





# Contents

<b>1</b>	<b>Introduction</b>	<b>9</b>
1.1	Point of view . . . . .	10
1.2	Prerequisites and conventions (in progress) . . . . .	12
1.2.1	Prerequisites . . . . .	12
1.2.2	Conventions . . . . .	13
1.3	Useful tools . . . . .	14
1.3.1	Division by monic polynomials . . . . .	14
1.3.2	Zorn's lemma . . . . .	15
<b>I</b>	<b>Linear algebra over rings</b>	<b>17</b>
<b>2</b>	<b>Warm-up I: Matrices with ring coefficients</b>	<b>19</b>
2.1	Introduction . . . . .	19
2.1.1	Review on formal polynomials . . . . .	19
2.1.2	Principle of the permanence of identities . . . . .	20
2.1.3	Cayley-Hamilton in $M_n(\mathbb{R})$ . . . . .	21
2.2	Maximal rank matrices . . . . .	22
2.3	Reminder on Gauss elimination method . . . . .	23
2.3.1	Some universal formulas . . . . .	24
2.3.2	The usual field case . . . . .	25
2.3.3	Normal subgroups of $GL(V)$ . . . . .	27
2.4	Exercises . . . . .	28
<b>3</b>	<b>Modules</b>	<b>31</b>
3.1	Introduction . . . . .	31
3.2	Definitions and first examples . . . . .	32
3.3	Quotient, cokernel . . . . .	34
3.4	Exact sequences and diagrams . . . . .	36
3.5	Functoriality and diagram chasing . . . . .	38

3.6	Universal properties . . . . .	41
3.6.1	Sum and product . . . . .	41
3.6.2	Kernel and cokernel . . . . .	42
3.7	A key example: the $k[T]$ -module $V_a$ . . . . .	43
3.8	Cokernel of diagonal matrices . . . . .	45
3.8.1	Determinantal ideals . . . . .	47
3.8.2	Fitting ideals . . . . .	48
3.9	Properties to handle with caution . . . . .	51
3.9.1	Finiteness . . . . .	51
3.9.4	Free modules . . . . .	52
3.9.5	Torsion . . . . .	53
3.9.6	Summary of some specifics of modules . . . . .	54
3.10	Exercises . . . . .	54
<b>4</b>	<b>Rings and modules</b>	<b>61</b>
4.1	Introduction . . . . .	61
4.2	Quotient rings . . . . .	61
4.2.1	Product rings . . . . .	62
4.2.2	Cyclic modules and quotient rings . . . . .	63
4.3	Algebras . . . . .	63
4.4	Integrality . . . . .	64
4.4.1	An application of Cayley-Hamilton . . . . .	64
4.4.2	Ring of integers . . . . .	65
4.5	The Chinese remainder lemma . . . . .	67
4.6	Exercises . . . . .	69
<b>5</b>	<b>Noetherianity</b>	<b>73</b>
5.1	Introduction . . . . .	73
5.2	Noetherian modules . . . . .	74
5.2.1	Stability under exact sequences . . . . .	75
5.2.2	Hilbert's Basis Theorem . . . . .	76
5.2.3	Krull's intersection theorem . . . . .	76
5.3	Exercises . . . . .	77
<b>6</b>	<b>Matrix and modules over PID</b>	<b>81</b>
6.1	Introduction . . . . .	81
6.2	Survival kit for PID and Euclidean rings . . . . .	82
6.3	Matrix equivalence in PID and Euclidean rings . . . . .	83
6.3.1	Invariant ideals of a matrix . . . . .	83

<i>CONTENTS</i>	5
6.4 Invariant factors of a module . . . . .	86
6.4.1 The Euclidean case . . . . .	87
6.5 About uniqueness of invariant ideals . . . . .	88
6.6 Supplementary Section: Insight into K-Theory . . . . .	89
6.7 Exercises . . . . .	90
<b>II Linear algebra over fields</b>	<b>93</b>
<b>7 Warm-up II: duality</b>	<b>95</b>
7.1 Introduction . . . . .	95
7.2 Basic notions . . . . .	95
7.3 Formal biorthogonality . . . . .	97
7.4 Ante-dual basis: biduality . . . . .	97
7.5 Orthogonal and polar in finite dimension . . . . .	98
7.6 Biduality conventions (Finite dimension) . . . . .	100
7.7 Contravariance . . . . .	100
7.8 Exercises . . . . .	101
<b>8 Similarity in <math>M_n(\mathbf{k})</math></b>	<b>105</b>
8.1 Introduction . . . . .	105
8.2 Similarity in $M_n(\mathbf{k})$ . . . . .	106
8.2.1 Similarity invariants . . . . .	106
8.2.2 Explicit computations of the similarity invariants . . . . .	107
8.3 An important example: diagonalization . . . . .	110
8.4 Frobenius Decomposition . . . . .	111
8.5 Commutant . . . . .	112
8.6 An algorithm from $\sim$ to $\approx$ . . . . .	113
8.7 Summary on similarity invariants . . . . .	114
8.8 Exercises . . . . .	115
<b>9 The irreducibility toolbox</b>	<b>119</b>
9.1 Introduction . . . . .	119
9.2 An UFD criterion . . . . .	120
9.2.1 Uniqueness condition . . . . .	120
9.2.2 Stable subspaces of endomorphisms . . . . .	123
9.2.3 Existence criterion . . . . .	123
9.3 GCD, LCM in UFD . . . . .	124
9.4 Transfer of the UFD property . . . . .	125

9.4.1	Gauss' content . . . . .	125
9.4.2	The Transfer theorem . . . . .	127
9.5	Irreducibility of the cyclotomic polynomial over $\mathbb{Q}$ . . . . .	127
9.6	Exercices . . . . .	130
<b>10</b>	<b>Primary decomposition in PID</b>	<b>133</b>
10.1	Introduction . . . . .	133
10.2	Torsion modules over PID . . . . .	133
10.2.1	Primary decomposition . . . . .	134
10.2.2	Invariant ideals and primary decomposition . . . . .	135
10.3	Application: Jordan reduction . . . . .	136
10.3.1	Examples . . . . .	137
10.4	Exercices . . . . .	138
<b>11</b>	<b>Semisimplicity</b>	<b>141</b>
11.1	Introduction . . . . .	141
11.2	Semisimple modules . . . . .	141
11.3	«Reminder» on perfect fields . . . . .	145
11.3.2	Sums of semisimple endomorphisms . . . . .	147
11.4	Jordan-Chevalley decomposition . . . . .	147
11.4.1	Hensel's lemma and existence . . . . .	147
11.4.2	Uniqueness . . . . .	149
11.4.3	Similarity class of the components . . . . .	150
11.4.4	Appendix: What about the algorithmic nature of the decomposition? . . . . .	150
11.5	Jordan-Chevalley and spectral projectors . . . . .	151
11.5.1	$d$ -th roots in $GL_n$ . . . . .	151
11.6	Exercices . . . . .	152
<b>12</b>	<b>Simultaneous reduction</b>	<b>155</b>
12.1	Introduction . . . . .	155
12.2	Commuting family of matrices . . . . .	156
12.3	The Burnside-Wedderburn theorem . . . . .	157
12.4	Stable family of nilpotent and unipotent matrices . . . . .	158
12.5	Connected solvable matrix subgroups . . . . .	159
12.5.1	Basics on solvable groups . . . . .	159
12.5.2	The Lie-Kolchin theorem . . . . .	160
12.6	Exercices . . . . .	161

<b>III</b>	<b>About continuity of matrix reduction</b>	<b>165</b>
<b>13</b>	<b>Topology of similarity classes</b>	<b>167</b>
13.1	Introduction . . . . .	167
13.2	$\chi$ -types . . . . .	168
13.3	$\underline{P} \preceq \underline{Q} \Rightarrow \underline{P} \leq \underline{Q}$ . . . . .	170
13.4	$\underline{P} \leq \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$ . . . . .	171
13.4.1	An elementary deformation . . . . .	171
13.4.2	$\leq = \preceq$ . . . . .	172
13.5	Topological applications . . . . .	174
13.5.1	Topology of the fibers $\mu^{-1}(\chi)$ . . . . .	175
13.5.2	Global properties of $M_n(\mathbf{k})/GL_n(\mathbf{k})$ . . . . .	176
13.6	Exercises . . . . .	178
<b>14</b>	<b>Eigenvalues and primary components</b>	<b>179</b>
14.1	Introduction . . . . .	179
14.2	Continuity of primary components ( $\chi$ fixed) . . . . .	180
14.3	Regularity of polynomial roots . . . . .	181
14.3.1	Continuity . . . . .	181
14.3.2	Smoothness of simple roots . . . . .	183
14.3.3	Properness . . . . .	184
14.4	Localizing eigenvalues . . . . .	185
14.4.1	Gershgorin disks . . . . .	185
14.4.2	Landau's inequality . . . . .	186
14.4.3	Spectral radius . . . . .	188
14.4.5	Smoothness of simple eigenspaces . . . . .	190
14.5	Perron-Frobenius for positive matrices . . . . .	190
14.5.1	Basics on graphs . . . . .	192
14.5.2	Perron-Frobenius for irreducible matrices . . . . .	193
14.5.3	A classical illustration . . . . .	194
14.5.4	Markov chains . . . . .	195
14.6	Exercises . . . . .	196
<b>15</b>	<b>Index et bibliography</b>	<b>199</b>



# Chapter 1

## Introduction

In 1872, Felix Klein asked the following question. “Given a multiplicity and a group, to study the entities from the point of view of properties which are not changed by the transformations of the group... this can also be expressed as: given a multiplicity and a transformation group; develop the theory of invariants relative to this group” ([15]).



Felix Klein

In this first volume, we concretely illustrate this visionary point of view by classifying geometric objects by invariants under different group actions (invariant factors, similarity invariants...) and different perspectives (algebraic, topological...). We focus our attention on linear objects, leaving the study of bilinear and quadratic objects to the next volume.

Our motivation is to give, starting from the basic knowledge of dimension theory in linear algebra and calculus, a bridge to modern methods of algebra with as little formal theory as possible. We will try to explain how a balance between the abstract use of diagrams and modules on the one hand and concrete matrices on the other hand allows to obtain non-trivial and hopefully interesting results quickly.

To illustrate our perspective, similarity questions of matrices with field coefficients will be our leitmotif example throughout this book for many reasons (importance of this problem, concrete character of the objects, deep insights into a lot of more general subjects like arithmetic, K-theory, algebraic geometry, . . . . It is definitely not our pretension to make a study of these advanced topics, but we have tried to use methods which will be useful later.

In the first part, we give an introduction to module language theory in order to solve the following problem as our typical illustration: how to decide when two square matrices are similar. We do not use reduction theory, eigenvalues, or irreducible elements to solve this classification problem. The gain is

that we can solve this problem in an algorithmic and field independent way, (contrary to any method based on eigenvalues because in general computing roots of polynomials or factorizing them is hopeless). The price to pay is the non-continuity of these algorithms (though they are semi-continuous in a sense). We discuss the intrinsic aspects of continuity topics in the last part of the book.

In the second (more classical) part we will discuss reduction theory, where the key point is the factorization of the characteristic polynomials into linear terms (eigenvalues) or, more generally, into irreducible polynomials. The good news is that this process has continuity properties. The bad news is that we do not know how to factorize a polynomial in general. We have included a section on the simultaneous reduction of matrices, emphasizing the important notion of irreducible action of matrices.

In the third part, we illustrate the interest in both perspectives by studying the topology of similarity classes, which are of fundamental importance in advanced mathematics.

We try to do this in a *concrete* way, i.e. with methods that lead to algorithms. After all, it is better to know how to construct an object than simply to know that it exists. However, our goal is not to provide optimized programs in terms of efficiency (that's another topic, and an interesting one at that!), but to explore the *how*. In particular, we do not restrict ourselves to formally constructivist methods ([3]), but try to provide as many existence theorems as possible that can explicitly lead to the construction of the object in question, for example by a computer. Remarkably, we encounter the typical numerical shortcomings of Gaussian elimination algorithms. These phenomena can be of a purely numerical nature or due to non-continuous behaviour, as will be clearly seen. We strongly advise the reader to implement the various algorithms on a machine: this will allow him to verify that he has thoroughly understood the proofs. For our part, we have used the program SAGEMATH, based on Python.

In a subsequent volume, we will look at bilinear/quadratic geometry.

The material of this book is more or less classical, only the perspective is somehow more original. There are many excellent books in the literature from the classical monographs ([20], [21], [5],[6], [16]. . .) that aim to give a coherent "state of the art" to the abundant academic literature at the post-calculus level. Our book has one thing in common with all these books: it is intended to be actively worked on, not just passively read. This explains why we have tried to strike a balance between a fully formal and dry exposition and a "ready to eat" style.

Photo credits: ChronoMaths, Flickr user Duncan, Patrick Fradin, Marcel Gotlib, UQAM, Wikipedia.

## 1.1 Point of view

There are many ways to do mathematics, and it is rarely the case that there is only one good way. Writing a book emphasizes some choices. Our main choice is not original, but it is important: morphisms are more important than objects! This is why matrices are so important in our approach.

---

<sup>0</sup>See 14.3.3.2 to temper this statement.

Let us illustrate our purpose by two extreme ways of thinking mathematics by two universal genius. Finding a path between these two peaks guided our work.



Alexander Grothendieck

In his huge *Récoltes et Semailles* writing<sup>1</sup>, explains how generalizing problems is a fruitful way to solve problems.

*Take, for example, the task of proving a theorem that remains hypothetical (which, to some, may seem to be the essence of mathematical work). I see two extreme approaches to the task. The first is the hammer and chisel approach, where the problem is seen as a tough, smooth nut, and the goal is to get to the nutritious core protected by the shell. The principle is simple: place the edge of the chisel against the shell and strike hard. If necessary, you repeat this in several different places until the shell cracks - and then you're satisfied. [...].*

*I could illustrate the second approach by sticking with the image of the nut that needs to be opened. The first metaphor that came to mind is that you soak the nut in an emollient liquid-why not just water? From time to time you rub it to help the liquid penetrate, but otherwise you let time do its work. As the weeks and months go by, the shell softens-and when the time is right, a gentle squeeze of the hand is enough to open the shell like that of a perfectly ripe avocado. Or the nut is left to ripen in the sun and rain, and perhaps even the frost of winter. When the time is right, a delicate sprout emerges from the nutritious kernel and pierces the shell as if in a game, or rather, the shell opens by itself and allows it to pass through. [...]*

*Readers who are even slightly familiar with some of my work will have no difficulty recognizing which of these two approaches is "mine".*

This way of going from the particular to the general contrasts with Decartes' method.<sup>2</sup>.

- *Not to accept as true anything which I did not clearly know to be so.*
- *To divide each difficulty I examined into as many parts as possible and as might be necessary for its best solution.*
- *To conduct my thoughts in an orderly manner, beginning with the simplest and easiest to know objects, in order to ascend little by little, as if by steps, to the knowledge of the most complex.*

<sup>1</sup>A. Grothendieck, *Récoltes et Semailles I, II: Réflexions et témoignage sur un passé de mathématicien*, Gallimard (2022)

<sup>2</sup>R. Descartes, *Discourse on the Method* (1637), Gallimard (2009).

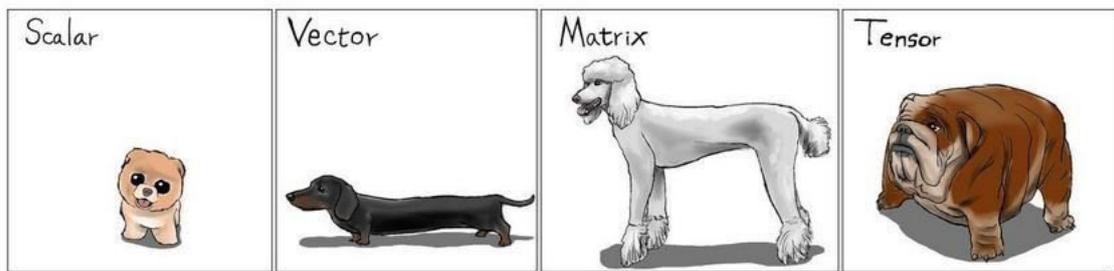


René Descartes

- *To make everywhere such complete enumerations, and such general surveys, that I may be sure of omitting nothing. This is the rule of enumeration. To make a complete review of objects, which involves prudence and circumspection.*

## 1.2 Prerequisites and conventions (in progress)

### 1.2.1 Prerequisites



We assume that the reader is familiar with basic definitions in algebra without any further expertise (general definitions of rings, ideals, points). For the convenience of the reader, we recall the notion of quotient (4.2). Some familiarity with basic algebraic properties of fields,  $\mathbf{Z}$  and  $\mathbf{k}[T]$ , is assumed (they are principal ideal rings -PID-). To make the reading easier, a proof of the main results is given in 6.2 and in (9).

No knowledge of linear algebra beyond the basics of dimension theory is assumed.<sup>3</sup> and the Gauss elimination method, the relationship between matrices and endomorphisms, and the elementary properties of the determinant. Strictly speaking, therefore, we do not assume any special knowledge of eigenvalue or reduction theory, although it is recommended to have taken an introductory course on the subject before studying our book.

Readers who have studied linear algebra in the context of real or complex vector spaces are just asked to accept (or verify) that nothing changes on an arbitrary field. It may happen that we use group notions

<sup>3</sup>Strictly speaking, it is easy to follow our path to all the results using only Gauss elimination and formal properties of the determinant

in a particular subsection, but these points can always be skipped on a first reading.

In Part III, we freely use basic notions from analysis, probability, and topology of metric spaces as taught in standard undergraduate programs.

## 1.2.2 Conventions

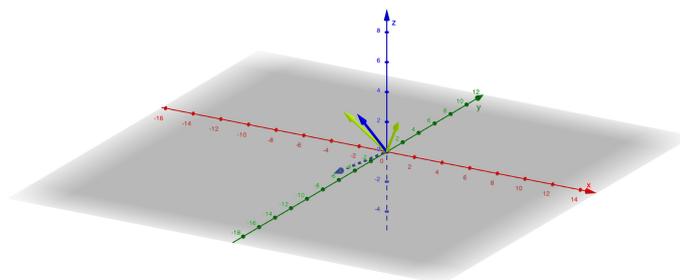
We will use at length the notation  $k$  for a (commutative) field and  $V$  for a  $k$  vector space, which is finite dimensional unless explicitly assumed otherwise.



Unless expressly otherwise stated <sup>4</sup>, rings are assumed to be *commutative* and with a unit element  $1$ , generally denoted  $R$ . Morphisms of rings are maps compatible with addition, product and unit element. Their multiplicative group of units is denoted  $R^\times$ .

We recall that  $R$  is a *domain* (or an integral domain) if  $R$  is nonzero and if the product of two nonzero elements is nonzero. Finally,  $x \in R$  is called *nilpotent* if one of its powers is zero.

As usual, we'll denote by  $E_{i,j} \in M_{p,q}(R)$  the matrix with all coefficients zero except the one at row  $i$  and column  $j$ , which is  $1$ . We call it the "standard basis" of  $M_{p,q}(R)$ , recalling that tautologically every matrix  $A = [a_{i,j}]$  has a unique decomposition  $A = \sum_{i,j} a_{i,j} E_{i,j}$  as a linear combination of these matrices. We say that  $A \in M_{p,q}(R)$  is diagonal if  $a_{i,j} = 0$  for all  $i \neq j$ . The coefficients  $a_{i,i}, i = 1, \dots, \min(p, q)$  are often denoted by  $a_i$  and called the diagonal coefficients. We will identify  $R^n$  as the set of columns  $M_{n,1}(R)$  when  $n \geq 1$  with the canonical family  $e_j = (\delta_{i,j})_i$ , which will be referred to as the canonical basis<sup>5</sup> of  $R^n$ .



Transvection  $T_{1,2}(2)$

We will often use the following square matrices.

**Definition 1.2.2.1** A square matrix is a

<sup>4</sup>We will say explicitly in this case *non commutative ring*.

<sup>5</sup>anticipating the module discussion below.

- *standard transvection*<sup>6</sup> if it is of the form  $T_{i,j}(r) = \text{Id} + rE_{i,j}$ ,  $i \neq j$ ;
- *a permutation matrix* if it is of the form  $M_\sigma = [\delta_{i,\sigma(j)}]$  for a permutation  $\sigma \in S_n$  where  $\delta_{i,j}$  is the Kronecker symbol equal to 1 if  $i = j$  and 0 if not;
- *dilatation* if it is of the form  $D(r) = \text{Id} + (r - 1)E_{1,1}$  with  $r \in \mathbb{R}^\times$ ;
- *a Bézout matrix* if it is of the form  $\text{diag}(A, \text{Id})$  with  $A \in M_2(\mathbb{R})$  of determinant 1.

By construction, transvections and Bézout matrices have determinant 1 and  $\det(D(r)) = r$ ,  $\det(M_\sigma) = \varepsilon(\sigma)$ . In general, it is recalled that line and column operations on rectangular matrices with coefficients in a ring  $\mathbb{R}$  are obtained by multiplication on the right or left by transvections or permutation matrices, these matrices being invertible (of determinant  $\pm 1$ ).

## 1.3 Useful tools

### 1.3.1 Division by monic polynomials

As the reader will see, it is often useful to adapt the usual division algorithm to polynomial rings with values in rings. The price is that we have to assume that the leading coefficient is invertible or, which remains the same, equal to 1. Let us make a precise statement.

**Proposition 1.3.1.1** [Left Euclidean Division] *Let  $\mathcal{R}$  be a non-necessarily commutative ring with unit and  $A, B \in \mathcal{R}[T]$ . If the leading term of  $B$  is invertible, there exists a unique pair  $Q, R \in \mathcal{R}[T]$  such that  $A = BQ + R$  and either  $R = 0$  or  $\deg(R) < \deg P$ .*

If we set  $\deg(0) = -\infty$ , the last condition  $A = BQ + R$  and either  $R = 0$  or  $\deg(R) < \deg P$  can simply be written as  $A = BQ + R$   $\deg(R) < \deg P$ . Of course, there is an analogous statement for right division (change  $\mathcal{R}$  to  $\mathcal{R}^{opp}$  with the multiplication in reverse order). Left and right division coincide in the commutative case (by uniqueness).

*Proof.* Uniqueness If  $(Q_1, R_1)$  and  $(Q_2, R_2)$  satisfy the necessary conditions, then

$$B(Q_1 - Q_2) = R_2 - R_1 \text{ and } \deg(B(Q_1 - Q_2)) = \deg(B) + \deg(Q_1 - Q_2)$$

since the leading coefficient of  $B$  is invertible. Since  $\deg(R_2 - R_1) \leq \max(\deg(R_2), \deg(R_1)) < \deg(B)$  we get  $\deg(Q_1 - Q_2) < 0$ , which gives  $Q_1 = Q_2$  and therefore  $R_1 = R_2$ .

Existence (induction on  $\deg(A)$ ).

<sup>6</sup>If there is no danger of confusion, just call it transvection. See 7.8.13 for the vocabulary.

If  $\deg(A) < \deg(B)$  we take  $Q = 0$  and  $R = A$ ;

If  $\deg(A) \geq \deg(B)$ : let  $a, b$  be the leading coefficients of  $A, B$  and  $M$  the monomial  $b^{-1}aT^{\deg A - \deg B}$ , then  $BM$  has the same leading monomial as  $A$ , so  $\deg(A - BM) < \deg(A)$ . By induction, there are two polynomials  $Q$  and  $R$  such that  $(A - BM) = BQ + R$  and  $\deg(R) < \deg(B)$ , so  $A = BQ + M + R$ .  $\square$

### 1.3.2 Zorn's lemma

Even though it is not necessary for us most of the time, the existence of maximal elements in a great generality is often convenient. Let us explain how Zorn's Lemma (which is equivalent to the axiom of choice) can be used to obtain the existence of maximal ideals.

Let  $E$  be a (partially) ordered set. For example, we can think of the set of subsets of a given set ordered by inclusion. But there are many more examples.

**Definition 1.3.2.1** We say that  $E$  is inductive if every non-empty totally ordered part has an upper bound in  $E$ .

**Example(s) 1.3.2.2**  $\mathbf{R}$  equipped with the usual order relation is not inductive. Similarly, the set of intervals  $[0, x], x \in \mathbf{R}$  ordered by inclusion is not inductive. On the other hand, the set of subsets of a set ordered by inclusion is inductive.



Max Zorn

**Lemma 1.3.2.3 (Zorn's lemma)** Every non-empty inductive set has a maximal element.

This lemma can be seen as an axiom of set theory, in fact equivalent to the axiom of choice: if  $(E_i)$  is a non-empty family of sets, then  $\prod E_i$  is non-empty. We will consider it as such.

**Corollary 1.3.2.4 [Krull's lemma]** Every non-zero ring has a maximal ideal. More generally, every proper ideal of a ring is contained in a maximal ideal.

*Proof.* Let  $E$  be the family of proper ideals of  $A$  containing a given proper ideal  $J$  (for example,  $J = \{0\}$  because our rings are nonzero). Since  $J$  is proper,  $E$  is not empty. Obviously,  $E$  is inductive: the union of a totally ordered family of proper ideals is still a proper ideal, which is an upper bound. Zorn's lemma finishes the job.  $\square$

We could also prove, essentially formally, that just as  $\mathbf{Q}$  is contained in the algebraically closed field  $\mathbf{C}$  (4.6.13), any field  $\mathbf{k}$  is contained in some algebraically closed field  $\Omega$ . We will use this result freely in some (rare) places (see for example [13], Theorem 4.7).

## **Part I**

# **Linear algebra over rings**



## Chapter 2

# Warm-up I: Matrices with ring coefficients



### 2.1 Introduction



#### Perspective

We explain how determinant identities and the Gauss elimination method give non-trivial general results without any reference to advanced linear algebra and reduction theory. This elementary but non-trivial part can be skipped in a first reading.

#### 2.1.1 Review on formal polynomials

We suggest that the reader skip this point, which is for reference only. Formally speaking, algebraic identities are polynomial identities. Let us recall some basic facts. A polynomial with one variable  $P(T) = \sum_{n \in \mathbb{N}} x_n T^n \in R[T]$  is nothing more than the sequence of its coefficients  $x_n \in R$ , assumed to be 0 for all but a finite number<sup>1</sup> of indices  $n$ . The degree  $\deg(P)$  of  $P \neq 0$  is the largest  $n$  such that  $a_n \neq 0$  as usual.

<sup>1</sup>in this case the family is said to be of *finite support* or *almost zero* and the sum is said to be finite)

More generally, let  $I$  be any set and  $I^{(\mathbb{N})}$  be the set of maps  $I \rightarrow \mathbb{N}$  which are zero for all but a finite number of indices<sup>2</sup>. A polynomial with several variables  $P(T_i) = \sum_{\nu=(n_i) \in I^{(\mathbb{N})}} x_\nu T^\nu \in R[T_i, i \in I]$  is nothing but the sequence of its coefficients  $x_\nu$  which are assumed to be 0 for all but a finite number of indices  $\nu$ . If  $\underline{i} = (\delta_{i,j})_{j \in I}$ , the “indeterminate”  $T_i$  is the polynomial  $1 \cdot T^{\underline{i}}$ .

The sum is defined as usual component by component and the product by

$$\sum x_\mu T^\mu \sum y_\nu T^\nu = \sum_{\mu+\nu=\kappa} x_\mu y_\nu T^\kappa$$

, giving  $R[T_i]$  the structure of a commutative ring with unit the constant polynomial associated with the sequence  $\delta_{(0),\mu}$ . As usual, we have  $T_i^0 = 1$  and  $T^\nu = \prod T_i^{\nu_i}$  (which is a finite product by construction).

The most important (universal) property of polynomial rings is summarised in their well-known evaluation rule (see 4.3.0.1). We want to stress the importance of the commutativity assumption (see 2.1.3.1).

**Lemma 2.1.1.1** *Let  $R$  be a commutative ring and  $r_i \in R, i \in I$ . Then there exists a unique evaluation morphism  $Z[T_i] \rightarrow R$  mapping  $T_i$  to  $r_i$ . The image of  $P$  is denoted by  $P(r_i)$ .*

*Proof.* Only the multiplicativity is unclear. With the above notation

$$P(r_i)Q(r_i) = \sum x_\mu r^\mu \sum y_\nu r^\nu = \sum_{\mu+\nu=\kappa} x_\mu y_\nu r^\mu r^\nu \stackrel{\text{commutativity}}{=} \sum_{\mu+\nu=\kappa} x_\mu y_\nu r^\kappa = (PQ)(r_i)$$

with  $r^\mu = \prod r_i^{\mu_i}$  (finite product which does not depend on the order of the factor by commutativity).  $\square$

## 2.1.2 Principle of the permanence of identities

**Proposition 2.1.2.1** *Let  $P \in Z[T_1, \dots, T_n]$  and  $I_i, i = 1, \dots, n$  be infinite sets of some field of characteristic zero  $k$ . If  $P$  vanishes on  $\prod I_i$ , then  $P = 0$ . In particular, for any ring  $R$  and any  $(r_i) \in R^n$ , we have  $P(r_1, \dots, r_n) = 0$ . For example, if a polynomial  $P$  of integral coefficients in the variables  $T_{i,j}, 1 \leq i \leq n, j \leq m$  vanishes on all complex matrices  $[t_{i,j}]$  (or even on some open set) of  $M_{n,m}(\mathbb{C})$ , then for any ring  $R$  and  $M \in M_{n,m}(R)$  we have  $P(M) = 0$ .*

*Proof.* We observe  $Z[T_1, \dots, T_n] \subset k[T_1, \dots, T_n]$  (because the characteristic of  $k$  is zero) and we reduce by induction to the fact that a polynomial in one variable not identically zero has only a finite number of roots.  $\square$

<sup>2</sup>This condition is not empty only for infinite  $I$ , which will rarely be useful to us.

**Corollary 2.1.2.2** *All integral formulas for the determinant which are valid for complex square matrices remain valid for square matrices in any commutative ring  $\mathbb{R}$ .*

*This is in particular the case for the Cramer's rule  ${}^t \text{Com}(A)A = A {}^t \text{Com}(A) = \det(A) \text{Id}$  for any  $A \in M_n(\mathbb{R})$  and its corollary the multiplicative group  $\text{GL}_n(\mathbb{R})$  of matrices having an inverse is equal to  $\{A \in M_n(\mathbb{R}) \mid \det(A) \in \mathbb{R}^\times\}$ .*

This also allows us to consider the special linear group  $\text{SL}_n(\mathbb{R}) = \text{Ker}(\text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times)$  which is of fundamental importance.

**Remark(s) 2.1.2.3** *As the interested reader can check, all formal properties of the determinant can easily be proved directly for matrices with coefficients in a ring without using any linear algebra in a field.*

### 2.1.3 Cayley-Hamilton in $M_n(\mathbb{R})$

Let us start with a simple lemma, which is usually considered more or less "obvious" in a commutative situation.

Let  $\tau \in \mathcal{R}$  be an element of a non-necessary commutative ring with unit  $\mathcal{R}$  and let  $\mathcal{R}[T] \rightarrow \mathcal{R}$  be the evaluation additive group morphism

$$P(T) = \sum_{i \geq 0} \pi_i T^i \mapsto P(\tau) = \sum_{i \geq 0} \pi_i \tau^i$$

In this non-commutative situation we have to be careful with its multiplicativity.

**Lemma 2.1.3.1** *Let  $P = \sum_i \pi_i T^i, \bar{P} = \sum \bar{\pi}_i T^i \in \mathcal{R}[T]$  and assume that  $t$  commutes with all the coefficients  $\bar{\pi}_i$  of  $\bar{P}$ . Then,*

$$(P\bar{P})(\tau) = P(\tau)\bar{P}(\tau).$$

*Proof.* We have

$$[P\bar{P}](\tau) = \sum_k \left( \sum_{i+j=k} \pi_i \bar{\pi}_j \right) \tau^k = \sum_{i,j} \pi_i \bar{\pi}_j \tau^{i+j}$$

and

$$P(\tau)\bar{P}(\tau) = \sum_i \pi_i \tau^i \sum_j \bar{\pi}_j \tau^j = \sum_{i,j} \pi_i \tau^i \bar{\pi}_j \tau^j \stackrel{\tau^i \bar{\pi}_j = \bar{\pi}_j \tau^i}{=} \sum_{i,j} \pi_i \bar{\pi}_j \tau^{i+j}$$

□

**Corollary 2.1.3.2** (Cayley-Hamilton) *Let  $A \in M_n(\mathbb{R})$  and  $\chi_A(T) = \det(T \text{Id} - A)$ . Then,  $\chi_A(A) = 0$ .*

*Proof.* For the first point, Cramer's rule applied to  $T \text{Id} - A \in M_n(\mathbb{R}[T]) = M_n(\mathbb{R})[T]$  gives the identity  $(*) {}^t \text{Com}(T \text{Id} - A)(T \text{Id} - A) = \chi_A(T) \text{Id}$ .

Since  $A$  commutes with the two coefficients  $\text{Id}$ ,  $A$  of  $T \text{Id} - A$ , the lemma 2.1.3.1 shows that the evaluation of  $(*)$  at  $\tau = A$  is the product of the evaluation of  ${}^t \text{Com}(T \text{Id} - A)$  at  $\tau = A$  and the evaluation at  $\tau = A$  of  $T - A$ , which is zero. So is the evaluation  $\chi_A(A)$  on the right.  $\square$

## 2.2 Maximal rank matrices

As usual, each  $A \in M_{p,q}(\mathbb{R})$  is identified with the ( $\mathbb{R}$ -linear) map  $X \mapsto AX$  from  $\mathbb{R}^q$  to  $\mathbb{R}^p$ . We assume that  $\mathbb{R}$  is not the zero ring.

**Proposition 2.2.0.1** *Let  $p, q$  ne positive integers and  $A \in M_{p,q}(\mathbb{R}), B \in M_{q,p}(\mathbb{R})$*

1. *If  $q < p$ , then  $\det(AB) = 0$ .*
2. *If  $A$  is surjective, then  $q \geq p$ .*
3. *If  $A$  is injective then  $q \leq p$ .*
4. *If  $A$  is bijective then  $q = p$*

*Proof.* (1). As before, we consider the generic matrices  $A = (X_{i,j}), B = (Y_{j,i})$  with  $X_{i,j}, Y_{j,i}, 1 \leq i \leq p, 1 \leq j \leq p$  are indeterminates and we look in the general matrix identity  $\det(AB) = 0$  which is a polynomial identity of  $q^2 p^2$  indeterminates in  $\mathbb{Z}[X_{i,j}, Y_{j,i}]$ . But this identity is true for complex matrices  $A_c, B_c$  because the square matrix  $A_c B_c$  cannot be injective because  $B_c : \mathbb{C}^p \rightarrow \mathbb{C}^q$  is not (for dimensional reasons).

(2). Let  $B_j \in \mathbb{R}^q, j = 1, \dots, m$  be such that  $AB_j = E_{1,j}$  ( $E_{1,j}$  is the usual "canonical basis" of  $\mathbb{R}^q$ ) and  $B \in M_{q,p}(\mathbb{R})$  be the corresponding matrix. You have  $AB = \text{Id}_q$ . Taking the determinant, we get  $q \geq p$  thanks to (1).

(3). Assume by contradiction  $q > p$  and let  $B = \begin{pmatrix} \text{Id}_p \\ 0_{q-p} \end{pmatrix}$  which defines the canonical injection  $\mathbb{R}^p \hookrightarrow \mathbb{R}^q$ . Let  $C = BA \in M_q(\mathbb{R})$  and  $L = (0, \dots, 0, 1) = E_{1,q} \in M_{1,q}(\mathbb{R})$ . Since  $q > p$ , you have  $LB = 0$ . By Cayley-Hamilton there exists a monic polynomial  $T^d + \sum_{i < d} a_i T^i$  which annihilates  $C$ . We can assume that  $d$  is minimal among these polynomials. Since  $C$  is injective as  $B$  and  $A$ , one has  $a_0 \neq 0$  by minimality. Left composing the equation  $C^d + \sum_{i < d} a_i C^i = 0$  with  $L$ , we get  $a_0 L = 0$  and therefore  $a_0 = 0$ , a contradiction.

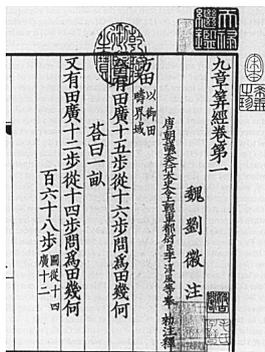
(4). Any (2) or (3) implies (4) (apply for both  $A$  and  $A^{-1}$ , the latter being defined as usual because  $A$  is bijective). □

**Remark(s) 2.2.0.2**

- A more natural, but less elementary, proof will be given below. Specifically, see 4.6.9 for (2) and (4) with an argument using the choice axiom, and 5.3.7 for (2), (3) and (4) with an argument not using the choice axiom. The idea in this last case is to reduce to this statement by reducing to the case of a matrix with coefficients in a field using Krull's lemma(1.3.2.4).
- I have learned the nice argument in (3) from the post <https://mathoverflow.net/q/47846> of Balasz Strenner.

## 2.3 Reminder on Gauss elimination method

Let us give a version of Gauss elimination which, as far as possible, does not use dilatations or permutation matrices.



The nine chapters



Karl Friedrich Gauss

The elimination method was rediscovered by Gauss and Jordan in the 19th century. But it was known to the Chinese at least in the 1st century BCE ([8]).

With definition 1.2.2.1 in mind, we set

**Definition 2.3.0.1** Let  $R$  be a ring and  $p, q \geq 1$  two integers. We denote by  $E_n(R)$  the subgroup of  $GL_n(R)$  generated by the transvections. We say that two matrices  $A, B$  of  $M_{p,q}(R)$  with  $p, q \geq 1$  are

- Gauss-equivalent ( $A \equiv B$ ) if they differ by a series of left and right multiplications by transvections (that we call Gauss-operations) or equivalently if there exists  $P \in E_p(R), Q \in E_q(R)$  with  $B = P^{-1}AQ$ ;

- equivalent ( $A \sim B$ ) if there exists matrices  $P \in GL_p(\mathbb{R})$ ,  $Q \in GL_q(\mathbb{R})$  with  $B = P^{-1}AQ$ .

Gauss equivalent  $\Rightarrow$  equivalent. Note also that the Gauss equivalence *a priori* uses permutation matrices. But they are hidden in the definition (see 2.3.1.1).

### 2.3.1 Some universal formulas

Although the reader can skip this (elementary) section, the following examples will be quite useful (see 8.4.0.1 below). This also illustrates how permutation matrices can play (or do not play) a role in the Gauss elimination method, no matter what the coefficients ring is a field. Recall that  $\mathbb{R}$  is an arbitrary (commutative) ring.

#### Lemma 2.3.1.1

1. Let  $D$  be an invertible diagonal matrix of  $M_n(\mathbb{R})$ . Then,  $D \equiv \text{diag}(\det(D), 1, \dots, 1)$ .
2. Let any permutation matrix  $M_\sigma$ ,  $\sigma \in S_n$  is Gauss equivalent in  $M_n(\mathbb{Z})$  hence in  $M_n(\mathbb{R})$  to  $\text{diag}(\varepsilon(\sigma), 1, \dots, 1)$ .
3. Let  $t, a_0, \dots, a_{n-1} \in \mathbb{R}$  and

$$C(t, a_{n-1}, \dots, a_0) = \begin{pmatrix} t & 0 & \cdots & a_{n-1} \\ -1 & t & 0 & \cdots & a_{n-2} \\ \vdots & \ddots & \ddots & \cdots & \vdots \\ \cdots & 0 & -1 & t & a_1 \\ \cdots & \cdots & 0 & -1 & a_0 \end{pmatrix} \in M_n(\mathbb{R}).$$

Then,  $C(t, a_{n-1}, \dots, a_0) \equiv \text{diag}(1, \dots, 1, \sum a_i t^{n-i})$ .

*Proof.*

1. An easy induction argument reduces to the  $n = 2$  case. And we just perform the Gauss operations (having in mind that the determinant remains 1 to simplify the computations<sup>3</sup>)

$$\begin{pmatrix} \mathbf{x} & 0 \\ 0 & y \end{pmatrix} \stackrel{\text{Col}}{\equiv} \begin{pmatrix} x & \mathbf{x} \\ 0 & y \end{pmatrix} \stackrel{\text{Lin}}{\equiv} \begin{pmatrix} x & x \\ 1-y & \mathbf{1} \end{pmatrix} \stackrel{\text{Col}}{\equiv} \begin{pmatrix} xy & x \\ 0 & \mathbf{1} \end{pmatrix} \stackrel{\text{Lin}}{\equiv} \begin{pmatrix} xy & 0 \\ 0 & \mathbf{1} \end{pmatrix}$$

2. Induction on  $n$  starting with the tautological  $n = 1$ . As always, the key point is  $n = 2$  which is solved thanks to the formula

$$(*) \quad M_{(1,2)} = \text{diag}(-1, 1)T_{1,2}(-1)T_{2,1}(1)T_{1,2}(-1) = T_{1,2}(1)T_{2,1}(-1)T_{1,2}(1) \text{diag}(-1, 1)$$

<sup>3</sup>We indicate the pivot and the bold coefficient is the pivot

If  $n > 2$ , using  $(1, 2, 3) = (1, 2)(2, 3)$  and  $(*)$ , we get that  $M_{(1,2,2)}$  is the product of  $(6!)$  transvections. In particular, a product of an even number of transvections is Gauss-equivalent to  $\text{Id}$  and finally using  $(*)$  again, we get the result.

3. Using successive columns operations of type  $C_n \mapsto C_n + x_j C_{n-j}$  for  $j > 1$ , we put zeros on the last column to get by inductions the equivalences

$$C(t, a_{n-1}, \dots, a_0) \equiv C(t, a_{n-1}, \dots, a_{p+1}, a_p + a_{p-1}t + \dots + a_0 t^p, 0, \dots, 0)$$

and finally

$$C(t, a_{n-1}, \dots, a_0) \equiv C(t, \sum a_i t^{n-i}, 0, \dots, 0) = C(t, 1, 0, \dots, 0) \cdot \text{diag}(1, \dots, 1, \sum a_i t^{n-i}).$$

But

$$C(t, 1, 0, \dots, 0) = \begin{pmatrix} t & 0 & \dots & 1 \\ -1 & t & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \dots & \vdots \\ \dots & 0 & -1 & t & 0 \\ \dots & \dots & 0 & -1 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & \dots & 1 \\ -1 & t & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \dots & \vdots \\ \dots & 0 & -1 & t & 0 \\ \dots & \dots & 0 & -1 & 0 \end{pmatrix}$$

and using line operations

$$\begin{pmatrix} -\mathbf{1} & t & 0 & \dots \\ \vdots & \ddots & \ddots & \dots \\ \dots & 0 & -1 & t \\ \dots & \dots & 0 & -1 \end{pmatrix} \equiv \begin{pmatrix} -1 & 0 & 0 & \dots \\ \vdots & \ddots & \ddots & \dots \\ \dots & 0 & -1 & t \\ \dots & \dots & 0 & -1 \end{pmatrix} \equiv \dots \equiv -\text{Id}_{n-1}$$

and therefore

$$C(t, 1, 0, \dots, 0) \equiv C(0, 1, 0, \dots, 0) = \text{diag}(1, -\text{Id}_{n-1})M_\sigma$$

where  $\sigma$  is the  $n$ -cycle  $(1, 2, \dots, n)$  of signature  $\varepsilon(\sigma) = (-1)^{n-1}$  giving the result by (1) and (2).

□

### 2.3.2 The usual field case

**Proposition 2.3.2.1** *Let  $A \in M_{p,q}(\mathbf{k}) - \{0\}$ .*

1. *There exists  $\delta \in \mathbf{k}^*$  such that  $A$  is Gauss-equivalent to  $\text{diag}(\delta, \text{Id}_\rho, 0_{p-\rho, q-\rho})$  with  $\rho = \text{rank}(A) - 1$ .*
2.  *$\text{GL}_n(\mathbf{k})$  is generated by transvections and dilatations.*
3.  *$\text{SL}_n(\mathbf{k})$  is generated by transvections.*

*Proof.*

(1). Induction on  $p + q \geq 2$ , the case  $p + q = 2$  being trivial we assume now  $p > 1$  or  $q > 1$ . If both the last column and line are zero, one applies the induction to the (necessarily non zero) remaining  $M_{p-1, q-1}(\mathbf{k})$  matrix.

The key point is showing that a non zero line  $(x, y)$  is Gauss equivalent to  $(0, 1)$ . We perform column operations with the pivot written in bold and the other (changing coefficient) by a  $\star$ . Because  $(\mathbf{x}, 0) \equiv (\star, x)$  we can assume  $y \neq 0$ . Then, we have,  $(\star, \mathbf{y}) \equiv (\mathbf{1}, \star) \equiv (\mathbf{1}, 0) \equiv (\star, \mathbf{1}) \equiv (0, 1)$  as wanted.

Transposing if necessary, we can assume that either the last line is nonzero, *i.e.* there exists  $j < q$  such that  $a_{p,j} \neq 0$ . Using the previous case (for the line of indices  $j, q$ ), one can assume  $a_{p,q} = 1$ .

Then, again using Gauss-operations  $C_j \mapsto C_j - a_{p,j}C_q$  and  $L_i \mapsto L_i - a_{i,q}C_q$ , one can now assume that the only non zero coefficient of the last line and column is  $a_{p,q} = 1$  and we finish by induction on the remaining  $M_{p-1, q-1}(\mathbf{k})$  matrix.

(2) and (3) are direct consequences of (1). □

Recall that the derived subgroup  $D(G)$  of a group  $G$  is the subgroup *generated* by the commutators  $[g, h] = ghg^{-1}h^{-1}$ ,  $g, h \in G$ . It is normal and  $G/D(G)$  is the largest abelian quotient of  $G$ .

**Corollary 2.3.2.2** *One has*

1.  $D(\mathrm{GL}(V)) = \mathrm{SL}(V)$  *except if*  $n = 2$  *and*  $\mathrm{Card}(\mathbf{k}) = 2$ .
2.  $D(\mathrm{SL}(V)) = \mathrm{SL}(V)$  *except if*  $n = 2$  *and*  $\mathrm{Card}(\mathbf{k}) = 2, 8$ .

A group  $G$  with  $D(G) = G$  is called perfect.

*Proof.* We identify  $V$  and  $\mathbf{k}^n$  by the choice of a basis of  $V$ . Proof of (1). Because the derived group is normal and all transvections are conjugate in  $\mathrm{GL}_n$  (due to the relation  $E_{\sigma(i), \sigma(j)} = M_\sigma E_{i,j} M_\sigma^{-1}$  for  $\sigma \in S_n$ ), it is enough to show that in our case one transvection is a commutator. If  $n \geq 3$  and any characteristic, one computes  $[\mathrm{Id} + E_{2,1}, \mathrm{Id} + E_{1,3}] = \mathrm{Id} + E_{2,3}$ . If  $n = 2$ , let us choose  $\lambda \neq 0, 1$ . Then,  $[\mathrm{diag}(\lambda, 1), T_{1,2}(\lambda)] = T_{1,2}(\lambda - 1)$  which is a transvection.

Proof of (2). If  $n \geq 3$ , two transvections  $\tau' = g\tau g^{-1}$  are certainly conjugate not only under  $\mathrm{GL}_n$  [Because one can change  $g$  by a dilation of ratio  $\det(g)^{-1}$  commuting with  $\tau$ ]. We leave the  $n = 2$  case in exercise (adapt the  $\mathrm{GL}_n$  argument with a general diagonal matrix in  $\mathrm{SL}_2$ ). □

Let  $V$  be an  $n$ -dimensional vector space with  $n \geq 2$ ,  $\mathbf{P}V$  its set of lines (dimension 1 linear subspaces),  $\mathbf{P}V^*$  its set of hyperplanes (dimension  $(n - 1)$  linear subspaces)<sup>4</sup>.

<sup>4</sup>At this stage, this is just a notation. Nothing has to be known about projective geometry.

### 2.3.3 Normal subgroups of $GL(V)$

We will explain the so-called Iwasawa to study normal subgroups of perfect groups  $G$ , or equivalently we will give a criterium of simplicity of  $G/Z(G)$  where  $Z(G)$  is the centrum of  $G$ .

**Definition 2.3.3.1** Let  $G$  be a group acting on a set  $X$ , and  $B \subseteq X$ .

1. We say that  $B$  is a  $G$ -block and if for all  $g \in G$ , the sets  $gB$  and  $B$  are either equal or disjoint. Blocks reduced to a point or to the whole  $X$  are called trivial.
2. We say  $G$  acts primitively on  $X$  if:
  - (a) The action of  $G$  on  $X$  is transitive;
  - (b) the only  $G$ -blocks are trivial.<sup>5</sup>
3. We say  $G$  acts 2-transitively on  $X$  if for all  $x_1, x_2, y_1, y_2 \in X$ ,  $x_1 \neq x_2$ ,  $y_1 \neq y_2$ , there exists  $g \in G$  such that  $g \cdot x_1 = y_1$  and  $g \cdot x_2 = y_2$ .

**Lemma 2.3.3.2** Let  $G$  be a group acting 2-transitively on a set  $E$ . Then the action is primitive.

For instance,  $SL(V)$  and  $GL(V)$  act 2-transitively on  $PV$  if  $\dim(V) \geq 2$ .

*Proof.* Let  $B$  be a subset of  $X$  having at least two elements and such that  $B \neq X$ . Let us show that there exists  $g \in G$  such that  $gB \neq B$  and  $gB \cap B \neq \emptyset$  and therefore that  $B$  is not a  $G$ -block.

Let  $a \neq b \in B$  and  $c \in X \setminus B$ . By 2-transitivity, there exists  $g \in G$  such that  $ga = a$  and  $gb = c$ . We have  $a \in gB \cap B$ , hence  $gB \cap B \neq \emptyset$ , and  $c \in gB$ ,  $c \notin B$ , hence  $gB \neq B$ .  $\square$

**Proposition 2.3.3.3 (Iwasawa criterium)** Let  $G$  be a group acting faithfully and primitively on a set  $X$ . We assume that there exists a family  $K_x \subset G_x$ ,  $x \in X$  such that

1. Each  $K_x$  is abelian.
2. For any  $g \in G$ ,  $G = \langle gK_xg^{-1} \rangle$ .
3.  $\cup_{x \in X} K_x$  generates  $G$ .

Then any normal subgroup acting non trivially on  $X$  contains  $D(G)$ .

*Proof.* We start with the direct part of the previous footnote.

<sup>5</sup>Or equivalently (exercise) if the stabilizer  $G_x$  of a point  $x \in X$  is a maximal subgroup of  $G$ .

**Lemma 2.3.3.4** *The stabilizer  $G_x$  of any primitive action is a maximal subgroup of  $G$ .*

*Proof.* Let  $G_x \subset H \subset G$  and  $B = \{hx, h \in H\}$ . I claim that  $B$  is a block. If not, assume  $B \cap g(B) \neq \emptyset$ . There exists  $h, h' \in H$  such that  $hx = gh'x$  hence  $h^{-1}gh' \in G_x \subset H$ . Therefore,  $g \in H$  and  $g(B) \subset B$  proving  $B = \{x\}$  and  $B = X$  by primitivity assumption. In the first case,  $H = G_x$  and we are done. In the second case,  $H$  acts transitively on  $X$ . Therefore, for any  $g \in G$  there exists  $h \in H$  such that  $gx = hx$  hence  $gh^{-1} \in G_x \subset H$  showing  $g \in H$ .  $\square$

Let  $N$  be a normal subgroup and let  $x \in X$ . Since  $N$  is normal,  $NG_x$  is a subgroup of  $G$  containing  $G_x$  and is therefore equal to  $G_x$  or  $G$  by maximality.

If  $NG_x = G_x$ , we have  $N \subseteq G_x$ , and therefore for all

$$g \in G, gNg^{-1} \subset gG_xg^{-1} = G_{gx}.$$

By normality of  $N$ , we get  $N = N \cap gNg^{-1} \subset G_x \cap G_{gx}$ , hence  $N$  acts trivially on  $X$  and therefore  $N = \{1\}$  because  $G$  hence  $N$  acts faithfully on  $X$ : we are done in this case.

Assume now  $NG_x = G$ . One has  $Nx = NG_x x = Gx = X$  because  $G$  acts transitively and therefore  $N$  acts transitively on  $X$ . Let  $y = nx, n \in N$  be any point of  $X$  and  $\kappa \in K_y = nK_x n^{-1}$  which can therefore be written  $\kappa = nkn^{-1}$  with  $(n, k) \in N \times K_x$ . We have

$$\kappa = nkn^{-1} = nkn^{-1}k^{-1}k \stackrel{N \triangleleft G}{\in} NK_x$$

proving  $K_y \subset NK_x$  for any  $y \in X$  hence  $G = NK_x$ . We deduce that the morphism  $k \mapsto k \bmod N$  is a surjection from the abelian group  $K_x$  to  $G/N$  commutative hence  $N \subset D(G)$ .  $\square$

**Corollary 2.3.3.5** *If  $\dim(V) \geq 2$ , any normal non trivial normal subgroup of  $GL(V)$  (or  $SL(V)$ ) contains  $SL(V)$  unless  $\mathbf{k}$  is a field with 2 (or 8) elements.*

*Proof.* Take  $X = \mathbf{P}(V)$  and  $K_x \xrightarrow{\sim} \text{Hom}(V/D_x, D_x)$  be the group of transvections of line  $D_x$  (cf. 7.8.8) and apply Iwasawa criterium and 2.3.2.2.  $\square$

## 2.4 Exercises

**Exercise 2.4.1** *Let  $\mathbf{k}$  be a field and  $R$  a ring.*

1. *Assume that  $R$  is a domain and let  $P, Q \in R[T] - \{0\}$ . Prove  $\deg(PQ) = \deg(P) + \deg(Q)$  and deduce that  $R[T]$  is a domain.*
2. *Show that the invertible elements of  $\mathbf{k}[T]$  are the non-zero constant polynomials from  $\mathbf{k}^*$  (compare with 2.4.7).*

3. Show that a matrix from  $M_n(\mathbf{R})$  is invertible if and only if its determinant is an invertible of  $\mathbf{R}^\times$ .
4. Deduce that  $M \in M_n(\mathbf{k}[\mathbf{T}])$  is invertible if and only if  $\det(M) \in \mathbf{k}^*$ .

**Exercise 2.4.2** Prove that the evaluation map of lemma 2.1.3.1 is a (skew)-ring morphism if and only if  $t$  commutes with any element of  $\mathcal{R}$ .

**Exercise 2.4.3** Give an example of square matrices  $\tau, A \in M_2(\mathbf{C})$  such that the evaluation at  $\tau$  of  ${}^t \text{Com}(\text{T Id} - A)(\text{T Id} - A) = \chi_A(\text{T Id})$  is not equal to the products of the evaluation at  $\tau$  of  ${}^t \text{Com}(\text{T Id} - A)$  and of  $(\tau - A)$ . What is the value of  $\chi_A(\tau)$  in this case ?

**Exercise 2.4.4** With the notation above prove the identity

$$\text{T}^n \chi_{AB}(\text{T}) = \text{T}^m \chi_{BA}(\text{T})$$

Hint : Consider the matrices  $C = \begin{bmatrix} \text{T Id}_m & B \\ A & \text{I}_n \end{bmatrix}$ ,  $D = \begin{bmatrix} \text{Id}_m & -B \\ 0 & \text{T Id}_n \end{bmatrix}$ . Give another proof of 2.1.3.2.(2)

**Exercise 2.4.5** Prove that  $\text{GL}_n, +(\mathbf{R})$  and  $\text{GL}_n(\mathbf{C})$  are connected (for their usual metric topology). Same questions for  $\text{SL}_n$ .

**Exercise 2.4.6** Give a computer program of 2.3.2.1 for instance using the open source SAGE mathematical software (with Python kernel). Evaluate its complexity and numerical complexity. How can you guarantee that your program is exact for matrix with rational coefficients ?

**Exercise 2.4.7** Let  $R$  be a ring and  $P = \sum_{i=0}^n a_i \text{T}^i \in R[\text{T}]$ .

1. Let  $x$  be a nilpotent element of  $R$ . Show that  $1 + x$  is invertible.
2. Show that  $P$  is nilpotent if and only if for all  $i \in \mathbf{N}$ ,  $a_i$  is nilpotent.
3. Show that  $P$  is invertible in  $R[\text{T}]$  if and only if  $a_0$  is invertible and for all  $i \geq 1$ ,  $a_i$  is nilpotent. Hint: if  $Q = \sum_{i=0}^m b_i \text{T}^i$  is an inverse of  $P$ , one could start by showing that for all  $r \geq 0$ ,  $a_n^{r+1} b_{m-r} = 0$ .

**Exercise 2.4.8** Let  $G$  act primitively and faithfully on a set  $X$ . Assume that for some  $x \in X$ , the  $G_x$  contains an abelian normal subgroup whose conjugate subgroups generate  $G$ . Then  $D(G) \subset G$  [Adapt the proof of Iwasawa criterium].

**Exercise 2.4.9** (Dedekind's independence lemma) Let  $G$  be a group and  $\chi_1, \dots, \chi_n : G \rightarrow \mathbf{k}^*$  distinct morphisms of groups. Show that the family  $(\chi_i)$  is free in the  $\mathbf{k}$ -vector space  $\text{Map}(G, \mathbf{k})$  [By contradiction, starting with a non trivial dependence relation of minimal length relation  $\sum \lambda_i \chi_i = 0$  with  $\lambda_i \in \mathbf{k}$ , construct a shorter one by evaluating this relation at  $g$  and  $gh$  for  $h$  suitably chosen].



# Chapter 3

## Modules



### 3.1 Introduction



#### Perspective

This chapter introduces the language of modules and diagrams in as light a manner as possible. The idea behind this is that all formal constructions of vector spaces or abelian groups apply *mutatis mutandis* to this general framework by accepting scalars valued in a ring rather than a field (or integers for abelian groups). As we shall see here and throughout the text, the diagrammatic perspective (see 3.4), once familiar, is extremely valuable, unifying and simplifying. Paradoxically, this attempt at abstraction not only opens the doors to deep, modern mathematics, but often makes it very concrete, even computable and algorithmic.

It is suggested that the reader first quickly browse through Section 3.2 to pay close attention to the next points (properties of the cokernel (3.5.0.1),  $k[T]$ -module associated to a vector endomorphism (3.7), fitting ideals) and then focus directly on the exercises. This will allow him to become progressively and concretely involved in these topics during the next chapters.

---

<sup>0</sup>See for example section 8.2 and chapters ?? and 13 dedicated to the study of the linear group and the similarity classes of square matrices.

Unlike the usual methods of linear algebra, which depend largely on the study of eigenvalues of endomorphisms, we will focus on polynomials and their action on endomorphisms. While annihilating polynomials play a special role, their roots are not really important in deciding whether two endomorphisms are similar. The advantage is that we usually do not know how to compute the roots of polynomials. Worse, the constructions of linear algebra are often discontinuous in the coefficients of matrices and thus poorly support the numerical approximation of these roots (13). Of course, the notion of eigenvalue remains essential, as will be seen repeatedly. But it is often useless if one cannot compute the roots of the characteristic polynomial or, worse, if the characteristic polynomial does not divide.

## 3.2 Definitions and first examples

We know that a vector space over a field  $k$  is an abelian group  $M$  equipped with an external law  $k \times M \rightarrow M$  verifying four usual compatibilities rules. The notion of a module is obtained exactly in the same way, by allowing the field  $k$  to be a ring  $R$  (recall that for us  $R$  is commutative with unit).

**Definition 3.2.0.1** *Let  $R$  be a ring.*

- An  $R$ -module  $M$  (or module over  $R$ ) is an abelian group equipped with a “scalar multiplication” map  $R \times M \rightarrow M$  verifying the four compatibility rules: for any  $x, x' \in R$  and  $m, m' \in M$

1.  $x(m + m') = xm + xm'$

2.  $(x + x')m = xm + x'm$

3.  $1m = m$

4.  $x(x'm) = (xx')m$

- A submodule  $N$  of  $M$  is a subgroup stable by scalar multiplication.
- A morphism of modules  $f : M \rightarrow M'$  is a morphism of abelian groups between two modules  $M, M'$  such that for all  $x \in R, m \in M$  we have  $f(xm) = xf(m)$ . The set of these morphisms is denoted by  $\text{Hom}_R(M, M')$ .

As in classical linear algebra,  $\text{Hom}_R(M, M')$  has a natural  $R$ -module structure (**exercise**) and as in linear algebra,  $f \in \text{Hom}_R(M, M')$  has an inverse  $g \in \text{Hom}_R(M', M)$  if and only if  $f$  is both injective and surjective (**exercise**).

**Example(s) 3.2.0.2** *By definition, modules over fields are vector spaces. Let's provide more interesting examples.*

1. The multiplication of  $R$  makes  $R$  an  $R$ -module whose submodules are by the very definition its ideals.

2.  $\mathbf{Z}$ -modules are identified with abelian groups through scalar multiplication

$$n.m = \text{sign}(n) \sum_{i=0}^{|n|} m, \quad n \in \mathbf{Z}, m \in M.$$

3. In general, if  $M$  is an arbitrary  $R$ -module and  $x \in R$ , we denote  $\text{Ann}_M(x) = \text{Ker}(M \xrightarrow{x} M)$  and  $M[r] = \cup_{n>0} \text{Ker}(M \xrightarrow{x^n} M)$ , which is indeed a submodule as a union of increasing submodules (*exercice*).

4. The set  $C_c(X, \mathbf{R})$  of continuous functions with compact support from a topological space  $X$  to  $\mathbf{R}$  is a module over the ring of continuous functions from  $X$  to  $\mathbf{R}$ . If  $T$  is a non-compact metric space,  $C_c(X, \mathbf{R})$  is an ideal but not a ring (*exercice*). This ideal is not finitely generated for example if  $X = \mathbf{R}^n$  (*exercice*).

5. Let  $M_i, i \in I$  be a family of modules. As in linear algebra, the abelian group product  $\prod M_i$  has a natural module structure: it is the unique structure such that all projections  $\pi_j : \prod M_i \rightarrow M_j$  are linear. In other terms,  $a.(m_i) = (am_i)$  (cf. 3.6.1).

6. With the previous notation, the subset  $\oplus M_i$  of  $\prod M_i$  consisting of almost null families is a submodule called the direct sum of  $M_i$ . The (finitely supported) family  $(m_i)$  is often denoted  $\sum m_i$ . If  $I$  is furthermore finite, then  $\oplus M_i = \prod M_i$  (cf. 3.6.1).

