



Melancholia, Albrecht Dürer

©Y. Laszlo

TBD

Volume I

Yves Laszlo

and

Laurent Moonens, Thomas Mordant, Damien Simon

Yves.Laszlo@universite-paris-saclay.fr

Beta version of March 16, 2025 with typos and mistakes

Contents

1	Introduction	9
1.1	Point of view	10
1.2	Prerequisites and conventions (in progress)	12
1.2.1	Prerequisites	12
1.2.2	Conventions	12
1.3	Useful tools	14
1.3.1	Division by Monic Polynomials	14
1.3.2	Zorn's Lemma and application	14
I	Linear Algebra over Rings	17
2	Warm-up I: review on basic linear algebra	19
2.1	Introduction	19
2.2	Euclidean plane	20
2.2.1	Euclidean Norm	20
2.2.2	Non oriented angle of pair of vectors or lines	21
2.2.3	Orthogonality in oriented Euclidean planes	22
2.2.4	Oriented angles of vectors	23
2.2.5	Isometries	24
2.2.6	Symmetric real matrices	26
2.3	General linear maps of the plane	27
2.3.1	Minimal polynomial	27
2.3.2	Cyclic vectors	27
2.4	Exercices	28
3	Warm-up II: duality	29
3.1	Introduction	29
3.2	Basic notions	29
3.3	Motivation	31

3.4	Formal Biorthogonality	31
3.5	Ante-dual Basis: Biduality	32
3.6	Orthogonal and Polar in Finite Dimension	32
3.7	Biduality Conventions (Finite Dimension)	33
3.8	Contravariance	34
3.9	Exercises	35
4	Matrices with Ring coefficients	37
4.1	Introduction	37
4.1.1	Algebraic identities extension principle	37
4.1.2	Cayley-Hamilton in $M_n(\mathbb{R})$	38
4.2	Maximal rank matrices	39
4.3	Reminder on Gauss elimination method	40
4.3.1	The usual field case	41
4.3.2	A few universal formulas	41
4.4	Application to subgroups of $GL_n(\mathbf{k})$	43
4.4.1	General transvections	44
4.4.2	Normal subgroups of $GL(V)$	44
4.5	Exercises	46
5	Modules	47
5.1	Introduction	47
5.2	Vocabulary and first examples	48
5.2.1	Modules	48
5.2.2	Morphisms	50
5.2.3	Quotient, cokernel	51
5.2.4	A key example: the $\mathbf{k}[T]$ -module V_a	53
5.3	Exact sequences and diagrams	53
5.3.1	Exact sequences	54
5.3.2	A key exact sequence	54
5.3.3	Commutative diagrams	55
5.4	Functoriality and diagram chasing	56
5.5	Universal properties	59
5.5.1	Sum and product	59
5.5.2	Kernel and cokernel	60
5.6	Cokernel of Diagonal Matrices	61
5.7	Invariant ideals of modules	63
5.7.1	Determinantal ideals	63

<i>CONTENTS</i>	5
5.7.2 Fitting ideals	64
5.8 Properties to handle with caution	67
5.8.1 Finiteness	67
5.8.2 Free modules	68
5.8.3 Torsion	69
5.8.4 Summary of some specifics of Modules	70
5.9 Exercises	70
6 Rings and Modules	75
6.1 Introduction	75
6.2 Quotient rings	75
6.2.1 Definition	75
6.2.2 Product Rings	76
6.2.3 Cyclic modules and quotient rings	77
6.3 Algebras	77
6.4 Integrality	78
6.4.1 An Application of Cayley-Hamilton	78
6.4.2 Rings of Integers	79
6.5 The Chinese remainder lemma	80
6.6 Exercises	82
7 Noetherianity	85
7.1 Introduction	85
7.2 Noetherian Modules	85
7.2.1 Stability under exact sequences	87
7.2.2 Hilbert's Basis Theorem	88
7.3 Exercises	88
8 Matrix and modules over PID	91
8.1 Introduction	91
8.2 Survival kit for PID and Euclidean rings	92
8.3 Matrix equivalence in PID and Euclidean rings	93
8.3.1 Invariant ideals of a matrix	93
8.4 Invariant factors of a module	95
8.4.1 The Euclidean case	96
8.5 About uniqueness of invariant ideals	97
8.6 Supplementary Section: Insight into K-Theory	98
8.7 Exercises	100

II	Linear Algebra over Fields	103
9	Similarity in $M_n(\mathbf{k})$	105
9.1	Introduction	105
9.2	Similarity in $M_n(\mathbf{k})$	106
9.2.1	Similarity invariants	106
9.2.2	Explicit computations of similarity invariants	107
9.3	An important example: diagonalization	109
9.4	Frobenius Decomposition	110
9.5	Applications	112
9.5.1	Stable subspaces	112
9.5.2	Commutant	113
9.6	An algorithm from \sim to \approx	114
9.7	Summary on Similarity Invariants	115
9.8	Exercises	116
10	The Irreducible Toolbox	117
10.1	Introduction	117
10.2	An UFD Criterion	117
10.2.1	Uniqueness Condition	118
10.2.2	Existence Criterion	120
10.3	GCD, LCM in UFD	121
10.4	Transfer of the UFD property	122
10.4.1	Gauss' content	122
10.4.2	The Transfer Theorem	123
10.5	Irreducibility of the Cyclotomic Polynomial Over \mathbf{Q}	124
10.6	Exercises	126
11	Primary decomposition in PID	127
11.1	Introduction	127
11.2	Torsion Modules over PID	127
11.2.1	Primary Decomposition	128
11.2.2	Invariant ideals and primary decomposition	129
11.3	Application: Jordan Reduction	130
11.3.1	Examples	131
11.4	Exercises	133

12 Semisimplicity	135
12.1 Introduction	135
12.2 Semi-simple Modules	135
12.3 «Reminder» on perfect fields	138
12.3.1 Sums of semi-simple endomorphisms	140
12.4 Jordan-Chevalley decomposition	140
12.4.1 Hensel's lemma and existence	140
12.4.2 Uniqueness	142
12.4.3 Similarity class of the components	142
12.4.4 Appendix: What about the algorithmic nature of the decomposition?	143
12.4.5 d -th roots in GL_n	144
12.5 Exercises	145
13 Simultaneous reduction	147
13.1 Introduction	147
13.2 Commuting family of matrices	148
13.3 The Burnside-Wedderburn theorem	149
13.4 Stable family of nilpotent and unipotent matrices	150
13.5 Connected solvable matrix subgroups	151
13.5.1 Basics on solvable groups	151
13.5.2 The Lie-Kolchin theorem	152
13.6 Exercises	153
III About continuity of matrix reduction	155
14 Topology of similarity classes	157
14.1 Introduction	157
14.2 χ -types	158
14.3 $\underline{P} \preceq \underline{Q} \Rightarrow \underline{P} \leq \underline{Q}$	160
14.4 $\underline{P} \leq \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$	161
14.4.1 An elementary deformation	161
14.4.2 $\leq = \preceq$	162
14.5 Topological applications	164
14.5.1 Topology of the fibers $\mu^{-1}(\chi)$	165
14.5.2 Global properties of $M_n(\mathbf{k})/GL_n(\mathbf{k})$	166
14.6 Exercises	168

15 Eigenvalues and primary components	169
15.1 Introduction	169
15.2 Continuity of primary components	169
15.3 Regularity of polynomial roots	171
15.3.1 Continuity	171
15.3.2 Smoothness of simple roots	173
15.4 Localizing eigenvalues	173
15.4.1 Gershgorin disks	173
15.4.2 Spectral radius	175
15.4.3 Smoothness of simple eigenspaces	176
15.4.4 Positive matrices	177
15.4.5 Basics on graphs	179
15.4.6 Irreducible matrices	180
15.4.7 A classical illustration	181
15.4.8 Markov chains	182
15.5 Exercices	182
16 Index et bibliography	185

Chapter 1

Introduction

À réécrire

In 1872, Felix Klein posed the following question. "Given a multiplicity and a group, to study the beings from the point of view of properties that are not altered by the transformations of the group... this can also be expressed as follows: given a multiplicity and a transformation group; develop the theory of invariants relative to this group" ([15]).



Felix Klein

In this first volume notes, we concretely illustrate this visionary viewpoint by classifying geometric objects via invariants under various group actions (invariant factors, similarity invariants...) and different perspectives (algebraic, topological...).

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

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 of a lot of more general subjects like arithmetic, K-theory, algebraic geometry, ...). It is definitely not our pretentiousness 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 the module language theory in order to solve the following problem as our typical illustration: how to decide when two square matrices are similar? We did not use any reduction theory, eigenvalue or irreducible elements to solve this classification problem. The gain is

that we can solve this problem in a perfectly algorithmic way, in a field independent way, (contrary to any method based on eigenvalues because in general computing roots of a polynomial is hopeless). The cost to pay is non continuity of these algorithms (even they are semi-continuous in some sense). We discuss the intrinsic aspects 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 in linear terms (eigenvalues) or more generally in irreducible polynomials. The good news is that this process has continuity properties. The cost to pay is that we do not know how to factorize a polynomial in general. We have include a section about simultaneous reductions of matrices stressing the important notion of irreducible action of matrices.

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

We strive to do so in a *concrete* manner, i.e., with methods that lead to algorithms. It is indeed better to know how to construct an object than to simply know of its existence. The aim of the course, however, is not to provide optimized programs in terms of efficiency (that's another subject, and interesting at that!), but to explore the *how-to*. One quickly encounters the numerical flaws of typical Gauss elimination algorithms.

It is not, however, about giving formally constructivist methods ([3]) but about providing as much as possible existence theorems that can explicitly lead to the construction of the object in question, for example, through a computer.

The material of this book is more or less classical, only the perspective being somehow more original.

We strongly advise the reader to implement the various algorithms on a machine: this will allow them to verify that they have thoroughly understood the proofs. On our part, we have used the SAGEMATH program, based on Python.

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

1.1 Point of view

There are plenty ways to do mathematics and is rarely the case to have a unique good one. Writing a book is emphasizes some choice. Finding a path between these two peaks guided our work.

Let us illustrate our purpose by two extreme ways of thinking mathematics by two universal genius. In his huge *Récoltes et Semailles* writing¹, explains how generalizing problems is a fruitful way to solve problems.

