N' + A\mathbf{u}_{m+1}.$$

Since the choice of $\mathbf{u}$ is arbitrary, this shows that

$$N = N' + A\mathbf{u}_{m+1}.$$

We also note that, for $a \in A$,

$$a\mathbf{u}_{m+1} \in N' \quad \Longleftrightarrow \quad a\, b_1 = 0 \quad \Longleftrightarrow \quad a = 0.$$

This shows that

$$N' \cap A\mathbf{u}_{m+1} = \{\mathbf{0}\},$$

hence $N = N' \oplus A\mathbf{u}_{m+1}$ as claimed. □

Example 8.3.2. Let $N = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} ;\, 2x + 3y + 6z = 0 \right\}$.

(i) Show that N is a $\mathbb{Z}$-submodule of $\mathbb{Z}^3$.

(ii) Find a basis of N as a $\mathbb{Z}$-module.

Solution: For (i), it suffices to show that N is a subgroup of $\mathbb{Z}^3$. We leave this as an exercise. For (ii), we set

$$I = \{x \in \mathbb{Z}\,;\, 2x + 3y + 6z = 0 \text{ for some } y, z \in \mathbb{Z}\},$$

$$N' = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in N\,;\, x = 0 \right\} \quad \text{and} \quad N'' = \left\{ \begin{pmatrix} y \\ z \end{pmatrix} \in \mathbb{Z}^2\,;\, 3y + 6z = 0 \right\},$$

as in the proof of Theorem 8.3.1. We see that

$$3y + 6z = 0 \quad \Longleftrightarrow \quad y = -2z,$$

hence

$$N'' = \left\{ \begin{pmatrix} -2z \\ z \end{pmatrix} ; z \in \mathbb{Z} \right\} = \mathbb{Z} \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

admits the basis $\left\{ \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\}$ and so $\left\{ \mathbf{u}_1 := \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix} \right\}$ is a basis of N'. We also see that, for $x \in \mathbb{Z}$, we have

$$\begin{aligned} x \in I \quad &\Longleftrightarrow \quad 2x = -3y - 6z \quad \text{for some } y, z \in \mathbb{Z} \\ &\Longleftrightarrow \quad 2x \in (-3, -6) = (3) \\ &\Longleftrightarrow \quad 3 \mid 2x \\ &\Longleftrightarrow \quad 3 \mid x. \end{aligned}$$

Thus $I = (3)$. Furthermore, 3 is the first component of

$$\mathbf{u}_2 = \begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix} \in N.$$

Repeating the arguments of the proof of Theorem 8.3.1, we see that

$$N = N' \oplus \mathbb{Z}\mathbf{u}_2 = \mathbb{Z}\mathbf{u}_1 \oplus \mathbb{Z}\mathbf{u}_2.$$

Thus $\left\{ \mathbf{u}_1 = \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}, \mathbf{u}_2 = \begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix} \right\}$ is a basis of N.

Exercises.

8.3.1. Let A be an arbitrary integral domain and let I be an ideal of A considered as an A-submodule of $A^1 = A$. Show that I is a free A-module if and only I is principal.

8.3.2. Let M be a free module over a euclidean domain A. Show that every A-submodule of M is free.

8.3.3. Let $N = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{Z}^3 ; 3x + 10y - 16z = 0 \right\}$.

(i) Show that N is a submodule of $\mathbb{Z}^3$.

(ii) Find a basis of N as a $\mathbb{Z}$-module.

8.3.4. Let $N = \left\{ \begin{pmatrix} p_1(x) \\ p_2(x) \\ p_3(x) \end{pmatrix} \in \mathbb{Q}[x]^3 \,;\, (x^2 - x)p_1(x) + x^2 p_2(x) - (x^2 + x)p_3(x) = 0 \right\}$.

(i) Show that N is a $\mathbb{Q}[x]$-submodule of $\mathbb{Q}[x]^3$.

(ii) Find a basis of N as a $\mathbb{Q}[x]$-module.

8.4 The column module of a matrix

Definition 8.4.1 (Column module). We define the *column module* of a matrix $U \in \mathrm{Mat}_{n\times m}(A)$ to be the A-submodule of A^n generated by the columns of A. We denote it by $\mathrm{Col}_A(U)$.

Theorem 8.3.1 shows that every submodule of A^n has a basis with at most n elements. Thus the column module of a matrix $U \in \mathrm{Mat}_{n\times m}(A)$ has a basis. The goal of this section is to give an algorithm for finding such a basis. More generally, this algorithm permits us to find a basis of an arbitrary submodule N of A^n provided that we know a system of generators $C_1, \ldots, C_m$ of N since N is then the column module of the matrix $(C_1 \cdots C_m) \in \mathrm{Mat}_{n\times m}(A)$ whose columns are $C_1, \ldots, C_m$.

We begin with the following observation:

Lemma 8.4.2. *Let $U \in \mathrm{Mat}_{n\times m}(A)$ and let U' be a matrix obtained from U by applying one of the following operations:*

(I) interchange two columns,

(II) add to one column the product of another column and an element of A,

(III) multiply a column by an element of $A^\times$.

Then U and U' have the same column module.

Proof. By construction, the columns of U' belong to $\mathrm{Col}_A(U)$ since they are linear combinations of the columns of U. Thus we have $\mathrm{Col}_A(U') \subseteq \mathrm{Col}_A(U)$. On the other hand, each of the operations of type (I), (III) or (III) is invertible: we can recover U from U' by applying an operation of the same type. Thus we also have $\mathrm{Col}_A(U) \subseteq \mathrm{Col}_A(U')$, and so $\mathrm{Col}_A(U) = \mathrm{Col}_A(U')$. □

The operations (I), (II), (III) of Lemma 8.4.2 are called *elementary column operations* (on A). From this lemma we deduce:

Lemma 8.4.3. *Let $U \in \mathrm{Mat}_{n\times m}(A)$ and let U' be a matrix obtained from U by applying a series of elementary column operation. Then $\mathrm{Col}_A(U) = \mathrm{Col}_A(U')$.*

Definition 8.4.4 (Echelon form). We say that a matrix $U \in \mathrm{Mat}_{n\times m}(A)$ is in *echelon form* if it is in the form

$$U = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \vdots & & & \vdots & \vdots & & \vdots \\ u_{i_1,1} & \vdots & \cdots & \cdots & \vdots & \vdots & & \vdots \\ * & 0 & & & \vdots & \vdots & & \vdots \\ \vdots & u_{i_2,2} & & & \vdots & \vdots & & \vdots \\ \vdots & * & & & 0 & \vdots & & \vdots \\ \vdots & \vdots & & & u_{i_r,r} & \vdots & & \vdots \\ \vdots & \vdots & & & * & \vdots & & \vdots \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ * & * & \cdots & \cdots & * & 0 & & 0 \end{pmatrix} \tag{8.9}$$

with $1 \le i_1 < i_2 < \cdots < i_r \le n$ and $u_{i_1,1} \neq 0, \ldots, u_{i_r,r} \neq 0$.

Lemma 8.4.5. *Suppose that $U \in \mathrm{Mat}_{n\times m}(A)$ is in echelon form. Then the nonzero columns of U form a basis of $\mathrm{Col}_A(U)$.*

Proof. Suppose that U is given by (8.9). Then the first r columns $C_1, \ldots, C_r$ of U generate $\mathrm{Col}_A(U)$. Suppose that we have

$$a_1C_1 + \cdots + a_rC_r = \mathbf{0}$$

for elements $a_1, \ldots, a_r$ of A. If $a_1, \ldots, a_r$ are not nonzero, there exists a smallest integer k such that $a_k \neq 0$. Then we have

$$a_kC_k + \cdots + a_rC_r = \mathbf{0}.$$

Taking the i_k-th component of each side of this equality, we see that

$$a_k u_{i_k,k} = 0.$$

Since $a_k \neq 0$ and $u_{i_k,k} \neq 0$, this is impossible (since A is an integral domain). This contradiction shows that we must have $a_1 = \cdots = a_r = 0$. Thus the columns $C_1, \ldots, C_r$ are linearly independent and so they form a basis of $\mathrm{Col}_A(U)$. □

The three preceding lemmas only use the fact that A is an integral domain. The following result uses in a crucial way the hypothesis that A is a euclidean domain.

Theorem 8.4.6. *Let $U \in \mathrm{Mat}_{n\times m}(A)$. It is possible to bring U to echelon form by a series of elementary column operations.*

Proof. Let $\varphi\colon A \setminus \{0\} \to \mathbb{N}$ be a euclidean function for A (see Definition 5.4.1). We consider the following algorithm:

Algorithm 8.4.7.

1. *If $U = 0$, the matrix U is already in echelon form and we are finished.*

2. *Suppose that $U \neq 0$. We locate the first nonzero row of U.*

$$\begin{pmatrix} & 0 & \\ \boxed{\quad \neq 0 \quad} \\ & * & \end{pmatrix} \leftarrow$$

2.1. *In this row we choose an element $a \neq 0$ for which $\varphi(a)$ is minimal and we permute the columns to bring this element to the first column.*

$$\left(\begin{array}{cccc} & 0 & & \\ \hline a \neq 0 & a_2 & \cdots & a_m \\ & * & & \end{array}\right)$$

2.2. *We divide each of the other elements $a_2, \dots, a_m$ of this row by a by writing*

$$a_j = q_j a + r_j$$

with $q_j, r_j \in A$ satisfying $r_j = 0$ or $\varphi(r_j) < \varphi(a)$, then, for $j = 2, \dots, m$, we subtract from the j-th column the product of the first column and q_j.

$$\begin{array}{c} \begin{array}{ccc} C_2 - q_2 C_1 & \cdots & C_m - q_m C_1 \\ \downarrow & & \downarrow \end{array} \\ \left(\begin{array}{cccc} & 0 & & \\ \hline a & r_2 & \cdots & r_m \\ & * & & \end{array}\right) \end{array}$$

2.3. *If $r_2, \dots, r_m$ are not all zero, we return to step 2.1.*

If they are all zero, the new matrix is in the form pictured to the right and we return to step 1, restricting ourselves to the submatrix formed by the last $m-1$ columns, that is, ignoring the first column.

$$\left(\begin{array}{c|cccc} 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \\ \hline a & 0 & \cdots & \cdots & 0 \\ * & & * & & \end{array}\right)$$

This algorithm terminates after a finite number of steps since each iteration of steps 2.1 to 2.3 on a row replaces the first element $a \neq 0$ of this row by an element $a' \neq 0$ of A with $\varphi(a') < \varphi(a)$, and this cannot be repeated indefinitely since φ takes values in $\mathbb{N} = \{0, 1, 2, \dots\}$. When completed, this algorithm produces a matrix in echelon form as required. □

Combining this theorem with the preceding lemmas, we conclude:

Corollary 8.4.8. *Let $U \in \mathrm{Mat}_{n\times m}(A)$. By a series of elementary column operations, we can transform U to a echelon matrix U'. Then the nonzero columns of U' form a basis of $\mathrm{Col}_A(U)$.*

Proof. The first assertion follows from Theorem 8.4.6. By Lemma 8.4.3, we have $\mathrm{Col}_A(U) = \mathrm{Col}_A(U')$. Finally, Lemma 8.4.5 shows that the nonzero columns of U' form a basis of $\mathrm{Col}_A(U')$, hence these also form a basis of $\mathrm{Col}_A(U)$. □

Example 8.4.9. Find a basis of $\mathrm{Col}_{\mathbb{Z}}(U)$ where $U = \begin{pmatrix} 3 & 7 & 4 \\ -4 & -2 & 2 \\ 1 & -5 & -6 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{Z})$.

Solution: We have

$$U \sim \begin{array}{c} \begin{array}{ccc} & C_2 - 2C_1 & C_3 - C_1 \end{array} \\ \begin{pmatrix} 3 & 1 & 1 \\ -4 & 6 & 6 \\ 1 & -7 & -7 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{array}{ccc} C_2 & C_1 & \end{array} \\ \begin{pmatrix} 1 & 3 & 1 \\ 6 & -4 & 6 \\ -7 & 1 & -7 \end{pmatrix} \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & C_2 - 3C_1 & C_3 - C_1 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 6 & -22 & 0 \\ -7 & 22 & 0 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{array}{ccc} & -C_2 & \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 6 & 22 & 0 \\ -7 & -22 & 0 \end{pmatrix} \end{array}.$$

Thus $\left\{ \begin{pmatrix} 1 \\ 6 \\ -7 \end{pmatrix}, \begin{pmatrix} 0 \\ 22 \\ -22 \end{pmatrix} \right\}$ is a basis of $\mathrm{Col}_{\mathbb{Z}}(U)$.

Example 8.4.10. Find a basis of

$$N := \left\langle \begin{pmatrix} x^2 - 1 \\ x + 1 \end{pmatrix}, \begin{pmatrix} x^2 - x \\ x \end{pmatrix}, \begin{pmatrix} x^3 - 7 \\ x - 1 \end{pmatrix} \right\rangle_{\mathbb{Q}[x]} \subseteq \mathbb{Q}[x]^2.$$

Solution: We have $N = \mathrm{Col}_{\mathbb{Q}[x]}(U)$ where

$$U = \begin{pmatrix} x^2 - 1 & x^2 - x & x^3 - 7 \\ x + 1 & x & x - 1 \end{pmatrix} \sim \begin{array}{c} \begin{array}{ccc} & C_2 - C_1 & C_3 - xC_1 \end{array} \\ \begin{pmatrix} x^2 - 1 & -x + 1 & x - 7 \\ x + 1 & -1 & -x^2 - 1 \end{pmatrix} \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} C_2 & C_1 & \end{array} \\ \begin{pmatrix} -x + 1 & x^2 - 1 & x - 7 \\ -1 & x + 1 & -x^2 - 1 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{array}{ccc} & -C_1 & \end{array} \\ \begin{pmatrix} x - 1 & x^2 - 1 & x - 7 \\ 1 & x + 1 & -x^2 - 1 \end{pmatrix} \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & C_2 - (x+1)C_1 & C_3 - C_1 \end{array} \\ \begin{pmatrix} x - 1 & 0 & -6 \\ 1 & 0 & -x^2 - 2 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{array}{ccc} -C_3 & C_1 & C_2 \end{array} \\ \begin{pmatrix} 6 & x - 1 & 0 \\ x^2 + 2 & 1 & 0 \end{pmatrix} \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & 6C_2 & \end{array} \\ \begin{pmatrix} 6 & 6(x-1) & 0 \\ x^2 + 2 & 6 & 0 \end{pmatrix} \end{array} \quad \text{since } 6 \in \mathbb{Q}[x]^\times = \mathbb{Q}^\times,$$

$$\sim \begin{array}{c} \begin{array}{ccc} & C_2 - (x-1)C_1 & \end{array} \\ \begin{pmatrix} 6 & 0 & 0 \\ x^2 + 2 & -x^3 + x^2 - 2x + 8 & 0 \end{pmatrix} \end{array}$$

Thus $\left\{ \begin{pmatrix} 6 \\ x^2+2 \end{pmatrix}, \begin{pmatrix} 0 \\ -x^3+x^2-2x+8 \end{pmatrix} \right\}$ is a basis of N over $\mathbb{Q}[x]$.

Exercises.

8.4.1. Find a basis of the subgroup of $\mathbb{Z}^3$ generated by $\begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}$.

8.4.2. Find a basis of the $\mathbb{R}[x]$-submodule of $\mathbb{R}[x]^2$ generated by the pairs $\begin{pmatrix} x^2-1 \\ x \end{pmatrix}$, $\begin{pmatrix} x^2-2x+1 \\ x-2 \end{pmatrix}$ and $\begin{pmatrix} x^3-1 \\ x^2-1 \end{pmatrix}$.

8.4.3. Let A be a euclidean domain, and let $U \in \mathrm{Mat}_{n\times m}(A)$. Show that the ideal I of A generated by the elements of the first row of U is not affected by the elementary column operations. Deduce that if a series of elementary column operations transforms U into a matrix whose first row is $(a, 0, \ldots, 0)$, then a is a generator of I.

8.5 Smith normal form

To define the notion of elementary row operation on a matrix, we replace everywhere the word "column" by "row" in statements (I) to (III) of Lemma 8.4.2:

Definition 8.5.1 (Elementary row operation). An *elementary row operation* on a matrix of $\mathrm{Mat}_{n\times m}(A)$ is any operation of one of the following types:

(I) interchange two rows,

(II) add to one row the product of another row and an element of A,

(III) multiply a row by an element of $A^\times$.

To study the effect of an elementary row operation on the column module of a matrix, we will use the following proof whose proof is left as an exercise (see Exercise 6.5.4).

Lemma 8.5.2. *Let $\varphi\colon M \to M'$ be a homomorphism of A-modules and let N be an A-submodule of M. Then*

$$\varphi(N) := \{\varphi(\mathbf{u})\,;\, \mathbf{u} \in M\}$$

is an A-submodule of M'. Furthermore:

(i) if $N = \langle \mathbf{u}_1, \dots, \mathbf{u}_m \rangle_A$, then $\varphi(N) = \langle \varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_m) \rangle_A$;

(ii) if N admits a basis $\{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ and φ is injective, then $\{\varphi(\mathbf{u}_1), \dots, \varphi(\mathbf{u}_m)\}$ is a basis of $\varphi(N)$.

We can now prove:

Lemma 8.5.3. *Let $U \in \mathrm{Mat}_{n\times m}(A)$ and let U' be a matrix obtained from U by applying an elementary row operation. Then there exists an automorphism φ of A^n such that*

$$\mathrm{Col}_A(U') = \varphi(\mathrm{Col}_A(U)).$$

Recall that an *automorphism* of an A-module is an isomorphism from this module to itself.

Proof. Let $C_1, \dots, C_m$ be the columns of U and let $C'_1, \dots, C'_m$ be those of U'. We split the proof into three cases.

If U' is obtained from U by applying an operation of type (I), we will simply assume that we have interchanged rows 1 and 2. The general case is similar but more complicated to write. In this case, the function $\varphi\colon A^n \to A^n$ given by

$$\varphi \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} u_2 \\ u_1 \\ u_3 \\ \vdots \\ u_n \end{pmatrix}$$

is an automorphism of A^n such that $\varphi(C_j) = C'_j$ for $j = 1, \dots, m$. Since $\mathrm{Col}_A(U) = \langle C_1, \dots, C_m \rangle_A$ and $\mathrm{Col}_A(U') = \langle C'_1, \dots, C'_m \rangle_A$, Lemma 8.5.2 then gives $\mathrm{Col}_A(U') = \varphi(\mathrm{Col}_A(U'))$.

If U' is obtained by an operation of type (II), we will suppose that we have added to row 1 the product of row 2 and an element a of A. Then we have $C'_j = \varphi(C_j)$ for $j = 1, \dots, m$ where $\varphi\colon A^n \to A^n$ is the function given by

$$\varphi \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} u_1 + a\, u_2 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}.$$

We verify that φ is an automorphism of A^n and the conclusion then follows from Lemma 8.5.2.

Finally, if U' is obtained by an operation of type (III), we will suppose that we have multiplied row 1 of U a unit $a \in A^\times$. Then $C'_j = \varphi(C_j)$ for $j = 1, \dots, m$ where $\varphi\colon A^n \to A^n$ is the automorphism of A^n given by

$$\varphi \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} a\, u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix},$$

and Lemma 8.5.2 gives $\mathrm{Col}_A(U') = \varphi(\mathrm{Col}_A(U))$. □

Combining Lemma 8.4.2 and 8.5.3, we get:

Theorem 8.5.4. *Let $U \in \mathrm{Mat}_{n\times m}(A)$ and let U' be a matrix obtained from U by applying a series of elementary row and column operations. Then there exists an automorphism $\varphi\colon A^n \to A^n$ such that*

$$\mathrm{Col}_A(U') = \varphi(\mathrm{Col}_A(U)).$$

Proof. By assumption, there exists a series of matrices

$$U_1 = U,\ U_2,\ U_3,\ \dots,\ U_k = U'$$

such that, for $i = 1, \dots, k-1$, the matrix U_{i+1} is obtained by applying to U_i an elementary row or column operation. In the case of a row operation, Lemma 8.5.3 gives

$$\mathrm{Col}_A(U_{i+1}) = \varphi_i(\mathrm{Col}_A(U_i))$$

for an automorphism φ_i of A^n. In the case of a column operation, Lemma 8.4.2 gives

$$\mathrm{Col}_A(U_{i+1}) = \mathrm{Col}_A(U_i) = \varphi_i(\mathrm{Col}_A(U_i))$$

where $\varphi_i = I_{A^n}$ is the identity function on A^n. We deduce that

$$\mathrm{Col}_A(U') = \mathrm{Col}_A(U_k) = \varphi_{k-1}(\dots\varphi_2(\varphi_1(\mathrm{Col}_A(U_1)))\dots) = \varphi(\mathrm{Col}_A(U))$$

where $\varphi = \varphi_{k-1} \circ \dots \circ \varphi_2 \circ \varphi_1$ is an automorphism of A^n. □

Theorem 8.5.4 is valid over an arbitrary commutative ring A. Using the assumption that A is euclidean, we show:

Theorem 8.5.5. *Let $U \in \mathrm{Mat}_{n\times m}(A)$. Applying to U a series of elementary row and column operations, we can bring it to the form*

$$\left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \tag{8.10}$$

for an integer $r \geq 0$ and nonzero elements $d_1, \dots, d_r$ of A with $d_1 \mid d_2 \mid \dots \mid d_r$.

We say that (8.10) is the *Smith normal form* of U. We can show that the elements $d_1, \dots, d_r$ are uniquely determined by U up to multiplication by a unit of A (see Exercise 8.5.4). We call them the *invariant factors* of U. The connection to the invariant factors mentioned after Theorem 7.2.5 is that the invariant factors there are the invariant factors (in the sense of Smith normal form) of the matrix $xI - A$, where A is the matrix associated to T in some basis.

Proof. If $U = 0$, the matrix U is already in Smith normal form with $r = 0$. We therefore suppose that $U \neq 0$. Then it suffices to show that U can be transformed into a matrix of type

$$\left(\begin{array}{c|ccc} d & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & U^* & \\ 0 & & & \end{array}\right) \tag{8.11}$$

where d is a nonzero element of A that divides all the coefficients of U^*.

Since $U \neq 0$, there exists a nonzero element a of U for which $\varphi(a)$ is minimal. By permuting the row and columns of U, we can bring this element to position (1,1):

$$\begin{pmatrix} & \vdots & \\ \cdots & a & \cdots \\ & \vdots & \end{pmatrix} \sim \begin{pmatrix} \cdots & a & \cdots \\ & \vdots & \\ & \vdots & \end{pmatrix} \sim \begin{pmatrix} a & \cdots & \cdots \\ \vdots & & \\ \vdots & & \end{pmatrix}$$

Step 1. Let $a_2, \ldots, a_m$ be the other elements of the first row. For $j = 2, \ldots, m$, we write $a_j = q_j a + r_j$ with $q_j, r_j \in A$ satisfying $r_j = 0$ or $\varphi(r_j) < \varphi(a)$, and then we subtract from column j the product of column 1 and q_j. This gives

$$\begin{array}{c} \begin{array}{cccc} & C_2 - q_2 C_1 & & C_m - q_m C_1 \end{array} \\ \left(\begin{array}{c|ccc} a & r_2 & \cdots & r_m \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right) \end{array}$$

If $r_1 = \cdots = r_m = 0$ (this happens when a divides all the elements of the first row), this matrix is of the form

$$\left(\begin{array}{c|ccc} a & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right).$$

Otherwise, we chose an index j with $r_j \neq 0$ for which $\varphi(r_j)$ is minimal and we interchange columns 1 and j to bring this element r_j to position $(1, 1)$. This gives a matrix of the form

$$\left(\begin{array}{c|ccc} a' & * & \cdots & * \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right)$$

with $a' \neq 0$ and $\varphi(a') < \varphi(a)$. We then repeat the procedure. Since every series of nonzero elements $a, a', a'', \ldots$ of A with $\varphi(a) > \varphi(a') > \varphi(a'') > \cdots$ cannot continue indefinitely, we

obtain, after a finite number of iterations, a matrix of the form

$$\left(\begin{array}{c|ccc} b & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right) \tag{8.12}$$

with $b \neq 0$ and $\varphi(b) \leq \varphi(a)$. Furthermore, we have $\varphi(b) < \varphi(a)$ if at the start a does not divide all the elements of row 1.

Step 2. Let $b_2, \ldots, b_m$ be the other elements of the first column of the matrix (8.12). For $i = 2, \ldots, n$, we write $b_i = q_i' b + r_i'$ with $q_i', r_i' \in A$ satisfying $r_i' = 0$ or $\varphi(r_i') < \varphi(b)$, and then we subtract from row i row 1 multiplied by q_i'. This gives

$$\left(\begin{array}{c|ccc} b & 0 & \cdots & 0 \\ \hline r_2' & & & \\ \vdots & & * & \\ r_n' & & & \end{array}\right) \begin{array}{c} R_2 - q_2' R_1 \\ \vdots \\ R_n - q_n' R_1 \end{array}$$

If $r_2' = \cdots = r_n' = 0$ (this happens when b divides all the elements of the first column), this matrix is of the form

$$\left(\begin{array}{c|ccc} b & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right).$$

Otherwise we choose an index i with $r_i' \neq 0$ for which $\varphi(r_i')$ is minimal and then with interchange rows 1 and i to bring this element r_i' to position $(1, 1)$. This gives a matrix of the form

$$\left(\begin{array}{c|ccc} b' & * & \cdots & * \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right)$$

with $b' \neq 0$ and $\varphi(b') < \varphi(b)$. We then return to step 1. Since every series of nonzero elements $b, b', b'', \ldots$ of A with $\varphi(b) > \varphi(b') > \varphi(b'') > \cdots$ is necessarily finite, we obtain, after a finite number of steps, a matrix of the form

$$\left(\begin{array}{c|ccc} c & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & U' & \\ 0 & & & \end{array}\right) \tag{8.13}$$

with $c \neq 0$ and $\varphi(c) \leq \varphi(a)$. Moreover, we have $\varphi(c) < \varphi(a)$ if initially a does not divide all the elements of the first row and first column.

Step 3. If c divides all the entries of the submatrix U' of (8.13) we have finished. Otherwise, we add to row 1 a row that contains an element of U' that is not divisible by c. We then return to step 1 with the resulting matrix

$$\left(\begin{array}{c|ccc} c & c_2 & \cdots & c_m \\ \hline 0 & & & \\ \vdots & & U' & \\ 0 & & & \end{array}\right) \quad R_1 + R_i \quad \text{where} \quad c \nmid R_i.$$

Since c does not divides all the entries of row 1 and column 1, this produces a new matrix

$$\left(\begin{array}{c|ccc} c' & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & U'' & \\ 0 & & & \end{array}\right)$$

with $c' \neq 0$ and $\varphi(c') < \varphi(c)$. Since every series of nonzero elements $c, c', c'', \ldots$ of A with $\varphi(c) > \varphi(c') > \varphi(c'') > \cdots$ is necessarily finite, we obtain, after a finite number of iterations, a matrix of the required form (8.10) where $d \neq 0$ divides all the entries of U^* $\square$

Example 8.5.6. Find the Smith normal form of $U = \begin{pmatrix} 4 & 8 & 4 \\ 4 & 10 & 8 \end{pmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$.

Solution: The calculation gives:

$$U \sim \begin{array}{c} \begin{array}{ccc} & C_2 - 2C_1 & C_3 - C_1 \end{array} \\ \begin{pmatrix} 4 & 0 & 0 \\ 4 & 2 & 4 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 2 & 4 \end{pmatrix} \\ \uparrow \\ \text{not divisible} \\ \text{by } 4 \end{array} R_2 - R_1 \sim \begin{pmatrix} 4 & 2 & 4 \\ 0 & 2 & 4 \end{pmatrix} R_1 + R_2$$

$$\sim \begin{array}{c} \begin{array}{ccc} C_2 & C_1 & \end{array} \\ \begin{pmatrix} 2 & 4 & 4 \\ 2 & 0 & 4 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{array}{ccc} & C_2 - 2C_1 & C_3 - 2C_1 \end{array} \\ \begin{pmatrix} 2 & 0 & 0 \\ 2 & -4 & 0 \end{pmatrix} \end{array} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & -4 & 0 \end{pmatrix} R_2 - R_1$$

$$\sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} -R_2$$

Example 8.5.7. Find the invariant factors of

$$U = \begin{pmatrix} x & 1 & 1 \\ 3 & x-2 & -3 \\ -4 & 4 & x+5 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{Q}[x]).$$

Solution: We have

$$U \sim \begin{array}{c} \begin{array}{ccc} C_2 & C_1 & \\ \end{array} \\ \begin{pmatrix} 1 & x & 1 \\ x-2 & 3 & -3 \\ 4 & -4 & x+5 \end{pmatrix} \end{array} \sim \begin{array}{c} \begin{array}{ccc} & C_2 - xC_1 & C_3 - C_1 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ x-2 & -x^2+2x+3 & -x-1 \\ 4 & -4x-4 & x+1 \end{pmatrix} \end{array}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x^2+2x+3 & -x-1 \\ 0 & -4x-4 & x+1 \end{pmatrix} \begin{array}{l} \\ R_2 - (x-2)R_1 \\ R_3 - 4R_1 \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & C_3 & C_2 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x-1 & -x^2+2x+3 \\ 0 & x+1 & -4x-4 \end{pmatrix} \end{array} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & x^2-2x-3 \\ 0 & 0 & -x^2-2x-1 \end{pmatrix} \begin{array}{l} \\ -R_2 \\ R_3 + R_2 \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & & C_3 - (x-3)C_2 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & -(x+1)^2 \end{pmatrix} \end{array} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & (x+1)^2 \end{pmatrix} \begin{array}{l} \\ \\ -R_3 \end{array}$$

Thus the invariant factors of U are 1, $x+1$ and $(x+1)^2$.

We conclude this section with the proof of Theorem 8.1.1:

Proof of Theorem 8.1.1. Let N be a submodule of A^n. By Theorem 8.3.1, N has a basis, hence in particular it has a finite system of generators $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ and thus we can write

$$N = \mathrm{Col}_A(U) \quad \text{where} \quad U = (\mathbf{u}_1 \cdots \mathbf{u}_m) \in \mathrm{Mat}_{n\times m}(A).$$

By Theorem 8.5.5, we can, by a series of elementary row and column operations, bring the matrix U to the form

$$U' = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

for an integer $r \geq 0$ and nonzero elements $d_1, \ldots, d_r$ of A with $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$. By Theorem 8.5.4, there exists an automorphism φ of A^n such that

$$\mathrm{Col}_A(U') = \varphi(\mathrm{Col}_A(U) = \varphi(N).$$

Denote by $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ the standard basis of A^n, and set $C_j = \varphi^{-1}(\mathbf{e}_j)$ for each $j = 1, \ldots, n$. Since φ^{-1} is an automorphism of A^n, Proposition 6.5.13 shows that $\{C_1, \ldots, C_n\}$ is a basis of A^n. Also, we know, thanks to Lemma 8.4.5, that $\{d_1\mathbf{e}_1, \ldots, d_r\mathbf{e}_r\}$ is a basis of $\mathrm{Col}_A(U')$. Then Lemma 8.5.2 applied to φ^{-1} tells us that

$$\{\varphi^{-1}(d_1\mathbf{e}_1), \ldots, \varphi^{-1}(d_r\mathbf{e}_r)\} = \{d_1C_1, \ldots, d_rC_r\}$$

is a basis of $\varphi^{-1}(\mathrm{Col}_A(U')) = N$. $\square$

Exercises.

8.5.1. Prove Lemma 8.5.2.

8.5.2. Find the invariant factors of each of the following matrices:

(i) $\begin{pmatrix} 6 & 4 & 0 \\ 2 & 0 & 3 \\ 2 & 2 & 8 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{Z})$, (ii) $\begin{pmatrix} 9 & 6 & 12 \\ 3 & 0 & 4 \end{pmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$,

(iii) $\begin{pmatrix} x^3 & 0 & x^2 \\ x^2 & x & 0 \\ 0 & x & x^3 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{Q}[x])$, (iv) $\begin{pmatrix} x^3-1 & 0 & x^4-1 \\ x^2-1 & x+1 & 0 \end{pmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Q}[x])$.

8.5.3. Let A be a euclidean domain and let $U \in \mathrm{Mat}_{n\times m}(A)$. Show that the ideal I of A generated by all the entries of U is not affected by elementary row or column operations. Deduce that the first invariant factor of U is a generator of I and that therefore this divisor is uniquely determined by U up to multiplication by a unit.

8.5.4. Let A and U be as in Exercise 8.5.3, and let k be an integer with $1 \le k \le \min(n, m)$. For all integers $i_1, \dots, i_k$ and $j_1, \dots, j_k$ with

$$1 \le i_1 < i_2 < \cdots < i_k \le n \quad \text{and} \quad 1 \le j_1 < j_2 < \cdots < j_k \le m,$$

we denote by $U^{j_1,\dots,j_k}_{i_1,\dots,i_k}$ the submatrix of U of size $k \times k$ formed by the entries of U appearing in the rows with indices $i_1, \dots, i_k$ and the columns with indices $j_1, \dots, j_k$. Let I_k be the ideal of A generated by the determinants of all these submatrices (called the $k \times k$ *minors* of U).

(i) Show that this ideal is not affected by elementary row or column operations.

(ii) Let $d_1, \dots, d_r$ be the invariant factors of U. Deduce from (i) that $I_k = (d_1 \cdots d_k)$ if $k \le r$ and that $I_k = (0)$ if $k > r$.

(iii) Conclude that the integer r is the greatest integer for which U contains a submatrix of size $r \times r$ with nonzero determinant, and that the invariant factors $d_1, \dots, d_r$ of U are uniquely determined by U up to multiplication by units in $A^\times$.

Note. This construction generalizes that of Exercise 8.5.3 since I_1 is simply the ideal of A generated by all the elements of U.

8.6 Algorithms

The proof of Theorem 8.1.1 given in the preceding section gives, in principle, a method of finding the basis $\{C_1, \dots, C_n\}$ of A^n appearing in the statement of the theorem. The goal of this section is to give a practical algorithm to achieve this goal, then to deduce an algorithm for calculating the rational canonical form of an endomorphism of a finite-dimensional vector space. We begin with the following observation:

Lemma 8.6.1. *Let $U \in \mathrm{Mat}_{n\times m}(A)$, let U' be a matrix obtaining by applying to U an elementary column operation, and let E be the matrix obtained by applying the same operation to I_m (the $m \times m$ identity matrix). Then we have:*

$$U' = U\,E.$$

Proof. Denote the columns of U by $C_1, \ldots, C_m$. We split the proof into three cases:

(I) The matrix U' is obtained by interchanging columns i and j of U, where $i < j$. We then have

$$\begin{aligned}
U' &= (C_1 \cdots \overset{\overset{i}{\vee}}{C_j} \cdots \overset{\overset{j}{\vee}}{C_i} \cdots C_m) \\
&= (C_1 \cdots C_i \cdots C_j \cdots C_m) \begin{array}{cc} \begin{array}{ccccccccc} & & & i & & j & & & \\ & & & \downarrow & & \downarrow & & & \end{array} & \\ \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & 1 & & & \\ & & & \vdots & \ddots & \vdots & & & \\ & & & 1 & \cdots & 0 & & & \\ & & & & & & 1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix} & \begin{array}{c} \\ \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \\ \end{array} \end{array} \\
&= U\,E.
\end{aligned}$$

(II) The matrix U' is obtained by adding to column i of U the product of column j of U and an element a of A, where $j \neq i$. In this case

$$\begin{aligned}
U' &= (C_1 \cdots C_i \overset{\overset{i}{\vee}}{+} aC_j \cdots \overset{\overset{j}{\vee}}{C_j} \cdots C_m) \\
&= (C_1 \cdots C_i \cdots C_j \cdots C_m) \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & \vdots & \ddots & & & \\ & & a & \cdots & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{array}{c} \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \end{array} \\
&= U\,E.
\end{aligned}$$

(This presentation supposes $i < j$. The case $i > j$ is similar.)