7. If  $V$  is a  $\mathbf{k}$ -vector space (or more generally an  $R$ -module), the set of formal polynomials<sup>1</sup> with coefficients in  $V$  is naturally a  $k[T]$ -module. Precisely, as a  $\mathbf{k}$ -vector space,  $V[T]$  is the set of formal polynomials with  $V$ -coefficients<sup>2</sup>

$$V[T] = \left\{ \sum_{\text{finite}} v_i T^i \right\} \xrightarrow{\sim} \oplus_{\mathbf{N}} V.$$

The scalar multiplication is then characterised by  $T \sum v_i T^i = \sum v_i T^{i+1}$ .

The following table summarizes how the formal constructions of linear algebras adapt to modules. To simplify the notation, the Greek letters  $\lambda, \mu \dots$  denote elements of a ring  $R$ , while the Latin letters  $x, m, n \dots$  denote elements of modules. The statements are implicitly universally quantified. So we write  $\lambda(\mu x) = (\lambda\mu)x$  for  $\forall \lambda, \mu \in R$  and  $\forall x \in M$ , we have  $\lambda(\mu x) = (\lambda\mu)x$ .

<sup>2</sup>That is, sums  $\sum_{i \geq 0} v_i T^i$  with  $v_i = 0$  if  $i$  is large enough.

 Generalities for modules		
Property/Definition	Vector space	Module
Scalars $R$	$R = \text{field}$	$R = \text{ring}$
Addition	$(M, +)$ abelian group	
External multiplication	$\lambda(\mu x) = (\lambda\mu)x$ and $1x = x$	
Distributivity	$\lambda(x + y) = \lambda x + \lambda y$ , $(\lambda + \mu)x = \lambda x + \mu x$	
Linear combination	$\sum_{\text{finite}} \lambda_i x_i$	
Subspace $N$	$N$ stable by linear combinations	
Generated subspace $\langle x_i \rangle$	$\langle x_i \rangle = \{\text{linear combinations of } x_i\}$	
Sum of subspaces $N_i$	$+N_i = \{\text{linear combinations of } x_i \in N_i\}$	
Product <sup>3</sup> of $N_i$	$\prod N_i = \{(x_i), x_i \in N_i\}$	
Direct sum <sup>3</sup> of $N_i$	$\oplus N_i = \{(x_i) \in \prod N_i \mid \text{Card}\{i \mid x_i \neq 0\} < \infty\}$	
$R^{(I)}, R^n$	$R^{(I)} = \oplus_I R$ , $R^n = \oplus_{i=1}^n R = \prod_{i=1}^n R$	

 Generalities on morphisms		
Property/Definition	Vector space	Module
Morphism $f \in \text{Hom}_R(M, M')$	morphisms of groups $\mid f(\lambda x) = \lambda f(x)$	
$f$ injective	$\text{Ker}(f) = \{0\}$	
Isomorphism	Bijective morphism	
$\text{Hom}_R(R^n, M)$	$\text{Hom}_R(R^n, M) \xrightarrow{f \mapsto (f(e_j))_j} M^n$	
Matrices	$\text{Hom}_R(R^n, R^m) = M_{m,n}(R)$	

### 3.3 Quotient, cokernel

The problem we are tackling is as follows. Let  $f : M \rightarrow N$  be a morphism of  $R$ -modules. The injectivity of  $f$  is characterized by the nullity of the kernel, denoted by  $\text{Ker}(f)$ . Is there a module whose nullity can

<sup>3</sup>See 3.6.1.

be used to measure the surjectivity of  $f$ ? We define a relation on  $N$  by the condition

$$n \sim n' \text{ if and only if } \exists m \text{ such that } n - n' = f(m).$$

This is an equivalence relation thanks to the additivity of  $f$ . The equivalence class of  $n \in N$  is defined as follows:

$$\bar{n} = \{n + f(m), m \in M\} = n + f(M)$$

We denote  $\text{Coker}(f)$  the set of equivalence classes of  $\sim$ . Thus, as a set,

$$\text{Coker}(f) = \{n + f(M), n \in N\}$$

and the application  $\pi : N \rightarrow \text{Coker}(f)$  defined by  $n \mapsto \pi(n) = \bar{n}$  is surjective. The following statement is both immediate and significant.

**Proposition 3.3.0.1** *There exists a unique  $R$ -module structure on  $\text{Coker}(f)$  such that  $\pi$  is a morphism. This structure is characterized by the following properties:  $n + n' = n + n'$  and  $n + n'$  is the neutral element, denoted by  $0$ . Furthermore,  $f$  is surjective if and only if  $\text{coker}(f) = 0$ .*

This completes the solution to the problem. A notable and fundamental case arises when  $f$  is the inclusion of a submodule.

**Definition 3.3.0.2** *Let  $j : N' \hookrightarrow N$  be the inclusion of a submodule  $N'$  of  $N$ . We say that  $\text{Coker}(j)$  is the quotient of  $N$  by  $N'$  and we denote it  $N/N'$ .*

It is important to note that the cokernel can be characterized by its properties, rather than by its construction. This concept is elaborated upon in section 3.6.2.1.

**Remark(s) 3.3.0.3** *In general, our focus is on modules up to canonical equivalence. To this end, we will identify two modules for which a canonical isomorphism exists, i.e., one that depends on no choice.*

- *For instance, as in linear algebra, we will most often identify an injective morphism  $j : M \rightarrow N$  with the submodule image  $j(M)$  because  $j$  defines a canonical isomorphism  $M \simeq j(M)$  and we simply say (but somewhat abusively) that  $M$  is a submodule of  $N$ .*
- *In linear algebra, the reader is likely accustomed to identifying a finite-dimensional vector space with its bidual (cf. 7.4.0.1), a Euclidean space with its dual (cf. 7.8.5), a square matrix of dimension 1 with its unique coefficient (actually its trace), and so on.*

*We will explore additional examples in the forthcoming sections.*

The following result is formal but important (compare with 3.6)

**Proposition 3.3.0.4** *If  $f \in \text{Hom}_R(M, N)$ , then  $f$  induces a canonical isomorphism  $\bar{f} : M/\text{Ker}(f) \simeq \text{Im}(f)$ .*

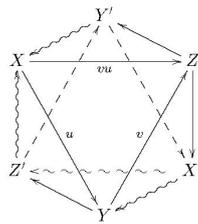
*Proof.* We define

$$\bar{f}(\bar{m}) = \bar{f}(m + \text{Ker}(f)) = f(m + \text{Ker}(f)) = f(m) + f(\text{Ker}(f)) = f(m) \in \text{Im}(f).$$

Thus,  $\bar{f}$  is well defined and linear. It is surjective. If  $\bar{m}$  is in the kernel,  $\bar{f}(\bar{m}) = f(m) = 0$  and therefore  $m \in \text{Ker}(f)$  so  $\bar{m} = 0$ . □

In particular, if a submodule  $N$  of  $M$  admits a complement<sup>4</sup>  $S$ , the restriction  $S \rightarrow M/N$  of the projection  $M \rightarrow M/N$  is an isomorphism (see more generally 3.10.6). But, contrary to usual linear algebra, the existence of complement is exceptional.

### 3.4 Exact sequences and diagrams



For  $f \in \text{Hom}(M, N)$  a morphism of modules; we have a canonical sequence of morphisms

$$(*) \quad 0 \rightarrow \text{Ker}(f) \xrightarrow{\iota} M \xrightarrow{f} N \xrightarrow{\pi} \text{Coker}(f) \rightarrow 0$$

We notice that the composition of two consecutive morphisms  $d \circ \delta$  (namely  $f \circ \iota$  and  $\pi \circ f$ ) are null, which is equivalent to the inclusions  $\text{Im}(\delta) \subset \text{Ker}(d)$ . But we have better: these inclusions are equalities! This leads to the following definition

**Definition 3.4.0.1** *Let  $d_i \in \text{Hom}(M_i, M_{i+1})$  morphisms, noted as a «sequence»:*

$$\cdots M_{i-1} \xrightarrow{d_{i-1}} M_i \xrightarrow{d_i} M_{i+1} \cdots$$

---

<sup>4</sup>Meaning as usual  $N \oplus S = M$ .

1. We say that the sequence is a complex (at  $i$ ) if  $d_i \circ d_{i-1} = 0$  ie  $\text{Im}(d_{i-1}) \subset \text{Ker}(d_i)$ .
2. We say that the sequence is exact (at  $i$ ) if in addition  $\text{Im}(d_{i-1}) \supset \text{Ker}(d_i)$  ie  $\text{Ker}(d_i) = \text{Im}(d_{i-1})$ .

An exact sequence is therefore a special complex and an (important) example of a diagram. By definition, the sequence  $0 \rightarrow M \xrightarrow{f} N$  is exact if and only if  $f$  is injective and  $M \xrightarrow{f} N \rightarrow 0$  is exact if and only if  $f$  is surjective. The reader will check that the sequence (\*) is exact.

We want to explain how to express properties of morphisms in terms of diagrams. Before we give a formal definition, let us illustrate this notion with an example.

Slightly generalizing the notion of matrix equivalence (see 2.3.0.1) and matrix similarity, let us recall standard definitions of linear algebra.

#### Definition 3.4.0.2

1.  $a \in \text{Hom}_{\mathbf{k}}(V, W)$  and  $a' \in \text{Hom}_{\mathbf{k}}(V', W')$  are said equivalent ( $a \sim a'$ ) if there exist isomorphisms  $f : V' \xrightarrow{\sim} V, g : W' \xrightarrow{\sim} W$  such that  $a' = g^{-1} \circ a \circ f$ .
2.  $a \in \text{End}_{\mathbf{k}}(V)$  and  $a' \in \text{End}_{\mathbf{k}}(V')$  are said similar ( $a \approx a'$ ) if there exist an isomorphism  $f : V' \xrightarrow{\sim} V$  such that  $a' = f^{-1} \circ a \circ f$ .

Graphically, (1) means that in the diagram

$$\begin{array}{ccc} V' & \xrightarrow{a'} & W' \\ f \downarrow & & \downarrow g \\ V & \xrightarrow{a} & W \end{array}$$

the two possible ways to join  $V'$  to  $W$  by successive compositions from above  $V' \rightarrow W' \rightarrow W$  and from below  $V' \rightarrow V \rightarrow W$  coincides (knowing that the vertical arrows are isomorphisms).

In the same way, (2) means that in the diagram

$$\begin{array}{ccc} V' & \xrightarrow{a'} & V' \\ f \downarrow & & \downarrow f \\ V & \xrightarrow{a} & V \end{array}$$

possible ways to join  $V$  to  $W$  by successive compositions from above  $V' \rightarrow V' \rightarrow V$  and from below  $V' \rightarrow V \rightarrow V$  coincides (knowing that the vertical arrows are isomorphisms).

composition is *commutative* with exact lines<sup>5</sup> (this last condition being empty for the first diagram).

A general formal definition (readers are encouraged not to waste too much time on the general definition, but rather to make it their own with the examples that follow) might be

<sup>5</sup>By convention, the lines of a diagram are horizontal, the columns vertical.

**Definition 3.4.0.3** Let  $G = (S, A)$  be a directed graph with vertices  $S$  and edges  $A$ .

1. A diagram<sup>6</sup> is the data for each vertex  $\Sigma \in S$  of a module  $M_\Sigma$  and for each edge  $a : \Sigma_{>} \rightarrow \Sigma_{<}$  of  $A$  of a morphism  $f_a : M_{\Sigma_{>}} \rightarrow M_{\Sigma_{<}}$ .
2. The diagram is said to be commutative if for every couple of vertices  $\Sigma, \Sigma'$ , the composed of the  $f_a$  associated with an oriented path from  $\Sigma$  to  $\Sigma'$  depends only on the vertices and not on the chosen path.

In practice, we will only deal with diagrams composed of squares or triangles for which the definition of commutativity will be obvious.

### 3.5 Functoriality and diagram chasing

Although very simple, the following functoriality statements are crucial. This is a very convenient form to formulate the universal properties of kernels and cokernels (cf. §3.6).

**Proposition 3.5.0.1** (Functoriality I) Assume we have a commutative diagram of  $R$ -modules where the top horizontal line is exact and the bottom line is a complex.

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\mu_1} & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & & & \\ N_1 & \xrightarrow{\nu_1} & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

Then there exists a unique morphism

$$f_3 : M_3 \rightarrow N_3$$

making the completed diagram commutative

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\mu_1} & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow f_3 & & \\ N_1 & \xrightarrow{\nu_1} & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

If in addition, the lower complex line is an exact sequence and the two arrows  $M_i \rightarrow N_i$ ,  $i = 1, 2$  are isomorphisms, then  $f_3$  is an isomorphism. In particular, there is canonical isomorphism  $\text{Coker}(\mu_1) = M_3$ .

<sup>6</sup>There are more general definitions, allowing diagrams with several arrows between two edges. We do not use these diagrams.

*Proof.* We focus on the existence and uniqueness of the commutative diagram

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\mu_1} & M_2 & \xrightarrow{\mu_2} & M_3 & \longrightarrow & 0 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \\ N_1 & \xrightarrow{\nu_1} & N_2 & \xrightarrow{\nu_2} & N_3 & & \end{array}$$

If there are two arrows  $f_3$  and  $f'_3$  that work, we have  $f_3 \circ \mu_2 = \nu_2 \circ f_2 = f'_3 \circ \mu_2$  so  $f_3$  and  $f'_3$  coincide on  $\mu_2(M_2) = M_3$  and therefore are equal, hence the uniqueness.

For existence, let  $m_3 \in M_3$  and consider  $m_2$  one antecedent by  $\mu_2$ . If  $m_2$  is not unique, it is defined modulo  $\text{Ker}(\mu_2) = \text{Im}(\mu_1)$ . By linearity, the image  $\nu_2 \circ f_2(m_2)$  is well defined modulo  $\nu_2 \circ f_2 \circ \mu_1(M_1)$ . But by commutativity of the left square, we have  $\nu_2 \circ f_2 \circ \mu_1 = \nu_2 \circ \nu_1 \circ f_1 = 0$  because  $\nu_2 \circ \nu_1 = 0$  by hypothesis. Thus,  $\nu_2 \circ f_2(m_2)$  is well defined, *i.e.* depends only on  $m_3$ . Then set  $f_3(m_3) = \nu_2 \circ f_2(m_2)$  which is checked to work.

For the second part, we can easily verify by hand that the bijectivity of  $f_1, f_2$  implies that of  $f_3$  (**exercice**). Let's give a «categorical»proof, which has the advantage of generalizing to other contexts. Under the bijectivity assumptions of  $f_1, f_2$ , we want to prove that  $f_3$  admits a left inverse  $g_3$  and a right inverse  $d_3$ . From  $g_3 \circ f_3 = \text{Id}_{M_3}$  we then obtain by composing on the right by  $d_3$  the equality  $g_3 = d_3$  and thus that  $f_3$  is invertible.

Let's show the existence of  $g_3$ . Call  $g_1, g_2$  the inverses of  $f_1, f_2$ . As  $f_2 \circ \mu_1 = \nu_1 \circ f_1$ , by composing on the left by  $g_2$  and on the right by  $g_1$  we have  $\nu_2 \circ g_1 = g_2 \circ \nu_1$  so we have a commutative diagram with exact lines

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\mu_1} & M_2 & \xrightarrow{\mu_2} & M_3 & \longrightarrow & 0 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \\ N_1 & \xrightarrow{\nu_1} & N_2 & \xrightarrow{\nu_2} & N_3 & \longrightarrow & 0 \\ \downarrow g_1 & & \downarrow g_2 & & \downarrow g_3 & & \\ M_1 & \xrightarrow{\nu_1} & M_2 & \xrightarrow{\nu_2} & M_3 & \longrightarrow & 0 \end{array}$$

that we can complete uniquely in a commutative diagram with exact lines according to the first point

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\mu_1} & M_2 & \xrightarrow{\mu_2} & M_3 & \longrightarrow & 0 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \\ N_1 & \xrightarrow{\nu_1} & N_2 & \xrightarrow{\nu_2} & N_3 & \longrightarrow & 0 \\ \downarrow g_1 & & \downarrow g_2 & & \downarrow g_3 & & \\ M_1 & \xrightarrow{\nu_1} & M_2 & \xrightarrow{\nu_2} & M_3 & \longrightarrow & 0 \end{array}$$

But by looking at the outer square, taking into account  $g_1 \circ f_1 = \text{Id}_{M_1}$  and  $g_2 \circ f_2 = \text{Id}_{M_2}$ , we have a commutative diagram with exact lines

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\nu_1} & M_2 & \xrightarrow{\nu_2} & M_3 & \longrightarrow & 0 \\ \downarrow \text{Id} & & \downarrow \text{Id} & & \downarrow g_3 \circ f_3 & & \\ M_1 & \xrightarrow{\nu_1} & M_2 & \xrightarrow{\nu_2} & M_3 & \longrightarrow & 0 \end{array}$$

But we also have a commutative diagram

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\nu_1} & M_2 & \xrightarrow{\nu_2} & M_3 & \longrightarrow & 0 \\ \downarrow \text{Id} & & \downarrow \text{Id} & & \downarrow \text{Id} & & \\ M_1 & \xrightarrow{\nu_1} & M_2 & \xrightarrow{\nu_2} & M_3 & \longrightarrow & 0 \end{array}$$

which, thanks to the uniqueness in the first point, gives  $g_3 \circ f_3 = \text{Id}_{M_3}$ . By exchanging the roles of  $M, N$ , we construct the right inverse of  $f_3$ .

Let us turn to the last point. By construction of the cokernel, we have a canonical exact sequence

$$(0) \quad M_1 \xrightarrow{\mu_1} M_2 \rightarrow \text{Coker}(\mu_1) \rightarrow 0$$

Apply the functoriality to the commutative diagram with exact lines

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\mu_1} & M_2 & \longrightarrow & \text{Coker}(\mu_1) & \longrightarrow & 0 \\ \downarrow \text{Id} & & \downarrow \text{Id} & & & & \\ M_1 & \xrightarrow{\mu_1} & M_2 & \xrightarrow{\mu_2} & M_3 & \longrightarrow & 0 \end{array}$$

□

We obtain exactly the same statement by «reversing the direction of the arrows»<sup>7</sup>

**Proposition 3.5.0.2 (Functoriality II)** *Suppose we have a commutative diagram of  $R$ -modules where the bottom horizontal line is exact and the top line is a complex.*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \xrightarrow{\mu_2} & M_3 \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \xrightarrow{\nu_2} & N_3 \end{array}$$

Then there exists a unique morphism

$$\iota_1 : M_1 \rightarrow N_1$$

making the completed diagram commutative

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \xrightarrow{\mu_2} & M_3 \\ & & \downarrow \iota_1 & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \xrightarrow{\nu_2} & N_3 \end{array}$$

If in addition, the top complex line is an exact sequence and the two arrows  $M_i \rightarrow N_i$ ,  $i = 2, 3$  are isomorphisms, then  $\iota_3$  is an isomorphism. In particular, there is canonical isomorphism  $N_1 = \text{Ker}(\nu_2)$ .

<sup>7</sup>an injection  $0 \rightarrow M \rightarrow N$  being thus replaced by a surjection  $M \rightarrow N \rightarrow 0$  and vice versa! This is a general phenomenon: any formal statement involving commutative diagrams, complexes, and exact sequences gives rise to an analogous statement by reversing the direction of the arrows. We can give a precise sense to this statement valid in any «abelian category». We will content ourselves, and it is quite sufficient, to see this as a meta-principle.

A sometimes useful generalization is the famous (and formal) five lemma

**Remark(s) 3.5.0.3** *The above result is most often in the following weakened form. Consider a commutative diagram of modules with exact lines*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & 0 \\ & & \downarrow f_2 & & \downarrow f_3 & & \downarrow f_4 & & \\ 0 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & 0 \end{array}$$

*If  $f_2, f_4$  bijective  $f_3$  bijective.*

## 3.6 Universal properties

The question posed is to characterize the various modules  $M$  in question by the “calculation” of

$$h(T) = \text{Hom}(T, M) \text{ or } h^\vee(T) = \text{Hom}(M, T)$$

for  $T$  an arbitrary “test module”. This treats  $T$  as a variable and  $h, h^\vee$  as a function of  $T$  whose values are sets. One should say functor: the composition with  $f \in \text{Hom}_R(M, N)$  defines a (linear) map  $h_f(T) : h_M(T) \rightarrow h_N(T)$  (resp.  $h_f^\vee : h^\vee(N) \rightarrow h_M^\vee(T)$ ), which is compatible with composition<sup>8</sup> The correct general framework for formulating what follows is that of the Yoneda lemma in categories, but we will stay within the framework of modules for the examples that interest us, to avoid unnecessary formalism.

### 3.6.1 Sum and product

Let  $M_i, i \in I$  be a family of modules. We denote  $M_i \xrightarrow{\varphi_i} \oplus M_i$  the canonical injections and  $\prod M_i \xrightarrow{\pi_i} M_i$  the canonical projections. If  $T$  is a test module we have the two tautological applications

$$\underline{h}^\vee(T) : \begin{cases} \text{Hom}_R(\oplus M_i, T) & \rightarrow & \prod \text{Hom}(M_i, T) \\ f & \mapsto & (\varphi_i \circ f) \end{cases}$$

and

$$\underline{h}(T) : \begin{cases} \text{Hom}_R(T, \prod M_i) & \rightarrow & \prod \text{Hom}(T, M_i) \\ g & \mapsto & (g \circ \pi_i) \end{cases}$$

**Lemma 3.6.1.1** (Universal properties of sum and product) *The applications  $\underline{h}(T)$  and  $\underline{h}^\vee(T)$  are bijective.*

<sup>8</sup>The reader will recognize the usual notion of «restriction» of a morphism for  $h_f(T)$  and dually of «transpose» for  $h^\vee(f)$ .

The proof is immediate and left as an **exercise**. In the case of the direct sum, the meaning of the lemma is that giving a morphism  $f : \oplus M_i \rightarrow T$  is equivalent to giving a collection of morphisms  $f_i : M_i \rightarrow T$  (thanks to the formula  $f(\sum m_i) = \sum f_i(m_i)$  which is well defined because the sum is actually finite).

### 3.6.2 Kernel and cokernel



Let  $f : M \rightarrow N$  be a morphism of modules. By construction, we have the two exact sequences

$$0 \rightarrow \text{Ker}(f) \xrightarrow{j} M \rightarrow N \xrightarrow{p} \text{Coker}(f) \rightarrow 0$$

that characterize kernel and cokernel (see also 3.10.2 and 3.10.5).

If  $T$  is a test module we have two tautological applications

$$h^\vee(T) : \begin{cases} \text{Hom}(\text{Coker}(f), T) & \rightarrow & \text{Hom}_0(N, T) = \{\psi \in \text{Hom}(N, T) \mid \psi \circ f = 0\} \\ \varphi & \mapsto & \varphi \circ p \end{cases}$$

and

$$h(T) : \begin{cases} \text{Hom}(T, \text{Ker}(f)) & \rightarrow & \text{Hom}_0(T, M) = \{\psi \in \text{Hom}(T, M) \mid f \circ \psi = 0\} \\ \varphi & \mapsto & j \circ \varphi \end{cases}$$

**Lemma 3.6.2.1** (Universal properties of kernel and cokernel) *The applications  $h(T)$  and  $h^\vee(T)$  are bijective.*

*Proof.* Let us prove, for example, the universal property of the cokernel ie construct the inverse of  $h^\vee(T)$ . Observing that we have an exact sequence  $0 \rightarrow T \xrightarrow{\text{Id}} T \rightarrow 0$ . Let then  $\psi \in \text{Hom}_0(N, T)$ . The condition  $\psi \circ f = 0$  precisely ensures the commutativity of the diagram

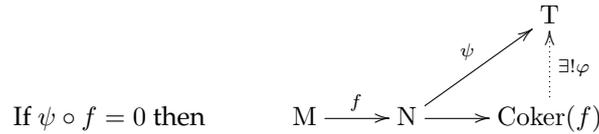
$$\begin{array}{ccccccc} M & \xrightarrow{f} & N & \xrightarrow{p} & \text{Coker}(f) & \longrightarrow & 0 \\ \downarrow & & \downarrow \psi & & & & \\ 0 & \longrightarrow & T & \xrightarrow{\text{Id}} & T & \longrightarrow & 0 \end{array}$$

so that 3.5.0.1 ensures the existence of a unique  $\varphi$  which makes the diagram

$$\begin{array}{ccccccc} M & \xrightarrow{f} & N & \xrightarrow{p} & \text{Coker}(f) & \longrightarrow & 0 \\ \downarrow & & \downarrow \psi & & \downarrow \varphi & & \\ 0 & \longrightarrow & T & \xrightarrow{\text{Id}} & T & \longrightarrow & 0 \end{array}$$

commute. We verify that the application  $\psi \mapsto \varphi$  is the inverse of  $h^\vee(T)$ .  $\square$

The meaning of the lemma is that providing a morphism  $\varphi$  from the cokernel to  $T$  is equivalent to providing a morphism  $\psi$  from  $N$  to  $T$  such that the composition  $\psi \circ f$  is zero, or  $\psi$  factors through the quotient (or is passing to the quotient) in  $\varphi$  if and only if  $\psi \circ f = 0$  (and the analogous for the kernel by reversing the directions of the arrows). From a diagrammatic perspective, we often summarize by retaining only the informal meaning of the statement:



Another way of expressing this, in terms of the functors  $h$  and  $h^\vee$ , is that the sequences of module morphisms

$$0 \rightarrow \text{Hom}(\text{Coker}(f), T) \rightarrow \text{Hom}(N, T) \rightarrow \text{Hom}(M, T)$$

and

$$0 \rightarrow \text{Hom}(T, \text{Ker}(f)) \rightarrow \text{Hom}(T, M) \rightarrow \text{Hom}(T, N)$$

are exact.

### 3.7 A key example: the $k[T]$ -module $V_a$



If  $R = k[T]$  and  $M$  is an  $R$ -module, multiplication by the elements of  $k$  seen as constant polynomials makes  $M$  a  $k$ -vector space. Furthermore, multiplication by  $T$  defines  $a \in \text{End}_k(M)$ : the homothety of ratio  $T$ . Conversely, if  $V$  is a  $k$ -vector space and  $a \in \text{End}_k(V)$ , we define a  $R$ -module structure  $V_a$  on  $V$  by the formula  $T.v = a(v)$  and by linearity

$$P(T).v = P(a)(v) \text{ for all } P \in R = k[T], v \in V_a = V$$

These two constructions are inverses of each other:

*The  $k[T]$ -modules are identified with the pairs  $(V, a)$ ,  $a \in \text{End}_k(V)$ .  
Submodules of  $V_a$  are then identified with subspaces of  $V$  stable by  $a$  (*exercice*).*

From the perspective of morphisms, the identification works as follows. If  $N = W_b$  is a second module associated with an endomorphism  $b \in \text{End}_k(W)$ , a morphism  $f \in \text{Hom}_R(M, N) = \text{Hom}_{k[T]}(V_a, V_b)$  is defined by  $f \in \text{Hom}_k(V, W)$  such that for any  $m \in M$

$$f \circ a(m) = f(Tm) = Tf(m) = b \circ f(m)$$

$$\text{Hom}_{\mathbf{k}[T]}(V_a, W_b) = \{f \in \text{Hom}_{\mathbf{k}}(V, W) \text{ such that } b \circ f = f \circ a\}$$

When  $a = b$ ,  $\text{End}_{\mathbf{k}[T]}(V_a)$  is therefore the  $\mathbf{k}$ -algebra of endomorphisms of  $V$  commuting with  $a$ .

**Corollary 3.7.0.1** *If  $f \in \text{Isom}_{\mathbf{k}[t]}(V_a, W_b)$  if and only if  $a = f^{-1} \circ b \circ f$  so that  $V_a$  and  $W_b$  are isomorphic if and only if  $a$  and  $b$  are similar.*

The corollary says that if we understand the module  $V_a$  up to isomorphism, we understand  $a$  up to similarity. The main tool for “computing”  $V_a$  is the following crucial proposition, which expresses  $V_a$  as a cokernel. This allows its computation using the cokernel functoriality 3.5.0.1 and matrix operations in  $M_n(\mathbf{k}[T])$ , as we will see later. Let us explain how to do this.

There is a unique lifting  $\tilde{a} \in \text{End}_{\mathbf{k}[T]}(V[T])$  of  $a$  to  $V[T]$  (see 3.2.0.2) characterized by  $\tilde{a}(vT^i) = a(v)T^i$ . Let  $\pi_a : \text{Hom}(V[T] \rightarrow V_a)$  the unique lifting of  $\text{Id}_V$  (we have  $\pi_a(\sum v_i T^i) = \sum a^i(v_i)$ ).

**Proposition 3.7.0.2** *The sequence*

$$(i) \quad 0 \rightarrow V[T] \xrightarrow{\mathbf{T}i - \tilde{a}} V[T] \xrightarrow{\pi_a} V_a \rightarrow 0$$

*is exact.*

*Proof.* Let  $v \in V$ . The image of the constant polynomial  $v \in V[T]$  by  $\pi_a$  is  $v$ . Therefore  $\pi_a$  is onto.

We then have

$$\pi_a \circ (\mathbf{T}i - \tilde{a})(v) = \mathbf{T}\pi_a(v) - a(v) = a(v) - a(v) = 0$$

hence  $\pi_a \circ (\mathbf{T}i - \tilde{a}) = 0$  since  $V$  generates  $V[T]$  and therefore  $\text{Im}(\mathbf{T}i - \tilde{a}) \subset \text{Ker}(\pi_a)$ .

Conversely, let  $v(T) = \sum_{i \geq 0} T^i v_i \in \text{Ker}(\pi_a)$ , i.e.

$$v_0 + \sum_{i \geq 1} a^i(v_i) = 0.$$

Thus, we have

$$v(T) = \sum_{i \geq 1} (\mathbf{T}^i i - \tilde{a}^i)(v_i).$$

But since  $\mathbf{T}i$  and  $\tilde{a}$  commute, we have (geometric series sum)

$$\mathbf{T}^i i - \tilde{a}^i = (\mathbf{T}i - \tilde{a}) \circ \left( \sum_{j=0}^{i-1} \mathbf{T}^j \tilde{a}^{i-1-j} \right)$$

and thus  $v(T) \in \text{Im}(\mathbf{T}i - \tilde{a})$ . Hence the exactness in the middle.

Let us turn to the exactness on the left (although it is not necessary for the purpose of studying matrix similarity). Indeed,  $\sum v_i T^i \in \text{Ker}(\mathbf{T} \text{Id} - \tilde{a})$  if and only if  $v_{i-1} - a(v_i) = 0$  for all  $i$  setting  $v_{-1} = 0$ . Because  $v_i = 0$  for  $i \gg 0$ , we get  $v_i = 0$  by descending induction.  $\square$

Although the proposition is true in full generality, let us focus to the finite dimension case. Let  $\mathcal{B} = (\varepsilon_i)_{1 \leq i \leq n}$  be a basis of  $V$  defining an isomorphism  $\mathbf{k}^n \xrightarrow{\sim} V$  (mapping the canonical basis element  $e_i$  to  $\varepsilon_i$ ) and  $A = \text{Mat}_{\mathcal{B}}(a) \in M_n(\mathbf{k}) = \text{End}_{\mathbf{k}}(\mathbf{k}^n)$ .

By definition,  $P(T) \in \mathbf{k}[T]$  acts on of the  $\mathbf{k}[T]$ -module on  $V_A = (\mathbf{k}^n)_A$  by the rule  $P(T)X = P(A)X$  for all  $X \in \mathbf{k}^n = M_{n,1}(\mathbf{k})$  and we have a surjective morphism  $\pi_A : (\mathbf{k}[T])^n \rightarrow (\mathbf{k}^n)_A$  defined by  $\pi_A(\sum X_i T^i) = \sum A^i X_i$ . By construction, the isomorphism  $\mathbf{k}^n \xrightarrow{\sim} V$  defined by  $\mathcal{B}$  defines an isomorphism of  $\mathbf{k}[T]$ -modules  $(\mathbf{k}^n)_A \xrightarrow{\sim} V_a$ . By abuse, we still denote the composite  $(\mathbf{k}[T])^n \xrightarrow{\pi_A} (\mathbf{k}^n)_A \xrightarrow{\sim} V_a$  by  $\pi_A$ .

**Corollary 3.7.0.3** *With the above notations*

1. The map  $(P_i(T) = \sum_j P_{i,j} T^j) \mapsto \sum_{i,j} P_{i,j} e_i T^j$  is an isomorphism of  $\mathbf{k}[T]$ -modules  $(\mathbf{k}[T])^n \xrightarrow{\sim} V[T]$ .
2. The above morphisms makes the following diagram commutative

$$\begin{array}{ccccccc}
 0 & \longrightarrow & (\mathbf{k}[T])^n & \xrightarrow{T\text{Id}-A} & (\mathbf{k}[T])^n & \xrightarrow{\pi_A} & V_A = (\mathbf{k}^n)_A \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & V[T] & \xrightarrow{T\text{Id}-a} & V[T] & \xrightarrow{\pi_a} & V_a \longrightarrow 0
 \end{array}$$

In other words,

$$\text{Coker}(T\text{Id} - A) \xrightarrow{\sim} V_a$$



Observe that the computation is functorial in the following sense. If  $B = \text{Mat}_{\mathcal{B}}(b)$  for  $b \in \text{End}_{\mathbf{k}}(V)$ , the diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & (\mathbf{k}[T])^n & \xrightarrow{T\text{Id}-A} & (\mathbf{k}[T])^n & \xrightarrow{\pi_A} & V_a \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & (\mathbf{k}[T])^n & \xrightarrow{T\text{Id}-B} & (\mathbf{k}[T])^n & \xrightarrow{\pi_B} & V_b \longrightarrow 0
 \end{array}$$

### 3.8 Cokernel of diagonal matrices

The following simple but crucial example generalizes the well-known exact sequence

$$\mathbf{Z} \xrightarrow{n} \mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z} \rightarrow 0$$

Let us consider a “diagonal rectangular matrix”  $D \in M_{p,q}(\mathbf{R})$  «diagonal» in the sense that its coefficients  $d_{i,j}$  are zero if  $i \neq j$  and define  $\nu = \min(p, q)$ ,  $\mu = \sup(p, q)$ . We have a block decomposition

$$D = (\Delta, 0) \text{ if } q \geq p \geq 1, D = \begin{pmatrix} \Delta \\ 0 \end{pmatrix} \text{ if } p \geq q \geq 1$$

with  $\Delta = \text{diag}(d_i) \in M_\nu(\mathbb{R})$  or in a synthetic way

$$D = \begin{pmatrix} \text{diag}(d_i)_{\nu,\nu} & 0_{\nu,q-\nu} \\ 0_{p-\nu,\nu} & 0_{p-\nu,q-\nu} \end{pmatrix}$$

(where matrices of size  $(a, b)$  with  $a$  or  $b$  non  $> 0$  are empty). In this setup, the morphism  $\mathbb{R}^q \xrightarrow{D} \mathbb{R}^p$  defines a sequence

$$(*) \quad \mathbb{R}^q = \mathbb{R}^\nu \times \mathbb{R}^{\mu-\nu} \xrightarrow{\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto D \begin{pmatrix} X \\ Y \end{pmatrix} = \Delta X} \mathbb{R}^p = \mathbb{R}^\nu \xrightarrow{X \mapsto (x_i \bmod d_i)_i} \prod_{i=1}^{\nu} \mathbb{R}/(d_i) \rightarrow 0 \text{ if } q \geq p$$

or

$$(*) \quad \mathbb{R}^q = \mathbb{R}^\nu \xrightarrow{X \mapsto DX = \begin{pmatrix} \Delta X \\ 0 \end{pmatrix}} \mathbb{R}^p = \mathbb{R}^\nu \times \mathbb{R}^{\mu-\nu} \xrightarrow{(X,Y) \mapsto ((x_i \bmod d_i)_i, Y)} \prod_{i=1}^{\mu} \mathbb{R}/(d_i) \times \mathbb{R}^{\nu-\mu} \rightarrow 0 \text{ if } p \geq q$$

**Lemma 3.8.0.1** *The sequence (\*) is exact. In particular, one has a canonical isomorphism*

$$\text{Coker}(D) = \prod_{i=1}^{\nu} \mathbb{R}/(d_i) \times \mathbb{R}^{(\mu-\nu)_+}.$$

*Proof.* Let's deal with the case  $q \geq p$ , the other case being completely analogous.

The arrow  $\mathbb{R}^p = \mathbb{R}^\nu \xrightarrow{X \mapsto (x_i \bmod d_i)_i} \prod_{i=1}^{\nu} \mathbb{R}/(d_i)$  is surjective. We just have to prove the exactness of the middle.

The composition of the two non trivial arrows is  $\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto (d_i x_i \bmod d_i)_i$  and is therefore zero proving the inclusion  $\text{Im} \subset \text{Ker}$ .

If  $X \in \mathbb{R}^\nu$  maps to zero, we have  $x_i \bmod d_i = 0$  for all  $i$  and therefore there exists  $X' \in \mathbb{R}^\nu$  such that  $x'_i = d_i x_i$  for all  $i$  or equivalently  $X = D \begin{pmatrix} X' \\ 0 \end{pmatrix}$  proving  $\text{Ker} \subset \text{Im}$  hence the exactness. The last point is just the functoriality of the cokernel. 3.5.0.1.  $\square$

With this generality, it's impossible to recover the diagonal coefficient only from the isomorphism class of cokernel. It is even the case when  $n = m = 1$ : the cokernel of the  $[6] \in M_1(\mathbb{Z})$  is  $\mathbb{Z}/6\mathbb{Z}$  but also  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  thanks to the usual Chinese remainder lemma. Let's fix this problem.

We say, mimicking the definition of a finite dimensional vector space:

**Definition 3.8.0.2** A module  $M$  is of finite type if it has a finite generating family  $(m_i)_{1 \leq i \leq n}$  or equivalently<sup>9</sup>, if there exists a surjective morphism  $\pi : R^n \rightarrow M$ .

Let  $M$  be a finite type module. We will define in general an increasing sequence of ideals depending only on  $M$  which are effectively computable in most of the case: its Fitting ideals<sup>10</sup>. If they do not fully determine  $M$ , they give a deep insight on  $M$  and even determine  $M$  when  $R$  is a PID as we will see later.

### 3.8.1 Determinantal ideals

Let  $A, B \in M_{p,q}(R)$ . Let us recall that for any integer subsets  $I \subset [1, \dots, p]$  and  $J \subset [1, \dots, q]$  of the same cardinality  $n$ , the *minor*  $A_{I,J}$  of  $A$  the size  $n$  square matrix  $A_{I,J} = (a_{i,j})_{i \in I, j \in J}$ . Its determinant is defined up to sign, depending on orderings on  $I$  and  $J$ .

**Definition 3.8.1.1** For  $n \in \mathbf{Z}$ , we define

$$\wedge^n(A) = \langle \det(A_{I,J}), I \subset [1, \dots, p], J \subset [1, \dots, q] \text{ and } \text{Card}(I) = \text{Card}(J) = n \rangle$$

the ideal generated by the determinant of all size  $n$  minors  $A$ .

If  $n \leq 0$ , the minors are the empty matrix whose determinant is 1 and  $\wedge^n(A) = R$ . If  $n > \min(p, q)$ , we have not any minor and  $\wedge^n(A) = \{0\}$ . Using the development of a matrix with respect to a row or column gives that  $\wedge^n(A)$  is a decreasing sequence of ideals.

**Lemma 3.8.1.2** Let  $A, B \in M_{p,q}(R)$  and  $Q \in M_{q,r}(R)$ .

1.  $\wedge^n(AQ) \subset \wedge^n(A)$  for any  $n \in \mathbf{Z}$ .
2. If  $A$  and  $B$  are equivalent then  $\wedge^n(A) = \wedge^n(B)$  for all  $n \in \mathbf{Z}$ .

*Proof.*

1. Each column of  $AQ$  is a linear combination of columns of  $A$ . The multilinearity of the determinant then ensures that the minor  $(AQ)_{I,J}$  is a linear combination of determinants of size  $n$  matrices whose columns are made from columns of  $A$  (possibly equal) and whose rows are indexed by  $I$ . If two columns are equal, the determinant is zero (the determinant is alternating). Otherwise, the set of columns in question is indexed by a set  $K$  of cardinality  $n$  and the determinant in question is of the

<sup>9</sup>Define  $\pi(x_i) = \sum x_i m_i$  and conversely starting from  $\pi$  defined  $m_i = \pi(e_i)$ .

<sup>10</sup>Our presentation is sort of mix between the original approach of H. Fitting [10] and a nice presentation due to Melvin Hochster.

form  $A_{I,K}$  which implies that  $\det(AP)_{I,J}$  is a linear combination of  $\det(A_{I,K})$  with  $\text{Card}(K) = n$ , and therefore belongs to  $\wedge^n(A)$ .

2. If  $Q \in M_q(\mathbb{R})$  is invertible, applying (1) to  $AQ$  and  $Q^{-1}$  yields an equality  $\wedge^n(AQ) = \wedge^n(A)$  in this case. Since the determinant of a matrix is equal to that of its transpose, we get  $\wedge^n(A) = \wedge^n({}^tA)$  for all  $n$  and therefore  $\wedge^n(PA) \subset \wedge^n(A)$  if  $P \in \text{GL}_p(\mathbb{R})$  hence the result.

□

**Example(s) 3.8.1.3** Because square invertible matrices are equivalent to  $\text{Id}$ , we get  $A \in M_n(\mathbb{R})$  invertible if (and only if!)  $\wedge^n(A) = \mathbb{R}$  for  $n \leq p$  and  $\wedge^n(A) = \{0\}$  for all  $n > p$ .

If  $\mathbb{R} = \mathbf{k}$  is a field, we know better (Gauss algorithm for instance): any  $A \in M_{p,q}(\mathbf{k})$  is equivalent to diagonal matrix  $D_r = \text{diag}(\mathbf{i}_r, 0) \in M_{p,q}(\mathbf{k})$  (with  $r = \text{rk}(A)$ ). By direct computation, we certainly have  $\wedge^n(D_r) = \{0\}$  for  $n > r$  and  $\wedge^n(D_r) = \mathbf{k}$  if  $n \leq r$ . We deduce

**Corollary 3.8.1.4** If  $A, B \in M_{p,q}(\mathbf{k})$ , then  $\text{rank}(A) \leq n$  if and only if  $\wedge^{n+1}(A) = \{0\}$ . It is equal to  $n$  if moreover  $\wedge^n(A) \neq \{0\}$ . Equivalently,  $A, B$  are equivalent if and only if  $\wedge^n(A) = \wedge^n(B)$  for all  $n \in \mathbf{Z}$ .

We will see later that this remains true if  $\mathbb{R}$  is a PID (6.3.1.2), but is not true in general (6.7.15).

### 3.8.2 Fitting ideals

Let  $\vec{m} = (m_i)_{1 \leq i \leq n}$  be generators of  $M$  and  $\pi : \mathbb{R}^n \xrightarrow{(m_1, \dots, m_n)} M$  the corresponding surjective morphism. By definition  $(x_j) \in \mathbb{R}^n$  belongs to  $\text{Ker}(\pi)$  if and only if there exists a relation  $\sum x_j m_j = 0$  between these generators.

Let  $K_J = (K_j)_{j \in J}$  be any family or relations (finite or not), i.e.  $K_j \in \text{Ker}(\pi)$ . We denote  $\wedge^p(\vec{m}, K_J)$  be the ideal generated by the size  $p$  minors extracted from  $K_J$  (meaning a size  $p$  minor of the  $(n, p)$  matrix  $K_{j_1, \dots, j_p}$  where  $j_1, \dots, j_p \in J$ ).

1. If  $p > n$ , there is not any such minor and  $\wedge^p(\vec{m}, K) = 0$ .
2. If  $p \leq 0$ , the matrix is empty whose determinant is 1 and  $\wedge^p(K) = \mathbb{R}$ .

Let  $J \subset J'$ . We certainly have  $\wedge^p(\vec{m}, K_J) \subset \wedge^p(\vec{m}, K_{J'})$  for all  $p$ . We certainly have equality when  $K_{J'}$  differs from  $K_J$  by just adding 0

(\*) if for all  $j' \in J' - J$  we have  $K_{j'} = 0$  then for all  $p$ ,  $\wedge^p(\vec{m}, K_J) = \wedge^p(\vec{m}, K_{J'})$

or, in down to earth term, adding 0 column *-i.e.* trivial relations- does not change  $\wedge^p$  (a minor of  $K_{J'}$  is either 0 or a minor of  $K_J$  depending if all the corresponding columns belong to  $J$  or not). More generally, let us prove

**Lemma 3.8.2.1**

If  $K_{j'} \in \text{Span}(K_j, j \in J)$  then for all  $p$   $\wedge^p(\vec{m}, K_{J'}) = \wedge^p(\vec{m}, K_J)$

*Proof.* We have to prove  $\wedge^p(\vec{m}, K_{J'}) \subset \wedge^p(\vec{m}, K_J)$ . Because any minor of  $K_{J'}$  involves finitely many columns which in turn are a linear combination of finitely many columns of  $K_J$ , one can assume  $J, J'$  finite. If we write  $K_{j'} = \sum a_{j,j'} K_j$  for each  $j' \in J'$ , we get  $K_{J'} = K_J A$  where  $A$  is a matrix of  $\text{Hom}_{\mathbb{R}}(\mathbb{R}^{J'}, \mathbb{R}^J)$ . This shows that  $(K_J, K_{J'}) = (K_J, 0) \begin{pmatrix} \text{Id} & A \\ 0 & \text{Id} \end{pmatrix}$  and  $(K_J, K_{J'})$  and  $(K_J, 0)$  equivalent. They have therefore the same invariant ideals and we get  $\wedge^p(\vec{m}, K_J, K_{J'}) = \wedge^p(\vec{m}, K_J, 0) \stackrel{(*)}{=} \wedge^p(\vec{m}, K_J)$ .  $\square$

The lemma immediately gives

**Corollary 3.8.2.2** If both  $K_J$  and  $K_{J'}$  generate  $\text{Ker}(\pi)$ , then  $\wedge^p(\vec{m}, K_J) = \wedge^p(\vec{m}, K_{J'})$  for all  $p$ . We will denote these common values by  $\wedge^p(\vec{m})$ .

In other words, the determinantal ideals  $\wedge^p(\vec{m})$  does not depend on the system of generators of  $\text{Ker}(\pi)$ . Let us prove in a analogous way that it does not depend on the choice of generators in the following sense.

**Lemma 3.8.2.3** Let  $m' \in M$ . Then  $\wedge^{p+1}(\vec{m}, m') = \wedge^p(\vec{m})$  for all  $p \geq 0$ . In other words,  $\wedge^{n+1-p}(\vec{m}, m') = \wedge^{n-p}(\vec{m})$  for all  $p \leq n$ .

*Proof.* Let us write  $m' = \sum_i x_i m_i$  and let  $\pi' : \mathbb{R}^{n+1} \xrightarrow{(\vec{m}, m')} M$ . Then  $\pi'(y_i) = 0$  if and only if  $0 = \sum y_i m_i + y_{n+1} m' = \sum (y_i - y_{n+1} x_i) m_i = \pi(y_i - y_{n+1} x_i) = 0$  giving  $\text{Ker}(\pi') = \text{Ker}(\pi) \oplus^t (-x_1, \dots, -x_n, 1)$ . If  $K_J$  is a family of generators of  $\text{Ker}(\pi)$  seen as a family of vectors of  $\mathbb{R}^n \subset \mathbb{R}^{n+1}$  with

last coordinate 0, we have  $K' = (K_J, \begin{pmatrix} -x_1 \\ \vdots \\ -x_n \\ 1 \end{pmatrix})$  generate  $\text{Ker}(\pi')$ . To compute a  $p+1$  minor of  $K'$ , we can

assume  $J$  finite and consider  $K'$  as a matrix in

$$K' = \begin{pmatrix} K & * \\ 0 & 1 \end{pmatrix} \in M_{n+1, q+1}$$

where  $q = \text{Card}(J)$ . But  $K'$  is equivalent (Gauss operations) to  $K' = \begin{pmatrix} K & 0 \\ 0 & 1 \end{pmatrix}$  whose  $p + 1$  minors are either those of  $K$  of size  $p$  or 0 depending if the last line and column is among the lines/rows defining the minor or not. By invariance of determinantal ideals under equivalence, the lemma follows.  $\square$

Thanks to the above independence lemma, the following definition makes senses.

**Definition 3.8.2.4** Let  $\vec{m} = (m_1, \dots, m_n)$  be a finite generating family of  $M$  and let  $p \geq 0$ . We define the sequence of Fitting ideals<sup>11</sup>  $\Phi_\bullet(M) = (\Phi_p(M))_p$  of  $M$  by the formula

$$\Phi_p(M) = \wedge^{n-p}(\vec{m}).$$

**Example(s) 3.8.2.5** If  $M = R^n$ , using the canonical basis as generators of  $R^n$  to compute the Fitting ideals, we get  $\text{Ker}(\pi) = \{0\}$  and all the minors are empty and therefore have determinant 1 and therefore  $\Phi_p(M) = R$  if  $p \leq n$  and  $\Phi_p(R^n) = \{0\}$  if  $p > n$ .

The main immediate but deep properties of Fitting ideals are summarized below.

**Proposition 3.8.2.6** Let  $M, M'$  be a finite type module and  $A \in M_{n,q}(R)$ .

1. We have  $\Phi_p(M) = \{0\}$  if  $p < 0$  and  $\Phi_p(M) = R$  if  $p > n$ .
2. For  $I$  and ideal of  $R$ , the only non trivial Fitting invariant is  $\Phi_0(R/I) = I$ .
3. The sequence  $\Phi_\bullet(M)$  is increasing.
4. If  $f : M \rightarrow M'$  is an isomorphism, then  $\Phi_\bullet(M) = \Phi_\bullet(M')$ .
5. If  $M = \text{Coker}(A)$ , the determinantal ideals  $\wedge^{n-p}(A) = \Phi_p(M)$  does not depend on  $A$  but only on  $M$ .
6.  $\Phi_p(M \oplus M') = \sum_{i+j=p} \Phi_i(M)\Phi_j(M')$ .

*Proof.*

1. By definition (see 3.8.1).
2. Use the projection  $R \rightarrow R/I$  to compute the (1) minors.

<sup>11</sup>In his seminal paper [10], Fitting considered the ideals associated to the family of  $\text{Ker}(\pi)$  generated by all its elements. But it's quite clear that it knew that a generating family is sufficient. His goal was to define invariants of modules.

3. Developing a determinant with some row gives  $\wedge^{n+1}(A) \subset \wedge^p(A)$  giving (1).
4. If  $\pi : R^n \rightarrow M$  is onto, so is  $f \circ \pi : R^n \rightarrow M'$  and  $\pi, f \circ \pi$  have the same kernel. Therefore, their Fitting ideals are equal because the corresponding set of relations are equal!
5. This is the independence of Fitting ideals from the generator set.
6. If  $\pi, \pi'$  are surjective morphisms  $R^n \rightarrow M, R^{n'} \rightarrow M'$  respectively, so is

$$\pi \oplus \pi' : R^{n+n'} = R^n \oplus R^{n'} \rightarrow M \oplus M'$$

with kernel the direct sum of the kernels. The corresponding minors are diagonal matrices of minors of  $\pi$  and  $\pi'$  whose determinant is their product.

□

### 3.9 Properties to handle with caution

Let us first summarize the notions we will be talking about. Unless their definitions are just mimicking classical linear algebra, their properties in the module case are heavily different as we will discuss.

 Finiteness and Freeness		
Property/Definition	Vector space	Module
Free family $(x_i)_{i \in I}$	$\sum \lambda_i x_i = 0 \Rightarrow \lambda_i \equiv 0$ or $R^{(I)} \xrightarrow{\lambda_i \mapsto \sum \lambda_i x_i} M$ injective	
Generating family $(x_i)_{i \in I}$	$\langle x_i \rangle = M$ or $R^{(I)} \xrightarrow{\lambda_i \mapsto \sum \lambda_i x_i} M$ surjective	
Base $(x_i)_{i \in I}$	$(x_i)$ free and generating or $R^{(I)} \xrightarrow{\lambda_i \mapsto \sum \lambda_i x_i} M$ bijective	
Free module M	$M \simeq R^{(I)}$ i.e. M admits a base	
Finite type module M	finite generating family or $R^n \rightarrow M$ surjective	

#### 3.9.1 Finiteness

We have defined the Fitting ideals of any finite type module M and we have seen that they are just determinants of minors of a matrix A provided  $M \xrightarrow{\sim} \text{Coker}(A)$ . These modules are called finite presentation modules.

<sup>11</sup>See 3.9.4.2 for the finite type case and chapter 5 in general.

**Definition 3.9.1.1** A module  $M$  is of finite presentation if there is an exact sequence  $R^m \rightarrow R^n \rightarrow M \rightarrow 0$ .

Down to earth, this means exactly that the kernel  $R^n \rightarrow M$  is finitely generated. Contrary to the case of vector spaces, for general rings it is not true that a submodule of a module of finite type is of finite type. As we will see in detail in the chapter 5, rings for which this pathology does not occur are *Noetherian* rings, a huge generalization of fields containing almost all rings that appear naturally in algebra or number theory. As a first approach, let us explain here how they are defined and what this means for our finiteness problem.

**Definition 3.9.1.2** A ring is *Noetherian* if every ideal is finitely generated.

For instance, fields and PID are Noetherian. By definition, any finite type module over a Noetherian ring is of finite presentation.

**Exercise 3.9.2** Show that the rings of continuous real functions on  $\mathbf{R}$  is non Noetherian.

**Proposition 3.9.2.1** Let  $M$  be a finite type module over a Noetherian ring  $R$  and  $N \subset M$  a submodule. Then  $N$  is of finite type.

*Proof.* Induction on the minimal number  $n$  of generators of  $M$  (obviously true for  $n = 0!$ ). Assume  $M$  is generated by  $n + 1$  element : we have a surjective morphism  $\pi : R^{n+1} \rightarrow M$  inducing a surjection  $\bar{N} = \pi^{-1}(N) \rightarrow N$ . We just have to prove that  $\bar{N}$  is of finite type. The kernel of the projection

$$p : \begin{cases} R^{n+1} & \rightarrow R \\ (x_1, \dots, x_{n+1}) & \rightarrow x_{n+1} \end{cases}$$

is  $R^n$  and we have an exact sequence  $0 \rightarrow \bar{N} \cap R^n \rightarrow \bar{N} \rightarrow p(\bar{N}) \rightarrow 0$ . By induction,  $\bar{N} \cap R^n$  has a finite number of generators  $g_i$ . But  $p(\bar{N})$  is an ideal of  $R$  which has a finite number of generators of the form  $p(\gamma_j)$ . The finite family  $(g_i, \gamma_j)$  generates  $\bar{N}$ .  $\square$

**Exercise 3.9.3** Adapt the proof below and prove that if  $R$  is a PID, any submodule of  $R^n$  is free (we will give a far more general statement in 6.4.0.1).

### 3.9.4 Free modules

The reader will convince himself that the data of a basis  $(e_i)_{i \in I}$  of  $M$  is equivalent of the data of an isomorphism  $R^{(I)} \xrightarrow{\sim} M$ . When such a data exists, we say that  $M$  is *free*. As soon as  $R$  is not a field, there

are plenty of non free module . Indeed, if  $x$  is neither 0 or invertible, the  $R$ -module  $R/(x)$  is never free (exercice).

**Example(s) 3.9.4.1**

- $R$  is a free module with base 1. More generally,  $R^m$  is free with base (canonical)  $(e_j = E_{1,j})_{1 \leq j \leq m}$  or even  $R^{(I)}$  is free with basis  $(e_j)_{j \in J}$  with  $e_j = (\delta_{i,j})_{j \in I}$ .
- $R_{<n}[T]$  is a free  $R$ -module with base  $T^i, i < n$  therefore of rank  $n$  for  $n \in \overline{\mathbf{N}} = \mathbf{N} \cup \{\infty\}$ .
- $M_{p,q}(R)$  is a free module with the standard base  $(E_{i,j})_{1 \leq i \leq p, 1 \leq j \leq q}$ .
- If  $(e_i)_{1 \leq i \leq n}$  is a basis of the  $\mathbf{k}$ -vector space  $V \subset V[T]$  (3.2.0.2), then  $(e_i)$  is a basis for  $V[T] \xrightarrow{\sim} (R[T])^n$ .

**Proposition 3.9.4.2** *Let  $M$  be a finite type module which is free. Then, there exist a unique integer  $n$  such that  $M$  is isomorphic to  $R^n$ . This integer is called the rank of  $M$ .*

*Proof.* Let  $(m_i)_{i \in I}$  be a basis of  $M$  and  $\pi : R^N \rightarrow M$  a surjection ( $M$  is of finite type). Let  $J \subset I$  be the finite set of indices involved in the decomposition of each  $\pi(e_k), k = 1, \dots, N$ . The image  $\text{Im}(\pi)$  is generated by  $(m_i)_{i \in J}$ . Because this subfamily is free, it generates a submodule  $M'$  of  $M$  isomorphic to  $R^J$ . By surjectivity of  $\pi$ , one has  $M' = M$  and we get therefore  $R^J \xrightarrow{\sim} M$  hence the existence of  $n = \text{Card}(J)$ . By (4) of 2.2.0.1,  $n$  is uniquely determined by  $M$ . □

**Remark(s) 3.9.4.3**

1. This property fails if  $R$  is no longer assumed to be commutative (see 3.10.8).
2. We already know that  $\bigoplus_{i \in I} M_i \rightarrow \prod_{i \in I} M_i$  is not an isomorphism unless all but a finite number of  $M_i$  are zero. In fact, if  $I$  is infinite, the direct product  $R^I$  is usually not even a free module<sup>12</sup> (see 3.10.11)!

**3.9.5 Torsion**

A torsion element of a module is an element of  $M$  annihilated by a nonzero element of  $R$ . If  $R$  is a field (vector space situation) this notion is empty : 0 is the only torsion element. A module whose all elements are torsion is called a torsion module.

**Example(s) 3.9.5.1** • Any finite ring is torsion.

- In finite dimension, the  $\mathbf{k}[T]$ -module  $V_a$  associated to  $a \in \text{End}(V)$  is canceled by  $\chi_a(T)$  for instance (2.1.3.2) and therefore is torsion (or perhaps more elementary, a dependence relation between the  $n^2 + 1$  elements  $\text{Id}, f, \dots, f^{n^2}$  in the  $n^2$ -dimensional vector space  $\text{End}_{\mathbf{k}}(V)$ ) meaning by construction  $P(T) \cdot V_a = \{0\}$ .
- More generally<sup>13</sup>, if  $I$  is a nonzero ideal of  $R$ , the quotient module  $R/I$  is torsion.

If  $R$  is an integral domain<sup>14</sup> and  $M$  a module, the set  $M_{\text{tors}}$  of torsion elements of  $M$  is a submodule called torsion module. It is no longer true if  $R$  is not integral (observe that  $2 \bmod 6$  and  $3 \bmod 6$  are torsion in  $\mathbf{Z}/6\mathbf{Z}$  but that  $5 \bmod 6$  is not). We will prove in the sequel that if  $R$  is PID, finite type modules are free<sup>6.4</sup> if and only if they have no torsion. This is far from being true in general (7.8.11).



### 3.9.6 Summary of some specifics of modules

 Bases, Finiteness, Complements		
Property/Definition	Vector space	Module
Torsion	$x \neq 0$ free	$x \neq 0$ free iff $x$ non torsion
Permanence of finiteness	subvector spaces of $\mathbf{k}^n$ are of finite dimension	submodules of $R^n$ of finite type iff $R$ Noetherian
Bases	Always free	Plenty of non free modules if $R \neq \mathbf{k}$
Complement submodules	Always exist	Usually don't exist
Exact sequences	Always split	Usually don't split

### 3.10 Exercises

#### Exercise 3.10.1

1. Show that an abelian group is finite if and only if the associated  $\mathbf{Z}$ -module is of finite type and torsion.
2. Show that if  $V_a$  corresponds to  $(V, a)$  (refer to 3.7), then  $V$  is finite-dimensional if and only if  $V_a$  is of finite type and torsion.

<sup>13</sup>The advanced reader will notice that  $V_a$  is isomorphic to  $\mathbf{k}[T]/(\mu_a)$  where  $\mu_a$  is the minimal polynomial of  $a$  in the case where  $a$  is a cyclic endomorphism. We will shortly discuss in detail these topics.

<sup>14</sup>Recall that this means that  $R$  is not zero and that the product of two nonzero elements is nonzero.

**Exercise 3.10.2** Let  $f \in \text{Hom}(M, N)$ .

1. Show that the sequence  $0 \rightarrow K \rightarrow M \xrightarrow{f} N$  is exact if and only if  $K$  can be identified (canonically) with the kernel of  $f$ . Compare with 3.5.0.2 infra.
2. Show that the product or direct sum of exact sequences is still exact.

**Exercise 3.10.3** Let  $R$  be an integral domain.

1. Show that the relation  $(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$  defines an equivalence relation on  $R \times (R \setminus \{0\})$ . Denote the equivalence class of an element  $(r, s)$  by  $\frac{r}{s}$ . Let  $\text{Frac}(R)$  denote the set of equivalence classes.
2. Define  $+$  and  $\cdot$  on  $\text{Frac}(R)$  by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \text{ and } \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

Show that  $\text{Frac}(R)$  is a field (the fraction field of  $R$ ) with respect to  $+$  and  $\cdot$  with  $0 = \frac{0}{1}$  and  $1 = \frac{1}{1}$ .

3. Can you state and prove a universal property of the fraction field?

**Exercise 3.10.4** Consider a commutative diagram of modules with exact lines

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \downarrow f_4 & & \downarrow f_5 \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

1. If  $f_2, f_4$  injective and  $f_1$  surjective, then  $f_3$  injective.
2. If  $f_2, f_4$  surjective and  $f_5$  injective, then  $f_3$  bijective.