Let's take, for example, the task of proving a theorem that remains hypothetical (which, for some, might seem to be the essence of mathematical work). I see two extreme approaches to tackling this. The first is the hammer and chisel method, where the problem is seen as a tough, smooth nut, and the goal is to

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



Alexander Grothendieck

reach the nourishing core protected by the shell. The principle is simple: you place the edge of the chisel against the shell and strike hard. If necessary, you repeat this in several different spots 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 my mind earlier is that you soak the nut in an emollient liquid—why not simply water? From time to time, you rub it to help the liquid penetrate better, but otherwise, you let time do its work. Over the weeks and months, the shell softens—and when the time is ripe, a gentle hand pressure is enough, and the shell opens like that of a perfectly ripe avocado. Or, you let the nut ripen under the sun and rain, and perhaps even the frost of winter. When the time is right, a delicate sprout emerges from the nourishing core, piercing the shell as if in play—or, better said, the shell opens on its own, allowing it passage. [...]

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

This way to go from the peculiar to the general contrasts with Descartes' method².



René Descartes

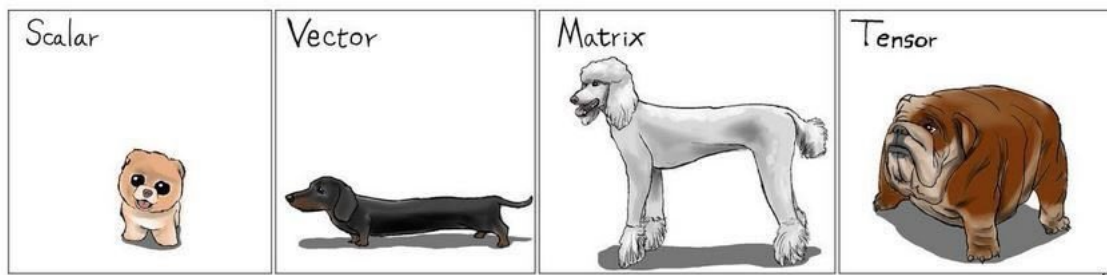
- *Not to accept anything as true that I did not clearly know to be so.*
- *To divide each of the difficulties I examined into as many parts as possible and as might be required for their best resolution.*
- *To conduct my thoughts in an orderly manner, beginning with the simplest and easiest-to-know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

²R. Descartes, *Discourse on the Method* (1637), Gallimard (2009).

- To make everywhere such complete enumerations, and such general reviews, that I might be assured 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 the reader familiar to the basic definition in algebra without any other expertise. From a general point of view, the reader is assumed to be familiar with the general definitions of rings, ideals. . . . For convenience of the reader, we recall the notion of quotient (6.2). Some familiarity with basic algebraic properties of fields, \mathbf{Z} and $\mathbf{k}[T]$, is assumed to be known (they are Principal Ideal Rings -PID-). To make the reading easier, a proof of the main results will be given in 8.2 and in (10).

No other knowledge of linear algebra is assumed beyond the basics of dimension theory³ and Gauss elimination method, the relationship between matrices and endomorphisms, and the elementary properties of the determinant. Strictly speaking we therefore do not assume any peculiar knowledge about 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 is just asking to accept (or verify) that nothing changes on an arbitrary field. It could happen that in some particular subsection we use group notions but these items can always be skipped in a first reading.

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

1.2.2 Conventions

We will use at length the notation \mathbf{k} for a (commutative) field and V for a \mathbf{k} -vector space which is finite dimensional unless otherwise explicitly assumed.

³Strictly speaking, it is easy following our way to recover all the results just using Gauss elimination and formal properties of determinant

⁴We will say explicitly in this case *non commutative ring*.



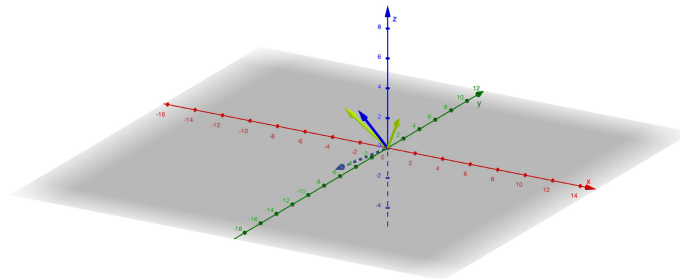
Unless expressly stated otherwise⁴, the rings are assumed to be *commutative* and with an identity, generally denoted \mathbb{R} . Their multiplicative group of units is denoted \mathbb{R}^\times .

This grants them the following property: Every nonzero ring admits a proper maximal ideal for inclusion (Krull's theorem (1.3.2.4), a result we could have considered as an axiom (in this generality, this is equivalent to the axiom of choice). For the convenience of the reader, we have explained how Zorn's lemma allows to prove Krull's theorem (1.3.2). Zorn's lemma also allows to demonstrate, essentially formally, that, just as \mathbb{Q} is contained in \mathbb{C} , any field \mathbf{k} is contained in an algebraically closed field Ω . We will use this result freely in some (rare) places (see for instance [13], theorem 4.7. or exercises TBD).

As usual, we'll denote where $E_{i,j} \in M_{p,q}(\mathbb{R})$ the matrix with all coefficients zero except the one at row i and column j , which is 1. We refer it as the "standard basis" of $M_{p,q}(\mathbb{R})$, recalling that tautologically any 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 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 a_i and called the diagonal coefficients.

We will identify \mathbb{R}^n as the set of columns $M_{n,1}(\mathbb{R})$ if $n \geq 1$.



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

We will often use the following square matrices.

Definition 1.2.2.1. A square matrix is a

- *transvection* 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 permutation⁵ $\sigma \in S_n$;
- *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 R are obtained by multiplication on the right or left by transvections or permutation matrices, these matrices being invertible (of determinant ± 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 in polynomial rings with values in rings. The cost to pay is that we have to assume that the leading coefficient is invertible, or, which remains to the same, equal to 1. Let us give a precise statement.

Proposition 1.3.1.1. *[Left Euclidean Division] Let \mathcal{R} be a non necessary 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 $A = BQ + R$ $\deg(R) < \deg P$. Of course, there exists 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) satisfies the required 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. Because $\deg(R_2 - R_1) \leq \max(\deg(R_2), \deg(R_1)) < \deg(B)$ we get $\deg(Q_1 - Q_2) < 0$ from which follows $Q_1 = Q_2$ and therefore $R_1 = R_2$.

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

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 exist two polynomials Q and R such that $(A - BM) = BQ + R$ and $\deg(R) < \deg(B)$ thus $A = BQ + M + R$. \square

1.3.2 Zorn's Lemma and application

Let E be a (partially) ordered set. We can think, for example, of the set of subsets of a given set ordered by inclusion. But there are many other examples.

⁵where $\delta_{i,j}$ is the Kronecker symbol equal to 1 if $i = j$ and 0 if not.

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 instance $J = \{0\}$ because our rings are nonzero). Because J is proper, E is non-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

Part I

Linear Algebra over Rings

Chapter 2

Warm-up I: review on basic linear algebra



2.1 Introduction



Perspective

The purpose of this introductory chapter is to prove the main theorems of Euclidean and general linear geometry in the real plane E . Our motivation is twice. First to refresh general linear algebra knowledge in this elementary context. Second, more fundamentally, to emphasize that almost all problems of linear algebras appear in dimension ≤ 2 . We'll see in many occasions that the general case follows from this small dimension study. In fact this simple observation is quite deep as the reader will see in the next coming years, for instance if he has to look at the theory of Lie or algebraic groups where the role of the 2 by 2 matrices of SL_2 is crucial.

2.2 Euclidean plane

We start with a "physical" perspective, namely we assume that our real plane E ($n = \dim(E) = 2$) has a metric, meaning a scalar product

$$\begin{cases} E \times E & \rightarrow & \mathbf{R} \\ (v, w) & \mapsto & \langle v, w \rangle \end{cases}$$

Recall that this means that this map is linear in each variable and positive definite (or > 0 for short): $q(v) = \langle v, v \rangle > 0$ unless $v = 0$.

Definition 2.2.0.1. *A Euclidean space is a real finite-dimensional vector space equipped with a scalar product. An isometry of Euclidean spaces is a linear isomorphism preserving the scalar products. An isometric endomorphism of positive determinant is called a rotation.*

Of course the typical examples are $E = \mathbf{C}$ with

$$\langle z, z' \rangle = \operatorname{Re}(\bar{z}z')$$

or \mathbf{R}^2 endowed with the standard scalar product

$$\langle (v_1, v_2), (w_1, w_2) \rangle = v_1w_1 + v_2w_2,$$

both being canonically isomorphic.

The set of isometries (resp. rotations) is a subgroup $O_2(E)$ of $GL_2(E)$ (resp. $SO_2(E)$ of $SL_2(E)$)¹.

2.2.1 Euclidean Norm

Proposition 2.2.1.1 (Cauchy-Schwartz). *Let $v, w \in E$ and let us write $\|v\| = \sqrt{\langle v, v \rangle}$.*

1. *One has $\langle v, w \rangle \leq \|v\|\|w\|$ with equality if and only if v, w are positively colinear.*
2. *One has $|\langle v, w \rangle| \leq \|v\|\|w\|$ with equality if and only if v, w are colinear.*

Proof. We may assume v and w are non-zero. The Cauchy-Schwartz inequality (1) is nothing but the inequality

$$2 - 2\langle v/\|v\|, w/\|w\| \rangle = q(v/\|v\| - w/\|w\|) \geq 0$$

with equality if and only if $v/\|v\| - w/\|w\| = 0$, namely if v, w are positively colinear. We get (2) from (1) changing w in $-w$. □

¹As usual, we'll simply write $O_2(\mathbf{R})$ (resp. $SO_2(\mathbf{R})$) for $O_2(E)$ (resp. for $SO_2(E)$) when E is the standard Euclidean plane \mathbf{R}^2

Theorem 2.2.1.2. *The mapping $v \mapsto \|v\|$ is a norm called the Euclidean norm.*

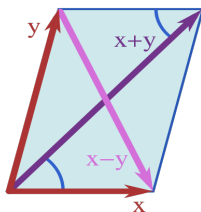
Proof. We define, for $v \in E$, $\|v\| = \langle v, v \rangle$. As q is positive definite, to show that $\|\cdot\|$ is a norm, it suffices to verify the triangle inequality

$$\begin{aligned} (\|v\| + \|w\|)^2 - \|v + w\|^2 &= \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 - \|v\|^2 - 2\langle v, w \rangle - \|w\|^2 \\ &= 2\|v\|\|w\| - 2\langle v, w \rangle \\ \text{(by Cauchy-Schwartz)} &\geq 0 \end{aligned}$$

□

Observe that equality in the triangle inequality is equivalent of equality in Cauchy-Schwartz and therefore to the fact that our vectors are (positively) linked.