(III) The matrix U' is obtained by multiplying the i-th column of U by a unit $a \in A^\times$. Then

$$U' = (C_1 \cdots \overset{\overset{i}{\vee}}{aC_i} \cdots C_m) = (C_1 \cdots \overset{\overset{i}{\vee}}{C_i} \cdots C_m) \begin{array}{c} \begin{array}{ccccc} & & i & & \\ & & \downarrow & & \end{array} \\ \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & a & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \end{array} = U\,E.$$

□

A similar result applies to elementary row operations. The proof of the following lemma is left as an exercise:

Lemma 8.6.2. *Let $U \in \mathrm{Mat}_{n\times m}(A)$, let U' be a matrix obtained from applying an elementary row operation to U, and let E be the matrix obtained by applying the same operation to I_n. Then we have:*

$$U' = E\,U.$$

We also note:

Lemma 8.6.3. *Let k be a positive integer. Every matrix obtained by applying an elementary column operation to I_k can also be obtained by applying an elementary row operation to I_k, and vice versa.*

Proof. (I) Interchanging columns i and j of I_k produces the same result as interchanging rows i and j

(II) Adding to column i of I_k its j-th column multiplied by an element a aof A, for distinct i and j is equivalent to adding to row j of I_k its i-th row multiplied by a:

$$\begin{array}{cl} \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & \vdots & \ddots & & & \\ & & a & \cdots & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \end{array} \end{array}$$

(III) Multiplying column i of I_k by a unit a produces the same result as multiplying row i by a. □

These results suggest the following definition.

Definition 8.6.4 (Elementary matrix). A $k \times k$ *elementary matrix* is any matrix of $\mathrm{Mat}_{k\times k}(A)$ obtained by applying an elementary row or column operation to I_k.

We immediately note:

Proposition 8.6.5. *An elementary matrix is invertible and its inverse is again an elementary matrix.*

Proof. Let $E \in \mathrm{Mat}_{k\times k}(A)$ be an elementary matrix. It is obtained by applying to I_k an elementary column operation. Let F be the matrix obtained by applying to I_k the inverse elementary operation. Then Lemma 8.6.1 gives $I_k = EF$ and $I_k = FE$. Thus E is invertible and $E^{-1} = F$. □

Note. The fact that an elementary matrix is invertible can also be seen by observing that its determinant is a unit of A (see Appendix B).

Using the notion of elementary matrices, we can reformulate Theorem 8.5.5 in the following manner:

Theorem 8.6.6. *Let $U \in \mathrm{Mat}_{n\times m}(A)$. There exist elementary matrices $E_1, \dots, E_s$ of size $n \times n$ and elementary matrices $F_1, \dots, F_t$ of size $m \times m$ such that*

$$E_s \cdots E_1\, U\, F_1 \cdots F_t = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \tag{8.14}$$

for some integer $r \geq 0$ and nonzero elements $d_1, \dots, d_r$ of A with $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$.

Proof. Theorem 8.5.5 tells us that we can transform U to a matrix of the form on the right side of (8.14) by a series of elementary row and column operations. Equality (8.14) follows by denoting by E_i the elementary matrix that encodes the i-th elementary row operation and by F_j the elementary matrix that encodes the j-th elementary column operation. □

Since every elementary matrix is invertible and a product of invertible matrices in invertible, we deduce:

Corollary 8.6.7. *Let $U \in \mathrm{Mat}_{n\times m}(A)$. There exists invertible matrices $P \in \mathrm{Mat}_{n\times n}(A)$ and $Q \in \mathrm{Mat}_{m\times m}(A)$ such that PUQ is in Smith normal form.*

To calculate P and Q, we can proceed as follows:

Algorithm 8.6.8. *Let $U \in \mathrm{Mat}_{n\times m}(A)$.*

- *We construct the "corner" table* $\left[\begin{array}{c|c} U & I_n \\ \hline I_m & \end{array}\right]$.

- *Applying a series of elementary operations to its first n row and its first m columns, we bring it to the form* $\left[\begin{array}{c|c} S & P \\ \hline Q & \end{array}\right]$ *were S denotes the Smith normal form of U.*

- *Then P and Q are invertible matrices such that $PUQ = S$.*

Proof. Let s be the number of elementary operations needed and, for $i = 0, 1, \ldots, s$, let

$$\left[\begin{array}{c|c} U_i & P_i \\ \hline Q_i & \end{array}\right]$$

be the table obtained after i elementary operation, so that the series of intermediate tables is

$$\left[\begin{array}{c|c} U & I_n \\ \hline I_m & \end{array}\right] = \left[\begin{array}{c|c} U_0 & P_0 \\ \hline Q_0 & \end{array}\right] \sim \left[\begin{array}{c|c} U_1 & P_1 \\ \hline Q_1 & \end{array}\right] \sim \cdots \sim \left[\begin{array}{c|c} U_s & P_s \\ \hline Q_s & \end{array}\right] = \left[\begin{array}{c|c} S & P \\ \hline Q & \end{array}\right].$$

We will show by induction that, for $i = 0, 1, \ldots, s$, the matrices P_i and Q_i are invertible and that $P_iUQ_i = U_i$. For $i = s$, this will show that P and Q are invertible with $PUQ = S$ as claimed.

For $i = 0$, the statement to prove is clear since I_n and I_m are invertible and $I_nUI_m = U$. Now suppose that we have $1 \leq i < s$, that P_{i-1} and Q_{i-1} are invertible and that $P_{i-1}UQ_{i-1} = U_{i-1}$. We split into two cases.

Case 1: The i-th operation is an elementary row operation (on the first n rows). In this case, if E is the corresponding elementary matrix, we have

$$U_i = EU_{i-1}, \quad P_i = EP_{i-1} \quad \text{and} \quad Q_i = Q_{i-1}.$$

Since E, P_{i-1} and Q_{i-1} are invertible, we deduce that P_i and Q_i are invertible and that

$$P_iUQ_i = EP_{i-1}UQ_{i-1} = EU_{i-1} = U_i.$$

Case 2: The i-th operation is an elementary column operation (on the first m columns). In this case, if F is the corresponding elementary matrix, we have

$$U_i = U_{i-1}F, \quad P_i = P_{i-1} \quad \text{and} \quad Q_i = Q_{i-1}F.$$

Since F, P_{i-1} and Q_{i-1} are invertible, so are P_i and Q_i and we obtain

$$P_iUQ_i = P_{i-1}UQ_{i-1}F = U_{i-1}F = U_i.$$

□

Example 8.6.9. Let $U = \begin{pmatrix} 4 & 8 & 4 \\ 4 & 10 & 8 \end{pmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$. We are looking for invertible matrices P and Q such that PUQ is in Smith normal form.

Solution: We retrace the calculations of Example 8.5.6, applying them to the table $\left[\begin{array}{c|c} U & I_2 \\ \hline I_3 & \end{array}\right]$. In this way, we find

$$\left[\begin{array}{ccc|cc} 4 & 8 & 4 & 1 & 0 \\ 4 & 10 & 8 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] \sim \begin{array}{c} \begin{array}{cc} C_2 - 2C_1 & C_3 - C_1 \end{array} \\ \left[\begin{array}{ccc|cc} 4 & 0 & 0 & 1 & 0 \\ 4 & 2 & 4 & 0 & 1 \\ \hline 1 & -2 & -1 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] \end{array}$$

$$\sim \left[\begin{array}{ccc|cc} 4 & 0 & 0 & 1 & 0 \\ 0 & 2 & 4 & -1 & 1 \\ \hline 1 & -2 & -1 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] R_2 - R_1 \sim \left[\begin{array}{ccc|cc} 4 & 2 & 4 & 0 & 1 \\ 0 & 2 & 4 & -1 & 1 \\ \hline 1 & -2 & -1 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] R_1 + R_2$$

$$\sim \begin{array}{c} \begin{array}{cc} C_2 & C_1 \end{array} \\ \left[\begin{array}{ccc|cc} 2 & 4 & 4 & 0 & 1 \\ 2 & 0 & 4 & -1 & 1 \\ \hline -2 & 1 & -1 & & \\ 1 & 0 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] \end{array} \sim \begin{array}{c} \begin{array}{cc} C_2 - 2C_1 & C_3 - 2C_1 \end{array} \\ \left[\begin{array}{ccc|cc} 2 & 0 & 0 & 0 & 1 \\ 2 & -4 & 0 & -1 & 1 \\ \hline -2 & 5 & 3 & & \\ 1 & -2 & -2 & & \\ 0 & 0 & 1 & & \end{array}\right] \end{array}$$

$$\sim \left[\begin{array}{ccc|cc} 2 & 0 & 0 & 0 & 1 \\ 0 & -4 & 0 & -1 & 0 \\ \hline -2 & 5 & 3 & & \\ 1 & -2 & -2 & & \\ 0 & 0 & 1 & & \end{array}\right] R_2 - R_1 \sim \left[\begin{array}{ccc|cc} 2 & 0 & 0 & 0 & 1 \\ 0 & 4 & 0 & 1 & 0 \\ \hline -2 & 5 & 3 & & \\ 1 & -2 & -2 & & \\ 0 & 0 & 1 & & \end{array}\right] -R_2$$

Thus $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ and $Q = \begin{pmatrix} -2 & 5 & 3 \\ 1 & -2 & -2 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{Z})$ are invertible matrices (over $\mathbb{Z}$) such that

$$PUQ = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$$

is the Smith normal form of U.

The following result shows in particular that every invertible matrix is a product of elementary matrices. Therefore, Corollary 8.6.7 is equivalent to Theorem 8.6.6 (each of the two statements implies the other).

Theorem 8.6.10. *Let $P \in \mathrm{Mat}_{n\times n}(A)$. The following conditions are equivalent:*

(i) P is invertible,

(ii) P can be transformed to I_n by a series of elementary row operations,

(iii) P can be written as a product of elementary matrices.

If these equivalent conditions are satisfied, we can, by a series of elementary row operations, transform the matrix $(P \,|\, I_n) \in \mathrm{Mat}_{n\times 2n}(A)$ to a matrix of the form $(I_n \,|\, Q)$ and then we have $P^{-1} = Q$.

In Exercises 8.6.2 and 8.6.3, we propose a sketch of a proof of this result as well as a method to determine if P is invertible and, if so, to transform P to I_n by elementary row operations.

Example 8.6.11. Let $P = \begin{pmatrix} x+1 & x^2+x+1 \\ x & x^2+1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Q}[x])$. Show that P is invertible and calculate P^{-1}.

Solution: We have

$$(P \,|\, I) = \left(\begin{array}{cc|cc} x+1 & x^2+x+1 & 1 & 0 \\ x & x^2+1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & x & 1 & -1 \\ x & x^2+1 & 0 & 1 \end{array}\right) R_1 - R_2$$

$$\sim \left(\begin{array}{cc|cc} 1 & x & 1 & -1 \\ 0 & 1 & -x & 1+x \end{array}\right) R_2 - xR_1 \sim \left(\begin{array}{cc|cc} 1 & 0 & x^2+1 & -x^2-x-1 \\ 0 & 1 & -x & x+1 \end{array}\right) R_1 - xR_2$$

Thus P is invertible (we can transform it to I_2 by a series of elementary row operations) and

$$P^{-1} = \begin{pmatrix} x^2+1 & -x^2-x-1 \\ -x & x+1 \end{pmatrix}.$$

Theorem 8.1.1 provides a basis of A^n adapted to each submodule N of A^n. The following algorithm gives a practical means of calculating such a basis when we know a system of generators of the module N.

Algorithm 8.6.12. *Let $U \in \mathrm{Mat}_{n\times m}(A)$ and let $N = \mathrm{Col}_A(U)$.*

- *Using Algorithm 8.6.8, we construct invertible matrices P and Q such that*

$$PUQ = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \tag{8.15}$$

for an integer $r \geq 0$ and nonzero elements $d_1, \ldots, d_r$ of A with $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$.

- *Then the columns of P^{-1} form a basis $\{C_1, \dots, C_n\}$ of A^n such that $\{d_1C_1, \dots, d_rC_r\}$ is a basis of N.*

Proof. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be the standard basis of A^n and let $C_1, \dots, C_n$ be the columns of P^{-1}. The function

$$\begin{array}{rccc} \varphi : & A^n & \longrightarrow & A^n \\ & X & \longmapsto & P^{-1}X \end{array}$$

is an isomorphism of A-modules (exercise) and so Proposition 6.5.13 tells us that

$$\{P^{-1}(\mathbf{e}_1), \dots, P^{-1}(\mathbf{e}_n)\} = \{C_1, \dots, C_n\}$$

is a basis of A^n. Then equality (8.15) can be rewritten

$$UQ = P^{-1}\left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right) = \begin{pmatrix} d_1C_1 & \cdots & d_rC_r & \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}.$$

Since Q is invertible, it is a product of elementary matrices (Theorem 8.6.10) and so UQ is obtained from U by a series of elementary column operations. By Lemma 8.4.3, we deduce that

$$N = \mathrm{Col}_A(U) = \mathrm{Col}_A(UQ) = \langle d_1C_1, \dots, d_rC_r\rangle_A.$$

Thus $\{d_1C_1, \dots, d_rC_r\}$ is a system of generators of N. If $a_1, \dots, a_r \in A$ satisfy

$$a_1(d_1C_1) + \cdots + a_r(d_rC_r) = \mathbf{0},$$

then $(a_1d_1)C_1 + \cdots + (a_rd_r)C_r = \mathbf{0}$, hence $a_1d_1 = \cdots = a_rd_r = 0$ since $C_1, \dots, C_n$ are linearly independent over A, and thus $a_1 = \cdots = a_r = 0$. This proves that $d_1C_1, \dots, d_rC_r$ are linearly independent and so $\{d_1C_1, \dots, d_rC_r\}$ is a basis of N. □

In fact, since the second part of Algorithm 8.6.12 does not use the matrix P, we can skip to calculating the matrix Q: it suffices to apply Algorithm 8.6.8 to the table $(U \mid I_n)$.

Example 8.6.13. Let $N = \left\langle \begin{pmatrix} x \\ x^2 \end{pmatrix}, \begin{pmatrix} x^2 \\ x \end{pmatrix}, \begin{pmatrix} x \\ x^3 \end{pmatrix} \right\rangle_{\mathbb{Q}[x]} \subseteq \mathbb{Q}[x]^2$. Then $N = \mathrm{Col}_{\mathbb{Q}[x]}(U)$ where $U = \begin{pmatrix} x & x^2 & x \\ x^2 & x & x^3 \end{pmatrix}$. We see

$$(U \mid I) = \left(\begin{array}{ccc|cc} x & x^2 & x & 1 & 0 \\ x^2 & x & x^3 & 0 & 1 \end{array}\right) \sim \begin{array}{c} \begin{array}{ccc} & C_2 - xC_1 & C_3 - C_1 \end{array} \\ \left(\begin{array}{ccc|cc} x & 0 & 0 & 1 & 0 \\ x^2 & x - x^3 & x^3 - x^2 & 0 & 1 \end{array}\right) \end{array}$$

$$\sim \left(\begin{array}{ccc|cc} x & 0 & 0 & 1 & 0 \\ 0 & x - x^3 & x^3 - x^2 & -x & 1 \end{array}\right) \begin{array}{c} \\ R_2 - xR_1 \end{array} \sim \begin{array}{c} \begin{array}{ccc} & C_2 + C_3 & \end{array} \\ \left(\begin{array}{ccc|cc} x & 0 & 0 & 1 & 0 \\ 0 & x - x^2 & x^3 - x^2 & -x & 1 \end{array}\right) \end{array}$$

$$\sim \left(\begin{array}{ccc|cc} x & 0 & \overset{C_3+xC_2}{0} & 1 & 0 \\ 0 & x-x^2 & 0 & -x & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} x & 0 & 0 & 1 & 0 \\ 0 & x^2-x & 0 & x & -1 \end{array}\right) \begin{array}{l} \\ -R_2 \end{array}$$

Therefore the invariant factors of N are x and $x^2 - x = x(x-1)$. Setting $P = \begin{pmatrix} 1 & 0 \\ x & -1 \end{pmatrix}$, we see that

$$(P \,|\, I) = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ x & -1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & -1 & -x & 1 \end{array}\right) \begin{array}{l} \\ R_2 - xR_1 \end{array} \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & x & -1 \end{array}\right) \begin{array}{l} \\ -R_2 \end{array}$$

hence $P^{-1} = \begin{pmatrix} 1 & 0 \\ x & -1 \end{pmatrix}$. Applying Algorithm 8.6.12, we conclude that

$$\left\{ C_1 = \begin{pmatrix} 1 \\ x \end{pmatrix},\ C_2 = \begin{pmatrix} 0 \\ -1 \end{pmatrix} \right\}$$

is a basis of $\mathbb{Q}[x]^2$ such that

$$\{xC_1,\ (x^2 - x)C_2\} = \left\{ \begin{pmatrix} x \\ x^2 \end{pmatrix}, \begin{pmatrix} 0 \\ -x^2 + x \end{pmatrix} \right\}$$

is a basis of N.

We conclude this chapter with the following result that refines Theorem 7.2.4 and that, combined with Theorem 7.2.5, allows us to construct a basis relative to which the matrix of a linear operator is in rational canonical form.

Theorem 8.6.14. *Let V be a vector space of finite dimension $n \geq 1$ over a field K, let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V, and let $T\colon V \to V$ be a linear operator. Then there exist invertible matrices $P, Q \in \mathrm{Mat}_{n\times n}(K[x])$ and monic polynomials $d_1(x), \ldots, d_n(x) \in K[x]$ with $d_1(x) \,|\, d_2(x) \,|\, \cdots \,|\, d_n(x)$ such that*

$$P\,(xI - [\,T\,]_{\mathcal{B}})\,Q \;=\; \begin{pmatrix} d_1(x) & & 0 \\ & \ddots & \\ 0 & & d_n(x) \end{pmatrix}. \tag{8.16}$$

Write

$$P^{-1} = \begin{pmatrix} p_{11}(x) & \cdots & p_{1n}(x) \\ \vdots & & \vdots \\ p_{n1}(x) & \cdots & p_{nn}(x) \end{pmatrix},$$

and, for the $K[x]$-module structure on V associated to T, set

$$\mathbf{u}_j \;=\; p_{1j}(x)\mathbf{v}_1 + \cdots + p_{nj}(x)\mathbf{v}_n$$

for $j = 1, \ldots, n$. Then we have

$$V = K[x]\mathbf{u}_k \oplus \cdots \oplus K[x]\mathbf{u}_n$$

where k denotes the smallest integer such that $d_k(x) \neq 1$. Furthermore, the annihilator of $\mathbf{u}_j$ is generated by $d_j(x)$ for $j = k, \ldots, n$.

Proof. Proposition 8.1.2 tells us that the function

$$\begin{array}{rccc} \psi\colon & K[x]^n & \longrightarrow & V \\ & \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} & \longmapsto & p_1(x)\mathbf{v}_1 + \cdots + p_n(x)\mathbf{v}_n \end{array}$$

is a surjective homomorphism of $K[x]$-modules, whose kernel is

$$\ker(\psi) = \mathrm{Col}_{K[x]}(xI - [\,T\,]_{\mathcal{B}}).$$

Algorithm 8.6.8 allows us to construct invertible matrices $P, Q \in \mathrm{Mat}_{n\times n}(K[x])$ such that

$$P(x\mathrm{I} - [\,T\,]_{\mathcal{B}})Q = \begin{pmatrix} d_1(x) & & & & & \\ & \ddots & & & & 0 \\ & & d_r(x) & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

for an integer $r \geq 0$ and nonzero polynomials $d_1(x), \ldots, d_r(x) \in K[x]$ with $d_1(x) \mid \cdots \mid d_r(x)$. Since the determinant of the left side of this equality is nonzero, we must have $r = n$. By changing P or Q, we can make $d_1(x), \ldots, d_n(x)$ monic. This proves the first assertion of the theorem.

Algorithm 8.6.12 tells us that the columns of P^{-1} form a basis $\{C_1, \ldots, C_n\}$ of $K[x]^n$ such that $\{d_1(x)C_1, \ldots, d_n(x)C_n\}$ is a basis of $\ker(\psi)$. By construction, we also have

$$\mathbf{u}_j = \psi(C_j)$$

for $j = 1, \ldots, n$. The conclusion now follows by retracing the proof of Theorem 7.2.1 given in Section 8.1 (with $A = K[x]$). □

This results provides a new proof of the Cayley-Hamilton Theorem. Indeed, we deduce:

Corollary 8.6.15. *In the notation of Theorem 8.6.14, we have*

$$\mathrm{char}_T(x) = d_1(x)d_2(x)\cdots d_n(x)$$

and $d_n(x)$ is the minimal polynomial of T. Furthermore, we have $\mathrm{char}_T(T) = 0$.

Proof. Taking the determinant of both sides of (8.16), we have

$$\det(P)\,\mathrm{char}_T(x)\,\det(Q) = d_1(x)\cdots d_n(x).$$

Since P and Q are invertible elements of $\mathrm{Mat}_{n\times n}(K[x])$, their determinants are elements of $K[x]^\times = K^\times$, hence the above equality can be rewritten

$$\mathrm{char}_T(x) = a\, d_1(x)\cdots d_n(x)$$

for some constant $a \in K^\times$. Since the polynomials $\mathrm{char}_T(x)$ and $d_1(x), \ldots, d_n(x)$ are both monic, we must have $a = 1$. Now, Theorem 7.2.4 tells us that $d_n(x)$ is the minimal polynomial of T. We deduce that

$$\mathrm{char}_T(T) = d_1(T) \circ \cdots \circ d_n(T) = 0.$$

□

Applying Theorem 7.2.5, we also obtain:

Corollary 8.6.16. *With the notation of Theorem 8.6.14, let $m_i = \deg(d_i(x))$ for $i = k, \ldots, n$. Then*

$$\mathcal{C} = \left\{\mathbf{u}_k, T(\mathbf{u}_k), \ldots, T^{m_k-1}(\mathbf{u}_k), \ldots\ldots, u_n, T(\mathbf{u}_n), \ldots, T^{m_n-1}(\mathbf{u}_n)\right\}$$

is a basis of V such that

$$[\,T\,]_{\mathcal{C}} = \begin{pmatrix} D_k & & 0 \\ & \ddots & \\ 0 & & D_n \end{pmatrix}$$

where D_i denotes the companion matrix of $d_i(x)$ for $i = k, \ldots, n$.

Example 8.6.17. Let V be a vector space over $\mathbb{Q}$ of dimension 3, let $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ be a basis of V, and let $T\colon V \to V$ be a linear operator for which

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 0 & -1 & -1 \\ -3 & 2 & 3 \\ 4 & -4 & -5 \end{pmatrix}.$$

Find a basis $\mathcal{C}$ of V such that $[\,T\,]_{\mathcal{C}}$ is in rational canonical form.

Solution: We first apply Algorithm 8.6.8 to the matrix

$$U = xI - [\,T\,]_{\mathcal{B}} = \begin{pmatrix} x & 1 & 1 \\ 3 & x-2 & -3 \\ -4 & 4 & x+5 \end{pmatrix}.$$

Since we only need the matrix P, we work with the table $(U \,|\, I)$. Retracing the calculations of Example 8.5.7, we find

$$\begin{aligned}
(U \,|\, I) &\sim \left(\begin{array}{ccc|ccc} C_2 & C_1 & & & & \\ 1 & x & 1 & 1 & 0 & 0 \\ x-2 & 3 & -3 & 0 & 1 & 0 \\ 4 & -4 & x+5 & 0 & 0 & 1 \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} & C_2 - xC_1 & C_3 - C_1 & & & \\ 1 & 0 & 0 & 1 & 0 & 0 \\ x-2 & -x^2+2x+3 & -x-1 & 0 & 1 & 0 \\ 4 & -4x-4 & x+1 & 0 & 0 & 1 \end{array}\right)
\end{aligned}$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -x^2+2x+3 & -x-1 & -x+2 & 1 & 0 \\ 0 & -4x-4 & x+1 & -4 & 0 & 1 \end{array}\right) \begin{array}{c} \\ R_2-(x-2)R_1 \\ R_3-4R_1 \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & C_3 & C_2 \end{array} \\ \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -x-1 & -x^2+2x+3 & -x+2 & 1 & 0 \\ 0 & x+1 & -4x-4 & -4 & 0 & 1 \end{array}\right) \end{array}$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & x+1 & x^2-2x-3 & x-2 & -1 & 0 \\ 0 & 0 & -x^2-2x-1 & -x-2 & 1 & 1 \end{array}\right) \begin{array}{c} \\ -R_2 \\ R_3+R_2 \end{array}$$

$$\sim \begin{array}{c} \begin{array}{ccc} & & C_3-(x-3)C_2 \end{array} \\ \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & x+1 & 0 & x-2 & -1 & 0 \\ 0 & 0 & -(x+1)^2 & -x-2 & 1 & 1 \end{array}\right) \end{array}$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & x+1 & 0 & x-2 & -1 & 0 \\ 0 & 0 & (x+1)^2 & x+2 & -1 & -1 \end{array}\right) \begin{array}{c} \\ \\ -R_3 \end{array}$$

Thus the invariant factors are 1, $x+1$ and $(x+1)^2$. We see that

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ x-2 & -1 & 0 \\ x+2 & -1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ x-2 & -1 & 0 \\ 4 & 1 & -1 \end{pmatrix}$$

(the verification of this calculation is left as an exercise). We deduce that

$$V = \mathbb{Q}[x]\mathbf{u}_2 \oplus \mathbb{Q}[x]\mathbf{u}_3 \quad \text{where} \quad \mathbf{u}_2 = -\mathbf{v}_2 + \mathbf{v}_3 \quad \text{and} \quad \mathbf{u}_3 = -\mathbf{v}_3.$$

Furthermore, the annihilator $\mathbf{u}_2$ is generated by $x+1$ and that of $\mathbf{u}_3$ is generated by $(x+1)^2 = x^2+2x+1$. We conclude that

$$\mathcal{C} = \{\mathbf{u}_2, \mathbf{u}_3, T(\mathbf{u}_3)\} = \{-\mathbf{v}_2+\mathbf{v}_3,\ -\mathbf{v}_3,\ \mathbf{v}_1-3\mathbf{v}_2+5\mathbf{v}_3\}$$

is a basis of V such that

$$[T]_{\mathcal{C}} = \begin{pmatrix} \boxed{-1} & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}$$

where, on the diagonal, we recognize the companion matrices of $x+1$ and x^2+2x+1.

Note. The first column of P^{-1} gives

$$\mathbf{u}_1 = 1\mathbf{v}_1 + (x-1)\mathbf{v}_2 + 4\mathbf{v}_3 = \mathbf{v}_1 + T(\mathbf{v}_2) - 2\mathbf{v}_2 + 4\mathbf{v}_3 = \mathbf{0}$$

as it should, since the annihilator of $\mathbf{u}_1$ is generated by $d_1(x) = 1$.

Exercises.

In all the exercises below, A denotes a euclidean domain.

8.6.1. Prove Lemma 8.6.2.

8.6.2. Let $P \in \mathrm{Mat}_{n\times n}(A)$.

(i) Give an algorithm for transforming P into an upper triangular matrix T by a series of elementary row operations.

(ii) Show that P is invertible if and only if the diagonal element of T are units of A.

(iii) If the diagonal elements of T are units, give an algorithm for transforming T into I_n by a series of elementary row operations.

(iv) Conclude that, if P is invertible, then P can be transformed into the matrix I_n by a series of elementary row operations.

Hint. For part (i), show that P is invertible if and only if T is invertible and use the fact that a matrix in $\mathrm{Mat}_{n\times n}(A)$ is invertible if and only if its determinant is a unit of A (see Appendix B).

8.6.3. Problem 8.6.2 shows that, in the statement of Theorem 8.6.10, the condition (i) implies condition (ii). Complete the proof of this theorem by proving the implications (ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (i), and then proving the last assertion of the theorem.

8.6.4. For each of the matrix U of Exercise 8.5.2, find invertible matrices P and Q such that PUQ is in Smith normal form.

8.6.5. In each case below, find a basis $\{C_1, \dots, C_n\}$ of A^n and nonzero elements $d_1, \dots, d_r$ of A with $d_1 \mid d_2 \mid \cdots \mid d_r$ such that $\{d_1C_1, \dots, d_rC_r\}$ is a basis of the given submodule N of A^n.

(i) $A = \mathbb{Q}[x], \quad N = \left\langle \begin{pmatrix} x \\ x+1 \\ x \end{pmatrix}, \begin{pmatrix} 0 \\ x \\ x^2 \end{pmatrix} \right\rangle_{\mathbb{Q}[x]}$

(ii) $A = \mathbb{R}[x], \quad N = \left\langle \begin{pmatrix} x+1 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} -4 \\ x+1 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ -2 \\ x-5 \end{pmatrix} \right\rangle_{\mathbb{R}[x]}$

(iii) $A = \mathbb{Z}, \quad N = \left\langle \begin{pmatrix} 4 \\ 8 \end{pmatrix}, \begin{pmatrix} 4 \\ 10 \end{pmatrix}, \begin{pmatrix} 2 \\ 8 \end{pmatrix} \right\rangle_{\mathbb{Z}}$

(iv) $A = \mathbb{Z}, \quad N = \left\langle \begin{pmatrix} 4 \\ 12 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 8 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 8 \\ -2 \end{pmatrix} \right\rangle_{\mathbb{Z}}$

8.6.6. Let V be a finite-dimensional vector space over a field K, and let $T\colon V \to V$ be a linear map. Show that $\min_T(x)$ and $\operatorname{char}_T(x)$ have the same irreducible factors in $K[x]$.

Hint. Use Corollary 8.6.15.

8.6.7. Let $T\colon \mathbb{Q}^3 \to \mathbb{Q}^3$ be a linear map. Suppose that $\operatorname{char}_T(x)$ admits an irreducible factor of degree ≥ 2 in $\mathbb{Q}[x]$. Show that $\mathbb{Q}^3$ is a cyclic $\mathbb{Q}[x]$-module.

8.6.8. Let V be a vector space of dimension 2 over $\mathbb{Q}$ with basis $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$, and let $T\colon V \to V$ be a linear map with $[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix}$.

(i) Find $\operatorname{char}_T(x)$ and $\min_T(x)$.

(ii) Find a basis $\mathcal{C}$ of V such that $[\,T\,]_{\mathcal{C}}$ is block diagonal with companion matrices of polynomials on the diagonal.

8.6.9. Let $A = \begin{pmatrix} 4 & 2 & 2 \\ 1 & 3 & 1 \\ -3 & -3 & -1 \end{pmatrix} \in \operatorname{Mat}_{3\times 3}(\mathbb{Q})$.

(i) Find $\operatorname{char}_A(x)$ and $\min_A(x)$.

(ii) Find a matrix D that is similar to A and that is block diagonal with companion matrices of polynomials on the diagonal.

Chapter 9

Duality and the tensor product

In this chapter, we present some linear algebraic constructions that play an important role in numerous areas of mathematics, as much in analysis as in algebra.

9.1 Duality

Definition 9.1.1. Let V be a vector space over a field K. The *dual* of V is the vector space $\mathcal{L}_K(V, K)$ of linear maps from V to K. We denote it by V^*. An element of V^* is called a *linear form* on V.

Example 9.1.2. Let X be a set and let $\mathcal{F}(X, K)$ be the vector space of functions $g\colon X \to K$. For all $x \in X$, the function

$$\begin{array}{rccc} E_x : & \mathcal{F}(X,K) & \longrightarrow & K \\ & g & \longmapsto & g(x) \end{array}$$

called *evaluation at the point* x, is linear, thus $E_x \in \mathcal{F}(X, K)^*$.

Proposition 9.1.3. *Suppose that V is finite dimensional over K and that $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V. For each $i = 1, \ldots, n$, we denote by $f_i\colon V \to K$ the linear map such that*

$$f_i(\mathbf{v}_j) = \delta_{ij} := \begin{cases} 0 & \text{if } j \neq i, \\ 1 & \text{if } j = i. \end{cases}$$

Then $\mathcal{B}^* = \{f_1, \ldots, f_n\}$ is a basis of V^*.

We say that $\mathcal{B}^*$ is the basis of V^* *dual* to $\mathcal{B}$.

Proof. We know that $\mathcal{E} = \{1\}$ is a basis of K viewed as a vector space over itself. Then Theorem 2.4.3 gives us an isomorphism

$$\begin{array}{rccc} \mathcal{L}_K(V,K) & \xrightarrow{\sim} & \mathrm{Mat}_{1\times n}(K)\,. \\ f & \longmapsto & [\,f\,]_{\mathcal{E}}^{\mathcal{B}} \end{array}$$

For $i = 1, \ldots, n$, we see that

$$[\, f_i \,]_{\mathcal{E}}^{\mathcal{B}} = \Big([f_i(\mathbf{v}_1)]_{\mathcal{E}} \ \cdots \ [f_i(\mathbf{v}_n)]_{\mathcal{E}} \Big) = (0, \ldots, \overset{\overset{i}{\vee}}{1}, \ldots, 0) = \mathbf{e}_i^t.$$

Since $\{\mathbf{e}_1^t, \ldots, \mathbf{e}_n^t\}$ is a basis of $\mathrm{Mat}_{1\times n}(K)$, we deduce that $\{f_1, \ldots, f_n\}$ is a basis of V^*. $\square$

Proposition 9.1.4. *Let V and W be vector spaces over K and let $T\colon V \to W$ be a linear map. For each linear form $g\colon W \to K$, the composition $g \circ T\colon V \to K$ is a linear form on V. Furthermore, the function*

$$\begin{array}{rccc} {}^tT : & W^* & \longrightarrow & V^* \\ & g & \longmapsto & g \circ T \end{array}$$

is linear.

We say that ${}^tT$ is the *transpose* of T.

Proof. The first assertion follows from the fact that the composition of two linear maps is linear. The fact that ${}^tT$ is linear follows from Proposition 2.3.1. $\square$

Example 9.1.5. Let X and Y be two sets, and let $h\colon X \to Y$ be a function. One can verify that the map

$$\begin{array}{rccc} T : & \mathcal{F}(Y, K) & \longrightarrow & \mathcal{F}(X, K) \\ & g & \longmapsto & g \circ h \end{array}$$

is linear (exercise). In this context, we determine ${}^tT(E_x)$ where $E_x \in \mathcal{F}(X, K)^*$ denotes the evaluation at a point x of X (see Example 9.1.2).

For all $g \in \mathcal{F}(Y, K)$, we have

$$({}^tT(E_x))(g) = (E_x \circ T)(g) = E_x(T(g)) = E_x(g \circ h) = (g \circ h)(x) = g(h(x)) = E_{h(x)}(g),$$

hence ${}^tT(E_x) = E_{h(x)}$.

Proposition 9.1.6. *Let U, V and W be vector spaces over K.*

(i) If $S, T \in \mathcal{L}_K(V, W)$ and $c \in K$, then

$${}^t(S + T) = {}^tS + {}^tT \quad \textit{and} \quad {}^t(cT) = c\,{}^tT.$$

(ii) If $S \in \mathcal{L}_K(U, V)$ and $T \in \mathcal{L}_K(V, W)$, then

$${}^t(T \circ S) = {}^tS \circ {}^tT.$$

The proof of this result is left as an exercise. Part (i) implies:

Corollary 9.1.7. *Let V and W be vector spaces over K. The function*

$$\begin{array}{rcl} \mathcal{L}_K(V,W) & \longrightarrow & \mathcal{L}_K(W^*,V^*) \\ T & \longmapsto & {}^tT \end{array}$$

is linear.

Theorem 9.1.8. *Let V and W be finite-dimensional vector spaces over K, let*

$$\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \quad \textit{and} \quad \mathcal{D} = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$$

be bases, respectively, of V and W, and let

$$\mathcal{B}^* = \{f_1, \ldots, f_n\} \quad \textit{and} \quad \mathcal{D}^* = \{g_1, \ldots, g_m\}$$

be the bases of V^* and W^* dual, respectively, to $\mathcal{B}$ and $\mathcal{D}$. For all $T \in \mathcal{L}_K(V,W)$, we have

$$[\,{}^tT\,]_{\mathcal{B}^*}^{\mathcal{D}^*} = \big([\,T\,]_{\mathcal{D}}^{\mathcal{B}}\big)^t\ .$$

In other words, the matrix of the transpose ${}^tT$ of T relative to the dual bases $\mathcal{D}^*$ and $\mathcal{B}^*$ is the transpose of the matrix of T relative to the bases $\mathcal{B}$ and $\mathcal{D}$.