**Exercise 3.10.5** (Snake lemma) Consider a commutative diagram of modules with exact rows:

$$\begin{array}{ccccccc} & & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{p'} & C' & & \end{array}$$

1. Show that  $i$  sends  $\text{Ker } f$  into  $\text{Ker } g$  and  $p$  sends  $\text{Ker } g$  into  $\text{Ker } h$ .
2. Show that  $i'$  induces a morphism  $\text{Coker } f \rightarrow \text{Coker } g$  and that  $p$  induces a morphism  $\text{Coker } g \rightarrow \text{Coker } h$ .
3. Show that there exists a unique morphism  $\delta : \text{Ker } h \rightarrow \text{Coker } f$  such that the following sequence is exact:

$$\text{Ker } f \longrightarrow \text{Ker } g \longrightarrow \text{Ker } h \xrightarrow{\delta} \text{Coker } f \longrightarrow \text{Coker } g \longrightarrow \text{Coker } h.$$

Show that if  $i$  is injective and  $p$  is surjective, then the following sequence is exact:

$$0 \longrightarrow \text{Ker } f \longrightarrow \text{Ker } g \longrightarrow \text{Ker } h \xrightarrow{\delta} \text{Coker } f \longrightarrow \text{Coker } g \longrightarrow \text{Coker } h \longrightarrow 0.$$

4. (Bonus) Retrieve the Five Lemma from the snake Lemma.

**Exercise 3.10.6** Consider an exact sequence of modules  $0 \rightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \rightarrow 0$ . It is said that  $\sigma \in \text{Hom}_R(M_3, M_2)$  is a section of  $f_2$  if  $f_2 \circ \sigma = \text{Id}_{M_3}$ . When such a section exists, the sequence is said to be split.

1. Assuming such a section exists, show that the application  $(m_1, m_3) \mapsto f_1(m_1) + \sigma(m_3)$  defines an isomorphism  $M_1 \oplus M_3 \simeq M_2$ . Deduce that  $M_1 \simeq f_1(M_1)$  then admits a supplement.
2. Conversely, assume that  $M_1 \simeq f_1(M_1)$  admits a complement  $S$ . Show that  $f_2$  defines an isomorphism  $S \simeq M_3$ .
3. Show that a submodule  $N$  of  $M$  is a direct factor if and only if the exact sequence  $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$  is split. In this case, show that every supplement of  $N$  is isomorphic to  $M/N$ .
4. Show that if  $n > 1$ , the canonical exact sequence  $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z} \rightarrow 0$  is not split. In particular  $n\mathbf{Z}$  has no complement in  $\mathbf{Z}$ .
5. Let  $\pi : \mathbf{R}^{n+m} \rightarrow \mathbf{R}^m$  be the projection onto the last  $m$  coordinates. Show that there is an exact sequence  $0 \rightarrow \mathbf{R}^n \rightarrow \mathbf{R}^{n+m} \xrightarrow{\pi} \mathbf{R}^m \rightarrow 0$  and that this sequence is split.
6. Suppose there are three square matrices  $A, B, C$  with coefficients in  $\mathbf{R}$  of size  $n, n+m, m$  making the diagram commutative

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mathbf{R}^n & \longrightarrow & \mathbf{R}^{n+m} & \longrightarrow & \mathbf{R}^m & \longrightarrow & 0 \\
 & & \downarrow A & & \downarrow B & & \downarrow C & & \\
 0 & \longrightarrow & \mathbf{R}^n & \longrightarrow & \mathbf{R}^{n+m} & \longrightarrow & \mathbf{R}^m & \longrightarrow & 0
 \end{array}$$

Show that  $B$  is block triangular and identify the diagonal blocks. State and prove a reciprocal and compare with the preceding remark.

**Exercise 3.10.7** Let  $R$  be a commutative ring. Let  $I$  be a directed ordered set, that is, for every  $i, j \in I$ , there exists  $k \in I$  such that  $k \geq i, j$ . Let  $(M_i)_{i \in I}$  be a family of  $R$ -modules. Assume that for every  $j \geq i$ , we are given an  $R$ -module homomorphism  $f_{ij} : M_i \rightarrow M_j$  such that  $f_{ii} = \text{Id}$  and  $f_{jk} \circ f_{ij} = f_{ik}$  for all  $i \leq j \leq k$ .

We consider the set  $E$  of pairs  $(i, x_i)$  with  $i \in I$  and  $x_i \in M_i$ ; in other words,  $E$  is the disjoint union of the  $M_i$ .

1. Define a relation  $\sim$  on  $E$  by declaring that  $(i, x_i) \sim (j, x_j)$  if there exists  $k \in I$  such that  $k \geq i, k \geq j$ , and  $f_{ik}(x_i) = f_{jk}(x_j)$ . Show that this is an equivalence relation.

The inductive limit of the  $M_i$  is defined as the quotient set  $M$  of  $E$  by this relation. Denote by  $\varphi_i$  the map from  $M_i$  to  $M$  sending  $x_i$  to the equivalence class of  $(i, x_i)$ .

2. Show that there exists a unique  $R$ -module structure on  $M$  such that each map  $\varphi_i$  is an  $R$ -module homomorphism. We write  $M = \varinjlim_{i \in I} M_i$ .
3. Show that if  $N$  is an  $R$ -module, then for every family of homomorphisms  $u_i : M_i \rightarrow N$  satisfying  $u_j \circ f_{ij} = u_i$  for all  $i \leq j$ , there exists a unique homomorphism  $u : M = \varinjlim_{i \in I} M_i \rightarrow N$  such that  $u_i = u \circ \varphi_i$ .

4. Given a map  $f : M_1 \rightarrow M_2$  with  $I = \{1, 2\}$ , show that  $\varinjlim M_i = \text{coker}(f)$ .
5. Let  $\mathcal{V}$  be the set of neighborhoods of 0 in the complex plane (with the usual topology), ordered by  $U \leq V$  if and only if  $V \subset U$ . Let  $\mathcal{O}(U)$  denote the complex vector space of holomorphic functions on  $U$ , and let  $f_{U,V}$  be the restriction map  $\mathcal{O}(U) \rightarrow \mathcal{O}(V)$ . Show that  $\varinjlim_{U \in \mathcal{V}} \mathcal{O}(U)$  is naturally isomorphic to the vector space of power series with nonzero radius of convergence.

**Exercise 3.10.8** We will show that if the ring  $\mathcal{R}$  is not assumed to be commutative, then it may occur that the  $\mathcal{R}$ -modules  $\mathcal{R}^n$ ,  $n \geq 1$  are all isomorphic. To this end, we fix a real vector space  $V$  equipped with a countable base  $(e_k)_{k \in \mathbf{N}}$  and we denote  $\mathcal{R}$  the ring of linear applications on  $V$  (equipped with composition), identified as «infinite matrices» of

$c\mathcal{R}^{\mathbf{N} \times \mathbf{N}}$ . Define two linear applications  $T$  and  $T'$  on  $V$  by the following relations for  $n \in \mathbf{N}$ :

$$\begin{cases} T(e_{2n}) = e_n, \\ T(e_{2n+1}) = 0, \end{cases} \quad \text{and} \quad \begin{cases} T'(e_{2n}) = 0, \\ T'(e_{2n+1}) = e_n. \end{cases}$$

Write the «matrices» of  $T$  and  $T'$ . Given  $n \in \mathbf{N}^*$ , we consider  $\mathcal{R}^n$  as an  $\mathcal{R}$ -module for scalar multiplication:

$$\mathcal{R} \times \mathcal{R}^n \rightarrow \mathcal{R}^n, \left( r, \begin{pmatrix} T_1 \\ T_2 \\ \vdots \\ T_n \end{pmatrix} \right) \mapsto \begin{pmatrix} r \circ T_1 \\ r \circ T_2 \\ \vdots \\ r \circ T_n \end{pmatrix}.$$

1. Provide a one-element base for the  $\mathcal{R}$ -module  $\mathcal{R}^1$ .
2. Show that  $(T, T')$  is also a base for the  $\mathcal{R}$ -module  $\mathcal{R}^1$ .
3. Show that  $\mathcal{R}^1$  and  $\mathcal{R}^2$  are isomorphic as  $\mathcal{R}$ -modules then that  $\mathcal{R}^n$  is isomorphic to  $\mathcal{R}$  for every  $n \in \mathbf{N}^*$ .

**Exercise 3.10.9** Let  $d \geq 1$  be a natural number,  $R$  a principal ring and  $M = R^d$ . Let  $N$  be a submodule of  $M$ . We aim to prove by induction on  $d$  that  $N$  is isomorphic to  $R^\delta$  with  $\delta \leq d$ . Assume  $d \geq 1$  and the theorem proven for submodules of  $R^{d'}$  if  $d' < d$ .

1. Let  $\underline{\nu} = (\nu_1, \dots, \nu_d) \in N^d - \{0\}$  and  $i$  such that  $\nu_i \neq 0$ . The map  $\pi_i : (x_1, \dots, x_d) \mapsto x_i$  induces an exact sequence

$$(ii) \quad 0 \rightarrow K \rightarrow N \xrightarrow{\pi_i} C \rightarrow 0$$

where  $C$  is a nontrivial submodule of  $A$  and  $K \subset R^{d-1}$ .

2. Show that there exist  $d' < d$  and an exact sequence

$$0 \rightarrow R^{d'} \xrightarrow{j} N \xrightarrow{\pi} R \rightarrow 0.$$

3. Show that there exists a section  $\sigma = A \rightarrow N$  of  $\pi$ , i.e., satisfying  $\pi \circ \sigma = \text{Id}_A$ .

4. Show that the map  $\begin{cases} \mathbf{R}^{d'} \oplus \mathbf{R} & \rightarrow & \mathbf{N} \\ (x, y) & \mapsto & j(x) + \sigma(y) \end{cases}$  is an isomorphism.

5. Conclude.

**Exercise 3.10.10** Let  $\mathbf{R}$  be the ring of continuous real-valued  $\pi$ -periodic functions, and let  $\mathbf{M}$  be the set of continuous functions  $f$  such that for all real  $x$ ,  $f(x + \pi) = -f(x)$ .

1. Show that function multiplication makes  $\mathbf{M}$  into an  $\mathbf{R}$ -module.
2. Show that every pair  $(f, g) \in \mathbf{M}^2$  can be uniquely written as  $(a \cos x - b \sin x, a \sin x + b \cos x)$  with  $a, b \in \mathbf{R}$ .
3. Show that  $\mathbf{M} \oplus \mathbf{M}$  is a free module. What is its rank?
4. Show that every  $f \in \mathbf{M}$  has at least one zero.
5. Show that  $\mathbf{M}$  is not a free module of rank 1.
6. Show that  $\mathbf{M}$  is not free.

**Exercise 3.10.11** Let  $\mathbf{N} = \mathbf{Z}^{(\mathbf{N})}$  (direct sum of countable many copies of  $\mathbf{Z}$ ). It is a free submodule of  $\mathbf{M} = \mathbf{Z}^{\mathbf{N}}$  (product of countable many copies of  $\mathbf{Z}$ ) with basis  $e_n = (\delta_{n,p})_{p \in \mathbf{N}}$ . Let  $\varphi \in \text{Hom}_{\mathbf{R}}(\mathbf{M}^*, \mathbf{M})$  be the morphism  $u \mapsto (u(e_n))_{n \in \mathbf{N}}$ . We will prove that  $\varphi$  defines an isomorphism  $\mathbf{M}^* \rightarrow \mathbf{N}$  and then conclude by a cardinality argument that  $\mathbf{M}$  is not free<sup>15</sup>.

A. Determination of  $\text{Ker}(\varphi)$

Let  $d \geq 2$  be an integer.

1. Show that  $\text{Ker } \varphi \xrightarrow{\sim} \mathbf{G}^*$ , where  $\mathbf{G} = \mathbf{M}/\mathbf{N}$ .
2. Let  $\mathbf{H}_d$  be the set of elements of  $\mathbf{G}$  divisible by  $d^k$  for all  $k$ . Show that  $\mathbf{H}_d$  is a submodule of  $\mathbf{G}$ .
3. Show that any linear form  $u : \mathbf{G} \rightarrow \mathbf{Z}$  vanishes on  $\mathbf{H}_d$ .
4. Determine  $\mathbf{H}_2 + \mathbf{H}_3$ . Conclude.

B. Determination of  $\text{Im}(\varphi)$

For any  $x = 2^v y \in \mathbf{Z}$ , with  $y$  odd, we define  $|x|_2 = 2^{-v}$ ; we set  $|0|_2 = 0$ .

1. Check that  $(x, y) \mapsto |y - x|^2$  is metric on  $\mathbf{Z}$ . Show that if  $x_1, \dots, x_n$  are integers such that the  $|x_i|_2$  are pairwise distinct, then  $\sum |x_i|_2$  is the largest among the  $|x_i|_2$ .
2. For  $x = (x_n)_{n \in \mathbf{N}} \in \mathbf{M}$ , define  $|x|_2 = \sup |x_n|_2$ . Show that  $|x|_2$  is a real number and  $\forall u \in \mathbf{M}^*, \forall x \in \mathbf{M}, |u(x)|_2 \leq |x|_2$ .
3. Let  $x = (a_n)_{n \in \mathbf{N}}$ . Under what condition does the sequence  $(|x - \sum_k a_k e_k|_2)_{n \in \mathbf{N}}$  converges to 0?

<sup>15</sup>This method of proof of Baer's result comes from [9]

4. Let  $u \in M^*$  and denote by  $S = \{n \mid u(e_n) \neq 0\}$  the support of  $\varphi(u)$ . Show that there exists  $x \in M$  be an element whose support is  $S$  and such that the mappings  $S \rightarrow |x_s|_2$  and  $s \mapsto u(e_s)|x_s|_2$  from  $S$  to  $\mathbf{R}$  are strictly decreasing.
5. Let  $A \subset \{0, 1\}^{\mathbf{N}}$  be the set of all sequences with value in  $\{0, 1\}$  vanishing outside  $S$ . For  $\varepsilon \in A$ , define  $\Psi(\varepsilon) = u(\varepsilon x)$ , where  $\varepsilon x = (\varepsilon_n x_n)_{n \in \mathbf{N}}$ . Determine  $|\Psi(\varepsilon) - \Psi(\varepsilon')|_2$  as a function of  $s_0 = \inf\{s \mid \varepsilon_s \neq \varepsilon'_s\}$ . Deduce that  $\Psi : A \rightarrow \mathbf{Z}$  is injective.
6. Prove  $\text{Im}(\varphi) = \mathbf{N}$  by considering the cardinality of  $A$  [Hint: use for instance the map  $\varepsilon \mapsto \sum_{k=0}^{\infty} \varepsilon^k 2^{-k} \in [0, 1]$  and use that  $[0, 1]$  is not countable.]

## C. Conclusion

1. Describe  $M^*$ .
2. Prove that  $M$  is not free by a cardinality argument?
3. Show that the evaluation biduality morphism  $\mathbf{N} \rightarrow \mathbf{N}^{**}$  defined by  $x \mapsto (\varphi \mapsto \varphi(x))$  is an isomorphism, even though  $\mathbf{N}$  is freely generated over  $\mathbf{Z}$  with infinite rank.

**Exercise 3.10.12** Using Krull's theorem, how can you generalize 3.9.4.2 for general free modules?



# Chapter 4

## Rings and modules



### 4.1 Introduction



Perspective

We will illustrate how modules are an important tool for studying rings and vice versa. In particular, we will emphasise the role of matrices, which are crucial, the first step towards the advanced notion of *resolution* of a module/ring.

### 4.2 Quotient rings

Recall that an ideal  $I$  of a ring  $R$  is a submodule of  $R$ , *i.e.* an additive subgroup of  $R$  such that  $\forall x \in R, xI \subset I$ . By 3.3 there is a unique group structure on  $R/I$  which makes the projection  $\pi : R \rightarrow R/I$  a morphism of additive groups. The main (simple but important) result is as follows:

**Proposition 4.2.0.1** *There exists a unique ring structure on  $R/I$  making the projection  $\pi : R \rightarrow R/I$  a morphism of rings whose kernel is  $I$ . Moreover,*

- One has the following universal property (cf. 3.6.2.1) : for any ring  $T$ , the natural sequence

$$0 \rightarrow \text{Hom}_{\text{ring}}(\mathbb{R}/I, T) \rightarrow \text{Hom}_{\text{ring}}(\mathbb{R}, T) \rightarrow \text{Hom}_{\mathbf{Z}}(I, T)$$

is exact.

- $f \in \text{Hom}(\mathbb{R}, \mathbb{R}')$  induces a canonical isomorphism of rings  $\bar{f} : \mathbb{R}/\text{Ker}(f) \simeq \text{Im}(f)$  (cf. 3.3.0.4).
- the maps  $\bar{J} \mapsto J = \pi^{-1}(\bar{J})$  and  $I \supset J \mapsto J/I$  identifies are inverse each other identifying ideals  $\bar{J}$  of  $\bar{\mathbb{R}} = \mathbb{R}/I$  and ideals  $J$  of  $\mathbb{R}$  containing  $I$ .
- $\pi$  induces an isomorphism  $\mathbb{R}/J \xrightarrow{\simeq} \bar{\mathbb{R}}/\bar{J}$  for any ideal  $I \supset J$ .

In a diagrammatic way, the main point summarizes as

$$\text{If } \psi(I) = 0 \text{ then} \quad \begin{array}{ccc} & & T \\ & \nearrow \psi & \uparrow \exists! \varphi \\ I \hookrightarrow \mathbb{R} & \longrightarrow & \mathbb{R}/I \end{array}$$

*Proof.* The proof goes straightforwardly as in the case of the module, except for the fact that  $\pi$  is multiplicative which follows from the computation

$$\pi(x_1)\pi(x_2) = (x_1 + I)(x_2 + I) + I = x_1x_2 + x_1I + x_2 + I^2 + I = x_1x_2 + I$$

because  $x_1I + x_2 + I^2 \subset I$  (recall that if  $I, J$  are ideals,  $IJ$  denotes the ideal generated by all products  $ij$  where  $i \in I, j \in J$ ). □

**Definition 4.2.0.2** An ideal  $I$  of  $\mathbb{R}$  is prime if and only if  $\mathbb{R}/I$  is an integral domain, maximal if  $\mathbb{R}/I$  is a field (cf. 4.6.9).

### 4.2.1 Product rings

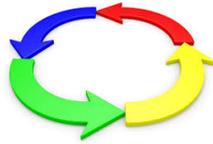
The group  $\prod \mathbb{R}_i$  has a natural ring structure defined by  $(x_i)(y_i) = (x_iy_i)$  for  $x_i, y_i \in \mathbb{R}_i$ . When the rings are fields, its ideals are easy to understand. Indeed, let  $F_t, t \in T$  be a finite family of fields,  $F_T = \prod_{t \in T} F_t$  and  $p_t : F_T \rightarrow F_t, t \in T$  the projection. For  $S \subset T$ , let  $I_S$  be the ideal

$$I_S = \{(x_t) \mid x_t = 0, \forall t \notin S\} = \text{Ker}(p_S : F_T \rightarrow F_S).$$

**Lemma 4.2.1.1** Let  $I$  be an ideal of  $F_T$  and  $S = \{t \in T \mid p_t(I) = \{0\}\}$ . Then  $I = I_S$  and  $F_T/I = F_S$ .

*Proof.* Let  $e_t = (\delta_{t,t'})_{t' \in T} \in F_T$ . We have  $p_S(I) = \{0\}$  by definition of  $S$  implying  $I \subset \text{Ker}(p_S)$ . Conversely, let  $(x_t) \in \text{Ker}(p_S)$  and  $t \notin S$ . Then  $p_t(I)$  is a nonzero ideal of the field  $F_t$  and therefore is equal to  $F_t$ . We can choose  $i_t \in I$  such that  $p_t(i_t) = 1 \in F_t$  and therefore  $e_t = e_t i_t \in I$ . Then,  $x = \sum_{t \notin S} x_t e_t \in I$  as wanted.  $\square$

## 4.2.2 Cyclic modules and quotient rings



As in the group case, a  $R$ -module is said *cyclic* if it can be generated by a single element. If  $R = \mathbf{Z}$ , it is well known that any cyclic group is isomorphic to  $\mathbf{Z}/n\mathbf{Z}$ . and that its subgroups are cyclic isomorphic to  $\mathbf{Z}/d\mathbf{Z}$  with  $n\mathbf{Z} \subset d\mathbf{Z}$ , i.e.  $d|n$ . In general, we get

**Lemma 4.2.2.1** (Cyclic modules) *A module  $M$  is cyclic if and only if it is isomorphic to  $R/I$  for some ideal  $I$ . In this case we have*

- $I = \text{Ann}_R(M) = \{\lambda \in R \mid \lambda M = \{0\}\}$ .
- The map  $(J \supset I) \mapsto N = JM \subset M$  has inverse  $N \mapsto J = \pi^{-1}(N) = \{\lambda \in R \mid \lambda x \in N\}$  and identifies the ideals of  $J \supset I$  and the submodules of  $N \subset M$ .
- We have  $J/I \xrightarrow{x} JM$  and  $R/J \xrightarrow{x} M/N$ .
- In particular, if the ideals of  $R$  can be generated by a single element<sup>1</sup>, all submodules of a cyclic module are cyclic.

*Proof.* Let  $x$  be a generator of  $M$ . Then, the map  $R/I \xrightarrow{x} M$  is an isomorphism and conversely the image of 1 by any such isomorphism is a generator of  $M$ . The rest is up to the reader.  $\square$

## 4.3 Algebras

Given two rings, we say that  $B$  is an  $A$ -algebra if  $B$  is further equipped with an  $A$ -module structure compatible with the product in the sense that

$$a \cdot (bb') = (a \cdot b)b' \quad \forall a \in A, b, b' \in B.$$

<sup>1</sup>Hence if  $R$  is a PID.

This is equivalent to giving a ring morphism  $f : A \rightarrow B$  since we can then define the module structure by  $a \cdot b = f(a)b$  for  $a \in A$ ,  $b \in B$ . For example,  $\mathbf{C}$  is an  $\mathbf{R}$ -algebra, and a ring is a  $\mathbf{Z}$ -algebra. A morphism  $f \in \text{Hom}_A(B, B')$  of  $A$ -algebras is an  $A$ -module morphism which is multiplicative with  $f(1_B) = 1_{B'}$ .

**Proposition 4.3.0.1** *Let  $B$  be an  $A$ -algebra and  $b \in B$ . There exists a unique algebra morphism  $A[T] \rightarrow B$  that sends  $T$  to  $b$ . Moreover, all morphisms are of this type.*

*Proof.* Let  $\varphi$  be such a morphism. Then, necessarily,  $\varphi(\sum_i a_i T^i) = \sum_i a_i \varphi(T)^i$  and thus is determined by  $b = \varphi(T)$ . Conversely, we know (2.1.3.1) that this  $A$ -module morphism

$$\sum_i a_i T^i \mapsto \sum_i a_i b^i$$

is also an  $A$ -algebra morphism. □

Using the identification  $A[X, Y] = A[X][Y]$ , we obtain that the algebra morphisms from  $A[X_1, \dots, X_n]$  to  $B$  are identified with  $n$ -tuples  $b = (b_1, \dots, b_n) \in B^n$  (to such an element is associated the evaluation morphism  $(P \mapsto P(b))$ ).

Note that if  $B$  is an  $A$ -algebra and  $I$  an ideal of  $B$ , then the quotient ring  $B/I$  is also an  $A$ -module (since  $B$  and  $I$  are  $A$ -modules) and thus  $B/I$  is canonically an  $A$ -algebra.

## 4.4 Integrality

### 4.4.1 An application of Cayley-Hamilton

**Proposition 4.4.1.1** (Determinant trick) *Let  $f$  be an endomorphism of a finitely generated  $R$ -module  $M$ . There exists a monic polynomial  $P \in R[T]$  that annihilates  $f$ . If additionally  $f(M) \subset IM$ , it can be assumed that the coefficients of  $f$  with index  $< \deg(P)$  belongs to  $I$ .*

*Proof.* Let  $m_i$ ,  $1 \leq i \leq n$  be a finite family of generators of  $M$  and write for each  $j$  (in a non-unique way)

$$f(m_j) = \sum_i a_{i,j} m_i$$

defining a matrix<sup>2</sup>  $A = [a_{i,j}]$  of  $f$ . Note that if  $f(M) \subset IM$ , we can assume  $a_{i,j} \in I$ . It is then enough to look at  $P = \det(T \text{Id} - A)$  and invoke Cayley-Hamilton theorem (2.1.3.2) for  $A \in M_n(R)$ . □

By applying the proposition to  $f = \text{Id}_M$ , we obtain the famous Nakayama Lemma which is very important in advanced commutative algebra.

<sup>2</sup>Depending on the non unique choices of the  $a_{i,j}$ .

**Corollary 4.4.1.2** (Nakayama) *Let  $M$  be a finitely generated module and  $I$  an ideal such that  $M = IM$ . Then, there exists  $i \in I$  such that  $(1 + i)M = 0$ . In particular, if  $1 + i$  is invertible (for instance if  $i$  is nilpotent), then  $M = 0$ .*

**Example(s) 4.4.1.3** *Let us show that, as in the vector space situation, any surjective endomorphism  $f$  of a finitely generated  $R$ -module  $M$  is an isomorphism. As in the vector case (3.7), we endow  $M$  with a structure of  $R[T]$  module  $M_f$  by the rule  $P(T)m = P(f)(m)$ . This module is finitely generated as  $M$  is and the surjectivity of  $f$  gives  $M_f = (T)M_f$ . There exists therefore  $P \in R[T]$  such that  $(1 + P(T))M = 0$ . If  $f(m) = 0$ , we therefore get  $(1 + TP(T))m = m + P(f)(f(m)) = 0$  hence the injectivity of  $f$ . The analogous statement for injective endomorphisms is definitely false (take  $\mathbf{Z} \xrightarrow{2} \mathbf{Z}$  for instance).*

## 4.4.2 Ring of integers

Let  $R'$  be an  $R$ -algebra (in other words, consider a ring morphism  $R \rightarrow R'$ ).

**Definition 4.4.2.1** *An element  $x \in R'$  is said to be integral over  $R$  if there exists a monic polynomial in  $R[T]$  with coefficients in  $R$  annihilating  $x$ .*

If  $R = \mathbf{k}$  is a field, these elements are also called *algebraic over  $\mathbf{k}$* , the integrality condition being equivalent to the usual algebraicity condition of the existence of a  $P \in \mathbf{k}[T] - \{0\}$  cancelling  $x$  (divide by the dominant coefficient of  $P$ ).

**Lemma 4.4.2.2**  *$x \in R'$  is integral over  $R$  if and only if it belongs to a subring of  $R'$  which is of finite type over  $R$ .*

*Proof.* If  $x$  is cancelled by a monic degree  $d$  polynomial of  $R[T]$ , then  $R[x]$  is generated by  $1, \dots, x^{d-1}$  hence the direct part. Conversely, if  $x$  belongs to a subring  $R''$  of  $R'$  which is of finite type over  $R$ , the determinant trick applied to the homothety  $h_x$  of ratio  $x$  on  $R''$  produces a monic annihilator  $P \in R[T]$  and therefore  $P(h_x)(1) = h_{P(x)}(1) = P(x) = 0$ .  $\square$

### Corollary 4.4.2.3

1. *The subset  $\mathcal{O}$  of  $R'$  of elements which integral over  $R$  forms a subring of  $R'$ .*

2. Any element of  $R'$  which is integral over  $\mathcal{O}$  belongs to  $\mathcal{O}$
3. If  $k$  is a subfield of a field  $k'$ , the subset of elements of  $k'$  that are algebraic over  $k$  forms a subfield of  $k'$ .

*Proof.* 1. If  $x, y \in \mathcal{O}$  are cancelled by monic polynomials of degree  $d_1, d_2$ , then  $R[x, y] \subset R'$  is generated by the monomials  $x^i y^j$ ,  $i < d_1, j < d_2$  and therefore is made of integral elements by the above lemma.

2. If  $x$  is integral over  $\mathcal{O}$ , the subring of  $R'$  generated by  $x$  and the coefficients of a monic polynomial of  $\mathcal{O}[T]$  cancelling  $x$  is of finite type over  $R$  and therefore  $x \in \mathcal{O}$ .
3. By (1), it suffices to show that the inverse of a nonzero algebraic element  $x \in k'$  is still nonzero. Suppose therefore  $P$  is a unitary annihilator of  $x$ . But then,  $T^{\deg(P)}P(1/T)$  is a nonzero annihilator of  $1/x$ .

□

**Definition 4.4.2.4** With the above notations,  $\mathcal{O}$  is called the integral closure of  $R$  in  $R'$ . If moreover  $R$  is an integral domain whose integral closure in its fraction field coincides with  $R$ , we say that  $R$  is an integrally closed domain.

The following lemma gives the coherence of the terminology (see more generally 9.6.1).

**Lemma 4.4.2.5**  $\mathbf{Z}$  is integrally closed (see more generally 9.6.1).

*Proof.* Let  $p/q \in \mathbf{Q}$  with  $\text{GCD}(p, q) = 1$  root of  $P(T) = T^n + \sum_{i < n} a_i T^i \in \mathbf{Z}[T]$ . We have

$$0 = q^n P(p/q) = p^n + \sum_{i < n} a_i p^i q^{n-i} = p^n + q \left( \sum_{i < n} a_i p^i q^{n-i-1} \right)$$

hence  $q|p^n$ . By Gauss lemma,  $q|p$  and therefore  $q = \pm 1$  and  $p/q \in \mathbf{Z}$ .

□

**Remark(s) 4.4.2.6** Observe that (2) shows that the field  $\overline{\mathbf{Q}}$  of complex numbers which are algebraic over  $\mathbf{Q}$  is an algebraically closed field, which is a good news. The set  $\overline{\mathbf{Z}}$  of complex numbers which are integral over  $\mathbf{Z}$  is a subring of  $\overline{\mathbf{Z}}$ . One will show  $\overline{\mathbf{Z}}$  is non Noetherian (5.3.3), which is a bad news in some extent.

**Remark(s) 4.4.2.7** *With a slight abuse, one often simply say that a complex number which is algebraic over  $\mathbf{Q}$  is algebraic, the non algebraic complex numbers being the transcendental ones. A simple countability argument shows that a randomly chosen complex number is almost surely (for the Lebesgue measure) transcendental. For instance, both  $e$  (due to C. Hermite, 1873) and  $\pi$  (F. Lindemann, 1883) are transcendental.*

## 4.5 The Chinese remainder lemma

We know that the rings  $\mathbf{Z}/nm\mathbf{Z}$  and  $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$  are isomorphic if  $n$  and  $m$  are coprime, and the reader probably knows more generally that  $R/(ab) \xrightarrow{\sim} R/(a) \times R/(b)$  for coprime ideals  $(a), (b)$  in a PID  $R$ . The latter condition can also be written as  $(a) + (b) = R$  according to Bézout's identity. We will give a useful (fortunately quite straightforward) generalization in the case where  $R$  is a (commutative with unit) algebra over some ring (recall that every ring has a unique structure of  $\mathbf{Z}$ -algebras). Let us give a slightly more general version.

«When General Han Ting arranges his soldiers in threes, there remain two soldiers, when he arranges them in fives, there remain three, and when he arranges them in sevens, there remain two. How many soldiers does Han Ting's army consist of? », Sun Zi, around the 4th century.



Terracotta Army  
Mausoleum of Emperor Qin

**Proposition 4.5.0.1** (Chinese remainder lemma) *Let  $I_1, \dots, I_n$ ,  $n \geq 2$  be ideals of  $R$  which are pairwise coprime, i.e., such that  $I_i + I_j = R$  for  $i \neq j$  and let  $M$  be an  $R$ -module. Let  $I(-j) = I_1 \cdots \widehat{I}_j \cdots I_n$  be the ideal product of the ideals  $I_i$  distinct from  $I_j$ <sup>3</sup>*

1.  $\sum_j I(-j) = R$  and  $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ .
2. The canonical morphism  $R \rightarrow \prod R/I_j$  factors through  $\cap I_j$  to give an algebra isomorphism

$$\varphi: R/I_1 \cap \cdots \cap I_n \simeq \prod R/I_j.$$

Let  $\varepsilon_j \in I(-j)$  such that  $\sum \varepsilon_j = 1$  and  $e_j = \varepsilon_j \bmod I_1 \cdots I_n$ .

3.  $\varphi(e_j) = (\delta_{i,j})_i$  and therefore  $e_i e_j = \delta_{i,j} e_i$  and  $\sum e_i = 1$  (complete family of orthogonal idempotents)<sup>4</sup>.

4. The canonical morphism  $M \rightarrow \prod M/I_j$  factors through  $\cap I_j$  to give an module isomorphism

$$\varphi_M : M/(\cap I_j)M \simeq \prod M/I_j M$$

whose inverse is  $(m_j) \mapsto \sum e_j m_j$

5. The canonical morphism  $\oplus \text{Ann}_M(I_j) \rightarrow M$  is an isomorphism of inverse  $m \mapsto \sum \varepsilon_j m$ .

*Proof.*

1. We can proceed by induction on  $n$ . If  $n = 2$ , this is the hypothesis  $I_2 + I_1 = R$ . Otherwise, we apply the induction hypothesis to  $I_1, \dots, I_{n-1}$ . We then obtain that the sum of the  $n - 1$  ideals  $I_1 \cdots \widehat{I_j} \cdots I_{n-1}$  is  $R$ . Multiplying by  $I_n$ , we get  $\sum_{j < n} I(-j) = I_n$  and the sum  $\sum_j I(-j)$  contains  $I_n$ . Reapplying the same process to  $I_2, \dots, I_n$ , we obtain that the sum contains  $I_1$ . Since  $I_1 + I_n = R$ , the sum equals  $R$ .

2. The kernel of  $R \rightarrow R/I_1 \times \cdots \times R/I_n$  is the intersection  $I_1 \cap \cdots \cap I_n$ . By the universal property of the quotient, we thus have an injective algebra morphism. Let us verify that  $\varphi$  is onto. We write  $1 = \sum_j \varepsilon_j$ ,  $\varepsilon_j \in I(-j)$ . Let  $x_j \text{ mod } I_j$  be arbitrary classes. Set  $x = \sum_j \varepsilon_j x_j$ . Observe that

$$(*) \quad \varepsilon_j \equiv 0 \text{ mod } I_i \text{ if } i \neq j \text{ and } \varepsilon_j \equiv 1 \text{ mod } I_j$$

and therefore  $x \equiv x_j \varepsilon_j \equiv x_j \text{ mod } I_j$  for all  $j$ .

3. The other items follow directly from (\*)

□

**Remark(s) 4.5.0.2** The reader should notice that the quotient rings  $R$  of a finite product of rings  $\prod_{i \in I} R_i$  (as in (2) above) is a finite direct product of quotient rings of  $R_i$ . For, let  $\text{Ker}$  be the ideal  $\text{Ker} = \text{Ker}(\prod R_i \rightarrow R)$  and  $e_i = (\delta_{i,j})_j$  the  $i$ -th idempotent of  $\prod R_i$ . Then,  $x = \sum e_i x \in \text{Ker}$  if and only if  $e_i x = 0$  proving  $\text{Ker} = \prod e_i \text{Ker}$  and  $R' = \prod R_i / e_i \text{Ker}$ . The ideals of fields being trivial, we get in particular that any quotient  $\prod_{i \in I} F_i$  of a finite product of fields is isomorphic to  $\prod_{j \in J} F_j$  where  $J = \{i \in I \mid e_i \text{Ker} = \{0\}\}$  (compare with 4.2.1.1).

<sup>4</sup>Recall that by definition its is the ideal generated by products of  $\prod_{i \neq j} x_i$  with  $x_i \in I_i$ .

<sup>4</sup>By definition, an idempotent of a ring is an element  $e$  such that  $e^2 = e$ . Two different idempotents are said to be orthogonal if there product vanishes. A finite family of orthogonal idempotents is complete if there sum equals to 1.

## 4.6 Exercises

**Exercise 4.6.1** Show that there is a one to one correspondence between  $R$ -module  $M$  canceled by an ideal  $I \subset R$  and  $R/I$ -modules.

**Exercise 4.6.2** Let  $M$  a cyclic module over a principal ideal ring (PID)  $R$  with annihilator  $\text{Ann}_R(M) = I$ . Prove that the submodules  $N$  of  $M$  are cyclic and are in one to one correspondence with ideals  $J$  containing  $I$ . If  $R = \mathbf{k}[T]$  or  $R = \mathbf{Z}$ , prove that their number is finite unless  $M \xrightarrow{\sim} R$  (or equivalently  $I = \{0\}$ )<sup>5</sup>. Prove that the ideal of polynomials in  $\mathbf{R}[T_1, T_2]$  vanishing at  $(0, 0)$  is not cyclic but is a submodule of cyclic module.

**Exercise 4.6.3** Describe an isomorphism of  $\mathbf{R}$ -algebras between  $\mathbf{R}[T]/(T^2 + T + 1)$  and  $\mathbf{C}$  on one hand, and between  $\mathbf{R}[T]/(T(T + 1))$  and  $\mathbf{R}^2$  on the other hand.

**Exercise 4.6.4** Generalize 4.3.0.1 to several variables (compare with 2.1.1.1).

**Exercise 4.6.5** Show that that integral closure of  $\mathbf{Z}[T^2, T^3]$  is  $\mathbf{Z}[T]$ . Prove that the  $\mathbf{Z}[T^2, T^3]$  and  $\mathbf{Z}[T_1, T_2]/(T_1^3 - T_2^2)$  are isomorphic.

**Exercise 4.6.6** Let  $R$  be a ring. We recall  $(R[T])^\times = R^\times + \text{TR}_{\text{nil}}[T]$  (2.4.7)

1. If  $x$  is nilpotent, show that  $1 + x \in R^\times$ .
2. Show that a nilpotent element belongs to any prime ideal of  $R$ .
3. If  $x \in R$  is non nilpotent, show that  $R[T]/(xT - 1)$  is nonzero. Deduce that it has a maximal ideal.
4. Prove that the intersection of prime ideals of  $R$  is the set of nilpotent elements of  $R$ .

**Exercise 4.6.7 (Resultant)** Let  $R$  be a ring and  $P, Q \in R[T]$  be two polynomials of degrees  $p, q > 0$ . Let  $\text{Res}(P, Q)$  denote the resultant of  $P$  and  $Q$ , defined as the determinant, in canonical bases (cf. 3.7), of the linear map between free modules of rank  $p + q$

$$\rho(P, Q) : \begin{cases} R_{<q}[T] \times R_{<p}[T] & \rightarrow R_{<p+q}[T] \\ (A, B) & \mapsto AP + BQ \end{cases}$$

1. Calculate  $\text{Res}(P, Q)$  if  $P$  has degree 1.
2. By considering the comatrix of  $\rho(P, Q)$ , show that there exist  $A, B \in R[T]$  of degrees  $q, p$  respectively such that  $AP + BQ = R(P, Q)$ . Hence deduce that if  $P, Q$  have a common root in  $R$ , then  $R(P, Q) = 0$ .
3. If  $P, Q$  are also monic, show that  $\rho(P, Q)$  is the matrix of the multiplication  $\mu : R[T]/(Q) \times R[T] \rightarrow R[T]/(PQ)$  in canonical bases (of monomial classes  $T^i$ ).
4. Still assuming  $P, Q$  are monic, show that there is a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & R[T]/(PQ) & \xrightarrow{(T-x)} & R[T]/((T-x)PQ) & \xrightarrow{\text{ev}_r} & R \longrightarrow 0 \\ & & \uparrow \rho(P,Q) & & \uparrow \rho((T-x)P,Q) & & \uparrow Q(x) \\ 0 & \longrightarrow & R[T]/(Q) \times R[T]/(P) & \xrightarrow{(1,(T-x))} & R[T]/(Q) \times R[T]/((T-x)P) & \xrightarrow{\text{ev}_Q(x)} & R \longrightarrow 0 \end{array}$$

where  $ev(A) = A(x)$  and  $ev_Q(A, B) = A(x)$ . Hence deduce that  $\rho((T - x)P, Q)$  is block triangular with diagonal  $\text{diag}(\rho(P, Q), Q(x))$ , and then that  $\text{Res}((T - x)P, Q) = Q(x) \text{Res}(P, Q)$ .

5. If  $Q$  is monic, show that  $\text{Res}(\prod(T - x_i), Q) = \prod Q(x_i)$ . What happens if  $Q$  is not assumed to be monic?
6. If  $R = \mathbf{k}$  is a field, show that  $\deg(\text{PGCD}(P, Q)) > 0$  if and only if there exist nonzero  $A, B \in \mathbf{k}[T]$  of degree  $< q$  and  $< p$  respectively such that  $AP = BQ$ . Deduce that  $P, Q$  are coprime if and only if their resultant  $\text{Res}(P, Q) \neq 0$ .

**Exercise 4.6.8** Let  $\sqrt{d} \in \mathbf{C}$  be a square root of the square free integer  $d$  and  $K = \mathbf{Q}(\sqrt{d}) = \{a + b\sqrt{d}, a, b \in \mathbf{Q}\}$ . Let  $x \in K$ .

1. Prove  $\mathbf{Q}[T]/(T^2 - d) \xrightarrow{\sim} K$  and  $K$  is a field of dimension 2 over  $\mathbf{Q}$ .
2. Compute the characteristic polynomial of the multiplication  $h_x$  of  $x$  on the  $\mathbf{Q}$ -vector space  $K$ .
3. Show that  $x$  is integral over  $\mathbf{Z}$  if and only if  $\det(h_x), \text{Tr}(h_x) \in \mathbf{Z}$ .
4. Prove that the subring of  $K$  of integral elements over  $\mathbf{Z}$  is  $\mathbf{Z}[\sqrt{d}]$  if  $d \equiv 2, 3 \pmod{4}$  and  $\mathbf{Z}[(1 + \sqrt{19})/2]$  if  $d \equiv 2, 3 \pmod{4}$ .
5. What is the integral closure of  $\mathbf{Z}[\sqrt{d}]$ ?

**Exercise 4.6.9** Let  $M$  be an  $R$ -module and  $I$  an ideal.

1. Show that  $I$  is prime if and only if  $I$  is a proper ideal and  $xy \in I \Rightarrow x \in I$  or  $y \in I$ .
2. Show that  $I$  is maximal among the family of proper ideals of  $R$  if and only if  $R/I$  is a field.
3. Show that  $M$  is of finite type if and only if there exists a surjective  $R$ -linear mapping  $R^n \rightarrow M$  for some  $n \in \mathbf{N}$ .
4. Show that if  $f \in \text{Hom}_R(R^m, R^n) = M_{n,m}(R)$  is surjective then  $m \geq n$ .

*Hint: Consider a maximal ideal  $I$  of  $R$  and see that after reduction modulo  $I$ , the application  $f$  remains surjective modulo  $I$ .*

5. Show that if  $f$  is an isomorphism, then  $n = m$ .
6. Show that a free module of finite type  $L$  has a finite basis and that all its bases have the same cardinality: the rank of  $L$ .
7. Show that the rank of  $L$  is the minimal cardinal of a finite generating family.

**Exercise 4.6.10** Let  $P$  be a polynomial with integer coefficients  $P$  without rational root,  $d$  its degree and  $x \in \mathbf{R}$  a real root of  $P$ . Let  $(p, q) \in \mathbf{Z} \times \mathbf{N}^*$ .

1. Show  $d > 1$ .

2. Show  $|\mathbf{P}(\frac{p}{q})| \geq \frac{1}{q^d}$ .
3. Show there exists  $C > 0$  such that if  $\frac{p}{q} \in [x - 1, x + 1]$  then

$$\left| x - \frac{p}{q} \right| \geq \frac{C}{q^d}.$$

4. Show that  $\ell = \sum_{n \geq 0} 10^{-n!}$  is transcendental [Hint : what can you say about the periodicity of a decimal expansion of a rational number ?].

**Exercise 4.6.11** Let  $n$  be a positive integer and  $z_1, \dots, z_n$  be complex numbers. Define  $P_m(T) = \prod_i (T - z_i^m)$  for  $m \geq 0$  and suppose that  $0 < |z_i| \leq 1$  for all  $i$  and that  $P_1 \in \mathbf{Z}[T]$ .

1. Show that the  $P_m(T)$  have integer coefficients.
2. Show that the set  $\{P_m, m \geq 0\}$  is finite.
3. Conclude that the  $z_i$  are roots of unity.

**Exercise 4.6.12** Let  $I$  be an ideal of  $R$  with  $I^2 = \{0\}$  and  $n \geq 1$ .

- Show that the reduction morphism  $SL_n(R) \rightarrow SL_n(R/I)$  is onto.
- Prove that there is an exact sequence of group

$$\{0\} \rightarrow M_n(R/I) \rightarrow SL_n(R) \rightarrow SL_n(R/I) \rightarrow \{1\}$$

- If  $p$  is a prime number, compute  $\text{Card}(SL_n(\mathbf{Z}/p\mathbf{Z}))$ .
- For any  $m > 0$ , compute  $\text{Card}(SL_n(\mathbf{Z}/m\mathbf{Z}))$  [Use the Chinese remainder theorem].

**Exercise 4.6.13** ( $\mathbf{C}$  is algebraically closed) Let  $P$  be a non constant complex polynomial.

1. Show that  $\lim_{|z| \rightarrow \infty} 1/P(z) = 0$ .
2. If  $P$  has no complex root, show that  $1/P$  is bounded over  $\mathbf{C}$ .
3. Using that any bounded holomorphic function on the plane is constant; deduce that  $\mathbf{C}$  is algebraically closed.



# Chapter 5

## Noetherianity



David Hilbert



Emmy Noether

### 5.1 Introduction



#### Perspective

Noetherian rings and modules are probably the most important notion encountered in this volume. This remarkably stable class of rings (and modules) allows in particular to write any finite-type module as a cokernel of some matrix, allowing to obtain quite general and non-trivial results in an easy way, such as the structure theorem for finite-type abelian groups (6.4.0.2) or more generally of finite-type modules over PID (6.4.0.1). This view is the gateway to advanced topics such as syzygies, homological algebra. . . .

The notion of a Noetherian ring inevitably leads back in 1890 to Hilbert's fundamental paper [14] with its three main theorems, the first being the fundamental theorem 5.2.2.1 in the case of polynomial rings. However, as a student rightly pointed out to us, it is unfair to talk only about this tremendous paper<sup>1</sup>. In fact, it was Emmy Noether who developed the general vision back in 1920 ([18]). We will give the basics of Noetherian rings and modules and explain the connection with linear algebra.

---

<sup>1</sup>The other two theorems in the article are none other than the Nullstellensatz and the Syzygy Theorem!

## 5.2 Noetherian modules

The image of a family of generators of a module through a morphism generates the image module. Thus, *every quotient of a finitely generated module is still finitely generated*. However, while a submodule of a finitely generated  $R$  module is still finitely generated when  $R$  is a field, this is generally not the case (cf 3.7). However, it is the case in a Noetherian setting.

**Lemma 5.2.0.1** *Let  $M$  be an  $R$  module. The following properties are equivalent.*

1. *Every submodule of  $M$  is finitely generated.*
2. *Every increasing sequence of submodules eventually stabilizes.*
3. *Every non-empty family of submodules of  $M$  has a maximal element for inclusion.*

*Proof.*

$1 \Rightarrow 2$ . Let  $M_i$  be an increasing sequence of submodules. Thus,  $\cup M_i$  is a submodule of  $M$  and is therefore finitely generated. Choose a finite family of generators: for  $n$  large enough, they all belong to  $M_n$  and therefore  $M_i = M_n$  if  $i \geq n$ .

$2 \Rightarrow 3$ . Let  $\mathcal{F}$  be a non-empty family of submodules  $M$  without any maximal element (proof by contradiction). We construct a strictly increasing sequence of elements of  $\mathcal{F} \neq \emptyset$  by induction by choosing  $M_0$  one of its elements arbitrarily then by induction, assuming the sequence built for  $i \leq n$ , we observe that  $M_n$  is not maximal thus there exists  $M_{n+1}$  in  $\mathcal{F}$  which strictly contains  $M_n$ .

$3 \Rightarrow 1$ . Thus, let  $N$  be a submodule of  $M$  and let  $\mathcal{F}$  be the family of its finitely generated submodules. As  $\{0\} \in \mathcal{F}$ , this family is non-empty. Let  $N'$  be a maximal element. It is finitely generated contained in  $N$  by construction. Conversely, let  $n \in N$ . The module  $Rn + N'$  is in  $\mathcal{F}$  and contains the maximal element  $N'$ : so it's equal to it, so  $n \in N'$ . So we have  $N' = N$  and therefore  $N$  is finitely generated.

□

### Definition 5.2.0.2

1. *A module that satisfies the previously mentioned equivalent conditions is said to be Noetherian.*
2. *A ring that is Noetherian as a module over itself is said to be a Noetherian ring.*

Thus, a ring  $R$  is Noetherian if and only if it satisfies one of the following three equivalent propositions:

1. Every ideal is finitely generated.
2. Any increasing sequence of ideals eventually stabilizes.

3. Every non-empty family of ideals has a maximal element for inclusion.

**Example(s) 5.2.0.3** *Fields, principal rings, and quotient rings of Noetherian rings are Noetherian. However, a subring of a Noetherian ring is generally not Noetherian (for example, a polynomial ring over a field with an infinity of variables is not Noetherian, whereas it is a subring of its fraction field of fraction (3.10.3) which is certainly Noetherian!).*

### 5.2.1 Stability under exact sequences

**Proposition 5.2.1.1** *Consider an exact sequence of modules*

$$0 \rightarrow M_1 \xrightarrow{j} M_2 \xrightarrow{p} M_3 \rightarrow 0.$$

*Then  $M_2$  is Noetherian if and only if  $M_1$  and  $M_3$  are.*

*Proof.*

$\Rightarrow$  A submodule of  $M_1$  is (isomorphic to) a submodule of  $M_2$  hence is of finite type. If  $N_3$  is a submodule of  $M_3$ ; its inverse image  $p^{-1}(N_3) \subset M_2$  is finitely generated. But  $p$  being onto, we have  $p(p^{-1}(N_3)) = N_3$  hence  $N_3$  is also finitely generated.

$\Leftarrow$  Assume  $M_1$  and  $M_3$  are Noetherian, and let  $M'_2$  be a submodule of  $M_2$ . We have an exact sequence

$$0 \rightarrow j^{-1}(M'_2) \rightarrow M'_2 \rightarrow p(M'_2) \rightarrow 0.$$

But  $j^{-1}(M'_2)$  and  $p(M'_2)$  are finitely generated as submodules of  $M_1$  and  $M_3$ . Therefore, one can choose a finite family of generators for  $p(M'_2)$  of the form  $p(g'_{2,i})$  and a finite family of generators  $g_{1,k}$  for  $j^{-1}(M'_2)$ . The finite family  $j(g_{1,k}), g'_{2,i}$  of  $M'_2$  generates it.  $\square$

In particular, if  $R$  is Noetherian, then  $R^n$  is a Noetherian module, and thus so is any quotient. This leads to the following important corollary.

**Corollary 5.2.1.2** *The Noetherian modules over a Noetherian ring are exactly the finitely generated modules.*

**Remark(s) 5.2.1.3** *Every Noetherian module is of finite presentation, meaning that there exists an exact sequence  $R^m \xrightarrow{A} R^n \rightarrow M \rightarrow 0$  or equivalently  $\text{Coker}(A) \xrightarrow{\sim} M$ . For, because  $M$  is of finite type, there exists a surjective morphism  $R^n \rightarrow M$  whose kernel  $\text{Ker}$  is again of finite type as submodule of the Noetherian module  $R^n$ .*

There exists therefore a surjective morphism  $R^m \rightarrow \text{Ker}$  and the composition with the inclusion  $\text{Ker} \rightarrow R^n$  gives the wanted exact sequence. By functoriality of the cokernel, two equivalent matrices define isomorphic modules: this is the reason of the deepness of the interplay between equivalence of matrices and modules study at least in the Noetherian situation.

## 5.2.2 Hilbert's Basis Theorem

**Theorem 5.2.2.1** *Let  $R$  be a Noetherian ring.*

1. *The polynomial ring  $R[T]$  is Noetherian.*
2. *Every finitely generated  $R$ -algebra is a Noetherian ring.*

*Proof.* The second point is a direct consequence of the first (by induction, every polynomial ring over  $R$  with  $n$  variables is Noetherian, and so is every quotient). Let's consider the first point.

Let  $I$  be an ideal of  $R[T]$  and  $I^* = I - \{0\}$ . If  $P$  is a nonzero polynomial, denote  $\text{dom}(P)$  its highest degree nonzero coefficient. The formula  $\text{dom}(T^n P) = \text{dom}(P)$  ensures that  $\{0\} \cup \text{dom}(I^*)$  is an ideal of  $R$  (**exercise**). Thus it has a finite number of generators of the form  $\text{dom}(P_i), P_i \in I^*$ , which can be assumed to be of degree  $d \geq 0$  according to the previous formula. An immediate induction that  $I = I \cap R_{\geq d}[T] + I \cap R_{\leq d}[T]$  is generated by  $(P_i)$  and  $I \cap R_{< d}[T]$ . But  $I \cap R_{< d}[T]$  is a sub- $R$ -module of  $R_{< d}[T] \simeq R^d$ : so it is a Noetherian  $R$ -module (5.2.1.2). So you can take a finite number of generators  $Q_j$  (as  $R$ -module) and the finite family  $(P_i, Q_j)$  generates  $I$ .  $\square$

In fact, we have reused the Euclidean division argument used to show that  $k[T]$  is principal, the problem being that we can only divide in  $R[T]$  if the leading coefficient of the polynomial is an invertible of  $R^\times$ . This is the reason for introducing the ideals of the leading coefficients of  $I$ .

## 5.2.3 Krull's intersection theorem

Let us start with a rather technical but fundamental lemma.

**Lemma 5.2.3.1** (Artin-Rees) *Let  $I$  be an ideal of a Noetherian ring  $R$  and  $N$  a submodule of a finitely generated module  $M$ . Then, for every  $n \geq 0$ , there exists  $m \geq 0$  such that  $I^m M \cap N \subseteq I^n N$ .*

*Proof.* The  $R$ -module

$$R(I) := \bigoplus_{n \geq 0} I^n T^n \subseteq R[T]$$

is a subring of  $R[T]$  (the Rees' ring). Choosing generators  $x_i, \dots, x_d$  of  $I$  defines an  $R$ -algebra surjective morphism  $R[T_1, \dots, T_d, T] \rightarrow R(I)$  sending any  $(T_i, T)$  to  $(x_i, T)$ . By 5.2.2.1, the Rees' ring is a Noetherian ring as a quotient of a Noetherian ring. As we did for vector spaces in 3.2.0.2, we can define the  $M[T]$  as the  $R$ -module of formal polynomials with coefficients in  $M$  with its natural  $R(I)$ -module. Let  $M(I) \supset M$  be the submodule

$$M(I) = \bigoplus_{n \geq 0} I^n M T^n \subseteq M[T]$$

Any family of generators of  $M$  generates  $M(I)$  hence  $M(I)$  is of finite type as its submodule

$$\bigoplus_{n \geq 0} (N \cap I^n M) T^n$$

Let us choose a finite number of its generators of the form  $\nu_n T^{d_n}$  with  $\nu_n \in N \cap I^{d_n} M$ . Assuming  $m \geq n + \max(d_j)$ , for any  $\nu \in N \cap I^m M$  there exists  $x_j \in I^{m-d_j} \in I^{m-D}$  such that

$$\nu T^m = \sum x_j \nu_j T^m = \sum (x_j T^{m-d_j}) \cdot (\nu_j T^{d_j}) \in I^n N T^m$$

□

**Corollary 5.2.3.2 (Krull)** *With the above notations, if  $N = \bigcap_{d \geq 1} I^d M$ , then  $IN = N$ . In particular, if  $I$  is contained in the intersection of all maximal ideals<sup>2</sup> of  $R$ , then  $N = 0$ .*

*Proof.* By Artin-Rees lemma, there exists  $m \geq 0$  such that  $I^m M \cap N \subset IN$  and therefore  $N \subset IN$  because  $N = \bigcap_{d \geq 1} I^d M \subseteq I^m M$  hence  $N = IN$ . By Nakayama's lemma, there exists  $i \in I$  such that  $(1+i)N = \{0\}$  but  $1+i$  is invertible because any non invertible element belongs to some maximal ideal by Krull's lemma (1.3.2.4). □

Proof of Theorem 4.1. Of course, we only need to show that  $N \subseteq IN$ . We apply the lemma for the submodule  $N$  of  $M$  to get a non-negative integer  $m$  such that  $I^m M \cap N \subseteq IN$ . However, since  $N \subseteq I^m M$ , this implies  $N \subseteq IN$ . The last assertion in the theorem is a consequence of Nakayama's lemma.

### 5.3 Exercises

**Exercise 5.3.1** *Let  $k \in \mathbf{N} \cup \infty$  and  $R = C^k(\mathbf{R}, \mathbf{R})$ .*

1. *Show there exists a unique  $f_n \in R$  such that  $f_n(x) = \exp(-2^{-n}x^{-2})$  for all  $x \neq 0$ .*
2. *Prove that the sequence of ideals  $(f_n)$  is strictly increasing.*
3. *Prove that  $R$  is not Noetherian.*

---

<sup>2</sup>This intersection is called the Jacobson's radical.

4. Give another proof using 5.2.3.2.

**Exercise 5.3.2** A germ of function is an equivalence of real functions of class  $C^k$ ,  $k \in \mathbf{N} \cup \{\infty\}$  which are defined in some neighborhood of  $0 \in \mathbf{R}^n$  where two such functions are equivalent if they coincide in some neighborhood of

0. Let  $R$  be the set of such germs and  $\mathfrak{m}$  be the set of germs vanishing at 0

1. Check that ordinary addition and products of functions make  $R$  a  $\mathbf{R}$ -algebra.
2. Show that  $R$  is not a domain.
3. Show that  $\mathfrak{m}$  is the unique maximal ideal of  $R$ . What are the invertible elements of  $R$ .
4. Show that  ${}^n \rightarrow M$  is onto if and only if  $(R/\mathfrak{m})^n \rightarrow M/\mathfrak{m}M$  is onto (look at the cokernel and use Nakayama's lemma).
5. If  $k = 0$ , show  $\mathfrak{m} = \mathfrak{m}^2$ . Deduce that  $\mathfrak{m}$  is non Noetherian (use Nakayama's lemma).
6. If  $k \in \mathbf{N}^*$ , show that  $\mathfrak{m}/\mathfrak{m}^2$  is a  $\mathbf{R}$ -vector space of infinite dimension. Deduce that  $\mathfrak{m}$  is non Noetherian (use Nakayama's lemma).
7. If  $k = \infty$ , prove that  $\dim_{\mathbf{R}} \mathfrak{m}/\mathfrak{m}^2 = n$ . Could you prove that  $R$  is non Noetherian?

**Exercise 5.3.3**

1. Prove that 2 is not invertible in  $\overline{\mathbf{Z}}$ .
2. Prove that the sequence of ideals  $(2^{1/2^n}) \subset \overline{\mathbf{Z}}$  is strictly increasing.
3. Conclude.

**Exercise 5.3.4** Let  $R$  be the ring of holomorphic functions on  $\mathbf{C}$ .

1. Prove that  $R$  is a domain.
2. Prove that for any  $n \geq 0$  there exists a unique  $f_n \in R$ , such that  $f_n(z) \prod_{k=0}^n (z - k) = \sin(\pi z)$ .
3. Compute  $f_n(k)$  for  $k \in \mathbf{Z}$ .
4. Prove that  $R$  is not Noetherian (see 9.6.9 and 9.6.10 for other properties of  $R$ ).

**Exercise 5.3.5** Let  $G$  be a finite group operating (on the left) on a ring  $R$ . Assume that the cardinality  $n$  of  $G$  is invertible in  $R$  and denote  $R^G$  the subring of  $R$  of elements invariant by  $G$ . Denote  $\pi : R \rightarrow R$  the application  $x \mapsto \frac{1}{n} \sum_{g \in G} gx$ .

1. Show that  $p$  is a projector of image  $R^G$ .
2. Show that  $p$  is  $R^G$ -linear.
3. Show that if  $R$  is Noetherian, then  $R^G$  is Noetherian.

**Exercise 5.3.6** Let  $M$  be a non zero finite type module of a Noetherian ring  $R$ .

1. Prove that there exists  $m \in M - \{0\}$  such that  $\text{Ann}_R(m)$  is a prime ideal  $\mathfrak{p}$  of  $M$ .
2. Prove that there exists a module injection  $A/\mathfrak{p} \hookrightarrow M$ .

**Exercise 5.3.7** Let  $R$  be any ring and  $A \in M_{m,n}(R)$ .

1. Prove Krull's theorem for Noetherian ring without the axiom of choice.
2. Prove that  $R$  is injective (resp. surjective) if and only if there exists a subring  $R_0$  of  $A$  such that  $A \in M_{m,n}(R_0)$  and the associate morphism  $A_0 : R_0^n \rightarrow R_0^m$  defined by  $A$  has the same property.
3. Give another proof of (2) and (4) of 2.2.0.1.
4. Using 5.3.6, give another proof of (3) and (4) of 2.2.0.1.



## Chapter 6

# Matrix and modules over PID



### 6.1 Introduction



#### Perspective

As explained in 5.2.1.3, the equivalence of matrices is deeply connected with the structure of modules. We will show how this remark leads to general and non-trivial results such as the structure theorem for finite type abelian groups (6.4.0.2) or, more generally, for finite-type modules over PID (6.4.0.1).

We study the equivalence relation  $\sim$  on  $M_{p,q}(R)$  for a PID  $R$  (the reader specifically interested in applications to abelian groups or similarity of matrices over fields (see chapter 8) may restrict to the Euclidean rings  $R = \mathbf{Z}$  or  $R = \mathbf{k}[T]$ ). If  $R$  is Euclidean, we will prove that the equivalence relation  $\sim$  of matrices coincides with the Gauss equivalence  $\equiv$  and give an efficient algorithm to handle this problem in this case. Specifically, we address two questions.

1. Describe the *quotient set*  $M_{p,q}(R)/\sim$  by giving a canonical representative in each similarity class. This is achieved in 6.3.1.2 (3).
2. Describe the quotient map  $M_{p,q}(R) \rightarrow M_{p,q}(R)/\sim$  by giving an algorithmic way to decide when  $A \sim B$ . This is achieved in 6.3.1.2 (1).

We have added a “cultural” chapter 6.6 giving some hints about advanced results that explain the deep and subtle differences between these two equivalence relations that already arise in this “simple” case of PID.

## 6.2 Survival kit for PID and Euclidean rings



Euclide by Raphael

As usual, for  $x \neq 0, y$  elements an integral ring  $R$ , we say that  $x|y$  if and only there exists  $z \in R$  such that  $y = xz$ . We write  $x|y$ . Recall that a principal ideal domain (PID) is an integral domain whose ideals can be generated by a single element. The usual examples of PIDs are fields, the ring of integers  $\mathbf{Z}$  or the rings of polynomials with field coefficients  $\mathbf{k}[T]$ . Their common pattern is the existence of an Euclidean division.