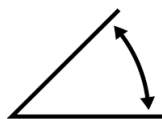
One immediately checks the important property of the Euclidean norm: the median equality



$$\text{For any } x, y \in E, \|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2).$$

2.2.2 Non oriented angle of pair of vectors or lines

By Cauchy-Schwartz inequality, the absolute value of the scalar product of two unit vectors is ≤ 1 therefore can define the angle $\widehat{(v, w)}$ between two nonzero vectors v, w by the formula



$$\widehat{(v, w)} = \arccos \left\langle \frac{v}{\|v\|}, \frac{w}{\|w\|} \right\rangle$$

thought as an element of $\mathbf{R}/2\pi\mathbf{Z}$ defined **up to sign**.

Thanks to trigonometry formulae, we obtain the usual formula from elementary geometry (the Chasles formula)

$$\widehat{(v_1, v_2)} + \widehat{(v_2, v_3)} = \widehat{(v_1, v_3)}.$$

Of course, the parity of the arccos function and the homogeneity of the scalar product ensures that the non oriented angle of two non zero vector neither depends on their order or on any nonzero multiple of them. This allows to define the (non oriented) angle of two lines ℓ_1, ℓ_2 by the non oriented angle of any vector basis of them, no matter the order of the lines.

Remark(s) 2.2.2.1. Rather than "angle" we should have said "measure of the angle" in an Euclidean plane (see 2.2.5.6).

2.2.3 Orthogonality in oriented Euclidean planes

If ℓ is a line (dimension $d = 1$), its orthogonal ℓ^\perp has equation $\langle \cdot, v \rangle = 0$ for any chosen basis v of ℓ and therefore has dimension $\dim(\ell^\perp) = n - d = 1$ (see ?? for the general case).

Remark(s) 2.2.3.1. Let us recall that two bases of some finite dimensional vector space define the same orientation if the determinant of the base change matrix is > 0 . An orientation is then defined by a basis defined up to the action of the group of matrix of positive determinant $\text{GL}_+(\mathbf{R})$. These bases are said positively oriented or direct.

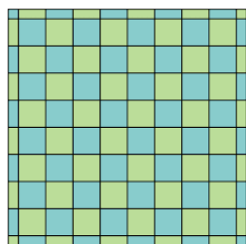
For instance, if we change the order of a basis of the plane, we change the orientation of the plane. Therefore, given a normed vector v of an oriented Euclidean plane, there exists a unique positive orthonormal basis of the plane (v, w) .

Notice that $\text{GL}_+(\mathbf{R})$ is connected (??). It follows that orientation is the only way to assign a continuous sign to any basis of E .

Because a line has obviously only two opposite normed vectors, we get just like in high school

Proposition 2.2.3.2. Let E be an oriented Euclidean plane. For any normed vector $v \in E$, there exists a unique normed vector v^\perp such that (v, v^\perp) is a positively oriented orthonormal basis.

In the standard Euclidean plane \mathbf{R}^2 with the usual orientation defined by the canonical basis, we have explicitly for $v = (a, b)$, $a^2 + b^2 = 1$ the usual formula $v^\perp = (-b, a)$.



We indeed have defined an algorithm, which will be heavily generalized: if we start with an arbitrary basis (v_1, v_2) of E , there exists a unique orthonormal basis $(e_1 = v_1/\|v_1\|, e_2 = e_1^\perp)$ such that $e_1 \in \mathbf{R}v_1$ and $(e_2, v_2) > 0$: this is the Gram-Schmidt process in the plane (see ?? in general).

The following statement is well-known and useful.

Proposition 2.2.3.3. 1. A morphism of Euclidean spaces (of any dimension) is an isometry (resp. a rotation) if and only if it maps an orthonormal (resp. direct orthonormal) basis to an orthonormal (resp. direct orthonormal) basis.

2. An endomorphism f of an Euclidean space (of any dimension) is an isometry if and only if its matrix M with respect to (any) orthonormal basis satisfies ${}^tMM = \text{Id}$

3. The determinant of an isometry is ± 1 . The determinant of a rotation is $+1$.

Proof. We assume the existence of orthonormal basis for granted in general (see ??). (1) is a direct consequence of the bilinearity of the scalar product.

(2) If (e_i) is our orthonormal basis, one has f isometry if and only if

$$(\text{Id})_{i,j} = \delta_{i,j} = \langle f(e_i), f(e_j) \rangle = \langle \sum_a m_{a,i} e_a, \sum_b m_{b,j} e_b \rangle = \sum_a m_{a,i} m_{a,j} = ({}^tMM)_{i,j}$$

proving (2).

(3) Follows from (2) and the multiplicativity of the determinant. □

We get the well-known formula

$$\text{SO}_n(\mathbf{R}) = \{M \mid {}^tMM = \text{Id} \text{ and } \det(M) = 1\}$$

Because the base change morphism between two orthonormal bases is an isometry, we get

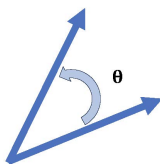
Corollary 2.2.3.4. Two Euclidean planes are (non canonically) isomorphic.

2.2.4 Oriented angles of vectors

Let E be an oriented Euclidean plane. Using the above results, we can define the oriented angle of two non zero vectors v, w as follows. If v, w are normed, one has a unique writing $w = av + bv^\perp$ with $a^2 + b^2 = 1$. Therefore, there exists a unique $\widehat{(v, w)} \in \mathbf{R}/2\pi\mathbf{Z}$ such that

$$(a, b) = (\cos(\widehat{(v, w)}), \sin(\widehat{(v, w)}))$$

Because $\langle w, v \rangle = a$, one has $\widehat{(w, v)} = |\widehat{(v, w)}|$.



In the general case, one defines $(\frac{v}{\|v\|}, \frac{w}{\|w\|}) \in \mathbf{R}/2\pi\mathbf{Z}$.

Remark(s) 2.2.4.1. By construction, if θ is the oriented angle between two normed vectors v, w , the base change matrix from (v, v^\perp) to (w, w^\perp) is $R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. The addition formulas for the trigonometric functions \sin, \cos give the important formula

$$R_\theta \circ R_{\theta'} = R_{\theta+\theta'}$$

Of course, we again obtain the usual formula of elementary geometry like the Chasles formula

$$\widehat{(v_1, v_2)} + \widehat{(v_2, v_3)} = \widehat{(v_1, v_3)}.$$

2.2.5 Isometries

Let E be an oriented Euclidean plane.

Proposition 2.2.5.1. Let v, w be two normed vectors and $\theta = \widehat{(v, w)}$.

1. There exists a unique rotation ρ_θ mapping v to w whose matrix in any direct orthonormal basis is R_θ .
2. One has

$$\cos(\widehat{(v, w)}) = \langle w, \rho(w) \rangle = \cos(\theta) = \frac{\text{tr}(\rho_{v, w})}{2}.$$

Proof. (1) The base change morphism from (v, v^\perp) to (w, w^\perp) is definitely a positive isometry, that is a rotation ρ giving the existence. Conversely any isometry mapping v to w maps v^\perp to $\pm v^\perp$ and therefore to w^\perp if it is positive giving the uniqueness. The matrix of ρ_θ in (v, v^\perp) is R_θ (cf. (2.2.4.1)). If $\mathcal{B} = (v_1, v_2)$ is another direct orthonormal basis, the base change matrix from (v, v^\perp) to \mathcal{B} is R_α (2.2.4.1). Therefore

$$\text{Mat}(\mathcal{B}, \rho) = R_\alpha^{-1} \circ R_\theta \circ R_\alpha = R(-\alpha + \theta + \alpha) = R_\theta$$

proving (1).

Let us chose any orientation on E . By (2.2.3.2), one can assume $v = e_1$ is the first vector of an orthonormal basis (e_1, e_2) . Because w is a unit vector, it can be written as $w = \cos(\theta)e_1 + \sin(\theta)e_2$ for a uniquely defined $\theta \in \mathbf{R}/2\pi\mathbf{Z}$. But $w, w' = -\sin(\theta)e_1 + \cos(\theta)e_2$ is the unique direct orthonormal basis with first vector w . Therefore the endomorphism ρ mapping (e_1, e_2) to (w, w') is the unique relevant positive isometry.

(2) follows directly from the proof of (1).

□

To specify the structure of isometries, let us choose a direct orthonormal basis \mathcal{B} of E . We will identify any endomorphism f with its matrix in \mathcal{B} .

Corollary 2.2.5.2. 1. The map $\theta \mapsto \rho_\theta$ defines an isomorphism

$$\mathbf{R}/2\pi\mathbf{Z} \simeq \text{SO}(E)$$

2. ρ_θ is complex diagonalizable with complex eigenvalues are $\exp(\pm i\theta)$.
3. ρ_θ is real diagonalizable if and only if $\theta \equiv 0 \pmod{2\pi}$ or $\theta \equiv \pi \pmod{2\pi}$ that is to say it is equal $\rho_\theta = \pm \text{Id}$.
4. The matrices negatives isometries are orthogonal symmetries.

Proof. Only the last point has not be proven yet. Let $\mathcal{B} = (e_1, e_2)$ be a direct orthonormal basis and $S_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the matrix of the orthogonal symmetry along the (second) diagonal $\mathbf{R}(e_1 + e_2)$. Then, for any negative isometry, the product of S_0 by its matrix S is some rotation $S_0S = R_\theta$. We get

$$R = S_0R_\theta = \begin{pmatrix} \sin(\theta) & \cos(\theta) \\ \cos(\theta) & -\sin(\theta) \end{pmatrix}$$

whose square is Id by direct calculation. □

From this, one recover any elementary facts about plane isometries known for the highschool time (see ?? in the general case).