Proof. Let $T \in \mathcal{L}_K(V,W)$. Write $[\,T\,]_{\mathcal{D}}^{\mathcal{B}} = (a_{ij})$. By definition, we have

$$T(\mathbf{v}_j) = a_{1j}\mathbf{w}_1 + \cdots + a_{mj}\mathbf{w}_m \quad (j = 1, \ldots, n).$$

We know that ${}^tT \in \mathcal{L}_K(W^*, V^*)$ and we want to find

$$[\,{}^tT\,]_{\mathcal{B}^*}^{\mathcal{D}^*} = \Big([{}^tT(g_1)]_{\mathcal{B}^*}\ \cdots\ [{}^tT(g_m)]_{\mathcal{B}^*}\Big).$$

Fix an index $j \in \{1, \ldots, m\}$. For all $i = 1, \ldots, n$, we have

$$({}^tT(g_j))(\mathbf{v}_i) = (g_j \circ T)(\mathbf{v}_i) = g_j(T(\mathbf{v}_i)) = g_j\Big(\sum_{k=1}^{m} a_{ki}w_k\Big) = a_{ji}.$$

We deduce that

$${}^tT(g_j) = \sum_{i=1}^{n} a_{ji}f_i$$

(see Exercise 9.1.1). Thus, $[{}^tT(g_j)]_{\mathcal{B}^*}$ is the transpose of the row j of $[\,T\,]_{\mathcal{D}}^{\mathcal{B}}$. This gives

$$[\,{}^tT\,]_{\mathcal{B}^*}^{\mathcal{D}^*} = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix} = \big([\,T\,]_{\mathcal{D}}^{\mathcal{B}}\big)^t$$

□

Definition 9.1.9 (Double dual). The *double dual* of a vector space V is the dual of V^*. We denote it V^{**}.

We thus have $V^{**} = \mathcal{L}_K(V^*, K)$. The following result is particularly important.

Theorem 9.1.10. *Let V be a vector space over K.*

(i) For all $\mathbf{v} \in V$, the function

$$\begin{array}{rccc} E_{\mathbf{v}} : & V^* & \longrightarrow & K \\ & f & \longmapsto & f(\mathbf{v}) \end{array}$$

is linear and so $E_{\mathbf{v}} \in V^{**}$.

(ii) The function

$$\begin{array}{rccc} \varphi : & V & \longrightarrow & V^{**} \\ & \mathbf{v} & \longmapsto & E_{\mathbf{v}} \end{array}$$

is also linear.

(iii) If V is finite-dimensional, then φ is an isomorphism.

Proof. (i) Let $\mathbf{v} \in V$. For all $f, g \in V^*$ and $c \in K$, we have

$$\begin{aligned} E_{\mathbf{v}}(f+g) &= (f+g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v}) = E_{\mathbf{v}}(f) + E_{\mathbf{v}}(g)\,, \\ E_{\mathbf{v}}(c\,f) &= (c\,f)(\mathbf{v}) = c\,f(\mathbf{v}) = c\,E_{\mathbf{v}}(f)\,. \end{aligned}$$

(ii) Let $\mathbf{u}, \mathbf{v} \in V$ and $c \in K$. For all $f \in V^*$, we have

$$\begin{aligned} E_{\mathbf{u}+\mathbf{v}}(f) &= f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = E_{\mathbf{u}}(f) + E_{\mathbf{v}}(f) = (E_{\mathbf{u}} + E_{\mathbf{v}})(f)\,, \\ E_{c\,\mathbf{v}}(f) &= f(c\,\mathbf{v}) = c\,f(\mathbf{v}) = c\,E_{\mathbf{v}}(f) = (c\,E_{\mathbf{v}})(f)\,, \end{aligned}$$

hence $E_{\mathbf{u}+\mathbf{v}} = E_{\mathbf{u}} + E_{\mathbf{v}}$ and $E_{c\,\mathbf{v}} = c\,E_{\mathbf{v}}$. This shows that φ is linear.

(iii) Suppose that V is finite-dimensional. Let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V and let $\mathcal{B}^* = \{f_1, \ldots, f_n\}$ be the basis of V^* dual to $\mathcal{B}$. We have

$$E_{\mathbf{v}_j}(f_i) = f_i(\mathbf{v}_j) = \delta_{ij} \quad (1 \le i, j \le n).$$

Thus $\{E_{\mathbf{v}_1}, \ldots, E_{\mathbf{v}_n}\}$ is the basis of $(V^*)^* = V^{**}$ dual to $\mathcal{B}^*$. Since φ maps $\mathcal{B}$ to this basis, the linear map φ is an isomorphism. □

It can be shown that the map φ defined in Theorem 9.1.10 is always injective (even if V is infinite-dimensional). It is an isomorphism if and only if V is finite-dimensional.

Exercises.

9.1.1. Let V be a finite-dimensional vector space over a field K, let $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V, and let $\mathcal{B}^* = \{f_1, \dots, f_n\}$ be the basis of V^* dual to $\mathcal{B}$. Show that, for all $f \in V^*$, we have

$$f = f(\mathbf{v}_1)f_1 + \cdots + f(\mathbf{v}_n)f_n.$$

9.1.2. Prove Proposition 9.1.6.

9.1.3. Consider the vectors $\mathbf{v}_1 = (1, 0, 1)^t$, $\mathbf{v}_2 = (0, 1, -2)^t$ and $\mathbf{v}_3 = (-1, -1, 0)^t$ of $\mathbb{R}^3$.

(i) If f is a linear form on $\mathbb{R}^3$ such that

$$f(\mathbf{v}_1) = 1, \quad f(\mathbf{v}_2) = -1, \quad f(\mathbf{v}_3) = 3,$$

and if $\mathbf{v} = (a, b, c)^t$, determine $f(\mathbf{v})$.

(ii) Give an explicit linear form f on $\mathbb{R}^3$ such that $f(\mathbf{v}_1) = f(\mathbf{v}_2) = 0$ but $f(\mathbf{v}_3) \neq 0$.

(iii) Let f be a linear form on $\mathbb{R}^3$ such that $f(\mathbf{v}_1) = f(\mathbf{v}_2) = 0$ and $f(\mathbf{v}_3) \neq 0$. Show that, for $\mathbf{v} = (2, 3, -1)^t$, we have $f(\mathbf{v}) \neq 0$.

9.1.4. Consider the vectors $\mathbf{v}_1 = (1, 0, -i)^t$, $\mathbf{v}_2 = (1, 1, 1)^t$ and $\mathbf{v}_3 = (i, i, 0)^t$ of $\mathbb{C}^3$. Show that $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a basis of $\mathbb{C}^3$ and determine the basis $\mathcal{B}^*$ of $(\mathbb{C}^3)^*$ dual to $\mathcal{B}$.

9.1.5. Let $V = \langle 1, x, x^2 \rangle_{\mathbb{R}}$ be the vector space of polynomial functions $p\colon \mathbb{R} \to \mathbb{R}$ of degree at most 2. We define three linear forms f_1, f_2, f_3 on V by setting

$$f_1(p) = \int_0^1 p(x)dx, \quad f_2(p) = \int_0^2 p(x)dx, \quad f_3(p) = \int_{-1}^0 p(x)dx.$$

Show that $\mathcal{B} = \{f_1, f_2, f_3\}$ is a basis of V^* and find its dual basis in V.

9.1.6. Let m and n be positive integers, let K be a field, and let $f_1, \dots, f_m$ be linear forms on K^n.

(i) Verify that the function $T\colon K^n \to K^m$ given by

$$T(\mathbf{v}) = \begin{pmatrix} f_1(\mathbf{v}) \\ \vdots \\ f_m(\mathbf{v}) \end{pmatrix} \quad \text{for all } \mathbf{v} \in K^n,$$

is a linear map.

(ii) Show that every linear map from K^n to K^m can be written in this way for some choice of $f_1, \dots, f_m \in (K^n)^*$.

9.1.7. Let n be a positive integer and let K be a field. Set $V = \mathrm{Mat}_{n\times n}(K)$. Recall that the *trace* of a matrix $A = (a_{i,j}) \in V$ is the sum of the elements of its diagonal: $\mathrm{trace}(A) = \sum_{i=1}^n a_{i,i}$.

(i) Verify that the function $\mathrm{trace}\colon V \to K$ is a linear form on V.

(ii) Let $B \in V$. Show that the map $\varphi_B\colon V \to K$ given by $\varphi_B(A) = \mathrm{trace}(AB)$ for all $A \in V$ is linear.

(iii) Show that the function $\Phi\colon V \to V^*$ given by $\Phi(B) = \varphi_B$ for all $B \in V$ is linear.

(iv) Show that $\ker \Phi = \{0\}$ and conclude that Φ is an isomorphism.

9.2 Bilinear maps

Let U, V and W be vector spaces over a field K.

Definition 9.2.1 (Bilinear map, bilinear form). A *bilinear map* from $U \times V$ to W is a function $B\colon U \times V \to W$ that satisfies

(i) $B(\mathbf{u}, \mathbf{v}_1 + \mathbf{v}_2) = B(\mathbf{u}, \mathbf{v}_1) + B(\mathbf{u}, \mathbf{v}_2)$,

(ii) $B(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}) = B(\mathbf{u}_1, \mathbf{v}) + B(\mathbf{u}_2, \mathbf{v})$,

(iii) $B(c\,\mathbf{u}, \mathbf{v}) = B(\mathbf{u}, c\,\mathbf{v}) = c\,B(\mathbf{u}, \mathbf{v})$

for every choice of $\mathbf{u}, \mathbf{u}_1, \mathbf{u}_2 \in U$, of $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$ and of $c \in K$. A *bilinear form* on $U \times V$ is a bilinear map from $U \times V$ to K.

Therefore, a bilinear map from $U \times V$ to W is a function $B\colon U \times V \to W$ such that,

1) for all $\mathbf{u} \in U$, the function $\begin{array}{rcl} V & \to & W \\ \mathbf{v} & \mapsto & B(\mathbf{u}, \mathbf{v}) \end{array}$ is linear;

2) for all $\mathbf{v} \in V$, the function $\begin{array}{rcl} U & \to & W \\ \mathbf{u} & \mapsto & B(\mathbf{u}, \mathbf{v}) \end{array}$ is linear.

We express condition 1) by saying that $\mathcal{B}$ is *right linear* and condition 2) by saying that $\mathcal{B}$ is *left linear*.

Example 9.2.2. The function

$$\begin{array}{rccc} B\colon & V \times V^* & \longrightarrow & K \\ & (\mathbf{v}, f) & \longmapsto & f(\mathbf{v}) \end{array}$$

is a bilinear form on $V \times V^*$ since, for every choice of $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$, of $f, f_1, f_2 \in V^*$ and of $c \in K$, we have

(i) $(f_1 + f_2)(\mathbf{v}) = f_1(\mathbf{v}) + f_2(\mathbf{v})$,

(ii) $f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2)$,

(iii) $f(c\,\mathbf{v}) = c\,f(\mathbf{v}) = (c\,f)(\mathbf{v})$.

Example 9.2.3. Proposition 2.3.1 shows that the function

$$\begin{array}{rcl} \mathcal{L}_K(U,V) \times \mathcal{L}_K(V,W) & \longrightarrow & \mathcal{L}_K(U,W) \\ (S,T) & \longmapsto & T \circ S \end{array}$$

is a bilinear map.

Definition 9.2.4. We denote by $\mathcal{L}_K^2(U,V;W)$ the set of bilinear maps from $U \times V$ to W.

The following result provides an analogue of Theorem 2.2.3 for bilinear maps.

Theorem 9.2.5. *For all $B_1, B_2 \in \mathcal{L}_K^2(U,V;W)$ and $c \in K$, the functions*

$$\begin{array}{rcl} B_1 + B_2 : U \times V & \longrightarrow & W \\ (\mathbf{u},\mathbf{v}) & \longmapsto & B_1(\mathbf{u},\mathbf{v}) + B_2(\mathbf{u},\mathbf{v}) \end{array} \quad \text{and} \quad \begin{array}{rcl} c\,B_1 : U \times V & \longrightarrow & W \\ (\mathbf{u},\mathbf{v}) & \longmapsto & c\,B_1(\mathbf{u},\mathbf{v}) \end{array}$$

are bilinear. The set $\mathcal{L}_K^2(U,V;W)$ equipped with the addition and scalar multiplication defined above is a vector space over K.

The proof of the first assertion is similar to that of Proposition 2.2.1 while the second assertion can be proved by following the model of the proof of Theorem 2.2.3. These proofs are left as exercises.

In Exercise 9.2.3, an outline is given of a proof that we have a natural isomorphism:

$$\begin{array}{rcl} \mathcal{L}_K^2(U,V;W) & \xrightarrow{\sim} & \mathcal{L}_K\big(U, \mathcal{L}_K(V,W)\big) \\ B & \longmapsto & (\mathbf{u} \mapsto (\mathbf{v} \mapsto (B(\mathbf{u},\mathbf{v}))) \end{array}$$

We conclude this section with the following results:

Theorem 9.2.6. *Suppose that U and V admit bases*

$$\mathcal{A} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\} \quad \text{and} \quad \mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$$

respectively. Then, for all $\mathbf{w}_{ij} \in W$ $(1 \le i \le m, 1 \le j \le n)$, there exists a unique bilinear map $B\colon U \times V \to W$ satisfying

$$B(\mathbf{u}_i, \mathbf{v}_j) = \mathbf{w}_{ij} \quad (1 \le i \le m, 1 \le j \le n). \tag{9.1}$$

Proof. Let $\mathbf{w}_{ij} \in W$ $(1 \le i \le m, 1 \le j \le n)$.

1st Uniqueness. If there is a bilinear map $B\colon U \times V \to W$ satisfying (9.1), then

$$\begin{aligned} B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} b_j \mathbf{v}_j\right) &= \sum_{i=1}^{m} a_i B\left(\mathbf{u}_i, \sum_{j=1}^{n} b_j \mathbf{v}_j\right) \\ &= \sum_{i=1}^{m} a_i \left(\sum_{j=1}^{n} b_j B(\mathbf{u}_i, \mathbf{v}_j)\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j \mathbf{w}_{ij} \end{aligned}$$

for all $a_1, \ldots, a_m, b_1, \ldots, b_n \in K$. This proves that there exists at most one such bilinear map.

2nd Existence. Consider the function $B\colon U \times V \to W$ defined by

$$B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} b_j \mathbf{v}_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j \mathbf{w}_{ij}.$$

It satisfies conditions (9.1). It remains to prove that it is bilinear. We have

$$\begin{aligned} B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} b_j \mathbf{v}_j + \sum_{j=1}^{n} b'_j \mathbf{v}_j\right) &= B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} (b_j + b'_j) \mathbf{v}_j\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i (b_j + b'_j) \mathbf{w}_{ij} \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j \mathbf{w}_{ij} + \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b'_j \mathbf{w}_{ij} \\ &= B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} b_j \mathbf{v}_j\right) + B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} b'_j \mathbf{v}_j\right), \end{aligned}$$

for all $a_1, \ldots, a_m, b_1, \ldots, b_n, b'_1, \ldots, b'_n \in K$. We also verify that

$$B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, c\sum_{j=1}^{n} b_j \mathbf{v}_j\right) = c\, B\left(\sum_{i=1}^{m} a_i \mathbf{u}_i, \sum_{j=1}^{n} b_j \mathbf{v}_j\right),$$

for all $c \in K$. Thus B is right linear. We check similarly that B is left linear. Therefore, B is bilinear. □

Theorem 9.2.7. *Suppose that U and V admit bases*

$$\mathcal{A} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\} \quad \textit{and} \quad \mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$$

respectively. Let $B\colon U \times V \to K$ be a bilinear form on $U \times V$. Then there exists a unique matrix $M \in \mathrm{Mat}_{m\times n}(K)$ such that

$$B(\mathbf{u}, \mathbf{v}) = [\mathbf{u}]_{\mathcal{A}}^t M [\mathbf{v}]_{\mathcal{B}} \tag{9.2}$$

for all $\mathbf{u} \in U$ and all $\mathbf{v} \in V$. The element in row i and column j of M is $B(\mathbf{u}_i, \mathbf{v}_j)$.

The matrix M is called the *matrix of the bilinear form B relative to the bases $\mathcal{A}$ of U and $\mathcal{B}$ of V.*

Proof. **1st Existence.** Let $\mathbf{u} \in U$ and $\mathbf{v} \in V$. They can be written in the form

$$\mathbf{u} = \sum_{i=1}^{m} a_i \mathbf{u}_i \quad \text{and} \quad \mathbf{v} = \sum_{j=1}^{n} b_j \mathbf{v}_j$$

with $a_1, \ldots, a_m, b_1, \ldots, b_n \in K$. We have

$$\begin{aligned} B(\mathbf{u}, \mathbf{v}) &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j B(\mathbf{u}_i, \mathbf{v}_j) \\ &= (a_1, \ldots, a_m) \begin{pmatrix} B(\mathbf{u}_1, \mathbf{v}_1) & \cdots & B(\mathbf{u}_1, \mathbf{v}_n) \\ \vdots & & \vdots \\ B(\mathbf{u}_m, \mathbf{v}_1) & \cdots & B(\mathbf{u}_m, \mathbf{v}_n) \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ &= [\mathbf{u}]_{\mathcal{A}}^t \Big(B(\mathbf{u}_i, \mathbf{v}_j) \Big) [\mathbf{v}]_{\mathcal{B}} \,. \end{aligned}$$

2nd Uniqueness. Suppose that $M \in \mathrm{Mat}_{m\times n}(K)$ satisfies condition (9.2) for all $\mathbf{u} \in U$ and all $\mathbf{v} \in V$. For $i = 1, \ldots, m$ and $j = 1, \ldots, n$, we have

$$\begin{aligned} B(\mathbf{u}_i, \mathbf{v}_j) &= [\mathbf{u}_i]_{\mathcal{A}}^t M [\mathbf{v}_j]_{\mathcal{B}} = (0, \ldots, \overset{\overset{i}{\vee}}{1}, \ldots, 0) M \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow j \\ \\ \\ \end{matrix} \\ &= \text{element in } (i, j) \text{ position of } M. \end{aligned}$$

□

Example 9.2.8. Suppose that $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V. Let $\mathcal{B}^* = \{f_1, \ldots, f_n\}$ be the dual basis of V^*. We calculate the matrix of the bilinear form

$$\begin{array}{rccc} B : & V \times V^* & \longrightarrow & K \\ & (\mathbf{v}, f) & \longmapsto & f(\mathbf{v}) \end{array}$$

relative to these bases.

Solution: We have $B(\mathbf{v}_i, f_j) = f_j(\mathbf{v}_i) = \delta_{ij}$ for $1 \le i, j \le n$, hence the matrix of B is $(\delta_{ij}) = I_n$, the $n \times n$ identity matrix.

Exercises.

9.2.1. Let V and W be vector spaces over a field K and let $\mathbf{v} \in V$. Show that the map

$$\begin{array}{rccc} B : & V^* \times W & \longrightarrow & W \\ & (f, \mathbf{w}) & \longmapsto & f(\mathbf{v})\mathbf{w} \end{array}$$

is bilinear.

9.2.2. Let T, U, V and W be vector spaces over a field K, let $B\colon U \times V \to T$ be a bilinear map and let $L\colon T \to W$ be a linear map. Show that the composite

$$L \circ B\colon U \times V \longrightarrow W$$

is a bilinear map.

9.2.3. Let U, V, W be vector spaces over a field K. For all $B \in \mathcal{L}_K^2(U, V; W)$ and all $\mathbf{u} \in U$, we denote by $B_{\mathbf{u}}\colon V \to W$ the linear map given by

$$B_{\mathbf{u}}(\mathbf{v}) = B(\mathbf{u}, \mathbf{v}) \quad (\mathbf{v} \in V).$$

(i) Let $B \in \mathcal{L}_K^2(U, V; W)$. Show that the map

$$\begin{array}{rccc} \varphi_B : & U & \longrightarrow & \mathcal{L}_K(V; W) \\ & \mathbf{u} & \longmapsto & B_{\mathbf{u}} \end{array}$$

is linear.

(ii) Show that the map

$$\begin{array}{rccc} \varphi : & \mathcal{L}_K^2(U, V; W) & \longrightarrow & \mathcal{L}_K(U, \mathcal{L}_K(V; W)) \\ & B & \longmapsto & \varphi_B \end{array}$$

is an isomorphism of vector spaces over K.

9.2.4. Let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be the standard basis of $\mathbb{R}^2$ and $\{\mathbf{e}'_1, \mathbf{e}'_2, \mathbf{e}'_3\}$ be the standard basis of $\mathbb{R}^3$. Give a formula for $f((x_1, x_2, x_3), (y_1, y_2))$ where $f\colon \mathbb{R}^3 \times \mathbb{R}^2 \to \mathbb{R}$ denotes the bilinear map determined by the conditions

$$\begin{array}{lll} f(\mathbf{e}'_1, \mathbf{e}_1) = 1, & f(\mathbf{e}'_1, \mathbf{e}_2) = 0, & f(\mathbf{e}'_2, \mathbf{e}_1) = 3, \\ f(\mathbf{e}'_2, \mathbf{e}_2) = -1, & f(\mathbf{e}'_3, \mathbf{e}_1) = 4, & f(\mathbf{e}'_3, \mathbf{e}_2) = -2. \end{array}$$

Deduce the value of $f(\mathbf{u}, \mathbf{v})$ if $\mathbf{u} = (1, 2, 1)^t$ and $\mathbf{v} = (1, 0)^t$.

9.2.5. Let U, V and W be vector spaces over a field K, let $B_i\colon U \times V \to W$ $(i = 1, 2)$ be bilinear maps, and let $c \in K$. Show that the maps

$$\begin{aligned} B_1 + B_2\colon U \times V &\longrightarrow W \\ (\mathbf{u}, \mathbf{v}) &\longmapsto B_1(\mathbf{u}, \mathbf{v}) + B_2(\mathbf{u}, \mathbf{v}) \end{aligned} \qquad \text{and} \qquad \begin{aligned} cB_1\colon U \times V &\longrightarrow W \\ (\mathbf{u}, \mathbf{v}) &\longmapsto cB_1(\mathbf{u}, \mathbf{v}) \end{aligned}$$

are bilinear. Then show that $\mathcal{L}^2_K(U, V\,;\, W)$ is a vector space for these operations (since this verification is a bit long, you can simply show the existence of an additive identity, that every element has an additive inverse and that one of the two axioms of distributivity holds).

9.2.6. Let V be a vector space of finite dimension n over a field K, and let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V. For every pair of integers $i, j \in \{1, \ldots, n\}$, we denote by $g_{i,j}\colon V \times V \to K$ the bilinear form determined by the conditions

$$g_{i,j}(\mathbf{v}_k, \mathbf{v}_\ell) = \begin{cases} 1 & \text{if } (k, \ell) = (i, j), \\ 0 & \text{otherwise.} \end{cases}$$

Show that $\mathcal{B} = \{\, g_{i,j}\,;\, 1 \le i, j \le n \,\}$ is a basis of the vector space $\mathrm{Bil}(V, K) := \mathcal{L}^2_K(V, V\,;\, K)$ of all bilinear maps from $V \times V$ to K.

9.2.7. Let V be a vector space over a field K of characteristic different from 2. We say that a bilinear form $f\colon V \times V \to K$ is *symmetric* if $f(\mathbf{u}, \mathbf{v}) = f(\mathbf{v}, \mathbf{u})$ for all $\mathbf{u} \in V$ and $\mathbf{v} \in V$. We say that it is *antisymmetric* if $f(\mathbf{u}, \mathbf{v}) = -f(\mathbf{v}, \mathbf{u})$ for all $\mathbf{u} \in V$ and $\mathbf{v} \in V$.

(i) Show that the set S of symmetric bilinear forms on $V \times V$ is a subspace of $\mathrm{Bil}(V, K) := \mathcal{L}^2_K(V, V\,;\, K)$.

(ii) Show that the set A of antisymmetric bilinear forms on $V \times V$ is also a subspace of $\mathrm{Bil}(V, K)$.

(iii) Show that $\mathrm{Bil}(V, K) = S \oplus A$.

9.2.8. Find a basis of the space of symmetric bilinear forms from $\mathbb{R}^2 \times \mathbb{R}^2$ to $\mathbb{R}$ and a basis of the space of antisymmetric bilinear forms from $\mathbb{R}^2 \times \mathbb{R}^2$ to $\mathbb{R}$.

9.2.9. Let $\mathcal{C}(\mathbb{R})$ be the vector space of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, and let V be the subspace of $\mathcal{C}(\mathbb{R})$ generated (over $\mathbb{R}$) by the functions 1, $\sin(x)$ and $\cos(x)$. Show that the function

$$\begin{aligned} B\colon V \times V &\longrightarrow \mathbb{R} \\ (f, g) &\longmapsto \textstyle\int_0^\pi f(t)g(\pi - t)dt \end{aligned}$$

is a bilinear form and find its matrix with respect to the basis $\mathcal{A} = \{1, \sin(x), \cos(x)\}$ of V.

9.2.10. Let $V = \langle\, 1, x, \ldots, x^n \,\rangle_{\mathbb{R}}$ be the vector space of polynomial functions $p\colon \mathbb{R} \to \mathbb{R}$ of degree at most n. Find the matrix of the bilinear map

$$\begin{aligned} B\colon V \times V &\longrightarrow \mathbb{R} \\ (f, g) &\longmapsto \textstyle\int_0^1 f(t)g(t)dt \end{aligned}$$

with respect to the basis $\mathcal{A} = \{1, x, \ldots, x^n\}$ of V.

9.3 Tensor product

Throughout this section, we fix two vector spaces U and V of finite dimension over a field K.

If T is a vector space, we can consider a bilinear map from $U \times V$ to T as a product

$$\begin{array}{rcl} U \times V & \longrightarrow & T \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} \otimes \mathbf{v} \end{array} \tag{9.3}$$

with values in T. To say that this map is bilinear means that the product in question satisfies:

$$\begin{aligned} (\mathbf{u}_1 + \mathbf{u}_2) \otimes \mathbf{v} &= \mathbf{u}_1 \otimes \mathbf{v} + \mathbf{u}_2 \otimes \mathbf{v}, \\ \mathbf{u} \otimes (\mathbf{v}_1 + \mathbf{v}_2) &= \mathbf{u} \otimes \mathbf{v}_1 + \mathbf{u} \otimes \mathbf{v}_2, \\ (c\,\mathbf{u}) \otimes \mathbf{v} &= \mathbf{u} \otimes (c\,\mathbf{v}) = c\,\mathbf{u} \otimes \mathbf{v}, \end{aligned}$$

for all $\mathbf{u}, \mathbf{u}_1, \mathbf{u}_2 \in U$, all $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$ and all $c \in K$.

Given a bilinear map as above in (9.3), we easily check that, for every linear map $L\colon T \to W$, the composite $B\colon U \times V \to W$ given by

$$B(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \otimes \mathbf{v}) \quad \text{for all } (\mathbf{u}, \mathbf{v}) \in U \times V \tag{9.4}$$

is a bilinear map (see Exercise 9.2.2).

Our goal is to construct a bilinear map (9.3) that is *universal* in the sense that every bilinear map $B\colon U \times V \to W$ can be written in the form (9.4) for a unique choice of linear map $L\colon T \to W$. A bilinear map (9.3) with this property is called a *tensor product* of U and V. The following definition summarizes this discussion.

Definition 9.3.1 (Tensor product). A *tensor product* of U and V is the data of a vector space T over K and a bilinear map

$$\begin{array}{rcl} U \times V & \longrightarrow & T \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} \otimes \mathbf{v} \end{array}$$

possessing the following property. For every vector space W and every bilinear map $B\colon U \times V \to W$, there exists a unique linear map $L\colon T \to W$ such that $B(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \otimes \mathbf{v})$ for all $(\mathbf{u}, \mathbf{v}) \in U \times V$.

This condition can be represented by the following diagram:

$$\begin{tikzcd} U \times V \arrow[r, "B"] \arrow[d, "\otimes"'] & W \\ T \arrow[ur, dotted, "L"'] & \end{tikzcd} \tag{9.5}$$

In this diagram, the vertical arrow represents the tensor product, the horizontal arrow represents an arbitrary bilinear map, and the dotted diagonal arrow represents the unique linear map L that, by composition with the tensor product, recovers B. For such a choice of L, the horizontal arrow B is the composition of the two other arrows and we say that the diagram (9.5) is *commutative*.

The following proposition gives the existence of a tensor product of U and V.

Proposition 9.3.2. *Let $\{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ be a basis of U, let $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V, and let $\{\mathbf{t}_{ij}\,;\, 1 \le i \le m, 1 \le j \le n\}$ be a basis of a vector space T of dimension mn over K. The bilinear map (9.3) determined by the conditions*

$$\mathbf{u}_i \otimes \mathbf{v}_j = \mathbf{t}_{ij} \quad (1 \le i \le m, 1 \le j \le n) \tag{9.6}$$

is a tensor product of U and V.

Proof. Theorem 9.2.6 shows that there exists a bilinear map $(\mathbf{u}, \mathbf{v}) \longmapsto \mathbf{u} \otimes \mathbf{v}$ from $U \times V$ to T satisfying 9.6. It remains to show that it satisfies the universal property required by Definition 9.3.1.

To do this, we fix an arbitrary bilinear map $B\colon U \times V \to W$. Since the set $\{\mathbf{t}_{ij}\,;\, 1 \le i \le m, 1 \le j \le n\}$ is a basis of T, there exists a unique linear map $L\colon T \to W$ such that

$$L(\mathbf{t}_{ij}) = B(\mathbf{u}_i, \mathbf{v}_j) \quad (1 \le i \le m, 1 \le j \le n). \tag{9.7}$$

Then the map $B'\colon U \times V \to W$ given by $B'(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \otimes \mathbf{v})$ for all $(\mathbf{u}, \mathbf{v}) \in U \times V$ is bilinear and satisfies

$$B'(\mathbf{u}_i, \mathbf{v}_j) = L(\mathbf{u}_i \otimes \mathbf{v}_j) = L(\mathbf{t}_{ij}) = B(\mathbf{u}_i, \mathbf{v}_j) \quad (1 \le i \le m,\ 1 \le j \le n).$$

By Theorem 9.2.6, this implies that $B' = B$. Thus the map L satisfies the condition

$$B(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \otimes \mathbf{v}) \quad \text{for all } (\mathbf{u}, \mathbf{v}) \in U \times V.$$

Finally, L is the only linear map from T to W satisfying this condition since the latter implies (9.7), which determines L uniquely. □

The proof given above uses in a crucial way the hypotheses that U and V are finite-dimensional over K. It is possible to prove the existence of the tensor product in greater generality, without this hypothesis, but we will not do so here.

We next observe that the tensor product is unique up to isomorphism.

Proposition 9.3.3. *Suppose that*

$$\begin{array}{ccc} U \times V & \longrightarrow & T \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} \otimes \mathbf{v} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} U \times V & \longrightarrow & T' \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} \otimes' \mathbf{v} \end{array}$$

are two tensor products of U and V. Then there exists an isomorphism $L\colon T \to T'$ such that

$$L(\mathbf{u} \otimes \mathbf{v}) = \mathbf{u} \otimes' \mathbf{v}$$

for all $(\mathbf{u}, \mathbf{v}) \in U \times V$.

Proof. Since $\otimes'$ is bilinear and $\otimes$ is a tensor product, there exists a linear map $L\colon T \to T'$ such that

$$\mathbf{u} \otimes' \mathbf{v} = L(\mathbf{u} \otimes \mathbf{v}) \tag{9.8}$$

for all $(\mathbf{u}, \mathbf{v}) \in U \times V$. It remains to prove that L is an isomorphism. For this, we first note that, symmetrically, since $\otimes$ is bilinear and $\otimes'$ is a tensor product, there exists a linear map $L'\colon T' \to T$ such that

$$\mathbf{u} \otimes \mathbf{v} = L'(\mathbf{u} \otimes' \mathbf{v}) \tag{9.9}$$

for all $(\mathbf{u}, \mathbf{v}) \in U \times V$. Combining (9.8) and (9.9), we obtain

$$(L' \circ L)(\mathbf{u} \otimes \mathbf{v}) = \mathbf{u} \otimes \mathbf{v} \quad \text{and} \quad (L \circ L')(\mathbf{u} \otimes' \mathbf{v}) = \mathbf{u} \otimes' \mathbf{v}$$

for all $(\mathbf{u}, \mathbf{v}) \in U \times V$. Now, the identity maps $I\colon T \to T$ and $I'\colon T' \to T'$ also satisfy

$$I(\mathbf{u} \otimes \mathbf{v}) = \mathbf{u} \otimes \mathbf{v} \quad \text{and} \quad I'(\mathbf{u} \otimes' \mathbf{v}) = \mathbf{u} \otimes' \mathbf{v}$$

for all $(\mathbf{u}, \mathbf{v}) \in U \times V$. Since $\otimes$ and $\otimes'$ are tensor products, this implies that $L' \circ L = I$ and $L \circ L' = I'$. Thus L is an invertible linear map with inverse L', and so it is an isomorphism. □

Combining Proposition 9.3.2 and 9.3.3, we obtain the following.

Proposition 9.3.4. *Let $\{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ be a basis of U, let $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V, and let $\otimes\colon U \times V \to T$ be a tensor product of U and V. Then*

$$\{\mathbf{u}_i \otimes \mathbf{v}_j \,;\, 1 \le i \le m, 1 \le j \le n\} \tag{9.10}$$

is a basis of T.