**Definition 6.2.0.1** *An integral ring  $R$  is said Euclidean if there exists a function  $\delta : R^* \rightarrow \mathbf{N}$  such that for any  $(a, b) \in R \times R^*$  there exists<sup>1</sup>  $q, r \in R$  such that  $a = bq + r$  and  $r = 0$  or  $f(r) < f(b)$ .*

**Lemma 6.2.0.2** *An Euclidean ring is a principal ideal domain.*

*Proof.* Let  $I$  be a non zero ideal of an Euclidean ring  $R$ . One can choose a nonzero  $b \in I$  such that  $f(b)$  is minimal in  $f(I - \{0\})$  (which is a nonempty subset of  $\mathbf{N}$ ). Certainly,  $(b) \subset I$ . Let  $a \in I$  and write  $a = bq + r$  with  $r = 0$  or  $f(r) < f(b)$ . Then,  $r = a - bq \in I$ . By minimality of  $f(b)$ , one has  $r = 0$  and  $I \subset (b)$ .  $\square$

<sup>1</sup>We do not require the uniqueness of  $(q, r)$ .

**Definition 6.2.0.3** Let  $(x_i)$  be a family of elements of an integral ring  $R$  and assume at least one of them is nonzero. We say that  $d \in R$  is a greatest common divisor of  $(x_i)$  if  $d$  divides all the  $x_i$ s and if  $d|x_i$  for all  $i$  implies  $d'|d$ . We write  $d = \text{GCD}(x_i)$ .

A GCD, when it exists, is unique up to multiplication by  $u \in R^\times$  (**exercise**): strictly speaking, the GCD is an element of the so called monoid<sup>2</sup>. All the equalities below involving GCD should be seen as equalities in this monoid in which the cautious reader will probably prefer to work.

**Proposition 6.2.0.4** (Bézout's theorem) Let  $(x_i)$  be a family of elements of an principal ring  $R$  and assume at least one of them is nonzero. Then, any generator of the ideal  $(x_i)$  generated by the  $x_i$ 's is a GCD of  $(x_i)$ . In particular, 1 is a GCD of the family  $(x_i)$  if and only if there exists an almost zero family  $y_i \in R$  such that  $\sum y_i x_i = 1$ . We say in this case that the  $x_i$ 's are (globally) coprime.

*Proof.* Let  $d$  such a generator of the ideal  $I$  generated by  $(x_i)$ . Its is  $\neq 0$  because at least one of the  $x_i$  is nonzero and therefore so is  $I$ . Because  $x_i \in I = (d)$ , we get  $d|x_i$ . Conversely, assume that  $d'|x_i$  for all  $i$ , i.e. there exists  $y_i|x_i = y_i d'$ . Because  $d$  belongs to  $I$ , one can write  $d = \sum_{finite} z_i x_i = d' \sum_{finite} z_i y_i$  hence  $d'|d$  and  $d = \text{GCD}(x_i)$ .

In particular,  $1 = \text{GCD}(x_i)$  implies the Bézout property: there exists a almost zero family  $y_i \in R$  such that  $\sum y_i x_i = 1$ . Conversely, if we have such a relation, we get  $1 \in I$  and therefore  $I = R = R \cdot 1$ .  $\square$

**Proposition 6.2.0.5** (Gauss lemma) Let  $R$  be a PID and  $a, b, c \in R^*$ . If  $\text{GCD}(a, b) = 1$  and  $a|bc$  then  $a|c$ .

*Proof.* Write a Bézout identity  $1 = au + bv$  and, multiplying by  $c$  we get  $c = au + bcv$ , which is a sum of two terms divisible by  $c$ .  $\square$

## 6.3 Matrix equivalence in PID and Euclidean rings

### 6.3.1 Invariant ideals of a matrix

In this section,

$R$  is a PID,  $A = [a_{i,j}] \in M_{p,q}(R)$  is a matrix and  $\nu = \min(p, q)$ .

Let us adapt Gauss elimination method 2.3.2.1 to prove the following proposition. We will need more than Gauss elementary operations in this case.

<sup>2</sup>The product on  $R^*$  induces an associative product of unit on  $R^*/R^\times$  (this kind of structure is called a monoid).

**Definition 6.3.1.1** Two matrices are Bézout equivalent if they differ by a series of left and right multiplications by transvections  $T_{i,j}(x)$ ,  $x \in R$  and matrices of the form  $\text{diag}(A, \text{Id})$  with  $A \in \text{SL}_2(\mathbf{R})$  (we call them Bézout matrices). We denote by  $\simeq$  the Bézout equivalence of matrices and by  $\omega(A)$  the corresponding equivalence class of  $A$ .

By construction, we have

$$\text{Gauss equivalence} \equiv \Rightarrow \text{Bézout equivalence} \simeq \Rightarrow \text{equivalence } \sim$$

The main observation is

$$\boxed{\text{If } d \text{ is a GCD of } (a, b) \in R^2 - \{0\}, \text{ we have } (a, b) \simeq (d, 0).}$$

Indeed, by Bézout theorem, there exists  $u, v \in R \mid au + bv = d$  and therefore

$$(a, b) \begin{pmatrix} u & b/d \\ v & -a/d \end{pmatrix} = (d, 0).$$

We say that  $A' = [a'_{i,j}] \in \omega(A)$  is extremal if one of its coefficient is maximal in the (nonempty) set of ideals  $\mathcal{F} = \{(a'_{i,j}), A' \in \omega(A)\}$ , the corresponding coefficient  $a'_{i,j}$  being called an extremal coefficient.

### Theorem 6.3.1.2

1.  $A$  is Bézout equivalent to a diagonal matrix  $\text{diag}(d_\nu, \dots, d_1)$  with  $(d_1) \subset \dots \subset (d_\nu)$ .

2.  $\text{Coker}(A) \xrightarrow{\sim} \bigoplus_{j=1}^n R/I_j$  where  $(I_j)_{1 \leq j \leq n}$  is the increasing sequence

$$I_j = (0) \text{ for } j = 1, \dots, n - \nu \text{ and } I_{j+n-\nu} = (d_j) \text{ for } j = 1, \dots, \nu$$

3. The Fitting ideals of  $\Phi_i(\text{Coker}(A))$ ,  $i \geq 0$  are equal to  $I_n \dots I_{i+1}$  and therefore to  $(d_\nu \dots d_{\nu-i+1})$  for  $0 \leq i \leq \nu - 1$  and to  $R$  if  $i > \nu$ .

4. The ideals  $I_j$  depend only on the equivalence class of  $A$ . They are called the invariant ideals<sup>3</sup> of  $A$ .

5. Two matrices are equivalent if and only if they have the same invariant ideals.

6.  $A \in \text{GL}_n(R)$  is Bézout equivalent to  $\text{diag}(\det(A), 1, \dots, 1)$ .

*Proof.*

<sup>3</sup>By a slight language abuse, one says often that the  $d_i$ 's are the invariant factor of the matrix, even they are defined up to multiplication by an invertible element.

1. We use induction on  $p + q$  starting with the obvious case  $p + q = 2$ . We can assume  $A \neq 0$ 
  - Transposing if necessary, one can assume  $q \leq p = \nu \geq 1$ . Recall that the ideal  $\wedge^1(A) \wedge^1(A)$  generated by the coefficients of  $A$  is invariant by matrix equivalence (3.8.1.2).
  - Assume first  $p = 1$  ( $A$  is a line matrix). I claim that  $A \simeq (d, 0, \dots, 0)$  with  $\wedge^1(A) = (d)$ . This is true if  $q = 1$  and, using the invariance of  $\wedge^1(A)$  by equivalence, is reduced by an immediate induction to the  $q = 2$  case which we already know to be true. By a transpose argument, this shows that we can replace a line or a column by a line or a column with all their coefficients being zero except the first one: we refer to that as Bézout replacement. So we are done if either  $p = 1$  or  $q = 1$ .
  - Assume now  $p, q > 1$ . One can assume that  $A$  is extremal with some  $a_{i,j}$  an extremal coefficient. By Bézout replacement,  $A$  is equivalent to  $A'$  with  $a'_{1,1} = a_{i,j}$ . Because  $(a'_{1,1}) = (a_{i,j})$  is maximal in  $\mathcal{F}$ ,  $A'$  is still extremal. One can therefore assume that  $d_\nu = a_{1,1}$  is extremal and  $d_\nu \neq 0$  because  $A \neq 0$ .  
If  $a_{1,j}, j > 1$  is not divisible by  $a_{1,1}$ , then  $(d_\nu)$  is strictly contained in  $(\wedge^1(d_\nu, a_{1,j}))$ . But using Bézout replacement, this contradicts the maximality of  $(d_\nu)$ .  
Therefore,  $d_\nu | a_{1,j}$  and (same argument  $d_\nu | a_{i,1}$  for all  $i, j$ ). By using usual Gauss operations, one can assume that  $a_{1,j} = a_{i,1} = 0$  for all  $i, j > 1$ , without losing extremality as before.
  - I claim that in this situation  $d_\nu | a_{i,j}$ . If  $i > 1$  say, the change  $L_1 \mapsto L_1 + L_i$  changes  $L_1$  to  $(d_\nu, 0, \dots, 0, a_{i,j}, 0, \dots, 0)$  and therefore  $d_\nu | a_{i,j}$  by the preceding Bézout replacement argument. The matrix  $A$  is therefore of the form  $d_\nu \text{diag}(1, \bar{A})$  with  $\bar{A} \in M_{p-1, q-1}(R)$  and we conclude by induction.
2. This is the functoriality of the cokernel and the computation of the cokernel in the diagonal case (3.8.0.1).
3. Direct consequences of the calculations of the Fitting ideals of a direct sum (3.8.2.6).
4. The number  $N$  of indices such that  $d_i = 0$  is the largest  $i \geq 0$  such that  $\Phi_i(\text{Coker}(A)) = (0)$  showing that independance of the number  $\rho = p - \nu + N$  of zero ideals  $I_i$ . For the others, observe that the sequence of product  $d_j \dots d_1$  determines the  $d_i, i \leq j$  provided  $d_i \neq 0$  because  $R$  is an integral domain.
5. The direct implication is (4). Conversely, if  $I_j$  are the invariant ideals of  $A, A' \in M_{p,q}(R)$ , by (1) and (4) they are Bézout equivalent to diagonal matrices  $\text{diag}(d_j), \text{diag}(d'_j)$  with  $(d_j) = (d'_j)$ . Writing  $d'_j = u_j d_j, u_j \in R^\times$ , we get  $\text{diag}(d'_j) = D \text{diag}(d_j)$  with a diagonal invertible matrix  $D$  hence the equivalence.
6. Direct consequence of (1) and 2.3.1.1.

□

**Remark(s) 6.3.1.3** The matrix  $\text{diag}(d_\nu, \dots, d_1)$  with  $(d_1) \subset \dots \subset (d_\nu) \in M_{p,q}(\mathbb{R})$  in (1) is sometimes called the Smith's normal form  $A$ .

## 6.4 Invariant factors of a module

Let us reap the benefits of our labor.

**Theorem 6.4.0.1** (Structure theorem of finite type modules over PID) *Let  $M$  be a finite type module over a PID  $R$ .*

1. Every submodule of  $M$  is of finite type.
2. There exists an exact sequence  $R^m \xrightarrow{A} R^n \rightarrow M \rightarrow 0$  and  $M \xrightarrow{\sim} \bigoplus R/I_j$  where  $(I_j)$  is the sequence of proper invariant ideals of  $A$ .
3. The Fitting ideals  $\Phi_i(M)$ ,  $i \geq 0$  are equal to  $I_n \dots I_{i+1}$ .
4. The proper invariant ideals of  $A$  does depend only on  $M$ : they are called the invariant factors of  $M$ .
5.  $M$  is (non canonically) isomorphic to  $M_{tors} \oplus R^r$  with  $r = \text{rank}(M) = \text{Card}\{j | I_j = (0)\}$  and

$$M_{tors} \xrightarrow{\sim} \bigoplus_{j > r} R/I_j = \bigoplus_{I_j \neq (0), R} R/I_j$$

6.  $M$  is free if and only if  $M$  has no torsion.
7. Every submodule  $N$  of a rank  $n$  free module  $M$  is free of rank  $r \leq n$ . Moreover, there exists a basis  $e_1, \dots, e_n$  of  $M$  and  $0 \neq d_r | \dots | d_1$  such that  $(d_i e_i)_{1 \leq i \leq r}$  is a (so called adapted) basis of  $N$ .

*Proof.* Let us explain why it is a reformulation of (6.3.1.2).

1.  $R$  is Noetherian and so is  $M$  (5.2.1.2).
2. The existence of the exact sequence is (5.2.1.3) and the remaining part is (6.3.1.2) taking into account account that  $R/I_j = \{0\}$  if  $I_j$  is not proper.
3. Cf. (6.3.1.2).
4. Cf. (6.3.1.2).
5. Direct consequence (2).
6. Direct consequence of the previous item and of 2.2.0.1.

7. By choosing basis of  $M$  and  $N$ , the inclusion  $N \rightarrow M$  becomes  $R^r \xrightarrow{A} R^n$  with  $A \in M_{n,r}(R)$  an injective matrix. Therefore, there exists  $D$  diagonal and  $P, Q$  invertible with  $A = PDQ$  (6.3.1.2). Then,  $N = PDQ(R^r) = PD(R^r)$  and we set  $e_j = (P_{i,j})_i$  the  $j$ -th column of  $P \in GL_n(R)$  and  $d_i = D_{i,i}$  for  $D_{i,i} \neq 0$ .

□

**Corollary 6.4.0.2** (Structure theorem of finite type abelian groups) *Let  $G$  be a finite type abelian group.*

1. *There exists a unique sequence of integers  $2 \leq d_n | \dots | d_1$  and  $r \geq 0$  such that  $G \xrightarrow{\sim} \bigoplus_i \mathbf{Z}/d_i \mathbf{Z} \oplus \mathbf{Z}^r$ .*
2. *If  $G$  is a subgroup of the multiplicative group  $\mathbf{k}^*$  of a field<sup>4</sup>, then  $G$  is cyclic.*

*Proof.* 1. Set  $M = G$  and  $R = \mathbf{Z}$  in the previous structure theorem.

2. Because  $G$  is finite, we can by (1) choose an isomorphism  $\varphi : G \xrightarrow{\sim} H = \bigoplus_i \mathbf{Z}/d_i$  with  $2 \leq d_n | \dots | d_1$ . It maps  $\Gamma = \{g \in G | g^{d_1} = 1\}$  isomorphically to  $\{h \in H | d_1 h = 0\}$  the latter group being equal to the whole  $H$ . In particular,  $\text{Card}(\Gamma) = d_1 \dots d_r$ . But  $T^{d_1} - 1$  has at most  $d_1$  roots in  $\mathbf{k}$  giving  $d_1 \dots d_r \leq d_1$  and therefore  $r = 1$ .

□

### 6.4.1 The Euclidean case

**Proposition 6.4.1.1** *Assume  $R$  is Euclidean. Then Bézout equivalence  $\Leftrightarrow$  Gauss equivalence*

*Proof.* Let  $L = (a_0, a_1) \in R \times R^*$  and  $a_0 = a_1 q_0 + a_2$  with  $f(a_2) < f(a_1)$  or  $a_2 = 0$ . Using the Gauss operation  $a_0 \mapsto a_0 - q_0 a_1$ , we get  $(a_0, a_1) \equiv (a_1, a_2)$  and we know  $\text{GCD}(a_0, a_1) \equiv \text{GCD}(a_1, a_2)$ . By induction, we construct  $a_i$  such that  $(a_i, a_i + 1) \equiv (a_{i+1}, a_{i+2})$  with  $\text{GCD}(a_i, a_i + 1) \equiv \text{GCD}(a_{i+1}, a_{i+2})$  and  $f(a_i)$  strictly decreasing until  $a_{i+1} = 0$  where in this case  $a_{i+1} = \text{GCD}(a_0, a_2)$ . It follows that for any  $a, b$ , one has  $(a, b) \equiv (\text{GCD}(a, b), 0)$ .

If know  $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is a Bézout matrix, it follows that  $B \equiv \begin{pmatrix} \text{GCD}(a, b) & 0 \\ \gamma & \delta \end{pmatrix}$  with  $\text{GCD}(a, b)\delta = 1$  because  $\det(B) = 1$ . By a Gauss operation, because  $\delta$  is invertible one can further assume  $\gamma = 0$  and we have  $B \equiv \text{diag}(\delta, \delta^{-1})$  and therefore  $B \equiv \text{Id}_2$  thanks to the previous lemma. Therefore, any Bézout operation is a Gauss operation. □

<sup>4</sup>or even of  $G \subset R^\times$  where  $R$  is an integral domain.

In particular, this shows that deciding whether two matrices with coefficients in an Euclidean ring are equivalent or not is an algorithmic question because the finer Gauss equivalence problem is.

**Corollary 6.4.1.2** *If  $R$  is Euclidean, every invertible matrix  $A \in \text{GL}_n(R)$  is Gauss equivalent to  $(\det(A), \text{Id}_{n-1})$ .*

*Proof.* If  $A$  is invertible, we know (6.3.1.2) that their invariant factors are equal to 1 proving that  $A$  is Gauss equivalent to an invertible diagonal matrix and we apply lemma 2.3.1.1. In particular,  $\text{SL}_n(R)$  is generated by transvections.  $\square$

## 6.5 About uniqueness of invariant ideals

This section can be skipped on a first reading, not because it is difficult, but because the results are more or less cultural than useful. In the PID situation we have seen that every module of finite type  $M$  is isomorphic to a direct sum  $\bigoplus_{i=1}^n M_i$  with  $\text{Ann}_R(M_1) \subset \text{Ann}_R(M_2) \subset \cdots \subset \text{Ann}_R(M_n)$ . In other words,  $M$  is isomorphic to  $\bigoplus_{i=1}^n R/I_i$ , where  $I_1 \subset I_2 \subset \cdots \subset I_n$  is an increasing sequence of proper ideals depending only on  $M$ . In general, there are many modules that do not have this form. But in the case where such a decomposition exists, let us show that the ideals are uniquely defined as in the PID case<sup>5</sup>. Assume therefore that  $M$  has such a decomposition but that  $R$  is no longer assumed to be a PID.

**Lemma 6.5.0.1** *Let Then*

1. *The minimal number of generators of  $M$  is  $n$ .*
2. *For  $k = 1, \dots, n$ , the ideal  $I_k$  is equal to the set of all  $x \in R$  such that  $xM$  can be generated by fewer than  $k$  elements.*

We say in this situation that the  $(I_k)$  as the invariant factor sequence of  $M$  (which generalize the PID terminology).

*Proof.*

1.  $M$  is a quotient of  $R^n$  and has therefore a generating set consisting of  $n$  elements. Conversely, if we have a generating family of  $d$  elements, we get a surjection  $R^d \mapsto \bigoplus R/I_k \rightarrow \bigoplus (R/I_n)^n$  which factors through a surjection  $(R/I_n)^d \rightarrow (R/I_n)^n$  implying  $d \geq n$  by 2.2.0.1.
2. Let  $x \in R$ , and let  $k \leq n$ . For any ideal  $I$  of  $R$ , let  $I_x = \{y \in R \mid xy \in I\}$ . By construction, the ideal  $I_x = R$  if and only if  $x \in I$ . The multiplication by  $x$  defines an isomorphism  $xM \cong \bigoplus_{k=1}^{n(x)} R/(I_k)_x$  where  $n(x)$  is the largest  $k$  such  $(I_k)_x \neq R$ . Because  $(I_k)_x$  is increasing, one can apply (1) to  $xM$  and

<sup>5</sup>With this generality, I learned this nice argument from <https://math.stackexchange.com/q/3147043>.

therefore  $xM$  can be generated by fewer than  $k$  elements if and only if the  $k$ -th factor  $R/(I_k)_x$  is zero *i.e.* when  $x \in I_k$ .

□

**Remark(s) 6.5.0.2**

- We recover the fact that  $R^n$  and  $R^m$  are isomorphic if and only if  $n = m$ .
- One could hope that Fitting ideals would give the result as in the PID case. This is not the case (cf. exercise 6.7.14).

## 6.6 Supplementary Section: Insight into K-Theory



This section is cultural and can be skipped at first sight. Its purpose is to introduce an important idea in mathematics: how to measure the obstacle to a result being true. Here the question is how to measure the potential impossibility of *diagonalising* matrices by Gaussian elimination in a ring  $R$ .

The precise question that naturally arises is: is the group  $GL_n(R)$  generated by the elementary matrices of pivot type transvections (1.2)? We will consider the matrices of permutations and dilatations (because they can be easily handled by the determinant function below).

The first step is to move away from  $n$ : to do this, we consider  $GL_n(R)$  as the subgroup of  $GL_{n+1}(R)$  consisting of block diagonal matrices of the form  $\text{diag}(M, 1)$ , where  $M \in GL_n(R)$ . This allows us to consider their infinite union  $GL(R)$ , seen as the set of matrices of infinite size containing all linear groups of finite size. We then define  $E(R) = \cup E_n(R)$  as the subgroup of  $GL(R)$  generated by all transvections (cf. 2.3), *i.e.* the determinant 1 matrices which we can obtain by Gauss elimination (even if we allow the matrices to grow).

The first result is both simple and remarkable, especially in the proof given by [17].

**Lemma 6.6.0.1** (Whitehead) *For any ring  $R$ , the group  $E(R)$  is the derived group  $[GL(R), GL(R)]$  generated by the commutators  $[A, B] = ABA^{-1}B^{-1}$  of matrices in  $GL(R)$ .*

In particular,  $E(R)$  is a normal subgroup, and the quotient  $K_1(R) = GL(R)/[GL(R), GL(R)]$  is a commutative group, as it is the abelianization of  $GL(R)$ ! This is the group of algebraic K-theory of degree 1. As

the determinant of any commutator is 1, the determinant map passes to the quotient (4.2) to define the special group of algebraic K-theory of degree 1:

$$\mathrm{SK}_1(\mathbf{R}) = \mathrm{Ker}(\mathrm{GL}(\mathbf{R}) \xrightarrow{\det} \mathbf{R}^\times).$$

This group avoids considering dilations and permutation matrices, which do not play a crucial role in pivoting. The inclusion  $\mathbf{R}^\times = \mathrm{GL}_1(\mathbf{R}) \hookrightarrow \mathrm{GL}(\mathbf{R})$  followed by the quotient projection  $\mathrm{GL}(\mathbf{R}) \twoheadrightarrow \mathrm{K}_1(\mathbf{R})$  allows us to define a map:

$$\mathbf{R}^\times \times \mathrm{SK}_1(\mathbf{R}) \rightarrow \mathrm{K}_1(\mathbf{R}),$$

which is visibly an isomorphism.

**Remark(s) 6.6.0.2** *This result is far from being banal. Precisely,  $\mathrm{E}_2(\mathbf{R})$  is not normal in  $\mathrm{GL}_2(\mathbf{R})$  for  $\mathbf{R} = \mathbf{k}[T_1, T_2]$ . Precisely, the matrix  $A = \begin{pmatrix} 1 + T_1 T_2 & T_1^2 \\ -T_2^2 & 1 - T_1 T_2 \end{pmatrix} \notin \mathrm{E}_2(\mathbf{k}[T_1, T_2])$  and one can show that  $\mathrm{AM}_{(1,2)} A^{-1} \notin \mathrm{E}_2(\mathbf{R})$ . More surprising, if  $\mathbf{R} = \mathbf{Z}[1/2 + \theta]$  with  $\theta = \sqrt{-19}/2$ , Cohn (op. cit.) has shown that  $A = \begin{pmatrix} 3 - \theta & 2 + \theta \\ -3 - 2\theta & 5 - 2\theta \end{pmatrix} \notin \mathrm{E}_2(\mathbf{R})$  and again  $\mathrm{AM}_{(1,2)} A^{-1} \notin \mathrm{E}_2(\mathbf{R})$  (Lam, op. cit.). And we know that  $\mathbf{R}$  is a PID (6.7.5)! On the other hand, Suslin has shown that  $\mathrm{E}_n(\mathbf{k}[T_1, \dots, T_m])$  is normal in  $\mathrm{GL}_n(\mathbf{k}[T_1, \dots, T_m])$  for  $n > 2$  and any  $m$ . These deep results are far from being easy (cf. T. Y. Lam, Serre's problem on projective modules, Springer Monographs in Mathematics, Springer, Berlin, 2006, §1.8).*

The group  $\mathrm{SK}_1(\mathbf{R})$  is obviously the obstacle to the Gauss elimination algorithm (infinite) being able to diagonalise matrices. And our results prove that if  $\mathbf{R}$  is Euclidean, then  $\mathrm{SK}_1(\mathbf{R}) = 0$ . It is worth noting that this obstacle is very sudden. For example, in the case of the non-Euclidean principal ring  $\mathbf{R} = \mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$ , we have  $\mathrm{SK}_1(\mathbf{R}) = \{1\}$  (this follows from a general deep theorem about so-called Dedekind rings, [2]). In other words, this is not an example where the pivot with elementary matrices is insufficient, at least if one allows to increase the size of the matrices. Finding a principal  $\mathbf{R}$  such that  $\mathrm{SK}_1(\mathbf{R})$  is non-trivial is difficult. An example is given in [12]: take the subring of  $\mathbf{Z}(\mathbf{T})$  generated by  $\mathbf{Z}[\mathbf{T}]$  and the  $(\mathbf{T}^m - 1)^{-1}$  for  $m \geq 1$ . This is a principal ring (!) whose  $\mathrm{SK}_1$  is even infinite.

## 6.7 Exercises

### Exercise 6.7.1

1. Show that  $\mathbf{R} = \mathbf{Z}[i] \subset \mathbf{C}$  is Euclidean (for  $(a, b) \in \mathbf{R} \times \mathbf{R}^*$  with  $a/b = x + iy$ ,  $x, y \in \mathbf{R}$ , define  $q = [x] + i[y]$  and  $f(z) = |z|$ ).
2. Show that  $\mathbf{R} = \mathbf{Z}[j] \subset \mathbf{C}$  is Euclidean with  $j = \exp(\frac{2i\pi}{3})$  (for  $(a, b) \in \mathbf{R} \times \mathbf{R}^*$  with  $a/b = x + yj$ ,  $x, y \in \mathbf{R}$ , define  $q = [x + 1/2] + j[y + 1/2]$  and  $f(z) = |z|$ ).

**Exercise 6.7.2** Prove that  $\mathbf{R}[T]$  is a PID if and only if  $\mathbf{R}$  is a field.

**Exercise 6.7.3** Let  $\mathbf{R}$  be an integral domain with fraction field  $\mathbf{K}$ . Prove that the  $\mathbf{R}$ -module  $\mathbf{K}$  is free if and only if  $\mathbf{R}$  is a field and therefore if and only if  $\mathbf{R} = \mathbf{K}$ . Deduce that if  $\mathbf{R}$  is a PID,  $\mathbf{K}$  is torsion free but not free as a  $\mathbf{R}$ -module.

**Exercise 6.7.4** Let  $\mathbf{R}$  be a Euclidean ring. Show that there exists  $x \in \mathbf{R} \setminus \mathbf{R}^*$  such that the restriction of the natural surjection  $\pi : \mathbf{R} \rightarrow \mathbf{R}/(x)$  to  $\mathbf{R}^* \cup \{0\}$  is surjective. Show that then  $\mathbf{R}/(x)$  is a field.

**Exercise 6.7.5** Let  $\mathbf{R} = \mathbf{Z} \left[ \frac{1+i\sqrt{19}}{2} \right] = \mathbf{Z}[\alpha] \subset \mathbf{C}$ .

1. Check that  $\mathbf{R}$  is an integral ring isomorphic to  $\mathbf{Z}[T]/(T^2 - T + 5)$ .
2. Prove that  $(2)$  is a maximal ideal of  $\mathbf{R}$ .
3. Prove that  $\mathbf{R}^\times = \{\pm 1\}$  (look at the square  $N(z) = |z|^2$  of the module of an invertible element  $z \in \mathbf{R}^\times$ ).
4. Deduce from the preceding exercise that  $\mathbf{R}$  is not Euclidean.
5. Assume that for all  $a, b \in \mathbf{R} \setminus \{0\}$ , there exist  $q, r \in \mathbf{A}$  such that  $N(r) < N(b)$  and

$$a = bq + r \quad \text{or} \quad 2a = bq + r.$$

6. Prove that this implies that  $\mathbf{R}$  is a PID.
7. Let  $a, b \in \mathbf{R} \setminus \{0\}$ . Prove that  $x$  can be written  $x = u + v\alpha$ , where  $u, v \in \mathbf{Q}$ .
8. Let  $n = [v]$  and assume  $v \notin [n + \frac{1}{3}, n + \frac{2}{3}]$ . Looking at the closest integers to  $u$  and  $v$ , prove that there exists there exist  $q, r \in \mathbf{A}$  such that  $N(r) < N(b)$  and  $a = bq + r$ .
9. Prove that if  $v \in [n + \frac{1}{3}, n + \frac{2}{3}]$ , there exist  $q, r \in \mathbf{A}$  such that  $N(r) < N(b)$  and

$$2a = bq + r$$

10. Conclude that  $\mathbf{R}$  is a PID.

**Exercise 6.7.6** Solve the following systems of equations, with the unknown  $x \in \mathbf{Z}$ :

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

**Exercise 6.7.7** Write a program computing the invariant ideals of a matrix with coefficients in  $\mathbf{Q}[T]$  or  $\mathbf{Z}$ . What can you say about its complexity? About its numerical stability?

**Exercise 6.7.8** Give an algorithm to solve a finite number of linear equations with integral coefficients and test in a suitable computer language like Python.

**Exercise 6.7.9** Transform the proof of 6.4.1.1 into an algorithm and then to a Python program (use SageMath for instance). What can you say about the complexity of this algorithm? About its numerical stability?

**Exercise 6.7.10** Let  $K$  be a nonempty compact connected subset of  $\mathbf{C}$ . We say that two holomorphic functions defined on some open neighborhood of  $K$  are equivalent if they are equal in some neighborhood of  $K$ .

1. Show that the set of equivalence classes  $R$  has a natural structure of ring.
2. Show that  $R$  is an integral domain.
3. Let  $f$  a representative of an element of  $R$ . Show that  $f$  has a finite number of zeroes in  $K$  and that  $f$  is invertible if and only if  $f$  does not vanish on  $K$ .
4. Show that the  $R$  is a PID.

**Exercise 6.7.11** Let  $R$  be ring of complex power series with positive convergence radius. Prove that  $R^\times$  is the set of series not vanishing at zero. Deduce that  $R$  is a PID and is even Euclidean (it is an example of the so called discrete valuation rings).

**Exercise 6.7.12** Let  $K$  be the fraction field of  $R$ . Show that the rank of  $A$  considered as a matrix in  $M_{n,m}(K)$  is equal to  $r = \text{Card}\{j | I_j \neq (0)\}$  and that  $\text{rank}(\text{Coker}(A)) = n - r$ .

**Exercise 6.7.13** Let  $P, Q \in k[T]$  be monic polynomials and  $A = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$ . Compute  $\delta_1(A)$  and  $\delta_2(A)$  and deduce that the invariant ideals of  $A$  are  $\text{GCD}(P, Q)$ ,  $\text{LCM}(P, Q)$ . Retrieve this result using Gauss algorithm. Deduce another algorithm than the Gauss elimination algorithm to compute the invariants ideals of a diagonal matrix in  $M_{p,q}(R)$ .

**Exercise 6.7.14** Let  $R = \mathbf{Q}[T, T_1, T_2]/(T^2(T_1 - T_2))$ . Show that  $M_i = R/(TT_i) \oplus R/(T)$  have the same Fitting ideals but distinct invariant sequences in the sense of 6.5. Can you produce an analogous example with  $R$  an integral domain?

**Exercise 6.7.15** Use 6.7.14 to give an example of non equivalent matrices with the same Fitting ideals.

## **Part II**

# **Linear algebra over fields**



# Chapter 7

## Warm-up II: duality



René Magritte

### 7.1 Introduction



Perspective

Vector subspaces can be either described by generating families or by linear equations. Duality is an important even formal tool formalizing the bridge between these two aspects.

### 7.2 Basic notions

As always,  $V$  denotes in this chapter a finite dimensional<sup>1</sup>  $\mathbf{k}$ -vector space and  $V^* = \text{Hom}(V, \mathbf{k})$  denotes its dual; the vector space of linear maps from  $V$  to  $\mathbf{k}$ , *i.e.* linear forms of  $V$ .

For any  $\varphi \in V^*$ ,  $v \in V$ , we denote  $\langle \varphi, v \rangle = \varphi(v)$  the duality bracket<sup>2</sup>  $V^* \times V \rightarrow \mathbf{k}$ . This bracket is clearly bilinear.

---

<sup>1</sup>Unless otherwise stated.

<sup>2</sup>Be careful, the dual acts to the right on vectors, cf. [5].

A hyperplane is the kernel of a non-zero linear form  $\varphi$ . Conversely, any hyperplane  $H$  determines  $\varphi$  up to multiplication by a non-zero scalar: choosing any  $v \notin H$  defines a direct sum decomposition  $H \oplus \mathbf{k}v = V$  and  $\varphi$  is unambiguously defined by any (nonzero) value of  $v$ .

We recall that any any free family of  $V$  can be completed in a basis of  $V$ . In particular, any proper subspace of  $V$  is contained in some hyperplane and in fact is precisely the intersection of hyperplanes that contain it (cf. 7.3 7.3.0.1).

**Proposition 7.2.0.1** *Let  $V$  be a  $n$ -dimensional vector space and let  $V_i$  finitely many proper vector subspaces. If  $\mathbf{k}$  is infinite or if the number of subspaces is  $\leq 2$ , then  $\cup V_i \neq V$ .*

*Proof.* By the above remark, we can assume that all the  $V_i$ 's are hyperplanes  $\text{Ker}(\varphi_i)$ . Choosing a (finite) basis of  $V$ , these linear forms  $\varphi_i$  are nothing but (homogeneous) degree one polynomial in the coordinates. By assumption  $\prod \varphi_i$  is zero on  $\mathbf{k}^n$  and therefore the polynomial  $\prod \varphi_i(X_1, \dots, X_n)$  is zero in  $\mathbf{k}[X_1, \dots, X_n]$  because  $\mathbf{k}$  is infinite. But a polynomial ring is an integral domain, showing that one the  $\varphi_i$  is zero, a contradiction. If  $\mathbf{k}$  is a finite field (of characteristic  $p \geq 2$ ), the cardinal of  $V$  is  $p^n$ . The union of two hyperplanes has cardinal at worst  $2p^{n-1} - 1 \leq p^n - 1$  (because 0 belongs to bot hyperplanes) and the proposition follows.  $\square$

Let  $\mathcal{B} = (e_i)$  be a (finite) basis of  $\mathcal{B} = (e_i) V$ . We define  $e_i^*$  by the formula

$$\langle e_j, e_i^* \rangle = \delta_{i,j}$$

In other words,  $e_i^*$  is the  $i$ -th coordinate function and we have

$$v = \sum_j \langle v, e_j^* \rangle e_j$$

From this formula we get that  $\mathcal{B}^* = (e_i^*)$  is a basis of  $V^*$  called the *dual basis* of  $\mathcal{B}$ . In particular,  $\dim(V^*) = \dim(V)$ .

If  $V = \mathbf{k}^n = M_{n,1}(\mathbf{k})$  (column vectors), we have  $M_{1,n}(\mathbf{k}) = \mathbf{k}^n = V^*$  (row vectors) and the duality bracket is  $\langle L, C \rangle = L^t C$  where

$$L \in (\mathbf{k}^n)^* \text{ is a row and } C \in \mathbf{k}^n \text{ a column.}$$

If  $\mathcal{B} = (e_j = [\delta_{i,j}]_{1 \leq i \leq n})$  is the canonical basis ( $E_{j,1} = e_j$ ) of  $\mathbf{k}^n = M_{n,1}(\mathbf{k}) = V$ , its dual basis  $\mathcal{B}^*$  is formed from the rows  $e_i^* = {}^t e_i$ , which is the canonical basis ( $E_{1,i} = e_i^*$ ) of  $M_{1,n}(\mathbf{k}) = \mathbf{k}^n = V^*$ .

If  $W$  is a subspace of  $V$  (or even a subset), we recall that its orthogonal is defined by

$$W^\perp = \{\varphi \in V^* | \langle \varphi, w \rangle = 0 \text{ for all } w \in W\} \subset V^*.$$

In concrete terms, the orthogonal of  $W \subset V$  is the set of linear equations satisfied by  $W$ . If now  $W_*$  is a subspace of  $V^*$  (or even a subset) its polar in  $V$  is defined by

$$W_*^\circ = \{v \in V | \langle \varphi, v \rangle = 0 \text{ for all } \varphi \in W_*\} \subset V.$$



If  $\mathcal{B}$  is a basis of an infinite dimensional vector space, the family  $\mathcal{B}^*$  is still free, but never a basis. For example, the linear form  $\varphi$  defined by  $\langle \varphi, e_i \rangle = 1$  for all  $i$  is certainly not in the span of  $\mathcal{B}^*$ . Even as a set,  $\text{Card}(V^*) > \text{Card}(V)$  (**exercise**). In fact, in the infinite dimensional case, the algebraic dual is not the good notion. As the reader who has notion in functional analysis knows, the good notion is an appropriate topological dual of topological vector spaces.

In concrete terms, the polar of  $W_* \subset V^*$  is the set of vectors satisfying all the equations in  $W_*$ .

**Example(s) 7.2.0.2** *An important example comes from differential geometry. If  $f$  is a regular function on an open  $\Omega$  of  $\mathbf{R}^n$ , its differential at  $\omega \in \Omega$  is a linear form on  $T_\omega\Omega = \mathbf{R}^n$ : the differential  $df(\omega)$ . In the canonical basis  $(\frac{d}{dx_i}(\omega))_i$  of  $T_\omega\Omega$ , this form is the Jacobian  $J(\omega) = (\frac{df}{dx_j}(\omega))_j$ , seen as a row matrix. The kernel of  $df(\omega)$  is none other than the tangent hyperplane at  $\omega$  to the hypersurface defined by the equation  $f = 0$ , as long as the differential at that point is not zero. The generalisation to more than one function is contained in the notion of higher dimensional submanifolds.*

### 7.3 Formal biorthogonality

Whether  $V$  is of finite dimension or not, every subspace  $W$  is tautologically contained in the space defined by the set of its equations

$$W \subset (W^\perp)^\circ \subset \{v \mid \langle \varphi, v \rangle = 0 \text{ for all } \varphi \in W^\perp\}.$$

**Lemma 7.3.0.1** *We have*

$$W = (W^\perp)^\circ = \{v \mid \langle \varphi, v \rangle = 0 \text{ for all } \varphi \in W^\perp\}.$$

*no matter what the dimensionality of  $V$  is.*

*Proof.* Indeed, if  $v \notin W$ , one can choose a complement  $S$  of  $W \oplus kv$  in  $W$  and define for example  $\varphi \in W^\perp$  by the conditions  $\langle \varphi, W \rangle = \langle \varphi, S \rangle = \{0\}$  and  $\langle \varphi, v \rangle = 1$  which implies  $v \notin (W^\perp)^\circ$  proving the reverse inclusion. □

### 7.4 Ante-dual basis: biduality

Henceforth, in this chapter,  $V$  is finite-dimensional.

**Proposition 7.4.0.1** *Let  $V$  be of dimension  $n < \infty$ . Then*

1. *The evaluation map*

$$ev : \begin{cases} V & \rightarrow & V^{**} \\ v & \mapsto & (\varphi \mapsto (\langle \varphi, v \rangle)) \end{cases}$$

*is a linear isomorphism.*

2. *For any basis  $\mathcal{B}_*$  of  $V^*$ , there exists a unique basis  $\mathcal{B}$  of  $V$  called ante-dual whose dual is  $\mathcal{B}_*$ , i.e. such that  $\mathcal{B}^* = \mathcal{B}_*$ .*

*Proof.*

1.  $ev$  is injective between spaces of the same finite dimension.
2.  $\mathcal{B} = ev^{-1}((\mathcal{B}_*)^*)$  is the unique solution to the problem posed.

□

**Example(s) 7.4.0.2** *Let  $(\alpha_1, \dots, \alpha_n)$  be  $n$  distinct real numbers. We define for  $i \in [1, n]$  the Lagrange interpolating polynomial*

$$L_i = \prod_{\substack{j=1 \\ j \neq i}}^n \frac{X - \alpha_j}{\alpha_i - \alpha_j}$$

*and define  $\varphi_i : P \mapsto P(\alpha_i)$  as the linear evaluation function at  $\alpha_i$ . We can verify that for all  $i, j \in [1, n]$   $\varphi_i(L_j) = \delta_{ij}$ . Thus, the basis  $(\varphi_1, \dots, \varphi_n)$  is the ante-dual basis of  $(L_1, \dots, L_n)$ . Therefore, for any polynomial  $P \in \mathbf{R}_n[X]$  we have  $P = \sum_{i=1}^n \varphi_i(P)L_i$  which leads to  $P = \sum_{i=1}^n P(\alpha_i)L_i$ .*

## 7.5 Orthogonal and polar in finite dimension

**Proposition 7.5.0.1** *Let  $W, W_*$  be two subspaces of  $V, V^*$  respectively. We have*

1.  $\dim(W) + \dim(W^\perp) = n$ .
2.  $\dim(W_*) + \dim(W_*^\circ) = n$ .
3.  $W_* = (W_*^\circ)^\perp$ .
4.  $W = (W^\perp)^\circ$ .
5.  $ev(W_*^\circ) = W_*^\perp$ .
6.  $ev(W) = W^{\perp\perp}$ .

*Proof.*

1. Choose a basis  $(e_i, 1 \leq i \leq d)$  of  $W$  and complete it to a basis  $\mathcal{B} = (e_i, 1 \leq i \leq n)$  of  $V$ . If  $\mathcal{B}^* = (e_i^*)$  is the dual basis, then by construction  $W^\perp = \text{Vect}(e_i, i > d)$ .
2. Choose a basis  $(\varphi_i, 1 \leq i \leq d)$  of  $W_*$  and complete it to a basis  $\mathcal{B}_* = (\varphi_i, 1 \leq i \leq n)$  of  $V^*$ . If  $\mathcal{B} = (e_i)$  is the ante-dual basis, then by construction  $W_*^\circ = \text{Vect}(\varphi_i, i > d)$ .
3. Applying the argument from (1) to  $W = W_*^\circ$  and using the basis  $\varepsilon_i = e_{n-i}$ , we get  $W^\perp = (W_*^\circ)^\perp = \text{Vect}(\varphi_i, i \leq d) = W_*$  which gives (3).
4. This has already been proved and is just added for reference (7.3.0.1).
5. If  $\varphi \in W_*^\circ$  and  $w \in W$ , then  $ev(v)(\varphi) = \varphi(w)$  which is null because  $\varphi \in W_*^\circ$  and therefore  $ev(W_*^\circ) \subset W^\perp$ . Since these two spaces have the same dimension as established previously, this inclusion is an equality.
6. If  $w \in W$ , and  $\varphi \in W^\perp$ , then  $ev(v)(\varphi) = \langle \varphi, v \rangle = 0$  so that  $W \subset W^{\perp\perp}$ . As these two spaces have the same dimension as established previously, this inclusion is an equality.

□

**Example(s) 7.5.0.2** If  $V$  is an euclidean space with scalar product  $(v, w) \mapsto v \cdot w$ , the partial linear map  $w \mapsto (v \mapsto v \cdot w)$  has zero kernel and is therefore an isomorphism  $V \mapsto V^*$ . One checks that this isomorphism identifies  $W^\perp$  with the usual Euclidean orthogonal  $\{v \in V | v \cdot W = \{0\}\}$  recovering the classical dimension formula in Euclidean geometry  $\dim(W^\perp) = n - \dim(W)$ . Moreover, with this identification,  $w \in W \cap W^\perp$  satisfies  $w \cdot w = 0$  and therefore is zero ensuring in the Euclidean space the so called usual orthogonal decomposition  $W \oplus W^\perp = V$ .

**Remark(s) 7.5.0.3** Note that orthogonality and polarity are strictly decreasing applications for inclusion.

**Corollary 7.5.0.4** Let  $\varphi_i \in V^*, i = 1, \dots, m$ . Then, the rank of  $\text{Vect}\{\varphi_i\}$  is that of the evaluation application

$$\begin{cases} V & \rightarrow & k^m \\ v & \mapsto & (\varphi_i(v))_i \end{cases}$$

*Proof.* It suffices to observe that the kernel of the evaluation is the polar of  $\text{Vect}\{\varphi_i\}$  and then to invoke the previous

proposition and the rank theorem.

□

## 7.6 Biduality conventions (Finite dimension)

The previous paragraph thus allows, in finite dimension, thanks to  $ev$ , to identify  $V$  and its bidual, polar  $W_*^\circ$  of  $W_*$  and orthogonal  $W_*^\perp$ ,  $W$  and biorthogonal  $W^{\perp\perp}$ . In general, we simply write  $W_*^\perp$  for  $W_*^\circ$ . In finite dimension we generally consider spaces and duals, but we do not dualise the dual thanks to  $ev$  and simply write  $W = W^{\perp\perp}$  whether  $W$  is a subspace of  $V$  or of  $V^*$ .

As an illustration, let's give the simple but important algebraic lemma which in real cases is the algebraic content of the theorem of linked extrema in differential geometry (interpret the result in terms of tangent spaces of submanifolds of  $\mathbf{R}^n$  in the spirit of the example 7.2.0.2).

The following lemma is the algebraic part of the search of extrema through constraints equalities (see 7.6.0.2 for constraint inequalities).

**Lemma 7.6.0.1** *Let  $\varphi$  and  $\varphi_i$ ,  $i \in I$  be linear forms of  $V$ . Then,  $\varphi$  is a linear combination of the  $\varphi_i$  if and only if  $\bigcap_i \text{Ker}(\varphi_i) \subset \text{Ker}(\varphi)$ .*

*Proof.* By strict decrease of the orthogonal, the condition

$$\bigcap_i \text{Ker}(\varphi_i) = \text{Span}(\varphi_i)^\perp \subset \text{Ker}(\varphi) = \text{Span}(\varphi)^\perp$$

is equivalent to the inclusion

$$\text{Span}(\varphi) = \text{Span}(\varphi)^{\perp\perp} \subset \text{Span}(\varphi_i)^{\perp\perp} = \text{Span}(\varphi_i).$$

□

**Remark(s) 7.6.0.2** (Farkas' Lemma) *If  $\mathbf{k} = \mathbf{R}$ , we have an analogous result for finite families of half-spaces  $H^+$ ,  $H_i^+$  defined by the inequalities  $f \geq 0$ ,  $f_i \geq 0$ . Indeed, it can be shown  $\bigcap_i H_i^+ \subset H^+$  if and only if  $\varphi$  is a linear combination with positive coefficients of the  $\varphi_i$ . See [1].*

## 7.7 Contravariance

Let  $V_i$ ,  $i = 1, 2, 3$ , be arbitrary vector spaces,

**Definition 7.7.0.1** *If  $f \in \text{Hom}_{\mathbf{k}}(V_1, V_2)$ , we note  ${}^t f \in \text{Hom}_{\mathbf{k}}(V_2^*, V_1^*)$  the transpose of  $f$  defined by  ${}^t f(\varphi_2) = \varphi_2 \circ f$ , in other words,  $\langle {}^t f(\varphi_2), v_1 \rangle = \langle \varphi_2, f(v_1) \rangle$  for every  $\varphi_2 \in V_2^*$ ,  $v_1 \in V_1$ .*

Let's recall that a matrix and its transpose have the same rank: this is for instance an immediate consequence of the fact that equivalent matrices have equivalent transpose and that equivalence classes of matrices (with coefficients in a field) are classified by the rank).

We have the following (formal) proposition

**Proposition 7.7.0.2** *If  $f \in \text{Hom}_{\mathbf{k}}(V_1, V_2)$  and  $\mathcal{B}_i$  are bases of  $V_i$ .*

1. *The application  $f \mapsto {}^t f$  is linear injective.*
2. *If  $f_i \in \text{Hom}_{\mathbf{k}}(V_i, V_{i+1})$ , we have (contravariance of the transpose)  ${}^t(f_2 \circ f_1) = {}^t f_1 \circ {}^t f_2$ .*

*Assuming further that the  $V_i$ 's are finite dimensional, we have*

3. *We have  $\text{Mat}_{\mathcal{B}_2^*, \mathcal{B}_1^*}({}^t f) = {}^t \text{Mat}_{\mathcal{B}_1, \mathcal{B}_2}(f)$ .*
4.  *$\text{rk}(f) = \text{rk}({}^t f)$ .*
5. *With the identifications (7.6), the transposition is involutive.*
6.  *$\text{Im}({}^t f) = \text{Ker}(f)^\perp$  and  $\text{Ker}({}^t f) = \text{Im}(f)^\perp$ .*
7. *If  $V_1 = V_2 = V$ , a subspace  $W$  of  $V$  is stable by  $f$  if and only if  $W^\perp$  is stable by  ${}^t f$ .*

*Proof.* Let us only give an argument for the fifth point (the verification of the rest is left as a **exercise**). First, it is enough to show one of the two formulas (change  $f$  to  ${}^t f$  and use the involution of the transposition and the orthogonal). Then, since  $\text{Im}({}^t f)$  and  $\text{Ker}(f)^\perp$  have the same dimension according to 1) and 7.5.0.1, it suffices to prove  $\text{Im}({}^t f) \subset \text{Ker}(f)^\perp$ . Now, if  $f(v_1) = 0$ , then  $\langle {}^t f(\varphi_2), v_1 \rangle = \langle \varphi_2, f(v_1) \rangle = 0$ .  $\square$

## 7.8 Exercises

**Exercise 7.8.1** *Compare the orthogonal of a sum or intersection of sub vector spaces with the sum or intersection of their orthogonals.*

**Exercise 7.8.2** *Let  $V$  be the real vector space of polynomial of degree  $\leq 3$ . Let  $a < c < b$  be reals and define  $I \in V^*$  by*

$$\langle I, P \rangle = \int_a^b P(t) dt.$$

*Compute  $\dim \text{Span}(ev_a, ev_c, ev_b, I)$  depending on the value of  $c$ . Deduce a formula for  $I$  depending only on evaluation forms.*

**Exercise 7.8.3** *Let  $\varphi_i, i = 1, \dots, N$  linear forms on  $V$  and  $\Psi \in \text{Hom}(V, \mathbf{k}^N) = (\varphi_i)$ . Prove that the rank of  $\Psi$  is the dimension of the span of the  $\varphi_i$ 's.*

**Exercise 7.8.4** Let  $X$  be any set and  $V$  a finite dimensional vector subspace of the  $\mathbf{R}$ -vector space of functions from  $X$  to  $\mathbf{R}$ . Let  $n = \dim(V)$ .

1. Show that the family  $(e_{v_x}), x \in X$  generates  $V^*$
2. Show that there exists  $f_i \in V, x_i \in X, i = 1, \dots, n$  such that  $\det(f_i(x_j)) \neq 0$ .
3. Assume that all the functions of  $V$  are bounded on  $X$ . Show that any pointwise convergent sequence of elements of  $V$  is uniformly convergent on  $X$ .
4. Does the result previous remain true if one no longer with no boundeness assumption?

**Exercise 7.8.5** Let  $V = \mathbf{R}^n$  with its canonical Euclidean structure  $\langle X, Y \rangle = \sum x_i y_i$ .

1. Prove that  $Y \mapsto (X \mapsto \langle X, Y \rangle)$  is an isomorphism  $V \rightarrow V^*$ .
2. Deduce that the Euclidean orthogonal  $W^\perp = \{Y \mid \langle X, Y \rangle = 0, \forall X \in W\}$  of a sub vector space  $W \subset V$  has dimension  $n - \dim(W)$ .

**Exercise 7.8.6** Let  $V = M_n(\mathbf{k})$ . For  $A \in M_n(\mathbf{k})$ , we recall that its trace is  $\text{Tr}(A) = \sum a_{i,i}$ .

1. Check that  $\text{Tr}(AB) = \text{Tr}(BA), \forall A, B \in M_n(\mathbf{R})$ . Deduce that  $\text{Tr}(PAP^{-1}) = \text{Tr}(A)$  for any  $P \in GL_n(\mathbf{R})$ .
2. Recall how to define the trace of an endomorphism of a finite dimensional vector space.
3. Show that the linear map  $A \mapsto (\text{Tr}(AB))$  is an isomorphism  $V \rightarrow V^*$ .
4. Show that the linear forms  $\varphi \in V^*$  such that  $\langle \varphi, AB \rangle = \langle \varphi, BA \rangle$  for all  $A, B \in V$  are the multiple of the trace map  $A \mapsto \text{Tr}(A)$ .
5. Prove that any hyperplane of  $V$  contains at least one invertible matrix.
6. What is the vector space generated by invertible matrices?

**Exercise 7.8.7** Let  $a \in \text{End}_{\mathbf{k}}(V)$  which is not an homotethy  $\lambda \text{Id}$ .

1. Show that there exists  $x \in V$  such that  $(a, a(x))$  is a free family.

Assume that  $\text{Tr}(a) = 0$ .

2. Deduce that there exists a basis  $\mathcal{B}$  of  $V$  such that the diagonal elements of  $\text{Mat}_{\mathcal{B}}(a)$  are zero.
3. Prove that  $a$  is the sum of two nilpotent endomorphism.
4. What is the vector space generated by nilpotent matrices?

**Exercise 7.8.8** (General transvections) Let  $\tau \in \text{End}_{\mathbf{k}}(V)$ . Show that following properties are equivalent.

1.  $H(\tau) = \text{Ker}(\tau - \text{Id})$  is a hyperplane of  $V$  containing  $D(\tau) = \text{Im}(\tau - \text{Id})$ , which is a line in  $V$ .
2. There exist  $\varphi \in V^*$  and  $v \in V$ , both nonzero, such that  $\tau(x) = x + \varphi(x)v$  with  $\varphi(v) = 0$ .

3. There exists a (unique)  $f \in \text{Hom}_{\mathbf{k}}(V/D(\tau), D(\tau))$  such that  $\tau$  is the composite morphism  $V \rightarrow V/D(\tau) \xrightarrow{f} D(\tau) \rightarrow V$ .

4. The restriction to the affine hyperplane defined by the equation  $\varphi(x) = 1$  is a translation by the vector  $v$ .

5. The natural morphism  $\text{Hom}(V/D, D) \rightarrow \text{GL}(V)$

6. The matrices of  $\tau$  are similar to  $\text{Id}_n + E_{1,2} = \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & 0 \\ 0 & \text{Id}_{n-2} \end{pmatrix}$ .

We say in this case that  $\tau$  is a transvection of  $V$  of type  $(D(\tau), H(\tau))$ . If  $\varphi, v$  are as above, we define  $\tau_\lambda(x) = x + \lambda\varphi(x)v$ ,  $\lambda \in \mathbf{k}$ . Under these conditions, show:

7.  $H(\tau) = \text{Ker}(\varphi), D(\tau) = \langle v \rangle$ ,

8. Transvections of type  $(\langle v \rangle, \langle \varphi \rangle)$  are given by  $\tau_\lambda$ ,  $\lambda \in \mathbf{k}^*$ , and  $\lambda \mapsto \tau_\lambda$  is an injective group morphism  $(\mathbf{k}, +) \rightarrow (\text{SL}(V), \times)$ ,

9.  ${}^t\tau$  is a transvection of  $V^*$  of type  $(H(\tau), D(\tau))$  in some sense to be explained by the reader.

**Exercise 7.8.9** Let  $V$  be the real vector space of polynomial function of degree  $\leq 3$ . Let  $a < c < b$  three real numbers and define  $ev_x, \iota \in V^*$ ,  $x \in \mathbf{R}$ ) by

$$\langle ev_x, P \rangle = P(x), \langle \iota, P \rangle = \int_a^b P(t)dt, P \in V$$

1. Compute  $\dim \text{Span}(ev_a, ev_b, ev_c, \iota)$  according to the value of  $c$ .

2. Deduce a simple formula for  $\int_a^b P(t)dt$ ,  $P \in V$ .

**Exercise 7.8.10** Define  $\Delta$  as the discrete differentiation operator  $\Delta : \mathbf{Q}_n[T] \rightarrow \mathbf{Q}_n[T]$ ,  $P \mapsto P(T+1) - P(T)$  and the family of linear forms  $(\varphi_1, \dots, \varphi_n)$  for all  $i \in [1, n]$  by:  $\varphi_i(P) = (\Delta^i P)(0)$

Define the family  $(H_n)$  by setting  $H_0 = 1$  and  $H_n = \frac{T(T-1)\dots(T-n+1)}{n!}, n > 0$

1. Prove  $\Delta H_n = H_n(T+1) - H_n(T)$

2. Prove that  $(\varphi_1, \dots, \varphi_n)$  is the dual basis of  $(H_1, \dots, H_n)$  and deduce  $P = \sum_{i=0}^n \Delta^i P(0)H_i$  for any  $P \in \mathbf{Q}_n[T]$ .

3. Let  $P \in \mathbf{Q}_n[T]$ . Prove  $P(\mathbf{Z}) \subset \mathbf{Z}$  if and only if there exist  $\alpha_0, \dots, \alpha_n \in \mathbf{Z}$  such that  $P = \sum_{i=0}^n \alpha_i H_i$ .

4. How can you generalize?

**Exercise 7.8.11** Show that the ideal of  $\mathbf{R} = \mathbf{Z}[T]$  generated by 2 and  $T$  is torsion free, of finite type but not free.

**Exercise 7.8.12** Assume  $\dim(V) \geq 2$ . We want to prove by contradiction that there does not exist any functorial isomorphism  $\alpha : V \rightarrow V^*$  in the following sense. Any  $f \in \text{End}_{\mathbf{k}}(V)$  gives rise to a commutative diagram

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & V^* \\ \downarrow f & & \uparrow {}^t f \\ V & \xrightarrow{\alpha} & V^* \end{array}$$

1. Prove

$$\langle \alpha(f(x)), f(y) \rangle = \langle \alpha(x), y \rangle \text{ for all } x, y \in V.$$

2. Prove that there exists  $x, y_1, y_2 \in V, f \in \text{End}_{\mathbf{k}}(V)$  such that  $(x, y_1)$  is free with

$$\langle \alpha(x), y_1 \rangle = 0 \text{ and } \langle \alpha(x), y_2 \rangle \neq 0$$

and  $f$  maps  $(x, y_1)$  to  $(x, y_2)$ .

3. Conclude.

**Exercise 7.8.13** Let  $\varphi \in V^*$  and  $v \neq 0$  cancelling  $\varphi$  and let  $H_1$  be the affine hyperplane of equation  $\varphi(x) = 1$

1. Show that there exists a unique  $\tau \in \text{End}_{\mathbf{k}}(V)$  such that  $\tau$  leaves  $H_1$  invariant with restriction the translation  $x \mapsto x + v$ .
2. Show that in a suitable basis, the matrix of  $\tau$  is the transvection  $T_{1,2}(1)$ .
3. Conversely, show that any standard transvection is associated as in (1) to a translation.

# Chapter 8

## Similarity in $M_n(\mathbf{k})$



### 8.1 Introduction



#### Perspective

We explain how the understanding of matrices with coefficients in the PID  $R = \mathbf{k}[T]$  allows to completely understand the similarity problem in  $M_n(\mathbf{k})$  in an algorithmic manner (3.7).

The aim of this chapter is to study the similarity relation  $\approx$  on  $M_n(\mathbf{k})$ , in other words we want to understand the quotient map<sup>1</sup> of sets  $M_n(\mathbf{k}) \rightarrow M_n(\mathbf{k})/\approx$ . We need to answer two questions

1. Describe  $M_n(\mathbf{k})/\approx$  by giving a canonical representative in each similarity class. This is done in 8.2.2.1.
2. Describe the map by giving an algorithmic way to decide when  $A \approx B$ . This is achieved in 8.4.0.2.

---

<sup>1</sup>The similarity relation  $\approx$  of square matrices is an equivalence relation which should not be confused with the equivalence of matrices  $\approx$  (3.4.0.2).

## 8.2 Similarity in $M_n(\mathbf{k})$

We use the dictionary between  $\mathbf{k}$ -endomorphisms and  $R = \mathbf{k}[T]$ -modules (3.7) to translate our problem in terms of the equivalence class in  $M_n(R)$  of  $T \text{Id} - A$  with  $A \in M_n(\mathbf{k})$  and then to use our understanding of these classes in this Euclidean situation (cf. 6.3.1.2).

### 8.2.1 Similarity invariants

Let  $a, b \in \text{End}_{\mathbf{k}}(V)$  be an endomorphism of an  $n$  dimensional vector space  $V$ .

**Lemma 8.2.1.1** *Let  $P_i, 1 \leq i \leq m$  the unique monic generator of the invariant factor  $I_i$  of  $V_a$ .*

1. *The torsion  $\mathbf{k}[T]$ -module  $V_a$  is of finite type and torsion.*
2. *The rank of the  $\mathbf{k}[T]$ -module  $V_a$  is zero and its invariant ideals are nonzero.*
3. *We have  $P_m | \dots | P_1$  and  $V_a \xrightarrow{\sim} \bigoplus_{i=1}^m \mathbf{k}[T]/(P_i)$  with  $m \leq n$ .*

*Proof.*

1. Any finite generating family of the  $\mathbf{k}$ -vector space  $V$  generates the  $\mathbf{k}[T]$ -module  $V_a$  which is therefore of finite type (and torsion by 3.9.5.1).
2. Use 6.4.0.1.
3. This is (5) of the structure theorem 6.4.0.1 taking into account  $\text{rank}(V_a) = 0$ . Looking at the dimension gives  $n = \sum \deg(P_i) \geq m$ .