Remark(s) 2.2.5.3. If one prefers the identification $E \sim \mathbf{C}$ with its orthogonal basis $(1, i)$, the corresponding statement is that rotations are as usual of the form $\theta \mapsto \exp(i\theta)z$ and symmetries of the form $\theta \mapsto \exp(i\theta)\bar{z}$.

Exercise 2.2.5.4. Show that the application which associates to an orthogonal symmetry its invariant vector line is a bijection from the set of symmetries onto the set of vector lines. Show that the compound of two symmetries associated with two lines making a (non-oriented) angle θ is a rotation whose (non-oriented) angle is 2θ .

Exercise 2.2.5.5. Determine the real and complex eigenvalues and the corresponding eigenspaces of any planar isometry. When are they diagonalizable over \mathbf{R} ? Over \mathbf{C} ?

Remark(s) 2.2.5.6. We could have defined an oriented angle in a non oriented plane as the former rotation itself. The value of the angle would then have been in $\text{SO}_2(\mathbf{R})$. The link between the our definition is that the choice of an orientation define a canonical isomorphism $\text{SO}_2(\mathbf{E}) \simeq \mathbf{R}/2\pi\mathbf{Z}$, recovering our notion of angle which could be in this context be defined as the measure of the angle. But the usual modern point of view is to see an angle as we did, and therefore we have to choose an orientation of the plane.

2.2.6 Symmetric real matrices

We know (2.2.5.1) that the matrices of a negative isometries in an orthonormal basis are of the form $\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$, in particular are symmetric. Like all symetries, they are diagonalizable with spectrum $\{\pm 1\}$. But, we have more. The eigenspaces are orthogonal. Indeed, if we identify \mathbf{E} with \mathbf{C} thanks to \mathcal{B} , our symmetry is nothing but $z \mapsto \exp(\mathbf{i}\theta)\bar{z}$ whose (real) $+1$ -eigenspace is the line $\mathbf{R}\exp(\mathbf{i}\theta/2)$ and (real) -1 -eigenspace is the orthogonal line $\mathbf{iR}\exp(\mathbf{i}\theta/2)$. We recover the well known fact that orthogonal symmetries are orthogonally diagonalizable. This fact is general.

Proposition 2.2.6.1. Symmetric matrices of $\text{M}_2(\mathbf{R})$ are exactly orthogonally diagonalizable matrices (with respect to the standard Euclidean structure of \mathbf{R}^2).

Proof. We identify \mathbf{E} with the standard Euclidean plan \mathbf{R}^2 with its standard orthogonal basis \mathcal{B} . If $X, Y \in \mathbf{R}^2$ and $M \in \text{M}_2(\mathbf{R})$, we have $\langle X, Y \rangle = {}^tXY$ and therefore

$$\langle MX, Y \rangle = {}^t(MX)Y = {}^tX{}^tMY = \langle X, {}^tMY \rangle.$$

The characteristic polynomial of $M = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$ is $\chi_M(T) = T^2 - (a+d)T + (ad - b^2)$ with discriminant $\Delta = (a+d)^2 - 4(ad - b^2) = (a-d)^2 + 4b^2 \geq 0$. Therefore, it is split over \mathbf{R} with distinct roots unless $b = 0$ and $a = d$, i.e. $M = a\text{Id}$.

If $\Delta = 0$, then M is scalar and the canonical orthonormal basis of \mathbf{R}^2 and therefore orthogonally *diagonal*. Assume $\Delta > 0$ and let $x, y \in \mathbf{R}$ the distinct roots of χ_M . If X, Y are normed eigenvector of our real symmetric matrix M relatively x, y , one gets

$$x\langle X, Y \rangle = \langle MX, Y \rangle = \langle X, MY \rangle = y\langle X, Y \rangle$$

hence $\langle X, Y \rangle = 0$. Therefore, after the orthonormal base change $\mathcal{B} \rightarrow (X, Y)$, the matrix becomes $\text{diag}(x, y)$. \square



In this section E denotes a rank real plane without any Euclidean structure. We will explain the reduction theory in this simple but non trivial case due to the fact that the scalar field \mathbf{R} is not algebraically closed (compare with the general results of 9.2.2.2 and 9.4).

2.3 General linear maps of the plane

Let $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbf{R})$.

2.3.1 Minimal polynomial

A direct computation shows that $\chi_M(T) = T^2 - (a + d)T + (ad - bc)$ annihilates M : this is the Cayley-Hamilton theorem in dimension 2. Because $\mathbf{R}[T]$ is a principal ideal domain, the ideal of real polynomials annihilating M is generated by a unique monic polynomial μ_M . Because $\chi_M(M) = 0$, one has $\mu_M | \chi_M$ and therefore

- either $\mu_M = \chi_M$
- either χ_M is of degree 1 and M is the scalar matrix $\frac{\text{tr}(M)}{2} \text{Id}$.

Definition 2.3.1.1. *If M is non scalar, we define the similarity invariants P_2, P_1 of M by $P_1 = \chi_M = \mu_M$ and $P_2 = 1$. If M is scalar, we define $P_1 = P_2 = \mu_M$.*

2.3.2 Cyclic vectors

Assume that M is not a scalar matrix. Then M has at most two eigenlines (because $\deg(\chi_M) = 2$). Let $X \in \mathbf{R}^2$ not belonging to these lines (a real plane is never the union of two lines!). Then X and MX are certainly independent vectors, and is therefore a basis of the plane. Writing M in this basis, remembering the equation $\chi_M(M).X = 0$, we get that M is similar to $C(\chi) = \begin{pmatrix} 0 & -\det(M) \\ 1 & \text{tr}(M) \end{pmatrix}$. Because a matrix is scalar if and only if $\deg(\mu_M) = 1$, we therefore get the plane version of the Frobenius theorem 9.4.

Theorem 2.3.2.1 (Jordan-Frobenius in the plane). *Let M be real matrix.*

1. *One has $P_2 | P_1$ and $P_2 P_1 = \chi_M$.*
2. *Two matrices are similar if and only if they have the same similarity invariants.*
3. *If M is not scalar, it is similar to the "companion" matrix $C(\chi)$ of $P_1 = \chi_M = \mu_M$.*

4. M is nilpotent if and only if it is similar to the standard matrix $J = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

In a certain extent, the rest of the book is dedicated to generalize these results in any dimension.

2.4 Exercices

Exercise 2.4.0.1. 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 2.2.1.1 and theorem 1.39 of [18]. [Hint : assume first $\sum z_i \in \mathbf{R}^+$].

Chapter 3

Warm-up II: duality



René Magritte

3.1 Introduction



Perspective

Sub-vector spaces 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.

3.2 Basic notions

As always, V denotes in this chapter a finite dimensional¹ \mathbf{k} -vector space and $V^* = \text{Hom}(V, \mathbf{k})$ denotes its dual; the vector space of linear applications from V to \mathbf{k} , *i.e.* linear forms of V .

If $\varphi \in V^*, v \in V$, we note $\langle \varphi, v \rangle = \varphi(v)$ the duality bracket² $V^* \times V \rightarrow \mathbf{k}$.

¹Unless otherwise stated.

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

A hyperplane is the kernel of a non-zero linear form φ . Conversely, any hyperplane H determines φ 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 φ 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 (i).

Proposition 3.2.0.1. *Let V be a n -dimensional vector space and let V_i finitely many proper sub-vector spaces. If \mathbf{k} is infinite or if the number of subspaces is ≤ 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 φ_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 φ_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

We recall that if $\mathcal{B} = (e_i)$ is a (finite) basis of V , we define the dual basis $\mathcal{B}^* = (e_i^*)$ of V^* by the formula $\langle e_i, e_j^* \rangle = \delta_{i,j}$. In other words, e_i^* is the i -th coordinate function and we have $v = \sum_j \langle v, e_j^* \rangle e_j$. 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 $L \in V^*$ is a row and $C \in V$ a column. If $\mathcal{B} = (e_i = [\delta_{i,j}]_{1 \leq j \leq n})$ is the canonical basis ($E_{i,1} = e_i$) of $k^n = M_{n,1}(\mathbf{k}) = V$, 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 \mathcal{B} is a basis of an infinite dimensional vector space, the family \mathcal{B}^* is still free but is never a basis. For instance, the linear form φ defined by $\langle \varphi, e_i \rangle$ for all i is certainly not in the span of \mathcal{B}^* . Even as a set, $\text{Card}(V^*) > \text{Card}(V)$ (**exercice**). 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 a the appropriate topological dual of topological vector spaces.



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

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

If now W_* is a subspace of V^* (or even a subset) its polar in V is defined by

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

Example(s) 3.2.0.2. *An important example comes from differential geometry. If f is a regular function on an open Ω 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 $T_x\Omega$, this form is the Jacobian $J(\omega) = (\frac{df}{dx_j}(\omega))_j$ thus seen as a row matrix. The kernel of $df(\omega)$ is none other than the tangent hyperplane at ω to the hypersurface defined by the equation $f = 0$ as long as the differential is non-null at that point. The generalization to several functions is contained in the notion of higher-dimensional submanifolds.*

3.3 Motivation

Two useful ways compete to define a vector subspace W of $V = k^n$.

1. Via generators $v_i \in V$: $W = \text{Vect}\{v_i\}$.
2. Via equations $eq_i \in V^*$: $W = \{v | \langle eq_i, v \rangle = 0\}$ with

$$\langle eq_i, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rangle = \sum_j a_{i,j}x_j = (a_{i,1}, \dots, a_{i,n}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

The duality first focus on the second point of view, thus on the dual V^* and the set of all possible equations of W : the orthogonal $W^\perp = \{\varphi \in V^* | \varphi(W) \equiv 0\}$ and then to the link with the first point of view.

3.4 Formal Biorthogonality

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

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

In general, this inclusion is formal in the sense that it is always an equality, without any further assumption about the dimensionality of V .

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

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.

3.5 Ante-dual Basis: Biduality

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

Proposition 3.5.0.1. *Let V be of dimension $n < \infty$. Then*

1. *The evaluation linear application*

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

is an 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. For (1), note that ev is injective between spaces of the same finite dimension.