Proof. Proposition 9.3.2 shows that there exists a tensor product $\otimes\colon U \times V \to T$ such that (9.10) is a basis of T. If $\otimes'\colon U \times V \to T'$ is another tensor product, then, by Proposition 9.3.3, there exists an isomorphism $L\colon T \to T'$ such that $\mathbf{u} \otimes' \mathbf{v} = L(\mathbf{u} \otimes \mathbf{v})$ for all $(\mathbf{u}, \mathbf{v}) \in U \times V$. Since (9.10) is a basis of T, we deduce that the products

$$\mathbf{u}_i \otimes' \mathbf{v}_j = L(\mathbf{u}_i \otimes \mathbf{v}_j) \quad (1 \le i \le m,\ 1 \le j \le n)$$

form a basis of T'. □

The following theorem summarizes the essential results obtained up to now:

Theorem 9.3.5. *There exists a tensor product $\otimes\colon U \times V \to T$ of U and V. If $\{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ is a basis of U and $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis of V, then $\{\mathbf{u}_i \otimes \mathbf{v}_j \,;\, 1 \le i \le m, 1 \le j \le n\}$ is a basis of T.*

We often say that T itself is the tensor product of U and V and we denote it by $U \otimes V$ or, more precisely, by $U \otimes_K V$ when we want to emphasize the fact that U and V are considered as vector spaces over K. Theorem 9.3.5 gives

$$\dim_K(U \otimes_K V) = \dim_K(U) \dim_K(V).$$

The fact that the tensor product is not unique, but is unique up to isomorphism, does not cause problems in practice, in the sense that the linear dependence relations between the products $\mathbf{u} \otimes \mathbf{v}$ with $\mathbf{u} \in U$ and $\mathbf{v} \in V$ do not depend on the tensor product $\otimes$. In fact if, for a given tensor product $\otimes\colon U \times V \to T$, we have:

$$c_1\mathbf{u}_1 \otimes \mathbf{v}_1 + c_2\mathbf{u}_2 \otimes \mathbf{v}_2 + \cdots + c_s\mathbf{u}_s \otimes \mathbf{v}_s = \mathbf{0} \tag{9.11}$$

with $c_1, \ldots, c_s \in K$, $\mathbf{u}_1, \ldots, \mathbf{u}_s \in U$ and $\mathbf{v}_1, \ldots, \mathbf{v}_s \in V$, and if $\otimes'\colon U \times V \to T'$ is another tensor product, then, denoting by $L\colon T \to T'$ the isomorphism such that $L(\mathbf{u} \otimes \mathbf{v}) = \mathbf{u} \otimes' \mathbf{v}$ for all $(\mathbf{u}, \mathbf{v}) \in U \times V$ and applying L to both sides of (9.11), we get

$$c_1\mathbf{u}_1 \otimes' \mathbf{v}_1 + c_2\mathbf{u}_2 \otimes' \mathbf{v}_2 + \cdots + c_s\mathbf{u}_s \otimes' \mathbf{v}_s = \mathbf{0}.$$

Example 9.3.6. Let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be the standard basis of K^2. A basis of $K^2 \otimes_K K^2$ is

$$\{\mathbf{e}_1 \otimes \mathbf{e}_1,\ \mathbf{e}_1 \otimes \mathbf{e}_2,\ \mathbf{e}_2 \otimes \mathbf{e}_1,\ \mathbf{e}_2 \otimes \mathbf{e}_2\}.$$

In particular, we have $\mathbf{e}_1 \otimes \mathbf{e}_2 - \mathbf{e}_2 \otimes \mathbf{e}_1 \neq \mathbf{0}$, hence $\mathbf{e}_1 \otimes \mathbf{e}_2 \neq \mathbf{e}_2 \otimes \mathbf{e}_1$. We also find

$$\begin{aligned}(\mathbf{e}_1 + \mathbf{e}_2) \otimes (\mathbf{e}_1 - \mathbf{e}_2) &= \mathbf{e}_1 \otimes (\mathbf{e}_1 - \mathbf{e}_2) + \mathbf{e}_2 \otimes (\mathbf{e}_1 - \mathbf{e}_2) \\ &= \mathbf{e}_1 \otimes \mathbf{e}_1 - \mathbf{e}_1 \otimes \mathbf{e}_2 + \mathbf{e}_2 \otimes \mathbf{e}_1 - \mathbf{e}_2 \otimes \mathbf{e}_2.\end{aligned}$$

More generally, we have

$$\begin{aligned}(a_1\mathbf{e}_1 + a_2\mathbf{e}_2) \otimes (b_1\mathbf{e}_1 + b_2\mathbf{e}_2) &= \Big(\sum_{i=1}^{2} a_i\mathbf{e}_i\Big) \otimes \Big(\sum_{j=1}^{2} b_j\mathbf{e}_j\Big) \\ &= \sum_{i=1}^{2}\sum_{j=1}^{2} a_ib_j\mathbf{e}_i \otimes \mathbf{e}_j \\ &= a_1b_1\mathbf{e}_1 \otimes \mathbf{e}_1 + a_1b_2\mathbf{e}_1 \otimes \mathbf{e}_2 + a_2b_1\mathbf{e}_2 \otimes \mathbf{e}_1 + a_2b_2\mathbf{e}_2 \otimes \mathbf{e}_2.\end{aligned}$$

Example 9.3.7. We know that the scalar product in $\mathbb{R}^n$ is a bilinear form

$$\begin{array}{rcl}\mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \mathbb{R}\ . \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \langle \mathbf{u}, \mathbf{v}\rangle\end{array}$$

Thus these exists a unique linear map $L\colon \mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^n \to \mathbb{R}$ such that

$$\langle \mathbf{u}, \mathbf{v}\rangle = L(\mathbf{u} \otimes \mathbf{v})$$

for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$. Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be the standard basis of $\mathbb{R}^n$. Then the set $\{\mathbf{e}_i \otimes \mathbf{e}_j\,;\, 1 \leq i \leq n, 1 \leq j \leq n\}$ is a basis of $\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^n$ and so L is determined by the conditions

$$L(\mathbf{e}_i \otimes \mathbf{e}_j) = \langle \mathbf{e}_i, \mathbf{e}_j\rangle = \delta_{ij} \quad (1 \leq i \leq n, 1 \leq j \leq n).$$

Exercises.

9.3.1. Let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be the standard basis of $\mathbb{R}^2$. Show that $\mathbf{e}_1 \otimes \mathbf{e}_2 + \mathbf{e}_2 \otimes \mathbf{e}_1$ cannot be written in the form $\mathbf{u} \otimes \mathbf{v}$ with $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$.

9.3.2. Let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be the standard basis of $\mathbb{R}^2$, let $B\colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$ be the bilinear map determined by the conditions

$$B(\mathbf{e}_1, \mathbf{e}_1) = (1, 0), \quad B(\mathbf{e}_1, \mathbf{e}_2) = (2, 1), \quad B(\mathbf{e}_2, \mathbf{e}_1) = (-1, 3) \quad \text{and} \quad B(\mathbf{e}_2, \mathbf{e}_2) = (0, -1),$$

and let $L\colon \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map such that $B(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \otimes \mathbf{v})$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$. Calculate

(i) $L(\mathbf{e}_1 \otimes \mathbf{e}_2 - \mathbf{e}_2 \otimes \mathbf{e}_1)$,

(ii) $L((\mathbf{e}_1 + 2\mathbf{e}_2) \otimes (-\mathbf{e}_1 + \mathbf{e}_2))$,

(iii) $L(\mathbf{e}_1 \otimes \mathbf{e}_1 + (\mathbf{e}_1 + \mathbf{e}_2) \otimes \mathbf{e}_2)$.

9.3.3. Let V be a finite-dimensional vector space over a field K. Show that there exists a unique linear form $L\colon V^* \otimes_K V \to K$ satisfying the condition $L(f \otimes \mathbf{v}) = f(\mathbf{v})$ for all $f \in V^*$ and $\mathbf{v} \in V$.

9.3.4. Let U and V be finite-dimensional vector spaces over a field K and let $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ be a basis of U. Show that every element $\mathbf{t}$ of $U \otimes_K V$ can be written in the form

$$\mathbf{t} = \mathbf{u}_1 \otimes \mathbf{v}_1 + \mathbf{u}_2 \otimes \mathbf{v}_2 + \cdots + \mathbf{u}_m \otimes \mathbf{v}_m$$

for a unique choice of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m \in V$.

9.3.5. Let U, V be finite-dimensional vector spaces over a field K.

(i) Let U_1 and V_1 be subspaces of U and V respectively and let T_1 be the subspace of $U \otimes_K V$ generated by the products $\mathbf{u} \otimes \mathbf{v}$ with $\mathbf{u} \in U_1$ and $\mathbf{v} \in V_1$. Show that the map

$$\begin{array}{rcl} U_1 \times V_1 & \longrightarrow & T_1 \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} \otimes \mathbf{v} \end{array}$$

is a tensor product of U_1 and V_1. We can then identify T_1 with $U_1 \otimes_K V_1$.

(ii) Suppose that $U = U_1 \oplus U_2$ and $V = V_1 \oplus V_2$. Show that

$$U \otimes_K V = (U_1 \otimes_K V_1) \oplus (U_2 \otimes_K V_1) \oplus (U_1 \otimes_K V_2) \oplus (U_2 \otimes_K V_2).$$

9.3.6. Let V be a finite-dimensional vector space over $\mathbb{R}$. Considering $\mathbb{C}$ as a vector space over $\mathbb{R}$, we form the tensor product $\mathbb{C} \otimes_{\mathbb{R}} V$.

(i) Show that, for all $\alpha \in \mathbb{C}$, there exists a unique linear map $L_\alpha \colon \mathbb{C} \otimes_{\mathbb{R}} V \to \mathbb{C} \otimes_{\mathbb{R}} V$ satisfying $L_\alpha(\beta \otimes \mathbf{v}) = (\alpha\beta) \otimes \mathbf{v}$ for all $\beta \in \mathbb{C}$ and $\mathbf{v} \in V$.

(ii) Show that, for all $\alpha, \alpha' \in \mathbb{C}$, we have $L_\alpha \circ L_{\alpha'} = L_{\alpha\alpha'}$ and $L_\alpha + L_{\alpha'} = L_{\alpha+\alpha'}$. Deduce that $\mathbb{C} \otimes_{\mathbb{R}} V$ is a vector space over $\mathbb{C}$ for the external multiplication given by $\alpha\mathbf{t} = L_\alpha(\mathbf{t})$ for all $\alpha \in \mathbb{C}$ and $\mathbf{v} \in V$.

(iii) Show that if $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V as a vector space over $\mathbb{R}$, then $\{1 \otimes \mathbf{v}_1, \ldots, 1 \otimes \mathbf{v}_n\}$ is a basis of $\mathbb{C} \otimes_{\mathbb{R}} V$ as a vector space over $\mathbb{C}$.

We say that $\mathbb{C} \otimes_{\mathbb{R}} V$ is the *complexification* of V.

9.3.7. With the notation of the preceding problem, show that every element $\mathbf{t}$ of $\mathbb{C} \otimes_{\mathbb{R}} V$ can be written in the form $\mathbf{t} = 1 \otimes \mathbf{u} + i \otimes \mathbf{v}$ for unique $\mathbf{u}, \mathbf{v} \in V$, and also that every complex number $\alpha \in \mathbb{C}$ can be written in the form $\alpha = a + ib$ for unique $a, b \in \mathbb{R}$. Given α and $\mathbf{u}$ as above, determine the decomposition of the product $\alpha\mathbf{t}$.

9.3.8. Let V and W be finite-dimensional vector spaces over a field K.

(i) Show that, for all $f \in V^*$ and $\mathbf{w} \in W$, the map

$$\begin{array}{rcl} L_{f,\mathbf{w}} \colon V & \longrightarrow & W \\ \mathbf{v} & \longmapsto & f(\mathbf{v})\mathbf{w} \end{array}$$

is linear.

(ii) Show also that the map

$$\begin{array}{rcl} V^* \times W & \longrightarrow & \mathcal{L}_K(V, W) \\ (f, \mathbf{w}) & \longmapsto & L_{f,\mathbf{w}} \end{array}$$

is bilinear.

(iii) Deduce that there exists a unique isomorphism $L \colon V^* \otimes_K W \xrightarrow{\sim} \mathcal{L}_K(V, W)$ satisfying $L(f \otimes \mathbf{w}) = L_{f,\mathbf{w}}$ for all $f \in V^*$ and $\mathbf{w} \in W$.

9.3.9. With the notation of the proceeding problem, let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V, let $\{f_1, \ldots, f_n\}$ be the basis of V^* dual to $\mathcal{B}$, and let $\mathcal{D} = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ be a basis of W. Fix $T \in \mathcal{L}_K(V, W)$ and set $[\,T\,]_{\mathcal{D}}^{\mathcal{B}} = (a_{ij})$. Show that, under the isomorphism L of part (iii) of the preceding problem, we have

$$T = L\left(\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} f_j \otimes \mathbf{w}_i\right).$$

9.3.10. Let K be a field of characteristic not equal to 2, and let V be a vector space over K of dimension n with basis $\mathcal{A} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. For every pair of elements $\mathbf{u}$, $\mathbf{v}$ of V, we define

$$\mathbf{u} \wedge \mathbf{v} := \frac{1}{2}(\mathbf{u} \otimes \mathbf{v} - \mathbf{v} \otimes \mathbf{u}) \quad \text{and} \quad \mathbf{u} \cdot \mathbf{v} := \frac{1}{2}(\mathbf{u} \otimes \mathbf{v} + \mathbf{v} \otimes \mathbf{u}).$$

Let $\bigwedge^2 V$ be the subspace of $V \otimes_K V$ generated by the vectors $\mathbf{u} \wedge \mathbf{v}$, and let $\mathrm{Sym}^2(V)$ be the subspace generated by the vectors $\mathbf{u} \cdot \mathbf{v}$.

(i) Show that the set $\mathcal{B}_1 = \{\mathbf{v}_i \wedge \mathbf{v}_j \,;\, 1 \leq i < j \leq n\}$ is a basis of $\bigwedge^2 V$ while $\mathcal{B}_2 = \{\mathbf{v}_i \cdot \mathbf{v}_j \,;\, 1 \leq i \leq j \leq n\}$ is a basis of $\mathrm{Sym}^2(V)$. Deduce that $V \otimes_K V = \bigwedge^2 V \oplus \mathrm{Sym}^2(V)$.

(ii) Show that the map $\varphi_1 \colon V \times V \to \bigwedge^2 V$ given by $\varphi_1(\mathbf{u}, \mathbf{v}) = \mathbf{u} \wedge \mathbf{v}$ is antisymmetric bilinear and that the map $\varphi_2 \colon V \times V \to \mathrm{Sym}^2(V)$ given by $\varphi_2(\mathbf{u}, \mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$ is symmetric bilinear (see Exercise 9.2.7 for the definitions).

(iii) Let $B \colon V \times V \to W$ be an arbitrary antisymmetric bilinear map. Show that there exists a unique linear map $L_1 \colon \bigwedge^2 V \to W$ such that $B = L_1 \circ \varphi_1$.

(iv) State and prove the analogue of (iii) for a symmetric bilinear map.

Hint. For (iii), let $L \colon V \otimes V \to W$ be the linear map satisfying $B(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \otimes \mathbf{v})$ for all $\mathbf{u}, \mathbf{v} \in V$. Show that $\mathrm{Sym}^2(V) \subseteq \ker(L)$ and that $B(\mathbf{u}, \mathbf{v}) = L(\mathbf{u} \wedge \mathbf{v})$ for all $\mathbf{u}, \mathbf{v} \in V$.

9.4 The Kronecker product

In this section, we fix finite-dimensional vector spaces U and V over a field K and we fix a tensor product

$$\begin{array}{ccc} U \times V & \longrightarrow & U \otimes_K V\,. \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} \otimes \mathbf{v} \end{array}$$

We first note:

Proposition 9.4.1. *Let $S \in \mathrm{End}_K(U)$ and $T \in \mathrm{End}_K(V)$. Then there exists a unique element of $\mathrm{End}_K(U \otimes_K V)$, denoted $S \otimes T$, such that*

$$(S \otimes T)(\mathbf{u} \otimes \mathbf{v}) = S(\mathbf{u}) \otimes T(\mathbf{v})$$

for all $(\mathbf{u}, \mathbf{v}) \in U \times V$.

Proof. The map

$$\begin{array}{rccc} B : & U \times V & \longrightarrow & U \otimes_K V \\ & (\mathbf{u}, \mathbf{v}) & \longmapsto & S(\mathbf{u}) \otimes T(\mathbf{v}) \end{array}$$

is left linear since

$$\begin{aligned} B(\mathbf{u}_1+\mathbf{u}_2,\mathbf{v}) &= S(\mathbf{u}_2+\mathbf{u}_2)\otimes T(\mathbf{v}) \\ &= (S(\mathbf{u}_1)+S(\mathbf{u}_2))\otimes T(\mathbf{v}) \\ &= S(\mathbf{u}_1)\otimes T(\mathbf{v})+S(\mathbf{u}_2)\otimes T(\mathbf{v}) \\ &= B(\mathbf{u}_1,\mathbf{v})+B(\mathbf{u}_2,\mathbf{v}) \end{aligned} \qquad \text{and} \qquad \begin{aligned} B(c\,\mathbf{u},\mathbf{v}) &= S(c\,\mathbf{u})\otimes T(\mathbf{v}) \\ &= (c\,S(\mathbf{u}))\otimes T(\mathbf{v}) \\ &= c\,(S(\mathbf{u})\otimes T(\mathbf{v})) \\ &= c\,B(\mathbf{u},\mathbf{v}) \end{aligned}$$

for all $\mathbf{u},\mathbf{u}_1,\mathbf{u}_2\in U$, $\mathbf{v}\in V$ and $c\in K$. Similarly, we verify that B is right linear. Thus it is a bilinear map. By the properties of the tensor product, we conclude that there exists a unique linear map $L\colon U\otimes_K V\to U\otimes_K V$ such that

$$L(\mathbf{u}\otimes\mathbf{v}) = S(\mathbf{u})\otimes T(\mathbf{v})$$

for all $\mathbf{u}\in U$ and $\mathbf{v}\in V$. □

The tensor product of the operators defined by Proposition 9.4.1 possesses a number of properties (see the exercises). We show here the following:

Proposition 9.4.2. *Let $S_1,S_2\in\mathrm{End}_K(U)$ and $T_1,T_2\in\mathrm{End}_K(V)$. Then we have*

$$(S_1\otimes T_1)\circ(S_2\otimes T_2) = (S_1\circ S_2)\otimes(T_1\circ T_2).$$

Proof. For all $(\mathbf{u},\mathbf{v})\in U\times V$, we have

$$\begin{aligned} ((S_1\otimes T_1)\circ(S_2\otimes T_2))(\mathbf{u}\otimes\mathbf{v}) &= (S_1\otimes T_1)((S_2\otimes T_2)(\mathbf{u}\otimes\mathbf{v})) \\ &= (S_1\otimes T_1)(S_2(\mathbf{u})\otimes T_2(\mathbf{v})) \\ &= S_1(S_2(\mathbf{u}))\otimes T_1(T_2(\mathbf{v})) \\ &= (S_1\circ S_2)(\mathbf{u})\otimes(T_1\circ T_2)(\mathbf{v}). \end{aligned}$$

By Proposition 9.4.1, this implies that $(S_1\otimes T_1)\circ(S_2\otimes T_2) = (S_1\circ S_2)\otimes(T_1\circ T_2)$. □

Definition 9.4.3 (Kronecker product). The *Kronecker product* of a matrix $A=(a_{ij})\in\mathrm{Mat}_{m\times m}(K)$ by a matrix $B=(b_{ij})\in\mathrm{Mat}_{n\times n}(K)$ is the matrix

$$A\dot{\times}B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{pmatrix} \in \mathrm{Mat}_{mn\times mn}(K).$$

Our interest in this notion comes from the following result:

Proposition 9.4.4. *Let $S\in\mathrm{End}_K(U)$ and $T\in\mathrm{End}_K(V)$, and let*

$$\mathcal{A}=\{\mathbf{u}_1,\dots,\mathbf{u}_m\} \quad \textit{and} \quad \mathcal{B}=\{\mathbf{v}_1,\dots,\mathbf{v}_n\}$$

be bases of U and V respectively. Then

$$\mathcal{C}=\{\mathbf{u}_1\otimes\mathbf{v}_1,\dots,\mathbf{u}_1\otimes\mathbf{v}_n;\mathbf{u}_2\otimes\mathbf{v}_1,\dots,\mathbf{u}_2\otimes\mathbf{v}_n;\dots\dots;\mathbf{u}_m\otimes\mathbf{v}_1,\dots,\mathbf{u}_m\otimes\mathbf{v}_n\}$$

is a basis of $U\otimes_K V$ and we have

$$[\,S\otimes T\,]_{\mathcal{C}} = [\,S\,]_{\mathcal{A}}\dot{\times}[\,T\,]_{\mathcal{B}}.$$

Proof. The matrix $[\,S \otimes T\,]_{\mathcal{C}}$ decomposes naturally in blocks:

$$\begin{array}{c} \\ \left\{\begin{array}{c}\mathbf{u}_1 \otimes \mathbf{v}_1 \\ \vdots \\ \mathbf{u}_1 \otimes \mathbf{v}_n\end{array}\right. \\ \vdots \\ \left\{\begin{array}{c}\mathbf{u}_m \otimes \mathbf{v}_1 \\ \vdots \\ \mathbf{u}_m \otimes \mathbf{v}_n\end{array}\right. \end{array} \begin{array}{c} \overbrace{\mathbf{u}_1 \otimes \mathbf{v}_1, \ldots, \mathbf{u}_1 \otimes \mathbf{v}_n} \quad \cdots \quad \overbrace{\mathbf{u}_m \otimes \mathbf{v}_1, \ldots, \mathbf{u}_m \otimes \mathbf{v}_n} \\ \left(\begin{array}{c|c|c} C_{11} & \cdots & C_{1m} \\ \hline \vdots & & \vdots \\ \hline C_{m1} & \cdots & C_{mm} \end{array}\right) \end{array}.$$

For fixed $k, l \in \{1, \ldots, m\}$, the block C_{kl} is the following piece:

$$\begin{array}{c} \\ \vdots \\ \mathbf{u}_k \otimes \mathbf{v}_1 \\ \vdots \\ \mathbf{u}_k \otimes \mathbf{v}_n \\ \vdots \end{array} \begin{array}{c} \cdots \quad \mathbf{u}_l \otimes \mathbf{v}_1, \ldots, \mathbf{u}_l \otimes \mathbf{v}_n \quad \cdots \\ \left(\begin{array}{c|c|c} & & \\ \hline & C_{kl} & \\ \hline & & \end{array}\right) \end{array}.$$

The (i, j) element of C_{kl} is thus equal to the coefficient of $\mathbf{u}_k \otimes \mathbf{v}_i$ in the expression of $(S \otimes T)(\mathbf{u}_l \otimes \mathbf{v}_j)$ as a linear combination of elements of the basis $\mathcal{C}$. To calculate it, write

$$A = [\,S\,]_{\mathcal{A}} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \quad \text{and} \quad B = [\,T\,]_{\mathcal{B}} = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.$$

We see that

$$\begin{aligned} (S \otimes T)(\mathbf{u}_l \otimes \mathbf{v}_j) &= S(\mathbf{u}_l) \otimes T(\mathbf{v}_j) \\ &= (a_{1l}\mathbf{u}_1 + \cdots + a_{ml}\mathbf{u}_m) \otimes (b_{1j}\mathbf{v}_1 + \cdots + b_{nj}\mathbf{v}_n) \\ &= \cdots + (a_{kl}b_{1j}\mathbf{u}_k \otimes \mathbf{v}_1 + \cdots + a_{kl}b_{nj}\mathbf{u}_k \otimes \mathbf{v}_n) + \cdots \end{aligned}$$

hence the (i, j) entry of C_{kl} is $a_{kl}b_{ij}$, equal to that of $a_{kl}B$. This proves that $C_{kl} = a_{kl}B$ and so

$$[\,S \otimes T\,]_{\mathcal{C}} = A \dot{\times} B = [\,S\,]_{\mathcal{A}} \dot{\times} [\,T\,]_{\mathcal{B}}.$$

$\square$

Exercises.

9.4.1. Denote by $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2\}$ the standard basis of $\mathbb{R}^2$ and by $\mathcal{E}' = \{\mathbf{e}'_1, \mathbf{e}'_2, \mathbf{e}'_3\}$ that of $\mathbb{R}^3$. Let $S\colon \mathbb{R}^2 \to \mathbb{R}^2$ and $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operators for which

$$[\,S\,]_{\mathcal{E}} = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad [\,T\,]_{\mathcal{E}'} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Calculate

(i) $(S \otimes T)(3\mathbf{e}_1 \otimes \mathbf{e}'_1)$,

(ii) $(S \otimes T)(2\mathbf{e}_1 \otimes \mathbf{e}'_1 - \mathbf{e}_2 \otimes \mathbf{e}'_2)$,

(iii) $(S \otimes T)(2(\mathbf{e}_1 + \mathbf{e}_2) \otimes \mathbf{e}'_3 - \mathbf{e}_2 \otimes \mathbf{e}'_3)$.

9.4.2. Let U and V be finite-dimensional vector spaces over a field K, and let $S\colon U \to U$ and $T\colon V \to V$ be invertible linear maps. Show that the linear map $S \otimes T\colon U \otimes_K V \to U \otimes_K V$ is also invertible, and give an equation relating S^{-1}, T^{-1} and $(S \otimes T)^{-1}$.

9.4.3. Let $S \in \mathrm{End}_K(U)$ and $T \in \mathrm{End}_K(V)$, where U and V denote finite-dimensional vector spaces over a field K. Let U_1 be an S-invariant subspace of U and let V_1 be a T-invariant subspace of V. Consider $U_1 \otimes_K V_1$ as a subspace of $U \otimes_K V$ as in Exercise 9.3.5. Under these hypotheses, show that $U_1 \otimes_K V_1$ is an $S \otimes T$-invariant subspace of $U \otimes_K V$ and that $(S \otimes T)|_{U_1 \otimes_K V_1} = S|_{U_1} \otimes T|_{V_1}$.

9.4.4. Let $S \in \mathrm{End}_{\mathbb{C}}(U)$ and $T \in \mathrm{End}_{\mathbb{C}}(V)$, where U and V denote vector spaces of dimensions m and n respectively over $\mathbb{C}$. We choose a basis $\mathcal{A}$ of U and a basis $\mathcal{B}$ of V such that the matrix $[\,S\,]_{\mathcal{A}}$ and $[\,T\,]_{\mathcal{B}}$ are in Jordan canonical form. Show that, for the corresponding basis $\mathcal{C}$ of $U \otimes_{\mathbb{C}} V$ given by Proposition 9.4.4, the matrix $[\,S \otimes T\,]_{\mathcal{C}}$ is upper triangular. By calculating its determinant, show that $\det(S \otimes T) = \det(S)^n \det(T)^m$.

9.4.5. Let U and V be finite-dimensional vector spaces over a field K.

(i) Show that the map

$$\begin{array}{rcl} B \,:\, \mathrm{End}_K(U) \times \mathrm{End}_K(V) & \longrightarrow & \mathrm{End}_K(U \otimes_K V) \\ (S, T) & \longmapsto & S \otimes T \end{array}$$

is bilinear.

(ii) Show that the image of B generates $\mathrm{End}_K(U \otimes_K V)$ as a vector space over K.

(iii) Conclude that the linear map from $\mathrm{End}_K(U) \otimes_K \mathrm{End}_K(V)$ to $\mathrm{End}_K(U \otimes_K V)$ associated to B is an isomorphism.

9.4.6. Let U and V be finite-dimensional vector spaces over a field K.

(i) Let $f \in U^*$ and $g \in V^*$. Show that there exists a unique linear form $f \otimes g \colon U \otimes_K V \to K$ such that $(f \otimes g)(\mathbf{u} \otimes \mathbf{v}) = f(\mathbf{u})g(\mathbf{v})$ for all $(\mathbf{u}, \mathbf{v}) \in U \times V$.

(ii) Show that the map $B \colon U^* \times V^* \to (U \otimes_K V)^*$ given by $B(f, g) = f \otimes g$ for all $(f, g) \in U^* \times V^*$ is bilinear and that its image generates $(U \otimes_K V)^*$ as a vector space over K. Conclude that the linear map from $U^* \otimes_K V^*$ to $(U \otimes_K V)^*$ associated to V is an isomorphism.

(iii) Let $S \in \mathrm{End}_K(U)$ and $T \in \mathrm{End}_K(V)$. Show that, if we identify $U^* \otimes_K V^*$ with $(U \otimes_K V)^*$ using the isomorphism established in (ii), then we have ${}^tS \otimes {}^tT = {}^t(S \otimes T)$.

9.5 Multiple tensor products

Theorem 9.5.1. *Let U, V, W be finite-dimensional vector spaces over a field K. There exists a unique isomorphism $L \colon (U \otimes_K V) \otimes_K W \to U \otimes_K (V \otimes_K W)$ such that*

$$L((\mathbf{u} \otimes \mathbf{v}) \otimes \mathbf{w}) = \mathbf{u} \otimes (\mathbf{v} \otimes \mathbf{w})$$

for all $(\mathbf{u}, \mathbf{v}, \mathbf{w}) \in U \times V \times W$.

Proof. Let $\{\mathbf{u}_1, \ldots, \mathbf{u}_l\}$, $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ and $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ be bases of U, V and W respectively. Then

$$\{(\mathbf{u}_i \otimes \mathbf{v}_j) \otimes \mathbf{w}_k \,;\, 1 \le i \le l, 1 \le j \le m, 1 \le k \le n\},$$
$$\{\mathbf{u}_i \otimes (\mathbf{v}_j \otimes \mathbf{w}_k) \,;\, 1 \le i \le l, 1 \le j \le m, 1 \le k \le n\}$$

are bases, respectively, of $(U \otimes_K V) \otimes_K W$ and $U \otimes_K (V \otimes_K W)$. Thus there exists a unique linear map L from $(U \otimes_K V) \otimes_K W$ to $U \otimes_K (V \otimes_K W)$ such that

$$L((\mathbf{u}_i \otimes \mathbf{v}_j) \otimes \mathbf{w}_k) = \mathbf{u}_i \otimes (\mathbf{v}_j \otimes \mathbf{w}_k)$$

for $i = 1, \ldots, l$, $j = 1, \ldots, m$ and $k = 1, \ldots, n$. By construction, L is an isomorphism. Finally, for arbitrary vectors

$$\mathbf{u} = \sum_{i=1}^{l} a_i \mathbf{u}_i \in U, \quad \mathbf{v} = \sum_{j=1}^{m} b_j \mathbf{v}_j \in V \quad \text{and} \quad \mathbf{w} = \sum_{k=1}^{n} c_k \mathbf{w}_k \in W,$$

we have

$$\begin{aligned}
L((\mathbf{u}\otimes\mathbf{v})\otimes\mathbf{w}) &= L\left(\left(\left(\sum_{i=1}^{l} a_i\mathbf{u}_i\right)\otimes\left(\sum_{j=1}^{m} b_j\mathbf{v}_j\right)\right)\otimes\left(\sum_{k=1}^{n} c_k\mathbf{w}_k\right)\right)\\
&= L\left(\sum_{i=1}^{l}\sum_{j=1}^{m}\sum_{k=1}^{n} a_ib_jc_k(\mathbf{u}_i\otimes\mathbf{v}_j)\otimes\mathbf{w}_k\right)\\
&= \sum_{i=1}^{l}\sum_{j=1}^{m}\sum_{k=1}^{n} a_ib_jc_k\,\mathbf{u}_i\otimes(\mathbf{v}_j\otimes\mathbf{w}_k)\\
&= \left(\sum_{i=1}^{l} a_i\mathbf{u}_i\right)\otimes\left(\left(\sum_{j=1}^{m} b_j\mathbf{v}_j\right)\otimes\left(\sum_{k=1}^{n} c_k\mathbf{w}_k\right)\right)\\
&= \mathbf{u}\otimes(\mathbf{v}\otimes\mathbf{w}),
\end{aligned}$$

as required. □

The isomorphism $(U\otimes_K V)\otimes_K W\simeq U\otimes_K(V\otimes_K W)$ given by Theorem 9.5.1 allows us to identify these two spaces, and to denote them by $U\otimes_K V\otimes_K W$. We then write $\mathbf{u}\otimes\mathbf{v}\otimes\mathbf{w}$ instead of $(\mathbf{u}\otimes\mathbf{v})\otimes\mathbf{w}$ or $\mathbf{u}\otimes(\mathbf{v}\otimes\mathbf{w})$.

In general, Theorem 9.5.1 allows us to omit the parentheses in the tensor product of an arbitrary number of finite-dimensional vector spaces $V_1,\dots,V_r$ over K. Thus, we write

$$V_1\otimes_K V_2\otimes_K\cdots\otimes_K V_r \quad\text{instead of}\quad V_1\otimes_K(V_2\otimes_K(\cdots\otimes_K V_r))$$

and

$$\mathbf{v}_1\otimes\mathbf{v}_2\otimes\cdots\otimes\mathbf{v}_r \quad\text{instead of}\quad \mathbf{v}_1\otimes(\mathbf{v}_2\times(\cdots\otimes\mathbf{v}_r)).$$

We then have

$$\dim_K(V_1\otimes_K V_2\otimes_K\cdots\otimes_K V_r)=\dim_K(V_1)\dim_K(V_2)\cdots\dim_K(V_r).$$

Exercises.

9.5.1. Let V and W be finite-dimensional vector space over a field K. Show that there exists a unique isomorphism $L\colon V\otimes_K W\to W\otimes_K V$ such that $L(\mathbf{v}\otimes\mathbf{w})=\mathbf{w}\otimes\mathbf{v}$ for all $\mathbf{v}\in V$ and $\mathbf{w}\in W$.

9.5.2. Let r be a positive integer and $V_1,\dots,V_r,W$ be vector spaces over K. We say that a function

$$\varphi\,:\,V_1\times\cdots\times V_r\longrightarrow W$$

is *multilinear* or *r-linear* if it is linear in each of its arguments, that is if it satisfies

ML1. $\varphi(\mathbf{v}_1, \ldots, \mathbf{v}_i + \mathbf{v}_i', \ldots, \mathbf{v}_r) = \varphi(\mathbf{v}_1, \ldots, \mathbf{v}_i, \ldots, \mathbf{v}_r) + \varphi(\mathbf{v}_1, \ldots, \mathbf{v}_i', \ldots, \mathbf{v}_r)$

ML2. $\varphi(\mathbf{v}_1, \ldots, c\,\mathbf{v}_i, \ldots, \mathbf{v}_r) = c\,\varphi(\mathbf{v}_1, \ldots, \mathbf{v}_i, \ldots, \mathbf{v}_r)$

for all $i \in \{1, \ldots, r\}, \mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_i, \mathbf{v}_i' \in V_i, \ldots, \mathbf{v}_r \in V_r$ and $c \in K$.

Show that the function

$$\begin{array}{rccc} \psi : & V_1 \times V_2 \times \cdots \times V_r & \longrightarrow & V_1 \otimes_K V_2 \otimes_K \cdots \otimes_K V_r \\ & (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r) & \longmapsto & \mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r \end{array}$$

is multilinear.

9.5.3. Let $V_1, \ldots, V_r$ and W be as in the preceding exercise. The goal of this new exercise is to show that, for any multilinear map $\varphi\colon V_1 \times \cdots \times V_r \to W$, there exists a unique linear map $L\colon V_1 \otimes_K \cdots \otimes_K V_r \to W$ such that

$$\varphi(\mathbf{v}_1, \ldots, \mathbf{v}_r) = L(\mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r)$$

for all $(\mathbf{v}_1, \ldots, \mathbf{v}_r) \in V_1 \times \cdots \times V_r$.

We proceed by induction on r. For $r = 2$, this follows from the definition of the tensor product. Suppose $r \geq 3$ and the result is true for multilinear maps from $V_2 \times \cdots \times V_r$ to W.

(i) Show that, for each choice of $\mathbf{v}_1 \in V_1$, there exists a unique linear map $L_{\mathbf{v}_1}\colon V_2 \otimes_K \cdots \otimes_K V_r \to W$ such that

$$\varphi(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r) = L_{\mathbf{v}_1}(\mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r)$$

for all $(\mathbf{v}_2, \ldots, \mathbf{v}_r) \in V_2 \times \cdots \times V_r$.

(ii) Show that the map

$$\begin{array}{rccc} B : & V_1 \times (V_2 \otimes_K \cdots \otimes_K V_r) & \longrightarrow & W \\ & (\mathbf{v}_1, \alpha) & \longmapsto & L_{\mathbf{v}_1}(\alpha) \end{array}$$

is bilinear.

(iii) Deduce that there exists a unique linear map $L\colon V_1 \otimes_K (V_2 \otimes_K \cdots \otimes_K V_r) \to W$ such that $\varphi(\mathbf{v}_1, \ldots, \mathbf{v}_r) = L(\mathbf{v}_1 \otimes (\mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r))$ for all $(\mathbf{v}_1, \ldots, \mathbf{v}_r) \in V_1 \times \cdots \times V_r$.

9.5.4. Let V be a finite-dimensional vector space over a field K. Using the result of the preceding exercise, show that there exists a unique linear map $L\colon V^* \otimes_K V \otimes_K V \to V$ such that $L(f \otimes \mathbf{v}_1 \otimes \mathbf{v}_2) = f(\mathbf{v}_1)\mathbf{v}_2$ for all $(f, \mathbf{v}_1, \mathbf{v}_2) \in V^* \times V \times V$.

9.5.5. Let V_1, V_2, V_3 and W be finite-dimensional vector spaces over a field K, and let $\varphi : V_1 \times V_2 \times V_3 \to W$ be a trilinear map. Show that there exists a unique bilinear map $B\colon V_1 \times (V_2 \otimes_K V_3) \to W$ such that $B(\mathbf{v}_1, \mathbf{v}_2 \otimes \mathbf{v}_3) = \varphi(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ for all $\mathbf{v}_j \in V_j$ $(j = 1, 2, 3)$.

Chapter 10

Inner product spaces

After a general review of inner product spaces, we define the notions of orthogonal operators and symmetric operators on these spaces and prove the structure theorems for these operators (the spectral theorems). We conclude by showing that every linear operator on a finite-dimensional inner product space is the composition of a positive definite symmetric operator followed by an orthogonal operator. This decomposition is called the *polar decomposition* of an operator. For example, in $\mathbb{R}^2$, a positive definite symmetric operator is a product of dilations along orthogonal axes, while an orthogonal operator is a rotation about the origin or a reflection in a line passing through the origin. Therefore every linear operator on $\mathbb{R}^2$ is the composition of dilations along orthogonal axes follwed by a rotation or reflection.

10.1 Review

Definition 10.1.1 (Inner product). Let V be a real vector space. An *inner product* on V is a bilinear form

$$\begin{array}{ccc} V \times V & \longrightarrow & \mathbb{R} \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \langle \mathbf{u}, \mathbf{v} \rangle \end{array}$$

that is *symmetric*:

$$\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle \quad \text{for all } \mathbf{u}, \mathbf{v} \in V$$

and *positive definite*:

$$\langle \mathbf{v}, \mathbf{v} \rangle \geq 0 \quad \text{for all } \mathbf{v} \in V, \quad \text{with} \quad \langle \mathbf{v}, \mathbf{v} \rangle = 0 \iff \mathbf{v} = \mathbf{0}\,.$$

Definition 10.1.2 (Inner product space). A *inner product space* is a real vector space V equipped with an inner product.