□

**Definition 8.2.1.2** *With the above notations, we set  $P_i = 1$  for  $m < i \leq n$  and we say that  $(P_n | \dots | P_1)$  are (is) the (sequence of) similarity invariants of  $a$ .*

**Corollary 8.2.1.3** (Similarity invariants of vector space endomorphisms) *Keeping the above notations, we have*

1.  $V_a \xrightarrow{\sim} \bigoplus_{i=1}^n \mathbf{k}[T]/(P_i)$ .
2. *If  $Q_n | \dots | Q_1$  are monic polynomials such that  $V_a \xrightarrow{\sim} \bigoplus_{i=1}^n \mathbf{k}[T]/(Q_i)$ , then  $P_i = Q_i$  for all  $i$ .*
3.  *$a$  and  $b$  are similar if and only if their similarity invariant are equal.*

*Proof.*

1. This is (3) of the above lemma taking into account  $\mathbf{k}[T]/(P_i) = \{0\}$  if  $i > m$ .
2. This is (4) of 6.4.0.1.
3. Direct consequence of the dictionary 3.7 and of the above lemma.

□

### 8.2.2 Explicit computations of the similarity invariants

Let  $\mathcal{B} = (e_i)_{1 \leq i \leq n}$  be a basis of  $V$  and  $A$  the matrix of  $a$  in this basis. With the notations and result of 3.7.0.2, let us recall that we have a functorial isomorphism

$$\text{Coker}(T \text{Id} - A) \xrightarrow{\sim} V_a$$

deduced from the exact sequences

$$0 \rightarrow V[T] \xrightarrow{T \text{Id} - \bar{a}} V[T] \xrightarrow{\pi_a} V_a \rightarrow 0$$

which in matrix terms reads in

$$0 \rightarrow (\mathbf{k}[T])^n \xrightarrow{T \text{Id} - A} (\mathbf{k}[T])^n \xrightarrow{\pi_A} (\mathbf{k}[T]^n)_A \xrightarrow{\sim} V_a \rightarrow 0$$

where  $\pi_A(\sum X_i T^i) = \sum A^i X_i$ .

Because  $\text{Coker}(T \text{Id} - A) \xrightarrow{\sim} V_a$  is torsion, the structure theorem 6.4.0.1 says that there exist nonzero polynomials

$$Q_n | \dots | Q_1 \in R = \mathbf{k}[T] \text{ such that } T \text{Id} - A \equiv \text{diag}(Q_i)$$

Moreover, we have  $\prod(Q_i) = \det(T \text{Id} - A)$  because Gauss equivalent square matrices have the same determinant. By 8.2.1.3, the sequence  $(Q_i)$  is up to  $R^\times$  the sequence of the similarity invariants of  $P_i$  of  $A$ . The diagonal matrix  $\text{diag}(Q_i/P_i)$  belongs therefore to  $\text{GL}_n(R)$  and its determinant thus belongs to  $R^\times$ . But  $\prod Q_i$  and  $\prod P_i$  being monic polynomials, we get  $\prod(Q_i) = \prod P_i$  and therefore  $\text{diag}(Q_i) \equiv \text{diag}(P_i)$  by 6.4.1.2. We have got

$$\boxed{T \text{Id} - A \equiv \text{diag}(P_i) \text{ where } P_i \text{ are the similarity invariants of } a.}$$

Taking this result into account, we can rewrite entirely 8.2.1.3.

**Corollary 8.2.2.1** *Let  $A, B \in M_n(\mathbf{k})$  be the matrices of  $a, b \in \text{End}_{\mathbf{k}}(V)$  in some basis. Let  $(P_n | \dots | P_1)_{1, \leq i \leq n}$  be a sequence of monic polynomials. The following assertions are equivalent*

- $(P_i)$  is the sequence of similarity invariant of  $a$

- $T \text{Id} - A \equiv \text{diag}(P_i)$ .
- $T \text{Id} - A \sim \text{diag}(P_i)$ .
- $V_a \xrightarrow{\sim} \bigoplus \mathbf{k}[T]/(P_i)$ .

Moreover, the following conditions are equivalent.

- $A$  and  $B$  are similar in  $M_n(\mathbf{k})$ .
- $T \text{Id} - A$  and  $T \text{Id} - B$  are equivalent in  $M_n(\mathbf{k}[T])$ .
- The  $\mathbf{k}[T]$ -modules  $V_a$  and  $V_b$  are isomorphic.



We get then the following relations between the similarity invariants.

**Corollary 8.2.2.2** *We have the following formulas.*

1.  $\prod_{i=1}^n P_i = \chi_a(T)$ .
2.  $P_1 | \chi_a | P_1^n$ . In particular  $\chi_a$  and  $P_1$  have the same roots in any extension of  $\mathbf{k}$  (hence have the same irreducible factors<sup>2</sup>).
3.  $P(a) = 0$  if and only if  $P_1 | P$ . In other words,  $P_1$  is the minimal polynomial of  $a$  (often denoted by  $\mu_a$ ).
4. The morphism of  $\mathbf{k}$ -algebras  $ev_a : \mathbf{k}[T] \rightarrow \mathbf{k}[a] \subset \text{End}_{\mathbf{k}}(V)$  induces a isomorphism  $\mathbf{k}[T]/(\mu_a) \xrightarrow{\sim} \mathbf{k}[a]$ .

*Proof.*

1. There exists  $Q, Q' \in GL_n(\mathbf{k})$  such that  $T \text{Id} - A = Q \text{diag}(P_i) Q'$ . Because  $\det(P) \in \mathbf{k}^*$ , their determinant  $\chi_a(T)$  and  $\prod P_i(T)$  differ by a multiplication by a scalar which is 1 because both polynomials are monic.

---

<sup>2</sup>Cf. chapter 9.

2. Because  $P_1$  is a multiple of each  $P_i$ , by taking the product, we find that  $P_1^n$  is a multiple of  $\chi_a$ , thus  $P_1 | \chi_a | P_1^n$ .
3.  $P$  kills  $V_a \xrightarrow{\sim} \bigoplus \mathbf{k}[T]/(P_i)$  iff and only if  $P$  kills all the  $\mathbf{k}[T]/(P_i)$  in other words when  $P_i | P$ . Because  $P_i | P$  for all  $i$ , we are done.
4. We have  $ev_a$  onto and  $\text{Ker}(ev_a) = (\mu_a)$  and we conclude by the universal property of the kernel (4.2.0.1).

□

**Remark(s) 8.2.2.3**

- Note that the above statement 8.2.2.2 denies the existence of  $\mu_a$  without any prior knowledge. By construction, it is the unique monic polynomial of lowest degree that annihilates  $a$ .
- The interested reader can check that we did not use the Cayley-Hamilton theorem (2.1.3.2) to prove these results. So the divisibility  $P_1 = \mu_a | \chi_a$  is another (too complicated) proof in the field case.
- As we will see later (e.g. 8.4.0.4), the last  $P_i$  are often equal to 1. They contribute through the zero module to  $V_a$ , as we have already observed.
- Unlike the characteristic polynomial, the similarity invariants do not vary continuously with  $a$ . For example, the similarity invariant of  $\text{diag}(0, t)$  is  $1, T(T - t)$  when  $t \neq 0$  and  $T, T$  when  $t = 0$ . We will discuss this phenomenon in full generality in the chapter 13.



Finally, let us give two classical results.

**Corollary 8.2.2.4** Let  $A, B \in M_n(\mathbf{k})$  and  $K$  a field containing  $\mathbf{k}$ . We have

1.  $A$  and  ${}^t A$  are similar.
2.  $A, B$  are similar in  $M_n(\mathbf{k})$  if and only if they are similar in  $M_n(K)$

*Proof.*

1. Observe that  $T - \text{Id } A = Q \text{diag}(P_i)Q'$  implies  $T - \text{Id } {}^t A = {}^t Q' \text{diag}(P_i) {}^t Q$ .
2. If  $P_i, \tilde{P}_i$  are the similarity invariants of  $A$  in  $M_n(\mathbf{k})$  and  $M_n(K)$ , we have  $T \text{Id} - A \equiv \text{diag}(P_i)$  in  $M_n(\mathbf{k}[T])$  and therefore  $T \text{Id} - A \equiv \text{diag}(P_i)$  in  $M_n(\mathbf{k}[T])$  because  $\text{GL}_n(\mathbf{k}[T]) \subset \text{GL}_n(K[T])$ . But by definition of  $\tilde{P}_i$ , we have also  $T \text{Id} - A \equiv \text{diag}(\tilde{P}_i)$  in  $M_n(K)$ . By uniqueness, we get  $P_i = \tilde{P}_i$ , hence the result.

□

### 8.3 An important example: diagonalization

Although the diagonalization of endomorphisms is not necessary to understand the similarity of matrices, we will illustrate our results in this special case. We will denote by  $\mathbf{k}_\lambda$  the  $\mathbf{k}[T]$  module  $\mathbf{k}_\lambda = \mathbf{k}[T]/(T - \lambda)$ . It is of dimension 1 as a  $\mathbf{k}$ -vector space, and conversely any  $\mathbf{k}[T]$  module of  $\mathbf{k}$  dimension 1 is of this form for a unique  $\lambda$  characterized by  $T \cdot 1 = \lambda$ .

By definition, we recall that  $a \in \text{End}_{\mathbf{k}}(V)$  is diagonalizable if and only if  $V$  has a basis of eigenvectors, *i.e.* if

$$V_a = \bigoplus_{\lambda \in \text{Spec}(A)} \text{Ker}(a - \lambda \text{Id})$$

where  $\text{Spec}(A) = \chi_a^{-1}(0) = \mu_a^{-1}(0)$  is the set of eigenvalues of  $a$ . Equivalently,  $a$  is diagonalizable if its matrix is similar to a diagonal matrix in some basis. In this case, the theory of similarity invariants reads as follows.

**Proposition 8.3.0.1** *The following assertions are equivalent.*

1.  $a$  is diagonalizable.
2.  $a$  is cancelled by some non zero  $P \in \mathbf{k}[T]$  which is split with  $\text{GCD}(P, P') = 1$ .
3.  $\mu_a$  is split with  $\text{GCD}(\mu_a, \mu'_a) = 1$ .
4.  $V_a$  is a direct sum of dimension 1 module  $\mathbf{k}_\lambda$ .

*In particular, the restriction of a diagonalizable morphism to a stable subspace is diagonalizable.*

*Proof.* We prove  $(1) \Rightarrow (2) \cdots \Rightarrow (4) \Rightarrow (1)$ .

1. If  $D$  is the diagonal matrix of  $a$  in a diagonalization basis, then  $P(T) = \prod (T - d_i)$  where  $d_i$  runs over the distinct diagonal terms of  $D$  cancels  $a$  hence (2).
2.  $\mu_a | P$  hence (3).
3. Each similarity invariant of  $P_i$  divides  $P_1 = \mu_a$  and therefore is a product of distinct linear factors. By the Chinese reminder lemma applied to  $I_\lambda = (T - \lambda), \lambda \in \text{Spec}(a)$ , we get

$$V_a = \bigoplus_{\lambda} \text{Ann}_M(T - \lambda) = \bigoplus \text{Ker}(a - \lambda \text{Id})$$

and any series of basis of  $\text{Ker}(a - \lambda \text{Id})$  defines the required sum by (4).

4. Tautology.

The last point follows from (2) because any polynomial which annihilates  $a$  cancels any restriction of  $a$  to a stable subspace. □

As we will see in chapter 11, diagonalizable endomorphisms is the typical example of semisimple endomorphisms.

## 8.4 Frobenius Decomposition



Ferdinand Georg Frobenius

We will rephrase the previous results in terms of companion matrices providing a canonical representative  $C(\underline{P})$  in each similarity class  $\bar{A}$ .

**Definition 8.4.0.1** Let  $\chi = T^n + \sum_{i=0}^{n-1} a_i T^i \in \mathbf{k}[T]$

1. A type (or  $n$ -type)  $\underline{P}$  is a sequence  $\underline{P} = (P_n | \cdots | P_1)$  a sequence of monic polynomials with  $\sum \deg(P_i) = n$ . It is a  $\chi$ -type if moreover  $\prod P_i = \chi$
2. The companion matrix  $C(\chi)$  of  $\chi$  is the matrix of the multiplication by  $T$  on  $\mathbf{k}[T]/(\chi)$ . Thus,  $C(\underline{P})$  is the empty matrix if  $\underline{P} = 1$
3. The generalized companion matrix of a type  $\underline{P}$  is  $C(\underline{P}) = \text{diag}(C(P_i)) \in M_n(\mathbf{k})$ .

Explicitly, one has

$$C(\chi) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

We already know (apply (3) of 2.3.1.1 with  $R = \mathbf{k}[T]$  and  $t \mapsto -T, a_i \mapsto -a_{n-i-1}$ )

$$(*) \quad T \text{Id}_n - C(\chi) \equiv \text{diag}(\chi, 1, \dots, 1) \in M_n(\mathbf{k}).$$

Using  $\deg(P_i) = n$ , we get more generally (using (1) of 2.3.1.1)

$$C(\underline{P}) \equiv \text{diag}(P_1, \dots, P_n)$$

We rewrite the similarity invariant theorem 8.2.2.1 as follows.

**Corollary 8.4.0.2** (Frobenius Reduction) *Let  $\underline{P} = (P_n | \cdots | P_1)$  be a type and  $A \in M_n(\mathbf{k})$ . Then,  $A \approx C(\underline{P})$  (i.e.  $A$  and  $C(\underline{P})$  are similar) if and only if  $\underline{P}$  is the sequence of similarity invariants of  $A$ .*

**Remark(s) 8.4.0.3** (Frobenius decomposition)

- *It is said that  $C(\underline{P})$  is the Frobenius normal form of  $A$ .*
- *Using 4.2.2.1, we can rephrase the Frobenius reduction theorem above as follows. With the above notations,  $\underline{P}$  is the sequence of similarity invariants of  $a$  if and only if there exists a direct sum decomposition  $V_a = \sum V_i$  into cyclic modules with  $\text{Ann}_{\mathbf{k}[T]}(V_i) = (P_i)$ .*
- *The degree condition  $n = \deg(P_i)$  forces very often a lot of components of a type  $\underline{P}$  to be equal to 1. This is the case for the type associated to a companion which will be appear the most likely (13.5.2.2).*
- *The reader will deduce easily (\*) from 8.2.2.1 in the field case, which is the usual way to prove that. We wanted to stress that this equivalence is formal and does not depend on the coefficient ring.*

Using 4.2.2.1, we get the more or less classical result in the case of a unique companion block  $C(P)$

**Corollary 8.4.0.4** *Let  $a \in \text{End}_{\mathbf{k}}(V)$ . The following statements are equivalent<sup>3</sup>:*

1. *The matrix of  $A$  in a suitable basis is the companion matrix  $C(\chi)$ .*
2.  *$\mu_a = \chi_a = \chi$ .*
3. *The similarity invariants are  $(1, \cdots, 1, \chi)$ .*
4.  *$V_a$  and  $\mathbf{k}[T]/(\chi)$  are isomorphic  $\mathbf{k}[T]$ -modules.*
5.  *$V_a$  is cyclic as  $(\mathbf{k}[T]$ -module) and  $\chi_a = \chi$ .*

## 8.5 Commutant

It is then easy to study the commutant (see 3.7.0.1)

$$\text{End}_{\mathbf{k}[T]}(V_a) \simeq \text{End}_{\mathbf{k}[T]}(\oplus \mathbf{k}[T]/(P_i)).$$

for example, to calculate its dimension.

<sup>3</sup>This also equivalent for infinite fields that  $V$  has a finite number of subspaces stable by  $a$  (9.2.2.2).

**Proposition 8.5.0.1** *The dimension of the commutant of  $a$  is  $\sum (2i - 1) \deg(P_i)$ . In particular,  $\dim \text{End}_{\mathbf{k}[T]}(V_a) \geq n$  with equality if and only if  $a$  is cyclic.*

*Proof.* We have

$$\text{End}_{\mathbf{k}[T]}(\oplus \mathbf{k}[T]/(P_i)) = \oplus_{i,j} \text{Hom}_{\mathbf{k}[T]}(\mathbf{k}[T]/(P_i), \mathbf{k}[T]/(P_j))$$

Since  $\mathbf{k}[T]/(P_i)$  is cyclic generated by the class of 1, an element of

$$\text{Hom}_{\mathbf{k}[T]}(\mathbf{k}[T]/(P_i), \mathbf{k}[T]/(P_j))$$

is determined by its image  $(P \bmod P_j)$  where  $P$  satisfies

$$(*) \quad P_i P \equiv 0 \pmod{P_j}$$

(universal property of the quotient 4.2.0.1). If  $i \leq j$ , we have  $P_j | P_i$ , and this condition is automatically satisfied so that

$$\text{Hom}_{\mathbf{k}[T]}(\mathbf{k}[T]/(P_i), \mathbf{k}[T]/(P_j)) \simeq \mathbf{k}[T]/(P_j) \text{ if } i \leq j$$

If  $i > j$ , we have  $P_i | P_j$  so the condition  $(*)$  reads  $P \equiv 0 \pmod{P_j/P_i}$  so that

$$\text{Hom}_{\mathbf{k}[T]}(\mathbf{k}[T]/(P_i), \mathbf{k}[T]/(P_j)) \simeq P_j/P_i \mathbf{k}[T]/(P_j) \simeq \mathbf{k}[T]/(P_i) \text{ if } i > j$$

We therefore have

$$\begin{aligned} \dim_{\mathbf{k}}(\text{End}_{\mathbf{k}[T]}(V_a)) &= \sum_{i \leq j} \deg(P_j) + \sum_{i > j} \deg(P_i) \\ &= \sum_j j \deg(P_j) + \sum_i (i-1) \deg(P_i) \\ &= \sum (2i-1) \deg(P_i) \end{aligned}$$

Using  $n = \sum \deg(P_i)$ , we get  $\dim \text{End}_{\mathbf{k}[T]}(V_a) - n = 2 \sum_{i=1}^n (i-1) \deg(P_i) \geq 0$ . Furthermore, equality implies  $(i-1) \deg(P_i) = 0$  for every  $i$ , thus  $\deg(P_i) = 0$  if  $i > 1$  so that equality is equivalent to the fact that  $a$  is cyclic.  $\square$

## 8.6 Appendix: Algorithm from equivalence to similarity

We know therefore that if  $T_i - A$  and  $T_i - B$  are equivalent, i.e., if there exist  $P(T), Q(T)$  polynomial and invertible matrices such that

$$P(T)(T_i - A) = (T_i - B)Q(T)^{-1},$$

then there exists  $P \in \text{GL}_n(\mathbf{k})$  such that  $B = PAP^{-1}$ .

**Proposition 8.6.0.1** (Thanks to O. Debarre) *There exists an algorithm for computing such a  $P$ .*

*Proof.* We can perform the divisions by monic (here of degree one) in  $\mathcal{R}[T]$  with  $\mathcal{R} = M_n(\mathbf{k}[T])$

$$\begin{aligned} P(T) &= (Ti - B)P_1(T) + P_0, \\ Q(T)^{-1} &= \tilde{Q}_1(T)(Ti - A) + \tilde{Q}_0, \end{aligned}$$

with  $P_0$  and  $\tilde{Q}_0$  in  $M_n(\mathbf{k})$  (let's stress that  $\mathcal{R}$  is not in a commutative ring<sup>4</sup>). We obtain by substituting

$$((Ti - B)P_1(T) + P_0)(Ti - A) = (Ti - B)(\tilde{Q}_1(T)(Ti - A) + \tilde{Q}_0)$$

or also

$$(Ti - B)(P_1(T) - \tilde{Q}_1(T))(Ti - A) = (Ti - B)\tilde{Q}_0 - P_0(Ti - A).$$

The left-hand side is therefore of degree at most 1 in  $T$ , which is only possible if  $P_1(T) = \tilde{Q}_1(T)$ . Thus  $(Ti - B)\tilde{Q}_0 = P_0(Ti - A)$  (argue by contradiction and look at the highest degree term). The equality of the coefficients of  $T$  gives  $\tilde{Q}_0 = P_0$ , that of the constant coefficients gives  $B\tilde{Q}_0 = P_0A$ . It remains to show that  $\tilde{Q}_0$  is invertible. We perform another division in  $\mathcal{R}[T]$

$$Q(T) = Q_1(T)(Ti - B) + Q_0$$

and we write

$$\begin{aligned} \mathbf{i} &= Q(T)^{-1}Q(T) \\ &= (\tilde{Q}_1(T)(Ti - A) + \tilde{Q}_0)Q(T) \\ &= \tilde{Q}_1(T)(Ti - A)Q(T) + \tilde{Q}_0Q(T) \\ &= \tilde{Q}_1(T)P(T)^{-1}(Ti - B) + \tilde{Q}_0(Q_1(T)(Ti - B) + Q_0) \\ &= (\tilde{Q}_1(T)P(T)^{-1} + \tilde{Q}_0Q_1(T))(Ti - B) + \tilde{Q}_0Q_0. \end{aligned}$$

Again, as  $\tilde{Q}_0Q_0$  is constant, the factor of  $Ti - B$  is zero and  $\tilde{Q}_0Q_0 = \mathbf{i}$ , hence the conclusion.  $\square$

## 8.7 Summary on similarity invariants

Collating what we have proved, we have the following results which was wanted in 5.1.

Let  $A, B \in M_n(\mathbf{k})$  and  $\underline{P} = (P_n | \cdots | P_1)$  a family of monic polynomials.

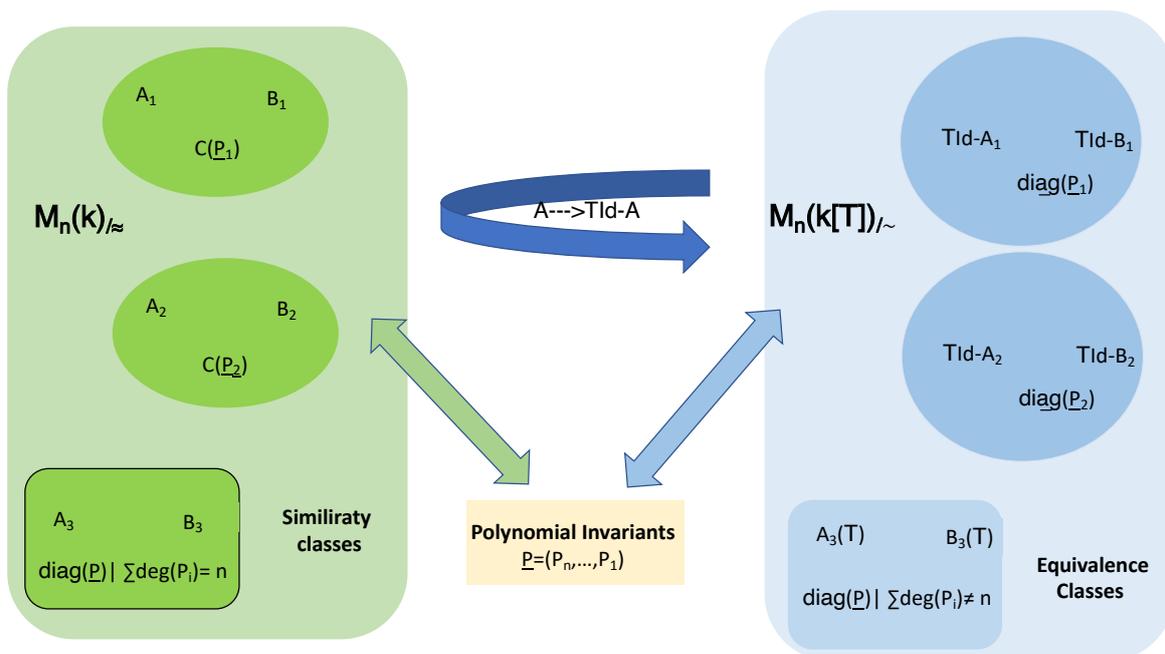
- $A$  and  $B$  are similar if and only if they have the same similarity invariants or equivalently if  $V_A \xrightarrow{\sim} V_B$ .
- The family of similarity invariants of  $C(\underline{P})$  is  $\underline{P}$  and the similarity invariants of  $C(P)$  are  $(1, \dots, 1, P)$ .

<sup>4</sup>See 1.3.1.1

If  $\underline{P}$  is the family of similarity invariants of  $A$ , we have:

- $A$  and  $C(\underline{P})$  are similar (Frobenius Reduction).
- $V_A \simeq \oplus \mathbf{k}[T]/(P_i)$  where  $A$  also denotes the endomorphism of  $V = \mathbf{k}^n$  associated.
- $T \text{Id} - A$  is equivalent to  $\text{diag}(P_1, \dots, P_n)$ .
- The GCD of minors of  $T \text{Id} - A$  of size  $i$  is equal to  $\delta_i = \prod_{j \geq n-i+1} P_j$ .
- $\underline{P}$  is calculated by Gauss elimination by “diagonalizing”  $T \text{Id} - A$  in  $M_n(\mathbf{k}[T])$ .
- We have  $\chi_A = P_1 \cdots P_n$  and  $P_1 = \mu_A$ .

The proof strategy is illustrated by the following diagram.



## 8.8 Exercises

**Exercise 8.8.1** Let  $(a_1, \dots, a_n) \in \mathbf{C}^n$ . Is the matrix  $(a_i a_j)_{1 \leq i, j \leq n}$  diagonalizable?

**Exercise 8.8.2** Let  $A, B \in M_n(\mathbf{C})$  with  $AB = BA$  and let  $M = \begin{pmatrix} A & B \\ 0 & A \end{pmatrix}$ . Give a condition for  $M$  to be diagonalizable.

**Exercise 8.8.3** Let  $a_0, \dots, a_{n-1}$  be complex numbers, and let

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ a_1 & \cdots & a_{n-1} & a_0 \end{pmatrix} \in M_n(\mathbf{C})$$

1. Prove that  $C = C(T^n - 1)$  is diagonalizable over  $\mathbf{C}$ .
2. Find a complex polynomial  $P$  such that  $A = P(C)$ .
3. Prove that  $A$  is diagonalizable and compute its eigenvalues.

**Exercise 8.8.4** Let  $A, B \in M(\mathbf{k})$  such that  $AB - BA = A$ .

1. Compute  $A^d B - BA^d$ .
2. Prove that  $A$  is nilpotent.
3. Can you give an example with  $A \neq 0$ ?

**Exercise 8.8.5** Let  $a, b \in \text{End}_{\mathbf{R}}(W)$  such that  $ab - ba = \text{Id}$  with  $W$  is an arbitrary real vector space.

1. Show that  $\dim(V) = \infty$ .
2. Assume that  $W$  is endowed with a norm and that  $a, b$  are continuous. Show that  $a$  would be nilpotent and then that  $a$  or  $b$  is not continuous (adapt 8.8.4).
3. Give an example [Hint: think at basics of quantum mechanics!].
4. What can you say if we replace  $\mathbf{k}$  with an arbitrary field?

**Exercise 8.8.6** Let  $P \in \mathbf{C}[T], a \in \text{End}_{\mathbf{C}}(V)$  is such that  $P'(a)$  is invertible. Show that:  $P(a)$  is diagonalizable if and only if  $a$  is diagonalizable.

**Exercise 8.8.7** Show that a diagonalizable endomorphism  $x$  is cyclic if and only  $\chi_a$  has simple roots.

**Exercise 8.8.8** Let  $A, B \in V = \mathbf{R}_n[T]$  with  $\text{GCD}(A, B) = 1$  and  $B = \prod (T - x_i)$  is split with simple roots. We define  $a \in \text{End}_{\mathbf{k}}(V)$  to itself that associates to any polynomial  $P$  the remainder of the Euclidean division of  $AP$  by  $B$ .

1. Prove that  $a$  is an endomorphism of  $E$ .
2. Prove that  $0 \in \langle a \rangle$  and determine the associated eigenspace.
3. Prove that for each  $k = 1, \dots, p$ , the polynomial

$$P_k(X) = \prod_{j \neq k} (T - x_j)$$

is an eigenvector of  $a$ .

4. Deduce that  $a$  is diagonalizable.

**Exercise 8.8.9** Let  $G \subset \mathrm{GL}_n(\mathbf{C})$  be a subgroup. Assume that there exists  $N > 0$  such that  $g^N = \mathrm{Id}$  for any  $g \in G$ .

1. Prove that any  $g \in G$  is diagonalizable.

2. Let  $\tau : G \rightarrow \mathbf{C}^d$  defined by  $g \mapsto (\mathrm{Tr}(gg_i))$  where  $g_1, \dots, g_d$  generates  $\mathrm{Span}(G) \subset M_n(\mathbf{C})$ .

3. Prove that  $\tau$  is injective.

4. Prove that  $G$  is finite.

**Exercise 8.8.10** Show that the restriction of a cyclic endomorphism to a stable subspace remains cyclic.

**Exercise 8.8.11** (difficult) Show that the inclusion  $\mathbf{k}[a]$  in his bicommutant, that is the set of endomorphisms that commute with all elements of  $\mathrm{End}_{\mathbf{k}[T]}(V_a)$ , is an equality.



# Chapter 9

## The irreducibility toolbox



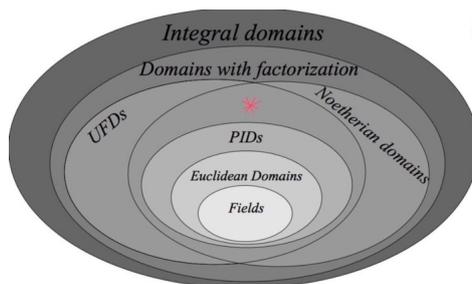
### 9.1 Introduction



#### Perspective

Even if it is difficult or almost impossible to compute the decomposition of an integer into prime factors, the existence of this unique decomposition is certainly of first importance. Analogously, even if it is mostly impossible to compute the eigenvalues of an endomorphism,<sup>1</sup> the existence of a unique decomposition of the characteristic polynomial into linear factors if  $\mathbf{k} = \mathbf{C}$  (or in irreducible polynomials in general) is of first importance. We explain the general theory behind these notions.

In this chapter,  $R$  denotes a *domain* (i.e. an integral commutative ring commutative with unit) and  $\mathbf{k}$  is its field of fractions(3.10.3).



## 9.2 An UFD criterion

**Definition 9.2.0.1** We say that  $x \in R^*$  is irreducible if it is non-invertible and if  $x = x_1x_2$  implies  $x_1$  or  $x_2$  is invertible.

In other words,  $x \in R^*$  is irreducible if its divisors are up to multiplication by a unit equal to 1 or  $x$ . Notice that whether  $x$  is irreducible only depends on the ideal  $(x)$ .

### Example(s) 9.2.0.2

- Irreducible elements of  $\mathbf{Z}$  are  $\pm$ -prime numbers.
- Irreducible polynomials in  $\mathbf{C}[T]$  are degree one polynomial.
- Irreducible polynomials in  $\mathbf{R}[T]$  are degree one polynomial and degree two polynomial without real root if  $\mathbf{k} = \mathbf{C}$  (exercise).

### 9.2.1 Uniqueness condition

We know that positive irreducible integers are precisely prime numbers. Generally, we only have one implication

**Lemma 9.2.1.1** Let  $x \in R^*$ . If the ideal  $(x)$  is prime then  $x$  is irreducible.

*Proof.* If  $x = x_1x_2$ , the product  $x_1x_2$  is zero in  $R/(x)$  which by definition is integral. Hence, the class  $(x_1 \bmod x)$  for example is zero so that  $x_1 = y_1x$  and  $x = y_1x_2$ . Simplifying by  $x$  (integrality), we get  $x_2 \in R^\times$ .  $\square$

<sup>1</sup>See 14.3.3.2 to temper this statement and more generally chapter 14.

The converse is the so called Euclid property and is the heart of the uniqueness property of irreducible decomposition.

**Definition 9.2.1.2** (Euclid's Property) *We say (by abuse) that  $R$  satisfies Euclid property if the ideal generated by an irreducible element is prime, that is if any irreducible element dividing a product divides one of the factors.*

We will use the following proposition at length in the sequel, especially for irreducible polynomials in  $\mathbf{k}[T]$ .

**Proposition 9.2.1.3** *The maximal ideals in a PID  $R$  which is not a field are ideals generated by irreducible elements.*

*Proof.* Assume  $p$  is irreducible and let  $a \not\equiv 0 \pmod{p}$ . Because  $\text{GCD}(a, p)$  divides  $p$ , it is equal to 1 or  $p$ . But  $p$  does not divide  $a$  therefore  $\text{GCD}(a, p) = 1$  and by Bézout theorem there exists  $u, v$  such that  $au + pv = 1$  and  $u \pmod{p}$  is the inverse of  $a \pmod{p} \in R/(p)$ . Moreover, because  $p$  is not invertible,  $R/(p)$  is nonzero and  $R/(p)$  is a field.

Conversely, if  $R/(p)$  is a field, it is a domain and  $(p)$  is prime and therefore  $p$  is irreducible.  $\square$

**Proposition 9.2.1.4** *A PID satisfies Euclide's property.*

*Proof.* Let  $x, x_1, x_2 \in R^*$  with  $x|x_1x_2$  irreducible and let  $d = \text{GCD}(x, x_1)$ . Because  $d|x$  and  $x$  irreducible, we again have  $d = 1$  or  $d = x$ . In the second case, we have done because  $x = d|x_1$  by definition. In the first case, we apply Gauss lemma for PID (6.2.0.5) and we get  $x|x_2$ .  $\square$

**Definition 9.2.1.5** *Let  $R$  be a domain and  $x \in R^*$ .*

*$R$  is a unique factorization domain (UFD) if*

1.  *$x$  has a decomposition  $x = u \prod_{i=1}^n p_i$  with  $u \in R^\times$  and  $p_i$  irreducible;*
2. *if  $x = u' \prod_{i=1}^{n'} p'_i$ , with  $u' \in R^\times$  and  $p'_i$  irreducible is another decomposition, then,  $n = n'$  and, up to renumbering,  $(p_i) = (p'_i)$  for all  $i$ .*

If  $x = u \prod_{i=1}^n p_i$  is a decomposition as above, we can therefore define for any irreducible element  $p$  the integer

$$v_p(x) = \text{Card}\{i | (p_i) = (p)\}.$$

The reader will check (strongly using uniqueness and not only existence of irreducible decompositions) the following properties for nonzero elements  $x, y$  of an UFD (**exercice**).

- $v_p(x)$  is the maximal power of  $p$  dividing  $x$ .
- $x|y$  if and only if  $v_p(x) \leq v_p(y)$  for any irreducible element  $p$ .
- $v_p(xy) = v_p(x) + v_p(y)$  and  $v_p(x + y) \geq \min(v_p(x), v_p(y))$ .
- $x$  is square free<sup>2</sup> if  $v_p(x) \leq 1$  for all  $p$ .

**Lemma 9.2.1.6** (Uniqueness Lemma) *Let  $R$  be an integral domain such that every element of  $R^*$  admits a decomposition into irreducible elements. Then  $R$  is UFD if and only if it satisfies Euclid's property.*

*Proof.* Assume  $R$  is UFD and let  $x$  be irreducible. Suppose we have a decomposition  $x = x_1 x_2$ . We decompose each  $x_i$  into irreducible elements  $x_i = u_i \prod_{j=1}^{n_i} p_{i,j}$  giving  $x = u_1 u_2 \prod_{i,j} p_{i,j}$ . Thus, we have two decompositions of  $x$  into irreducible elements, one having of length 1, the other of length  $n_1 + n_2$ . Thus, by uniqueness,  $1 = n_1 + n_2$  and for instance  $n_1 = 0$  which proves that  $x_1$  is invertible hence  $R$  satisfies Euclid's property.

Assume now that  $R$  satisfies Euclid's property. We prove the uniqueness by induction on the sum  $\ell$  of the lengths of two possible decompositions of the same non-zero element. If  $\ell = 0$ , there is nothing to prove. Assume that we have (with the previous notation)

$$u_1 \prod_{j=1}^{n_1} p_{1,j} = u_2 \prod_{j=1}^{n_2} p_{2,j}$$

with  $\ell = n_1 + n_2 \geq 1$ . We have for instance  $n_1 \geq 1$  and  $p_{1,1} | \prod_{j=1}^{n_2} p_{2,j}$ . By Euclid's property, renumbering if necessary, one has  $(p_{1,1}) = (p_{2,1})$  implying at once  $n_2 \geq 1$ . Changing  $u_2$  to another unit, we get by integrality of  $R$

$$u_1 \prod_{j=2}^{n_1} p_{1,j} = u_2 \prod_{j=2}^{n_2} p_{2,j}$$

and we conclude by induction. □

**Corollary 9.2.1.7** *Up to multiplication by  $R^\times$ , the number of divisors of a nonzero element of an UFD is finite.*

This property is not true in general (see 9.6.8).

---

<sup>2</sup>with no non unit square divisor

### 9.2.2 Stable subspaces of endomorphisms

We know that the stable subspaces by  $a \in \text{End}_{\mathbf{k}}(V)$  are its submodules (3.7). Therefore if  $V_a$  is cyclic they are also cyclic because  $\mathbf{k}[T]$  is a PID (4.2.2.1) and in one to one correspondence to ideals  $J$  containing  $(\mu_a) = \text{Ann } V_a$ . Therefore, the stable subspaces of a cyclic endomorphism are exactly the  $P(a)(V)$  with  $P$  being monic divisors of  $\chi$ . In particular, they are finite in number (9.2.1.7). Remarkably, the converse is essentially true.

**Proposition 9.2.2.1** *If  $\mathbf{k}$  is infinite, an endomorphism that has only a finite number of stable subspaces is cyclic.*

*Proof.* Let  $a$  be such an endomorphism. We have to find some cyclic vector for  $a$ . The family of stable strict subspaces) of  $V$  is a finite family of strict subspaces. Since  $\mathbf{k}$  is infinite, this union is a proper subspace (7.2.0.1) and any point in the complement is a cyclic vector.  $\square$

Obviously, if  $\mathbf{k}$  is finite the proposition is false since there is only a finite number of subspaces of  $V$  in this case, stable or not.

**Remark(s) 9.2.2.2** *When  $\mathbf{k} = \mathbf{C}$ , any endomorphism  $a$  in dimension  $> 1$  admits non-trivial stable spaces (take proper lines). When  $\mathbf{k} = \mathbf{R}$ , either it admits stable lines (real eigenvalues) or stable planes (take for example the plane defined by the real and imaginary parts of the coordinates of a non-zero eigenvalue vector of the matrix of  $a$  in a base or, what comes to the same, consider an irreducible degree 2 polynomial characteristic factor). If  $\mathbf{k} = \mathbf{Q}$  and if  $P \in \mathbf{Q}[T]$  is irreducible of degree  $n$  (take for example  $P(T) = T^n - 2$  which is irreducible over  $\mathbf{Q}$  by Eisenstein's criterion (9.6.4), then the multiplication endomorphism by  $T$  on  $\mathbf{Q}[T]/(P)$  has no non-trivial stable subspaces since it is cyclic and its minimal does not have a strict divisor: the stable subspaces of an endomorphism depend strongly on the arithmetic of the base field. See chapter 11 for more results about the existence of stable complements of stable subspaces.*

### 9.2.3 Existence criterion

**Lemma 9.2.3.1** *Every nonzero and non-invertible element in a Noetherian domain  $R$  is a product of irreducible elements.*

*Proof.* Then, let  $\mathcal{F}$  be the set of proper and nonzero principal ideals  $(x)$  of  $R$  with  $x$  is not a product of irreducible elements. If  $\mathcal{F}$  were non-empty, it would have a maximal element  $(x) \in \mathcal{F}$  for inclusion. If  $x$  were irreducible,  $x = x$  is a decomposition of  $x$  into product of irreducible elements contradicting  $(x) \in \mathcal{F}$ . Therefore  $x$  is not irreducible and  $x$  can be written  $x_1x_2$  with  $x_1$  and  $x_2$  non-invertible. Thus

$(x) \subsetneq (x_i)$ . By maximality,  $(x_i) \notin \mathcal{F}$  so that each  $x_i$  is a product of irreducible elements, and so is their product  $x$ . A contradiction.  $\square$

We summarize the main preceding results in the following corollary.

### Corollary 9.2.3.2

- An integral Noetherian domain is UFD if and only if it satisfies Euclid's property.
- A PID is UFD.
- In a PID, the number of divisors (up to multiplication by a unit), is finite.

In particular,  $\mathbf{k}[T]$  is UFD. Using the Chinese Remainder lemma and (4.2.1.1), we get

**Corollary 9.2.3.3**  $P \in \mathbf{k}[T]$  is square free if and only if  $\mathbf{k}[T]/(P)$  is a product of fields and more generally, any quotient of  $\mathbf{k}[T]/(P)$  is a product of fields

Notice that lemma 9.2.3.1 implies that the existence of decomposition into irreducible elements is very often automatic, but, unfortunately, is more or less useless without uniqueness. For example, according to the above, the ring  $\mathbf{R}[T_1, T_2]/(T_1^2 - T_2^3)$  is Noetherian, obviously integral (exercise). But  $T_1$  and  $T_2$  are irreducible in the quotient and the element  $T_1^2 = T_2^3$  of the quotient has two distinct decompositions (exercise).

**Remark(s) 9.2.3.4** The ring  $\overline{\mathbf{Z}}$  of complex algebraic integers over  $\mathbf{Z}$  has no irreducible element and therefore is neither Noetherian (that we already know, see 5.3.3) nor UFD. We already know that  $\overline{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$  therefore  $\overline{\mathbf{Z}}$  is not a field (because  $1/2 \notin \overline{\mathbf{Z}}$  for instance). If  $\overline{\mathbf{Z}}$  were Noetherian or UFD, there would exist at least one irreducible element  $p$  (9.2.3.1). But  $\sqrt{p}$  is cancelled by  $T^2 - p \in \overline{\mathbf{Z}}[T]$  and therefore  $\sqrt{p} \in \overline{\mathbf{Z}}$  (4.4.2.3). The formula  $p = (\sqrt{p})^2$  contradicts the irreducibility of  $p$ .

## 9.3 GCD, LCM in UFD

Let  $(x_i)$  be a finite family of nonzero elements of an integral domain  $R$ . Recall that an element  $x \in R^*$  is a GCD of  $(x_i)$  if it is maximal (for the divisibility partial order) among the common divisors to the  $x_i$ . Since  $R$  is a domain, a GCD of a family, if it exists, is defined up to multiplication by a unit. Considering minimal common multiples, we get the notion of LCM. As in the case of integers, we have

**Lemma 9.3.0.1** *If  $R$  is UFD, the GCD and the LCM of  $(x_i)$  exist. Moreover, GCD and LCM are homogeneous : for any  $x \in R^*$ , we have<sup>3</sup>  $\text{GCD}(xx_i) = x \text{GCD}(x_i)$  and  $\text{LCM}(xx_i) = x \text{LCM}(x_i)$*

*Proof.* Let us chose one generator for each ideal generated by an irreducible element and let  $\mathcal{P}$  be the set of all these elements. Then, there is a unique decomposition in a finite product (almost all terms are equal to 1)

$$x_i = u_i \prod_{p \in \mathcal{P}} p^{v_p(x_i)}, \quad u_i \in R^\times$$

and we define

$$\text{GCD}(x_i) = \prod_{p \in \mathcal{P}} p^{\min_i(v_p(x_i))} \quad \text{and} \quad \text{LCM}(x_i) = \prod_{p \in \mathcal{P}} p^{\max_i(v_p(x_i))}$$

which are verified to be suitable. The equality  $v_p(xx_i) = v_p(x) + v_p(x_i)$  gives the homogeneity.  $\square$

Note  $\text{GCD}(x_i)$  is also the greatest common divisor of the family  $(0, x_i)$  allowing to define the GCD for a finite family with at least one non zero element.

## 9.4 Transfer of the UFD property

We now demonstrate the following UFD transfer theorem to polynomial rings

**Theorem 9.4.0.1** *If  $R$  is UFD, then  $R[T]$  is UFD.*

We need to treat both the uniqueness of decompositions (thus Euclid's property) and their existence. For this, we will compare the notion of irreducible elements in  $R[T]$  and  $k[T]$  (where  $k$  is the fraction field of  $R$ ) using the notion of content (due to Gauss). We will look closely at the irreducible decomposition of  $P \in R[T]$  into the UFD ring  $k[T]$  by comparing the irreducibility of  $P$  in  $R[T]$  and  $k[T]$ .

Recall the equality  $(R[T])^\times = R^\times$ , which holds for any domain  $R$  (only because in this case we have  $\deg(PQ) = \deg(P) + \deg(Q)$ , see exercise 2.4.7 for the general case).

### 9.4.1 Gauss' content

In the remainder of this chapter,  $R$  denotes an UFD domain.

<sup>3</sup>Let us again emphasize that GCD, LCM and below contents  $c(P)$  are only defined up to multiplication by a unit. Therefore any equality involving them has to be understood as equality up to multiplication by a unit.

**Definition 9.4.1.1** Let  $P \in R[T]$  be a nonzero polynomial. We define the content  $c(P)$  of  $P$  as the GCD of its coefficients. A polynomial with content  $c(P) = 1$  is said to be primitive.

For example, monic polynomials of  $R[T]$  are primitive. The content is homogeneous of weight 1 with respect to multiplication by nonzero element such as the GCD.

**Theorem 9.4.1.2 (Gauss)** Let  $P, Q$  be nonzero polynomials of  $R[T]$ . Then,  $c(PQ) = c(P)c(Q)$ .

*Proof.* By homogeneity, we may assume  $P, Q$  are primitive and let us prove that  $PQ$  is primitive. Otherwise, let  $p$  be an irreducible of  $R$  dividing  $c(PQ)$ . Since  $R$  is UFD, it satisfies Euclid's lemma: the quotient  $\bar{R} = R/(p)$  is integral. The reduction morphism  $R \rightarrow \bar{R}$  induces a ring morphism  $R[T] \rightarrow \bar{R}[T]$  such that  $0 = \overline{PQ} = \bar{P} \cdot \bar{Q}$ . Since  $\bar{R}[T]$  is an integral domain like  $\bar{R}$ , for example  $\bar{P} = 0$ , i.e.  $p|c(P)$ , a contradiction because  $c(P) = 1$ .  $\square$

**Corollary 9.4.1.3** The irreducible elements of  $R[T]$  are

1. The irreducible elements of  $R$ ;
2. The primitive polynomials of  $R[T]$  that are irreducible in  $\mathbf{k}[T]$ .

*Proof.* Recall the equality  $(R[T])^* = R^\times$ . The first point follows immediately for degree reasons.

Assume now that  $P$  of  $> 0$  degree is irreducible in  $R[T]$ . Then  $P$  is primitive according to the first point. Suppose that  $P$  is the product of two polynomials  $\tilde{P}_1, \tilde{P}_2 \in \mathbf{k}[T]$ . By reducing to a common denominator  $d_i \in R^*$  of the coefficients of  $\tilde{P}_i$ , we can write  $\tilde{P}_i = P_i/d_i$  with  $P_i \in R[T]$ . We then have

$$(*) \quad d_1 d_2 P = P_1 P_2$$

so that  $d_1 d_2 = d_1 d_2 c(P) = c(P_1)c(P_2)$  (homogeneity and multiplicativity of content). Replacing in (\*), we get

$$P = P_1/c(P_1)P_2/c(P_2)$$

with  $P_i/c(P_i) \in R[T]$  by definition of content. Because  $P$  is irreducible in  $R[T]$ , we deduce for example that  $P_1/c(P_1) \in \mathbf{R}[T]^\times = R^\times$ . Therefore,  $\deg(P_1/c(P_1)) = \deg(\tilde{P}_1) = 0$  hence the irreducibility of  $P$  in  $\mathbf{k}[T]$ .

The converse is tautological (who can do more can do less)  $\square$

### 9.4.2 The Transfer theorem

We can now prove the transfer theorem 9.4.0.1.

*Proof.* As before, the defining properties of UFD being invariant under multiplication by a unit, for simplicity we simply write during the proof an equality for an equality up to  $\mathbb{R}^\times$ . We know that  $\mathbb{R}[T]$  is a domain. We just have to prove the existence and uniqueness of decompositions into irreducible elements.

- Existence. Let  $P \in \mathbb{R}[T]$  be non-zero. If  $P$  is a constant  $x \in \mathbb{R}^*$ , we write the decomposition  $x = \prod p_i$  into irreducible factors in  $\mathbb{R}$  and invoke (9.4.1.3). If  $P$  is of degree  $> 0$ , by factoring out a GCD of its coefficients, we can assume  $P$  is primitive. As in the proof of 9.4.1.3, a common denominator argument then allows us to write its decomposition in the principal therefore UFD  $\mathbb{k}[T]$

$$P = \prod P_i/d_i$$

with  $P_i \in \mathbb{R}[T]$  irreducible in  $\mathbb{k}[T]$  and  $d_i \in \mathbb{R}^*$ . By taking the contents, we have  $c(P) = \prod d_i$  and  $P = \prod P_i/c(P_i)$  which is the sought decomposition.

- Uniqueness. Let us show that  $\mathbb{R}[T]$  satisfies Euclid's lemma (9.2.1.2). Suppose that the irreducible polynomial divides the product of  $P_1, P_2 \in \mathbb{R}[T]$ .

If  $P$  is of degree  $> 0$ , it is primitive and irreducible in  $\mathbb{k}[T]$  according to (9.4.1.3). As  $\mathbb{k}[T]$  is UFD since principal,  $P|P_1$  for example (in  $\mathbb{k}[T]$ ) and a common denominator argument allows once more to write  $dP_1 = Q_1 \cdot P$  with  $d \in \mathbb{R}^*$ ,  $Q_1 \in \mathbb{R}[T]$ . By taking the contents we again have  $dc(P_1) = c(Q_1)$  and therefore  $P_1 = c(P_1)Q_1/c(Q_1)P$  and thus  $P$  divides  $P_1$  in  $\mathbb{R}[T]$ .

If  $P$  is a constant  $p \in \mathbb{R}^*$ , then  $p$  is irreducible in  $\mathbb{R}$  and  $\bar{\mathbb{R}} = \mathbb{R}/(p)$  is a domain by Euclid's lemma. Reducing  $P|P_1P_2 \pmod p$  yields  $\bar{P}_1\bar{P}_2 = 0$  in the domain  $\bar{\mathbb{R}}[T]$  hence  $\bar{P}_1 = 0$  or  $\bar{P}_2$  meaning  $P|P_1$  or  $P|P_2$ .

□

For example, a polynomial ring in  $n$  variables over a field or more generally over PID is UFD. But beware, this remarkable stability of the UFD property does not carry over to quotients, as does the property of being Noetherian. The knowledgeable reader will relate this to the notion of non-singularity in geometry.

## 9.5 Irreducibility of the cyclotomic polynomial over $\mathbb{Q}$

From now on, in the rest of this chapter,  $k = \mathbb{Q}$  and  $\Omega = \mathbb{C}$ .

We can take here  $\zeta_n = \exp\left(\frac{2i\pi}{n}\right)$  so that the primitive  $n$ -th roots of unity (in  $\mathbb{C}$ ) are the complex numbers of the form  $\zeta_n^m = \exp\left(\frac{2i\pi m}{n}\right)$ , where  $m \in (\mathbb{Z}/n\mathbb{Z})^*$ .

**Definition 9.5.0.1** We define the  $n$ -th cyclotomic polynomial

$$\Phi_n(T) = \prod_{m \in (\mathbf{Z}/n\mathbf{Z})^*} \left( T - \exp\left(\frac{2i\pi m}{n}\right) \right).$$

Let us show that  $\Phi_n$  is irreducible and has integer coefficients.

**Lemma 9.5.0.2** We have  $\Phi_n(T) \in \mathbf{Z}[T]$ .

*Proof.* Then, every  $n$ -th root of unity has an order  $d$  that divides  $n$ : it is a primitive  $d$ -th root of 1. Conversely, if  $\zeta$  is a primitive  $d$ -th root of 1 with  $d|n$ , it is an  $n$ -th root of 1. We deduce that the set of  $n$ -th roots of 1 is the disjoint union parametrized by the divisors  $d$  of  $n$  of the primitive  $d$ -th roots. As

$$T^n - 1 = \prod_{\zeta \in \mu_n} (T - \zeta),$$

we deduce the formula

$$(i) \quad T^n - 1 = \prod_{d|n} \Phi_d(T).$$

Starting from  $\Phi_1(T) = T - 1 \in \mathbf{Z}[T]$ , we assume by induction on  $d$  that  $\Phi_d$  has integer coefficients according to whatever  $d < n$ . We just have to recall that the quotient of an integer coefficient polynomial by a monic integer coefficients polynomial is an integer coefficient polynomial (1.3.1.1) to conclude this is also true for  $d = n$ .  $\square$

Recall that a complex number is said to be an *algebraic integer* if it is the root of a monic polynomial with integral coefficients. And the roots of 1 are definitely algebraic integers!

**Proposition 9.5.0.3 (Gauss)** Let  $P \in \mathbf{Z}[T]$  be a non-constant monic polynomial.

1. If  $P$  is irreducible in  $\mathbf{Z}[T]$ , it is irreducible in  $\mathbf{Q}[T]$ .
2. If  $P$  is monic, then the monic irreducible factors of the factorization of  $P$  in  $\mathbf{Q}[T]$  have integer coefficients.
3. The minimal polynomial of an algebraic integer has integral coefficients.

*Proof.*

1. Immediate consequence of (9.4.1.3) with  $R = \mathbf{Z}$  ("who can do most can do less").
2. Take an irreducible decomposition  $P = \prod P_i$  in  $\mathbf{Z}[T]$ . Because  $P$  is monic, all the dominant coefficients of the  $P_i$ 's are equal to  $\pm 1$  and we can therefore assume that they are monic. They are therefore primitive hence irreducible in  $\mathbf{Q}[T]$  by (9.4.1.3).

3. Let  $P$  be a monic integral polynomial cancelling  $x \in \overline{\mathbf{Z}}$  and let  $Q$  be an irreducible factor in  $\mathbf{Z}[T]$  cancelling  $x$ . Then,  $\pm Q$  is monic because  $P$  is and  $Q$  is irreducible in  $\mathbf{Q}[T]$  by 9.4.1.3: it is the (monic) minimal polynomial of  $x$  which has therefore integral coefficients.

□

Then:

**Theorem 9.5.0.4** *The cyclotomic polynomial  $\Phi_n$  is irreducible over  $\mathbf{Q}$ .*

The proof, due to Gauss, is very smart.

*Proof.* Let  $P$  be the minimal polynomial of  $\zeta_n$ . It suffices to prove  $\Phi_n | P$ , or that all primitive roots of unity cancel  $P$ .

Let  $p$  be a prime not dividing  $n$  and let  $\zeta$  be a root of  $P$ . Then  $\zeta$  is necessarily a primitive root because  $P | \Phi_n$ . The key is the following lemma.

**Lemma 9.5.0.5**  *$\zeta^p$  is a root of  $P$ .*

*Proof.* Suppose, by contradiction,  $P(\zeta^p) \neq 0$ . Write

$$T^n - 1 = P(T)S(T)$$

with  $S(T) \in \mathbf{Q}[T]$ . Since  $\zeta_n$  is an integer, we have  $P(T) \in \mathbf{Z}[T]$  according to Corollary 9.5.0.3.  $P(T)$  being moreover monic,  $S(T) \in \mathbf{Z}[T]$ . Since  $P(\zeta^p) \neq 0$ , we have  $S(\zeta^p) = 0$ . Thus, the polynomials  $P(T)$  and  $Q(T) = S(T^p)$  have a common complex root. Their GCD (calculated over  $\mathbf{Q}$ ) is therefore non-constant, so that  $P$  divides  $Q$  in  $\mathbf{Q}[T]$  (irreducibility of  $P$ ) and also in  $\mathbf{Z}[T]$  since  $P$  is moreover monic. Reduce modulo  $p$ . We obtain

$$\overline{Q}(T) = \overline{S}(T^p) = (\overline{S}(T))^p$$

using the Frobenius morphism. Since by hypothesis  $n \neq 0$  in  $\mathbf{F}_p$ ,  $T^n - 1$  and its derivative  $nT^{n-1}$  have no common root in  $\overline{\mathbf{F}}_p$ , so that  $T^n - 1$  and  $\overline{P}$  have no common factor in  $\mathbf{F}_p[T]$ . Let  $\Pi$  be an irreducible factor of  $\overline{P}$ . As it divides  $\overline{S}^p$ , it divides  $\overline{S}$ , so that  $\Pi^2 | T^n - 1$  in  $\mathbf{F}_p[T]$ . We obtain a contradiction since  $\overline{P}$  is separable. □

We can now finish the proof of Theorem 9.5.0.4.

Let then  $\zeta$  be a root of  $P$  and  $\zeta'$  be any root of  $\Phi_n$ . We write  $\zeta' = \zeta^m$  with  $\text{GCD}(m, n) = 1$  (because  $\zeta'$  is primitive). By decomposing  $m$  into a product of prime factors, a repeated application of the lemma gives that  $\zeta'$  is a root of  $P$  and therefore  $\Phi_n | P$ . □

## 9.6 Exercices

**Exercise 9.6.1** Let  $K$  be the fraction field of an UFD  $R$ . Show that  $x \in K$  is integral over  $R$  if and only if it belongs to  $R$  (an UFD is integrally closed, see 4.4.2.5).

**Exercise 9.6.2** For which value of  $n$  are the polynomials  $T(T+1)\dots(T+n) \pm 1$  irreducible in  $\mathbf{Q}[T]$ ?

**Exercise 9.6.3** Let  $P \in \mathbf{Z}[T]$  be a monic polynomial and  $p$  a prime number.

1. Show that if  $P \bmod p$  is irreducible in  $\mathbf{Z}/p\mathbf{Z}[T]$ , then  $P$  is irreducible in  $\mathbf{Q}[T]$ .
2. Show that there is only two irreducible polynomials of degree 2 in  $\mathbf{Z}/2\mathbf{Z}[T]$ .
3. Show that  $T^5 - T - 1$  is irreducible in  $\mathbf{Q}[T]$ .

**Exercise 9.6.4** [Eisenstein's criterion] Let  $\mathbf{k}$  be the fraction field of a PID  $R$  and  $P(T) = a_n T^n + a_{n-1} T^{n-1} + \dots + a_1 T + a_0 \in R[T]$ . Assume that there exists  $p \in R$  irreducible such that the following three conditions hold

1.  $p$  divides each  $a_i$  for  $0 \leq i < n$ ,
2.  $p$  does not divide  $a_n$ ,
3.  $p^2$  does not divide  $a_0$ .

Prove that  $P$  is irreducible in  $\mathbf{k}[T]$ .

**Exercise 9.6.5** Let  $R = \mathbf{Z}[2i] = \{a + 2bi \mid a, b \in \mathbf{Z}\} \subset \mathbf{C}$  and  $P_1 = 2iT + 2$ ,  $P_2 = -2iT + 2$ . For  $P \in R[T]$ , we define its content ideal  $c(P) \subset R$  as the ideal generated by its coefficients<sup>4</sup>. Show that  $c(P_1 P_2) \neq c(P_1) c(P_2)$ . Deduce that  $R$  is not UFD.

**Exercise 9.6.6** (Berlekamp's Algorithm) Let  $p$  be a prime number and let  $P \in \mathbf{F}_p[T]$  be a monic polynomial. We write

$$P = \prod_{i=1}^n P_i^{m_i},$$

where each  $m_i > 0$  and the  $P_i$  are distinct, monic, irreducible polynomials. Our goal is to compute this factorization.

1. Explain how computing  $\text{GCD}(P, P')$  allows us to reduce to the case where  $P$  square-free, which we will assume from now on.
2. Show that there is a ring isomorphism  $R = \mathbf{F}_p[T]/(P) \xrightarrow{\sim} \prod_{i=1}^n \mathbf{F}_p[T]/(P_i)$  which is also an isomorphism of  $\mathbf{F}_p$ -vector spaces.
3. Show that the Frobenius morphism  $F : x \mapsto x^p$  of  $R$  is  $\mathbf{F}_p$ -linear and compute  $\dim_{\mathbf{F}_p}(\text{Ker}(F - \text{Id}))$ .

---

<sup>4</sup>This example is due to Kaplanski

4. Deduce from the previous question an effective criterion for testing the irreducibility of a polynomial over a finite field.

Assume  $n > 1$  and let  $Q \in \text{Ker}(F - \text{Id}) - \mathbf{F}_p$ .

5. Let  $Q \in \text{Ker}(F - \text{Id})$ . Show that the following identity holds in  $\mathbf{F}_p[T]$ :  $P = \prod_{\alpha \in \mathbf{F}_p} \text{GCD}(P, Q - \alpha)$ .
6. Show that all of the  $\alpha_i \in \mathbf{F}_p$  (for  $i = 1, \dots, n$ ) are equal if and only if  $Q \in \mathbf{F}_p \subset \mathbf{F}_p[T]/(P)$ .
7. Show that there exists  $\alpha \in \mathbf{F}_p$  such that:  $\text{GCD}(P, Q - \alpha) \neq 1$  and  $\text{GCD}(P, Q - \alpha) \neq P$ .
8. Conclude.

**Exercise 9.6.7** Consider the polynomial  $P(T) = T^4 + 1$  in  $\mathbf{Z}[T]$ . The goal of this exercise is to show that  $P$  is irreducible in  $\mathbf{Z}[T]$ , but reducible mod  $p$  for every prime number  $p$ .

1. Find the roots of  $P$  in  $\mathbf{C}$ , and express  $P$  as a product of two complex polynomials of degree 2 in all possible ways.
2. Deduce that  $P$  is irreducible in  $\mathbf{Z}[T]$ . Is it irreducible in  $(\mathbf{Z}[i])[T]$ ,  $(\mathbf{Z}[\sqrt{2}])[T]$ , and  $(\mathbf{Z}[i\sqrt{2}])[T]$ ?
3. Recall that for any prime number  $p$ , the group  $(\mathbf{Z}/p\mathbf{Z})^*$  is cyclic (6.4.0.2). Show that for every  $p$ , there exists an element  $x \in \mathbf{Z}/p\mathbf{Z}$  such that  $x^2 \in \{-1, 2, -2\}$ .
4. Deduce that for every prime  $p$ , the reduction  $\bar{P} \in (\mathbf{Z}/p\mathbf{Z})[T]$  of  $P$  mod  $p$  is not irreducible.

**Exercise 9.6.8** Let  $R \subset \mathbf{C}[T]$  the ring<sup>5</sup> of complex polynomial  $P$  such that  $P(0) \in \mathbf{R}$ .

1. Show that  $R$  is Noetherian.
2. Show that  $T$  is irreducible in  $R$ .
3. Show that for any  $x \in \mathbf{R}$ , we have  $(x + i)T | T^2$ .
4. Show if  $x, y$  are two distinct real numbers,  $((x + i)T) \neq ((y + i)T)$ .