For (2), note that $\mathcal{B} = ev^{-1}((\mathcal{B}_*)^*)$ is the unique solution to the problem posed. \square

3.6 Orthogonal and Polar in Finite Dimension

Proposition 3.6.0.1. *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. For (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 $W^\perp = \text{Vect}(e_i, i > d)$.

For (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 $W_*^\circ = \text{Vect}(\varphi_i, i > d)$.

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) is added for reference and does not use finite dimension (i).

For (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.

For (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. \square

Example(s) 3.6.0.2. If V is an euclidean space with scalar product $(v, w) \mapsto v.w$, the partial linear map $w \mapsto (v \mapsto v.w)$ has zero kernel and is therefore an isomorphism $V \mapsto V^*$. One checks that this isomorphism identifies W^\perp with the usual Euclidean orthogonal $\{v \in V | v.W = \{0\}\}$ 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 $w.w = 0$ and therefore is zero ensuring in the Euclidean space the so called usual orthogonal decomposition $W \oplus W^\perp = V$.

Remark(s) 3.6.0.3. Note that orthogonality and polarity are strictly decreasing applications for inclusion.

Corollary 3.6.0.4. Let $\varphi_i \in V^*$, $i = 1, \dots, m$. Then, the rank of $\text{Vect}\{\varphi_i\}$ is that of the evaluation application $\left\{ \begin{array}{l} V \rightarrow k^m \\ v \mapsto (\varphi_i(v))_i \end{array} \right.$

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. \square

Exercise 3.6.0.5. Let V be the real vector space of polynomial of degree ≤ 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.

3.7 Biduality Conventions (Finite Dimension)

The previous paragraph allows, in finite dimension therefore, thanks to ev to identify V and its bidual, polar W_*° of W_* and orthogonal W_*^\perp , W and biorthogonal $W^{\perp\perp}$. We generally simply note W_*^\perp for W_*° .

Generally, in finite dimension, we consider spaces and dual, but we do not dualize the dual thanks to ev and we simply write $W = W^{\perp\perp}$ whether W is a subspace of V or of V^* .

As an illustration, let's give the algebraic lemma, easy but important, 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 3.2.0.2).

Exercise 3.7.0.1. Compare the orthogonal of a sum or intersection of sub vector spaces with the sum or intersection of their orthogonals.

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

Lemma 3.7.0.2. Let φ and $\varphi_i, i \in I$ be linear forms of V . Then, φ is a linear combination of the φ_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

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

□

Exercise 3.7.0.3. Les $\varphi_i, i = 1, \dots, N$ linear forms on V and $\Psi \in \text{Hom}(V, \mathbf{k}^N) = (\varphi_i)$. Prove that the rank of Ψ is the dimension of the span of the φ_i 's.

Remark(s) 3.7.0.4 (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 φ is a linear combination with positive coefficients of the φ_i . See [1].

3.8 Contravariance

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

Definition 3.8.0.1. 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 3.8.0.2. *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 (3.7), 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's just give an argument for 5)(the verification of the rest is left as an **exercise**). First, it suffices to show one of the two formulas (change f to ${}^t f$ and use the involution of the transposition and of the orthogonal). Then, $\text{Im}({}^t f)$ and $\text{Ker}(f)^\perp$ having the same dimension according to 1) and 3.6.0.1, it suffices to prove $\text{Im}({}^t f) \subset \text{Ker}(f)^\perp$. Now, if $f(v_1) = 0$, then $\langle {}^t f(\varphi_2), v_1 \rangle = \langle \varphi_2, f(v_1) \rangle = 0$.

□

3.9 Exercises

Exercise 3.9.0.1. *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?*

Chapter 4

Matrices with Ring coefficients



4.1 Introduction



Perspective

We explain how determinant identities and 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.

4.1.1 Algebraic identities extension principle

Proposition 4.1.1.1. *Let $P \in \mathbf{Z}[T_1, \dots, T_n]$ and $I_i, 1 = 1, \dots, n$ be infinite sets of some field of characteristic zero k . Then, 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 instance, 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 $M_{n,m}(\mathbf{C})$, then for all ring R and $M \in M_{n,m}(R)$, one has $P(M) = 0$.*

Proof. We observe $\mathbf{Z}[T_1, \dots, T_n] \subset k[T_1, \dots, T_n]$ (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. □

Corollary 4.1.1.2. *All integral formulas for the determinant valid for complex square matrices remain valid for square matrices in any commutative ring 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 $A \in M_n(R)$ and its corollary: the multiplicative group $\text{GL}_n(R)$ of matrices having an inverse is equal to $\{A \in M_n(R) \mid \det(A) \in R^\times\}$.*

Remark(s) 4.1.1.3. *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.*

4.1.2 Cayley-Hamilton in $M_n(R)$

Let us start with an easy lemma, which is usually more or less considered as "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 $\mathcal{R}[T] \rightarrow \mathcal{R}$ 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 cautious with its multiplicity.

Lemma 4.1.2.1. *Let $P = \sum_i \pi_i T^i, \bar{P} = \sum \bar{\pi}_i T^i \in \mathcal{R}[T]$ and assume that t commute 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 4.1.2.2 (Cayley-Hamilton). *Let $A \in M_n(R)$ and $\chi_A(T) = \det(T \text{Id} - A)$. Then, $\chi_A(A) = 0$.*

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

Because A commutes with the two coefficients Id, A of $T \text{Id} - A$, lemma 4.1.2.1 shows that the evaluation of $(*)$ at $\tau = A$ is the product 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 $\chi_A(A)$ of the right hand side. \square

4.2 Maximal rank matrices

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

Proposition 4.2.0.1. *Let n, m be positive integers and $A \in M_{m,n}(\mathbb{R}), B \in M_{n,m}(\mathbb{R})$*

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

Proof. (1). As before, we consider the generic matrices $A = (X_{i,j}), B = (Y_{j,i})$ with $X_{i,j}, Y_{i,j}, 1 \leq i \leq m, 1 \leq j \leq n$ are indeterminates and we look in the the general matrix identity $\det(AB) = 0$ which is a polynomial identity of $n^2 m^2$ 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 $B_c : \mathbb{C}^m \rightarrow \mathbb{C}^n$ is not (for dimension reasons).

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

(3). Assume by contradiction $n > m$ and let $B = \begin{pmatrix} \text{Id}_m \\ 0_{n-m} \end{pmatrix}$ defining the canonical injection $\mathbb{R}^m \hookrightarrow \mathbb{R}^n$. Let $C = BA \in M_n(\mathbb{R})$ and $L = (0, \dots, 0, 1) = E_{1,n} \in M_{1,n}(\mathbb{R})$. Because $n > m$, one has $LB = 0$. By Cayley-Hamilton, there exists a monic polynomial $T^d + \sum_{i < d} a_i T^i$ annihilating C . One can assume that d is minimal among these polynomials. Because C is injective as B and A , one has $a_0 \neq 0$ by minimality. Left composing the equation $C^d + \sum_{i < d} a_i C^i = 0$ by L , we get $a_0 L = 0$ and therefor $a_0 = 0$, a contradiction.

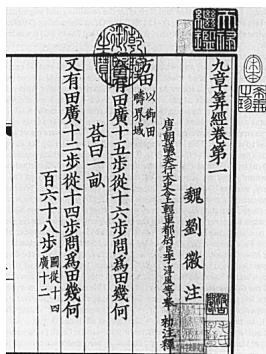
(4). Each (2) or (3) implies (4) (apply to both A and A^{-1} , the latter being defined as usual because A is bijective). \square

Remark(s) 4.2.0.2. • One will give below more natural proofs in some way, but less elementary. Precisely, see 6.6.0.5 for (2) and (4) with an argument using the choice axiom see and 7.3.0.5 for (2), (3) and (4) with an argument not using the choce axiom-. The idea in this last case is to reduce to this statement by reducing to the case of 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.

4.3 Reminder on Gauss elimination method

Let us give a version of Gauss elimination not using dilatations nor permutation matrices as far as possible.



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 4.3.0.1. Let R be a ring and $p, q \geq 1$ two integers. We denote by $E_n(R)$ the subgroup of $GL_n(R)$ genrated 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 the exists $P \in E_p(R), Q \in E_q(R)$ with $B = P^{-1}AQ$;
- equivalent ($A \sim B$) if the exists matrices $P \in GL_p(R), Q \in GL_q(R)$ with $B = P^{-1}AQ$.

Gauss-equivalent \Rightarrow equivalent. Notice also that Gauss equivalence does not use permutation matrices.

4.3.1 The usual field case

Proposition 4.3.1.1. *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).

□

Exercise 4.3.1.2. *Give a computer program of 4.3.1.1 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 ?*

4.3.2 A few universal formulas

Although the reader can skip this (elementary) section, the following examples will be quite useful (compare with 9.4.0.1 below). This also illustrate how permutation matrices can play a(or do not play) a role in Gauss elimination method, no matter the coefficients ring is a field. Recall that R is any (commutative) ring.

Lemma 4.3.2.1.

1. *Let D be an invertible diagonal matrix of $M_n(R)$. Then, $D \equiv \text{diag}(\det(D), 1, \dots, 1)$.*

2. Let any permutation matrix M_σ , $\sigma \in S_n$ is Gauss equivalent 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 computations¹)

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

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

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

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 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

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

¹We indicate the pivot and the bold coefficient is the pivot

and using line operations

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

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

4.4 Application to subgroups of $GL_n(\mathbf{k})$

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 4.4.0.1. *One has*

1. $D(GL_n(V)) = SL_n(V)$ *except if* $n = 2$ *and* $\text{Card}(\mathbf{k}) = 2$.
2. $D(SL_n(V)) = SL_n(V)$ *except if* $n = 2$ *and* $\text{Card}(\mathbf{k}) = 2, 8$.

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

Proof. Proof of (1). Because the derived group is normal and all transvections are conjugate in $GL(V)$, it is enough to show that in our case one transvection is a commutator. If $n \geq 3$ and any characteristic, one computes $[\text{Id} + E_{2,1}, \text{Id} + E_{1,3}] = \text{Id} + E_{2,3}$. If $n = 2$, let us choose $\lambda \neq 0, 1$. Then, $[\text{diag}(\lambda, 1), T_{1,2}(\lambda)] = T_{1,2}(\lambda - 1)$ which is a transvection.