Example 10.1.3. Let n be a positive integer. We define an inner product on $\mathbb{R}^n$ by setting

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = x_1 y_1 + \cdots + x_n y_n.$$

Equipped with this inner product, $\mathbb{R}^n$ becomes an inner product space, called *euclidean space*. When we speak of $\mathbb{R}^n$ as an inner product space without specifying the inner product, we are implicitly using the inner product defined above.

Example 10.1.4. Let V be the vector space of continuous functions $f\colon \mathbb{R} \to \mathbb{R}$ that are 2π-periodic, that is, which satisfy $f(x+2\pi) = f(x)$ for all $x \in \mathbb{R}$. Then V is an inner product space for the inner product

$$\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)\mathrm{d}x\,.$$

Example 10.1.5. Let n be a positive integer. Then $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is an inner product space for the inner product $\langle A, B\rangle = \mathrm{trace}(AB^t)$.

For the rest of this section, we fix an inner product space V with inner product $\langle\ ,\ \rangle$. We first note:

Proposition 10.1.6. *Every subspace W of V is an inner product space for the inner product of V restricted to W.*

Proof. Indeed, the inner product of V induces, by restriction, a bilinear map

$$\begin{array}{ccc} W \times W & \longrightarrow & \mathbb{R} \\ (\mathbf{w}_1, \mathbf{w}_2) & \longmapsto & \langle \mathbf{w}_1, \mathbf{w}_2\rangle \end{array}$$

and it is easily verified that this is an inner product in the sense of Definition 10.1.1. □

When we refer to a subspace of V as an inner product space, it is this inner product we are referring to.

Definition 10.1.7 (Norm, unit vector). The *norm* of a vector $\mathbf{v} \in V$ is

$$\|\mathbf{v}\| = \langle \mathbf{v}, \mathbf{v}\rangle^{1/2}.$$

We say that a vector $\mathbf{v} \in V$ is a *unit vector* if $\|\mathbf{v}\| = 1$.

Recall that the norm possesses the following properties, the first two of which follow immediately from the definition:

Proposition 10.1.8. *For all $\mathbf{u}, \mathbf{v} \in V$ and $c \in \mathbb{R}$, we have*

(i) $\|\mathbf{v}\| \geq 0$ *with equality if and only if* $\mathbf{v} = \mathbf{0}$,

(ii) $\|c\,\mathbf{v}\| = |c|\,\|\mathbf{v}\|$,

(iii) $|\langle \mathbf{u}, \mathbf{v}\rangle| \leq \|\mathbf{u}\|\|\mathbf{v}\|$ *(Cauchy-Schwarz inequality),*

(iv) $\|\mathbf{u}+\mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ *(triangle inequality).*

Relations (i), (ii) and (iv) show that $\|\cdot\|$ is indeed a norm in the proper sense of the term. The norm allows us to measure the "length" of vectors in V. It also allows us to define the "distance" $\mathrm{d}(\mathbf{u},\mathbf{v})$ between two vectors $\mathbf{u}$ and $\mathbf{v}$ of V by setting

$$\mathrm{d}(\mathbf{u},\mathbf{v}) = \|\mathbf{u}-\mathbf{v}\|.$$

Thanks to the triangle inequality, it is easily verified that this defines a metric on V.

Inequality (iii), called the Cauchy-Schwarz inequality, allows us to define the angle $\theta \in [0,\pi]$ between two nonzero vectors $\mathbf{u}$ and $\mathbf{v}$ of V by setting

$$\theta = \arccos\left(\frac{\langle \mathbf{u},\mathbf{v}\rangle}{\|\mathbf{u}\|\|\mathbf{v}\|}\right). \tag{10.1}$$

In particular, this angle θ is equal to $\pi/2$ if and only if $\langle \mathbf{u},\mathbf{v}\rangle = 0$. For this reason, we say that the vectors $\mathbf{u},\mathbf{v}$ of V are *perpendicular* or *orthogonal* if $\langle \mathbf{u},\mathbf{v}\rangle = 0$.

Finally, if $\mathbf{v} \in V$ is nonzero, it follows from (ii) that the product

$$\|\mathbf{v}\|^{-1}\mathbf{v}$$

is a unit vector parallel to $\mathbf{v}$ (the angle between it and $\mathbf{v}$ is 0 radians by (10.1)).

Definition 10.1.9. Let $\mathbf{v}_1,\dots,\mathbf{v}_n \in V$.

1) We say that $\{\mathbf{v}_1,\dots,\mathbf{v}_n\}$ is an *orthogonal subset* of V if $\mathbf{v}_i \neq \mathbf{0}$ for $i = 1,\dots,n$ and if $\langle \mathbf{v}_i,\mathbf{v}_j\rangle = 0$ for every pair of integers (i,j) with $1 \leq i,j \leq n$ and $i \neq j$.

2) We say that $\{\mathbf{v}_1,\dots,\mathbf{v}_n\}$ is an *orthogonal basis* of V, if is it both a basis of V and an orthogonal subset of V.

3) We say that $\{\mathbf{v}_1,\dots,\mathbf{v}_n\}$ is an *orthonormal basis* of V if it is an orthogonal basis of V consisting of unit vectors, that is, such that $\|\mathbf{v}_i\| = \langle \mathbf{v}_i,\mathbf{v}_i\rangle^{1/2} = 1$ for $i = 1,\dots,n$.

The following proposition summarizes the importance of these ideas.

Proposition 10.1.10.

(i) Every orthogonal subset of V is linearly independent.

(ii) Suppose that $\mathcal{B} = \{\mathbf{v}_1,\dots,\mathbf{v}_n\}$ is an orthogonal basis of V. Then, for all $\mathbf{v} \in V$, we have

$$\mathbf{v} = \frac{\langle \mathbf{v},\mathbf{v}_1\rangle}{\langle \mathbf{v}_1,\mathbf{v}_1\rangle}\mathbf{v}_1 + \cdots + \frac{\langle \mathbf{v},\mathbf{v}_n\rangle}{\langle \mathbf{v}_n,\mathbf{v}_n\rangle}\mathbf{v}_n.$$

(iii) If $\mathcal{B} = \{\mathbf{v}_1,\dots,\mathbf{v}_n\}$ is an orthonormal basis of V, then, for all $\mathbf{v} \in V$, we have

$$[\mathbf{v}]_{\mathcal{B}} = \begin{pmatrix} \langle \mathbf{v},\mathbf{v}_1\rangle \\ \vdots \\ \langle \mathbf{v},\mathbf{v}_n\rangle \end{pmatrix}.$$

Proof. Suppose first that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is an orthogonal subset of V, and that $\mathbf{v} \in \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle_{\mathbb{R}}$. We can write

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

with $a_1, \ldots, a_n \in \mathbb{R}$. Taking the inner product of both sides of this equality with $\mathbf{v}_i$, we have

$$\langle \mathbf{v}, \mathbf{v}_i \rangle = \Big\langle \sum_{j=1}^{n} a_j\mathbf{v}_j, \mathbf{v}_i \Big\rangle = \sum_{j=1}^{n} a_j \langle \mathbf{v}_j, \mathbf{v}_i \rangle = a_i \langle \mathbf{v}_i, \mathbf{v}_i \rangle$$

and so

$$a_i = \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} \quad (i = 1, \ldots, n).$$

If we choose $\mathbf{v} = \mathbf{0}$, this formula gives $a_1 = \cdots = a_n = 0$. Thus the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly independent and thus it is a basis of $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle_{\mathbb{R}}$. This proves both (i) and (ii). Statement (iii) follows immediately from (ii). □

The following result shows that, if V is finite-dimensional, it possesses an orthogonal basis. In particular, this holds for every finite-dimensional subspace of V.

Theorem 10.1.11 (Gram-Schimdt orthogonalization procedure)**.**
Suppose that $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ is a basis of V. We recursively define:

$$\begin{aligned}
\mathbf{v}_1 &= \mathbf{w}_1, \\
\mathbf{v}_2 &= \mathbf{w}_2 - \frac{\langle \mathbf{w}_2, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle}\mathbf{v}_1, \\
\mathbf{v}_3 &= \mathbf{w}_3 - \frac{\langle \mathbf{w}_3, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle}\mathbf{v}_1 - \frac{\langle \mathbf{w}_3, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_2, \mathbf{v}_2 \rangle}\mathbf{v}_2, \\
&\vdots \\
\mathbf{v}_n &= \mathbf{w}_n - \frac{\langle \mathbf{w}_n, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle}\mathbf{v}_1 - \cdots - \frac{\langle \mathbf{w}_n, \mathbf{v}_{n-1} \rangle}{\langle \mathbf{v}_{n-1}, \mathbf{v}_{n-1} \rangle}\mathbf{v}_{n-1}.
\end{aligned}$$

Then, for all $i = 1, \ldots, n$, the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_i\}$ is an orthogonal basis of the subspace $\langle \mathbf{w}_1, \ldots, \mathbf{w}_i \rangle_{\mathbb{R}}$. In particular, $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is an orthogonal basis of V.

Proof. It suffices to show the first assertion. For this, we proceed by induction on i. For $i = 1$, it is clear that $\{\mathbf{v}_1\}$ is an orthogonal basis of $\langle \mathbf{w}_1 \rangle_{\mathbb{R}}$ since $\mathbf{v}_1 = \mathbf{w}_1 \neq \mathbf{0}$. Suppose that $\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\}$ is an orthogonal basis of $\langle \mathbf{w}_1, \ldots, \mathbf{w}_{i-1} \rangle_{\mathbb{R}}$ for an integer i with $2 \leq i \leq n$. By definition, we have

$$\mathbf{v}_i = \mathbf{w}_i - \frac{\langle \mathbf{w}_i, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle}\mathbf{v}_1 - \cdots - \frac{\langle \mathbf{w}_i, \mathbf{v}_{i-1} \rangle}{\langle \mathbf{v}_{i-1}, \mathbf{v}_{i-1} \rangle}\mathbf{v}_{i-1}, \tag{10.2}$$

and we note that the denominators $\langle \mathbf{v}_1, \mathbf{v}_1 \rangle, \ldots, \langle \mathbf{v}_{i-1}, \mathbf{v}_{i-1} \rangle$ of the coefficients of $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$ are nonzero since each of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$ is nonzero. We deduce from this formula that

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i \rangle_{\mathbb{R}} = \langle \mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{w}_i \rangle_{\mathbb{R}} = \langle \mathbf{w}_1, \ldots, \mathbf{w}_{i-1}, \mathbf{w}_i \rangle_{\mathbb{R}}.$$

Then, to conclude that $\{\mathbf{v}_1, \dots, \mathbf{v}_i\}$ is an orthogonal basis of $\langle \mathbf{w}_1, \dots, \mathbf{w}_i \rangle_{\mathbb{R}}$, it remains to show that this is an orthogonal set (by Proposition 10.1.10). For this, it suffices to show that $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ for $j = 1, \dots, i-1$. By (10.2), we see that

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \langle \mathbf{w}_i, \mathbf{v}_j \rangle - \sum_{k=1}^{i-1} \frac{\langle \mathbf{w}_i, \mathbf{v}_k \rangle}{\langle \mathbf{v}_k, \mathbf{v}_k \rangle} \langle \mathbf{v}_k, \mathbf{v}_j \rangle = 0$$

for $j = 1, \dots, i-1$. This completes the proof. □

We end this section with a review of the notion of orthogonal complement and two related results.

Definition 10.1.12 (Orthogonal complement). The *orthogonal complement* of a subspace W of V is

$$W^{\perp} := \{\mathbf{v} \in V \,;\, \langle \mathbf{v}, \mathbf{w} \rangle = 0 \text{ for all } \mathbf{w} \in W\}.$$

Proposition 10.1.13. *Let W be a subspace of V. Then $W^{\perp}$ is a subspace of V that satisfies $W \cap W^{\perp} = \{\mathbf{0}\}$. Furthermore, if $W = \langle \mathbf{w}_1, \dots, \mathbf{w}_m \rangle_{\mathbb{R}}$, then*

$$W^{\perp} = \{\mathbf{v} \in V \,;\, \langle \mathbf{v}, \mathbf{w}_i \rangle = 0 \textit{ for } i = 1, \dots, m\}.$$

Proof. We leave it as an exercise to show that $W^{\perp}$ is a subspace of V. We note that, if $\mathbf{w} \in W \cap W^{\perp}$, then we have $\langle \mathbf{w}, \mathbf{w} \rangle = 0$ and so $\mathbf{w} = 0$. This shows that $W \cap W^{\perp} = \{\mathbf{0}\}$. Finally, if $W = \langle \mathbf{w}_1, \dots, \mathbf{w}_m \rangle$, we see that

$$\begin{aligned} \mathbf{v} \in W^{\perp} &\iff \langle \mathbf{v}, a_1\mathbf{w}_1 + \cdots + a_m\mathbf{w}_m \rangle = 0 \quad \forall\, a_1, \dots, a_m \in \mathbb{R} \\ &\iff a_1\langle \mathbf{v}, \mathbf{w}_1 \rangle + \cdots + a_m\langle \mathbf{v}, \mathbf{w}_m \rangle = 0 \quad \forall\, a_1, \dots, a_m \in \mathbb{R} \\ &\iff \langle \mathbf{v}, \mathbf{w}_1 \rangle = \cdots = \langle \mathbf{v}, \mathbf{w}_m \rangle = 0, \end{aligned}$$

and thus the final assertion of the proposition follows. □

It follows from Proposition 10.1.13 that $V^{\perp} = \{0\}$. In other words, for $v \in V$, we have

$$v = 0 \iff \langle u, v \rangle = 0 \text{ for all } u \in V.$$

Theorem 10.1.14. *Let W be a finite-dimensional subspace of V. Then we have:*

$$V = W \oplus W^{\perp}.$$

Proof. Since, by Proposition 10.1.13, we have $W \cap W^{\perp} = \{\mathbf{0}\}$, it remains to show that $V = W + W^{\perp}$. Let $\{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ be an orthogonal basis of W (such a basis exists since W is finite-dimensional). Given $\mathbf{v} \in V$, we set

$$\mathbf{w} = \frac{\langle \mathbf{v}, \mathbf{w}_1 \rangle}{\langle \mathbf{w}_1, \mathbf{w}_1 \rangle}\mathbf{w}_1 + \cdots + \frac{\langle \mathbf{v}, \mathbf{w}_m \rangle}{\langle \mathbf{w}_m, \mathbf{w}_m \rangle}\mathbf{w}_m. \tag{10.3}$$

For $i = 1, \ldots, m$, we see that

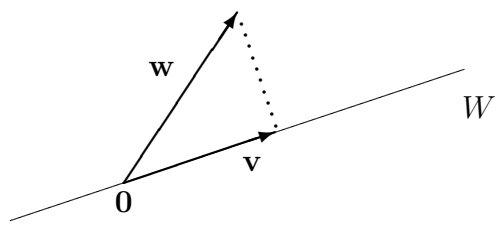
$$\langle \mathbf{v} - \mathbf{w}, \mathbf{w}_i \rangle = \langle \mathbf{v}, \mathbf{w}_i \rangle - \langle \mathbf{w}, \mathbf{w}_i \rangle = 0,$$

thus $\mathbf{v} - \mathbf{w} \in W^\perp$, and so

$$\mathbf{v} = \mathbf{w} + (\mathbf{v} - \mathbf{w}) \in W + W^\perp.$$

Since the choice $\mathbf{v} \in V$ is arbitrary, this shows that $V = W + W^\perp$, as claimed. □

If W is a finite-dimensional subspace of V, Theorem 10.1.14 tells us that, for all $\mathbf{v} \in V$, there exists a unique vector $\mathbf{w} \in W$ such that $\mathbf{v} - \mathbf{w} \in W^\perp$.



We say that this vector $\mathbf{w}$ is the *orthogonal projection* of $\mathbf{v}$ on W. If $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ is an orthogonal basis of W, then this projection $\mathbf{w}$ is given by (10.3).

Example 10.1.15. Calculate the orthogonal projection of $\mathbf{v} = (0, 1, 1, 0)^t$ on the subspace W of $\mathbb{R}^4$ generated by $\mathbf{w}_1 = (1, 1, 0, 0)^t$ and $\mathbf{w}_2 = (1, 1, 1, 1)^t$.

Solution: We first apply the Gram-Schmidt algorithm to the basis $\{\mathbf{w}_1, \mathbf{w}_2\}$ of W. We obtain

$$\begin{aligned} \mathbf{v}_1 &= \mathbf{w}_1 = (1, 1, 0, 0)^t \\ \mathbf{v}_2 &= \mathbf{w}_2 - \frac{\langle \mathbf{w}_2, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \mathbf{v}_1 = (1, 1, 1, 1)^t - \frac{2}{2}(1, 1, 0, 0)^t = (0, 0, 1, 1)^t. \end{aligned}$$

Thus $\{\mathbf{v}_1, \mathbf{v}_2\}$ is an orthogonal basis of W. The orthogonal projection of $\mathbf{v}$ on W is therefore

$$\frac{\langle \mathbf{v}, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \mathbf{v}_1 + \frac{\langle \mathbf{v}, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_2, \mathbf{v}_2 \rangle} \mathbf{v}_2 = \frac{1}{2}\mathbf{v}_1 + \frac{1}{2}\mathbf{v}_2 = \frac{1}{2}(1, 1, 1, 1)^t.$$

Exercises.

10.1.1. Show that $\mathcal{B} = \{(1, -1, 3)^t, (-2, 1, 1)^t, (4, 7, 1)^t\}$ is an orthogonal basis of $\mathbb{R}^3$ and calculate $[(a, b, c)^t]_{\mathcal{B}}$.

10.1.2. Find $a, b, c \in \mathbb{R}$ such that the set

$$\{(1, 2, 1, 0)^t, (1, -1, 1, 3)^t, (2, -1, 0, -1)^t, (a, b, c, 1)^t\}$$

is an orthogonal basis of $\mathbb{R}^4$.

10.1.3. Let U and V be inner product spaces equipped with inner products $\langle\ ,\ \rangle_U$ and $\langle\ ,\ \rangle_V$ respectively. Show that the formula

$$\big\langle(\mathbf{u}_1, \mathbf{v}_1),\, (\mathbf{u}_2, \mathbf{v}_2)\big\rangle = \langle \mathbf{u}_1, \mathbf{u}_2\rangle_U + \langle \mathbf{v}_1, \mathbf{v}_2\rangle_V$$

defines an inner product on $U \times V$ for which $(U \times \{0\})^\perp = \{0\} \times V$.

10.1.4. Let V be an inner product space of dimension n equipped with an inner product $\langle\ ,\ \rangle$.

(i) Verify that, for each $\mathbf{u} \in V$, the function $f_{\mathbf{u}} \colon V \to \mathbb{R}$ given by

$$f_{\mathbf{u}}(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v}\rangle \quad \text{for all } \mathbf{v} \in V$$

belongs to V^*. Then verify that the map $\varphi \colon V \to V^*$ given by $\varphi(\mathbf{u}) = f_{\mathbf{u}}$ for all $\mathbf{u} \in V$ is an isomorphism of vector spaces over $\mathbb{R}$.

(ii) Let $\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ be an orthonormal basis of V. Show that the basis of V^* dual to $\mathcal{B}$ is $\mathcal{B}^* = \{f_1, \ldots, f_n\}$, where $f_i := \varphi(\mathbf{u}_i) = f_{\mathbf{u}_i}$ for $i = 1, \ldots, n$.

10.1.5. Let V be the vector space of continuous functions $f \colon \mathbb{R} \to \mathbb{R}$ that are 2π-periodic.

(i) Show that the formula

$$\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)\mathrm{d}x$$

defines an inner product on V.

(ii) Show that $\{1, \sin(x), \cos(x)\}$ is an orthogonal subset of V for this inner product.

(iii) Let $f \colon \mathbb{R} \to \mathbb{R}$ be the periodic "sawtooth" function given on $[0, 2\pi]$ by

$$f(x) = \begin{cases} x & \text{if } 0 \le x \le \pi, \\ 2\pi - x & \text{if } \pi \le x \le 2\pi, \end{cases}$$

and extended by periodicity to all of $\mathbb{R}$. Calculate the projection of f on the subspace W of V generated by $\{1, \sin(x), \cos(x)\}$.

10.1.6. Let $V = \mathrm{Mat}_{n\times n}(\mathbb{R})$.

(i) Show that the formula $\langle A\,,\, B\rangle = \mathrm{trace}(AB^t)$ defines an inner product on V.

(ii) For $n = 3$, find an orthonormal basis of the subspace $S = \{A \in V\,;\, A^t = A\}$ of symmetric matrices.

10.1.7. Consider the vector space $\mathcal{C}[-1,1]$ of continuous functions from $[-1,1]$ to $\mathbb{R}$, equipped with the inner product

$$\langle f, g\rangle = \int_{-1}^{1} f(x)g(x)\,dx\,.$$

Find an orthogonal basis of the subspace $V = \langle\, 1, x, x^2 \,\rangle_{\mathbb{R}}$.

10.1.8. Let W be the subspace of $\mathbb{R}^4$ generated by $(1,-1,0,1)^t$ and $(1,1,0,0)^t$. Find a basis of $W^\perp$.

10.1.9. Let W_1 and W_2 be subspaces of a finite-dimensional inner product space V. Show that $W_1 \subseteq W_2$ if and only if $W_2^\perp \subseteq W_1^\perp$.

10.2 Orthogonal operators

In this section, we fix an inner product space V of finite dimension n, and an orthonormal basis $\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ of V. We first note:

Lemma 10.2.1. *For all $\mathbf{u}, \mathbf{v} \in V$, we have*

$$\langle \mathbf{u}, \mathbf{v}\rangle = \big([\mathbf{u}]_{\mathcal{B}}\big)^t\,[\mathbf{v}]_{\mathcal{B}}.$$

Proof. Let $\mathbf{u}, \mathbf{v} \in V$. Write

$$\mathbf{u} = \sum_{i=1}^{n} a_i\mathbf{u}_i \quad \text{and} \quad \mathbf{v} = \sum_{i=1}^{n} b_i\mathbf{u}_i$$

with $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$. We have

$$\langle \mathbf{u}, \mathbf{v}\rangle = \left\langle \sum_{i=1}^{n} a_i\mathbf{u}_i, \sum_{j=1}^{n} b_j\mathbf{v}_j \right\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} a_ib_j\langle \mathbf{u}_i, \mathbf{v}_j\rangle = \sum_{i=1}^{n} a_ib_i$$

since $\langle \mathbf{u}_i, \mathbf{u}_j\rangle = \delta_{ij}$. In matrix form, this equality can be rewritten

$$\langle \mathbf{u}, \mathbf{v}\rangle = (a_1, \ldots, a_n)\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = [\mathbf{u}]_{\mathcal{B}}^t\,[\mathbf{v}]_{\mathcal{B}}.$$

□

Using this lemma, we can now show:

Proposition 10.2.2. *Let $T\colon V \to V$ be a linear operator. The following conditions are equivalent:*

(i) $\|T(\mathbf{u})\| = 1$ *for all* $\mathbf{u} \in V$ *with* $\|\mathbf{u}\| = 1$,

(ii) $\|T(\mathbf{v})\| = \|\mathbf{v}\|$ *for all* $\mathbf{v} \in V$,

(iii) $\langle T(\mathbf{u}), T(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$ *for all* $\mathbf{u}, \mathbf{v} \in V$,

(iv) $\{T(\mathbf{u}_1), \ldots, T(\mathbf{u}_n)\}$ *is an orthonormal basis of* V,

(v) $[\,T\,]_{\mathcal{B}}^t\,[\,T\,]_{\mathcal{B}} = I_n$,

(vi) $[\,T\,]_{\mathcal{B}}$ *is invertible and* $[\,T\,]_{\mathcal{B}}^{-1} = [\,T\,]_{\mathcal{B}}^t$.

Proof. (i)$\Longrightarrow$(ii): Suppose first that $T(\mathbf{u})$ is a unit vector for every unit vector $\mathbf{u}$ in V. Let $\mathbf{v}$ be an arbitrary vector in V. If $\mathbf{v} \neq \mathbf{0}$, then $\mathbf{u} := \|\mathbf{v}\|^{-1}\mathbf{v}$ is a unit vector, hence $T(\mathbf{u}) = \|\mathbf{v}\|^{-1}T(\mathbf{v})$ is a unit vector and so $\|T(\mathbf{v})\| = \|\mathbf{v}\|$. If $\mathbf{v} = \mathbf{0}$, we have $T(\mathbf{v}) = \mathbf{0}$ and then the equality $\|T(\mathbf{v})\| = \|\mathbf{v}\|$ is again verified.

(ii)$\Longrightarrow$(iii): Suppose that $\|T(\mathbf{v})\| = \|\mathbf{v}\|$ for all $\mathbf{v} \in V$. Let $\mathbf{u}, \mathbf{v}$ be arbitrary vectors in V. We have

$$\begin{aligned} \|\mathbf{u}+\mathbf{v}\|^2 &= \langle \mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v}\rangle \\ &= \langle \mathbf{u}, \mathbf{u}\rangle + 2\langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{v}, \mathbf{v}\rangle \\ &= \|\mathbf{u}\|^2 + 2\langle \mathbf{u}, \mathbf{v}\rangle + \|\mathbf{v}\|^2. \end{aligned} \tag{10.4}$$

Applying this formula to $T(\mathbf{u}) + T(\mathbf{v})$, we obtain

$$\|T(\mathbf{u}) + T(\mathbf{v})\|^2 = \|T(\mathbf{u})\|^2 + 2\langle T(\mathbf{u}), T(\mathbf{v})\rangle + \|T(\mathbf{v})\|^2. \tag{10.5}$$

Since $\|T(\mathbf{u}) + T(\mathbf{v})\| = \|T(\mathbf{u}+\mathbf{v})\| = \|\mathbf{u}+\mathbf{v}\|$, $\|T(\mathbf{u})\| = \|\mathbf{u}\|$ and $\|T(\mathbf{v})\| = \|\mathbf{v}\|$, comparing (10.4) and (10.5) gives $\langle T(\mathbf{u}), T(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$.

(iii)$\Longrightarrow$(iv): Suppose that $\langle T(\mathbf{u}), T(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$ for all $\mathbf{u}, \mathbf{v} \in V$. Since $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is an orthonormal basis of V, we deduce that

$$\langle T(\mathbf{u}_i), T(\mathbf{u}_j)\rangle = \langle \mathbf{u}_i, \mathbf{u}_j\rangle = \delta_{ij} \quad (1 \leq i, j \leq n).$$

Thus $\{T(\mathbf{u}_1), \ldots, T(\mathbf{u}_n)\}$ is an orthogonal subset of V consisting of unit vectors. By Proposition 10.1.10(i), this set is linearly independent. Since it consists of n vectors and V is of dimension n, it is a basis of V, hence an orthonormal basis of V.

(iv)$\Longrightarrow$(v): Suppose that $\{T(\mathbf{u}_1), \ldots, T(\mathbf{u}_n)\}$ is an orthonormal basis of V. Let $i, j \in \{1, \ldots, n\}$. By Lemma 10.2.1, we have

$$\delta_{ij} = \langle T(\mathbf{u}_i), T(\mathbf{u}_j)\rangle = [T(\mathbf{u}_i)]_{\mathcal{B}}^t\,[T(\mathbf{u}_j)]_{\mathcal{B}}.$$

Now, $[T(\mathbf{u}_i)]_{\mathcal{B}}^t$ is the i-th row of the matrix $[\,T\,]_{\mathcal{B}}^t$, and $[T(\mathbf{u}_j)]_{\mathcal{B}}$ is the j-th column of $[\,T\,]_{\mathcal{B}}$. Thus $[T(\mathbf{u}_i)]_{\mathcal{B}}^t\,[T(\mathbf{u}_j)]_{\mathcal{B}} = \delta_{ij}$ is the entry in row i and column j of $[\,T\,]_{\mathcal{B}}^t\,[\,T\,]_{\mathcal{B}}$. Since the choice of $i, j \in \{1, \ldots, n\}$ was arbitrary, this implies that $[\,T\,]_{\mathcal{B}}^t\,[\,T\,]_{\mathcal{B}} = I$.

(v)$\Longrightarrow$(vi): Suppose that $[\,T\,]_{\mathcal{B}}^t\,[\,T\,]_{\mathcal{B}} = I$. Then $[\,T\,]_{\mathcal{B}}$ is invertible with inverse $[\,T\,]_{\mathcal{B}}^t$.

(vi)$\Longrightarrow$(i): Finally, suppose that $[\,T\,]_{\mathcal{B}}$ is invertible and that $[\,T\,]_{\mathcal{B}}^{-1} = [\,T\,]_{\mathcal{B}}^{t}$. If $\mathbf{u}$ is an arbitrary unit vector in V, we see, by Lemma 10.2.1, that

$$\begin{aligned}\|T(\mathbf{u})\|^2 &= \langle T(\mathbf{u}), T(\mathbf{u})\rangle = [T(\mathbf{u})]_{\mathcal{B}}^{t}\,[T(\mathbf{u})]_{\mathcal{B}} \\ &= ([\,T\,]_{\mathcal{B}}[\mathbf{u}]_{\mathcal{B}})^{t}\,([\,T\,]_{\mathcal{B}}[\mathbf{u}]_{\mathcal{B}}) = [\mathbf{u}]_{\mathcal{B}}^{t}\,[\,T\,]_{\mathcal{B}}^{t}\,[\,T\,]_{\mathcal{B}}[\mathbf{u}]_{\mathcal{B}} = [\mathbf{u}]_{\mathcal{B}}^{t}\,[\mathbf{u}]_{\mathcal{B}} = \langle \mathbf{u}, \mathbf{u}\rangle = \|\mathbf{u}\|^2 = 1.\end{aligned}$$

Thus $T(\mathbf{u})$ is also a unit vector. □

Definition 10.2.3 (Orthogonal operator, orthogonal matrix).

- A linear operator $T\colon V \to V$ satisfying the equivalent conditions of Proposition 10.2.2 is called a *orthogonal operator* or a *real unitary operator*.
- An invertible matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ such that $A^{-1} = A^{t}$ is called an *orthogonal matrix*.

Condition (i) of Proposition 10.2.2 requires that T sends the set of unit vectors in V to itself. This explains the terminology of a unitary operator.

Condition (iii) of Proposition 10.2.2 means that T preserves the inner product. In particular, this requires that T maps each pair of orthogonal vectors $\mathbf{u}, \mathbf{v}$ in V to another pair of orthogonal vectors. For this reason, we say that such an operator is orthogonal.

Finally, condition (vi) means:

Corollary 10.2.4. *A linear operator $T\colon V \to V$ is orthogonal if and only if its matrix relative to an <u>orthonormal</u> basis of V is an orthogonal matrix.*

Example 10.2.5. The following linear operators are orthogonal:

- a rotation about the origin in $\mathbb{R}^2$,
- a reflection in a line passing through the origin in $\mathbb{R}^2$,
- a rotation about a line passing through the origin in $\mathbb{R}^3$,
- a reflection in a plane passing through the origin in $\mathbb{R}^3$.

Definition 10.2.6 ($\mathcal{O}(V)$, $\mathcal{O}_n(\mathbb{R})$). We denote by $\mathcal{O}(V)$ the set of orthogonal operators on V and by $\mathcal{O}_n(\mathbb{R})$ the set of orthogonal $n \times n$ matrices.

We leave it as an exercise to show that $\mathcal{O}(V)$ is a subgroup of $\mathrm{GL}(V) = \mathrm{End}_K(V)^{\times}$, that $\mathcal{O}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R}) = \mathrm{Mat}_{n\times n}(\mathbb{R})^{\times}$, and that these two groups are isomorphic.

Example 10.2.7. Let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operator whose matrix relative to the standard basis $\mathcal{E}$ of $\mathbb{R}^3$ is

$$[\,T\,]_{\mathcal{E}} = \frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}.$$

Show that T is an orthogonal operator.

Solution: Since $\mathcal{E}$ is an orthonormal basis of $\mathbb{R}^3$, it suffices to show that $[\,T\,]_{\mathcal{E}}$ is an orthogonal matrix. We have

$$[\,T\,]_{\mathcal{E}}^t\,[\,T\,]_{\mathcal{E}} = \frac{1}{9}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix} = I,$$

hence $[\,T\,]_{\mathcal{E}}^{-1} = [\,T\,]_{\mathcal{E}}^t$, as required.

Exercises.

10.2.1. Let $T\colon V \to V$ be an orthogonal operator. Show that T preserves angles, that is, if $\mathbf{u}$ and $\mathbf{v}$ are nonzero vectors in V, the angle between $T(\mathbf{u})$ and $T(\mathbf{v})$ is equal to the angle between $\mathbf{u}$ and $\mathbf{v}$.

10.2.2. Let $T\colon V \to V$ be an invertible linear operator. Show that the following conditions are equivalent:

(i) $\langle T(\mathbf{u}), T(\mathbf{v})\rangle = 0$ for all $\mathbf{u}, \mathbf{v} \in V$ satisfying $\langle \mathbf{u}, \mathbf{v}\rangle = 0$.

(ii) $T = c\,S$ for a (real) unitary operator $S\colon V \to V$ and a real number $c \neq 0$.

Note. The above shows that we cannot define an orthogonal operator to be a linear operator that preserves orthogonality. In this sense, the terminology of a unitary operator is more appropriate.

10.2.3. Let $\mathcal{E}$ be an orthonormal basis of V and let $\mathcal{B}$ be an arbitrary basis of V. Show that the change of basis matrix $P = [\,I\,]_{\mathcal{E}}^{\mathcal{B}}$ is orthogonal if and only if $\mathcal{B}$ is also an orthonormal basis.

10.2.4. Let $T\colon V \to V$ be an orthogonal operator. Suppose that W is a T-invariant subspace of V. Show that $W^{\perp}$ is also T-invariant.

10.2.5. Let $T\colon V \to V$ be an orthogonal operator. Show that $\det(T) = \pm 1$.

10.2.6. Let V be an inner product space of dimension n. Show that $\mathcal{O}(V)$ is a subgroup of $\mathrm{GL}(V) = \mathrm{End}_K(V)^\times$, that $\mathcal{O}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R}) = \mathrm{Mat}_{n\times n}(\mathbb{R})^\times$, and define an isomorphism $\varphi\colon \mathcal{O}(V) \xrightarrow{\sim} \mathcal{O}_n(\mathbb{R})$.

10.2.7. Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be an orthogonal matrix. Show that the columns of A form an orthonormal basis of $\mathbb{R}^n$.

10.2.8. Let V and W be arbitrary inner product spaces. Suppose that there exists a function $T\colon V \to W$ such that $T(\mathbf{0}) = \mathbf{0}$ and $\|T(\mathbf{v}_1) - T(\mathbf{v}_2)\| = \|\mathbf{v}_1 - \mathbf{v}_2\|$ for all $\mathbf{v}_1, \mathbf{v}_2 \in V$.

(i) Show that $\langle T(\mathbf{v}_1), T(\mathbf{v}_2)\rangle = \langle \mathbf{v}_1, \mathbf{v}_2\rangle$ for all $\mathbf{v}_1, \mathbf{v}_2 \in V$.

(ii) Deduce that $\|c_1T(\mathbf{v}_1) + c_2T(\mathbf{v}_2)\| = \|c_1\mathbf{v}_1 + c_2\mathbf{v}_2\|$ for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $c_1, c_2 \in \mathbb{R}$.

(iii) Conclude that, for all $\mathbf{v} \in V$ and $c \in \mathbb{R}$, we have $\|T(c\,\mathbf{v}) - c\,T(\mathbf{v})\| = 0$, hence $T(c\,\mathbf{v}) = c\,T(\mathbf{v})$.

(iv) Using similar reasoning, show that, for all vectors $\mathbf{v}_1, \mathbf{v}_2 \in V$, we have $\|T(\mathbf{v}_1 + \mathbf{v}_2) - T(\mathbf{v}_1) - T(\mathbf{v}_2)\|$=0, hence $T(\mathbf{v}_1 + \mathbf{v}_2) = T(\mathbf{v}_1) + T(\mathbf{v}_2)$.