**Exercise 9.6.9** We keep the notations of 5.3.4. Let  $\xi \in \mathbf{C}$ .

1. Show that  $R$  is an integral domain.
2. Compute  $R^\times$ .
3. Show that the ideal of  $f \in R$  such that  $f(\xi) = 0$  is principal and maximal. What is the quotient field  $R/I_\xi$ ?
4. Show that  $\xi \neq \xi' \Rightarrow I_\xi \neq I_{\xi'}$ .
5. What are the irreducible elements of  $R$ ?

<sup>5</sup>This example comes from D.D. Anderson, D.F. Anderson, M.Zafrullah, Factorization in integral domains, Journal of Pure and Applied Algebra, Volume 69 (1), 1990, 1-19.

6. Show that  $\mathbb{R}$  satisfies Euclide's lemma but that  $\mathbb{R}$  is not a UFD.

**Exercise 9.6.10** We keep the notations of 9.6.9. We "recall" that the set of zeroes of  $f \in \mathbb{R}^*$  is a countable family  $(z_n)$  of  $\mathbb{C}$  with no limit point<sup>6</sup>. Conversely (see [19]), we "recall" Weierstrass' theorem: for any countable family  $(z_n)$  with no limit point and any sequence of integer  $d_n \geq 1$ , there exists  $f \in \mathbb{R}, c_n \in \mathbb{C}^*$  such that

$$f(z) \sim_{z_n} c_n (z - z_n)^{d_n} \text{ and } z \neq z_n \Rightarrow f(z) \neq 0$$

1. Show that any non zero family in  $\mathbb{R}$  has a GCD.
2. Show that any ideal of finite type is principal.
3. Is  $\mathbb{R}$  a PID?
4. What about LCM?

**Exercise 9.6.11** Let  $m, n, x$  be positive integers and  $p$  a prime number dividing the integer  $\Phi_n(x)$ .

1. Compute  $\Phi_n(0)$  and prove  $(a \bmod p) \in (\mathbb{Z}/p\mathbb{Z})^*$ .
2. Show that  $\text{GCD}(T^n - 1, T^m - 1) = T^{\text{GCD}(n,m)} - 1$ .
3. If  $m|n$  and  $m \neq n$ , show that we have  $\Phi_n(T)(T^m - 1) | T^n - 1$  in  $\mathbb{Z}[T]$ .
4. Show  $p|n$  or  $p \equiv 1 \bmod n$  [Look at the order  $m$  of  $(x \bmod p)$  in the multiplicative group  $(\mathbb{Z}/p\mathbb{Z})^*$ ].

Suppose there are only finitely many prime numbers  $p_1, \dots, p_r$  such that  $p_k \equiv 1 \bmod n$  for  $k=1, \dots, r$  and assume  $x = np_1 \cdots p_r$ .

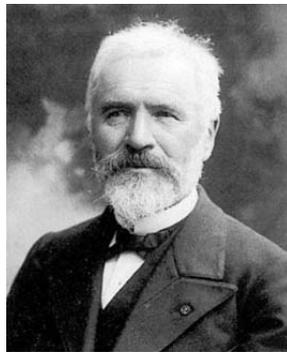
5. Show  $n > 2$  and  $\Phi_n(x) \geq 2$ .
6. Show  $\Phi_n(x \equiv 1 \bmod (p))$ .
7. Conclude.

---

<sup>6</sup>This point is elementary, **exercice**.

# Chapter 10

## Primary decomposition in PID



Camille Jordan

### 10.1 Introduction



**Perspective**

We explain how to decompose torsion modules over PIDs using its their UFD property and the Chinese remainder lemma. We illustrate this result showing how the Frobenius reduction of  $V_a$  immediately leads to Jordan reduction of endomorphisms.

### 10.2 Torsion modules over PID

Let  $M$  be a torsion module ( $M = M_{tors}$ ) over a PID ring  $R$  and let  $\mathcal{P}$  be the set of nonzero prime ideals of  $R$ .



### 10.2.1 Primary decomposition

**Definition 10.2.1.1** Let  $(p) = \mathfrak{p} \in \mathcal{P}$ . The  $\mathfrak{p}$ -primary (or  $p$ -primary) part of  $M$  is the submodule  $M[\mathfrak{p}] = M[p] = \{x \in M \mid \exists n \geq 1 \text{ such that } p^n x = 0\}$ .

Observe that the primary components are functorial in the following sense. For any  $\mathfrak{p} \in \mathcal{P}$ , the diagram

$$\begin{array}{ccc} M[\mathfrak{p}] & \hookrightarrow & M \\ \downarrow & & \downarrow \\ N[\mathfrak{p}] & \hookrightarrow & N \end{array}$$

commutes. In this context, the Chinese remainder lemma (4.5.0.1) gives the following important result.

**Proposition 10.2.1.2** Let  $M$  be module.

1. Assume  $xM = \{0\}$  for some nonzero  $x \in R$ .
  - (a) For all  $j$ , there exists  $\varepsilon_j \in (\prod_{i \neq j} p_i^{v_i})$  such that  $\sum_j \varepsilon_j = 1$ .
  - (b) The natural map  $\bigoplus_{\mathfrak{p} \in \mathcal{P}} M[\mathfrak{p}] \rightarrow M$  is an isomorphism of inverse  $m \mapsto \sum \varepsilon_i m$ .
  - (c) The scalar multiplication by  $\varepsilon_i$  is the projection  $\pi_i : M \xrightarrow{\sim} \bigoplus_j M[p_j] \rightarrow M[p_i] \hookrightarrow M$ .
  - (d) The family of projections  $\pi_i$  is orthogonal (meaning  $\sum \pi_i = \text{Id}_M$  and  $\pi_i \circ \pi_j = \delta_{i,j} \pi_i$ ).
2. Assume  $M$  is torsion. Then the natural map  $\bigoplus_{\mathfrak{p} \in \mathcal{P}} M[\mathfrak{p}] \rightarrow M$  is still an isomorphism.

*Proof.*

- We have  $\text{GCD}(p_i^{v_i}, p_j^{v_j}) = 1$  and therefore (Bézout's theorem)  $I_i + I_j = R$  if  $i \neq j$  with  $I_j = (p_j^{v_j})$ . Then, and (1) is just (5) of the Chinese remainder lemma.
- Because  $M = \bigcup_{x \in R^*} \text{Ann}_M(x)$ , we have  $M[\mathfrak{p}] = \bigcup_{x \in R^*} \text{Ann}_M(x)$ . Applying (1) to each  $\text{Ann}_M(x)$ , the functoriality of primary components gives (2).

□

**Example(s) 10.2.1.3** Let  $a \in \text{End}_k[V]$ .

- Let  $P, Q \in k[T]$  coprime polynomials. Applying 10.2.1.2 to  $V_a$ , we get the famous “kernel lemma”  $\text{Ker}(PQ(f)) = \text{Ker}(P(a)) \oplus \text{Ker}(Q(a))$ .
- If  $\chi_a(T) = \prod_{\lambda \in \text{Spec}(a)} (T - \lambda)^{v_\lambda}$  splits (or equivalently if  $\mu_a$  splits), we have  $\chi_a(T)V_a = \{0\}$  and

$$V_a[T - \lambda] = \bigoplus_{\lambda \in \text{Spec}(a)} \text{Ker}(a - \lambda \text{Id})^{v_\lambda}$$

with spectral projection  $e_\lambda(a) : V_a \rightarrow V_a[T - \lambda]$  belonging to  $k[a]$ . This is the classical “characteristic spaces decomposition”<sup>1</sup>

### 10.2.2 Invariant ideals and primary decomposition

Assume is finite type and torsion. Its invariant ideals  $(d_1) \subset \dots \subset (d_n)$  are nonzero because  $M$  is torsion. Let  $d_1 = \prod_j p_j^{d_{1,j}}$  be a prime irredundant decomposition of  $d_1$  (i.e.  $(p_i) \neq (p_j)$  if  $i \neq j$ ). Then, up to unit, each  $d_i$  can be uniquely written

$$d_i = \prod_j p_j^{d_{i,j}} \text{ with } d_{1,j} \geq d_{2,j} \dots \geq d_{x,j} \geq 0.$$

By definition, we have  $M \xrightarrow{\sim} R/(d_i)$  and the Chinese remainder lemma gives

$$M[p_j] \xrightarrow{\sim} \bigoplus_i R/(p_j^{d_{i,j}}).$$

Conversely, assume that we have some direct sum decomposition

$$M \xrightarrow{\sim} \bigoplus_{i,j} R/(p_j^{d_{i,j}}).$$

Reordering if necessary, we can assume that each sequence  $(\underline{d}_{i,j})_{i \geq 1}$  is decreasing with  $\underline{d}_{i,j} = 0$  for  $i$  large enough. Then, we define

$$\underline{d}_i = \prod_j p_j^{\underline{d}_{i,j}}.$$

The sequence of ideals  $(\underline{d}_i)$  is increasing and its proper terms are the invariant ideals of  $M$ . Graphically, for each prime  $(p_j)$ , we order powers that appear in descending order  $(\underline{d}_{i+1,j} \leq \underline{d}_{i,j})$  in the  $j^{\text{th}}$  column,

$\underline{d}_1 \rightarrow$	$p_1^{\underline{d}_{1,1}}$	$p_2^{\underline{d}_{1,2}}$	$\dots$
$\underline{d}_2 \rightarrow$	$p_1^{\underline{d}_{2,1}}$	$p_2^{\underline{d}_{2,2}}$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

and read off the invariant factors  $\underline{d}_1, \underline{d}_2$ , etc., from the **rows** (starting from the first one).

<sup>1</sup>These terminologies are only French Universal.

### 10.3 Application: Jordan reduction

We retain the previous notations (and remind that a matrix of size  $\leq 0$  is an empty matrix).

Let  $A \in M_n(\mathbf{k})$  and  $\underline{P} = (P_n | \dots | P_1 = \mu_A)$  the similarity invariants of  $A$ . Assume  $\chi_A$ , or equivalently<sup>2</sup>  $\mu_A$ , splits over  $\mathbf{k}$  and denote by  $\Lambda$  the set of its distinct roots. One gets

$$\chi_A(T) = \prod_{\lambda \in \Lambda} (T - \lambda)^{d_\lambda}.$$

If we specialize to the case  $\chi_A = T^n$ , we have  $P_i = T^{d_i}$  with  $d_i \geq 0$  decreasing and  $\sum d_i = n$ .

**Definition 10.3.0.1** *A partition of an integer  $n \geq 0$  is a decreasing sequence  $\underline{d} = (d_i)_{1 \leq i \leq n}$  of non negative integers such that  $\sum d_i = n$ .*

Since each  $P_i$  divides  $\chi_A$ , we have

$$P_i = \prod_{\lambda \in \Lambda} (T - \lambda)^{d_{\lambda,i}} \text{ where } \underline{d}_\lambda = (d_{\lambda,i})_i \text{ is a partition of } d_\lambda.$$

The primary decomposition of the Frobenius decomposition of  $V_A$  implies

$$V_A[T - \lambda] = \text{Ker}(a - \lambda \text{Id})^{d_\lambda} \xrightarrow{\sim} \oplus_i \mathbf{k}[T]/((T - \lambda)^{d_{\lambda,i}})$$

and

$$V_A \xrightarrow{\sim} \oplus_\lambda \oplus_i \mathbf{k}[T]/((T - \lambda)^{d_{\lambda,i}}).$$

Let  $\mathcal{B}_{\lambda,i} = ((T - \lambda_j) \bmod (T - \lambda)^{d_{\lambda,i}})_{j < d_{\lambda,i}}$ . It is a  $\mathbf{k}$ -basis of  $\mathbf{k}[T]/((T - \lambda)^{d_{\lambda,i}})$ . The formula

$$T(T - \lambda)^j = (T - \lambda)^{j+1} + \lambda_j(T - \lambda)^j$$

ensures that the matrix  $\text{Mat}_{\mathcal{B}_{\lambda,i}}(T)$  the multiplication by  $T$  on  $\mathbf{k}[T]/((T - \lambda)^{d_{\lambda,i}})$  is  $\lambda + J_{d_{\lambda,i}}$

$$J_m = C(T^m) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in M_n(\mathbf{k})$$

is the standard Jordan block of size  $m$ . Using 10.2.2, we get

**Theorem 10.3.0.2 (Jordan Reduction)** *Under the above assumptions and notations above, we have with*

$$\chi_A(T) = \prod_{\lambda \in \Lambda} (T - \lambda)^{d_\lambda}$$

<sup>2</sup>see 8.2.2.2

1.  $A$  is similar to a unique diagonal matrix  $\text{diag}(\lambda + J_{d_{i,\lambda}})$  with for every  $\lambda$  the sequence  $(d_{i,\lambda})_i$  being a partition of  $d_\lambda$ .
2. In particular, if  $\chi_A = T^n$  (i.e.,  $A$  is nilpotent), there exists a unique partition  $\underline{d} = (d_i)$  of  $n$  verifying  $A$  is similar to the diagonal block matrix  $J_{\underline{d}} = \text{diag}(J_{d_n}, \dots, J_{d_1})$ . The similarity invariants of  $A$  are  $T^{d_n}, T^{d_{n-1}}, \dots, T^{d_1}$ .

### 10.3.1 Examples

(1) The elementary divisors of the Jordan reduction

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

(where  $\lambda \neq \mu$ ), are

$$\begin{aligned} & (T - \lambda)^2 \quad (T - \mu) \\ & (T - \lambda)^2 \\ & (T - \lambda). \end{aligned}$$

The similarity invariants are thus

$$(T - \lambda), (T - \lambda)^2, (T - \lambda)^2(T - \mu).$$

(2) If  $M = \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$ , we have

$$TI - M = \begin{pmatrix} T & -4 & -2 \\ 1 & T + 4 & 1 \\ 0 & 0 & T + 2 \end{pmatrix}.$$

Let's perform elementary operations according to the algorithm - or rather its outline - described in the proof of the proposition 6.3.1.2 :

$$\begin{array}{ccc}
\begin{pmatrix} T & -4 & -2 \\ 1 & T+4 & 1 \\ 0 & 0 & T+2 \end{pmatrix} & \xrightarrow{L_1 \leftrightarrow L_2} & \begin{pmatrix} 1 & T+4 & 1 \\ T & -4 & -2 \\ 0 & 0 & T+2 \end{pmatrix} \\
\begin{array}{c} \xrightarrow{L_2 \rightarrow L_2 - TL_1} \\ \\ \xrightarrow{L_2 \rightarrow L_2 + L_3} \end{array} & \begin{pmatrix} 1 & T+4 & 1 \\ 0 & -4 - T(T+4) & -2 - T \\ 0 & 0 & T+2 \end{pmatrix} & \begin{array}{c} \xrightarrow{C_2 \rightarrow C_2 - (T+4)C_1} \\ \xrightarrow{C_3 \rightarrow C_3 - C_1} \\ \\ \xrightarrow{C_1 \leftrightarrow C_2} \\ \xrightarrow{L_1 \leftrightarrow L_2} \end{array} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & (T+2)^2 & -2 - T \\ 0 & 0 & T+2 \end{pmatrix} \\
& & & \begin{pmatrix} 1 & 0 & 0 \\ 0 & (T+2)^2 & 0 \\ 0 & 0 & T+2 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & T+2 & 0 \\ 0 & 0 & (T+2)^2 \end{pmatrix}.
\end{array}$$

The similarity invariants are thus  $T + 2$  and  $(T + 2)^2$  and the Jordan reduction is  $\begin{pmatrix} -2 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$ . An

endomorphism with matrix  $M$  is not cyclic.

(3) If  $M = \begin{pmatrix} 3 & 1 & 0 & 0 \\ -4 & -1 & 0 & 0 \\ 6 & 1 & 2 & 1 \\ -14 & -5 & -1 & 0 \end{pmatrix}$ , we obtain as the reduction for  $T I - M$  the matrix

$$\begin{pmatrix} (T-1)^2 & 0 & 0 & 0 \\ 0 & (T-1)^2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The invariant factors are  $(T - 1)^2$  and  $(T - 1)^2$ , and the Jordan reduction is  $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ . An endomorphism with matrix  $M$  is not cyclic.

(4) An endomorphism is cyclic if and only if, for each eigenvalue, there is only one Jordan block.

## 10.4 Exercises

**Exercise 10.4.1** Find the Jordan reduction of the following matrices:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 & -1 \\ -3 & 3 & 1 & -3 \\ -2 & 1 & 2 & -2 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

**Exercise 10.4.2** What are the primary parts of  $(\mathbf{Q}^5)_A$  for  $A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$ ?

**Exercise 10.4.3** Let  $M \in M_n(\mathbf{k})$  be a nilpotent matrix.

1. Show that  $\text{rk}(M) = n - 1$  if and only if the Jordan reduction is  $J_n$ .
2. If  $\mathbf{k} = \mathbf{R}$ , show that the set of nilpotent matrices of rank  $n - 1$  is the largest open set of the set of nilpotent matrices on which the Jordan reduction is continuous (with the topology defined by a norm on  $M_n(\mathbf{R})$ ).
3. Show that  $\text{rk}(M) = n - 2$  if and only if  $M$  has exactly two Jordan blocks  $J_p, J_{n-p}$  where  $p$  is the index of nilpotency of  $M$ . Show that  $p \geq n/2$ .
4. Let  $p \geq n/2$ , an integer  $q = n - p$ , and set for  $t \in \mathbf{k}$ , let  $M_t = \text{diag}(J_p, J_q) + tE_{p+q,p}$  (adding  $t$  at the bottom of the  $p$ -th column). Calculate the index of nilpotency of  $M_t$  depending on  $t$ . Deduce that the Jordan reduction of  $M_t$  is  $\text{diag}(J_{p+1}, J_{q-1})$  if  $t \neq 0$  and  $\text{diag}(J_p, J_q)$  otherwise.
5. Assume  $\mathbf{k} = \mathbf{R}$ . What is the set of continuity of the Jordan reduction application restricted to the subset of nilpotent matrices of rank  $n - 2$  (with the topology defined by a norm on  $M_n(\mathbf{R})$ )?

**Exercise 10.4.4**

1. How many similarity classes are there of matrices  $A \in M_8(\mathbf{k})$  such that  $\text{Im } A = \text{Ker } A$ ?
2. How many similarity classes are there of nilpotent matrices  $A \in M_5(\mathbf{k})$  such that the rank of  $A^2$  is 2?
3. How many similarity classes are there of nilpotent matrices  $A \in M_9(\mathbf{k})$  such that the rank of  $A^3$  is 5?

**Exercise 10.4.5** Let  $A \in M_n(\mathbf{k})$  and  $x \neq 1$  (we assume  $\text{Card}(\mathbf{k}) > 2$ ). Show that  $A$  and  $xA$  are similar if and only if  $A$  is nilpotent. Deduce an example of a pair of nilpotent commuting matrices in  $M_2(\mathbf{k})$  which do not admit a common Jordan basis (compare with (12.2.0.2) below).

**Exercise 10.4.6** Let  $M$  be a complex invertible matrix. Show that  $M$  generates a compact subgroup of  $\text{GL}_n(\mathbf{C})$  if and only if  $M$  is diagonalizable with module 1 eigenvalues.

**Exercise 10.4.7** Let  $\mathbf{k}$  be the field of real or complex numbers. Let  $M$  be the  $\mathbf{k}[T]$ -module  $= \mathbf{k}(T)/\mathbf{k}[T]$  where  $\mathbf{k}(F) = \text{Frac}(\mathbf{k}[T])$ . Let  $r(T) = P(T)/Q(T) \in \mathbf{k}(T)$  with  $\text{GCD}(P, Q) = 1$ .

1. Let  $z \in \mathbf{k}$ . Show that  $(T - z)^{-n}, n \geq 0$  is a basis of the  $(T - z)$ -primary part of  $M$ .
2. If some denominator  $Q$  is split, show that there exists a unique decomposition

$$r(T) = E(T) + \sum_{z,n} \frac{\lambda_{z,n}}{(T - z)^n}$$

where  $(\lambda_{z,n})$  is an almost zero family of  $\mathbf{k}$  and  $E(T) \in \mathbf{R}$ .

Assume  $\mathbf{k} = \mathbf{R}$ .

3. Let  $\tau(T) = T^2 + aT + b \in \mathbf{R}$  with  $a^2 - 4b < 0$ . Show that  $1, T, \tau, T\tau, \tau^2, T\tau^2, \dots$  is a basis of the  $\tau$ -primary part of  $M$ .
4. Show that there exists a unique decomposition

$$r(T) = E(T) + \sum_{z,n} \frac{\lambda_{z,n}}{(T - z)^n} + \sum_{\tau,n} \frac{\lambda_\tau + \mu_\tau T}{\tau(T)^n}$$

where  $E(T) \in \mathbf{R}$  and

$$(\lambda_z, n, \lambda_{\tau,n}, \mu_{\tau,n})$$

is an almost zero family of  $\mathbf{k}^3$  and  $\tau$  runs over the monic degree two polynomials of negative discriminant.

**Exercise 10.4.8** Adapt 10.4.7 to give and prove a Jordan reduction theorem for real matrices.

# Chapter 11

## Semisimplicity



Jorge Luis Borges

“Simplicity// It opens, the gate to the garden/ with the docility of a page/  
that frequent devotion questions and inside, my gaze/ has no need to fix  
on objects/ that already exist, exact, in memory.// I know the customs and  
souls/ and that dialect of allusions/ that every human gathering goes weav-  
ing./ I’ve no need to speak/ nor claim false privilege;/ they know me well  
who surround me here,/ know well my afflictions and weakness.// This is to  
reach the highest thing,/ that Heaven perhaps will grant us:/ not admiration  
or victory/ but simply to be accepted/ as part of an undeniable Reality,/ like  
stones and trees.”

### 11.1 Introduction



#### Perspective

Following Descartes’ philosophy, we are interested in semisimple endomorphisms, the simplest class of endomorphisms generalizing that of diagonalizable endomorphisms. We explain how to canonically decompose any endomorphism into a semisimple part and a nilpotent part reducing somehow the study of square matrices to these two classes.

### 11.2 Semisimple modules

**Definition 11.2.0.1** Let  $\mathcal{M}$  be the set of maximal ideals of  $R$  and  $\mathfrak{m} \in \mathcal{M}$ . Let  $M$  be an  $R$ -module.

1. We define  $M(\mathfrak{m}) = \text{Ann}_M(\mathfrak{m}) = \{m \in M \mid \mathfrak{m}.m = \{0\}\}$  and  $\mathbf{k}(\mathfrak{m}) = R/\mathfrak{m}$  (which is a field by definition).



Ryoan-ji, Kyoto

2.  $M$  is said

- semisimple if every submodule of  $M$  has a complement;
- simple if  $M$  non-zero and has no non-trivial submodules.

3. An endomorphism  $a \in \text{End}_{\mathbf{k}}(V)$  is semisimple if the  $\mathbf{k}[T]$ -module  $V_a$  is.

In this commutative situation, the theory is very... simple. The key lemma is the following.

**Lemma 11.2.0.2** Let  $M$  be a semisimple module and  $N$  a submodule and  $S$  a complement of  $N$ .

1.  $N$  is isomorphic to the quotient  $M/S$  and  $\overline{M} = M/N$  is isomorphic to the submodule  $S$ .
2. Submodules and quotient modules of  $M$  are semisimple.

*Proof.*

1. Clear.
2. Enough to prove that  $M/N$  is semisimple by (1). Let  $\pi : M \rightarrow \overline{M}$  be the canonical surjection and  $S'$  a complement of  $\pi^{-1}(\overline{N})$  in  $M$ . Then  $\pi(S')$  is a complement of  $\overline{N}$  in  $\overline{M}$  (**check !**).

□

**Example(s) 11.2.0.3** If  $R$  is a field, recall that any vector space has a basis and that any subvector space has a complement obtained by complementing a given basis. It follows that in this field case any module is definitely semisimple and simple modules are dimension 1 vector spaces.

If  $p$  is irreducible in a UFD,  $R/(p^2)$  is certainly not semisimple: if  $pR/(p^2) \xrightarrow{\sim} R/(p)$  had a complement  $S$ , we would have  $R/(p^2) \xrightarrow{\sim} R/(p) \oplus S \xrightarrow{\sim} R/(p) \oplus R/(p)$ . In particular,  $R/(p^2)$  would be canceled by  $p$ , which is not the case.

Let us observe that,  $(\mathfrak{m})$  canceling  $M(\mathfrak{m})$ , the  $R$ -module structure on  $M$  defines a canonical  $\mathfrak{k}(\mathfrak{m})$ -vector space structure on  $M(\mathfrak{m})$ . In particular,  $M(\mathfrak{m})$  is semisimple no matter the properties of  $M$  itself.

**Proposition 11.2.0.4** *Let  $M$  be an  $R$ -module. Then,  $M$  is semi simple if and only if the natural morphism  $\bigoplus_{\mathfrak{m} \in \mathcal{M}} M(\mathfrak{m}) \rightarrow M$  is an isomorphism. In particular,*

1. *Up to isomorphism,  $\{\mathfrak{k}(\mathfrak{m}), \mathfrak{m} \in \mathcal{M}\}$  is the set of all simple modules.*
2.  *$M$  is semisimple module if and only if it is a direct sum of simple modules.*

*Proof.* Let us observe that  $\bigoplus_{\mathfrak{m} \in \mathcal{M}} M(\mathfrak{m}) \rightarrow M$  is injective without any hypothesis on  $M$ . Let  $(m_{\mathfrak{m}} \in M(\mathfrak{m}))_{\mathfrak{m} \in F}$  be a finite family such that  $\sum_F m_{\mathfrak{m}} = 0$  (\*). Let  $I = \prod_{\mathfrak{m} \in F} \mathfrak{m}$  and  $e_{\mathfrak{m}} \in R/I$  be the complete family of idempotents the Chinese remainder lemma 4.5.0.1. The action of  $R$  on  $\bigoplus_{\mathfrak{m} \in F} M(\mathfrak{m})$  factors through  $R/I$  and we have  $e_{\mathfrak{m}} m_{\mathfrak{m}'} = \delta_{\mathfrak{m}\mathfrak{m}'} m_{\mathfrak{m}}$  for all  $\mathfrak{m}, \mathfrak{m}' \in F$ . Multiplying (\*) by each  $e_{\mathfrak{m}}$  we get  $m_{\mathfrak{m}} = 0$  for all  $\mathfrak{m} \in F$  hence the injectivity.

Assume  $M$  is semisimple and let us turn to the surjectivity. Let  $S$  be a complement of (the image of)  $\bigoplus_{\mathfrak{m} \in \mathcal{M}} M(\mathfrak{m})$  in  $M$ . If  $S \neq \{0\}$ , let  $s \in S - \{0\}$  and  $\mathfrak{m} \in \mathcal{M}$  containing  $J = \text{Ann}_R(s)$  (Krull's lemma 1.3.2.4). Then  $R_s$  is semisimple (11.2.0.2) and isomorphic to  $R/J$  which is also semisimple (11.2.0.2 again). But  $\mathfrak{k}(\mathfrak{m}) = R/(\mathfrak{m})$  is a quotient of  $R/J = R_s$  and therefore isomorphic a submodule of  $R_s \subset S$ . But the image of 1 in  $S$  is canceled by  $(\mathfrak{m})$  and therefore belongs to  $M(\mathfrak{m})$ , a contradiction.

Conversely, assume  $\iota : \bigoplus_{\mathfrak{m} \in \mathcal{M}} M(\mathfrak{m}) \rightarrow M$  is surjective and let  $N$  be a a submodule of  $M$ . Because  $N(\mathfrak{m}) = N \cap M(\mathfrak{m})$ , the injection  $\bigoplus_{\mathfrak{m} \in \mathcal{M}} N(\mathfrak{m}) \rightarrow \bigoplus_{\mathfrak{m} \in \mathcal{M}} M(\mathfrak{m})$  is surjective because  $\iota$  is. Let  $S_{\mathfrak{m}}$  be any complement of  $N(\mathfrak{m})$  in  $M(\mathfrak{m})$  as  $\mathfrak{k}(\mathfrak{m})$ -vector spaces. Then  $S = \bigoplus_{\mathfrak{m} \in \mathcal{M}} S_{\mathfrak{m}}$  with its canonical  $R$ -module structure is a complement of  $N$  in  $M$ .

Using (again) the existence of basis of vector spaces, the rest of the proposition follows. □

**Remark(s) 11.2.0.5**

- *It follows that every semisimple module is a torsion module (except if  $R$  is a field).*
- *If  $R$  is a field any module is semisimple : this the existence of complement of vector spaces which is at the earth of the preceding proof and depends on Zorn's lemma.*

- If  $M$  is of finite type, semisimple modules are Noetherian modules thanks to 11.2.0.2. The reader will check by himself (*exercise*) that the use of Zorn's lemma is unnecessary in this case (which would be sufficient for our purpose).

Let us recall (8.2.2.2) the canonical isomorphism of  $\mathbf{k}$ -algebras

$$\mathbf{k}[\mathbf{T}]/(\mu_a) \xrightarrow{\sim} \mathbf{k}[a]$$

and (8.2.1.3) the (non canonical) isomorphism of  $\mathbf{k}[\mathbf{T}]$ -modules

$$V_a \xrightarrow{\sim} \bigoplus_{i=1}^n \mathbf{k}[\mathbf{T}]/(P_i)$$

where  $P_n | \dots | P_1 = \mu_a$  are the similarity invariants of  $a$ .

**Corollary 11.2.0.6** *Let  $a \in \text{End}_{\mathbf{k}}(V)$  with  $V$  of finite dimension. The following conditions are equivalent.*

1.  $a$  is semisimple.
2.  $\mu_a$  is square free in  $\mathbf{k}[\mathbf{T}]$ .
3.  $\mathbf{k}[a]$  is a (finite) product of fields containing  $\mathbf{k}$ .
4.  $\mathbf{k}[a]$  is reduced<sup>1</sup>

*In particular, diagonalizable endomorphisms are semisimple.*

*Proof.*

(1)  $\Rightarrow$  (2). If  $P_1 = \mu_a$  is divisible by a square  $P^2$  of some irreducible polynomial  $P$ , the quotient  $\mathbf{k}[\mathbf{T}]/(P^2)$  of  $V_a$  is not semisimple (11.2.0.3) and therefore  $V_a$  neither.

(2)  $\Rightarrow$  (3). Because  $\mathbf{k}[\mathbf{T}]/(\mu_a) \xrightarrow{\sim} \mathbf{k}[a]$ , 11.2.0.3 gives the result.

(3)  $\Rightarrow$  (4). A product of fields has no nilpotent elements.

(4)  $\Rightarrow$  (1). If  $\mathbf{k}[\mathbf{T}]/(\mu_a) \xrightarrow{\sim} \mathbf{k}[a]$  is reduced, then  $\mu_a$  is square free (if  $\mu_a$  is divisible by  $P^2$ , then the square of the non zero element  $\mu_a/P \bmod (\mu_a)$  is zero). Therefore, all similarity invariants  $P_i$  are square free because they divide  $\mu_a$  implying that  $\mathbf{k}[\mathbf{T}]/(P_i)$  is a product of fields (11.2.0.3), and so is  $V_a \xrightarrow{\sim} \bigoplus \mathbf{k}[\mathbf{T}]/(P_i)$  which is therefore semisimple by 11.2.0.4.

□

<sup>1</sup>A ring is reduced if 0 is the only nilpotent element, i.e. if it is the only element which has a positive power equal to 0.

**Example(s) 11.2.0.7** If  $\mu_a$  splits, semisimple means diagonalizable. More generally, if  $\text{GCD}(P, P') = 1$  then  $P$  is square free. Therefore,  $\text{GCD}(\mu_a, \mu'_a) = 1 \Rightarrow a$  is semisimple. The converse being true for characteristic zero or more generally for perfect fields (11.3.0.4). This (partly) explains why semisimplicity is the appropriate generalization of diagonalizability if  $\mu_a$  is non split. We will discuss in full details this topic and more generally the diagonalizable endomorphisms in the next chapter.

### 11.3 «Reminder» on perfect fields

On a general field  $K$ , it may happen that a polynomial without squared factors has multiple roots in a larger field. For example, this is the case with  $T^2 + t$  in  $K = \mathbf{F}_2(t)$ , the fraction field (3.10.3) of the polynomial ring  $\mathbf{F}_2[t]$  [ $t$  is assumed to be transcendental over  $\mathbf{F}_2$ ]. This does not occur for perfect fields.

**Definition 11.3.0.1** Let  $R$  be a ring and  $p \geq 0$  the generator of the ideal  $\{n \in \mathbf{Z} \mid n \cdot R = \{0\}\} = \{n \in \mathbf{Z} \mid n \cdot 1_R = 0\}$ . If  $p = 0$  or if  $p$  is a prime number<sup>2</sup>, we say that  $p$  is the characteristic of  $R$ .

In particular,  $R$  is of characteristic  $p$  if and only if  $\mathbf{Z}/p\mathbf{Z}$  embeds in  $R$  (notice that this embedding is unique). In particular, a field  $k$  is of characteristic  $p$  if  $\mathbf{Q} \subset k$  ( $p = 0$ ) or  $\mathbf{F}_p \subset k$  ( $p$  prime and  $\mathbf{F}_p$  the finite field  $\mathbf{Z}/p\mathbf{Z}$ ).

**Proposition 11.3.0.2** Let  $R$  be a ring with positive characteristic  $p$ . Then, the application  $F : x \mapsto x^p$  is a ring morphism called the Frobenius morphism. If  $R$  is moreover a domain (for instance a field),  $F$  is injective.

*Proof.*  $F$  certainly preserves product and unit element. For addition, recall the well-known divisibility  $p \mid \binom{p}{n}$  for  $1 \leq n \leq p - 1$ . Then, for  $x, y \in R$ , we have by Newton's formula

$$F(x + y) = (x + y)^p = x^p + \sum_{n=1}^{p-1} \binom{p}{n} x^n y^{p-n} + y^p = F(x) + F(y)$$

Assume moreover  $R$  is a domain and  $x \in \text{Ker}(F)$ . We have  $x^p = 0$  and therefore  $x = 0$  hence the injectivity.  $\square$

<sup>2</sup>If  $p$  is composite, the notion of characteristic is useless. Observe that the characteristic of a domain is always defined (exercise).

**Definition 11.3.0.3** A field  $\mathbf{k}$  of characteristic  $p$  is said to be perfect if  $p = 0$  or if every  $x \in \mathbf{k}$  admits a (necessarily unique)  $p$ -th root  $x^{1/p}$ , i.e. if its Frobenius morphism is an isomorphism.

Thus, any algebraically closed field or any finite field is perfect (since an injection between finite sets is bijective). We have to prove the following statement.

**Lemma 11.3.0.4** Let  $\mathbf{k}$  be a perfect field and  $P \in \mathbf{k}[T]$ .

- Then,  $P$  is square-free if and only if  $\text{GCD}(P, P') = 1$ . In particular, if  $P$  irreducible, then  $\text{GCD}(P, P') = 1$ .
- If  $K$  is a field containing  $\mathbf{k}$ , then  $A \in M_n(\mathbf{k})$  is semisimple if and only if it is semisimple in  $M_n(K)$ . In particular,  $A$  is semisimple if and only if  $A$  is diagonalizable in  $M_n(\Omega)$  for some algebraically closed  $\Omega$  containing  $\mathbf{k}$ .

*Proof.* The second item follows from the first and the invariance of the GCD from  $\mathbf{k}[T]$  to  $K[T]$ .

The direction  $\Leftarrow$  immediately follows from Bézout's identity. Let's consider the direct direction. Suppose  $P$  is without squared factors and write  $P = \prod P_i$  with  $P_i$  irreducible. If  $\text{GCD}(P, P') \neq 1$ , one of the  $P_i$  divides  $P' = \sum_i P'_i \prod_{j \neq i} P_j$  and thus  $P_i | P'_i$ . By comparing degrees, we have  $P'_i = 0$ . This implies that the characteristic of  $\mathbf{k}$  is a prime number  $p$  and that all coefficients of  $P_i$  of indices not multiples of  $p$  are zero:  $P_i = \sum_n a_{np} T^{np}$ . But in this case, we have  $P_i = (\sum_n a_{np}^{1/p} T^n)^p$ , the Frobenius of  $\mathbf{k}[T]$  being a ring morphism because  $p\mathbf{k}[T] = \{0\}$ , a contradiction with the irreducibility of  $P_i$ .  $\square$

This corollary is false in the non perfect case.

**Remark(s) 11.3.0.5** When the base field  $K$  is not perfect, there are semisimple matrices over  $K$  which, considered in an overfield, are no longer semisimple. With the notations of 11.3, this is the case with  $A = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix}$  over  $K = \mathbf{F}_2(t)$  because  $\chi_A(T) = T^2 + t$  is irreducible over  $K$  but not over  $K(t^{1/2}) = K[\tau]/(\tau^2 - t)$  and a fortiori over  $\Omega \supset K$ . Moreover,  $A + t^{1/2} \text{Id}$  is even nilpotent! The correct notion in the non-perfect case is that of absolute simplicity defined by the condition  $\text{GCD}(\mu_a, \mu'_a) = 1$ , a condition which is stronger than semisimplicity.

**Exercise 11.3.1** Let  $V$  be a  $\mathbf{k}$ -vector space of finite dimension and  $\varphi$  an automorphism of  $\mathbf{k}$ . Denote  $[\varphi] \otimes V$  as the vector space with underlying group  $V$  and external law  $\lambda \cdot_{[\varphi]} v = \varphi(\lambda)v$ . Show  $\dim(V) = \dim([\varphi] \otimes V)$ . Deduce that any field of finite dimension over a perfect field is still perfect.

### 11.3.2 Sums of semisimple endomorphisms

The next lemma is a generalization of the classical diagonalizability result for two commuting diagonalizable endomorphisms (result which will be discussed in the next chapter). In our context, one has to be a little bit cautious.

**Lemma 11.3.2.1** *Let  $a, b \in \text{End}_{\mathbf{k}}(V)$  which commutes and let  $P \in \mathbf{k}[T_1, T_2]$ . Assume  $a$  is semisimple and  $\text{GCD}(\mu_a, \mu_b) = 1$  (in the perfect case, this is equivalent to  $a, b$  semisimple by 11.3.0.4). Then  $P(a, b)$  is semisimple. In particular  $a + b$  is semisimple.*

*Proof.* Because  $\mathbf{k}[P(a, b)] \subset \mathbf{k}[a, b] \subset \text{End}_{\mathbf{k}}(V)$ , its enough to show that  $\mathbf{k}[a, b]$  is reduced. But the  $\mathbf{k}$ -algebra surjective morphism  $\mathbf{k}[T_1, T_2] \rightarrow \mathbf{k}[a, b]$  defined by  $T_1 \mapsto a, T_2 \mapsto b$  factors through

$$R = \mathbf{k}[T_1, T_2]/(\mu_a(T_1), \mu_b(T_2)) = \mathbf{k}[a][T_2]/(\mu_b(T_2))$$

But  $\mathbf{k}[a]$  is a finite product of fields  $K_i$  (containing  $\mathbf{k}$ ) by 11.2.0.6. Because the GCD does not depends on the subfield where it is calculated by Euclide's algorithm,  $\mu_b$  is also square free in  $K_i[T_2]$  and

$$R = \prod K_i[T_2]/(\mu_b(T_2))$$

is therefore a product of fields implying that its quotient  $\mathbf{k}[a, b]$  is reduced by 11.2.0.3.  $\square$

## 11.4 Jordan-Chevalley Decomposition

Let's begin with a very important result, although easily demonstrated, which allows the construction of polynomial roots step-by-step (adaptation of Newton's method).

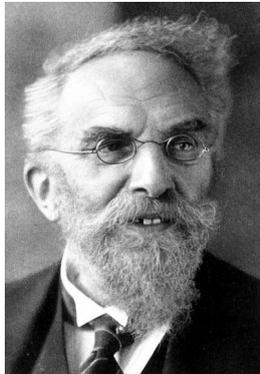
### 11.4.1 Hensel's lemma and existence

**Lemma 11.4.1.1** (Hensel-Newton) *Let  $I$  be a nilpotent ideal ( $I^N = 0$ ) of an arbitrary ring  $R$  and  $P \in R[T]$ . Assume there exists  $x_0 \in R$  such that  $P(x_0) \equiv 0 \pmod{I}$  and  $P'(x_0) \pmod{I}$  is invertible. Then, there exists  $x \in R$  such that  $x \equiv x_0 \pmod{I}$  and  $P(x) = 0$ .*

*Proof.* First, observe that if  $a \pmod{I}$  is invertible, then  $a$  is invertible in  $R$ . Indeed, if  $b \pmod{I}$  is its inverse,  $ab = 1 - i$  with  $i \in I$ . Formally expanding  $1/(1 - i)$  into a series, we deduce that  $1 - i$  is invertible with the inverse  $\sum_{k < N} i^k$  since  $i^k = 0$  for  $k \geq N$  and thus  $b/(1 - i)$  is the inverse of  $a$ .

We will compute (algorithmically) an approximate root

$$x_k \pmod{I^{2^k}} \mid P(x_k) \equiv 0 \pmod{I^{2^k}} \text{ and } x_k \equiv x_0 \pmod{I}$$



*Kurt Hensel*

Kurt Hensel



© Gotlib

Isaac Newton

by successive approximations. Proceed by induction on  $k \geq 0$  (with tautological initialization). Assuming the property holds at rank  $k$ , we then seek  $x_{k+1}$  in the form  $x_k + \varepsilon$ ,  $\varepsilon \in I^{2^k}$  so that  $x_{k+1}$  is indeed an approximation of  $x_k \pmod{I^{2^k}}$ .

The integral Taylor formula for polynomials<sup>3</sup> gives

$$P(x_{k+1}) = P(x_k) + \varepsilon P'(x_k) + \varepsilon^2 Q(x_k, \varepsilon)$$

with  $Q[T, Y] \in R[T, Y]$  (**check this!**). Since  $x_k \equiv x_0 \pmod{I}$ , we have  $P'(x_k) \equiv P'(x_0) \pmod{I}$  and therefore  $P'(x_k)$  is invertible in  $R$  (a representative of an inverse  $\pmod{I^{2^k}}$  would be enough for our purpose). We then set  $\varepsilon = -P(x_k)/P'(x_k)$  which belongs to  $I^{2^k}$  because  $P(x_k) \equiv 0 \pmod{I^{2^k}}$  by induction hypothesis. As  $\varepsilon^2 \in I^{2^{k+1}}$ , this choice is suitable to achieve the induction.

To conclude, we choose  $k$  such that  $2^k \geq N + 1$  and set  $x = x_k$ : the algorithm converges exponentially<sup>4</sup>!

□

**Corollary 11.4.1.2 (Existence)** *Let  $a \in \text{End}_{\mathbf{k}}(V)$  (with  $\mathbf{k}$  a perfect field). There exist  $d, \nu \in \mathbf{k}[a] \subset \text{End}_{\mathbf{k}}[a]$  such that  $a = d + \nu$  and  $d$  semisimple,  $\nu$  nilpotent. In particular,  $d$  and  $\nu$  commute.*

*Proof.* Let  $\pi \in \mathbf{k}[T]$  be the product of the irreducible factors of the minimal  $\mu_a$  of  $a$ . As it is without squared factors, it is coprime with its derivative. Choose  $\alpha, \beta \in \mathbf{k}[T]$  such that  $\alpha\pi + \beta\pi' = 1$ .

<sup>3</sup>Which is a direct consequence of Newton's expansion in this case.

<sup>4</sup>without the usual problems of bad choices of initial values in usual Newton's real method.

Let  $I$  be the ideal  $\pi(a)\mathbf{k}[a]$  of  $\mathbf{k}[a]$ . We have  $\mu_a | \pi^n$  and therefore  $\pi^n(a) = 0$  so that  $I^n = 0$ . Furthermore, we have  $\beta(a)\pi'(a) = 1 \pmod I$  and thus  $\pi'(a) \pmod I$  is invertible. By setting  $x_0 = a \in \mathbf{k}[a]$ , we deduce the existence of  $x \in \mathbf{k}[a]$  such that  $x = a \pmod I$  and  $\pi(x) = 0 \pmod I^n = (0)$ . We then set  $d = x$  and  $\nu = a - P(a)$ . As  $\pi(d) = 0$ ,  $d$  is semisimple. Since  $\nu = a - P(a) \in I$  and  $I^n = 0$  implying that  $\nu$  is nilpotent. □

**Remark(s) 11.4.1.3** *This is essentially Chevalley's proof. Beyond its (very fast) algorithmic character, it is important because it allows the definition of semisimple and nilpotent parts within the context of Lie algebras and algebraic groups (on a perfect field), see for example the excellent [4].*

### 11.4.2 Uniqueness

**Theorem 11.4.2.1** (Jordan-Chevalley) *We still assume  $\mathbf{k}$  is a perfect field. For any  $a \in \text{End}_{\mathbf{k}}(V)$ , there exists a unique pair  $(d, \nu)$  with  $d$  semisimple,  $\nu$  nilpotent,  $d$  and  $\nu$  commuting with  $a = d + \nu$ . Moreover  $d, \nu \in R = \mathbf{k}[a] \subset \text{End}_{\mathbf{k}}[a]$ .*

*Proof.* Only uniqueness requires an argument given the above. Suppose  $d, \nu$  as in the theorem and a pair  $d', \nu' \in \mathbf{k}[a]$  as in Corollary 11.4.1.2. Since  $d, \nu$  commute with each other, they commute with  $d + \nu = a$ . They therefore also commute with  $d', \nu'$  because these are polynomials in  $a$ . But  $d + \nu = d' + \nu'$  i.e.,  $d - d' = \nu' - \nu$ . However,  $\nu' - \nu$  is nilpotent (as a sum of commuting nilpotents) and  $d - d'$  semisimple (as a sum of commuting semisimples, 11.3.2.1); an endomorphism that is both semisimple and nilpotent being zero since its minimal polynomial has no squared factors and divides  $T^n$ , we indeed have  $d = d'$  and  $\nu = \nu'$ . □

A diagonalizable endomorphism  $a$  thus decomposes into  $d = a$  and  $\nu = 0$ . Thus  $a = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$  decomposes into  $a + 0$  and not into  $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$  as one might be tempted to write. Furthermore, the assumption of  $\mathbf{k}$  being a perfect field cannot be relaxed: the matrix  $\begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix}$  from 11.3.0.5 does not have a Jordan-Chevalley decomposition. ◊

If one wants such a decomposition in the imperfect case, one must restrict to endomorphisms with *separable* characteristic polynomials and replace semisimple with absolutely semisimple. The proof is then identical.

### 11.4.3 Similarity class of the components

We retain the previous notation.  $a = d + \nu$ . The invariant factors of the semisimple part  $d$  are entirely determined by  $\chi_a$  since two diagonalizable endomorphisms with the same characteristic polynomials are similar over  $\Omega$  and the invariants do not depend on the base field (cf. 11.6.9). Similarly, the similarity invariants of  $a$  determine the nilpotent type  $\underline{d}_a$  of  $\nu$ . One way to see this is to observe that the nilpotent parts of two similar matrices have similar nilpotent parts by uniqueness of the Jordan-Chevalley decomposition.

### 11.4.4 Appendix: What about the algorithmic nature of the decomposition?

On re-examining the proofs *supra*, it is easy to see that finding  $d$  and  $\nu$  is algorithmic if you know the product  $\pi$  of the different irreducible factors of  $P_n$ . SageMath does this very well thanks to the “factor” command. But what if this command did not exist? In characteristic zero, one is easily convinced of the formula

$$\pi = P_n / \text{GCD}(P_n, P'_n)$$

so the process is algorithmic thanks to Euclid’s GCD algorithm in  $\mathbf{k}[T]$ . In characteristic  $p > 0$  it is more complicated because there are polynomials with a zero derivative: the polynomials in  $T^p$ .

The exercise 11.6.9 provides an “algorithm” to find  $\pi$  for a perfect field of characteristic  $p > 0$ . The quotes are justified by the assumption that the inverse of Frobenius<sup>5</sup>  $F : x \mapsto x^p$  of  $\mathbf{k}$  is known algorithmically.

Regarding Hensel’s lemma, the very writing of the proof is an algorithm that lives in the  $\mathbf{k}[a] \subset M_d(\mathbf{k})$  where  $d = \dim(V)$ . It involves computing the inverse of  $P'(x_n)$  as long as  $2^n < d$ . This is a small number of times, but if the matrices are large, the calculation is heavy. One way to make it easier is to consider the algebraic isomorphism  $k[T]/\mu_a \xrightarrow{\sim} k[a]$  and work within that quotient, which is less computationally demanding.

However, these algorithms are very unstable. For two reasons. The first is that the Gaussian pivot is a numerically unstable algorithm. And working with polynomial coefficients does not help. The second is more serious. As will be seen below, the similarity invariants do not vary continuously with the coefficients of the matrix (see, for example, the theorem 13.2.0.3). Therefore, approximating the values of the coefficients becomes dangerous. If the matrices have rational coefficients or are in finite fields, one can, with great care, control the height of the coefficients and thus work with true equalities. Although these algorithms tend to explode the sizes of the integers involved... In short, a real subject for reflection, one of the motivations that led us to include the topological study of similarity classes in chapter 13.

---

<sup>5</sup>is true for finite fields, for example.

## 11.5 Jordan-Chevalley and spectral projectors

Assume  $\chi_a(T) = \prod (X - \lambda)^{v_\lambda}$  splits giving the primary decomposition (10.2.1.3)

$$V_a = \bigoplus_{\lambda \in \text{Spec}(a)} V_a[T - \lambda] = \bigoplus_{\lambda \in \text{Spec}(a)} \text{Ker}(a - \lambda)^{v_\lambda}$$

The Jordan-Chevalley decomposition  $a = d + \nu$  is simply calculated by

$$d = \sum \lambda e_\lambda(a) \text{ and } \nu = a - d$$

as we have just seen. Matrixwise, if  $\mathcal{B} = \sqcup \mathcal{B}_\lambda$  where  $\mathcal{B}_\lambda$  is a basis of  $\text{Ker}(a - \lambda)^{v_\lambda}$ , we have

$$A = \text{Mat}_{\mathcal{B}}(a) = \text{diag}(\lambda \text{Id} + N_\lambda) \text{ with } N_\lambda \text{ nilpotent}$$

and

$$D = \text{Mat}_{\mathcal{B}}(d) = \text{diag}(\lambda \text{Id}), \quad N = \text{Mat}_{\mathcal{B}}(\nu) = \text{diag}(N_\lambda)$$

Of course, one could even chose a Jordan basis (10.3.0.2) to have nicer form of  $N_\lambda$ .

### 11.5.1 $d$ -th roots in $\text{GL}_n$

An immediate and useful application is the existence of polynomial  $d$ -th roots in the algebraically closed case.

**Proposition 11.5.1.1** *Let  $d$  be an integer  $> 0$  and assume  $\mathbf{k}$  is algebraically closed with characteristic prime to  $d$ . Let  $\chi$  be unitary of degree  $n$ . There exists  $P_{d,\chi} \in \mathbf{k}[T]$  such that for any matrix  $A \in \text{GL}_n(\mathbf{k})$  with  $\chi_A = \chi$  we have  $P_{d,\chi}(A)^d = A$ .*

*Proof.* Since  $\chi(0) \neq 0$ , the polynomials  $\chi$  and  $T$  are coprime and we can write a Bézout identity  $UT + V\chi = 1$  in  $\mathbf{k}[T]$ . With the previous notations, since  $\chi_D = \chi_A = \chi$ , the matrix  $D$  is invertible with inverse  $U(D)$ . Since  $D$  and  $N$  commute,

$$A = D(\text{Id} + D^{-1}N) = D(\text{Id} + U(D)N)$$

with  $D^{-1}N$  being nilpotent. We can then write a  $d$ -th root of  $D$  as

$$D^{1/d} = \sum \lambda^{1/d} e_\lambda(A)$$

which is therefore a polynomial depending only on  $\chi$  and  $d$  evaluated in  $A$ . Furthermore, the coefficients of the power series  $(1 + z)^{1/d}$  are the generalized binomial coefficients  $\binom{1/d}{i}$ ,  $i \geq 0$  and thus are in  $\mathbf{Z}[1/d]$ . Since  $d$  is invertible in  $\mathbf{k}$  and  $(D^{-1}N)^n = 0$ , we have a  $d$ -th root

$$(D^{-1}N)^{1/d} = \sum_{i < d} \binom{1/d}{i} (D^{-1}N)^i$$

which is indeed a polynomial depending only on  $\chi$  and  $d$  evaluated in  $A$  as are  $D^{-1}$  and  $N$ , which is what we wanted.  $\square$

We cannot hope for more. On the one hand, the statement is clearly false in the general case of non-algebraically closed fields, already in the case  $n = 1$ . On the other hand, a non-zero nilpotent matrix  $N$  does not admit a  $d$ -th root. In fact, it would be nilpotent so that its  $n$ -th power would be zero, but also equal to  $n!$

## 11.6 Exercises

**Exercise 11.6.1** Let  $\lambda$  be an eigenvalue of  $a$  and  $d_\lambda$  its multiplicity as root of  $\chi_a$ . Prove  $\dim(a - \lambda \text{Id}) \leq d_\lambda$  (\*). Prove that  $a$  is diagonalizable if and only if  $\chi_a$  splits over  $\mathbf{k}$  with equality in (\*) for all eigenvalues.

**Exercise 11.6.2** Let  $M$  be a complex square matrix of size  $n > 1$ . We denote by  $M_{nil}$  the nilpotent component of its Jordan-Chevalley decomposition. The goal is to give some properties of  $M_{nil}$ . Recall that the exponential of  $M$  is defined by the absolutely convergent series (for any norm on  $M_n(\mathbf{C})$ )

$$\exp(M) = \sum_{k=0}^{\infty} \frac{M^k}{k!}$$

and that the exponential of the sum of two commuting matrices is the product of their exponentials.

1. Compute  $\exp(M)_{nil}$  in terms of  $M_{nil}$  and  $M$ .
2. Show that  $\exp(M)_{nil} = 0$  if and only if  $M_{nil} = 0$ . What can be deduced from this?
3. Show that the set of diagonalizable complex matrices is dense in  $M_n(\mathbf{C})$ .
4. Show that the map  $M \mapsto M_{nil}$  is not continuous on  $M_n(\mathbf{C})$ .
5. What is the set of points of continuity of the map  $M \mapsto M_{nil}$  (Difficult)?

**Exercise 11.6.3** Recall that the exponential of a complex square matrix of  $M$  is defined by the absolutely convergent series (for any norm on  $M_n(\mathbf{C})$ ):

$$\exp(M) = \sum_{k=0}^{\infty} \frac{M^k}{k!}$$

and that the exponential of the sum of two commuting matrices is the product of their exponentials.

1. If  $M \in M_n(\mathbf{R})$ , prove that  $\det(M) \geq 0$ .
2. Show that  $\exp(M_n(\mathbf{R}))$  is the set of square of real matrices.
3. If  $n > 1$ , show that there exists real matrices of size  $n$  with positive determinant but who are not square of any real matrix.

**Exercise 11.6.4** Let  $p$  be prime,  $K$  the fraction field of  $\mathbf{F}_p[T]$  and  $V = K[X, Y]/(X^p - T, Y^p - T)$ . Show that  $V$  is of finite dimension over  $K$  and that the  $K$ -endomorphisms of  $V$  multiplying by  $X$  and  $Y$  respectively are semisimple, commute but their difference is nilpotent (this is exercise 14 chapter VII.5 [6] rewritten without tensor product).

**Exercise 11.6.5** Let  $A, B \in M_n(\mathbf{k})$  be two commuting matrices. Show that the  $\mathbf{k}$ -algebra  $\mathbf{k}[A, B]$  is a quotient of  $\mathbf{k}[T_1, T_2]/(\mu_A, \mu_B)$ . Deduce using 4.5.0.2 that if the minimal of  $A, B$  and their respective derivatives are coprime, any element  $C$  of  $\mathbf{k}[A, B]$  is semisimple (without using 11.3.2.1). Is  $\mu_C$  necessary coprime with its derivative?

**Exercise 11.6.6** Let  $d$  be the semisimple part of  $a$  in its Chevalley-Jordan decomposition. Prove  $\chi_a = \chi_d$ .

**Exercise 11.6.7** Let  $(P_n, \dots, P_1)$  be the similarity invariants of  $a \in \text{End}_{\mathbf{k}}(V)$ . Assume that  $\mathbf{k}$  is perfect. Let  $P_i = \prod_j P_{i,j}^{v_{i,j}}$  be an irredundant decomposition into irreducible factors. Compute the type of the nilpotent part of the Jordan-Chevalley decomposition of  $a$  in terms of  $v_{i,j}$  and  $\deg(P_{i,j})$ . Can you find an effective algorithm to compute this type?

**Exercise 11.6.8** (Hensel's lemma) Let  $I$  be an ideal of  $R$  with  $I^2 = (0)$  and  $P \mapsto \bar{P}$  the canonical morphism  $R[T] \rightarrow R/I[T]$ . Let  $P, Q, \Pi \in R[T]$  be monic polynomials such that

- $\bar{\Pi} = \bar{P}\bar{Q}$
- There is a Bézout relation in  $\bar{R}[T]$

$$(*) \quad \bar{U}\bar{P} + \bar{V}\bar{Q} = 1 \text{ with } U, V \in R[T]$$

The goal is to show that there is factorization of  $\Pi$  in  $R$  lifting  $(*)$  (compare with 11.4.1.1).

1. Show that one can assume  $UP + VQ = 1$ .
2. Show that one can assume  $\deg(U) < \deg(Q)$  and  $\deg(V) < \deg(P)$ .
3. Conclude.

**Exercise 11.6.9** Let  $\mathbf{k}$  be a field and  $\chi = \prod \pi_i^{n_i}$  the decomposition into unitary irreducible factors of  $P$  a unitary polynomial of degree  $n$ . We denote  $\chi_{\text{red}} = \prod \pi_i$ . In the first four questions,  $\mathbf{k}$  is assumed to be a perfect field of characteristic  $p > 0$  and  $I$  the set of indices  $i$  such that  $n_i$  is coprime with  $p$ .

1. Show that  $\chi / \text{GCD}(\chi, \chi') = \prod_{i \in I} \pi_i$ .
2. Show that  $\prod_{i \notin I} \pi_i$  is a  $p$ -th power in  $\mathbf{k}[T]$ .
3. Write an algorithm computing  $\prod_{i \in I} \pi_i$  and  $\prod_{j \notin I} \pi_j^{n_j/p}$ .
4. Deduce an algorithm computing  $\chi_{\text{red}}$ .
5. What is  $\chi_{\text{red}}$  in characteristic zero?

6. Program the algorithm on  $\mathbf{F}_p$ ? On  $\mathbf{F}_{p^n}$ ? On a general perfect field?
7. How to generalize on a non-perfect field?
8. Always for  $\mathbf{k}$  a general field, consider the sequence of polynomials  $\underline{\chi}_{\text{red}} = (\chi_i)_{1 \leq i \leq n}$  defined by  $\chi_1 = \chi_{\text{red}}$ ,  $\chi_{i+1} = (\chi / (\prod_{j \leq i} \chi_j))_{\text{red}}$ . Show that  $\underline{\chi}_{\text{red}}$  is the sequence of invariant factors of the semisimple endomorphisms with characteristic polynomial  $\chi$ .
9. Assuming again  $\mathbf{k}$  perfect and let  $D, N$  be the Jordan-Chevalley decomposition of  $M \in M_n(\mathbf{k})$ . What are the similarity invariants of  $D$  based on the invariants  $\underline{P}$  of  $M$  [Use the previous question]? Can you similarly describe the invariants of  $N$  based on  $P_i$  [Place yourself in  $\bar{\mathbf{k}}$  and study the application  $P_i \mapsto P_i/P_{i,\text{red}}$  and its iterates]? Program the obtained algorithm for example on  $\mathbf{F}_p$ .

**Exercise 11.6.10** Let  $p$  be a prime number and  $\Omega$  be an algebraically closed field containing  $\mathbf{Z}/p\mathbf{Z}$ .

1. Show that a finite subfield of  $\Omega$  has cardinality  $q = p^n$  for some  $n > 0$ .
2. Conversely, show that for any  $n > 0$ , the set  $\mathbf{F}_q$  of roots of  $T^q - T$  in  $\Omega$  is the unique subfield of  $\Omega$  of cardinality  $q$ .

Let  $F$  be the Frobenius morphism of  $\mathbf{F}_q$  with  $q = p^n$ . Let  $x$  be a generator of the cyclic group  $\mathbf{F}_q^*$  (6.4.0.2).

3. Check  $F \in \text{End}_{\mathbf{F}_p}(\mathbf{F}_q)$ .
4. Prove that  $x, F(x), \dots, F^{n-1}(x)$  are pairwise distinct.
5. Using 2.4.9, prove that  $\text{Id}, F, \dots, F^{n-1}$  are linearly independent in  $\text{End}_{\mathbf{F}_p}(\mathbf{F}_q)$ .
6. Prove that the minimal polynomial of  $F$  is  $T^n - 1$ .
7. Prove that  $F$  is a cyclic endomorphism and give its Frobenius reduction.
8. Study the diagonalization/semisimplicity of  $F$ .

# Chapter 12

## Simultaneous reduction

# FURTHER REDUCTION

### 12.1 Introduction



#### Perspective

This chapter gives criteria for simultaneously reducing matrices in simpler forms (diagonal, triangular). These are fundamental tools for understanding the general linear group  $GL_n(\mathbf{k})$ . This topic also allows to introduce the important notion of irreducible action on a *nonzero* finite dimensional  $\mathbf{k}$  vector space  $V$ .

**Definition 12.1.0.1** Let  $\mathcal{A}$  be a nonempty subset of  $\text{End}_{\mathbf{k}}(V)$  (or  $M_n(\mathbf{k})$  for  $V = \mathbf{k}^n$ ). We say that  $\mathcal{A}$  acts irreducibly on  $V$  if the only subspaces which are stable by all elements of  $\mathcal{A}$  are  $\{0\}$  and  $V$ . If  $\mathcal{A}$  is reduced to a single element  $a$ , we say that  $a$  acts irreducibly<sup>1</sup>

The reason to be interested in this notion in our context is the following. If  $W$  is stable by  $\mathcal{A}$ , the maps  $V \xrightarrow{a} V \rightarrow V/W$  factors through  $V/W$  into  $a_{V/W} \in \text{End}_{\mathbf{k}}(V/W)$ . In matrix terms, this simply means that completing a basis of  $W$  in a basis  $\mathcal{B}$  of  $V$ , we have for all  $a \in \mathcal{A}$

$$\text{Mat}_{\mathcal{B}}(a) = \begin{pmatrix} \text{Mat}(a_W) & * \\ 0 & \text{Mat}(a_{V/W}) \end{pmatrix}$$

<sup>1</sup>The most common use of this notion is when  $\mathcal{A}$  is at least stable by product, or even a group or a  $\mathbf{k}$ -sub-algebra of  $\text{End}_{\mathbf{k}}(V)$ .

allowing to do induction on  $\dim(V)$  for statements "passing" to the diagonal blocs. This will be our **"valuable stable space tool"** for various induction arguments.