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

²At this stage, this is just a notation. Nothing has to be known about projective geometry.

4.4.1 General transvections

If $f \in \text{Hom}_{\mathbf{k}}(V/D, D)$ we denote by $\tilde{f} \in \text{End}_{\mathbf{k}}(V)$ the linear map $\tilde{x} \mapsto x + f(x \bmod D)$.

Proposition 4.4.1.1. *Let $\tau \in \text{End}_{\mathbf{k}}(V)$. The 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 $\tau = \tilde{f}$.
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 $\text{Hom}(V/D, D) \rightarrow \text{GL}(V)$

$$6. \text{ The matrices of } \tau \text{ are similar to } \text{Id}_n + E_{1,2} = \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & 0 \\ 0 & \text{Id}_{n-2} \end{pmatrix}.$$

We say that τ is a transvection of V of type $(D(\tau), H(\tau)) \in \mathbf{P}V \times \mathbf{P}V^*$. If φ, v are as above, let us define $\tau_\lambda(x) = x + \lambda\varphi(x)v$, $\lambda \in \mathbf{k}$. Under these conditions, we have:

- $H(\tau) = \text{Ker}(\varphi), D(\tau) = \langle v \rangle$,
- Transvections of type $(\langle v \rangle, \langle \varphi \rangle)$ are given by τ_λ , $\lambda \in \mathbf{k}^*$, and $\lambda \mapsto \tau_\lambda$ is an injective group morphism $(\mathbf{k}, +) \rightarrow (\text{SL}(V), \times)$,
- ${}^t\tau$ is a transvection of V^* of type $(H(\tau), D(\tau)) \in \mathbf{P}V^* \times \mathbf{P}V$.

4.4.2 Normal subgroups of $\text{GL}(V)$

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 4.4.2.1. *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.³.

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 4.4.2.2. *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 $\mathbf{P}V$ 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 4.4.2.3 (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 $g \in G$, $G = \langle gKg^{-1} \rangle$.*
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.

Lemma 4.4.2.4. *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

³Or equivalently (Exercice if the stabilizer G_x of a point $x \in X$ is a maximal subgroup of G).

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 4.4.2.5. *If $\dim(V) \geq 2$, any normal nontrivial 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. 4.4.1.1) and apply Iwasawa criterium and 4.4.0.1. \square

4.5 Exercises

Exercise 4.5.0.1. *Prove that the evaluation map of lemma 4.1.2.1 is a (skew)-ring morphism if and only if t commutes with any element of \mathcal{R} .*

Exercise 4.5.0.2. *Give an example of square matrices $\tau, A \in M_2(\mathbf{C})$ such that the evaluation at τ of ${}^t \text{Com}(T \text{Id} - A)(T \text{Id} - A) = \chi_A(T) \text{Id}$ is not equal to the products of the evaluation at τ of ${}^t \text{Com}(T \text{Id} - A)$ and of $(\tau - A)$. What is the value of $\chi_A(\tau)$ in this case ?*

Exercise 4.5.0.3. *With the notation above prove the identity*

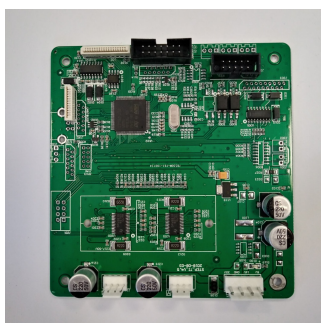
$$T^n \chi_{AB}(T) = T^m \chi_{BA}(T)$$

Hint : Consider the matrices $C = \begin{bmatrix} T \text{Id}_m & B \\ A & I_n \end{bmatrix}$, $D = \begin{bmatrix} \text{Id}_m & -B \\ 0 & T \text{Id}_n \end{bmatrix}$. Give another proof of 4.1.2.2.(2)

Exercise 4.5.0.4. *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].*

Chapter 5

Modules



5.1 Introduction



Perspective

This chapter introduces the language of modules and diagrams in as light a manner as possible. It is suggested that the reader first browse through it focusing on solving the exercises, then later familiarize himself with its use in the following chapters in a concrete manner.

Thus, it will only be consulted afterward if absolutely necessary: the idea is that all the formal constructions of vector spaces or abelian groups apply *mutatis mutandis* to this general framework by accepting scalars valued in a ring rather than in a field (or integers for abelian groups).

As will be seen here and throughout the text, the diagrammatic perspective (see 5.3) once familiar is extremely valuable, unifying, and simplifying. Paradoxically, this effort in abstraction, besides opening the doors to modern and deep mathematics, often makes them very concrete, even computable and algorithmic.

This will be particularly illustrated in the section 9.2 and the chapters 12 and 14 dedicated to the study of the linear group and the similarity classes of square matrices. Unlike the usual methods of linear algebra that largely depend 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 actually important for deciding whether two endomorphisms are similar, for example. The advantage is generally... we 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. Of course, the notion of eigenvalue remains essential as will be seen repeatedly. But it is often useless when one cannot compute the roots of the polynomial characteristic or, worse, when the characteristic polynomial is not split.

5.2 Vocabulary and first examples

5.2.1 Modules

We know that a vector space over a field \mathbf{k} is an abelian group M equipped with an external law $\mathbf{k} \times M \rightarrow M$ verifying for all $a, a' \in \mathbf{k}$ and $m, m' \in M$ (on the left say) the four usual compatibilities.

1. $a(m + m') = am + am'$
2. $(a + a')m = am + a'm$
3. $1m = m$
4. $a(a'm) = (aa')m$

The notion of a module is obtained exactly in the same way, by allowing the field \mathbf{k} to be a ring R (recall that for us R is commutative with unit):

Definition 5.2.1.1. *A module M over a unitary ring R is an abelian group equipped with a "scalar multiplication" map $R \times M \rightarrow M$ verifying the previous compatibility properties. A submodule N of M is a subgroup stable by scalar multiplication.*

Example(s) 5.2.1.2. *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. *If V is a \mathbf{k} -vector space, the set of formal polynomials¹ with coefficients in V is naturally a $k[\mathbf{T}]$ -module.*

4. In general, if M is an arbitrary R -module, we denote $\text{Ann}_M(r) = \text{Ker}(r : M \rightarrow M)$ and $M[r] = \cup_{n>0} \text{Ker}(r^n : M \rightarrow M)$, which is indeed a submodule as a union of increasing submodules (*exercice*).
5. The set $C_c(\mathbb{T}, \mathbf{R})$ of continuous functions with compact support from a topological space \mathbb{T} to \mathbf{R} is a module over the ring of continuous functions from \mathbb{T} to \mathbf{R} . If \mathbb{T} is a non-compact metric space, $C_c(\mathbb{T}, \mathbf{R})$ is an ideal but not a ring (*exercice*). This ideal is not finitely generated for example if $\mathbb{T} = \mathbf{R}^n$ (*exercice*).
6. 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. 5.5.1).
7. 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. 5.5.1).

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

¹That 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	$\sum_{finite} \lambda_i x_i$	
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 ² of N_i	$\prod N_i = \{(x_i), x_i \in N_i\}$	
Direct sum ² of N_i	$\oplus N_i = \{(x_i) \in \prod N_i \mid \text{Card}\{i \mid x_i \neq 0\} < \infty\}$	
$R^{(I)}, R^n$	$R^{(I)} = \oplus_I R, R^n = \oplus_{i=1}^n R = \prod_{i=1}^n R$	

5.2.2 Morphisms

The notion of a linear application is translated into that of module morphisms as in the following table, the notion of kernel, image and quotient³ being the same as in linear algebra.

Definition 5.2.2.1. A morphism of modules $f : M \rightarrow N$ is a linear map: for any $x, y \in M, \lambda \in R, f(x + y) = f(x) + f(y)$ and $f(\lambda x) = \lambda f(x)$.

The set $\text{Hom}_R(M, N)$ of morphisms is a group for the addition. As in linear algebra, f has an inverse $g \in \text{Hom}_R(N, M)$ if and only if f is both injective and surjective.

Specifically, we have, e_j being the "canonical basis" of R^n

²See 5.5.1.


³See 5.2.3.

Lemma 5.2.2.2. *If M, N are two R -modules, the set of morphisms $\text{Hom}_R(M, N)$ is naturally a module. If $M = R^n$, the natural application*

$$\begin{cases} \text{Hom}_R(R^n, N) & \rightarrow & N^n \\ f & \mapsto & (f(e_j)) \end{cases}$$

is an isomorphism. In particular, $\text{Hom}_R(R^n, R^m) = M_{m,n}(R)$.

Proof. As in classical linear algebra. □

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

5.2.3 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 $\text{Ker}(f)$ of f . Can we find a module whose nullity measures the surjectivity?

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 linearity of f for the law $+$. The equivalence class of $n \in N$ is

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

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 also as immediate as it is important.

Proposition 5.2.3.1. *There exists a unique R -module structure on $\text{Coker}(f)$ such that π is a morphism. It is characterized by $\overline{n} + \overline{n'} = \overline{n + n'}$ and $\lambda\overline{n} = \overline{\lambda n}$; its neutral is $\overline{0}$ simply noted 0. Moreover, f is surjective if and only if $\text{Coker}(f) = \{0\}$.*

Thus, we have solved our problem. A particular, fundamental case is when f is injective. In this case, f induces an isomorphism of M onto its image $f(M)$ which is thus a submodule N' of N .

Definition 5.2.3.2. *Let N' be a submodule of N and denote j the inclusion of N' in N . We say that $\text{Coker}(j)$ is the quotient of N by N' and we denote it N/N' .*

It is important to characterize the cokernel, up to canonical isomorphism, by its properties rather than by its construction. This is what is explained in 5.5.2.1.