(v) Conclude that T is a linear map. In particular, show that if $V = W$ is finite-dimensional, then T is an orthogonal operator in the sense of Definition 10.2.3.

A function $T\colon V \to W$ satisfying the conditions given at the beginning of this exercise is called an *isometry*.

Hint. For (i), use formula (10.4) with $\mathbf{u} = T(\mathbf{v}_1)$ and $\mathbf{v} = -T(\mathbf{v}_2)$, then with $\mathbf{u} = \mathbf{v}_1$ and $\mathbf{v} = -\mathbf{v}_2$. For (ii), use the same formula with $\mathbf{u} = c_1T(\mathbf{v}_1)$ and $\mathbf{v} = c_2T(\mathbf{v}_2)$, then with $\mathbf{u} = c_1\mathbf{v}_1$ and $\mathbf{v} = c_2\mathbf{v}_2$.

10.3 The adjoint operator

Using the same notation as in the preceding section, we first show:

Theorem 10.3.1. *Let $B\colon V \times V \to \mathbb{R}$ be a bilinear form on V. There exists a unique pair of linear operators S and T on V such that*

$$B(\mathbf{u}, \mathbf{v}) = \langle T(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, S(\mathbf{v})\rangle \tag{10.6}$$

for all $\mathbf{u}, \mathbf{v} \in V$. Furthermore, let $\mathcal{E}$ be an orthonormal basis of V and let M be the matrix of B relative to the basis $\mathcal{E}$. Then we have

$$[\,S\,]_{\mathcal{E}} = M \quad \text{and} \quad [\,T\,]_{\mathcal{E}} = M^t. \tag{10.7}$$

Proof. **1st Existence.** Let S and T be linear operators on V determined by conditions (10.7), and let $\mathbf{u}, \mathbf{v} \in V$. Since M is the matrix of V in the basis $\mathcal{E}$, we have

$$B(\mathbf{u}, \mathbf{v}) = [\mathbf{u}]_{\mathcal{E}}^t \, M[\mathbf{v}]_{\mathcal{E}}.$$

Since $[T(\mathbf{u})]_{\mathcal{E}} = M^t \, [\mathbf{u}]_{\mathcal{E}}$ and $[S(\mathbf{v})]_{\mathcal{E}} = M[\mathbf{v}]_{\mathcal{E}}$, Lemma 10.2.1 gives

$$\begin{aligned} \langle T(\mathbf{u}), \mathbf{v} \rangle &= \left(M^t \, [\mathbf{u}]_{\mathcal{E}}\right)^t [\mathbf{v}]_{\mathcal{E}} = [\mathbf{u}]_{\mathcal{E}}^t \, M[\mathbf{v}]_{\mathcal{E}} = B(\mathbf{u}, \mathbf{v}) \\ \textit{and} \quad \langle \mathbf{u}, S(\mathbf{v}) \rangle &= [\mathbf{u}]_{\mathcal{E}}^t \, (M[\mathbf{v}]_{\mathcal{E}}) = B(\mathbf{u}, \mathbf{v}), \end{aligned}$$

as required.

2nd Uniqueness. Suppose that S', T' are arbitrary linear operators on V such that

$$B(\mathbf{u}, \mathbf{v}) = \langle T'(\mathbf{u}), \mathbf{v} \rangle = \langle \mathbf{u}, S'(\mathbf{v}) \rangle$$

for all $\mathbf{u}, \mathbf{v} \in V$. By subtracting these equalities from (10.6), we get

$$0 = \langle T'(\mathbf{u}) - T(\mathbf{u}), \mathbf{v} \rangle = \langle \mathbf{u}, S'(\mathbf{v}) - S(\mathbf{v}) \rangle$$

for all $\mathbf{u}, \mathbf{v} \in V$. We deduce that, for all $\mathbf{u} \in V$, we have

$$T'(\mathbf{u}) - T(\mathbf{u}) \in V^{\perp} = \{\mathbf{0}\},$$

hence $T'(\mathbf{u}) = T(\mathbf{u})$ and so $T' = T$. Similarly, we see that $S' = S$. □

Corollary 10.3.2. *For any linear operator T on V, there exists a unique linear operator on V, denoted T^*, such that*

$$\langle T(\mathbf{u}), \mathbf{v} \rangle = \langle \mathbf{u}, T^*(\mathbf{v}) \rangle$$

for all $\mathbf{u}, \mathbf{v} \in V$. If $\mathcal{E}$ is an orthonormal basis of V, we have $[T^*]_{\mathcal{E}} = [\,T\,]_{\mathcal{E}}^t$.

Proof. The function $B \colon V \times V \to \mathbb{R}$ given by $B(\mathbf{u}, \mathbf{v}) = \langle T(\mathbf{u}), \mathbf{v} \rangle$ for all $(\mathbf{u}, \mathbf{v}) \in V \times V$ is bilinear (exercise). To conclude, it suffices to apply Theorem 10.3.1 to this bilinear form. □

Definition 10.3.3 (Adjoint, symmetric, self-adjoint). Let T be a linear operator on V. The operator $T^* \colon V \to V$ defined by Corollary 10.3.2 is called the *adjoint* of T. We say that T is *symmetric* of *self-adjoint* if $T^* = T$.

By Corollary 10.3.2, we immediately obtain:

Proposition 10.3.4. *Let $T \colon V \to V$ be a linear operator. The following conditions are equivalent:*

(i) T is symmetric,

(ii) $\langle T(\mathbf{u}), \mathbf{v} \rangle = \langle \mathbf{u}, T(\mathbf{v}) \rangle$ for all $\mathbf{u}, \mathbf{v} \in V$,

(iii) there exists an orthonormal basis $\mathcal{E}$ of V such that $[\,T\,]_{\mathcal{E}}$ is a symmetric matrix,

(iv) $[\,T\,]_{\mathcal{E}}$ *is a symmetric matrix for every orthonormal basis* $\mathcal{E}$ *of* V.

The proof of the following properties is left as an exercise.

Proposition 10.3.5. *Let* S *and* T *be linear operators on* V*, and let* $c \in \mathbb{R}$*. We have:*

(i) $(c\,T)^* = c\,T^*$,

(ii) $(S+T)^* = S^* + T^*$,

(iii) $(S \circ T)^* = T^* \circ S^*$,

(iv) $(T^*)^* = T$.

(v) Furthermore, if T *is invertible, then* T^* *is also invertible and* $(T^*)^{-1} = (T^{-1})^*$.

Properties (i) and (ii) imply that the map

$$\begin{array}{rcl} \mathrm{End}_{\mathbb{R}}(V) & \longrightarrow & \mathrm{End}_{\mathbb{R}}(V) \\ T & \longmapsto & T^* \end{array}$$

is *linear*. Properties (ii) and (iii) can be summarized by saying that $T \mapsto T^*$ is a *ring anti-homomorphism* of $\mathrm{End}_{\mathbb{R}}(V)$. More precisely, because of (iv), we say that it is a ring *anti-involution*.

Example 10.3.6. Every symmetric matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ defines a symmetric operator on $\mathbb{R}^n$

$$\begin{array}{rrcl} T_A: & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & X & \longmapsto & A\,X \end{array}.$$

We can verify this directly from the definition by noting that, for all $X, Y \in \mathbb{R}^n$, we have

$$\langle T_A(X), Y\rangle = (A\,X)^t\,Y = X^t\,A^t\,Y = X^t\,A\,Y = \langle X, T_A(Y)\rangle.$$

This also follows from Proposition 10.3.4. Indeed, since the standard basis $\mathcal{E}$ of $\mathbb{R}^n$ is orthonormal and $[\,T_A\,]_{\mathcal{E}} = A$ is a symmetric matrix, the linear operator T_A is symmetric.

Example 10.3.7. Let W be a subspace of V, and let $P\colon V \to V$ be the orthogonal projection on W (that is, the linear map that sends $\mathbf{v} \in V$ to its orthogonal projection on W). Then P is a symmetric operator.

Theorem 10.1.14 shows that $V = W \oplus W^{\perp}$. The function P is simply the projection on the first factor of this sum followed by the inclusion of W into V. Let $\mathbf{u}, \mathbf{v}$ be arbitrary vectors in V. We have

$$\langle P(\mathbf{u}), \mathbf{v}\rangle = \langle P(\mathbf{u})\,,\,(\mathbf{v} - P(\mathbf{v})) + P(\mathbf{v})\rangle = \langle P(\mathbf{u})\,,\,\mathbf{v} - P(\mathbf{v})\rangle + \langle P(\mathbf{u}), P(\mathbf{v})\rangle.$$

Since $P(\mathbf{u}) \in W$ and $\mathbf{v} - P(\mathbf{v}) \in W^{\perp}$, we have $\langle P(\mathbf{u}), \mathbf{v} - P(\mathbf{v})\rangle = 0$ and the last equality can be rewritten

$$\langle P(\mathbf{u}), \mathbf{v}\rangle = \langle P(\mathbf{u}), P(\mathbf{v})\rangle.$$

A similar calculation gives

$$\langle \mathbf{u}, P(\mathbf{v})\rangle = \langle P(\mathbf{u}), P(\mathbf{v})\rangle.$$

Thus, we have $\langle \mathbf{u}, P(\mathbf{v})\rangle = \langle P(\mathbf{u}), \mathbf{v}\rangle$, which shows that P is symmetric.

Exercises.

10.3.1. Prove Proposition 10.3.5.

10.3.2. Let $T\colon V \to V$ be a linear operator. Show that $\ker(T^*) = (\mathrm{Im}(T))^\perp$ and that $\mathrm{Im}(T^*) = (\ker(T))^\perp$.

10.3.3. Let $T\colon V \to V$ be a linear operator. Show that T is an orthogonal operator if and only if $T^* \circ T = I$.

10.3.4. We know that $V = \mathrm{Mat}_{n\times n}(\mathbb{R})$ is an inner product space for the inner product $\langle A, B\rangle = \mathrm{trace}(AB^t)$ (see Exercise 10.1.6). Fix $C \in V$ and consider the linear operator $T\colon V \to V$ given by $T(A) = CA$ for all $A \in V$. Show that the adjoint T^* of T is given by $T^*(A) = C^t A$ for all $A \in V$.

Hint. Use the fact that $\mathrm{trace}(AB) = \mathrm{trace}(BA)$ for all $A, B \in V$.

10.4 Spectral theorems

We again fix an inner product space V of finite dimension $n \geq 1$. We first show that:

Lemma 10.4.1. *Let $T\colon V \to V$ be a linear operator on V. There exists a T-invariant subspace of V of dimension 1 or 2.*

Proof. We consider V as an $\mathbb{R}[x]$-module for the product $p(x)\mathbf{v} = p(T)(\mathbf{v})$. Let $\mathbf{v}$ be a nonzero element of V. By Proposition 7.1.7, the annihilator of $\mathbf{v}$ is generated by a monic polynomial $p(x) \in \mathbb{R}[x]$ of degree ≥ 1. Write $p(x) = q(x)a(x)$ where $q(x)$ is a monic irreducible factor of $p(x)$, and set $\mathbf{w} = a(x)\mathbf{v}$. Then the annihilator of $\mathbf{w}$ is the ideal of $\mathbb{R}[x]$ generated by $q(x)$. By Proposition 7.1.7, the submodule $W := \mathbb{R}[x]\mathbf{w}$ is a T-invariant subspace of V of dimension equal to the degree of $q(x)$. Now, Theorem 5.6.5 shows that all the irreducible polynomials of $\mathbb{R}[x]$ are of degree 1 or 2. Thus W is of dimension 1 or 2. $\square$

This lemma suggests the following definition:

Definition 10.4.2 (Minimal invariant subspace, irreducible invariant subspace). Let $T\colon V \to V$ be a linear operator on V. We say that a T-invariant subspace W of V is *minimal* or *irreducible* if $W \neq \{\mathbf{0}\}$ and if the only T-invariant subspaces of V contained in W are $\{\mathbf{0}\}$ and W.

It follows from this definition and Lemma 10.4.1 that every nonzero T-invariant subspace of V contains a minimal T-invariant subspace W, and that such a subspace W is of dimension 1 or 2.

For an orthogonal or symmetric operator, we have more:

Lemma 10.4.3. *Let $T\colon V \to V$ be an orthogonal or symmetric linear operator, and let W be a T-invariant subspace of V. Then $W^\perp$ is also T-invariant.*

Proof. Suppose first that T is orthogonal. Then $T|_W\colon W \to W$ is an orthogonal operator on W (it preserves the norm of the elements of W). Then $T|_W$ is invertible and, in particular, surjective. Thus $T(W) = W$.

Let $\mathbf{v} \in W^\perp$. For all $\mathbf{w} \in W$, we see that

$$\langle T(\mathbf{v}), T(\mathbf{w})\rangle = \langle \mathbf{v}, \mathbf{w}\rangle = 0,$$

thus $T(\mathbf{v}) \in (T(W))^\perp = W^\perp$. This shows that $W^\perp$ is T-invariant.

Now suppose that T is symmetric. Let $\mathbf{v} \in W^\perp$. For all $\mathbf{w} \in W$, we have

$$\langle T(\mathbf{v}), \mathbf{w}\rangle = \langle \mathbf{v}, T(\mathbf{w})\rangle = 0,$$

since $T(\mathbf{w}) \in W$. So we have $T(\mathbf{v}) \in W^\perp$. Since the choice of $\mathbf{v} \in W^\perp$ was arbitrary, this shows that $W^\perp$ is T-invariant. □

Lemma 10.4.3 immediately implies:

Proposition 10.4.4. *Let $T\colon V \to V$ be an orthogonal or symmetric linear operator. Then V is a direct sum of minimal T-invariant subspaces*

$$V = W_1 \oplus \cdots \oplus W_s$$

which are pairwise orthogonal, that is, such that $W_i \subseteq W_j^\perp$ for every pair of distinct integers i and j with $1 \le i, j \le s$.

To complete our analysis of symmetric or orthogonal linear operators $T\colon V \to V$, it thus suffices to study the restriction of T to a minimal T-invariant subspace. By Lemma 10.4.1, we know that such a subspace is of dimension 1 or 2. We begin with the case of an orthogonal operator.

Proposition 10.4.5. *Let $T\colon V \to V$ be an orthogonal operator, let W be a minimal T-invariant subspace of V, and let $\mathcal{B}$ be an orthonormal basis of W. Then either*

$$\dim_{\mathbb{R}}(W) = 1 \quad \textit{and} \quad [T|_W]_{\mathcal{B}} = (\pm 1)$$

for a choice of sign $\pm$, or

$$\dim_{\mathbb{R}}(W) = 2 \quad \textit{and} \quad [T|_W]_{\mathcal{B}} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

for some real number θ.

Proof. By Lemma 10.4.1, the subspace W is of dimension 1 or 2. Furthermore, the restriction $T|_W \colon W \to W$ of T to W is an orthogonal operator since $T|_W$ preserves the norm (see Definition 10.2.3). Thus $[T|_W]_{\mathcal{B}}$ is an orthogonal matrix, by Corollary 10.2.4.

1st If $\dim_{\mathbb{R}}(W) = 1$, then $[T|_W]_{\mathcal{B}} = (a)$ with $a \in \mathbb{R}$. Since $[T|_W]_{\mathcal{B}}$ is an orthogonal matrix, we must have $(a)^t(a) = 1$, hence $a^2 = 1$ and so $a = \pm 1$.

2nd If $\dim_{\mathbb{R}}(W) = 2$, then the columns of $[T|_W]_{\mathcal{B}}$ form an orthonormal basis of $\mathbb{R}^2$ (see Exercise 10.2.7), and so this matrix can be written

$$[T|_W]_{\mathcal{B}} = \begin{pmatrix} \cos(\theta) & -\epsilon\sin(\theta) \\ \sin(\theta) & \epsilon\cos(\theta) \end{pmatrix}$$

with $\theta \in \mathbb{R}$ and $\epsilon = \pm 1$. We deduce that

$$\mathrm{char}_{T|_W}(x) = \begin{vmatrix} x - \cos(\theta) & \epsilon\sin(\theta) \\ -\sin(\theta) & x - \epsilon\cos(\theta) \end{vmatrix} = x^2 - (1+\epsilon)\cos(\theta)x + \epsilon.$$

If $\epsilon = -1$, the polynomial becomes $\mathrm{char}_{T|_W}(x) = x^2 - 1 = (x-1)(x+1)$. Then 1 and -1 are the eigenvalues of $T|_W$, and for each of these eigenvalues, the operator $T|_W \colon W \to W$ has an eigenvector. But if $\mathbf{w} \in W$ is an eigenvector of $T|_W$ then $\mathbb{R}\mathbf{w}$ is a T-invariant subspace of V of dimension 1 contained in W, contradicting the hypothesis that W is a minimal T-invariant subspace. Therefore, we must have $\epsilon = 1$ and the proof is complete. □

In the case of a symmetric operator, the situation is even simpler.

Proposition 10.4.6. *Let $T \colon V \to V$ be a symmetric operator, and let W be a minimal T-invariant subspace of V. Then W is of dimension 1.*

Proof. We know that W is of dimension 1 or 2. Suppose that it is of dimension 2, and let $\mathcal{B}$ be an orthonormal basis of W. The restriction $T|_W \colon W \to W$ is a symmetric operator on W since for all $\mathbf{w}_1, \mathbf{w}_2 \in W$, we have

$$\langle T|_W(\mathbf{w}_1), \mathbf{w}_2\rangle = \langle T(\mathbf{w}_1), \mathbf{w}_2\rangle = \langle \mathbf{w}_1, T(\mathbf{w}_2)\rangle = \langle \mathbf{w}_1, T|_W(\mathbf{w}_2)\rangle.$$

Thus, by Proposition 10.3.4, the matrix $[T|_W]_{\mathcal{B}}$ is symmetric. It can therefore be written in the form

$$[T|_W]_{\mathcal{B}} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

with $a, b, c \in \mathbb{R}$. We then have

$$\mathrm{char}_{T|_W}(x) = \begin{vmatrix} x - a & -b \\ -b & x - c \end{vmatrix} = x^2 - (a+c)x + (ac - b^2).$$

The discriminant of this polynomial is

$$(a+c)^2 - 4(ac - b^2) = (a-c)^2 + 4b^2 \geq 0.$$

Thus $\mathrm{char}_{T|_W}(x)$ has at least one real root. This root is an eigenvalue of $T|_W$ and so it corresponds to an eigenvector $\mathbf{w}$. Then $\mathbb{R}\mathbf{w}$ is a T-invariant subspace of V contained in W, contradicting the minimality hypothesis on W. Thus W is necessarily of dimension 1. □

Combining the last three propositions, we obtain a description of orthogonal and symmetric operators on V.

Theorem 10.4.7. *Let $T\colon V \to V$ be a linear operator.*

(i) If T is orthogonal, there exists an orthonormal basis $\mathcal{B}$ of V such that $[\,T\,]_{\mathcal{B}}$ is block diagonal with blocks of the form

$$(1), \quad (-1) \quad \text{or} \quad \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \tag{10.8}$$

(with $\theta \in \mathbb{R}$) on the diagonal.

(ii) If T is symmetric, there exists an orthonormal basis $\mathcal{B}$ of V such that $[\,T\,]_{\mathcal{B}}$ is a diagonal matrix.

Result (ii) can be interpreted as saying that a symmetric operator is diagonalizable in an orthonormal basis.

Proof. By Proposition 10.4.4, the space V can be decomposed as a direct sum

$$V = W_1 \oplus \cdots \oplus W_s$$

of minimal T-invariant subspaces $W_1, \ldots, W_s$ which are pairwise orthogonal. Choose an orthonormal basis $\mathcal{B}_i$ of W_i for each $i = 1, \ldots, s$. Then

$$\mathcal{B} = \mathcal{B}_1 \amalg \cdots \amalg \mathcal{B}_s$$

is an orthonormal basis of V such that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} [\,T|_{W_1}\,]_{\mathcal{B}_1} & & 0 \\ & \ddots & \\ 0 & & [\,T|_{W_s}\,]_{\mathcal{B}_s} \end{pmatrix}.$$

If T is an orthogonal operator, Proposition 10.4.5 shows that each of the blocks $[\,T|_{W_i}\,]_{\mathcal{B}_i}$ on the diagonal is of the form (10.8). On the other hand, if T is symmetric, Proposition 10.4.6 shows that each W_i is of dimension 1. Thus, in this case, $[\,T|_{W}\,]_{\mathcal{B}}$ is diagonal. $\square$

Corollary 10.4.8. *Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a symmetric matrix. There exists an orthogonal matrix $P \in \mathcal{O}_n(\mathbb{R})$ such that $P^{-1}A\,P = P^t\,A\,P$ is diagonal.*

In particular, this corollary tells us that every real symmetric matrix is diagonalizable over $\mathbb{R}$.

Proof. Let $\mathcal{E}$ be the standard basis of $\mathbb{R}^n$ and let $T_A\colon \mathbb{R}^n \to \mathbb{R}^n$ be the linear operator associated to A, with matrix $[\,T_A\,]_{\mathcal{E}} = A$. Since A is symmetric and $\mathcal{E}$ is an orthonormal basis of $\mathbb{R}^n$, the operator T_A is symmetric (Proposition 10.3.4). Thus, by Theorem 10.4.7, there exists an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^n$ such that $[\,T_A\,]_{\mathcal{B}}$ is diagonal. Setting $P = [\,I\,]_{\mathcal{E}}^{\mathcal{B}}$, we have

$$[\,T_A\,]_{\mathcal{B}} = P^{-1}[\,T_A\,]_{\mathcal{E}}P = P^{-1}A\,P$$

(see Section 2.6). Finally, since $\mathcal{B}$ and $\mathcal{E}$ are two orthonormal basis of $\mathbb{R}^n$, Exercise 10.2.3 tells us that P is an orthogonal matrix, that is, invertible with $P^{-1} = P^t$. □

Example 10.4.9. Let $\mathcal{E}$ be the standard basis of $\mathbb{R}^3$ and let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operator whose matrix in the basis $\mathcal{E}$ is

$$[\,T\,]_{\mathcal{E}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

It is easily verified that $[\,T\,]_{\mathcal{E}}^t\,[\,T\,]_{\mathcal{E}} = I$. Since $\mathcal{E}$ is an orthonormal basis of $\mathbb{R}^3$, this implies that T is an orthogonal operator. We see that

$$\mathrm{char}_T(x) = \begin{vmatrix} x & 0 & -1 \\ -1 & x & 0 \\ 0 & -1 & x \end{vmatrix} = x^3 - 1 = (x-1)(x^2+x+1),$$

and so 1 is the only real eigenvalue of T. Since

$$[\,T\,]_{\mathcal{E}} - I = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

is of rank 2, we see that the eigenspace of T for the eigenvalue 1 is of dimension 1 and is generated by the unit vector

$$\mathbf{u}_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Then $W_1 = \langle \mathbf{u}_1 \rangle_{\mathbb{R}}$ is a T-invariant subspace of $\mathbb{R}^3$ and so we have a decomposition

$$\mathbb{R}^3 = W_1 \oplus W_1^{\perp}$$

where

$$W_1^{\perp} = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} ;\, x+y+z = 0 \right\}$$

is also a T-invariant subspace of $\mathbb{R}^3$. We see that

$$\left\{ \mathbf{u}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \mathbf{u}_3 = \frac{1}{\sqrt{6}}\begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} \right\}$$

is an orthonormal basis of $W_1^\perp$. Direction computation gives

$$T(\mathbf{u}_2) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} = -\frac{1}{2}\mathbf{u}_2 + \frac{\sqrt{3}}{2}\mathbf{u}_3, \quad T(\mathbf{u}_3) = \frac{1}{\sqrt{6}}\begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} = -\frac{\sqrt{3}}{2}\mathbf{u}_2 - \frac{1}{2}\mathbf{u}_3.$$

We also have $T(\mathbf{u}_1) = \mathbf{u}_1$ since $\mathbf{u}_1$ is an eigenvector of T for the eigenvalue 1. We conclude that $\mathcal{B} = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is an orthonormal basis of $\mathbb{R}^3$ such that

$$[\,T\,]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & -\sqrt{3}/2 \\ 0 & \sqrt{3}/2 & -1/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\pi/3) & -\sin(2\pi/3) \\ 0 & \sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix}.$$

We see from this matrix that T fixes each vector of the line W_1, while it performs a rotation through the angle $2\pi/3$ in the plane $W_1^\perp$. Thus T is a rotation through angle $2\pi/3$ about the line W_1.

Note. This latter description of T does not completely determine it since T^{-1} is also a rotation through an angle $2\pi/3$ about W_1. To distinguish T from T^{-1}, one must specify the direction of the rotation.

Exercises.

10.4.1. Let $R\colon \mathbb{R}^4 \to \mathbb{R}^4$ be the linear map whose matrix relative to the standard basis $\mathcal{E}$ of $\mathbb{R}^4$ is

$$[\,R\,]_{\mathcal{E}} = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

(i) Show that R is an orthogonal operator.

(ii) Find an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^3$ in which the matrix of R is block diagonal with blocks of size 1 or 2 on the diagonal, and give $[\,R\,]_{\mathcal{B}}$.

10.4.2. Let $A = \dfrac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$.

(i) Show that A is an orthogonal matrix.

(ii) Find an orthogonal matrix U for which the product $U^t\,A\,U$ is block diagonal with blocks of size 1 or 2 on the diagonal, and give this product (i.e. give this block diagonal matrix).

10.4.3. For each of the following matrices A, find an orthogonal matrix U such that $U^t\,A\,U$ is a diagonal matrix and give this diagonal matrix.

$$\text{(i) } A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \text{(ii) } A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \text{(iii) } A = \begin{pmatrix} 0 & 2 & -1 \\ 2 & 3 & -2 \\ -1 & -2 & 0 \end{pmatrix}.$$

10.4.4. Let T be a symmetric operator on an inner product space V of dimension n. Suppose that T has n distinct eigenvalues $\lambda_1, \ldots, \lambda_n$ and that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are respective eigenvectors for these eigenvalues. Show that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is an orthogonal basis of V.

10.4.5. Let T be a symmetric operator on a finite-dimensional inner product space V. Show that the following conditions are equivalent:

(i) All the eigenvalues of T are positive.

(ii) We have $\langle T(\mathbf{v}), \mathbf{v}\rangle > 0$ for all $\mathbf{v} \in V$ with $\mathbf{v} \neq 0$.

10.4.6. Let V be a finite-dimensional inner product space, and let S and T be symmetric operators on V that commute (i.e. $S \circ T = T \circ S$). Show that each eigenspace of T is S-invariant. Deduce from this observation that there exists an orthogonal basis $\mathcal{B}$ of V such that $[\,S\,]_{\mathcal{B}}$ and $[\,T\,]_{\mathcal{B}}$ are both diagonal. (We say that S and T are *simultaneously diagonalizable*.)

10.5 Polar decomposition

Let V be a finite-dimensional inner product space.

Definition 10.5.1 (Positive definite). We say that a symmetric operator $S\colon V \to V$ is *positive definite* if the symmetric bilinear form

$$\begin{array}{ccc} V \times V & \longrightarrow & \mathbb{R} \\ (\mathbf{u}, \mathbf{v}) & \longmapsto & \langle S(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, S(\mathbf{v})\rangle \end{array} \tag{10.9}$$

associated to it is positive definite, that is, if it satisfies

$$\langle S(\mathbf{v}), \mathbf{v}\rangle > 0 \quad \text{for all} \quad \mathbf{v} \in V \setminus \{\mathbf{0}\}.$$

By Definition 10.1.1, this amounts to requiring that (10.9) is an inner product on V.

Example 10.5.2. Let $T\colon V \to V$ be an arbitrary invertible operator. Then $T^* \circ T\colon V \to V$ is a positive definite symmetric linear operator.

Indeed, the properties of the adjoint given by Proposition 10.3.5 show that

$$(T^* \circ T)^* = T^* \circ (T^*)^* = T^* \circ T,$$

and so $T^* \circ T$ is a symmetric operator. Also, for all $\mathbf{v} \in V \setminus \{\mathbf{0}\}$, we have $T(\mathbf{v}) \neq \mathbf{0}$, and so

$$\langle (T^* \circ T)(\mathbf{v}), \mathbf{v}\rangle = \langle T^*(T(\mathbf{v})), \mathbf{v}\rangle = \langle T(\mathbf{v}), T(\mathbf{v})\rangle > 0.$$

This implies that $T^* \circ T$ is also positive definite.

Proposition 10.5.3. *Let $S\colon V \to V$ be a linear operator. The following conditions are equivalent:*

(i) S is a positive definite symmetric operator;

(ii) There exists an orthonormal basis $\mathcal{B}$ of V such that $[\,S\,]_{\mathcal{B}}$ is a diagonal matrix with positive numbers on the diagonal.

Proof. (i)$\Longrightarrow$(ii): First suppose that S is positive definite symmetric. Since S is symmetric, Theorem 10.4.7 tells us that there exists an orthonormal basis $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ of V such that $[\,S\,]_{\mathcal{B}}$ can be written in the form

$$[\,S\,]_{\mathcal{B}} = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \end{pmatrix} \tag{10.10}$$

with $\sigma_1, \dots, \sigma_n \in \mathbb{R}$. Then, for $j = 1, \dots, n$, we have $S(\mathbf{u}_j) = \sigma_j \mathbf{u}_j$ and so

$$\langle S(\mathbf{u}_j), \mathbf{u}_j\rangle = \sigma_j \langle \mathbf{u}_j, \mathbf{u}_j\rangle = \sigma_j \|\mathbf{u}_j\|^2 = \sigma_j.$$

Since S is positive definite, we conclude that the elements $\sigma_1, \dots, \sigma_n$ on the diagonal of $[\,S\,]_{\mathcal{B}}$ are positive.

(ii)$\Longrightarrow$(i): Conversely, suppose that $[\,S\,]_{\mathcal{B}}$ can be written in the form (10.10) for an orthonormal basis $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ and positive real numbers $\sigma_1, \dots, \sigma_n$. Since $[\,S\,]_{\mathcal{B}}$ is symmetric, Proposition 10.3.4 shows that S is symmetric operator. Furthermore, if $\mathbf{v}$ is a nonzero vector of V, it can be written in the form $\mathbf{v} = a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n$ with $a_1, \dots, a_n \in \mathbb{R}$ not all zero, and we have

$$\langle S(\mathbf{v}), \mathbf{v}\rangle = \left\langle \sum_{j=1}^n a_j S(\mathbf{u}_j), \sum_{j=1}^n a_j \mathbf{u}_j \right\rangle = \left\langle \sum_{j=1}^n a_j \sigma_j \mathbf{u}_j, \sum_{j=1}^n a_j \mathbf{u}_j \right\rangle = \sum_{j=1}^n a_j^2 \sigma_j > 0,$$

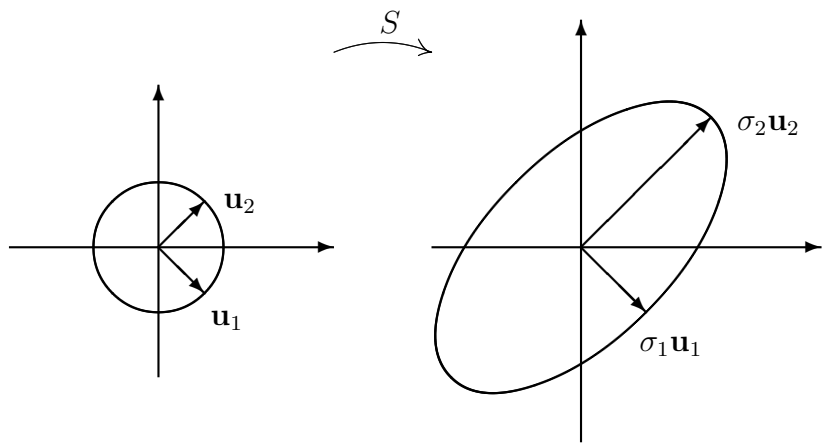
hence S is positive definite. $\square$

Geometric interpretation in $\mathbb{R}^2$

Let $S\colon \mathbb{R}^2 \to \mathbb{R}^2$ be a symmetric operator on $\mathbb{R}^2$, and let $\mathcal{B} = \{\mathbf{u}_1, \mathbf{u}_2\}$ be an orthonormal basis of $\mathbb{R}^2$ such that

$$[\,S\,]_{\mathcal{B}} = \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix} = \begin{pmatrix} \sigma_1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sigma_2 \end{pmatrix}$$

with $\sigma_1 > 0$ and $\sigma_2 > 0$. Then S can be viewed as the composition of two "dilations" along orthogonal axes, one by a factor of σ_1 in the direction $\mathbf{u}_1$ and the other by a factor of σ_2 in the direction $\mathbf{u}_2$. The overall effect is that S sends the circle of radius 1 centred at the origin to the ellipse with semi-axes $\sigma_1\mathbf{u}_1$ and $\sigma_2\mathbf{u}_2$.



Proposition 10.5.4. *Let $S\colon V \to V$ be a positive definite symmetric operator. There exists a unique positive definite symmetric operator $P\colon V \to V$ such that $S = P^2$.*

In other words, a positive definite symmetric operator admits a unique square root of the same type.

Proof. By Proposition 10.5.3, there exists an orthonormal basis $\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ of V such that

$$[\,S\,]_{\mathcal{B}} = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \end{pmatrix}$$

with $\sigma_1, \ldots, \sigma_n > 0$. Let $P\colon V \to V$ be the linear operator for which

$$[\,P\,]_{\mathcal{B}} = \begin{pmatrix} \sqrt{\sigma_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\sigma_n} \end{pmatrix}.$$

Since $[\,S\,]_{\mathcal{B}} = ([\,P\,]_{\mathcal{B}})^2 = [\,P^2\,]_{\mathcal{B}}$, we have $S = P^2$. Since $[\,P\,]_{\mathcal{B}}$ is also diagonal with positive numbers on its diagonal, Proposition 10.5.3 tells us that it is a positive definite symmetric operator. For the uniqueness of P, see Exercise 10.5.1. $\square$

We conclude this chapter with the following result, which gives a decomposition of invertible linear operators $T\colon V \to V$ similar to the polar decomposition of a complex number $z \neq 0$ in the form $z = r\,u$ where r is a positive real number and u is a complex number of norm 1 (see Exercise 10.5.3).