**Example(s) 12.1.0.2** *The following sets*

1. *act irreducibly:  $\text{End}_{\mathbf{k}}(V)$ , a plane rotation of angle  $\neq 0, \pi$ , the so-called dihedral group  $D_6$  of isometries preserving an equilateral triangle. . . ;*
2. *do not act irreducibly (in dimension  $> 1$ ): the set of upper-triangular matrices, any complex matrix, any real matrix of size  $> 2$ , any commuting sets of complex matrices (see) . . .*

The following formal observation is useful

**Lemma 12.1.0.3**  *$\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$  acts irreducibly on  $V$  if and only if  ${}^t\mathcal{A} = \{{}^t a, a \in \mathcal{A}\} \subset \text{End}_{\mathbf{k}}(V^*)$  acts irreducibly on  $V^*$ .*

*Proof.* Observe that  $W$  is invariant under  $\mathcal{A}$  if and only if its orthogonal  $W^\perp$  is invariant under  ${}^t\mathcal{A}$  (7.7.0.2). □

## 12.2 Commuting family of matrices

The main observation is the following.

**Lemma 12.2.0.1** *If  $a, b \in \text{End}_{\mathbf{k}}(V)$  commute, then any eigenspace of  $a$  is  $b$ -stable.*

*Proof.* Let  $v \in \text{Ker}(a - \lambda \text{Id})$ . One has  $a(b(v)) = b(a(v)) = b(\lambda v) = \lambda b(v)$  proving  $b(v) \in \text{Ker}(a - \lambda \text{Id})$ . □

**Proposition 12.2.0.2** *Let  $\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$  be an arbitrary set of commuting endomorphisms.*

1. *If  $\chi_a$  splits for all  $a \in \mathcal{A}$ , then there exists a common trigonalization basis  $\mathcal{B}$  for  $\mathcal{A}$ .*
2. *If  $a$  is diagonalizable for all  $a \in \mathcal{A}$ , then there exists a common diagonalization basis  $\mathcal{B}$  for  $\mathcal{S}$ .*

*Proof.*

1. Induction on  $\dim(V)$ : by the "valuable stable space tool", one can assume  $\mathcal{A}$  acts irreducibly. By 12.2.0.1, any eigenspace of  $a$  is invariant under  $\mathcal{A}$  and therefore is equal to  $V$  showing that  $a$  is scalar (and  $\dim(V) = 1$ ) which proves (1).

2. We use induction on  $n = \dim(V) \geq 0$ . We may assume that  $n > 0$  and that the statement is true in dimension  $< n$ . If all the  $a_i$  are homotheties  $\lambda_i \text{Id}$ , any base is suitable. Otherwise, let  $i$  such that  $a_i$  is not a homothety. Then,  $a_i$  has at least two distinct eigenvalues so that all its eigenspaces  $E_i(\lambda)$  are of dimension  $< n$ . But they are stable by all the  $a_j$  and their restrictions  $a_j(\lambda)$  to each  $E_i(\lambda)$  are diagonalizable for all  $j$  (8.3.0.1). For each  $\lambda$ , we then choose a common diagonalization base for the  $a_j(\lambda)$  and the union of these bases suits.

□

**Remark(s) 12.2.0.3** *These results are of fundamental importance in group theory. This shows that commutative subgroups of  $\text{GL}_n(\mathbb{C})$  of diagonalizable matrices are conjugate to subgroups of the groups of invertible diagonal matrices the converse being obviously true (this is (2) of the above result). For (1), this shows that commutative subgroups of  $\text{GL}_n(\mathbb{C})$  are conjugate to subgroups of the groups of upper triangular matrices the converse being obviously false. The good generalization of commutative groups is the notion of solvable groups. In this case, one can show that connected solvable subgroups of  $\text{GL}_n(\mathbb{C})$  are exactly connected subgroups of  $\text{GL}_n(\mathbb{C})$  (see 12.5). But the connectedness assumption cannot be dropped (see exercise 12.6.1).*

## 12.3 The Burnside-Wedderburn theorem

This result is important and classical<sup>2</sup>

**Theorem 12.3.0.1** *Let  $\mathcal{A} \subset \text{End}_{\mathbb{k}}(V)$  acting irreducibly on  $V$ . Assume moreover that  $\chi_{\mathcal{A}}$  is split and that  $\mathcal{A}$  is stable by (nonempty) product<sup>3</sup>. Then either  $\mathcal{A} = \{0\}$  or  $\vec{\mathcal{A}} = \text{End}_{\mathbb{k}}(V)$ .*

*Proof.*

- If  $\mathcal{A} = \{0\}$ , observe that  $V$  is a line.
- We can assume  $\mathcal{A} \neq \{0\}$  and, changing  $\mathcal{A}$  to  $\text{Span}(\mathcal{A})$  that  $\mathcal{A}$  is a  $\mathbb{k}$ -algebra (*a priori* without unit). Let  $d = \min\{\text{rk}(a), a \in \mathcal{A} - \{0\}\}$ . We have  $d > 0$  and we will first prove  $d = 1$ .
- Assume  $d > 1$  and let  $\alpha \in \mathcal{A}$  with  $\text{rk}(\alpha) = d$ . One can therefore choose  $x, y \in V$  such that  $\alpha(x)$  and  $\alpha(y)$  are independent. But  $\mathcal{A}.\alpha(x)$  is invariant under  $\mathcal{A}$  and therefore  $\mathcal{A}.\alpha(x) = \{0\}$  or  $\mathcal{A}.\alpha(x) = V$ . In the first case  $\mathcal{A}.\alpha(x) = \{0\}$ , the nonzero line  $\text{Span}(\alpha(x))$  is invariant under  $\mathcal{A}$  and therefore the whole  $V$  contradicting  $d > 1$ .

<sup>2</sup>Our proof is a mild adaptation of the nice note I. Halperin and P. M. Rosenthal, Burnside's theorem on algebras of matrices, Amer. Math. Monthly **87** (1980), no. 10, 810.

<sup>3</sup>The nonempty assumption means that we do not assume  $\text{Id} \in \mathcal{A}$ .

Thus  $\mathcal{A} \cdot \alpha(x) = V$  and we can choose  $a \in \mathcal{A}$  such that  $a(\alpha(x)) = y$  implying that .

Let  $\lambda \in \mathbf{k}$  be an eigenvalue of the restriction of  $\alpha a$  to its stable space  $\text{Im}(\alpha)$  (by hypothesis,  $\chi_{\alpha a}$  splits and so does the characteristic polynomial of  $\alpha a|_{\text{Im}(\alpha)}$ ): we have

$$\text{rk}(\alpha a \alpha - \lambda \alpha) = \dim \text{Im}((\alpha a - \lambda \text{Id})|_{\text{Im}(\alpha)}) < d.$$

But because  $\alpha a \alpha(x)$  and  $\alpha(x)$  independent, we also have  $\text{rk}(\alpha a \alpha - \lambda \alpha)$  contradicting the minimality of  $d$ .

- We have therefore  $d = 1$  and  $\text{Im}(\alpha)$  is a line generated by some  $x \neq 0$ . There exists a nonzero linear form  $\varphi \in V^*$  such that  $\alpha = \varphi \otimes x : v \mapsto \varphi(v)x$  for all  $v \in V$ . By 12.1.0.3, we have  ${}^t\mathcal{A} \cdot \varphi = V^*$ . The formula  $\alpha a(v) = {}^t a(\varphi)(v)x$  show that  $\Psi \otimes x : v \mapsto \Psi(v)x$  belongs to  $\mathcal{A}$  for every  $\Psi \in V^*$ . Analogously, the formulas  $a\Psi \otimes x(v) = \Psi(v)a(x)$  and  $\alpha a(v) = {}^t a(\varphi)(v)x$  show that  $\Psi \otimes y \in \mathcal{A}$  for every  $\Psi \in V^*, y \in V$ . The theorem follows because every rank 1 morphism is of the form  $\Psi \otimes y$  for some  $\Psi \in V^*, y \in V$  [recall that  $E_{i,j} = e_j^* \otimes e_i$  is a basis of  $\text{End}_{\mathbf{k}}(V)$  if  $(e_i)$  is some basis of  $V$ ].

□

## 12.4 Stable family of nilpotent and unipotent matrices

**Theorem 12.4.0.1** (Kolchin) *Let  $\varepsilon \in \{0, 1\}$ . Assume<sup>4</sup>  $\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$  is stable by product and that  $\chi_a(T) = (T - \varepsilon)^n$  for all  $a \in \mathcal{A}$ . Then, then there exists a common trigonalization basis  $\mathcal{B}$  for  $\mathcal{A}$ .*

*Proof.* Because the characteristic polynomial of a block triangular matrix  $a$  above  $\begin{pmatrix} \text{Mat}(a_W) & * \\ 0 & \text{Mat}(a_{V/W}) \end{pmatrix}$  is the product of the characteristic polynomials of the blocks, the "valuable stable space tool" shows that we just have to prove that all element have a (nonzero) common eigenvector, meaning

$$(*) \quad \bigcap_{a \in \mathcal{A}} \text{Ker}(a - \varepsilon \text{Id}) \neq \{0\}$$

Using the "valuable stable space tool" again, we can assume that  $\mathcal{A}$  acts irreducibly on  $V$ .

If  $\mathcal{A} = \{0\}$  we are done (and we have  $\varepsilon = 0$  in this case).

If  $\mathcal{A} \neq \{0\}$ , we have  $\vec{\mathcal{A}} = \text{End}_{\mathbf{k}}(V)$  by 12.3.0.1. In particular we have  $\varepsilon = 1$  giving  $\text{Tr}(a) = n = \text{Tr}(ab)$  for any  $a, b \in \mathcal{A}$ . Therefore,  $\text{Tr}(a(\text{Id} - b)) = 0$  for any  $a \in \mathcal{A}$  and therefore for also any  $a \in \text{End}_{\mathbf{k}}(V)$ . But  $\text{Tr}(AB) = 0$  for any  $A \in M_n(\mathbf{k}) \Rightarrow B = 0$  because  $0 = \text{Tr}(E_{i,j}B) = B_{j,i}$ . This gives  $b = \text{Id}$  for all  $b \in \mathcal{A}$  (and  $n = 1$  but does not matter) hence the common eigenvalue. □

<sup>4</sup>See I. Kaplansky, The Engel-Kolchin theorem revisited, in *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, pp. 233–237, Academic Press, New York-London for some (mild) generalizations.

An endomorphism  $g \in \text{End}_{\mathbf{k}}(V)$  such that  $\text{Spec}(g) = \{1\}$  is called unipotent. A subgroup of  $\text{GL}(V)$  whose elements are unipotent is called unipotent.

**Corollary 12.4.0.2** *Every unipotent subgroup of  $\text{GL}_n(\mathbf{k})$  is contained in a maximal unipotent subgroup which is conjugate to the group of upper triangular matrices with 1 in the diagonal.*

## 12.5 Connected solvable matrix subgroups

This section can be skipped in a first reading. In this section we assume the reader to be familiar with basics of quotient groups.

### 12.5.1 Basics on solvable groups

We will look at a large class of groups which contains the example encountered in this chapter: the commutative groups and all subgroups of the group of triangular matrices.

**Definition 12.5.1.1** A group  $G$  is said to be *solvable* if it has a decreasing sequence of subgroups

$$\{1\} = G_n \subset \cdots \subset G_0 = G$$

such that for  $0 \leq i \leq n-1$ , the group  $G_{i+1} \subset G_i$  is normal in  $G_i$  and the quotient group  $G_i/G_{i+1}$  is commutative.

**Example(s) 12.5.1.2** *Any commutative group is solvable. Any sous-group of the group of invertible upper-triangular matrices is solvable (see 12.5.1.4 and 12.6.4). The groups  $S_3$  and  $S_4$  are non-commutative and solvable (12.6.1).*

Let us characterize solvable groups using the derived subgroup. Recall that the derived subgroup  $DG$  of a group  $G$  is normal and that the quotient  $G/DG$  is the maximal commutative quotient of  $G$ .

**Lemma 12.5.1.3**  *$G$  is solvable if and only if  $D^n G$  is trivial for  $n$  large enough.*

*Proof.* If  $G$  is solvable and  $G_i$  is as in the definition, the image of a commutator in the abelian group  $G_0/G_1$  is trivial so that  $D^1 G$  is contained in  $G_1$ . By induction, we show that  $D^i G$  is contained in  $G_i$  and therefore  $D^n G$  is trivial. Conversely, if  $D^n G$  is trivial, we set  $G_i = D^i G$ .  $\square$

We define for  $G$  solvable its length  $\ell(G) = \min\{i \geq 0 \mid D^i(G) = \{1\}\}$ .

**Corollary 12.5.1.4** *If*

$$1 \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow 1$$

*is exact, then  $G_2$  is solvable if and only if  $G_1$  and  $G_3$  are solvable.*

*Proof.* On the one hand, we have  $D^n G_2 \rightarrow D^n G_3$  surjective and  $D^n G_1 \rightarrow D^n G_2$  injective so that  $G_2$  being solvable implies  $G_1$  and  $G_3$  are solvable. Conversely, if  $D^n G_3$  is trivial, the image of  $D^n G_2$  in  $G_3$  is zero and therefore  $D^n G_2$  is contained in  $G_1$ . If now we also have  $D^m G_1 = 1$ , we deduce  $D^{m+n} G_2 \subset D^m G_1 = 1$ , hence the converse.  $\square$

**Remark(s) 12.5.1.5** *Therefore, the class of solvable groups is the smallest class of subgroups stable by isomorphisms and exact sequences. In fact, we have better. If  $G$  has an increasing sequence of subgroups*

$$1 = G_0 \subset \cdots \subset G_n = G$$

*with  $G_i$  normal in  $G_{i+1}$  and  $G_{i+1}/G_i$  solvable, then  $G$  is solvable.*

## 12.5.2 The Lie-Kolchin theorem

In this section, we assume that  $\mathbf{k}$  is a subfield of  $\mathbf{C}$  which induces a metric topology on  $M_n(\mathbf{k})$  associated to any norm on  $M_n(\mathbf{C})$ . The following theorem is both classical and important.

**Theorem 12.5.2.1** (Lie-Kolchin) *Let  $G \subset GL_n(V)$  be a solvable connected subgroup such that  $\chi_g$  is split for every  $g \in G$ . There exists a common trigonalization basis  $\mathcal{B}$  for  $G$ .*

*Proof.*

- As before, by the "valuable stable space tool", one can assume that  $G$  acts irreducibly on  $V$ .
- If  $\Gamma$  is any connected group, then  $D(\Gamma)$  is connected. Indeed, the set  $\Gamma^i$  of products of  $i$  commutators  $[\gamma_1 \gamma_2 \gamma_1^{-1} \gamma_2^{-1}]$  is a continuous image<sup>5</sup> of the connected set  $\Gamma^{2i}$  and is therefore connected. Then  $D(\Gamma)$  is a union of connected set having  $\text{Id}$  as common point: it is connected.
- If  $\ell(G) \leq 1$ , then  $G$  is commutative and there is a common trigonalization basis  $\mathcal{B}$  for  $G$  (12.2.0.2).

<sup>5</sup>product and inverse are polynomial in the entries and therefore define continuous maps

- Assume now  $\ell(G) > 1$  and set  $H = D^{\ell(G)-1}(H)$ . The group  $H$  is connected and solvable with  $\ell(H) = 1$  and therefore it is commutative. By (12.2.0.2), one can choose a non zero common eigenvector  $v$  for  $H$  (with eigenvalue  $\lambda(h) \in \mathbf{k}$ ). Let  $(g, h) \in G \times H$  and  $v^* \in V^*$  such that  $\langle v^*, v \rangle = 1$ . Because  $H$  is normal in  $G$ , one has

$$(*) \quad hg(v) = g(g^{-1}hg(v)) = \lambda(g^{-1}hg)g(v)$$

Applying  $v^* \circ g$  to  $(*)$  we get  $\langle v^*, g^{-1}hg(v) \rangle = \lambda(g^{-1}hg)$  proving that  $(g, h) \mapsto \lambda(g^{-1}hg)$  is continuous. If  $h$  is fixed,  $g \mapsto \lambda(g^{-1}hg)$  takes value in the finite set  $\text{Spec}(h)$  and therefore is constant because  $G$  is connected. Taking its value at  $g = \text{Id}$ , we get  $\lambda(g^{-1}hg) = \lambda(h)$ . Using  $(*)$ , we get that  $hg(v) = \lambda(h)g(v) = gh(v)$ .

- Because  $v$  was an arbitrary common  $H$ -eigenvector,  $hg$  and  $gh$  coincides on each such vector. By  $(*)$ ,  $g(v)$  is such a vector proving  $hg - gh = 0$  on  $\text{Span}(Gv) \stackrel{\text{irreducibility}}{=} V$  proving that  $g$  and  $h$  commute.
- Any eigenspace of  $h$  is both nonzero and invariant by  $G$  hence is equal to  $V$  proving that  $h = \lambda(h) \text{Id}$  for all  $h \in H$ . Because  $\ell > 1$ , we have  $H \subset DG \subset \text{SL}(V)$  and therefore  $\lambda(h)$  is a  $(n = \dim(V))^{\text{th}}$ -root of 1. Therefore  $H$  is finite hence  $H = \{\text{Id}\}$  because it is connected.

□

**Corollary 12.5.2.2** *Assume  $\mathbf{k}$  is algebraically closed. Every connected solvable subgroup of  $\text{GL}_n(\mathbf{k})$  is contained in a maximal connected solvable subgroup which is conjugate to the group of upper triangular matrices.*

## 12.6 Exercises

### Exercise 12.6.1

- Show that the hyperplane of equation  $\sum x_i = 0$  of  $\mathbf{k}^n$  is invariant by  $\mathcal{A} = \{M_\sigma, \sigma \in S_n\}$ .
- Show that  $\mathcal{A}$  does not act irreducibly on  $\mathbf{k}^n$  but that its image in  $\text{End}_{\mathbf{k}}(H)$  (through the restriction  $M \mapsto M|_H$ ) is irreducible.
- Show that  $S_3$  embeds in  $\text{GL}_2(\mathbf{C})$  but that is not conjugate to any subgroup of the group of invertible upper-triangular matrices.
- More generally, does the group of invertible upper-triangular matrices contain any group isomorphic to  $S_3$ ?

### Exercise 12.6.2

1. Show that  $(1, 2, 3)$  generates a normal subgroup of  $S_3$ .
2. Show that  $K = \{\text{Id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$  is an abelian normal subgroup of  $S_4$ .

3. Deduce that neither  $S_3$  or  $S_4$  is solvable.

**Exercise 12.6.3** Show that the set  $\mathcal{A}$  of rotations of the Euclidean plane  $V$  acts irreducibly. Compute  $\text{Span}(\mathcal{A}) \subset \text{End}_{\mathbf{k}}(V)$ .

**Exercise 12.6.4** We aim to show that the group  $B$  of matrices of  $\text{GL}_n(\mathbf{k})$  that are upper triangular is solvable ( $\mathbf{k}$  is a field). Let  $U$  be the subgroup of  $B$  of matrices whose eigenvalues are all equal to 1 (unipotent matrices).

1) Show that we have an exact sequence of groups

$$1 \rightarrow U \rightarrow B \rightarrow (\mathbf{k}^*)^n \rightarrow 1.$$

Deduce that  $B$  is solvable if and only if  $U$  is solvable.

Let  $(e_i)$  be the canonical basis of  $\mathbf{k}^n$ . For  $i \leq n$ , let  $F_i$  be the subspace of  $\mathbf{k}^n$  generated by  $e_1, \dots, e_i$ . We have  $F_i = (0)$  if  $i \leq 0$  and  $F_n = \mathbf{k}^n$ . For all  $f \in U$ , we denote by  $\ln(f)$  the matrix  $f - \text{Id}$ . For all  $j = 0, \dots, n$ , let  $U_j$  be the subset of  $U$  comprising the matrices  $f$  such that  $\ln(f)(F_i) \subset F_{i-j}$  for  $i \leq n$ .

2) Verify that we have

$$(1) = U_n \subset U_{n-1} \subset \dots \subset U_1 = U.$$

Show that  $U_i$  is a normal subgroup of  $U$  for all  $i \leq n$  and therefore also of  $U_{i-1}$ .

3) Let  $f \in U_j$ . Show that for all  $i \leq n$ , the restriction  $\ln(f)_{i,j}$  of  $\ln(f)$  to  $F_i$  induces a linear map of  $F_i/F_{i-j-1}$  which is zero if and only if  $\ln(f)(F_i) \subset F_{i-j-1}$ .

4) Show that the map

$$\ln_j : \begin{cases} U_i & \rightarrow \prod_i \text{End}(F_i/F_{i-j}) \\ f & \mapsto (\ln(f)_{i,j}) \end{cases}$$

is a group morphism and calculate its kernel.

5) Deduce that  $U$  is solvable. Conclude.

**Exercise 12.6.5** Compute the maximal number of commuting symmetries of  $\text{GL}_n(\mathbf{R})$ . Deduce that the groups  $\text{GL}_n(\mathbf{R})$  and  $\text{GL}_m(\mathbf{R})$  are isomorphic if and only if  $n = m$ . How can you generalize?

**Exercise 12.6.6** Show that a non trivial unipotent subgroup of  $\text{GL}(V)$  does not contain any compact subgroup (compare with 10.4.6).

**Exercise 12.6.7** Following Kaplanski, generalize Kolchin's theorem (12.4.0.1) as follows. Let  $\varepsilon \in \{0, 1\}$ . Assume  $\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$  is stable by product and that  $\chi_a^{-1}(0) \subset \{0, 1\}$  for all  $a \in \mathcal{A}$ . Then, then there exists a common trigonalization basis  $\mathcal{B}$  for  $\mathcal{A}$  [Remember that a vector space is not the union of two proper subspaces].

**Exercise 12.6.8** Let  $n > 0$  and  $F_{i,j} \in M_n(\mathbf{k}) - \{0\}$  such that  $F_{i,j}F_{k,l} = \delta_{j,k}F_{i,l}$  for all  $i, j, k, l \in \{1, \dots, n\}$ . Let  $\varphi \in \text{End}_{\mathbf{k}}(M_n(\mathbf{k}))$  such that  $\varphi(AB) = \varphi(A)\varphi(B)$  for all  $A, B \in M_n(\mathbf{k})$ .

1. If  $n = 1$ , show that there exists  $\lambda_i \in \mathbf{k}^*$  such that  $F_{i,j} = \lambda_i/\lambda_j$  for all  $i, j$ .

2. Show that there exists a common diagonalization basis  $\mathcal{B} = (f_i)$  of  $E_{i,i}$ ,  $i = 1, \dots, n$ .
3. Show that there exists  $\lambda_{i,j} \in \mathbf{k}^*$  such that  $E_{i,j}(f_l) = \delta_{j,l} \lambda_{i,j} f_l$ .
4. Show that  $\varphi$  is either 0 or an isomorphism [Look at  $\text{Ker}(\varphi)$ ].
5. If  $\varphi \neq 0$ , show that there exists  $P \in \text{GL}_n(\mathbf{k})$ , uniquely defined up to non zero scalar, such that  $\varphi(A) = PAP^{-1}$  for all  $A \in M_n(\mathbf{k})$ .



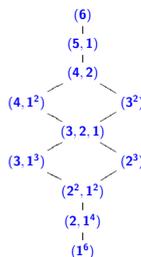
## **Part III**

# **About continuity of matrix reduction**



# Chapter 13

## Topology of similarity classes



Hasse Diagram of  $M_6$

### 13.1 Introduction



**Perspective**

Here we provide a perspective on the geometry of similarity classes through their topology. To avoid formalism, we restrict ourselves to matrices in  $M_n(\mathbf{k})$ , where  $\mathbf{k}$  is any subfield of  $\mathbb{C}$  endowed with the metric topology<sup>1</sup> derived from any norm on  $M_n(\mathbb{C})$ . We have chosen to keep our module-theoretic method in high detail, even though the proofs might be a bit shorter here and there by first reducing to the nilpotent case. The reason for this is to provide “natural proofs” and, more importantly, to illustrate the modern notion of deformation/family of modules.

We will study the topology of the set of matrices up to similarity. In other words, we will study the quotient map  $f : M_n(\mathbf{k}) \rightarrow M_n(\mathbf{k})/GL_n(\mathbf{k})$ , where  $P \in GL_n(\mathbf{k})$  acts on  $A \in M_n(\mathbf{k})$  by  $P.A = PAP^{-1}$ . Specifically,  $f(M) = O(M)$ , where  $O(M)$  is the conjugacy class of  $M$ . Because the action  $GL_n(\mathbf{k}) \times$

<sup>1</sup>As mentioned above, in the case of a general infinite field, the Zariski topology should be considered, which poses no real difficulty once its definition is known (see exercise 13.6.10). In fact, the topology must be finer than that of Zariski, the usual operations on matrices must be continuous, and the points of  $\mathbf{k}$  must not be open, ensuring that the closure of  $\mathbf{k}^*$  is  $\mathbf{k}$ . This is where the infinity of the field comes into play in the case of Zariski topology.

$M_n(\mathbf{k}) \rightarrow GL_n(\mathbf{k})$  is certainly continuous, our quotient has a canonical topological structure : the finest topology making  $f$  continuous. In other words,  $U \subset M_n(\mathbf{k})/GL_n(\mathbf{k})$  is open if and only if  $f^{-1}(U)$  is open. Be cautious that even this topology is very natural, it comes not from any metric as we will illustrate in detail later (see also 13.6.1).

**Remark(s) 13.1.0.1** *The reader will verify (exercice) the following universal property of this topology, which is the natural generalization of the quotient map universal property in our context. If  $T$  is any topological space, the map*

$$\begin{cases} \text{Hom}_{cont}(M_n(\mathbf{k})/GL_n(\mathbf{k}), T) & \rightarrow & \text{Hom}_{inv}(M_n(\mathbf{k}), T) \\ \varphi & \mapsto & \varphi \circ f \end{cases}$$

is bijective where

$$\text{Hom}_{inv}(M_n(\mathbf{k}), T) = \{\varphi \in \text{Hom}_{cont}(M_n(\mathbf{k}), T) | \forall (P, A) \in GL_n(\mathbf{k}) \times M_n(\mathbf{k}), \varphi(P.A) = \varphi(P)\}.$$

In particular, because the characteristic polynomial is invariant by conjugation, the characteristic polynomial map

$$\gamma : \begin{cases} M_n(\mathbf{k}) & \rightarrow & \mathbf{k}^n \\ A & \mapsto & \det(T \text{Id} - A) \end{cases}$$

defines a continuous (polynomial!) map  $\gamma$  which is invariant and by the above universal property defines a continuous map

$$\mu : M_n(\mathbf{k})/GL_n(\mathbf{k}) \rightarrow \mathbf{k}^n$$

where we identify a monic degree  $n$  polynomial with its first  $n$  coefficients. Because the image of  $\mu$  is well understood (its just an affine space), we will mainly focus our study to the topology of the various fibers  $\mu^{-1}(\chi)$  or, which remains to the same, to the various fibers  $\gamma^{-1}(\chi)$ . This is achieved in 13.5.1.4.

### 13.2 $\chi$ -types

Let  $\chi \in \mathbf{k}[T]$  be a degree  $n$  monic polynomial and recall (8.4.0.1) that a  $\chi$ -type is a sequence  $\underline{P} = (P_n | \dots | P_1)$  of monic polynomials of  $\mathbf{k}[T]$  such that  $\prod P_i = \chi$ .

**Definition 13.2.0.1** *We denote  $O(\underline{P})$  the set of matrices in  $M_n(\mathbf{k})$  similar to the companion matrix  $C(\underline{P})$ . We define the degree of  $\underline{P}$  by  $\text{deg}(\underline{P}) = n = \sum \text{deg}(P_i)$ .*

So  $O(\underline{P})$  is the orbit of  $C(\underline{P})$  under the action of  $GL_n(\mathbf{k})$  by conjugation. The theory of similarity invariants tells us that  $O(\underline{P})$  consists of matrices with similarity invariants  $\underline{P}$  and that  $M_d(\mathbf{k})$  is the disjoint

union of  $O(\underline{P})$ , since  $\underline{P}$  covers all  $n$ -types (8.7). From the point of view of the introduction 13.1 this means that

$$\boxed{\text{the set of types of degree } n \text{ is identified with } M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k}).}$$

Our goal is to study the closure  $\overline{O(\underline{P})}$  of the orbit  $O(\underline{P})$ . We define a (topological) relation  $\preceq$  on  $\chi$ -types (or types for short) as follows.

$$\boxed{\underline{P} \preceq \underline{Q} \text{ if and only if } O(\underline{P}) \text{ is contained in the closure } \overline{O(\underline{Q})}.}$$

By continuity of the characteristic polynomial, we have  $\underline{P} \preceq \underline{Q} \Rightarrow \prod P_i = \prod Q_j$  allowing to restrict ourselves to  $\chi$ -types for a given  $\chi$ . The relation  $\preceq$  is a reflexive and transitive relation on types<sup>2</sup>. Since  $\overline{O(\underline{Q})}$  is invariant by conjugation, it is a union of orbits and we have

$$\overline{O(\underline{Q})} = \cup_{\underline{P} \preceq \underline{Q}} O(\underline{P}).$$

Our goal is to characterize this relation in a combinatorial manner. We define a (combinatorial<sup>3</sup>) relation on degree  $n$ -types by

$$\boxed{(*) \quad \underline{P} \leq \underline{Q} \text{ if and only if } \forall i = 1, \dots, n, \prod_{j \leq i} P_j \mid \prod_{j \leq i} Q_j.}$$

This relation is a (partial) order. For degree reasons, we have  $\underline{P} \leq \underline{Q} \Rightarrow \prod P_i = \prod Q_j$ .

$$\boxed{\text{We will therefore restrict ourselves to } \chi\text{-types.}}$$

Dividing (\*) by  $\chi$ , we get

$$(*) \quad \underline{P} \leq \underline{Q} \Leftrightarrow \forall i = 2, \dots, n, \prod_{j \geq i} Q_j \mid \prod_{j \geq i} P_j.$$

**Example(s) 13.2.0.2** We have  $(T, T) \leq (1, T^2)$ . Moreover  $O(T, T) = O(0_2) = \{0_2\}$  and  $O(1, T^2)$  is the set of all non zero nilpotent matrices in  $M_2(\mathbf{k})$ . In particular,  $0_2 \in \overline{O(1, T^2)}$  because  $\lim \begin{pmatrix} 0 & 1/m \\ 0 & 0 \end{pmatrix} = 0$  hence  $(T, T) \preceq (1, T^2)$ .

Because we have only two types in this dimension 2 case, we deduce in this case  $\underline{P} \preceq \underline{Q} \Leftrightarrow \underline{P} \leq \underline{Q}$ .

The result is general.

**Theorem 13.2.0.3** Let  $\underline{P}, \underline{Q}$  be two  $\chi$ -types. Then,  $\underline{P} \preceq \underline{Q}$  if and only if  $\underline{P} \leq \underline{Q}$ . In other words, the topological and combinatorial orders on  $n$ -types coincide.

<sup>2</sup>At this stage, the anti-symmetry is not clear (cf. 13.3.0.2).

<sup>3</sup>Compare with cf. 13.4.2.

**Remark(s) 13.2.0.4** *This theorem is a reformulation, more transparent in my opinion, of Theorem 4 from [11]. Indeed, to our knowledge, it was Gerstenhaber who fully elaborated the structure of orbit closures, although we have not been able to stricto sensu find this statement.*

### 13.3 $\underline{P} \preceq \underline{Q} \Rightarrow \underline{P} \leq \underline{Q}$

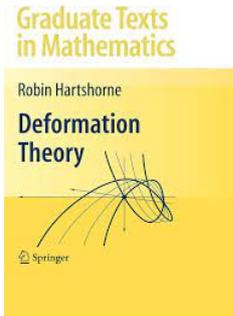
This implication follows from the continuity of determinants using the calculation of similarity invariants using minors (8.7).

**Lemma 13.3.0.1** *Let  $\alpha = (\alpha_k)$  be a converging sequence of degree  $d$  complex polynomials<sup>4</sup>. Assume that each  $\alpha_k$  is a multiple of some monic polynomial  $\beta \in \mathbf{k}[T]$ . Then,  $\beta | \lim(\alpha)$ .*

*Proof.* Let  $\mathcal{R}$  be the  $\mathbf{k}$ -subalgebra of the algebra of complex sequences generated by the  $d+1$ -sequences of coefficients of  $\alpha$ . All elements of  $\mathcal{R}$  are converging sequences (because sums and products of converging sequences are converging). By 1.3.1.1, one can perform the division  $\alpha \in \mathcal{R}[T]$  by the monic polynomial  $\beta \in \mathbf{k}[T] \subset \mathcal{R}[T]$  to obtain  $\alpha = \beta q + r$  with  $\deg(r) < \deg(\beta)$ . Because  $\beta | \alpha_k$  for every  $k$ , we get that  $r_k \in \mathbf{k}[T]$  is zero and finally  $r = 0$ . Because all elements of  $\mathcal{R}$  are converging sequences, we get by continuity of the product  $\lim(\alpha) = \beta \lim(q)$ .  $\square$

**Corollary 13.3.0.2** *We have the direct implication  $\underline{P} \preceq \underline{Q} \Rightarrow \underline{P} \leq \underline{Q}$ . In particular,  $\preceq$  is a ordering.*

*Proof.* Let  $(A_k)$  be a sequence of matrices of with similarity invariants  $\underline{Q}$  converging to some matrix  $A_\infty \in M_n(\mathbf{k})$  with similarity invariants  $\underline{P}$ . Then, we know that  $\delta_i(\underline{Q}) = \prod_{j \geq n-i+1} Q_j$ ,  $i = 1, \dots, n$  is the GCD of the minors of size  $i$  of all the matrices  $T \text{Id} - A_k$  (8.7). In particular,  $\delta_i(\underline{Q})$  divides the determinant of each these minors  $M_{I,J}(A_k)$  which are converging to the corresponding  $\det(M_{I,J}(A_\infty))$  of  $A_\infty$  by continuity of the determinant. By the lemma above,  $\delta_i(\underline{Q}) | \delta_i(\underline{P})$ . Using  $\prod_{j \geq 1} P_j = \prod_{j \geq 1} Q_j$ , we get  $\prod_{j \leq n-i} P_j | \prod_{j \leq n-i} Q_j$ ,  $i = 1, \dots, n$  and therefore  $\underline{P} \leq \underline{Q}$  because we have equality if  $i = 0$  in the preceding relation.  $\square$



The main point is to construct a family of matrices indexed by some parameter  $\varepsilon$  which are similar to  $C(\underline{Q})$  for  $\varepsilon \neq 0$  and to  $C(\underline{P})$  if  $\varepsilon = 0$ . We will achieve this goal in a simple but typical case using an important idea: constructing such a family remains to construct a family of modules thanks to the dictionary between modules and endomorphism. This is lemma 13.4.1.1. As the reader will see, a new condition on our family of modules appear : the freeness property of (4) in the lemma *op. cit.* . This is the *flatness* condition which is omnipresent in modern algebraic or number theory.

## 13.4 $\underline{P} \leq \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$

### 13.4.1 An elementary deformation

Let  $R = \mathbf{k}[\tau]$  be the polynomial ring in the variable  $\tau$ .

**Lemma 13.4.1.1** Let  $(P_2, P_1) = \underline{P} \leq \underline{Q} = (Q_2, Q_1)$  two  $\chi$ -type of degree  $n$  and  $A(\tau) \in M_2(R[\mathbf{T}]) = \text{End}_{R[\mathbf{T}]}(R[\mathbf{T}]^2)$  be the matrix

$$A(\tau) = \begin{pmatrix} P_2 & \tau Q_2 \\ 0 & P_1 \end{pmatrix}$$

and  $C[\tau]$  the  $R[\mathbf{T}]$ -module  $C[\tau] = \text{Coker}(A(\tau))$ . For  $\varepsilon \in \mathbf{k}$ , we define

$$C(\varepsilon) = C[\tau]/(\tau - \varepsilon)$$

as a  $R[\mathbf{T}]/(\mathbf{T} - \varepsilon) = \mathbf{k}[\mathbf{T}]$ -module.

1. We have an isomorphism of  $\mathbf{k}[\mathbf{T}]$ -modules  $C(\varepsilon) \xrightarrow{\sim} \text{Coker}(A(\varepsilon))$ .
2. If  $\varepsilon \in \mathbf{k}^*$ , then the invariant ideals of  $C(\varepsilon)$  are  $\underline{Q}$ .
3. If  $\varepsilon = 0 \in \mathbf{k}^*$ , then the invariant ideals of  $C(0)$  are  $\underline{P}$ .
4. The  $R$ -module  $C(\tau)$  is free of rank  $n$ .

*Proof.* 1. By definition, we have an exact sequence

$$R[\mathbf{T}]^2 \xrightarrow{A(\tau)} R[\mathbf{T}]^2 \rightarrow C[\tau] \rightarrow 0.$$

But in general, if  $M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$  is exact then it is straightforward to check that  $M_1/IM_1 \rightarrow M_2/IM_2 \rightarrow M_3/IM_3 \rightarrow 0$  is exact for any ideal  $I$  and follows from the functoriality of the cokernel.

<sup>4</sup>Because all norms on  $\mathbf{k}_{\leq d}[\mathbf{T}]$  are equivalent, we can use any norm to define the convergence notion. Notice that convergence of sequence of polynomials is equivalent to the convergence of each coefficients sequences.

2.  $\underline{P} \leq \underline{Q}$  means  $Q_2|P_2$  and therefore the GCD of the coefficients of  $A(\varepsilon)$  is  $Q_2$  hence is its second similarity invariant. Because its determinant of  $A(\varepsilon)$  is  $P_2P_1 = \chi = Q_2Q_1$ , the second is  $Q_1$ .
3. Clear.
4. Let  $\varphi$  be the natural composition  $\varphi : R_{<d_2}[T] \oplus R_{<d_1}[T] \rightarrow R[T] \oplus R[T] \rightarrow \text{Coker}(A(\tau))$  with  $d_i = \deg(P_i)$ . Let us show that  $\varphi$  is an  $R$ -linear isomorphism.

Surjectivity. Let  $(X_2, X_1) \in R[T]^2$ . We write  $X_1 = Y_1P_1 + R_1$  with  $\deg(R_1 < d_1)$  (division by the monic polynomial  $P_1$ ) and  $X_2 - \tau Q_2 Y_1 = P_2 Y_2 + R_2$  with  $\deg(R_2) < d_2$  (division by the monic polynomial  $P_2$ ). We have

$$\begin{pmatrix} X_2 \\ X_1 \end{pmatrix} = A(\tau) \begin{pmatrix} Y_2 \\ Y_1 \end{pmatrix} + \begin{pmatrix} R_2 \\ R_1 \end{pmatrix}$$

hence the surjectivity.

Injectivity. Let  $(X_2, X_1) \in R_{<d_2}[T] \oplus R_{<d_1}[T]$  in  $\text{Ker}(\varphi)$ , i.e. such that

$$\begin{pmatrix} X_2 \\ X_1 \end{pmatrix} = A(\tau) \begin{pmatrix} Y_2 \\ Y_1 \end{pmatrix}$$

for some  $(Y_2, Y_1) \in R[T]^2$ . We have  $P_1 Y_1 = X_1$ . Because  $P_1$  is monic, we get  $d_1 > \deg(X_1) = \deg(P_1 Y_1) = \deg(P_1) + \deg(Y_1) = d_1 + \deg(Y_1)$  hence  $Y_1 = 0$ . The second relation  $X_2 = P_2 Y_2 + \tau Q_2 Y_1 = P_2 Y_2$  yields in the same way  $d_2 > \deg(X_2) = \deg(P_2 Y_2) = \deg(P_2) + \deg(Y_2) = d_2 + \deg(Y_2)$  hence  $Y_2 = 0$ .

□

**Corollary 13.4.1.2**  $\underline{P} \leq \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$ .

*Proof.* Let  $\mathcal{B}$  be the basis  $(1, \dots, T^{d_2-1}) \sqcup (1, \dots, T^{d_1-1})$  of  $R_{<d_2}[T] \oplus R_{<d_1}[T] \xrightarrow{\sim} R^n$  and  $H(\tau) = \text{Mat}_{\mathcal{B}}(\varphi^{-1} \circ h_T \circ \varphi) \in M_n(R)$  where  $h_T$  is the multiplication by  $T$  on  $C(\tau)$ . By just rephrasing the lemma 13.4.1.1 we get that the similarity invariants of  $H(\varepsilon)$  are  $\underline{Q}$  if  $\varepsilon \neq 0$  and are  $\underline{P}$  if  $\varepsilon = 0$ , hence  $\underline{P} \preceq \underline{Q}$ . □

Our family of  $k[T]$ -modules  $C(\varepsilon)$ ,  $\varepsilon \in k$  is the typical example of an (algebraic) *deformation* of our module  $C(0)$ .

### 13.4.2 $\leq = \preceq$

**Definition 13.4.2.1** Let  $\underline{P}, \underline{Q}$  be  $\chi$ -types and  $\mathcal{P}$  is the (finite) set of irreducible divisors of  $\chi$ . We say that  $\underline{P}$  is an elementary deformation of  $\underline{Q}$  if there exists  $\pi \in \mathcal{P}$ , monic polynomials  $\tilde{P}_i$  and  $n \geq j > i \geq 1$  such that

$$\underline{P} = (\tilde{P}_n, \dots, \pi \tilde{P}_j, \dots, \tilde{P}_i, \dots, \tilde{P}_1), \text{ and } \underline{Q} = (\tilde{P}_n, \dots, \tilde{P}_j, \dots, \pi \tilde{P}_i, \dots, \tilde{P}_1)$$

i.e.

$$P_k = Q_k = \tilde{P}_k \text{ if } k \neq i, j \text{ and } P_j = \pi Q_j = \pi \tilde{P}_j, Q_i = \pi P_i = \pi \tilde{P}_i.$$

We write in this case  $\underline{P} \preceq_e \underline{Q}$

The definition is justified by

**Lemma 13.4.2.2** *With the notation above,  $\underline{P} \preceq_e \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$ .*

*Proof.* Apply lemma 13.4.1.1 to  $(P_i, \pi Q_j) \leq (\pi P_i, Q_j)$ . □

The main theorem 13.2.0.3 is now a consequence of the following proposition.

**Proposition 13.4.2.3** *Let  $\underline{P} \preceq \underline{Q}$  be two distinct  $\chi$ -types.*

1. *There exists a finite series of elementary deformations  $\underline{P} = R^0 \underset{e}{\prec} R^1 \underset{e}{\prec} \dots \underset{e}{\prec} R^{N-1} \underset{e}{\prec} R^N = \underline{Q}$ .*
2.  $\underline{P} \preceq \underline{Q}$ .

*Proof.* (1)  $\Rightarrow$  (2) thanks to the preceding lemma. It suffices to prove the existence of a partition  $\underline{R}$  such that  $\underline{P} \underset{e}{\preceq} \underline{R} \preceq \underline{Q}$  when  $\underline{P} \neq \underline{Q}$  and to iterate the process (which eventually stops when  $\underline{R}_N = \underline{Q}$  because the number of  $\chi$ -types is finite.)

Because  $\underline{P} \neq \underline{Q}$ , one can choose  $\pi \in \mathcal{P}$ ,  $\ell \in [1, \dots, n]$  such that

$$(*) \quad v_\pi(P_\ell) \neq v_\pi(Q_\ell)$$

Because  $\underline{P} \leq \underline{Q}$ , we have

$$(1) \quad \forall k, v_\pi(P_1 \dots P_k) \leq v_\pi(Q_1 \dots Q_k).$$

(\*) implies that the inequality (1) is strict for some  $k$ . Let  $i$  be the smallest integer such that (1) is strict.

We have therefore

$$(1') \quad P_k = Q_k \text{ if } k < i \text{ and } \pi P_i | Q_i.$$

Dividing (1) by  $\chi$  we get

$$(2) \quad \forall k, v_\pi(Q_n \dots Q_k) \leq v_\pi(P_n \dots P_k).$$

Again (\*) implies that the inequality (2) is strict for some  $k$ . Let  $j$  be the largest integer such that (2) is strict. We have therefore

$$(2') \quad Q_k = P_k \text{ if } k > j \text{ and } \pi Q_j | P_j.$$

If  $i \geq j$ , we have  $\underline{P} = \underline{Q}$  by (1') and (2'), a contradiction. Therefore  $j > i$ .

Let  $R = (R_k)_{1 \leq k \leq n}$  be the family

$$R_k = P_k \text{ if } k \neq i, j \text{ and } R_i = \pi P_i, R_j = P_j / \pi \in \mathbf{k}[T].$$

We have  $\prod R_i = \chi$ . Let us verify that  $R$  is divisibility decreasing which will prove that  $R$  is a  $\chi$ -type with the wanted property.

For  $k \in X = [1, n] - \{i, j\}$ , we have  $P_k = R_k$  implying that the restriction of  $R$  to  $X$  is decreasing. We have to show  $R_k | R_{k-1}$  for  $k \in \{i, i+1, j, j+1\}$ .

- If  $k = i$  we have  $R_i = \pi P_i \mid^{(1')} Q_i | Q_{i-1} = P_{i-1} = R_{i-1}$ .
- If  $k = i+1$ 
  - If  $j \neq i+1$ , we have  $R_{i+1} = P_{i+1} | P_i | R_i$ .
  - If  $j = i+1$ , we have  $R_{i+1} = R_j = P_j / \pi |^{j>i} P_i | R_i$ .
- If  $k = j$ 
  - If  $j \neq i+1$ , we have  $R_j = P_j / \pi | P_j | P_{j-1} = R_{j-1}$ .
  - If  $j = i+1$ , already done.
- If  $k = j+1$  we have  $R_{j+1} = P_{j+1} = Q_{j+1} | Q_j \mid^{(2')} P_j / \pi = R_j$ .

Certainly  $\underline{P} \leq \underline{R}$ . Let us finally verify  $\underline{R} \leq \underline{Q}$ .

- It is true for  $k < i$  because  $R$  and  $\underline{P}$  coincides in this range.
- For  $i \leq k < j$ , by (2'), one has  $\prod_{l \leq k} R_l = \pi \prod_{l \leq k} P_l \mid^{(1')} \prod_{l \leq k} Q_l$ .
- For  $k \geq j$ , one has  $\prod_{l \leq k} R_l = \prod_{l \leq k} Q_l$ .

□

This concludes the proof of theorem 13.2.0.3.



## 13.5 Topological applications

We want to study  $M_n(\mathbf{k}) / GL_n(\mathbf{k})$  using our continuous  $\mu$  to  $\mathbf{k}^n$  defined by the characteristic polynomial (13.1). We start with its fibers  $\mu^{-1}(\chi)$  or, what remains to the same by definition of the topology of the set  $\gamma^{-1}(\chi)$  of matrices with given characteristic polynomial  $\chi$ .

### 13.5.1 Topology of the fibers $\mu^{-1}(\chi)$

We keep the notations above and we denote by  $\mathcal{T}$  be the set of  $\chi$ -types ordered by  $\leq = \preceq$ . Let

$$M_\chi = \{A \in M_n(\mathbf{k}) \mid \chi_A = \chi\} \stackrel{13.1}{=} \gamma^{-1}(\chi).$$

If  $P$  is a monic degree  $n \geq 1$  polynomial, we define  $P_{red}$  as the product of its (monic) irreducible divisors. As we have already observed, in our zero characteristic zero case, characteristic,  $P_{red} = P / \text{GCD}(P, P')$  and can be algorithmically computed (cf. 11.6.9 for the general case).

#### Lemma 13.5.1.1

1. There exists<sup>5</sup> a unique decreasing sequence of monic polynomials  $P_{r,i} \in \mathbf{k}[T]$ 
  - If  $P, Q$  are coprime polynomials, one has  $(PQ)_{r,i} = P_{r,i}Q_{r,i}$  for all  $i \geq 1$ .
  - If  $P = \pi^d$  for some irreducible polynomial  $\pi$ , we have  $P_{r,i} = \pi$  if  $i \leq d$  and  $P_{r,i} = 1$  if  $i > d$ .
2. All  $P_{r,i}$  are square free,  $P_{r,i} = 1$  for  $i > n$  and  $\prod P_i = P$ .
3.  $\underline{\chi}_{ss}$  is the smallest element of  $\mathcal{T}$ .
4.  $\underline{\chi}_{cycl}$  is the largest element of  $\mathcal{T}$ .

*Proof.* (1) and (2) are just reflecting that  $\mathbf{k}[T]$  is UFD.

(3) Let  $\underline{Q} \in \mathcal{T}$ . Because  $P \mid Q$  if and only if  $v_\pi(Q)$  for any irreducible  $\pi$ , one can assume  $\chi = \pi^d$  and  $\underline{Q} = (\pi^{\delta_1}, \dots, \pi^{\delta_n})$  for some partition  $\underline{\delta}$  of  $d$ . But the corresponding partition of  $\pi^d$  is  $(1, \dots, 1)$  which is certainly  $\leq \underline{\delta}$  and therefore  $\underline{\chi}_{ss} \leq \underline{Q}$ .

(4) We have  $\prod_{i \leq k} Q_i \mid \prod_{i \leq n} Q_i = \chi = \prod_{i \leq k} Q_i$  for any  $i \leq 1$ . □

**Definition 13.5.1.2**  $\underline{\chi}_{cycl} = (1, \dots, 1, \chi)$  is called the cyclic  $\chi$ -type and  $\underline{\chi}_{ss} = (\chi_{r,n}, \dots, \chi_{r,1})$  the semi-simple type. The corresponding similarity classes are called the cyclic (resp. semi-simple) orbits.

**Remark(s) 13.5.1.3** The cyclic type  $\underline{\chi}_{cycl}$  is the  $\chi$ -type of the companion matrix  $C(\chi)$  and the semi-simple type  $\underline{\chi}_{ss}$  is the  $\chi$ -type of the multiplication  $h_T$  by  $T$  on  $V = \oplus \mathbf{k}[T]/(\chi_{r,i})$  which is therefore semi-simple because each  $\chi_{r,i}$  is square free.

<sup>5</sup>See 13.6.7 for an alternative algorithmic definition

By definition, the cyclic orbit is the subset of  $M_\chi$  of cyclic elements the semi-simple orbit is the subset of  $M_\chi$  of semi-simple elements.

#### Corollary 13.5.1.4

1.  $M_\chi = \sqcup_{\underline{P} \in \mathcal{T}} O(\underline{P})$ . In particular  $\mu^{-1}(\chi)$  is finite.
2.  $\overline{O(\underline{P})} = \sqcup_{\underline{Q} \leq \underline{P}} O(\underline{Q})$ .
3. The cyclic orbit is the only orbit which is open (resp. dense) in  $M_\chi$ .
4. The semi-simple orbit is the only closed orbit in  $M_\chi$  (and therefore in the whole  $M_n(\mathbf{k})$ ).
5.  $\mu^{-1}(\chi)$  is closed if and only if  $C(\chi)$  is both semi-simple and cyclic<sup>6</sup> or equivalently if  $\text{Card}(\mu^{-1}(\chi)) = 1$ .
6. More generally,  $O(\underline{P})$  is open and dense in its closure  $\overline{O(\underline{P})}$ .
7.  $\overline{O(\underline{P})} = \overline{O(\underline{Q})}$  if and only if  $\underline{P} = \underline{Q}$ .

*Proof.* 1. It is a rephrasing the main theorem of similarity invariants (see 8.7).

2.  $\leq = \preceq$ .

3. Use (2) and (3) of lemma 13.5.1.1.

4. Use (2) and (4) of lemma 13.5.1.1.

5. Use (3) and (4).

6. Use (2).

7.  $\leq = \preceq$ .

□

### 13.5.2 Global properties of $M_n(\mathbf{k})/GL_n(\mathbf{k})$

Let us start with a general lemma.

**Lemma 13.5.2.1** *Let  $\emptyset \neq \Omega \subset \mathbf{k}^n$  which is defined by the non vanishing of a finite number of polynomials. Then,  $\Omega$  is dense in  $\mathbf{k}^n$ .*

<sup>6</sup>If moreover  $\chi(0) \neq 0$ , a matrix similar to  $C(\chi)$  is called regular element of  $GL_n(\mathbf{k})$ . Observe  $A$  is regular if and only if its complex eigenvalues are distinct (exercise).

*Proof.* Let  $P_i \neq 0$  be the polynomial inequations defining  $\Omega$  and  $\omega \in \Omega$ . Let  $x \in \mathbf{k}^n - \Omega$  and consider  $D_t^0 = \{\omega + tx \in \Omega, t \in \mathbf{k}\}$ . The one variable polynomial  $P_i(\omega + Tx)$  does not vanish at  $T = 0$ . Therefore, its set of roots  $Z_i$  is finite and so is the union  $\cup Z_i$ . Therefore,  $D_t^0$  is the complement of finite set in the line  $\langle \omega, x \rangle \subset \mathbf{k}^n$  and there are certainly points of  $D_t^0$  arbitrary close of  $x$  by the density of  $\mathbf{k}$  in  $\mathbf{C}$ .  $\square$

### Proposition 13.5.2.2

1.  $M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k})$  is connected.
2. The set of cyclic classes is open and dense.
3. Both the set of regular classes (both semi-simple and cyclic) is open and dense.
4. The set of rank  $\geq r$  matrices is open and dense (semi-continuity of the rank).

*Proof.*

1.  $M_n(\mathbf{Q})$  is dense in  $M_n(\mathbf{C})$  and therefore  $M_n(\mathbf{k})$  is dense in  $M_n(\mathbf{C})$ . Because the latter is connected,  $M_n(\mathbf{k})$  is connected and so is its continuous image  $M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k})$ .
2. By definition of the quotient topology, we have to show that the inverse image of the set of cyclic classes is open and dense in  $M_n(\mathbf{k})$  and therefore that the set of cyclic matrices  $A$  is so. But writing that  $A$  is cyclic is writing  $\deg(\mu_A) = n$  or  $\mathrm{Id}, \dots, A^{n-1}$  is a free family. This condition can be written by the non vanishing of a bunch of determinants of matrices whose coefficients are polynomial in the coefficients of the  $A^i$ 's, and we get the openness (or use item (4) above). We conclude by 13.5.2.1.
3. Because a matrix in  $M_n(\mathbf{k})$  is cyclic if and only if its characteristic polynomial of degree  $n$ , the regularity condition is equivalent to  $\mathrm{GCD}(\chi, \chi') = 1$  (recall that  $\mathbf{k}$  is perfect being of zero characteristic). The latter condition can be written  $\mathrm{Res}(\chi, \chi') \neq 0$  where  $\mathrm{Res} \in \mathbf{k}[T_{i,j}]$  (4.6.7). We conclude by 13.5.2.1 again.
4. Apply the determinant characterization  $\delta_r(A) \neq \{0\}$  of 3.8.1.4.

$\square$

**Remark(s) 13.5.2.3** *It's easy and useful to prove openness and density of regular matrices without using the resultant (see 14.3.1.1) but the corresponding result is weaker because we do not get the algebraic nature of the locus and therefore that it is huge (for instance we don't get that Lebesgue almost surely any polynomial has distinct roots).*

## 13.6 Exercises

**Exercise 13.6.1** Assume  $n \geq 2$ . Show that the image of  $tE_{1,2}$ ,  $t \in \mathbf{k}$  in  $M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k})$  is constant except for  $t = 0$ . Deduce that  $M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k})$  is not separated.

**Exercise 13.6.2** Let  $g : M_n(\mathbf{k}) \rightarrow \mathbf{k}$  be a continuous  $\mathrm{GL}_n(\mathbf{k})$ -invariant function. Show that there exists a unique continuous function  $\bar{g}$  on  $\mathbf{k}^n$  such that  $g = \bar{g} \circ f$  with  $f$  the quotient map  $f : M_n(\mathbf{k}) \rightarrow M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k})$ .

**Exercise 13.6.3** Show that there does not exist any norm on  $M_n(\mathbf{k})$ ,  $\mathbf{k} = \mathbf{R}, \mathbf{C}$  invariant under similarity.

**Exercise 13.6.4** Let  $p : M_n(\mathbf{R}) \rightarrow \mathbf{R}^+$  be an application satisfying the triangle inequality, positively homogeneous ( $p(tA) = |t|p(A)$  for  $t \in \mathbf{R}$ )<sup>7</sup> and invariant by similarity.

1. Give a non trivial example of invariant semi-norm on  $M_n(\mathbf{R})$ .
2. Show that  $A$  is nilpotent if and only if  $A$  and  $2A$  are similar. Deduce the value of  $p(A)$ .
3. Show  $p(A) = 0$  if  $A$  is a traceless matrix (Use 7.8.7).
4. Compute  $p$ .

**Exercise 13.6.5** Let  $H_6$  be the graph whose vertex are the nilpotent  $T^6$ -types and with a vertex between two types  $\underline{P}, \underline{Q}$  if and only if  $\underline{P} \leq \underline{Q}$ . Draw  $H_6$  and compare with the Hasse diagram at the beginning of the chapter.

**Exercise 13.6.6** Let  $\emptyset \neq \Omega \subset \mathbf{C}^n$  which is defined by the non vanishing of a finite number of polynomials. Show that almost surely relative to the Lebesgue measure,  $x \in \mathbf{C}^n$  belongs to  $\Omega$ .

**Exercise 13.6.7** With the notations of 13.5.1.1, prove that  $P_{r,1} = P_{red}$  and  $P_{r,i+1} = (P/P_{r,i})_{red}$  for  $i \geq 1$ . Deduce an effective algorithm to compute these polynomials (see 11.6.9). Can you generalize to the perfect case?

**Exercise 13.6.8** The semi-simple part of the Jordan-Chevalley decomposition of  $a \in M_\chi$  is  $\underline{\chi}_{ss}$  (cf. 11.4.2.1).

**Exercise 13.6.9** Show that the semi-simple orbit of  $\mu^{-1}(\chi)$  is the only closed point and that the cyclic orbit is an open and dense point. Show that  $\mu^{-1}(\chi)$  is separated if and only if  $\mathrm{Card}(\mu^{-1}(\chi)) = 1$ . Prove if  $\underline{P} \neq \underline{Q}$  are points of  $\mu^{-1}(\chi)$ , there exists an open subset of  $\mu^{-1}(\chi)$  such that either  $\underline{P} \in U$  and  $\underline{Q} \notin U$  or  $\underline{Q} \in U$  and  $\underline{P} \notin U$  (this property is sometimes called the Kolmogorov separation property).

**Exercise 13.6.10** Prove that  $\overline{O(\underline{P})}$  is the zero set of a finite family of polynomials<sup>8</sup> in  $\mathbf{k}[T_{i,j}]$ .

**Exercise 13.6.11** Prove that the set of regular matrices of size  $n \geq 2$  is not open. What is its topological interior?

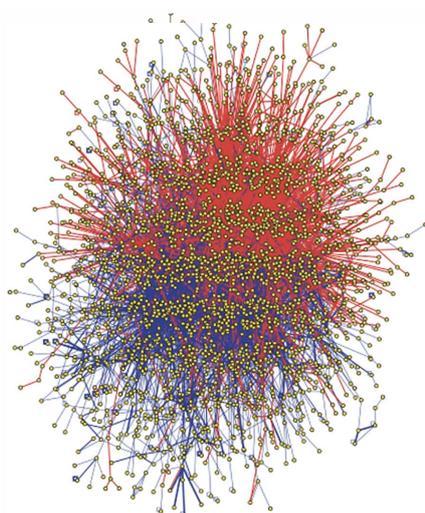
**Exercise 13.6.12** Show that any continuous  $\mathrm{GL}_n$ -invariant (by conjugation) function on  $M_n(\mathbf{C})$  factors through  $\gamma$  (13.1). Deduce that  $\mu : M_n(\mathbf{k})/\mathrm{GL}_n(\mathbf{k}) \rightarrow \mathbf{k}^n$  induces an isomorphism of there algebra of numerical functions although  $\mu$  is not a homeomorphism.

<sup>7</sup>Such an application is called a *semi-norm*.

<sup>8</sup>The advanced reader will rephrase this statement by saying that these closures are Zariski closed. He will verify that it implies that our closure coincides with the corresponding Zariski closure.

## Chapter 14

# Eigenvalues and primary components



Human interactome

Image reprinted by permission from Macmillan Publishers Ltd: Rual et al. Nature 2005: 437 (4).

### 14.1 Introduction



#### Perspective

We focus our attention on the eigenvalues of complex and real matrices, with particular attention to matrices with non-negative coefficients. Our aim is to understand their continuity properties with respect to the matrix coefficients, which is a necessary condition for being able to approximate them appropriately.

In this chapter we consider  $\mathbf{k} \subset \mathbf{C}$  and  $a \in \text{End}_{\mathbf{k}}(V)$  with matrix  $A \in M_n(\mathbf{k})$  in a basis with characteristic polynomial  $\chi$ . We are mainly interested in the set  $\text{Spec}(A)$  of its complex eigenvalues.

## 14.2 Continuity of primary components ( $\chi$ fixed)

We know from the chapter 13 that the similarity invariants do not vary continuously with the coefficients of the matrix, even when the characteristic polynomial is a given monic polynomial  $\chi$ . The counterpart of this bad news is that they can be computed in an effective exact way, but with an algorithm that is numerically unstable by nature. However, if the matrix has  $\mathbf{Q}$  coefficients, for example, or more generally if the field is “fully computable”, we can perform exact calculations with a computer. In summary,

Frobenius decomposition is exactly computable, but in general difficult if not impossible to approximate because it is not continuous, even if  $\chi_a$  is fixed.

On the other hand, we have in hand another decomposition (10.2.1.2) of  $V_a$  which in our case reads as follows. We write the irredundant prime decomposition

$$\chi = \prod P_i^{v_i}$$

of  $\chi$  in monic irreducible polynomials and, remembering  $\chi(a) = 0$  hence  $\chi \cdot V_a = \{0\}$  by Cayley-Hamilton, we get

$$(*) \quad V_a = \bigoplus V_a[P_i]$$

where

$$V_a[P_i] = \text{Ker}(P_i^{v_i}(a))$$

is the  $P_i$ -primary part of the  $\chi$ -torsion module. We denote by  $\pi_i(a)$  the spectral projection onto  $V_a[P_i]$  parallel to  $\bigoplus_{j \neq i} V_a[P_j]$ .