Remark(s) 5.2.3.3. *In general, we are interested in modules up to isomorphism. Thus, we will identify two modules between which exists a canonical isomorphism, that is, one that depends on no choice. The reader is, for example, used in linear algebra to identify a finite-dimensional vector space with its bidual (cf. 3.5.0.1), a Euclidean space with its dual (cf. more generally ??), a square matrix of dimension 1 with its unique coefficient (its trace actually)... Similarly, 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 M . We will see other examples.*

The following result is formal but important (compare with 5.5)

Proposition 5.2.3.4. *If $f \in \text{Hom}_R(M, N)$, then f induces a canonical isomorphism $\overline{f} : M/\text{Ker}(f) \simeq \text{Im}(f)$.*

Proof. We define

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

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

Exercise 5.2.3.5. *Quotient et supplémentaire d'un ev. TBD.*

5.2.4 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

$$P(T).v = P(a)(v) \forall P \in R = k[T], v \in V_a = V$$

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

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

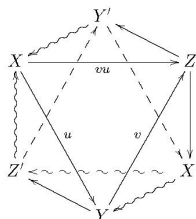
i.e.

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

Corollary 5.2.4.1. *If $f \in \text{Isom}_{k[t]}(V_a, W_b)$ 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.*

Recall that $a, b \in \text{End}_k(V)$ are similar if and only if there exists an isomorphism f of V such that $b = f^{-1} \circ a \circ f$ and we write in this case $a \approx b$. This defines an equivalence relation \approx on $\text{End}_k(V)$. In particular, when $a = b$, the k -algebra $\text{End}_{k[T]}(V_a)$ is the set of endomorphisms of V commuting with a .

5.3 Exact sequences and diagrams



5.3.1 Exact sequences

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

$$\text{Ker}(f) \xrightarrow{\iota} M \xrightarrow{f} N \xrightarrow{\pi} \text{Coker}(f).$$

We notice that the composed of two successive 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 5.3.1.1. Let $d_i \in \text{Hom}(M_i, M_{i+1})$ morphisms, noted as a «sequence»:

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

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

Exercise 5.3.1.2. Let $f \in \text{Hom}(M, N)$.

- Show that $0 \rightarrow M \xrightarrow{f} N$ is exact if and only if f is injective. What is the analogue for surjectivity?
- Show that the sequence $0 \rightarrow \text{K} \rightarrow M \xrightarrow{f} N$ is exact if and only if K can be identified (canonically) with the kernel of f . Compare with 5.4.0.2 infra.
- Show that the product or direct sum of exact sequences is still exact.

5.3.2 A key exact sequence

Let $a \in \text{End}_{\mathbf{k}}(V)$ and V_a be the associated $\mathbf{k}[T]$ -module (5.2.4). We define the $\mathbf{k}[T]$ -module as follows. As a \mathbf{k} -vector space, $V[T]$ is the set of formal polynomials with V coefficients

$$V[T] = \{v(T) = \sum_{\text{finite}} v_i T^i\} \xrightarrow{\sim} V^{(\mathbf{N})}.$$

The scalar multiplication is then characterized by $T \sum v_i T^i = \sum v_i T^{i+1}$. There is a unique lifting $\tilde{a} \in \text{End}_{\mathbf{k}[T]}(V[T])$ of a to $V[T]$ characterized by $\tilde{a}(vT^i) = a(v)T^i$. Let $\pi_a \in \text{Hom}(V[T] \rightarrow V_a)$ the unique lifting of Id_V (we have $\pi_a(\sum v_i T^i) = \sum a^i(v_i)$).

Lemma 5.3.2.1. *The sequence*

$$(ii) \quad 0 \rightarrow V[\mathbb{T}] \xrightarrow{\text{TId} - \tilde{a}} V[\mathbb{T}] \xrightarrow{\pi_a} V_a \rightarrow 0$$

is exact.

Proof. Let $v \in V$. The image of the constant polynomial $v \in V[\mathbb{T}]$ by π_a is v . Therefore π_a is onto.

We then have

$$\pi_a \circ (\text{TId} - \tilde{a})(v) = \text{T}\pi_a(v) - a(v) = a(v) - a(v) = 0$$

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

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

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

Thus, we have

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

But since TId and \tilde{a} commute, we have (geometric series sum)

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

and thus $v(\mathbb{T}) \in \text{Im}(\text{TId} - \tilde{a})$. Hence the exactness in the middle. The exactness on the left, being unnecessary for us, is left as an (interesting) **exercise**. □

5.3.3 Commutative diagrams

We want to see properties of morphisms in terms of diagrams. For example, to say that $f, g \in \text{Hom}_k(V, W)$ are equivalent endomorphisms in the sense of linear algebra is to say there exist endomorphisms p, q of W, V such that $p \circ f = g \circ q$ with p, q isomorphisms. The first condition $p \circ f = g \circ q$ (resp. both conditions) is then translated by saying that the diagram

$$\begin{array}{ccc} V & \xrightarrow{p} & V \\ g \downarrow & & \downarrow f \\ W & \xrightarrow{q} & W \end{array} \quad \text{resp.} \quad \begin{array}{ccccccc} 0 & \longrightarrow & V & \xrightarrow{p} & V & \longrightarrow & 0 \\ & & g \downarrow & & \downarrow f & & \\ 0 & \longrightarrow & W & \xrightarrow{q} & W & \longrightarrow & 0 \end{array}$$

is *commutative* with exact lines⁴ (this last condition being empty for the first diagram). A general formal definition (which we encourage the reader not to read!) might be

⁴By convention, the lines of a diagram are horizontal, the columns vertical.

Definition 5.3.3.1. Let $G = (S, A)$ be a directed graph with vertices S and edges A .

- A diagram⁵ is the data for each vertex $\Sigma \in S$ of a module M_Σ and for each edge $a : \Sigma_{>} \rightarrow \Sigma_{<}$ of A of a morphism $f_a : M_{\Sigma_{>}} \rightarrow M_{\Sigma_{<}}$.
- The diagram is said to be commutative if for every couple of vertices Σ, Σ' , the composed of the f_a associated with an oriented path from Σ to Σ' 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.

5.4 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. §5.5).

Proposition 5.4.0.1 (Functoriality I). Assume we have a commutative diagram of \mathbb{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 $\text{Coker}(\mu_1) = M_3$.

⁵There are more general definitions, allowing diagrams with several arrows between two edges. We don't 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 μ_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's 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»⁶

Proposition 5.4.0.2 (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 ι_3 is an isomorphism. In particular, there is canonical isomorphism $N_1 = \text{Ker}(\nu_2)$.

⁶an 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

Exercise 5.4.0.3. Consider a

commutative diagram of modules with exact lines

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

- If f_2, f_4 injective and f_1 surjective, then f_3 injective.
- If f_2, f_4 surjective and f_5 injective, then f_3 bijective.

Remark(s) 5.4.0.4. 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.

5.5 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». Thus, T is seen 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 an application (linear) $h_f(T) : h_M(T) \rightarrow h_N(T)$ (resp. $h_f^\vee : h^\vee(N) \rightarrow h_M^\vee(T)$) which is compatible with composition⁷ The correct general framework to formulate what follows is that of the Yoneda lemma in categories, but we will stay in the framework of modules for the examples that interest us to avoid unnecessary formalism.

5.5.1 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 two tautological applications

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

⁷The reader will recognize the usual notion of «restriction» of a morphism for $h_f(T)$ and dually of «transpose» for $h^\vee(f)$.

and

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

Lemma 5.5.1.1 (Universal properties of sum and product). *The applications $\underline{h}(\mathbb{T})$ and $\underline{h}^{\vee}(\mathbb{T})$ are bijective.*

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

5.5.2 Kernel and cokernel



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

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

and

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

that characterize kernel and cokernel (see also 5.3.1.2 and 5.9.0.3).

If \mathbb{T} is a test module we have two tautological applications

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

and

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

Lemma 5.5.2.1 (Universal properties of kernel and cokernel). *The applications $h(\mathbb{T})$ and $h^{\vee}(\mathbb{T})$ are bijective.*

Proof. Let's prove, for example, the universal property of the cokernel ie construct the inverse of $h^\vee(T)$. Observing that we have an exact sequence $0 \rightarrow T \xrightarrow{Id} T \rightarrow 0$. Let then $\psi \in \text{Hom}_0(N, T)$. The condition $\psi \circ f = 0$ precisely ensures the commutativity of the diagram

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

so that 5.4.0.1 ensures the existence of a unique φ making the diagram

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

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

The meaning of the lemma is that providing a morphism φ from the cokernel to T is equivalent to providing a morphism ψ from N to T such that the composition $\psi \circ f$ is zero, or ψ factors through the quotient (or passes to the quotient) in φ 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 keeping only the informal meaning of the statement:

If $\psi \circ f = 0$ then
$$\begin{array}{ccc} & & T \\ & \nearrow \psi & \uparrow \exists! \varphi \\ M & \xrightarrow{f} N & \longrightarrow \text{Coker}(f) \end{array}$$

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

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

and

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

are exact.

5.6 Cokernel of Diagonal Matrices

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

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

Let us consider a "diagonal" rectangular matrix $D \in M_{n,m}(\mathbb{R})$ «diagonal» in the sense that its coefficients $d_{i,j}$ are zero if $i \neq j$. Thus, we have a block decomposition

$$D = (\Delta, 0) \in M_{\nu,\mu}(\mathbb{R}) \text{ if } m \geq n, D = \begin{pmatrix} \Delta \\ 0 \end{pmatrix} \in M_{\mu,\nu}(\mathbb{R}) \text{ if } n \geq m$$

with $\Delta = \text{diag}(d_i) \in M_\nu(\mathbb{R})$, $\nu = \min(m, n)$, $\mu = \sup(m, n)$ or in a synthetic way

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

(and where allow with one non-positive size are empty!).

In this setup, the sequence (*) becomes (**)

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

or

$$(**) \quad \mathbb{R}^m = \mathbb{R}^\nu \xrightarrow{X \mapsto DX = \begin{pmatrix} \Delta X \\ 0 \end{pmatrix}} \mathbb{R}^n = \mathbb{R}^\mu \times \mathbb{R}^{\nu-\mu} \xrightarrow{(r,r') \mapsto ((r_i \bmod d_i)_i, r')} \prod_{i=1}^{\mu} \mathbb{R}/(d_i) \times \mathbb{R}^{\nu-\mu} \rightarrow 0 \text{ if } m \leq n$$

Lemma 5.6.0.1. *The sequence (**) is exact. In particular, one has a canonical isomorphism*

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

Proof. Let's deal with the case $m \geq n$, the other case being completely analogous.