Theorem 10.5.5. *Let $T\colon V \to V$ be an invertible linear operator. There exists a unique positive definite symmetric operator $P\colon V \to V$ and a unique orthogonal operator $U\colon V \to V$ such that $T = U \circ P$.*

Proof. By Example 10.5.2, we have that $T^* \circ T\colon V \to V$ is a positive definite symmetric operator. By Proposition 10.5.4, there exists a positive definite symmetric operator $P\colon V \to V$ such that

$$T^* \circ T = P^2.$$

Since P is positive definite, it is invertible. Let

$$U = T \circ P^{-1}.$$

Then we have

$$U^* = (P^{-1})^* \circ T^* = (P^*)^{-1} \circ T^* = P^{-1} \circ T^*$$

and so

$$U^* \circ U = P^{-1} \circ (T^* \circ T) \circ P^{-1} = P^{-1} \circ P^2 \circ P^{-1} = I.$$

This shows that U is an orthogonal operator (see Exercise 10.3.3). So we have $T = U \circ P$ as required. For the uniqueness of P and U, see Exercise 10.5.2. □

Example 10.5.6. Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the linear operator given by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x - y \\ 2x + 2y \end{pmatrix}.$$

Its matrix relative to the standard basis $\mathcal{E}$ of $\mathbb{R}^2$ is

$$[\,T\,]_{\mathcal{E}} = \begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix}.$$

Direct computation gives

$$[\,T^* \circ T\,]_{\mathcal{E}} = \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 3 & 5 \end{pmatrix},$$

and so the characteristic polynomial of $T^* \circ T$ is $x^2 - 10x + 16 = (x-2)(x-8)$. Thus the eigenvalues of this operator are 2 and 8. We find that $(1,-1)^t$ and $(1,1)^t$ are eigenvectors of $T^* \circ T$ for these eigenvalues. By Exercise 10.4.4, the latter form an orthogonal basis of $\mathbb{R}^2$. Then

$$\mathcal{B} = \left\{ \mathbf{u}_1 := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix},\ \mathbf{u}_2 := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

is an orthonormal basis of $\mathbb{R}^2$ such that

$$[\,T^* \circ T\,]_{\mathcal{B}} = \begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}.$$

So we have $T^* \circ T = P^2$ where $P\colon \mathbb{R}^2 \to \mathbb{R}^2$ is the positive definite symmetric operator for which

$$[\,P\,]_{\mathcal{B}} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{8} \end{pmatrix}.$$

We have that

$$[\,I\,]_{\mathcal{E}}^{\mathcal{B}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad \text{and} \quad [\,I\,]_{\mathcal{B}}^{\mathcal{E}} = ([\,I\,]_{\mathcal{E}}^{\mathcal{B}})^{-1} = ([\,I\,]_{\mathcal{E}}^{\mathcal{B}})^t = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},$$

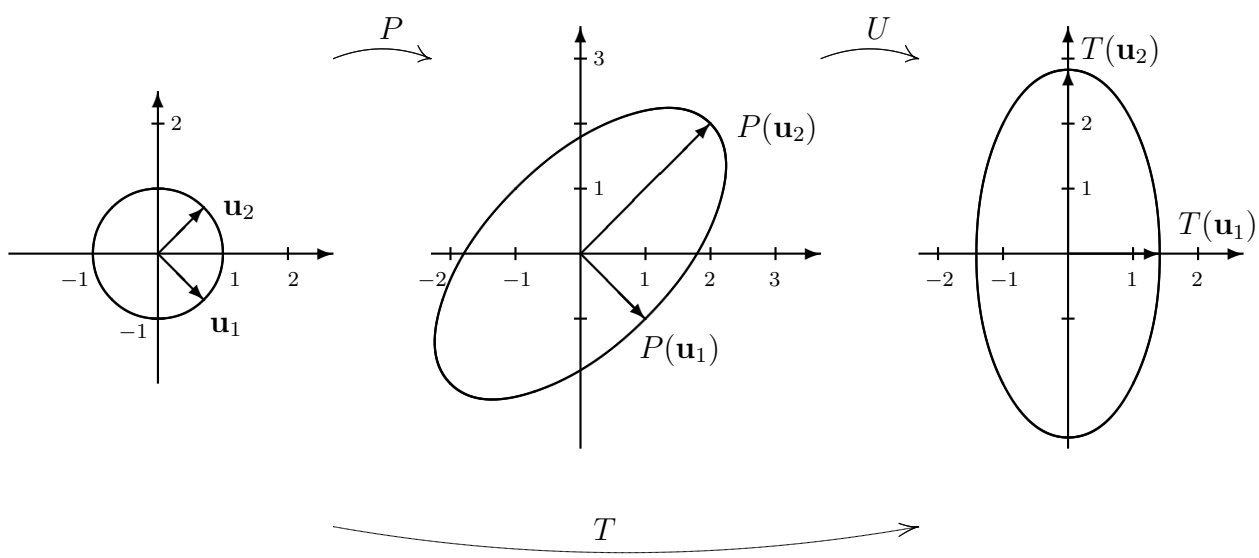
where the latter calculation uses the fact that, since $\mathcal{E}$ and $\mathcal{B}$ are orthonormal basis of $\mathbb{R}^2$, the matrix $[\,I\,]_{\mathcal{E}}^{\mathcal{B}}$ is orthogonal (see Exercise 10.2.3). The matrix of P in the standard basis is therefore

$$[\,P\,]_{\mathcal{E}} = [\,I\,]_{\mathcal{E}}^{\mathcal{B}}\,[\,P\,]_{\mathcal{B}}\,[\,I\,]_{\mathcal{B}}^{\mathcal{E}} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 2\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

We note in passing that this matrix is indeed symmetric, as it should be. Finally, following the steps of the proof of Theorem 10.5.5, we set $U = T \circ P^{-1}$. We find that

$$[\,U\,]_{\mathcal{E}} = \begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix} \frac{1}{4\sqrt{2}} \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \cos(\pi/4) & -\sin(\pi/4) \\ \sin(\pi/4) & \cos(\pi/4) \end{pmatrix}.$$

In this form, we recognize that U is the rotation through an angle $\pi/4$ about the origin in $\mathbb{R}^2$. In particular, U is indeed an orthogonal operator and we have obtained the required decomposition $T = U \circ P$, with P the symmetric operator that dilates vectors by a factor of $\sqrt{2}$ in the direction $\mathbf{u}_1$ and by a factor of $\sqrt{8}$ in the direction $\mathbf{u}_2$.



Exercises.

10.5.1. Let $P\colon V \to V$ and $S\colon V \to V$ be positive definite symmetric operators such that $P^2 = S$. Show that, for every eigenvalue λ of P, the eigenspace of P for the eigenvalue λ coincides with that of S for the eigenvalue λ^2. Conclude that P is the unique positive definite symmetric operator on V such that $P^2 = S$.

10.5.2. Let $P\colon V \to V$ be a positive definite symmetric operator, let $U\colon V \to V$ be an orthogonal operator, and let $T = U \circ P$. Show that $T^* \circ T = P^2$. Using the preceding exercise, deduce that P is the unique positive definite symmetric operator and U is the unique orthogonal operator such that $T = U \circ P$.

10.5.3. Consider $\mathbb{C}$ as a real vector space and equip it with the inner product

$$\langle a + ib, c + id\rangle = ac + bd.$$

Fix a complex number $z \neq 0$ and consider the $\mathbb{R}$-linear map $T\colon \mathbb{C} \to \mathbb{C}$ given by $T(w) = zw$ for all $w \in \mathbb{C}$.

(i) Verify that $\langle w_1, w_2\rangle = \mathrm{Re}(w_1\overline{w_2})$ for all $w_1, w_2 \in \mathbb{C}$.

(ii) Show that the adjoint T^* of T is given by $T^*(w) = \overline{z}w$ for all $w \in \mathbb{C}$.

(iii) Let $r = |z|$ and let $u = r^{-1}z$. Show that the operator $P\colon \mathbb{C} \to \mathbb{C}$ of multiplication by r is symmetric positive definite, that the operator $U\colon \mathbb{C} \to \mathbb{C}$ of multiplication by u is orthogonal and that $T = U \circ P$ is the polar decomposition of T.

Appendices

Appendix A

Review: groups, rings and fields

Throughout this course, we will call on notions of algebra seen in MAT 2143. In particular, we will use the idea of a *ring*, which is only touched on in MAT 2143. This appendix presents a review of the notions of groups, rings and fields, together with their simplest properties. We omit most proofs already covered in MAT 2143.

A.1 Monoids

A *binary operation* on a set E is a function $*\colon E \times E \to E$ which, to each pair of elements (a, b) of E, associates an element of E denoted $a * b$. The symbol used to designate the operation can vary. Often, when it will not cause confusion, we simply write ab to denote the result of a binary operation applied to the pair $(a, b) \in E \times E$.

Definition A.1.1 (Associative, commutative). We say that a binary operation $*$ on a set E is:

- *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in E$
- *commutative* if $a * b = b * a$ for all $a, b \in E$.

Examples A.1.2. Addition and multiplication in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are binary operations that are both associative and commutative. On the other hand, for an integer $n \geq 2$, multiplication in the set $\mathrm{Mat}_{n\times n}(\mathbb{R})$ of square matrices of size n with coefficients in $\mathbb{R}$ is associative but not commutative. Similarly, composition in the set $\mathrm{End}(S)$ of maps from a set S to itself is associative but not commutative if $|S| \geq 3$. The vector product (cross product) on $\mathbb{R}^3$ is a binary operation that is neither commutative nor associative.

One important fact is that if an operation $*$ on a set E is associative, then the way in which we group terms in a product of a finite number of elements $a_1, \ldots, a_n$ of E does not

affect the result, as long as the order is preserved. For example, there are five ways to form the product of four elements $a_1, \ldots, a_4$ of E if we maintain their order. They are:

$$((a_1 * a_2) * a_3) * a_4, \quad (a_1 * (a_2 * a_3)) * a_4, \quad (a_1 * a_2) * (a_3 * a_4),$$
$$a_1 * (a_2 * (a_3 * a_4)), \quad a_1 * ((a_2 * a_3) * a_4).$$

We can check that if $*$ is associative, then all of these products are equal. For this reason, if $*$ is an associative operation, we simply write

$$a_1 * a_2 * \cdots * a_n$$

to denote the product of the elememtns $a_1, \ldots, a_n$ of E, in that order (without using parentheses).

If the operation $*$ is both associative and commutative, then the order in which we multiply the elements of E does not affect their product. We have, for example,

$$a_1 * a_2 * a_3 = a_1 * a_3 * a_2 = a_3 * a_1 * a_2 = \cdots .$$

Here, the verb "to multiply" and the term "product" are taken in the generic sense: "multiply" means "apply the operation" and the word "product" means "the result of the operation". When we wish to be more precise, we will use the terms that apply to the specific situation.

Special case: The symbol $+$ is reserved for commutative associative operations. We then say that the operation is an *addition* and we speak of *adding* elements. The result of an addition is called a *sum*.

Definition A.1.3 (Identity element). Let $*$ be a binary operation on a set E. We say that an element e of E is an *identity element* for $*$ if

$$a * e = e * a = a$$

for all $a \in E$.

One can show that if E has an identity element for an operation $*$, then it only has one such element. Generally, we denote this element by 1, but if the operation is written as $+$, we denote it by 0.

Examples A.1.4. Let n be a positive integer. The identity element for the addition in $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is the zero matrix O_n of size $n \times n$ whose entries are all zero. The identity element for the multiplication in $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is the identity matrix I_n of size $n \times n$ whose element on the diagonal are all equal to 1 and the others are all equal to 0.

Definition A.1.5 (Monoid). A *monoid* is a set E equipped with an associative binary operation for which E has an identity element.

A monoid is therefore a pair $(E, *)$ consisting of a set E and an operation $*$ on E with the above properties. When we speak of a monoid E, without specifying the operation, it is because the operation is implied. In this case, we generally write ab to indicate the product of two elements a and b in E.

Example A.1.6. The pairs $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ are monoids (recall that $\mathbb{N} = \{0, 1, 2, \dots\}$ denotes the set of nonnegative integers). For each integer $n \geq 1$, the pairs $(\mathrm{Mat}_{n\times n}(\mathbb{R}), +)$ and $(\mathrm{Mat}_{n\times n}(\mathbb{R}), \cdot)$ are also monoids. Finally, if S is a set, then $(\mathrm{End}(S), \circ)$ is a monoid.

Definition A.1.7. Let $(E, *)$ be a monoid. For an integer $n \geq 1$ and $a \in E$, we denote by

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ times}}$$

the product of n copies of a. If the operation is denoted $+$ (hence is commutative), we instead write

$$n\,a = \underbrace{a + a + \cdots + a}_{n \text{ times}}$$

to denote the sum of n copies of a.

In this context, we have the following rule:

Exponent rule. *If $(E, *)$ is a monoid, we have*

$$a^m * a^n = a^{m+n} \quad \textit{and} \quad (a^m)^n = a^{mn}$$

for all $a \in E$ and all pairs of integers $m, n \geq 1$. Furthermore, if $(E, *)$ is a commutative monoid*, that is if $*$ is commutative (in addition to being associative), we also have*

$$a^m * b^m = (a * b)^m$$

for every all integers $m \geq 1$ and $a, b \in E$.

Finally, if $(E, +)$ is a commutative monoid written additively, these formulas become

$$ma + na = (m + n)a, \quad n(ma) = (nm)a \quad \textit{and} \quad ma + mb = m(a + b)$$

for all $a, b \in E$ and integers $m, n \geq 1$.

A.2 Groups

The notion of a group is central in algebra. In this course, the groups will encounter will mostly be abelian groups, but since we will also see nonabelian groups, it is appropriate to recall the more general notion. We first recall:

Definition A.2.1 (Invertible). Let $(E, *)$ be a monoid. We say that an element a of E is *invertible* (for the operation $*$) if there exists $b \in E$ such that

$$a * b = b * a = 1 \tag{A.1}$$

One can show that if a is an invertible element of a monoid $(E, *)$, then there exists a unique element b of E that satisfies Condition (A.1). We call it *inverse* of a and denote it a^{-1}. We therefore have

$$a * a^{-1} = a^{-1} * a = 1 \tag{A.2}$$

for every invertible element a of $(E, *)$. We can also show:

Lemma A.2.2. *Let a and b be invertible elements of a monoid $(E, *)$. Then*

(i) a^{-1} is invertible and $(a^{-1})^{-1} = a$,

(ii) ab is invertible and $(ab)^{-1} = b^{-1}a^{-1}$.

Important special case: If the operation of a commutative monoid is written $+$, we write $-a$ to denote the inverse of an invertible element a and we have:

$$a + (-a) = 0.$$

If a, b are two invertible elements of $(E, +)$, the assertions (i) and (ii) of Lemma A.2.2 become:

(i') $-a$ is invertible and $-(-a) = a$.

(ii') $a + b$ is invertible and $-(a + b) = (-a) + (-b)$.

Examples A.2.3.

1. All elements of $(\mathbb{Z}, +)$ are invertible.
2. The set of invertible elements of $(\mathbb{Z}, \cdot)$ is $\{1, -1\}$.
3. If S is a set, the invertible elements of $(\mathrm{End}(S), \circ)$ are the bijective maps $f \colon S \to S$.

Definition A.2.4 (Group). A *group* is a monoid $(G, *)$ whose elements are all invertible.

If we make this definition more explicit by including the preceding definitions, a group is a set E equipped with a binary operation $*$ possessing the following properties:

G1. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;

G2. there exists $1 \in G$ such that $1 * a = a * 1 = a$ for all $a \in G$;

G3. for all $a \in G$, there exists $b \in G$ such that $a * b = b * a = 1$.

Definition A.2.5 (Abelian group). We say that a group $(G, *)$ is *abelian* or *commutative* if the operation is commutative.

Examples A.2.6.

1. The pairs $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are abelian groups.
2. If S is a set, the set $\mathrm{Aut}(S)$ of bijections from S to itself is a group under composition.

The second example above is a special case of the following result:

Proposition A.2.7. *The set E^* of invertible elements of a monoid E is a group for the operation of E restricted to E^*.*

Proof. Lemmat A.2.2 shows that if $a, b \in E^*$, then their product ab remains in E^*. Therefore, by restriction, the operation of E induces a binary operation on E^*. It is associative and, since $1 \in E^*$, it has an identity element in E^*. Finally, for all $a \in E^*$, Lemma A.2.2 shows that the inverse a^{-1} (in E) belongs to E^*. Since it satisfies $a\,a^{-1} = a^{-1}\,a = 1$, it is also the inverse of a in E^*. □

Example A.2.8. If S is a set, the invertible elements of $(\mathrm{End}(S), \circ)$ are the bijective maps from S ot itself. Therefore the set $\mathrm{Aut}(S)$ of bijections $f\colon S \to S$ is a group under composition.

Example A.2.9. Fix an integer $n \geq 1$. We know that the set $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is a monoid under multiplication. The invertible elements of this monoid are the $n \times n$ matrices with nonzero determinant. These therefore form a group under multiplication. We denote this group $\mathrm{GL}_n(\mathbb{R})$:

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n\times n}(\mathbb{R})\,;\, \det(A) \neq 0\}.$$

We call it the *general linear group of order n on $\mathbb{R}$*.

Definition A.2.10. Let a be an element of a group G. For every integer $n \in \mathbb{Z}$, we define

$$a^n := \begin{cases} \underbrace{a\,a\,\cdots\,a}_{n \text{ times}} & \text{if } n \geq 1, \\ 1 & \text{if } n = 0, \\ \underbrace{a^{-1}\cdots a^{-1}}_{-n \text{ times}} & \text{if } n \leq -1. \end{cases}$$

Then the Exponent Rule becomes:

Proposition A.2.11. *Let a be an element of a group G. For all integers $m, n \in \mathbb{Z}$, we have:*

(i) $a^m a^n = a^{m+n}$

(ii) $(a^m)^n = a^{mn}$.

If G is abelian and if $a, b \in G$, we also have

(iii) $(ab)^m = a^m b^m$ *for all* $m \in \mathbb{Z}$.

The Exponent Rule implies as a special case $(a^{-1})^{-1} = a^{(-1)(-1)} = a^1 = a$.

In the case of an abelian group $(G, +)$ denoted additively, we define instead, for all $n \in \mathbb{Z}$,

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}} & \text{if } n \geq 1, \\ 0 & \text{if } n = 0, \\ \underbrace{(-a) + \cdots + (-a)}_{-n \text{ times}} & \text{if } n \leq -1, \end{cases}$$

and the rule becomes

(i) $(ma) + (na) = (m + n)a$,

(ii) $m(na) = (mn)a$,

(iii) $m(a + b) = ma + mb$,

for all integers $m, n \in \mathbb{Z}$ and elements $a, b \in G$.

A.3 Subgroups

Definition A.3.1 (Subgroup). A *subgroup* of a group G is a subset H of G such that

SG1. $1 \in H$,

SG2. $ab \in H$ for all $a, b \in H$,

SG3. $a^{-1} \in H$ for all $a \in H$.

It is easy to see that a subgroup H of a group G is itself a group under the operation of G restricted to H (thanks to **SG2**, the product in G induces a product on H by restriction).

Examples A.3.2.

1. The set $2\mathbb{Z}$ of even integers is a subgroup of $(\mathbb{Z}, +)$.
2. The set $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ of nonzero real numbers is a group under multiplication and the set $\mathbb{R}^*_+ = \{x \in \mathbb{R}\,;\, x > 0\}$ of positive real numbers is a subgroup of $(\mathbb{R}^*, \cdot)$.

We also recall that the set of subgroups of a group G is stable under intersection.

Proposition A.3.3. *Let* $(G_i)_{i \in I}$ *be a collection of subgroups of a group* G. *Then their intersection* $\bigcap_{i \in I} G_i$ *is also a subgroup of* G.

For example, if X is a subset of a group G, the intersection of all the subgroups of G containing X is a subgroup of G and, since it contains X, it is the smallest subgroup of G that contains X. We call it the *subgroup of G generated by X* and we denote it $\langle X \rangle$. In the case that X is a singleton (i.e. contains a single element) we have the following:

Proposition A.3.4. *Let a be an element of a group G. The subgroup of G generated by a is*

$$\langle a \rangle = \{a^n \,;\, n \in \mathbb{Z}\}.$$

Proof. Let $H = \{a^n \,;\, n \in \mathbb{Z}\}$. We have

$$1 = a^0 \in H.$$

Furthermore, for all $m, n \in \mathbb{Z}$, the Exponent Rule (Proposition A.2.11) gives

$$a^m a^n = a^{m+n} \in H \quad \text{and} \quad (a^m)^{-1} = a^{-m} \in H.$$

Therefore, H is a subgroup of G. It contains $a^1 = a$. Since every subgroup of G that contains a must also contain all of H, H is the smallest subgroup of G containing a, and so $H = \langle a \rangle$. □

Whether or not G is abelian, the subgroup $\langle a \rangle$ generated by a single elements is always abelian. If G is abelian with its operation written additively, then the subgroup generated by an element a of G is instead written:

$$\langle a \rangle = \{n\, a \,;\, n \in \mathbb{N}\}.$$

Definition A.3.5 (Cyclic group). We say that a group G is *cyclic* if G is generated by a single element, that is, if there exists $a \in G$ such that $G = \langle a \rangle$.

Example A.3.6. The group $(\mathbb{Z}, +)$ is cyclic, generated by 1.

Example A.3.7. Let n be a positive integer. The set $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ of nonzero complex numbers is a group under multiplication and the set

$$C_n = \{z \in \mathbb{C}^* \,;\, z^n = 1\}$$

of n-th roots of unity is the subgroup of $\mathbb{C}^*$ generated by $e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n)$.

A.4 Group homomorphisms

Definition A.4.1 (Group homomorphism). Let G and H be two groups. A *(group) homomorphism* from G to H is a function $\varphi : G \to H$ such that

$$\varphi(a\, b) = \varphi(a)\, \varphi(b)$$

for all pairs of elements a, b of G.

We recall that if $\varphi : G \to H$ is a group homomorphism, then:

$$\varphi(1_G) = 1_H \quad \text{and} \quad \varphi(a^{-1}) = \varphi(a)^{-1} \text{ for all } a \in G,$$

where 1_G and 1_H denote, respectively, the identity elements of G and H. More generally, we have

$$\varphi(a^n) = \varphi(a)^n$$

for all $a \in G$ and $n \in \mathbb{Z}$.

In the case where G and H are abelian groups written additively, we must interpret Definition A.4.1 in the following manner: a *homomorphism* from G to H is a function $\varphi : G \to H$ such that

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

for every pair of elements a, b of G. Such a function satisfies $\varphi(0_G) = 0_H$ and $\varphi(-a) = -\varphi(a)$ for all $a \in G$, and more generally $\varphi(na) = n\varphi(a)$ for all $n \in \mathbb{Z}$ and $a \in G$.

We also recall the following results:

Proposition A.4.2. *Let $\varphi : G \to H$ and $\psi : H \to K$ be group homomorphisms.*

(i) The composition $\psi \circ \varphi : G \to K$ is a homomorophism.

(ii) If φ is bijective, the inverse function $\varphi^{-1} : H \to G$ is also a bijective homomorphism.

A bijective homomorphism is called an *isomorphism*. We say that a group G is *isomorphic* to a group H is there exists an isomorphism from G to H. This defines an equivalence relation on the class of groups.

Example A.4.3. The map

$$\begin{array}{rccc} \exp : & \mathbb{R} & \to & \mathbb{R}_+^* \\ & x & \mapsto & e^x \end{array}$$

is a group homomorphism since $e^{x+y} = e^x e^y$ for all $x, y \in \mathbb{R}$. Since it is bijective, it is an isomorphism. Therefore the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_+^*, \cdot)$ are isomorphic.

Proposition A.4.4. *Let $\varphi : G \to H$ be a group homomorphism.*

(i) The set

$$\ker(\varphi) := \{a \in G\,;\, \varphi(a) = 1_H\}$$

is a subgroup of G, called the kernel *of φ.*

(ii) The set

$$\mathrm{Im}(\varphi) := \{\varphi(a)\,;\, a \in G\}$$

is a subgroup of H called the image *of φ.*

(iii) The map φ is injective if and only if $\ker(\varphi) = \{1_G\}$. It is surjective if and only if $\mathrm{Im}(\varphi) = H$.

Example A.4.5. The map

$$\begin{array}{rccc} \varphi : & \mathbb{R}^* & \longrightarrow & \mathbb{R}^* \\ & x & \longmapsto & x^2 \end{array}$$

is a group homomorphism with kernel $\ker(\varphi) = \{-1, 1\}$ and image $\mathrm{Im}(\varphi) = \mathbb{R}^*_+$.

Example A.4.6. Let $n \in \mathbb{N}^*$. The map

$$\begin{array}{rccc} \varphi : & \mathrm{GL}_n(\mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ & A & \longmapsto & \det(A) \end{array}$$

is a group homomorphism since $\det(AB) = \det(A)\det(B)$ for every pair of matrices $A, B \in \mathrm{GL}_n(\mathbb{R})$ (see Example A.2.9 for the definition of $\mathrm{GL}_n(\mathbb{R})$). Its kernel is

$$\mathrm{SL}_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R})\,;\, \det(A) = 1\}.$$

We call it the *special linear group* of order n on $\mathbb{R}$. It is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. In addition, we can easily verify that the image of φ is $\mathbb{R}^*$, that is, φ is a surjective homomorphism.

Example A.4.7. Let G and H be two group. Then cartesian product

$$G \times H = \{(g, h)\,;\, g \in G, h \in H\}$$

is a group for the componentwise product:

$$(g, h) \cdot (g', h') = (gg', hh').$$

For this group structure, the projection

$$\begin{array}{rccc} \pi : & G \times H & \longrightarrow & G \\ & (g, h) & \longmapsto & g \end{array}$$

is a surjective homomorphism with kernel

$$\ker(\pi) = \{(1_G, h)\,;\, h \in H\} = \{1_G\} \times H.$$

A.5 Rings

Definition A.5.1 (Ring). A *ring* is a set A equipped with two binary operations

$$\begin{array}{rccc} A \times A & \longrightarrow & A \\ (a, b) & \longmapsto & a + b \end{array} \quad \text{and} \quad \begin{array}{rccc} A \times A & \longrightarrow & A\,, \\ (a, b) & \longmapsto & ab \end{array}$$

called, respectively, *addition* and *multiplication*, that satisfy the following conditions:

(i) A is an abelian group under the addition,

(ii) A ia a monoid under the multiplication,

(iii) the multiplication is distributive over the addition: we have

$$a(b+c) = ab + ac \quad \text{and} \quad (a+b)c = ac + bc$$

for all $a, b, c \in A$.

Explicitly, the three conditions of the definition are equivalent to the following eight axioms:

A1. $a + (b + c) = (a + b) + c \quad \forall a, b, c \in A$.

A2. $a + b = b + a \quad \forall a, b \in A$.

A3. There exists an element 0 of A such that $a + 0 = a$ for all $a \in A$.

A4. For all $a \in A$, there exists $-a \in A$ such that $a + (-a) = 0$.

A5. $a(bc) = (ab)c \quad \forall a, b, c \in A$.

A6. There exists an element 1 of A such that $a\,1 = 1\,a = a$.

A7. $a(b + c) = ab + ac \quad \forall a, b, c \in A$.

A8. $(a + b)c = ac + bc \quad \forall a, b, c \in A$.

We say that a ring is *commutative* if the multiplication is commutative, in which case Conditions **A7** and **A8** are equivalent.

Since a ring is an abelian group under addition, the sum of n elements $a_1, \cdots, a_n$ of a ring A does not depend on either the grouping of terms or the order in which we add them. The sum of these elements is simply denoted

$$a_1 + \cdots + a_n \quad \text{or} \quad \sum_{i=1}^{n} a_i.$$

The identity element for the addition, characterized by condition **A3**, is called the *zero* of the ring A and we denote it 0. Each element a of A has a unique additive inverse, denoted $-a$ and characterized by Condition **A4**. For all $n \in \mathbb{Z}$, we define

$$na = \begin{cases} \underbrace{a + +a + \cdots + a}_{n \text{ times}} & \text{if } n \geq 1, \\ 0 & \text{if } n = 0, \\ \underbrace{(-a) + \cdots + (-a)}_{-n \text{ times}} & \text{if } n \leq -1, \end{cases}$$

as in the case of abelian groups. Then we have

$$(m + n)a = ma + na, \quad m(na) = (mn)a \quad \text{and} \quad m(a + b) = ma + mb,$$

for all $m, n \in \mathbb{Z}$ and $a, b \in A$.

Also, since a ring is a monoid under the multiplication, the product of n elements $a_1, a_2, \ldots, a_n$ of a ring A does not depend on the way we group the terms in the product as long as we maintain the order. The product of these elements is simply denoted

$$a_1\, a_2 \cdots a_n.$$

If the ring A is commutative, the product of elements of A also does not depend on the order in which we multiply them. Finally, the identity element of A for the multiplication is denoted 1 and is characterized by Condition **A5**, if is called the *unit*. For every $n \geq 1$ and $a \in A$, we define, as usual,

$$a^n = \underbrace{a\, a \cdots a}_{n \text{ times}}.$$

We also have the Exponent Rule:

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn} \tag{A.3}$$

for all integers $m, n \geq 1$ and $a \in A$.

We say that two elements a, b of A *commute* if $ab = ba$. In this case, we also have

$$(ab)^m = a^m b^m$$

for all $m \in \mathbb{N}^*$. In particular, this formula is satisfied for all $a, b \in A$ if A is a commutative ring.

We say that an element a of a ring A is *invertible* if it has a multiplicative inverse, that is, if there exists $b \in A$ such that $ab = ba = 1$. As seen in Section A.2, this element b is then characterized by this condition. We denote it a^{-1} and call it the *inverse* of a. For an invertible element a of A, we can extend the definition of a^m to any integer $m \in \mathbb{Z}$ and formulas (A.3) remain valid for all $m, n \in \mathbb{Z}$ (see Section A.2).

In a ring A, the laws of addition and multiplication are related by the conditions of distributivity in two terms **A7** and **A8**. By induction on n, we can deduce the properties of distributivity in n terms:

$$\begin{aligned} a(b_1 + \cdots + b_n) &= ab_1 + \cdots + ab_n\,, \\ (a_1 + \cdots + a_n)b &= a_1 b + \cdots + a_n b\,, \end{aligned}$$

for all $a, a_1, \ldots, a_n, b, b_1, \ldots, b_n \in A$. Still more generally, combining these two properties, we find

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m} a_i \left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$$

for all $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$. Moreover, if $a, b \in A$ commute, we obtain the "binomial formula"

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Finally, the axioms of distributivity imply

$$(ma)b = a(mb) = m(ab)$$

for all $a, b \in A$ and $m \in \mathbb{Z}$. In particular, taking $m = 0$ and $m = -1$, we recover the well know properties

$$0\,a = a\,0 = 0 \quad \text{and} \quad (-a)b = a(-b) = -(ab)$$

where, in the first series of equalities, the symbol 0 represents the zero in the ring.

We also recall that, since a ring A is a monoid under the multiplication, the set of invertible elements of A forms a group under the multiplication. We denote this group A^*.

Example A.5.2. For every integer $n \geq 1$, the set $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is a ring under the addition and multiplication of matrices. The group $(\mathrm{Mat}_{n\times n}(\mathbb{R}))^*$ of invertible element of this ring is denoted $\mathrm{GL}_n(\mathbb{R})$ (see Example A.2.9).

Example A.5.3. Let $n \geq 1$ be an integer and let A be an arbitrary ring. The set

$$\mathrm{Mat}_{n\times n}(A) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} ;\, a_{11}, \ldots, a_{nn} \in A \right\}$$

of $n \times n$ matrices with entries in A is a ring for the operations

$$\begin{aligned} (a_{ij}) + (b_{ij}) &= (a_{ij} + b_{ij}) \\ (a_{ij}) \cdot (b_{ij}) &= (c_{ij}) \quad \text{where } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}. \end{aligned}$$

This does not require that the ring A be commutative.

Example A.5.4. Let X be a set and let A be a ring. We denote by $\mathcal{F}(X, A)$ the set of functions from X to A. Given $f, g \in \mathcal{F}(X, A)$, we define $f + g$ and fg to be the functions from X to A given by

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x)$$

for all $x \in X$. Then $\mathcal{F}(X, A)$ is a ring for these operations.

Example A.5.5. The triples $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ are commutative rings.

Example A.5.6. Let n be a positive integer. We define an equivalence relation on $\mathbb{Z}$ by setting

$$a \equiv b \mod n \iff n \text{ divides } a - b.$$

Then $\mathbb{Z}$ is partitioned into exactly n equivalence classes represented by the integers $0, 1, \ldots, n-1$. We denote by $\bar{a}$ the equivalence class of $a \in \mathbb{Z}$ and we call it more precisely the *congruence*

class of a modulo n. The set of congruence classes modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$. We therefore have

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}.$$

We define the sum and product of two congruence classes module n by

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a}\,\overline{b} = \overline{ab}\,,$$

the resulting classes $\overline{a+b}$ and $\overline{ab}$ being independent of the choices of representatives a of $\overline{a}$ and b of $\overline{b}$. For these operations, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with n elements. We call it the *ring of integers modulo* n.

A.6 Subrings

Definition A.6.1 (Subring). A *subring* of a ring A is a subset B of A such that

SR1. $0, 1 \in B$.

SR2. $a + b \in B$ for all $a, b \in B$.

SR3. $-a \in B$ for all $a \in B$.

SR4. $ab \in B$ for all $a, b \in B$.

Such a subset B is itself a ring for the operations of A restricted to B. The notion of subring is transitive: if B is a subring of a ring A and C is a subring of B, then C is a subring of A.

Example A.6.2. In the chain of inclusions $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ each ring is a subring of its successor.

Example A.6.3. Let A be an arbitrary ring. The set

$$P := \{m\,1_A\,;\, m \in \mathbb{Z}\}$$

of integer multiples of the unit 1_A of A is a subring of A. Indeed, we have

$$0_A = 0 \cdot 1_A \in P, \qquad 1_A = 1 \cdot 1_A \in P,$$

and, for all $m, n \in \mathbb{Z}$,

$$\begin{aligned}(m\,1_A) + (n\,1_A) &= (m+n)\,1_A \in P,\\ -(m\,1_A) &= (-m)\,1_A \in P,\\ (m\,1_A)(n\,1_A) &= (mn)\,1_A \in P.\end{aligned}$$

This subring P is the smallest subring of A.

Example A.6.4. Let A be a subring of a *commutative* ring C and let $c \in C$. The set

$$A[c] := \{a_0 + a_1\,c + \cdots + a_n\,c^n\,;\, n \in \mathbb{N}^*, a_0, \ldots, a_n \in A\}$$

is the smallest subring of C containing A and c (exercise).

A.7 Ring homomorphisms

Definition A.7.1. Let A and B be two rings. A *ring homomorphism* from A to B is a map $\varphi : A \to B$ such that

1) $\varphi(1_A) = 1_B$,

2) $\varphi(a + a') = \varphi(a) + \varphi(a')$ for all $a, a' \in A$,

3) $\varphi(a\, a') = \varphi(a)\varphi(a')$ for all $a, a' \in A$.

Condition 2) means that $\varphi : A \to B$ is a homomorphism of abelian groups under addition. In particular, it implies that $\varphi(0_A) = 0_B$. On the other hand, Condition 3) does *not* necessarily imply that $\varphi(1_A) = 1_B$. That is why we add Condition 1).

If $\varphi\colon A \to B$ is a ring homomorphism and $a \in A$, we have

$$\begin{aligned} \varphi(na) &= n\varphi(a) \quad \text{for all } n \in \mathbb{Z}, \\ \varphi(a^n) &= \varphi(a)^n \quad \text{for all } n \in \mathbb{N}^* . \end{aligned}$$

Example A.7.2. Let A be a ring. It is easily verified that the set

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} ; a, b, c \in A \right\}$$

is a subring of $\mathrm{Mat}_{2\times 2}(A)$ and that the map $\varphi\colon U \to A$ given by

$$\varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a$$

is a ring homomorphism.

Proposition A.7.3. *Let $\varphi\colon A \to B$ and $\psi\colon B \to C$ be ring homomorphisms.*

(i) The composition $\psi \circ \varphi\colon A \to C$ is a ring homomorphism.

(ii) If φ is bijective, then the inverse map $\varphi^{-1}\colon B \to A$ is also a bijective ring homomorphism.

As in the case of groups, a bijective ring homomorphism is called a *ring isomorphism*. We say that a ring A is *isomorphic* to a ring B if there exists a ring isomorphism from A to B. This defines an equivalence relation on the class of rings.

Definition A.7.4 (Kernel and image). Let $\varphi\colon A \to B$ be a ring homomorphism. We define the *kernel* of φ by

$$\ker(\varphi) := \{a \in A\,;\, \varphi(a) = 0\}$$

and the *image* of φ by

$$\mathrm{Im}(\varphi) := \{\varphi(a)\,;\, a \in A\}.$$

These are, respectively, the kernel and image of φ viewed as a homomorphism of abelian groups. If follows that $\ker(\varphi)$ is a subgroup of A under addition, and $\mathrm{Im}(\varphi)$ is a subgroup of B under addition. In view of part (iii) of Proposition A.4.4, we can conclude that a ring homomorphism $\varphi : A \to B$ is

- injective $\iff$ $\ker(\varphi) = \{0\}$,
- surjective $\iff$ $\mathrm{Im}(\varphi) = B$.

We can also verify more precisely that $\mathrm{Im}(\varphi)$ is a subring of B. However, $\ker(\varphi)$ is *not* generally a subring of A. Indeed, we see that

$$1_A \in \ker(\varphi) \quad \iff \quad 1_B = 0_B \quad \iff \quad B = \{0_B\}.$$

Thus $\ker(\varphi)$ is a subring of A if and only if B is the trivial ring consisting of a single element $0 = 1$. We note however that if $a \in A$ and $x \in \ker(\varphi)$, then we have

$$\varphi(a\,x) = \varphi(a)\varphi(x) = \varphi(a)0 = 0$$

$$\varphi(x\,a) = \varphi(x)\varphi(a) = 0\varphi(a) = 0$$

and so ax and xa belong to $\ker(\varphi)$. This motivates the following definition:

Definition A.7.5 (Ideal). An *ideal* of a ring A is a subset I of A such that

(i) $0 \in I$

(ii) $x + y \in I$ for all $x, y \in I$,

(iii) $ax, xa \in I$ for all $a \in A$ and $x \in I$.