**Lemma 14.2.0.1** *One has  $\dim V_a[P_i] = v_i \deg(P_i)$ .*

*Proof.* The minimal polynomial of the restriction of  $a$  to  $\dim V_a[P_i]$  is a power of  $P_i$  and therefore so is its characteristic polynomial  $\chi = P_i^{w_i}$ . But  $\dim \dim V_a[P_i] = \deg(\chi_i) = w_i \deg(P_i)$ . By multiplicativity of the determinant, we get  $\prod P_i^{v_i} = \chi = \prod \chi_i = \prod P_i^{w_i}$  and by uniqueness of the irredundant decomposition the lemma follows.  $\square$

**Corollary 14.2.0.2** *Let  $\lambda \in \text{Spec}(a)$ . One has  $v_\lambda(\chi_a) \geq \dim \text{Ker}(a - \lambda \text{Id})$ . Moreover,  $a$  is diagonalizable if and only  $\chi_a$  is split and we have  $v_\lambda(\chi_a) = \dim \text{Ker}(a - \lambda \text{Id})$  for all  $\lambda$ .*

*Proof.* The lemma with  $P_\lambda = T - \lambda$  and the inclusion  $\text{Ker}(a - \lambda \text{Id}) \subset V_a[T - \lambda]$  gives the inequality and (\*) the equality criterium.  $\square$

**Proposition 14.2.0.3** *Let  $\alpha : S \rightarrow M_n(\mathbf{k})$  be a continuous. Assume that  $\chi_{\alpha(s)} = \chi$  for all  $s \in S$ .*

1. *There exists polynomials  $e_i \in \mathbf{k}[T]$  depending on  $\chi$  (and not on  $\alpha$ ) such that  $\pi_i(\alpha(s)) = e_i(\alpha(s))$ .*
2.  *$\pi_i(\alpha(s))$  is continuous of constant rank  $\dim V_{\alpha(s)}[P_i] = v_i \deg(P_i)$ .*

*Proof.*

1. This is the Chinese remainder lemma 4.5.0.1.
2. A polynomial is continuous, so is its composition with  $\alpha$ . Apply then the preceding lemma.

□

In summary,

The prime decomposition of  $\chi$  is not exactly computable in general. But given a prime decomposition of  $\chi$ , the primary parts vary continuously with  $a$ , provided  $\chi_a = \chi$  is fixed. In particular, unlike the Frobenius decomposition, the primary parts behave well by approximation.

If  $\chi = \prod_{\lambda_i \in \text{Spec}(A)} (T - \lambda_i)^{v_i}$  is split (for instance if  $\mathbf{k} = \mathbf{C}$ ), we have  $P_i(T) = T - \lambda_i$ ,  $V_i[P_i] = \text{Ker}(a - \lambda_i)^{v_i}$ . If we now want to vary  $\chi$  and understand  $P_i$ , we therefore have to look at the continuity of the eigenvalues.

## 14.3 Regularity of polynomial roots

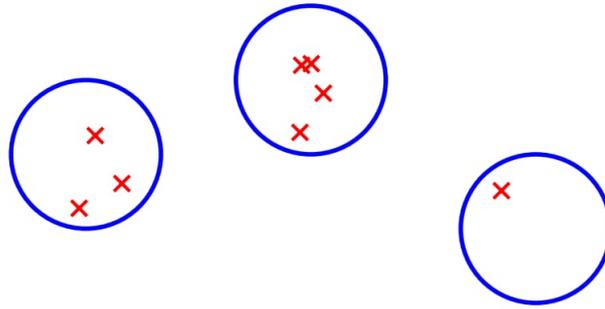
### 14.3.1 Continuity

Let  $Z$  be set of complex roots of a monic degree  $d$ -polynomial  $P$ . Let  $P_n$  be a sequence of monic degree  $d$  polynomials converging<sup>1</sup> to  $P$  and  $Z_n$  be set of complex roots of  $P_n$ .

**Proposition 14.3.1.1** *Let  $\lambda$  be a root of  $P$  with multiplicity  $m_\lambda$ .*

1. *For any  $\varepsilon > 0$ , there exists  $N$  such that for all  $n > N$  the number of complex roots of  $P_n$  in  $B(\lambda, \varepsilon)$  counted with multiplicity is  $m_\lambda$ .*
2. *There exists  $d$  converging sequences  $\lambda_{i,n}$ ,  $1 \leq i \leq d$  such that  $P_n = \prod_i (T - \lambda_{i,n}) = P_n(T)$ .*
3. *If all the roots of the  $P_n$  are real, so are the roots of  $P$ .*

<sup>1</sup>With respect to an arbitrary norm on  $\mathbf{C}_d[T]$ .



$$P(T) = T^3(T - 2 - i)(T - 4 + i)$$

*Proof.* <sup>2</sup> We prove (1)+(2) by induction on  $d$ , the case  $d = 1$  being tautological. Assume  $d > 1$ . For any  $n$ , let  $\lambda_{1,n}$  be a root of  $P_n$  which is the closest of  $\lambda$ . We have  $P_n(T) = \prod (T - \mu_i)$  where  $\mu_i \in \mathbb{C}$  and therefore  $|P_n(\lambda)| = \prod |\lambda - \mu_i| \geq |\lambda - \lambda_{1,n}|^d$ . But  $\lim P_n(\lambda) = P(\lambda) = 0$  and therefore we have  $\lim \lambda_{1,n} = \lambda$ . In particular, for  $n \gg 0$ , we have  $\lambda_{1,n} \in B(\lambda, \varepsilon)$ .

Let  $R$  be ring of convergent complex sequence. The sequence  $(P_n(T))$  belongs to  $R[T]$  and the rest of its Euclidean division (1.3.1.1) by  $T - (\lambda_{1,n})$  vanishes (it is a constant and vanishes on  $T = (\lambda_{1,n})$ ). Therefore, one can write  $P_n(T) = (T - \lambda_{1,n})Q_n(T)$  where  $Q_n(T)$  is a converging sequence of monic degree  $d - 1$  polynomials. We have also  $P(T) = (T - \lambda)Q(T)$  where  $Q(T)$  is a monic degree  $d - 1$  polynomial. By continuity of the product, we have  $(T - \lambda) \lim Q_n(T) = (T - \lambda)Q(T)$  implying  $\lim Q_n(T) = Q(T)$  and we apply the induction hypothesis to  $(Q_n)$ .

(3) follows from directly (2).

□

**Remark(s) 14.3.1.2** *The following statement, although equivalent, is sometimes useful. Let  $X \subset \mathbb{C}$  and define the number of roots in  $X$  of a polynomial  $P$  counted with multiplicity as*

$$\deg_X(P) = \sum_{\lambda \in X} m_P(\lambda).$$

*Then, if  $\Omega$  is open in  $\mathbb{C}$ , then  $\deg_X$  restricted to the space  $\mathcal{M}_d$  of monic degree  $d$  complex polynomial is lower semi-continuous in the following sense: for any  $n$ ,*

$$\{P \in \mathcal{M}_d \mid \deg_\Omega(P) \geq n\} \text{ is open in } \mathcal{M}_d.$$

<sup>2</sup>We have chosen to give a proof which can be generalized to algebraically closed normed fields rather giving a proof baser on residue formula. We encourage the reader to give a proof (in the complex case) using this idea.

**Corollary 14.3.1.3** *Let  $\pi : \mathbf{C}^d \rightarrow \mathcal{M}$  be the continuous map  $(\lambda_i) \mapsto \prod(\mathbf{T} - \lambda_i)$  and  $f : \mathbf{C}^d \rightarrow \mathbf{C}$  be a continuous function invariant through the natural action of  $S_d$  on  $\mathbf{C}^d$ . Then, there exists a unique  $\bar{f} : \mathcal{M} \rightarrow \mathbf{C}$  such that  $f = \bar{f} \circ \pi$ .*

*Proof.* Observe that  $\pi$  is surjective ( $\mathbf{C}$  is algebraically closed) giving the uniqueness.

Moreover,  $\pi(\lambda) = P$  exactly means that  $\lambda_i$  are the roots of  $P$  and therefore  $P$  determines  $(\lambda)$  up to reordering. This gives the existence of  $\bar{f}$  as a map of sets.

Let  $(P_n \stackrel{14.3.1.1}{=} \prod_i(\mathbf{T} - \lambda_{i,n}))$  be a sequence  $\mathcal{M}$  converging to  $P \in \mathcal{M}$ . We have

$$\lim \bar{f}(P_n) = \lim f((\lambda_{i,n})) = f(\lim(\lambda_{i,n})) \stackrel{\text{invariance}}{=} f((\lambda_i)) = \bar{f}(P)$$

hence the continuity of  $\bar{f}$ . □

### 14.3.2 Smoothness of simple roots

Let  $\varphi : \mathbf{C}^d \times \mathbf{C} \rightarrow \mathbf{C}$  be the “universal” polynomial function  $(a_i, z) \mapsto z^d + \sum_{i < d} a_i z^i$  defining polynomials  $P_a \in \mathbf{C}[\mathbf{T}]$ ,  $a = (a_i)$ . By smoothness we mean  $C^\infty$  (or even holomorphic for the advanced reader).

**Proposition 14.3.2.1** *Let  $\alpha = (\alpha_i) \in \mathbf{C}^d$  and  $\lambda_0$  is a simple root of the polynomial  $P_\alpha$ . There exists a smooth function  $\lambda$  defined in a neighborhood  $U \subset \mathbf{C}^d$  of  $a$  and a neighborhood  $D \subset \mathbf{C}$  of  $\lambda$  such that  $\lambda(a)$  is the only root of  $P_a$  belonging to  $D$  for any  $a \in U$ . Moreover, this root is simple.*

*Proof.* Because  $\varphi$  is smooth, we just have to verify that the hypothesis of the implicit function theorem are fulfilled, namely that the differential  $d_2\varphi(\lambda_0, \alpha)$  of

$$\begin{aligned} \mathbf{C} = \mathbf{R}^2 &\rightarrow \mathbf{C} \\ (x, y) &\mapsto \varphi(\alpha, x + iy) \end{aligned}$$

is not zero at  $\lambda_0$ . But the (polynomial) Taylor expansion  $P_\alpha(\lambda_0 + h) = P_\alpha(\lambda_0 + h) + hP'_\alpha(\lambda_0) + o(h)$  shows that the differential  $d_2\varphi(\lambda_0, \alpha)$  is the complex similarity  $h \mapsto P'_\alpha(\lambda_0)h$  which is invertible because  $P'_\alpha(\lambda_0) \neq 0$ . □

**Remark(s) 14.3.2.2** *We could have used this proposition to show that the locus of polynomials with distinct roots is open.*

### 14.3.3 Properness

**Proposition 14.3.3.1** *Let  $z$  be a root  $P = \sum_{i \leq n} a_i T^i$  be a degree  $n$  complex polynomial.*

1. *We have the bound  $|z| \leq \max\{1, \sum_{i < n} |a_i|/|a_n|\} = B(P)$ .*
2. *The continuous map  $\pi : \mathbf{C}^n \mapsto \mathbf{C}_n[\mathbf{T}]$  mapping  $(z_1, \dots, z_n)$  to  $\prod(\mathbf{T} - z_i)$  is proper.*

*Proof.*

1. If  $|z| \geq 1$ , we write

$$|z| = \left| -\sum_{i < n} a_i/a_n z^{i-n} \right| \leq \sum_{i < n} |a_i|/|a_n| |z|^{i-n} \leq \sum_{i < n} |a_i|/|a_n|$$

2. If the coefficients of the monic polynomial  $P$  are bounded by  $M \geq 1$ , its roots are bounded by  $nM$  by (1). The inverse image of a compact by  $\pi$  is therefore bounded and moreover closed in  $\mathbf{C}^n$  (continuity of  $\pi$ ) hence compact by Bolzano-Weierstrass theorem. By definition,  $\pi$  is therefore proper<sup>3</sup> of  $\pi$ .

□

**Remark(s) 14.3.3.2** *This bound show that it is always possible, at least theoretically, to handle the factorization problem of polynomials with integer coefficients. For, if  $Q = T^m + \sum_{i < m} b_i T^i \in \mathbf{Z}[\mathbf{T}]$ ,  $m < n$  is a monic divisor of a monic  $P \in \mathbf{Z}[\mathbf{T}]$ , its roots are bounded by  $B(P)$ . But, up to sign,  $b_i$  is the sum of all products of  $i$  distinct of its roots leading to the bound  $|b_i| \leq \binom{m}{i} (B(P))^i$ . This shows, that there is only a finite number of  $Q$  which are candidate to divide  $P$  and that their coefficients are in the (huge) box  $[-2^{n-2}(B(P))^{n-1}, 2^{n-2}(B(P))^{n-1}]$ . So if we have a computer with huge capacity, we could decide whether  $P$  is irreducible over  $\mathbf{Q}$  or not. But this method is of exponential complexity. Fortunately, there exists algorithms in polynomial time using factorization of polynomial in finite fields (see for instance Berlekamp's algorithm in 9.6.6 or [13]) and Hensel's lemma (see 11.6.8) as starting points and subtle and difficult results about Euclidean lattices<sup>4</sup>. But the starting point of these algorithms is to improve these kind of bounds as we will do now.*

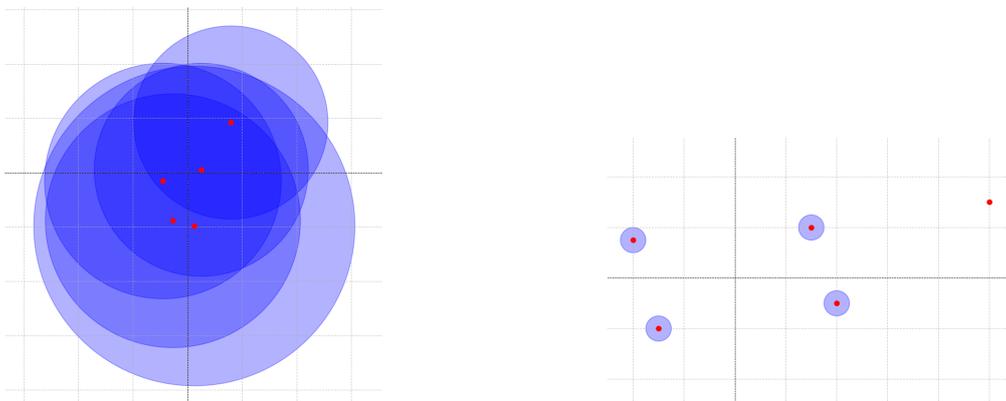
<sup>3</sup>The reader will give another proof of (2) using the continuity of roots.

<sup>4</sup>A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovasz, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), no.

**Remark(s) 14.3.3.3** Let  $A \in M_n(\mathbf{C})$ . We can certainly bound the coefficient of  $\chi_A$  in terms of the norm of  $A$ . For instance, using the polynomial definition of the determinant, we get (*exercise*) the very rough bound for these coefficients  $2^n n! (1 + \max |a_{i,j}|)^n$  giving a polynomial bound (at fixed  $n$ )  $i$  for the eigenvalues of  $A$ . We will explain how to get linear bounds in terms of the norm of  $A$ .

## 14.4 Localizing eigenvalues

### 14.4.1 Gershgorin disks



Gershgorin disks

We denote by  $D(z_0, R)$  the closed disk  $D(z_0, R) = \{z \in \mathbf{C} \text{ such that } |z - z_0| \leq R\}$ .

**Proposition 14.4.1.1** Let  $A \in M_n(\mathbf{C})$  and  $R_i = \sum_{j \neq i} |a_{ij}|$ ,  $i = 1, \dots, n$ .

1. (*Hadamard*) If  $A$  is strictly dominant diagonal, i.e.

$$\forall i \in \{1, \dots, n\}, \quad |a_{ii}| > R_i$$

then  $A$  is an invertible matrix.

2. (*Gershgorin I*) In general,

$$\text{Spec}(A) \subseteq \bigcup_{i=1}^n D(a_{ii}, R_i).$$

3. (*Gershgorin II*)<sup>5</sup> If  $F$  is a connected component<sup>6</sup> of  $\Gamma = \bigcup_{i=1}^n D(a_{ii}, R_i)$ , then the number of eigenvalues counted with multiplicities which are in  $F$  is the number of indices such that  $F$  is the union of the Gershgorin's disks  $D_i$ . In other words,  $\deg_F(\chi_A) = \text{Card}\{i | a_{i,i} \in F\}$ .

*Proof.*

1. Assume  $x = (x_i)$  is a nonzero vector in  $\text{Ker}(A)$  and let  $i$  such that  $|x_i|$  is maximal among the modulus of the coordinates of  $x$ . The  $i^{\text{th}}$  coordinate of  $Ax$  is  $\sum a_{i,j}x_j = 0$ . Therefore,

$$|a_{i,i}| |x_i| \leq \sum_{j \neq i} |a_{i,j}| |x_j| \leq |x_i| \sum_{j \neq i} |a_{i,j}|$$

and  $A$  is not dominant diagonal because one can divide this inequality by  $|x_i| > 0$ .

2. Apply (2) to  $A - \lambda \text{Id}$  with  $\lambda \in \text{Spec}(A)$ .
3. Let  $F'$  be the (finite) union of the connected components of  $\Gamma$  and  $d \in [0, \dots, n]$ . They are closed in  $\Gamma$  as any connected component and therefore are closed in  $\mathbf{C}$  because  $\Gamma$  is closed (even compact). The Gershgorin's disks  $D$  of  $A_t$  are  $D_i(A_t) = D(a_{i,i}, tR_i)$  and therefore are contained in  $D_i(A_1) = D_i(A)$ . In particular,  $\text{Spec}(A_t) \subset F \sqcup F'$  for all  $t \in [0, 1]$ . Let  $\Omega' = \mathbf{C} - F'$ . Let

$$A_t = \text{diag}(a_{i,i}) + t(A - \text{diag}(a_{i,i})), \quad t \in [0, 1]$$

Because  $F \subset \Omega'$ , one has  $\deg_{\Omega}(\chi_{A_0}) = d$  and by continuity of the roots of a polynomial (14.3.1.2)

$$\{t \mid \deg_F(\chi_{A_t}) \geq d\} = \{t \mid \deg_{\Omega'}(\chi_{A_t}) \geq d\}$$

is open in  $[0, 1]$ . But  $\text{Spec}(A_t) \subset F \sqcup F'$  and therefore,

$$\{t \mid \deg_F(\chi_{A_t}) \leq d\} = \{t \mid \deg_{F'}(\chi_{A_t}) \geq n - d\}$$

is also open and so is  $U_d = \{t \mid \deg_F(\chi_{A_t}) = d\}$  and  $[0, 1] = \sqcup_{d \leq n} U_d$ . By connectedness of  $[0, 1]$ , only one of the  $U_d$ 's is nonempty and equal to  $[0, 1]$ . But for  $d = \text{Card}\{i \mid a_{i,i} \in F\}$ , we have  $0 \in U_d$  because  $A_0 = \text{diag}(a_{i,i})$ .

□

Observe that one can shrink  $\Gamma$  using  $\text{Spec}(A) = \text{Spec}({}^t A)$ .

Using that the characteristic polynomial of a companion matrix  $C(P)$  of  $P(T) = T^n + \sum_{i < n} a_i T^i$  is  $P$ , we get the bound

**Corollary 14.4.1.2** *If  $P(z) = 0$ , then  $|z| \leq \max\{|a_0|, 1 + |a_i|, i > 0\} \leq 1 + \|P\|_{\infty}$ .*

## 14.4.2 Landau's inequality

<sup>5</sup>This refinement of Gershgorin can certainly be skipped in first reading. We give a proof because all the proofs that we have been able to find are at best incomplete. We assume that the reader is familiar with basics on connectedness.

<sup>6</sup>The reader will observe that a disk being connected,  $F$  is an union of some of the  $D_i$ 's.

**Proposition 14.4.2.1** (Landau) *Let  $P = a_n T^n + \dots + a_0 = a_n \prod (T - z_i) \in \mathbf{C}[T]$  be a polynomial of degree  $n$ , with complex roots  $z_1, \dots, z_n$  and*

$$M(P) = |a_n| \prod \max(1, |z_j|).$$

Then,

1.  $M(P)$  is multiplicative.
2.  $\frac{1}{2\pi} \ln \int_0^{2\pi} |P(e^{i\theta})|^2 d\theta = \|P\|^2$  (Parseval equality for polynomials).
3.  $\ln M(P) = \frac{1}{2\pi} \int_0^{2\pi} \ln |P(e^{i\theta})| d\theta$  (Jensen's equality for polynomials).
4.  $M(P) \leq \|P\|_2$  where  $(\sum |a_j|^2)^{1/2}$  is the standard Hermitian norm of  $P \in \mathbf{C}_n[T]$ .

This inequality is due to Landau and we give the following nice argument due to K. Mahler<sup>7</sup>

*Proof.*

1. Direct consequence of the formula  $a_n \prod_{i \in I} (T - z_i) a'_m \prod_{j \in J} (T - z_j) = a_n a'_m \prod_{k \in I \cup J} (T - z_k)$ .
2. Direct consequence of the formulas

$$|P(e^{i\theta})|^2 = P(e^{i\theta}) \overline{P(e^{i\theta})} = \sum_{k,l} a_k \bar{a}_l e^{i(k-l)\theta} \text{ and } \frac{1}{2\pi} \ln \int_0^{2\pi} e^{i(k-l)\theta} = \delta_{k,l}$$

3. Observe that if the equality is true for  $P, Q$  it is true for  $PQ$ . Because it is true in degree 0, we just have to prove the equality for  $P(T) = T - z$ . Recall that the logarithm function

$$z \mapsto \ln(1 - z) = - \sum_{n \geq 0} z^n / (n + 1)$$

is holomorphic on the open unit disk  $D$ . Moreover,  $\ln |1 - z|^2 - \ln(1 - z) - \ln(1 - \bar{z})$  is continuous on  $D$  with value in  $2i\pi\mathbf{Z}$  and therefore is equal to 0 for  $z \in D$ . We have for any  $\theta \in \mathbf{R}, z \in \mathbf{C}$  with  $|z| < 1$

$$2 \ln |e^{i\theta} - z| = \ln |1 - ze^{-i\theta}|^2 = \ln(1 - ze^{-i\theta}) + \ln(1 - \bar{z}e^{i\theta}) = - \sum_{n \geq 0} z^n e^{-ni\theta} - \sum_{n \geq 0} \bar{z}^n e^{ni\theta} / (n + 1)$$

with normal convergence in  $\theta$ . Integrating, we get

$$(*) \quad \frac{1}{2\pi} \int_0^{2\pi} \ln(|e^{i\theta} - z|) d\theta = 0 = \ln(\max(1, |z|)) \text{ if } |z| < 1$$

<sup>7</sup>K. Mahler, An application of Jensen's formula to polynomials, *Mathematika* 7 (1960), 98-100. We just simplify the argument avoiding the use of the general Jensen's formula for holomorphic functions.

If  $|z| > 1$ , we write

$$\frac{1}{2\pi} \int_0^{2\pi} \ln |e^{i\theta} - z| d\theta = \ln |z| + \frac{1}{2\pi} \int_0^{2\pi} \ln |z^{-1} e^{i\theta} - 1| d\theta = \ln |z| + \frac{1}{2\pi} \int_0^{2\pi} \ln |z^{-1} - e^{-i\theta}| d\theta$$

and by (\*) for  $z^{-1}$

$$\frac{1}{2\pi} \int_0^{2\pi} \ln |e^{i\theta} - z| d\theta = \ln(|z|) + \frac{1}{2\pi} \int_0^{2\pi} \ln |z^{-1} - e^{i\theta}| d\theta = \ln(|z|) = \ln(\max(1, |z|))$$

If  $|z| = 1$ , a continuity argument gives the result.

4. The logarithm being concave on  $\mathbf{R}$ , we have<sup>8</sup>,

$$\ln M(P)^2 \stackrel{(3)}{\leq} \frac{1}{2\pi} \int_0^{2\pi} \ln |P(e^{i\theta})|^2 d\theta \leq \ln \frac{1}{2\pi} \int_0^{2\pi} |P(e^{i\theta})|^2 d\theta \stackrel{(2)}{=} \ln \|P\|^2$$

□

### 14.4.3 Spectral radius

We define the spectral radius  $\rho(A)$  of  $A \in M_n(\mathbf{C})$  as

$$\rho(A) = \max_{\lambda \in \text{Spec}(A)} |\lambda|.$$

We want to estimate  $\rho(A)$  in terms of the size of  $A$ , precisely its norm, or better its operator norm. Any norm  $\|\cdot\|$  on  $\mathbf{C}^n$  induces a norm on  $M_n(\mathbf{C})$  by the rule

$$\|A\| = \sup_{x \neq 0} \|Ax\| / \|x\| = \sup_{\|x\|=1} \|Ax\|.$$

Such a norm is called an *operator norm* on  $M_n(\mathbf{C})$ . Although all norms are equivalent in finite dimension, the main asset of the operator norm is their multiplicativity property (check!)

$$(*). \quad \|AB\| \leq \|A\| \|B\|$$

**Exercise 14.4.4** Show that the operator norms of  $A \in M_n(\mathbf{C})$  associated to the 1-norm  $\|x\|_1 = \sum |x_i|$  is the sup of the 1-norm of the column of  $A$ .

Let  $\mathcal{N}$  be the set of operator norms on  $M_n(\mathbf{C})$

**Proposition 14.4.4.1** Let  $A \in M_n(\mathbf{C})$ .

- $\rho$  is a continuous in  $A$ .
- (Householder)  $\rho(A) = \inf_{\|\cdot\| \in \mathcal{N}} \|A\|$ .
- (Gelfand) For any norm on  $M_n(\mathbf{C})$ , one has  $\rho(A) = \lim_{k \rightarrow +\infty} \|A^k\|^{1/k}$ .

<sup>8</sup>This is Jensen's inequality in general, which is a simple exercise in our continuous case using approximation of integrals by Riemann's sums.

Let us start with a lemma. Although it a straightforward of Jordan reduction theorem, let us give a more elementary proof.

**Lemma 14.4.4.2** For any real  $\varepsilon > 0$ ,  $A$  is similar to some upper triangular matrix  $T_\varepsilon = ((t_{i,j}^\varepsilon)_{1 \leq i,j \leq n})$  such that:

$$\max_{1 \leq i \leq n} \sum_{j=i+1}^n |t_{i,j}^\varepsilon| < \varepsilon$$

*Proof.* Since the matrix  $A \in M_n(\mathbb{C})$  is triangularizable, one can assume  $A = ((t_{i,j})_{1 \leq i,j \leq n})$  is upper triangular. For  $\delta > 0$ , we have:

$$A_\delta = D_\delta^{-1} A D_\delta = \begin{pmatrix} a_{1,1} & \delta a_{1,2} & \dots & \delta^{n-1} a_{1,n} \\ 0 & a_{2,2} & \dots & \vdots \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & a_{n,n} \end{pmatrix} \text{ where } D_\delta = \text{diag}(1, \delta, \dots, \delta^{n-1})$$

Then  $A_\delta$  makes the job for  $\delta$  small enough. □

*Proof.* (Continuity) Use 14.3.1.3.

(Householder) Let  $x \in \mathbb{C}^n$  be a unit eigenvector of  $A$  whose eigenvalue has maximum modulus. We have  $\rho(A)\|x\| = \|Ax\| \leq \|A\|$  which gives:  $\rho(A) \leq \inf_{\|x\| \in \mathbb{N}} \|A\|$ .

Let us prove the reverse inequality. Let  $\varepsilon > 0$ , and, thanks to the preceding lemma, let us choose  $P_\varepsilon \in GL_n(\mathbb{C})$  such that  $A = P_\varepsilon^{-1} T_\varepsilon P_\varepsilon$  with  $T_\varepsilon$  as in the lemma. We choose the operator norm induced by  $\|x\| = \|P_\varepsilon x\|_\infty$ . where  $\|x\|_\infty = \sup(|x_i|)$  as usual. We obtain

$$\|A\| = \sup_{x \neq 0} \|Ax\|/\|x\| = \sup_{P_\varepsilon^{-1}x \neq 0} \|AP_\varepsilon^{-1}x\|/\|P_\varepsilon^{-1}x\| = \sup_{x \neq 0} \|P_\varepsilon AP_\varepsilon^{-1}x\|_\infty/\|x\|_\infty = \|P_\varepsilon^{-1}AP_\varepsilon\|_\infty.$$

Therefore,

$$\|A\| = \|P_\varepsilon^{-1}AP_\varepsilon\|_\infty = \|T_\varepsilon\|_\infty = \max_{1 \leq i \leq n} \left( |t_{n,n}|, |t_{i,i}| + \sum_{j=i+1}^n |t_{i,j}^\varepsilon| \right) \leq \rho(A) + \varepsilon$$

which gives reverse inequality  $\rho(A) = \inf_{\|x\| \in \mathbb{N}} \|A\|$ .

(Gelfand) Assume first  $\|\cdot\| \in \mathbb{N}$ . With the above notation, or  $k \in \mathbb{N}^*$ :

$$\|A^k\| = \|P_\varepsilon T_\varepsilon^k P_\varepsilon^{-1}\|_\infty \leq \gamma_\varepsilon \|A^k\|_\infty \leq \gamma_\varepsilon (\rho(A) + \varepsilon)^k$$

where  $\gamma_\varepsilon = \|P_\varepsilon\|_\infty \|P_\varepsilon^{-1}\|_\infty$ . Thus  $\|A^k\|^{1/k} \leq \gamma_\varepsilon^{1/k} (\rho(A) + \varepsilon)$ . On the other hand  $\rho(A)^k = \rho(A^k) \leq \|A^k\|$ . Since  $\gamma_\varepsilon^{1/k} \rightarrow 1$  as  $k \rightarrow +\infty$ , we deduce  $\rho(A) = \lim \|A^k\|^{1/k}$ . Now, if  $N$  is any norm on  $M_n(\mathbb{C})$ , there exists  $a, b > 0$  such that  $a\|A^k\| \leq N(A^k) \leq b\|A^k\|$  (equivalence of norms in finite dimension). Because  $\lim a^{1/k} = \lim b^{1/k} = 1$ , we get the result. □

### 14.4.5 Smoothness of simple eigenspaces

Let  $A_0 \in M_d(\mathbf{C})$  and assume  $\lambda_0 \in \text{Spec}(A)$  a simple root of  $\chi_{A_0}$ . Using the smoothness of simple roots (14.3.2.1) and the smoothness of  $A \mapsto \chi_A$ , we know that there exists a neighborhood  $\Omega$  of  $A_0$  and  $V \subset \mathbf{C}$  of  $\lambda_0$  and a smooth function  $\lambda : \Omega \rightarrow \mathbf{C}$  such that  $\lambda(A_0) = \lambda_0$  and  $\lambda(A)$  is the unique eigenvector of  $A$  belonging to  $V$  which can be assumed to be simple shrinking  $U$  if necessary. Let  $\pi_\lambda : U \rightarrow M_d(\mathbf{C})$  be the rank 1 projector onto  $\text{Ker}(A - \lambda \text{Id})$  (parallel to the other primary components).

**Proposition 14.4.5.1** *The projector  $\pi_\lambda$  is smooth.*

*Proof.* Let  $R$  be the ring of complex smooth functions on  $\Omega$ . By 1.3.1.1, one can write  $\chi_A = (T - \lambda)Q(T)$  for  $Q(T) \in R[T]$  and we have  $Q(\lambda) = \chi'_A(\lambda) \neq 0$  for all  $A \in \Omega$ . Dividing  $Q$  by  $T - \lambda$  in  $R[T]$  yields  $Q(T) = (T - \lambda)\tilde{Q}(T) + r$ ,  $r \in R$  and evaluating at  $\lambda$ , we get  $r = Q(\lambda)$  and therefore a Bézout relation

$$Q(T)/Q(\lambda) - (T - \lambda)\tilde{Q}(T)/Q(\lambda) = 1.$$

And using the Chinese Remainder Lemma as always, we have  $\pi_\lambda = Q(A)/Q(\lambda)$  which is smooth.  $\square$

Notice that, shrinking if necessary, we can choose continuously a basis of  $\text{Im}(\pi_\lambda)$  : pick a minimal number of independent columns of  $\pi_{\lambda_0}(A_0)$  and look at the locus of  $\Omega$  where these columns  $\pi_\lambda(A)$  are independent (semi-continuity of the rank).

## 14.5 Perron-Frobenius for positive matrices

We will present the nice presentation [7] of the classical Perron-Frobenius theory for real positive matrices due to Hannah Cairns with her kind permission. In the sequel, we say that a possibly rectangular real matrix  $A$  is non negative ( $A \geq 0$ ) if all its coefficients are  $\geq 0$  and positive  $A > 0$  if they are  $> 0$ .

**Theorem 14.5.0.1** (Perron-Frobenius I) *Let  $A \in M_n(\mathbf{R}^+)$  a positive matrix. Then:*

1.  $\rho = \rho(A)$  is a simple root of  $\chi_A$  and is nonzero.
2. The eigenspace of  $\rho$  is one dimensional generated by a positive vector.
3. All eigenvalues  $\lambda \neq \rho$  have modulus  $|\lambda| < \rho$ .

*Proof.* Let  $x \in \mathbf{C}^n$ . We will denote by  $|x|$  the vector whose components are  $|x_i|$ . If moreover  $x \in \mathbf{R}^n$ , we will use repeatedly the obvious but key fact

$$(*) \quad x \geq 0 \text{ and } x \neq 0 \Rightarrow Ax > 0$$

(choose  $x_j > 0$  and write  $(Ax)_i = \sum_k A_{i,k}x_k \geq A_{i,j}x_j > 0$ ).

In particular, we get  $A^k > 0$  /  $\text{Rightarrow} A^\ell > 0$  for  $\ell \geq k$  and therefore  $A$  cannot be nilpotent showing  $\rho > 0$ .

**Assume first  $A > 0$ .**

The key observation is the following.

Let  $\lambda \in \text{Spec}(A)$  with  $|\lambda| = \rho$  and  $x \neq 0$  an eigenvector for  $\lambda$ . Then,  $A|x| = \rho|x|$  and  $|x| > 0$ .

By the triangle inequality,  $A|x| \geq |Ax|$ , so  $A|x| \geq |Ax| = |\lambda x| = \rho|x|$ . If the two sides are equal, then we are done. Suppose that  $A|x| \neq \rho|x|$ . Then (\*) gives the strict inequality  $A^2|x| > \rho A|x|$ . By continuity, there is some  $r > \rho$  with  $A^2|x| \geq rA|x|$  and by induction using (\*) again we get for any  $m \geq 1$

$$A^{m+1}|x| \geq rA^m|x| \geq \dots \geq r^m A|x|$$

The miracle is that the 1-norm of a non negative vector is just the sum of its coefficients! Therefore, taking the 1-norm of both sides we get

$$\|A^{m+1}|x|\|_1 \geq \|r^m A|x|\|_1$$

or because both  $x$  and  $Ax$  are non zero,  $r^m \leq C\|A^{m+1}|x|\|_1$  for some  $C > 0$ . By Gelfand's theorem (14.4.4.1), this gives  $\rho < r \leq \rho$ , a contradiction and therefore  $A|x| = \rho|x|$ . Because  $A|x| > 0$  thanks to (\*) and  $\rho > 0$ , we get also  $|x| > 0$  hence (1).

Thus, we have proved that  $\rho \in \text{Spec}(A)$  and that  $|x|$  is a positive eigenvector for  $\rho$ . Hence we have  $|Ax| = \rho|x| = A|x|$  giving for instance

$$\sum A_{1,j} |x_j| = \left| \sum A_{1,j} x_j \right|$$

which is an equality in the triangle equality in  $\mathbf{C}^n$ . There exists therefore (14.6.1)  $\alpha \in \mathbf{C}$  such that  $A_{1,j}x_j = \alpha A_{1,j} |x_j|$  and therefore  $x = \alpha |x|$  proving  $\lambda = \rho$  because  $|x|$  is a nonzero eigenvector for both  $\rho$  and  $\lambda$  which proves (3).

For (2), let us choose  $x_0$  a non zero real vector of  $A$  for  $\rho$  and let  $y$  another such non-zero real eigenvectors for  $\rho$ . By (\*),  $|x_0|$  is an eigenvector for  $\rho$  and by the preceding point, there exists  $\alpha \in \mathbf{C}$  such that  $y = \alpha|x_0|$ . Because  $y, x_0$  are real,  $\alpha \in \mathbf{R}$  and  $|x_0|$  is a basis of the eigenspace of  $\rho$ , proving (2).

(3) is a duality argument. Because  ${}^tA$  and  $A$  have the same eigenvalues and  ${}^tA > 0 > 0$ , one can choose  $y > 0$  such that  ${}^tAy = \rho y$  or equivalently  ${}^tyA = \rho{}^ty$ . Let  $x$  be a positive basis of the line  $\text{Ker}(A - \rho \text{Id})$ . The hyperplane  $H_y$  defined by  $y$  is stable by  $A$  and has equation  $\{x|{}^tyx = 0\}$  (see cf. chapter 7 or check directly). Because  $x, y > 0$ , one has  ${}^tyx > 0$  and  $\mathbf{R}x \cap H_y = \{0\}$  and a decomposition in stable spaces  $\mathbf{R}^n = \mathbf{R}x \oplus H_y$  and  $A$  is similar to  $\text{diag}(\rho, B)$  for  $B \in M_{n-1}(\mathbf{R})$  and we have  $\chi_A(T) = (T - \rho)\chi_B(T)$ . If  $\rho$  is not simple,  $\chi_B(\rho) = 0$  and  $\rho \in \text{Spec}(B)$  which contradicts  $\dim \text{Ker}(A - \rho \text{Id}) = 1$  proving (3).

**Assume  $A^k > 0$  for some  $k > 0$ .**

We reduce to the previous case more or less straightforwardly. Let the eigenvalues of  $A$  be  $\lambda_1, \dots, \lambda_n$  in decreasing order of absolute value, repeated with respect with their multiplicity. Then the eigenvalues of the positive matrix  $A^k$  are  $\lambda_1^k, \dots, \lambda_n^k$ , again in decreasing order of absolute value.

By the above result,  $\lambda_1^k = \rho(A)^k$  is positive and has a positive eigenvector  $|x|$ , and the other eigenvalues  $\lambda_i^k$  are strictly smaller in absolute value, so  $\lambda_1^k > |\lambda_2|^k \geq \dots \geq |\lambda_n|^k$ . Taking the  $k$ th root, we get  $|\lambda_1| > |\lambda_2| \geq \dots \geq |\lambda_n|$ , so  $\lambda_1$  is a simple root of  $\chi_A$  and  $|\lambda_1| = \rho$ . In particular, the corresponding eigenspace  $V_{\lambda_1}(A)$  is one dimensional. But  $V_{\lambda_1}(A) \subset V_{\lambda_1^k}(A^k) = \mathbf{R}|x|$ , so the two spaces are equal and  $A|x| = \lambda_1|x|$ . Therefore,  $\lambda_1|x| = A|x| > 0$  and  $\lambda_1 > 0$  which shows  $\lambda_1 = \rho$ .  $\square$

**Corollary 14.5.0.2** *Assume  $A \geq 0$ . Then,  $\rho = \rho(A) \in \text{Spec}(A)$  and there is a non negative eigenvector  $x \neq 0$  for  $\rho(A)$ .*

*Proof.* Let  $A_k, k \geq 1$  be the sequence of positive matrices  $A_k = (a_{i,j} + 1/k)$  and take  $x_k$  a positive eigenvector of  $A_k$  for  $\rho(A_k)$  with  $\|x_k\|_1 = 1$ . By compactness of the (positive quadrant) of the unit sphere, one can assume  $\lim x_k = x$  with  $x \geq 0$  of norm 1 and (continuity of  $\rho$ )  $Ax = \rho x$ .  $\square$

### 14.5.1 Basics on graphs

For us, an oriented (finite) graph is a pair  $\mathcal{G} = (\mathcal{V}, \mathcal{E} \subset \mathcal{V} \times \mathcal{V})$  where  $\mathcal{V}$  is the (finite) set of vertices and  $\mathcal{E}$  the set of edges. As usual, we represent  $\mathcal{V}$  as a collection of points and each  $v, v'$  as an arrow  $v \rightarrow v'$ . There is obvious notions of paths from  $v$  to  $v'$ , length of path and so on.

To each graph is associated its adjacency matrix  $G$  defined by  $G_{v,v'} = 1$  if  $(v, v') \in \mathcal{E}$  and  $G_{v,v'} = 0$  else. An immediate induction shows that the number of length  $k$ -paths from  $v$  to  $v'$  of  $\mathcal{G}$  is  $G_{v,v'}^k$ . Certainly,  $G$  is a non-negative matrix.

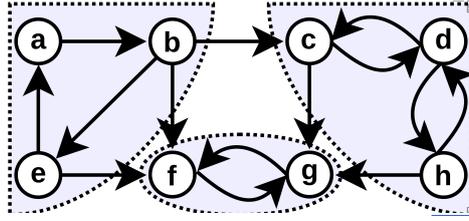
**Lemma 14.5.1.1** *The shortest length of a path from  $v$  to  $v'$  is  $\leq n$  where  $n$  is the number of vertices of  $G$ . In particular, matrix terms, if  $G_{v,v'}^k \neq 0$  for some  $k > 0$ , then  $G_{v,v'}^k \neq 0$  for some  $k$  with  $0 < k < n$ .*

*Proof.* A path of shortest length (when it exists!) has certainly distinct vertices and by the pigeon holes principle this number is  $\leq \text{Card}(\mathcal{V}) = n$  and its length is  $\leq n - 1$ .  $\square$

In general, mimicking the connected equivalence relation, for  $v, v' \in \mathcal{V}$ , we say

$$v \equiv v' \Leftrightarrow \text{there is a path from } v \text{ to } v' \text{ and from } v' \text{ to } v.$$

This is an equivalence relation and the equivalence classes are called the strongly connected components. An oriented graph is then said to be *strongly connected* if there is a unique connected component, i.e. if it is nonempty and if for any ordered pair  $(v, v') \in \mathcal{V} \times \mathcal{V}$ , there is a path from  $v$  to  $v'$ .



3 strong connected components

Conversely, to any  $A \in M_n(\mathbf{k})$ , one can associate a graph  $\mathcal{G} = \mathcal{G}(A)$  with  $\mathcal{V} = \{1, \dots, n\}$  and  $(i, j)$  is an edge if and only if  $a_{i,j} \neq 0$ . If  $A$  is moreover a non negative real matrix and  $G$  is the adjacency matrix of its graph, we have as before  $A_{i,j}^k \neq 0$  if and only if  $G_{i,j}^k \neq 0$  and therefore  $A_{i,j}^k \neq 0$  for some  $k > 0$  if and only if  $A_{i,j}^k \neq 0$  for some  $k$  with  $0 < k \leq n$ .

### 14.5.2 Perron-Frobenius for irreducible matrices

**Definition 14.5.2.1** A non negative matrix  $A \in M_n(\mathbf{R})$  is said to be irreducible if its graph  $\mathcal{G}(A)$  is strongly connected. In particular,  $A \neq 0$ .

Therefore, because

$$A \text{ is irreducible if for any } i, j, \text{ there exists } 1 \leq k \leq n - 1 \text{ such that } A_{i,j}^k > 0.$$

Of course, if  $A \geq 0$  satisfies  $A^k > 0$  for some  $k > 0$ , then  $A$  is irreducible. The converse is not true but one can compare precisely the two notions in terms of spectral radius.

**Lemma 14.5.2.2** Let  $A \geq 0$ . Then,  $A$  is irreducible if and only if  $(\text{Id} + A)^{n-1} > 0$ .

*Proof.* Let  $(i, j) \in \{1, \dots, n\}$ .

$\Rightarrow$  Let  $1 \leq k \leq n - 1$  such that  $A_{i,j}^k > 0$ . By the Newton formula, we have

$$(\text{Id} + A)_{i,j}^{n-1} = \sum_{\ell \leq n-1} \binom{n-1}{\ell} A_{i,j}^\ell \geq \sum_{1 \leq \ell \leq n-1} \binom{n-1}{\ell} A_{i,j}^\ell \geq A_{i,j}^k > 0.$$

$\Leftarrow$  If  $i \neq j$ , we have in the same way

$$0 < (\text{Id} + A)_{i,j}^{n-1} = \sum_{\ell \leq n-1} \binom{n-1}{\ell} A_{i,j}^\ell = \sum_{1 \leq \ell \leq n-1} \binom{n-1}{\ell} A_{i,j}^\ell$$

and there certainly exists  $1 \leq \ell \leq n - 1$  such that  $A_{i,j}^\ell > 0$ . If  $i = j$ , one has  $(\text{Id} + A)_{i,i}^{n-1} \geq 1 > 0$ .  $\square$

**Theorem 14.5.2.3** (Perron-Frobenius II) *Let  $A \in M_n(\mathbf{R}^+)$  be an irreducible matrix. Then:*

1.  $\rho = \rho(A)$  is a simple root of  $\chi_A$ .
2. The eigenspace of  $\rho$  is one dimensional generated by a positive vector.
3. All eigenvalues  $\lambda \neq \rho$  have modulus  $|\lambda| < \rho$ .
4.  $\rho(A) > 0$ .

*Proof.* I claim  $\rho(\text{Id} + A) = 1 + \rho(A)$ . Indeed, let  $1 + \lambda \in \sigma(\text{Id} + A)$ . We have  $\lambda \in \sigma(A)$  and by triangle inequality  $1 + |\lambda| \leq 1 + |\lambda| \leq 1 + \rho(A)$  showing  $\rho(\text{Id} + A) \leq 1 + \rho(A)$ . Conversely, by 14.5.0.2,  $\rho(A)$  is an eigenvalue of  $A$  and therefore  $1 + \rho(A)$  is an eigenvalue of  $\text{Id} + A$  implying  $1 + \rho(A) \leq \rho(\text{Id} + A)$ .

1. By 14.5.0.1 for  $\text{Id} + A$  we know therefore that  $1 + \rho(A)$  is a simple root of  $\chi_{(\text{Id} + A)}(T) = \chi_A(T - 1)$ .
2. By 14.5.0.2, let  $x \neq 0$  be a non negative eigenvector of  $A$  for  $\rho(A)$  and therefore a non negative eigenvector of the positive matrix  $(\text{Id} + A)^{n-1}$ . By 14.5.0.1 (2) applied to  $\text{Id} + A$ , we get  $x > 0$ .
3. Follows directly from 14.5.0.1 (3) applied to  $\text{Id} + A$  and  $\text{Spec}(\text{Id} + A) = \{1 + \lambda, \lambda \in \text{Spec}(A)\}$ .
4. We have  $Ax = \rho(A)x$  and  $x > 0$ . Therefore  $Ax > 0$  and  $\rho(A) > 0$ .

□

**Terminology:** An eigenvalue  $\lambda$  of  $A \in M_n(\mathbf{C})$  is called a *dominant eigenvalue* if  $\lambda$  has multiplicity 1 in  $\chi_A$  and  $|\lambda| > |\mu|$  for all eigenvalues  $\mu \neq \lambda$ .

### 14.5.3 A classical illustration

Rather than classically choosing the historical (and nowadays quite old-fashioned) PageRank algorithm of Google<sup>9</sup>, let us explain how primitive matrices are used in population dynamics through the so called Leslie model<sup>10</sup>.

Lets divide the population in  $n$  age classes  $G_k$ . We assume that the birth  $b_k$  rate and survival  $s_k$  rate in each age class  $G_k$  is independent of the (discrete) time  $t \in \mathbf{N}$ . If  $N_k(t) = \text{Card } G_k$ , this means  $N_1(t + 1) = b_1N_1(t) + b_2N_2(t) + \dots + b_nN_n(t)$  for the offsprings (the birth rate includes the early deaths in the first

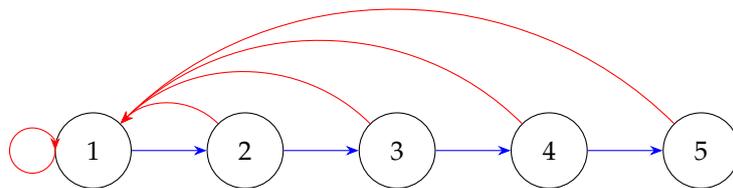
<sup>9</sup>Cf. the historical paper "The PageRank Citation Ranking: Bringing Order to the Web" by L. Page, S. Brin, R. Motwani and T. Winograd. <http://ilpubs.stanford.edu:8090/422/> and for the mathematics behind for instance A. N. Langville and C. D. Meyer Jr. A survey of eigenvector methods for Web information retrieval, SIAM Rev. 47 (2005), no. 1, 135–161

<sup>10</sup>P. H. Leslie. On the Use of Matrices in Certain Population Mathematics. Biometrika 33, no. 3 (1945): 183–212. <https://doi.org/10.2307/2332297>.

age class)  $N_k(t + 1) = s_{k-1}N_{k-1}(t)$   $k = 2, \dots, n$  that is  $N(t + 1) = AN(t)$  where  $A$  is the Leslie matrix

$$A = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ s_1 & 0 & \dots & 0 \\ 0 & s_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & & s_{n-1} & 0 \end{pmatrix}.$$

If we restrict to age class of the population of childbearing age, one can assume that  $b_i, s_j > 0$  and the graph of  $A$  has shape



and is certainly strongly connected. Using the Perron-Frobenius II theorem 14.5.2.3, we show immediately that the normalized histogram of the population defined the normalized vector  $N(t)/\|N(t)\|$  where  $N(t) = {}^t(N_1(t), \dots, N_n(t))$  will converge when  $t$  goes to  $\infty$  to the unique positive eigenvector of  $A$  for  $\rho(A)$  of 1-norm 1.

### 14.5.4 Markov chains

In this item, we assume that the reader is familiar with basics on probabilities. We consider a sequence of random variables  $X_0, X_1, \dots$  with values in  $\{1, \dots, n\}$  on some probability space  $\Omega$ . We assume (which is a very strong assumption) that the transition probability matrix  $P \geq 0$  defined by

$$P_{i,j} = \text{Prob}(X_{t+1} = i \mid X_t = j)$$

does not depend on on the (discrete) time  $t$ .

Writing  $\Omega = \sqcup_i X_{t+1} = i$ , we get  $\sum_i P_{i,j} = 1$  for all  $j$ : the 1-norm of each column is 1 (a positive matrix with this property is called *stochastic*).

Writing  $\Omega = \sqcup_j X_t = j$ , we get  $\sum_i P_{i,j} p_{t,i} = 1$  where  $p_t = (\text{Prob}(X_t = i))_i$  is the probability distribution of  $X_t$ . In other words, we have

$$p_{t+1} = Pp_t.$$

If we assume that  $P$  is moreover irreducible, the Perron-Frobenius II theorem 14.5.2.3 shows that  $p_t$  converges when the discrete time  $t$  goes to  $\infty$  to the unique positive eigenvector of  $P$  for  $\rho(P)$  of 1-norm 1 as before. Of course, more can be said by analyzing carefully the speed of convergence for instance and so on.

## 14.6 Exercices

**Exercise 14.6.1** Let  $z_i$  be  $n$  complex numbers such that the triangle inequality is an equality  $|\sum z_i| = \sum |z_i|$ . Show that there exists  $\alpha \in \mathbf{C}$  such that  $(z_i) = \alpha(|z_i|)$ . Compare with theorem 1.39 of [19]. [Hint : assume first  $\sum z_i \in \mathbf{R}^+$ ].

**Exercise 14.6.2** Continuité avec  $P'/P$ .

**Exercise 14.6.3** Généralités sur la topo quotient

**Exercise 14.6.4**  $\mathbf{C}^n/S_n = \mathbf{C}^n$  comme métrique

**Exercise 14.6.5** distance Hausdorff

**Exercise 14.6.6** Let  $\mathcal{R} \subset M_n(\mathbf{C})$  the set of matrices with real spectrum. We define the eigenvalue functions on  $\mathcal{R}$  by ordering the eigenvalues of  $A \in \mathcal{R}$ ,  $\lambda_1(A) \geq \lambda_2 \geq \dots \geq \lambda_n(A)$ . Let  $\Omega \subset \mathcal{R}$  be the open subset of  $M_n(\mathbf{R})$  of matrices with distinct real eigenvalues.

1. Prove that  $\lambda_i$  is a continuous function on  $\mathcal{R}$ .
2. Prove that the restriction of  $\lambda_i$  to  $\Omega$  is a smooth function.
3. If  $n \geq 2$ , prove that there exists no continuous function  $\lambda$  on  $M_2(\mathbf{C})$  such that  $\lambda(A) \in \text{Spec}(A)$  for all  $A \in \text{Spec}(A)$ .

**Exercise 14.6.7** 1. Prove that the closure in  $M_n(\mathbf{R})$  of diagonalizable matrices in the set of trigonalizable matrices.

2. What is its interior ?
3. Same questions replacing  $\mathbf{R}$  by any subfield of  $\mathbf{C}$ .

**Exercise 14.6.8** Let  $A(a, b, c) = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$  and  $\Omega$  the set of  $(a, b, c) \in \mathbf{C}^3$  such that  $\det(A) = 0$ . Compute the spectral projector  $e_0$  and observe that it is smooth on the whole  $\Omega$ . Show that there does not exist any continuous function  $v_0 : \Omega \rightarrow \mathbf{C}^3 - \{0\}$  such that  $v_0(a, b, c)$  is a basis of  $A(a, b, c)$ .

**Exercise 14.6.9** Let  $\Omega \rightarrow M_2(\mathbf{C})$  be the set of rank 1 matrices. Show

1.  $\Omega$  is open.
2. There does not exist any continuous map  $x : \Omega \subset \mathbf{C}^2 - \{0\}$  such that  $Ax = 0$  for all  $A \in \Omega$ .

**Exercise 14.6.10** We keep the hypothesis of the theorem and let  $x \in \mathbf{R}^n - \{0\}$  such that  $x \geq 0$ .

1. Show that  $\lim (A/\rho)^k = \pi_\rho$ .
2. Prove  $\pi_\rho(x) \neq x$ .
3. Prove that  $A^k x / \|A^k x\|$  is well defined if  $k \gg 0$  and converges to a positive basis of  $\text{Ker}(A - \rho \text{Id})$ .

4. How can you generalize if we only assume that  $A$  has a unique eigenvalue of maximal modulus?

**Exercise 14.6.11** (Power method) Let  $M \in M_d(\mathbf{C})$ . Show that  $A$  has a dominant eigenvalue if and only if there is a sequence of complex numbers  $z_n$  such that  $\lim z_n A^n$  is a rank 1 projector. Can you give a way to approximate the corresponding eigenvalue?

**Exercise 14.6.12** Let  $A = (a_{i,j})_{1 \leq i,j \leq 2}$  be a random matrix with coefficients 4 independent centered Gaussian variables. Prove that the probability that  $\chi_A$  is split over  $\mathbf{R}$  is  $1/2$ . How can you generalize?

**Exercise 14.6.13** Let  $A : \mathbf{R} \rightarrow M_n(\mathbf{C})$  be a smooth application and assume that  $A(0)$  has a dominant eigenvalue. Show that  $t \mapsto \rho(A(t))$  is smooth in a neighborhood of 0.

**Exercise 14.6.14** Let  $x$  be a complex number algebraic over  $\mathbf{Q}$ .

1. Show that there exists a unique primitive polynomial  $P \in \mathbf{Z}[T]$  with positive dominant coefficient which cancels  $x$  and is irreducible over  $\mathbf{Q}$ .
2. We define the height of  $x$  by  $1/d \ln M(P)$  (cf. Landau's inequality). Show that there exists a finite number of algebraic numbers with bounded height and degree.



## **Chapter 15**

# **Index et bibliography**

# Index

- algebraic,
  - element, 65
  - integer, 65
- basis,
  - adapted basis, 86
  - ante-dual, 97
  - dual, 96
- Berlekamp's algorithm, 130
- bicommutant, 117
- Bézout equivalence, 84
- Bézout matrix, 13
- Cayley-Hamilton Theorem, 22
- characteristic of a ring, 145
- Chinese remainder lemma, 67
- cokernel, 34
- commutant, 112
- commutative diagram, 38
- commutator, 26
- companion matrices, 111
- complement of a submodule, 36
- complex of modules, 37
- content, 125
- decomposition,
  - Frobenius, 112
- derived subgroup, 26
- determinant trick, 64
- diagonalizable, 110
- diagram, 38
- dilatation, 13
- domain, 13
- dominant eigenvalue, 194
- duality,
  - bracket, 95
  - contravariance, 101
  - convention of biduality, 100
  - differential, 97
  - Jacobian, 97
  - orthogonal, 96
  - polar, 96
  - transpose, 100
- endomorphism,
  - cyclic, 112
  - absolutely semisimple, 146
- equivalence of endomorphisms, 37
- equivalent matrices, 23
- Euclidean division in  $\mathcal{R}[T]$ , 14
- exact sequence, 36
- finite presentation modules, 51
- Fitting ideals, 50
- flatness, 171
- fraction field, 55
- Frobenius normal form, 112
- functor, 41
- functoriality,
  - of the cokernel, 38
  - of the kernel, 40
- Gauss,
  - elimination, 23
  - equivalent, 23
- GCD, 124

- Gershgorin disks, 185
- graph,
  - strongly connected, 192
- greatest common divisor GCD, 83
- group
  - solvable, 159
  - unipotent, 159
- idempotent, 68
- inductive set, 15
- integers,
  - rings of, 65
- integral domain, 54
- integral element, 65
- irreducibility of  $\Phi_n$  over  $\mathbf{Q}$ , 129
- irreducible element,
  - existence, 123
  - uniqueness of the decomposition into, 122
- irreducible elements,
  - of  $\mathbf{R}[T]$ , 126
- irreducible matrix, 193
- Jordan-Chevalley decomposition, 147
- Krull's intersection theorem, 76
- Landau's inequality, 186
- LCM, 124
- lemma,
  - Euclid, 121
  - five, 55
  - Gauss lemma for PID, 83
  - Hensel, 147
  - Krull, 15
  - Nakayama, 65
  - Zorn, 15
- Leslie matrix, 195
- minor of a matrix, 47
- module, 32
- module,
  - $V_a$ , 43
  - torsion, 54
  - associated with an endomorphism, 43
  - cyclic, 63
  - free, 52
  - Noetherian, 74
  - quotient, 34
  - semisimple, 141
- morphism,
  - Frobenius, 145
- Noetherian,
  - Hilbert's basis theorem, 76
  - module, 74
  - ring, 74
- operator norm, 188
- order,
  - $\leq$  on types, 169
  - $\leq$  on partitions, 172
  - $\preceq$  on types, 169
- partition of an integer, 136
- perfect group, 26
- Permanence principle of algebraic identities, 20
- permutation matrix, 13
- Perron-Frobenius Matrices, 190
- polynomial
  - cyclotomic, 128
- primary decomposition, 133
- primitive, 126
- quotient, 34
- reduced ring, 144
- reduction,
  - Jordan, 136
  - Frobenius, 112
- ring,

- Euclidean, 82
  - Noetherian, 74
  - Noetherian UFD, 124
  - PID, 82
  - UFD or factorial, 121
- semi-continuity of the rank, 177
- semisimple,
- endomorphism, 142
  - module, 141
- similarity invariants, 106, 108
- similarity of endomorphisms, 37
- Smith's normal form, 86
- Snake lemma, 55
- spectral projection, 135
- spectral radius, 188
- stable subspace, 43
- theorem,
- structure of finite type modules over PID, 86
  - Bézout, 83
- torsion, 53
- transvection, 13
- type, 168
- unipotent matrix, 159
- universal property,
- of the cokernel, 42
  - of the kernel, 42
  - of the product of modules, 41
  - of the sum of modules, 41

# Bibliography

- [1] D. Bartl. A very short algebraic proof of the farkas lemma. *Math Meth Oper Res*, page 101–104, 2012.
- [2] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for  $SL_n$  ( $n \geq 3$ ) and  $Sp_{2n}$  ( $n \geq 2$ ). *Inst. Hautes Études Sci. Publ. Math.*, 33:59–137, 1967.
- [3] E. Bishop. *Foundations of constructive analysis*. McGraw-Hill Book Co., New York-Toronto-London, 1967.
- [4] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.
- [5] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 1 à 3*. Hermann, Paris, 1970.
- [6] N. Bourbaki. *Algebra. Chapters 4–7*. Springer-Verlag, Berlin, 2007.
- [7] H. Cairns. Perron’s theorem in an hour. *Amer. Math. Monthly*, 128(8):748–752, 2021.
- [8] K. Chemla and S. Guo. *The Nine Chapters: A Mathematical Classic of Ancient China and its Commentaries*. Dunod, Paris, 2005.
- [9] R. Douady and A. Douady. *Algèbre et théories galoisiennes. 1*. CEDIC, Paris, 1977.
- [10] H. Fitting. Die Determinantenideale eines Moduls. *Jahresber. Dtsch. Math.-Ver.*, 46:195–228, 1936.
- [11] M. Gerstenhaber. On dominance and varieties of commuting matrices. *Ann. of Math. (2)*, 73:324–348, 1961.
- [12] D. R. Grayson. Sk1 of an interesting principal ideal domain. *Journal of Pure and Applied Algebra*, 20:157–163, 1981.
- [13] D. Hernandez and Y. Laszlo. *Introduction to Galois theory*. Springer Undergraduate Mathematics Series. Springer, 2024.
- [14] D. Hilbert. Ueber die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890.
- [15] F. Klein. *Le programme d’Erlangen*. Collection “Discours de la Méthode”. Gauthier-Villars Éditeur, Paris-Brussels-Montreal, Que., 1974. Considérations comparatives sur les recherches géométriques

modernes, Traduit de l'allemand par H. Padé, Préface de J. Dieudonné, Postface de François Russo.

- [16] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [17] J. Milnor. Whitehead torsion. *Bull. Amer. Math. Soc.*, 72:358–426, 1966.
- [18] E. Noether. Idealtheorie in Ringbereichen. *Math. Ann.*, 83(1-2):24–66, 1921.
- [19] W. Rudin. *Real and complex analysis*. McGraw-Hill Book Co., New York, third edition, 1987.
- [20] B. L. van der Waerden. *Modern Algebra. Vol. I*. Frederick Ungar Publishing Co., New York, N. Y., 1949.
- [21] B. L. van der Waerden. *Modern Algebra. Vol. II*. Frederick Ungar Publishing Co., New York, N. Y., 1950.