Condition (iii) implies that $-x = (-1)x \in I$ for all $x \in I$. Thus an ideal of A is a subgroup of A under addition that satisfies Condition (iii). When A is commutative, this last condition becomes simply

$$ax \in I \quad \text{for all } a \in A \text{ and } x \in I.$$

In light of the observations preceding Definition A.7.5, we can conclude:

Proposition A.7.6. *The kernel of a ring homomorphism $\varphi : A \to B$ is an ideal of A.*

Example A.7.7. For the homomorphism $\varphi : U \to A$ of Example A.7.2, we have

$$\ker(\varphi) = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} ; b, c \in A \right\}.$$

The latter is an ideal of U.

A.8 Fields

Definition A.8.1 (Field). A *field* is a commutative ring K with $0 \neq 1$, all of whose nonzero elements are invertible.

If K is a field, each nonzero element a of K has a multiplicative inverse a^{-1}. In addition, using the addition an multiplication, we can therefore define an operation of subtraction in K by

$$a - b := a + (-b)$$

and an operation of division by

$$\frac{a}{b} := a\, b^{-1} \quad \text{if } b \neq 0.$$

Example A.8.2. The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields for the usual operations.

Finally, we recall the following result:

Proposition A.8.3. *Let $n \in \mathbb{N}^*$. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.*

For each prime number p, we denote by $\mathbb{F}_p$ the field with p elements.

For $p = 2$, the addition and multiplication tables for $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ are given by

$$\begin{array}{c|cc} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \end{array} \quad \text{and} \quad \begin{array}{c|cc} \cdot & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} \end{array}.$$

In $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, they are given by

$$\begin{array}{c|ccc} + & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{1} & \bar{2} \\ \bar{1} & \bar{1} & \bar{2} & \bar{0} \\ \bar{2} & \bar{2} & \bar{0} & \bar{1} \end{array} \quad \text{and} \quad \begin{array}{c|ccc} \cdot & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} & \bar{2} \\ \bar{2} & \bar{0} & \bar{2} & \bar{1} \end{array}.$$

Appendix B

The determinant

Throughout this appendix, we fix an arbitrary commutative ring A, with $0 \neq 1$. We extend the notion of determinants to square matrices with entries in A and we show that most of the usual properties of the determinant (those we know for matrices with entries in a field) apply to this general situation with minor modifications. To do this, we use the notion of A-module presented in Chapter 6.

B.1 Multilinear maps

Definition B.1.1 (Multilinear map). Let $M_1, \ldots, M_s$ and N be A-modules. We say that a map

$$\varphi\colon M_1 \times \cdots \times M_s \to N$$

is *multilinear* if it satisfies

ML1. $\varphi(\mathbf{u}_1, \ldots, \mathbf{u}'_j + \mathbf{u}''_j, \ldots, \mathbf{u}_s) = \varphi(\mathbf{u}_1, \ldots, \mathbf{u}'_j, \ldots, \mathbf{u}_s) + \varphi(\mathbf{u}_1, \ldots, \mathbf{u}''_j, \ldots, \mathbf{u}_s)$,

ML2. $\varphi(\mathbf{u}_1, \ldots, a\mathbf{u}_j, \ldots, \mathbf{u}_s) = a\varphi(\mathbf{u}_1, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_s)$,

for every integer $j = 1, \ldots, s$, all $\mathbf{u}_1 \in M_1, \ldots, \mathbf{u}_j, \mathbf{u}'_j, \mathbf{u}''_j \in M_j, \ldots, \mathbf{u}_s \in M_s$, and all $a \in A$.

In other words, a map $\varphi\colon M_1 \times \cdots \times M_s \to N$ is multilinear if, for each integer $j = 1, \ldots, s$ and all $\mathbf{u}_1 \in M_1$, ... , $\mathbf{u}_s \in M_s$, the function

$$\begin{array}{rcl} \overline{\varphi} : M_j & \longrightarrow & N \\ \mathbf{u} & \longmapsto & \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_{j-1}, \mathbf{u}, \mathbf{u}_{j+1}, \ldots, \mathbf{u}_s) \end{array}$$

is a homomorphism of A-modules.

Proposition B.1.2. *Let $M_1, \dots, M_s$ be free A-modules, and let $\{\mathbf{v}_1^{(j)}, \dots, \mathbf{v}_{n_j}^{(j)}\}$ be a basis of M_j for $j = 1, \dots, s$. For every A-module N and all*

$$\mathbf{w}_{i_1 \dots i_s} \in N \quad (1 \le i_1 \le n_1, \dots, 1 \le i_s \le n_s),$$

there exists a unique multilinear map $\varphi\colon M_1 \times \cdots \times M_s \to N$ such that

$$\varphi(\mathbf{v}_{i_1}^{(1)}, \dots, \mathbf{v}_{i_s}^{(s)}) = \mathbf{w}_{i_1 \dots i_s} \quad (1 \le i_1 \le n_1, \dots, 1 \le i_s \le n_s). \tag{B.1}$$

Proof. Suppose that a multilinear map $\varphi\colon M_1 \times \cdots \times M_s \to N$ satisfies Conditions (B.1). For all $\mathbf{u}_1 \in M_1, \dots, \mathbf{u}_s \in M_s$, we can write

$$\mathbf{u}_1 = \sum_{i_1=1}^{n_1} a_{i_1,1}\mathbf{v}_{i_1}^{(1)}, \quad \mathbf{u}_2 = \sum_{i_2=1}^{n_2} a_{i_2,2}\mathbf{v}_{i_2}^{(2)}, \ \dots \ , \ \mathbf{u}_s = \sum_{i_s=1}^{n_s} a_{i_s,s}\mathbf{v}_{i_s}^{(s)}, \tag{B.2}$$

for some elements $a_{i,j}$ of A. Then, by the multilinearity of φ, we have

$$\begin{aligned}
\varphi(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_s) &= \sum_{i_1=1}^{n_1} a_{i_1,1}\, \varphi(\mathbf{v}_{i_1}^{(1)}, \mathbf{u}_2, \dots, \mathbf{u}_s) \\
&= \sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2} a_{i_1,1}\, a_{i_2,2}\, \varphi(\mathbf{v}_{i_1}^{(1)}, \mathbf{v}_{i_2}^{(2)}, \mathbf{u}_3, \dots, \mathbf{u}_s) \\
&\quad \cdots\cdots \\
&= \sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2}\cdots\sum_{i_s=1}^{n_s} a_{i_1,1}a_{i_2,2}\dots a_{i_s,s}\, \varphi(\mathbf{v}_{i_1}^{(1)}, \mathbf{v}_{i_2}^{(2)}, \dots, \mathbf{v}_{i_s}^{(s)}) \\
&= \sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2}\cdots\sum_{i_s=1}^{n_s} a_{i_1,1}a_{i_2,2}\dots a_{i_s,s}\, \mathbf{w}_{i_1\dots i_s}.
\end{aligned} \tag{B.3}$$

This proves that there is at most one multilinear map φ satisfying (B.1). On the other hand, for given $\mathbf{u}_1 \in M_1, \dots, \mathbf{u}_s \in M_s$, there is only one choice of $a_{ij} \in A$ satisfying (B.2) and so formula (B.3) does indeed define a function $\varphi\colon M_1 \times \cdots \times M_s \to N$. We leave it as an exercise to verify that this function is multilinear and satisfies (B.1). □

In this appendix, we are interested in a particular type of multilinear map:

Definition B.1.3 (Alternating multilinear map). Let M and N be A-modules, and let n be a positive integer. We say that a multilinear map

$$\varphi : M^n \longrightarrow N$$

is *alternating* if it satisfies $\varphi(\mathbf{u}_1, \dots, \mathbf{u}_n) = \mathbf{0}$ for all $\mathbf{u}_1, \dots, \mathbf{u}_n \in M$ not all distinct.

The qualifier "alternating" is justified by the following proposition:

Proposition B.1.4. *Let $\varphi\colon M^n \longrightarrow N$ be an alternating multilinear map, and let i and j be integers with $1 \leq i < j \leq n$. For all $\mathbf{u}_1, \ldots, \mathbf{u}_n \in M$, we have*

$$\varphi(\mathbf{u}_1, \ldots, \overset{\overset{i}{\vee}}{\mathbf{u}_j}, \ldots, \overset{\overset{j}{\vee}}{\mathbf{u}_i}, \ldots, \mathbf{u}_n) = -\varphi(\mathbf{u}_1, \ldots, \overset{\overset{i}{\vee}}{\mathbf{u}_i}, \ldots, \overset{\overset{j}{\vee}}{\mathbf{u}_j}, \ldots, \mathbf{u}_n).$$

In other words, the sign of φ changes when we permute two of its arguments.

Proof. Fix $\mathbf{u}_1, \ldots, \mathbf{u}_n \in M$. For all $\mathbf{u} \in M$, we have:

$$\varphi(\mathbf{u}_1, \ldots, \overset{\overset{i}{\vee}}{\mathbf{u}}, \ldots, \overset{\overset{j}{\vee}}{\mathbf{u}}, \ldots, \mathbf{u}_n) = 0.$$

Choosing $\mathbf{u} = \mathbf{u}_i + \mathbf{u}_j$ and using the multilinearity of φ, we have

$$\begin{aligned}
0 &= \varphi(\mathbf{u}_1, \ldots, \overset{\overset{i}{\vee}}{\mathbf{u}_i + \mathbf{u}_j}, \ldots, \overset{\overset{j}{\vee}}{\mathbf{u}_i + \mathbf{u}_j}, \ldots, \mathbf{u}_n) \\
&= \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_n) + \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_n) \\
&\quad + \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_n) + \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_n) \\
&= \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_n) + \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_j, \ldots, \mathbf{u}_i, \ldots, \mathbf{u}_n).
\end{aligned}$$

The conclusion follows. □

Let S_n be the set of bijections from the set $\{1, 2, \ldots, n\}$ to itself. This is a group under composition, called the *group of permutations* of $\{1, 2, \ldots, n\}$. We say that an element τ of S_n is a *transposition* if there exist integers i and j with $1 \leq i < j \leq n$ such that $\tau(i) = j$, $\tau(j) = i$ and $\tau(k) = k$ for all $k \neq i, j$. In the course MAT 2143 on group theory, you saw that every $\sigma \in S_n$ can be written as a product of transpositions

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\ell.$$

This expression is not unique, but for each one the parity of the integer ℓ is the same. We define the *signature* of σ by

$$\epsilon(\sigma) = (-1)^\ell$$

and so all transposition have a signature of -1. You also saw that the resulting map $\epsilon\colon S_n \to \{1, -1\}$ is a group homomorphism. Using these notions, we can generalize Proposition B.1.4 as follows.

Proposition B.1.5. *Let $\varphi\colon M^n \longrightarrow N$ be an alternating multilinear map, and let $\sigma \in S_n$. For all $\mathbf{u}_1, \ldots, \mathbf{u}_n \in M$, we have*

$$\varphi(\mathbf{u}_{\sigma(1)}, \ldots, \mathbf{u}_{\sigma(n)}) = \epsilon(\sigma)\varphi(\mathbf{u}_1, \ldots, \mathbf{u}_n).$$

Proof. Proposition B.1.4 shows that, for every transposition $\tau \in S_n$, we have

$$\varphi(\mathbf{u}_{\tau(1)}, \ldots, \mathbf{u}_{\tau(n)}) = -\varphi(\mathbf{u}_1, \ldots, \mathbf{u}_n).$$

for any choice of $\mathbf{u}_1, \ldots, \mathbf{u}_n \in M$. From this we conclude that

$$\varphi(\mathbf{u}_{\nu(\tau(1))}, \ldots, \mathbf{u}_{\nu(\tau(n))}) = -\varphi(\mathbf{u}_{\nu(1)}, \ldots, \mathbf{u}_{\nu(n)}) \tag{B.4}$$

for all $\nu \in S_n$.

Write $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_\ell$ where $\tau_1, \tau_2, \ldots, \tau_\ell$ are transpositions. Let $\sigma_0 = 1$ and

$$\sigma_i = \tau_1 \circ \cdots \circ \tau_i \quad \text{for} \quad i = 1, \ldots, \ell,$$

so that $\sigma_i = \sigma_{i-1} \circ \tau_i$ for $i = 1, \ldots, \ell$. For each integer i, Relation (B.4) gives

$$\varphi(\mathbf{u}_{\sigma_i(1)}, \ldots, \mathbf{u}_{\sigma_i(n)}) = -\varphi(\mathbf{u}_{\sigma_{i-1}(1)}, \ldots, \mathbf{u}_{\sigma_{i-1}(n)}).$$

Since $\sigma = \sigma_\ell$, these ℓ relations imply

$$\varphi(\mathbf{u}_{\sigma(1)}, \ldots, \mathbf{u}_{\sigma(n)}) = (-1)^\ell \varphi(\mathbf{u}_1, \ldots, \mathbf{u}_n).$$

The conclusion follows, since $\epsilon(\sigma) = (-1)^\ell$. □

Proposition B.1.5 implies the following:

Theorem B.1.6. *Let M be a free A-module with basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, and let $c \in A$. There exists a unique alternating multilinear map $\varphi : M^n \to A$ such that $\varphi(\mathbf{e}_1, \ldots, \mathbf{e}_n) = c$. It is given by*

$$\varphi\Big(\sum_{i=1}^n a_{i,1}\mathbf{e}_i\,, \ \ldots\ , \sum_{i=1}^n a_{i,n}\mathbf{e}_i\Big) = c \sum_{\sigma \in S_n} \epsilon(\sigma)\, a_{\sigma(1),1} \ldots a_{\sigma(n),n} \tag{B.5}$$

for all $a_{i,j} \in A$.

Proof. First suppose that there exists an alternating multilinear map $\varphi : M^n \to A$ such that $\varphi(\mathbf{e}_1, \ldots, \mathbf{e}_n) = c$. Let

$$\mathbf{u}_1 = \sum_{i=1}^n a_{i,1}\mathbf{e}_i, \quad \mathbf{u}_2 = \sum_{i=1}^n a_{i,2}\mathbf{e}_i, \ \ldots, \ \mathbf{u}_n = \sum_{i=1}^n a_{i,n}\mathbf{e}_i \tag{B.6}$$

be elements of M written as linear combinations of $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Since φ is multilinear, we have

$$\varphi(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n) = \sum_{i_1=1}^n \sum_{i_2=1}^n \cdots \sum_{i_n=1}^n a_{i_1,1} a_{i_2,2} \ldots a_{i_n,n}\, \varphi(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \ldots, \mathbf{e}_{i_n}) \tag{B.7}$$

(this a particular case of Formula (B.3)). For integers $i_1, \ldots, i_n \in \{1, 2, \ldots, n\}$ not all distinct, we have $\varphi(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_n}) = 0$ by Definition B.1.3. One the other hand, if $i_1, \ldots, i_n \in \{1, 2, \ldots, n\}$ are distinct, they determine a bijection σ of $\{1, 2, \ldots, n\}$ given by $\sigma(1) = i_1, \sigma(2) = i_2, \ldots, \sigma(n) = i_n$ and, by Proposition B.1.5, we get

$$\varphi(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_n}) = \varphi(\mathbf{e}_{\sigma(1)}, \ldots, \mathbf{e}_{\sigma(n)}) = \epsilon(\sigma)\, \varphi(\mathbf{e}_1, \ldots, \mathbf{e}_n) = c\, \epsilon(\sigma).$$

Thus Formula (B.7) can be rewritten as

$$\varphi(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n) = c \sum_{\sigma \in S_n} \epsilon(\sigma)\, a_{\sigma(1),1} a_{\sigma(2),2} \dots a_{\sigma(n),n}.$$

This shows that φ is necessarily given by (B.5).

To conclude, we need to show that the function $\varphi : M^n \to A$ given by (B.5) is alternating multilinear. We first note that it is multilinear (exercise). Thus it remains to check that, if $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n \in M$ are not all distinct, then $\varphi(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n) = 0$.

Suppose therefore that there exist indices i and j with $1 \le i < j \le n$ such that $\mathbf{u}_i = \mathbf{u}_j$. We denote by E the set of permutations σ of S_n such that $\sigma(i) < \sigma(j)$, by τ the transposition of S_n that interchanges i and j, and by E^c the complement of E in S_n, that is the set of permutations σ of S_n such that $\sigma(i) > \sigma(j)$. Then an element of S_n belongs to E^c if and only if it is of the form $\sigma \circ \tau$ with $\sigma \in E$. From this we deduce that

$$\varphi(\mathbf{u}_1, \dots, \mathbf{u}_n) = c \sum_{\sigma \in E} \Big(\epsilon(\sigma)\, a_{\sigma(1),1} \dots a_{\sigma(n),n} + \epsilon(\sigma \circ \tau)\, a_{\sigma(\tau(1)),1} \dots a_{\sigma(\tau(n)),n} \Big).$$

Then, for all $\sigma \in S_n$, we have both $\epsilon(\sigma \circ \tau) = \epsilon(\sigma)\epsilon(\tau) = -\epsilon(\sigma)$ and

$$a_{\sigma(\tau(1)),1} \dots a_{\sigma(\tau(n)),n} = a_{\sigma(1),\tau(1)} \dots a_{\sigma(n),\tau(n)} = a_{\sigma(1),1} \dots a_{\sigma(n),n},$$

the last equality following from the fact that $\mathbf{u}_i = \mathbf{u}_j$. We conclude that $\varphi(\mathbf{u}_1, \dots, \mathbf{u}_n) = 0$, as claimed. □

Corollary B.1.7. *Let M be a free A-module. Then all bases of M contain the same number of elements.*

Proof. Suppose on the contrary that $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ and $\{\mathbf{f}_1, \dots, \mathbf{f}_m\}$ are two bases of M of different cardinalities. Without loss of generality, suppose that $m < n$ and denote by $\varphi\colon M^n \longrightarrow A$ the alternating multilinear form such that $\varphi(\mathbf{e}_1, \dots, \mathbf{e}_n) = 1$. Since $\{\mathbf{f}_1, \dots, \mathbf{f}_m\}$ is a basis of M, we can write

$$\mathbf{e}_1 = \sum_{i=1}^{m} a_{i,1}\mathbf{f}_i \ , \ \dots \ , \ \mathbf{e}_n = \sum_{i=1}^{m} a_{i,n}\mathbf{f}_i$$

for some elements $a_{i,j}$ of A. Since φ is multilinear, we conclude that

$$\varphi(\mathbf{e}_1, \dots, \mathbf{e}_n) = \sum_{i_1=1}^{m} \cdots \sum_{i_n=1}^{m} a_{i_1,1} \dots a_{i_n,n}\, \varphi(\mathbf{f}_{i_1}, \dots, \mathbf{f}_{i_n}). \tag{B.8}$$

Thus, for all $i_1, \dots, i_n \in \{1, \dots, m\}$, at least two of the integers $i_1, \dots, i_n$ are equal (since $n > m$) and therefore, since φ is alternating, we get $\varphi(\mathbf{f}_{i_1}, \dots, \mathbf{f}_{i_n}) = 0$. Thus, Equality (B.8) implies $\varphi(\mathbf{e}_1, \dots, \mathbf{e}_n) = 0$. Since we chose φ such that $\varphi(\mathbf{e}_1, \dots, \mathbf{e}_n) = 1$, this is a contradiction. □

B.2 The determinant

Let n be a positive integer. We know that

$$A^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \; ; \, a_1, \dots, a_n \in A \right\}$$

is a free A-module with basis

$$\left\{ \mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} , \, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} , \, \dots , \mathbf{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\} .$$

Theorem B.1.6 applied to $M = A^n$ shows that, for this choice of basis, there exists a unique alternating multilinear map $\varphi \colon (A^n)^n \to A$ such that $\varphi(\mathbf{e}_1, \dots, \mathbf{e}_n) = 1$, and that it is given by

$$\varphi \left(\begin{pmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \end{pmatrix} , \begin{pmatrix} a_{1,2} \\ \vdots \\ a_{n,2} \end{pmatrix} , \dots , \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{n,n} \end{pmatrix} \right) = \sum_{\sigma \in S_n} \epsilon(\sigma) \, a_{\sigma(1),1} \dots a_{\sigma(n),n} \, .$$

Now, the cartesian product $(A^n)^n = A^n \times \dots \times A^n$ of n copies of A^n can be naturally identified with the set $\mathrm{Mat}_{n \times n}(A)$ of $n \times n$ matrices with entries in A. One associates to each element $(C_1, \dots, C_n)$ of $(A^n)^n$ the matrix $(C_1, \dots, C_n) \in \mathrm{Mat}_{n \times n}(A)$ whose columns are $C_1, \dots, C_n$. In this way, the n-tuple $(\mathbf{e}_1, \dots, \mathbf{e}_n) \in (A^n)^n$ corresponds to the identity matrix I_n of size $n \times n$. We thus obtain:

Theorem B.2.1. *There exists a unique function* $\det \colon \mathrm{Mat}_{n \times n}(A) \to A$ *that satisfies* $\det(I_n) = 1$ *and that, viewed as a function on the n columns of a matrix, is alternating multilinear. It is given by*

$$\det \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} = \sum_{\sigma \in S_n} \epsilon(\sigma) \, a_{\sigma(1),1} \dots a_{\sigma(n),n} \, . \tag{B.9}$$

This function is called the *determinant*. We can deduce the effect of an elementary column operation on the determinant:

Proposition B.2.2. *Let $U \in \mathrm{Mat}_{n \times n}(A)$ and let U' be a matrix obtained by applying to U an elementary column operation. There are three cases:*

(I) If U' is obtained by interchanging two columns of U, then $\det(U') = -\det(U)$*;*

(II) If U' is obtained by adding to column i of U the product of column j of U and an element a of A, for distinct integers i and j, then $\det(U') = \det(U)$*;*

(III) If U' is obtained by multiplying column i of U by a unit $a \in A^*$, then $\det(U') = a \det(U)$.

Proof. Denote the columns of U by $C_1, \ldots, C_n$. The equality $\det(U') = -\det(U)$ of case (I) follows from Proposition B.1.4. In case (II), we see that

$$\begin{aligned}\det(U') &= \det(C_1, \ldots, \overset{\overset{i}{\vee}}{C_i + a\, C_j}, \ldots, \overset{\overset{j}{\vee}}{C_j}, \ldots, C_n) \\ &= \det(C_1, \ldots, \overset{\overset{i}{\vee}}{C_i}, \ldots, \overset{\overset{j}{\vee}}{C_j}, \ldots, C_n) + a \det(C_1, \ldots, \overset{\overset{i}{\vee}}{C_j}, \ldots, \overset{\overset{j}{\vee}}{C_j}, \ldots, C_n) \\ &= \det(U)\end{aligned}$$

since the determinant of a matrix with two equal columns is zero. Finally, in case (III), we have

$$\det(U') = \det(C_1, \ldots, \overset{\overset{i}{\vee}}{a\, C_i}, \ldots, C_n) = a \det(C_1, \ldots, \overset{\overset{i}{\vee}}{C_i}, \ldots, C_n) = a \det(U)$$

as claimed. □

When A is a euclidean domain, we can bring every matrix $U \in \mathrm{Mat}_{n\times n}(A)$ into lower triangular form by a series of elementary column operations (see Theorem 8.4.6). By the preceding proposition, we can follow the effect of these operations on the determinant. To deduce the value of $\det(U)$ from this, we then use:

Proposition B.2.3. *If $U \in \mathrm{Mat}_{n\times n}(A)$ is a lower triangular matrix, its determinant is the product of the elements on its diagonal.*

Proof. Write $U = (a_{ij})$. Since U is lower triangular, we have $a_{ij} = 0$ si $i > j$. For every permutation $\sigma \in S_n$ with $\sigma \neq 1$, there exists an integer $i \in \{1, 2, \ldots, n\}$ such that $\sigma(i) > i$ and so we obtain

$$a_{\sigma(1),1} \ldots a_{\sigma(i),i} \ldots a_{\sigma(n),n} = 0.$$

Then Formula (B.9) gives $\det(U) = a_{1,1}\, a_{2,2} \ldots a_{n,n}$. □

We also note that the determinant of every square matrix is equal to the determinant of its transpose:

Proposition B.2.4. *For every matrix $U \in \mathrm{Mat}_{n\times n}(A)$ we have* $\det(U^t) = \det(U)$.

Proof. Write $U = (a_{ij})$. For all $\sigma \in S_n$, we have

$$a_{\sigma(1),1} \ldots a_{\sigma(n),n} = a_{1,\sigma^{-1}(1)} \ldots a_{n,\sigma^{-1}(n)}.$$

Since we also have $\epsilon(\sigma^{-1}) = \epsilon(\sigma)^{-1} = \epsilon(\sigma)$, Formula (B.9) gives

$$\det(U) = \sum_{\sigma\in S_n} \epsilon(\sigma^{-1})\, a_{1,\sigma^{-1}(1)} \ldots a_{n,\sigma^{-1}(n)} = \sum_{\sigma\in S_n} \epsilon(\sigma)\, a_{1,\sigma(1)} \ldots a_{n,\sigma(n)} = \det(U^t).$$

□

In light of this result, we deduce that the function $\det\colon \mathrm{Mat}_{n\times n}(A) \to A$, viewed as a function of the n rows of a matrix is alternating multilinear. We also get the following analogue of Proposition B.2.2 for elementary row operations, replacing everywhere the word "column" by "row".

Proposition B.2.5. *Let $U \in \mathrm{Mat}_{n\times n}(A)$ and let U' be a matrix obtained by applying to U an elementary row operation. There are three cases:*

(I) If U' is obtained by interchanging two rows of U, then $\det(U') = -\det(U)$;

(II) If U' is obtained by adding to row i of U the product of row j of U and an element a of A, for distinct integers i and j, then $\det(U') = \det(U)$;

(III) If U' is obtained by multiplying row i of U by a unit $a \in A^*$, then $\det(U') = a\det(U)$.

Proof. For example, in case (II), the matrix $(U')^t$ is obtained from U^t by adding to column i of U^t the product of column j of U and a. Proposition B.2.2 gives in this case $\det((U')^t) = \det(U^t)$. By Proposition B.2.4, we conclude that $\det(U') = \det(U)$. □

Similarly, we have:

Proposition B.2.6. *The determinant of a triangular matrix $U \in \mathrm{Mat}_{n\times n}(A)$ is equal to the product of the elements of its diagonal.*

Proof. If U is lower triangular, this follows form Proposition B.2.3. If U is upper triangular, its transpose U^t is lower triangular, and so $\det(U) = \det(U^t)$ is the product of the element on the diagonal of U^t. Since these elements are the same as those on the diagonal of U, the result follows. □

We finish this section with the following result.

Theorem B.2.7. *For every pair of matrices $U, V \in \mathrm{Mat}_{n\times n}(A)$, we have*

$$\det(UV) = \det(U)\det(V).$$

Proof. Fix a matrix $U \in \mathrm{Mat}_{n\times n}(A)$, and consider the function $\varphi\colon (A^n)^n \to A$ given by

$$\varphi(C_1, \ldots, C_n) = \det(UC_1, \ldots, UC_n)$$

for every choice of n columns $C_1, \ldots, C_n \in A^n$. We claim that φ is alternating multilinear. Furthermore, if $C_1, \ldots, C_n$ are the columns of a matrix V, then $UC_1, \ldots, UC_n$ are the columns of UV. Therefore, we also have

$$\varphi(\mathbf{e}_1, \ldots, \mathbf{e}_n) = \det(UI) = \det(U).$$

Since Theorem B.1.6 shows that there exists a unique alternating multilinear function from $(A^n)^n$ to A such that $\varphi(\mathbf{e}_1, \ldots, \mathbf{e}_n) = \det(U)$ and the function $\psi\colon (A^n)^n \to A$ given by

$$\psi(C_1, \ldots, C_n) = \det(U)\det(C_1, \ldots, C_n)$$

is another, we have $\det(UC_1, \ldots, UC_n) = \det(U)\det(C_1, \ldots, C_n)$ for all $(C_1, \ldots, C_n) \in (A^n)^n$, and so $\det(UV) = \det(U)\det(V)$ for all $V \in \mathrm{Mat}_{n\times n}(A)$. □

B.3 The adjugate

The goal of this last section is to show that the usual formulas for expanding a determinant along a row or column remain valid for all matrices with entries in an arbitrary commutative ring A, and that the notion of the adjugate and its properties also extend to this situation. To do this, we start with an alternate presentation of the determinant which is more useful for describing the determinant of a submatrix.

We first recall that the *number of inversions* of an n-tuple of distinct integers $(i_1, \dots, i_n)$, denoted $N(i_1, \dots, i_n)$, is defined to be the number or pairs of indices (k, ℓ) with $1 \leq k < \ell \leq n$ such that $i_k > i_\ell$. For example, we have $N(1, 5, 7, 3) = 2$ and $N(4, 3, 1, 2) = 4$. Every permutation σ of S_n can be identified with the n-tuple $(\sigma(1), \dots, \sigma(n))$ of its values, and we show in algebra that

$$\epsilon(\sigma) = (-1)^{N(\sigma(1),\dots,\sigma(n))}.$$

Then Formula (B.9) applied to a matrix $U = (a_{i,j}) \in \mathrm{Mat}_{n\times n}(A)$ becomes

$$\det(U) = \sum_{(i_1,\dots,i_n)\in S_n} (-1)^{N(i_1,\dots,i_n)} a_{i_1,1} \cdots a_{i_n,n}.$$

Since the determinant of U is equal to that of its transpose, we again deduce that

$$\det(U) = \sum_{(j_1,\dots,j_n)\in S_n} (-1)^{N(j_1,\dots,j_n)} a_{1,j_1} \cdots a_{n,j_n}.$$

Thanks to this formula, if $1 \leq f_1 < f_2 < \cdots < f_k \leq n$ and $1 \leq g_1 < g_2 < \cdots < g_k \leq n$ are two increasing subsequences of k elements chosen from the integers $1, 2, \dots, n$, then the submatrix $U' = (a_{f(i),g(j)})$ of U of size $k \times k$ formed from the elements of U belonging to the rows with indices $f_1, \dots, f_k$ and the columns with indices $g_1, \dots, g_k$ has determinant

$$\det(U') = \sum (-1)^{N(j_1,\dots,j_k)} a_{f_1,j_1} \cdots a_{f_k,j_k} \tag{B.10}$$

where the sum if over all permutations $(j_1, \dots, j_k)$ of $(g_1, \dots, g_k)$.

Definition B.3.1 (Minor, cofactor matrix, adjugate). Let $U = (a_{i,j})$ be an $n \times n$ matrix with entries in A. For $i, j = 1, \dots, n$, the (i, j)-*minor* of U, denoted $M_{i,j}(U)$, is the determinant of the $(n-1) \times (n-1)$ submatrix of U obtained by removing from U its i-th row and j-th column. The (i, j)-*cofactor* of U is

$$C_{i,j}(U) := (-1)^{i+j} M_{i,j}(U).$$

The *cofactor matrix* of U is the $n \times n$ matrix whose (i, j) entry is the (i, j)-cofactor of U. Finally, the *adjugate* of U, denoted $\mathrm{Adj}(U)$ is the transpose of the cofactor matrix of U.

We first give the formula for expansion along the first row:

Lemma B.3.2. *Let* $U = (a_{i,j}) \in \mathrm{Mat}_{n\times n}(A)$. *We have* $\det(U) = \sum_{j=1}^{n} a_{1,j} C_{1,j}(U)$.

Proof. Formula (B.10) applied to the calculation on $M_{1,j}(U)$ gives

$$M_{1,j}(U) = \sum_{(j_1,\dots,j_{n-1})\in E_j} (-1)^{N(j_1,\dots,j_{n-1})} a_{2,j_1}\cdots a_{n,j_{n-1}},$$

the sum being over the set E_j of permutations $(j_1,\dots,j_{n-1})$ of $(1,\dots,\widehat{j},\dots,n)$ that is the set of $(n-1)$-tuples of integers $(j_1,\dots,j_{n-1})$ such that $(j,j_1,\dots,j_{n-1})\in S_n$. Since $N(j,j_1,\dots,j_{n-1}) = N(j_1,\dots,j_{n-1}) + j - 1$ for each of these $(n-1)$-tuples, we see that

$$\begin{aligned}\det(U) &= \sum_{(j_1,\dots,j_n)\in S_n} (-1)^{N(j_1,\dots,j_n)} a_{1,j_1}\cdots a_{n,j_n}\\ &= \sum_{j=1}^{n} a_{1,j} \sum_{(j_1,\dots,j_{n-1})\in E_j} (-1)^{N(j,j_1,\dots,j_{n-1})} a_{2,j_1}\cdots a_{n,j_{n-1}}\\ &= \sum_{j=1}^{n} a_{1,j}(-1)^{j-1} C_{1,j}(U),\end{aligned}$$

and the assertion follows. □

More generally, we have the following formulas:

Proposition B.3.3. *Let $U = (a_{i,j}) \in \mathrm{Mat}_{n\times n}(A)$ and let $k,\ell \in \{1,2,\dots,n\}$. We have*

$$\sum_{j=1}^{n} a_{k,j}C_{\ell,j}(U) = \sum_{j=1}^{n} a_{j,k}C_{j,\ell}(U) = \begin{cases}\det(U) & \text{if } k=\ell,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. First suppose that $k=\ell$ and denote by U' the matrix obtained from U by dragging its k-th row from position k to position 1, in such a way that, for all $j = 1,\dots,n$, we have $M_{1,j}(U') = M_{k,j}(U)$. Applying Lemma B.3.2 to the matrix U', we have

$$\det(U) = (-1)^{k-1}\det(U') = (-1)^{k-1}\sum_{j=1}^{n} a_{k,j}C_{1,j}(U') = \sum_{j=1}^{n} a_{k,j}C_{k,j}(U).$$

If $k\neq\ell$, we deduce from the above formula that $\sum_{j=1}^{n} a_{k,j}C_{\ell,j}(U)$ is equal to the determinant of the matrix U'' obtained from U by replacing its ℓ-th row by its k-th row. Since this matrix has two identical row (the k-th and ℓ-th rows), its determinant is zero. Thus we have $\sum_{j=1}^{n} a_{k,j}C_{\ell,j}(U) = \det(U)\delta_{k,\ell}$ for all k and ℓ. Applying this formula to the matrix U^t and noting that $C_{j,\ell}(U) = C_{\ell,j}(U^t)$ for all j and ℓ, we have

$$\det(U)\delta_{k,\ell} = \det(U^t)\delta_{k,\ell} = \sum_{j=1}^{n} a_{j,k}C_{\ell,j}(U^t) = \sum_{j=1}^{n} a_{j,k}C_{j,\ell}(U).$$

□

Theorem B.3.4. *For every matrix* $U \in \mathrm{Mat}_{n\times n}(A)$*, we have*

$$U\mathrm{Adj}(U) = \mathrm{Adj}(U)U = \det(U)I.$$

Proof. Indeed, the element in position (ℓ, j) of $\mathrm{Adj}(U)$ is $C_{j,\ell}(U)$, and so the formulas of Proposition B.3.3 imply that the (k, ℓ) entry of the product $U\mathrm{Adj}(U)$ and the (ℓ, k) entry of the product $\mathrm{Adj}(U)U$ are both equal to $\det(U)\delta_{k,\ell}$ for all $k, \ell \in \{1, \dots, n\}$. □

We conclude with the following criterion:

Corollary B.3.5. *The invertible elements of the ring* $\mathrm{Mat}_{n\times n}(A)$ *are those whose determinant is an invertible element of* A*.*

Proof. Let $U \in \mathrm{Mat}_{n\times n}(A)$. If U is invertible, there exists a matrix $V \in \mathrm{Mat}_{n\times n}(A)$ such that $UV = I$. Taking the determinant of both sides of this equality, we have, thanks to Theorem B.2.7, $\det(U)\det(V) = \det(I) = 1$. Since $\det(V) \in A$, we deduce that $\det(U) \in A^*$. Conversely if $\det(U) \in A^*$, there exists $c \in A$ such that $c\det(U) = 1$ and so the above theorem shows that the matrix $V = c\mathrm{Adj}(U)$ of $\mathrm{Mat}_{n\times n}(A)$ satisfies $UV = VU = c\det(U)I = I$, thus U is invertible. □

Index