The arrow $\mathbb{R}^n = \mathbb{R}^\mu \xrightarrow{r \mapsto (r_i \bmod d_i)_i} \prod_{i=1}^{\mu} \mathbb{R}/(d_i)$ being surjective as product of surjective maps, we 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 $r \in \mathbb{R}^\mu$ maps to zero, we have $r_i \bmod d_i = 0$ for all i and therefore there exists $x_i \in \mathbb{R}$ such that $r_i = d_i x_i$ for all i . We have $D \begin{pmatrix} (x_i)_i \\ 0 \end{pmatrix} = r$ proving $\text{Ker} \subset \text{Im}$ hence the exactness. The last point is just the functoriality of the cokernel 5.4.0.1. \square

With this generality, it's impossible to recover the diagonal coefficient only from the cokernel. It is even true for $n = m = 1$: 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 lemma. Let's fix this problem.

5.7 Invariant ideals of modules

Mimicking the definition of finite dimensional vector space, we say that a module M is of finite type if it has a finite generating family or, equivalently, if there exists a surjective morphism $R^n \rightarrow M$.

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 ideals⁸. 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.

5.7.1 Determinantal ideals

Let $A, B \in M_{p,q}(R)$. Let's 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 5.7.1.1. 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.

Example(s) 5.7.1.2. If $A \in M_p(R)$ is triangular and invertible, we have $\wedge^n(A) = R$ for $n \leq p$ and $\wedge^n(A) = 0$ for all $n > p$.

For instance,

Lemma 5.7.1.3. Let $A, B \in M_{p,q}(R)$ and $C \in M_{q,r}(R)$.

1. $\wedge^n(AC) \subset \wedge^n(A)$ 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.

⁸Our presentation is sort of mix between the original approach of H. Fitting ([10]) and the nice simple presentation by M. Hochster.

1. Each column of AP is a linear combination of columns of A . The multilinearity of the determinant then ensures that the minor $(AP)_{I,J}$ is a linear combination of determinants of size n matrices whose columns are columns of A (possibly equal) and 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 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 is indeed in $\wedge^n(A)$.
2. If $C \in M_q(\mathbb{R})$ is invertible, applying (1) to AC and C^{-1} yields an equality $\wedge^n(AC) \subset \wedge^n(A)$ 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 $\wedge^n(CA) \subset \wedge^n(A)$ if $C \in \text{GL}_p(\mathbb{R})$ hence the result.

□

If $\mathbb{R} = \mathbf{k}$ is a field, we know (Gauss algorithm for instance) that a r matrix in $M_{p,q}(\mathbf{k})$ is equivalent to $D_r = \text{diag}(\text{Id}_r, 0)$. Moreover, we have by direct computation $\wedge^n(D_r) = \{0\}$ for $n > r$ and $\wedge^n(D_r) = \mathbf{k}$ if $n \leq r$. We deduce

Corollary 5.7.1.4. *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.

5.7.2 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 its 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 $j_1, \dots, j_p \in J$).

- If $p > n$, there is not any such minor and $\wedge^p(\vec{m}, K) = 0$.
- 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 observe the two obvious properties

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

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, if

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

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 $\wedge^p(\vec{m}, K_J, K_{J'}) = \wedge^p(\vec{m}, K_J, 0) \stackrel{(*)}{=} \wedge^p(\vec{m}, K_J)$. Property $(**)$ immediately gives

Corollary 5.7.2.1. *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^k does not depend on the system of generators of $\text{Ker}(\pi)$. Let us prove in a analogous way that it does not depend neither of the choice of generators in the following sense.

Lemma 5.7.2.2. *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 5.7.2.3. Let $\vec{m} = (m_1, \dots, m_n)$ be a finite generating family of M . Let $p \geq 0$. We define the sequence of Fitting ideals⁹ $\Phi_\bullet(M) = (\Phi_p(M))_p$ of M by the formula

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

Example(s) 5.7.2.4. 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.

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

Proposition 5.7.2.5. 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 5.7.1).
2. Use the projection $R \rightarrow R/I$ to compute the (1) minors.
3. Developing a determinant with some row gives $\wedge^{n+1}(A) \subset \wedge^n(A)$ 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.


⁹In 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.

6. If π, π' are surjective morphisms $R^n \rightarrow M, R^{n'} \rightarrow M'$ respectively, so is $\pi \oplus \pi' : R^{n+n'} = R^n \oplus R^{n'} \rightarrow M \oplus M'$. The corresponding minors are diagonal matrices of minors of π and π' whose determinant is their product.

□

5.8 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>i.e.</i> M admits a base	
Finite type module M	finite generating family or $R^n \rightarrow M$ surjective	

5.8.1 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.

Definition 5.8.1.1. *A module M is of finite presentation if there is an exact sequence $R^m \rightarrow R^n \rightarrow M \rightarrow 0$.*

In down to earth term, this exactly means that the kernel $R^n \rightarrow M$ is finitely generated. Contrary to the vector space case, for general rings, it is not true that a submodule of a finite type module is of finite type.. As we will see in full detail in chapter 7, rings for which this pathology does not happen are *Noetherian* rings, a huge generalization of fields containing almost all rings appearing naturally in



⁹See 5.8.2.2 for the finite type case and chapter 7 in general.

algebra or number theory. In a first approach¹⁰, let us explain here how they are defined and what this is relevant for our finiteness problem.

Definition 5.8.1.2. *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 5.8.1.3. *Show that the rings of continuous real functions on \mathbf{R} is non Noetherian.*

Proposition 5.8.1.4. *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, γ_j) generates \bar{N} . \square

Exercise 5.8.1.5. *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 8.4.0.1).*

5.8.2 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) 5.8.2.1. 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 $e_j = \delta_{i,j}, i \in I$.

2. $R_{<n}[T]$ is a free R -module with base $T^i, i < n$ therefore of rank n for $n \in \bar{\mathbf{N}} = \mathbf{N} \cup \{\infty\}$.

¹⁰See 7.2 and 7.2.0.2 below



3. $M_{n,m}(R)$ is a free module with the standard base $(E_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}$.
4. The module R^m is free with base (canonical) $(e_j = E_{1,j})_{1 \leq j \leq m}$.
5. If $(e_i)_{1 \leq i \leq n}$ is a basis of the \mathbf{k} -vector space V , the e_i seen as constant polynomials of $V[T]$ form a basis for $V[T]$, a module which we will thus identify with $\mathbf{k}[T]^n$ through this means. Explicitely, once V has been identified to \mathbf{k}^n thanks to the basis e_j ,
6. the formula $(\sum_j \lambda_{i,j} T^j)_i = \sum_j (\lambda_{i,j})_i T^j$ identifies $(\mathbf{k}[T])^n$ and $(\mathbf{k}^n)[T] = V[T]$ which we will do henceforth.

Proposition 5.8.2.2. *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 π , one has $M' = M$ and we get therefore $R^J \xrightarrow{\sim} M$ hence the existence of $n = \text{Card}(J)$. By (4) of 4.2.0.1, n is uniquely determined by M . \square

Exercise 5.8.2.3. *Using Krull's theorem, how can you generalize the proposition for general free modules ?*

Remark(s) 5.8.2.4.

- This property fails if R is no longer assumed to be commutative (see 5.9.0.5).
- 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 module¹¹ (see 5.9.0.7)!



5.8.3 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) 5.8.3.1. Any finite ring is torsion. In finite dimension, the $\mathbf{k}[T]$ -module V_a associated to $a \in \text{End}(V)$ is torsion (use 4.1.2.2 for instance). More generally¹², if I is a nonzero ideal of R , the quotient module R/I (which will acquire a ring structure in the next chapter) is torsion.

If R is an integral domain¹³ and M a module, the set M_{tors} of torsion elements of M is a submodule called torsion module. It is no longer true if R is not integral (observe that $2 \pmod 6$ and $3 \pmod 6$ are torsion in $\mathbf{Z}/6\mathbf{Z}$ but that $5 \pmod 6$ is not). We will prove in the sequel that if R is PID, finite type modules are free^{8.4} if and only if they have no torsion. Not this not true in general (exercice TBD).



5.8.4 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

5.9 Exercises

Exercise 5.9.0.1. 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 5.2.4), then V is finite-dimensional if and only if V_a is of finite type and torsion.

Exercise 5.9.0.2. Let \mathbf{k} be a field and R a ring.

- Show that the invertibles of $\mathbf{k}[T]$ are the non-zero constant polynomials from \mathbf{k}^* .

¹²The advanced reader will notice that V_a is isomorphic to $\mathbf{k}[T]/(\mu_a)$ where μ_a is the minimal polynomial of a in the case where a is a cyclic endomorphism. We will shortly discuss in detail these topics.

¹³Recall that this means that R is not zero and that the product of two nonzero elements is nonzero.

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

Exercise 5.9.0.3 (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 5.9.0.4. 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 $\sigma \in \text{Hom}_{\mathbb{R}}(M_3, M_2)$ 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_3 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 $\pi : \mathbb{R}^{n+m} \rightarrow \mathbb{R}^m$ be the projection onto the last m coordinates. Show that there is an exact sequence $0 \rightarrow \mathbb{R}^n \rightarrow \mathbb{R}^{n+m} \xrightarrow{\pi} \mathbb{R}^m \rightarrow 0$ and that this sequence is split.
6. Suppose there are three square matrices A, B, C with coefficients in \mathbb{R} of size $n, n + m, m$ making the diagram commutative

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

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

Exercise 5.9.0.5. 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 $(e_k)_{k \in \mathbb{N}}$ and we denote \mathcal{R} the ring of linear applications on V (equipped with composition), identified as «infinite matrices» of $c\mathbb{R}^{\mathbb{N} \times \mathbb{N}}$. Define two linear applications T and T' on V by the following relations for $n \in \mathbb{N}$:

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

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

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

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 $n \in \mathbb{N}^*$.

Exercise 5.9.0.6. 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^δ 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

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

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 π , 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 5.9.0.7. 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 φ defines an isomorphism $\mathbf{M}^* \rightarrow \mathbf{N}$ and then conclude by a cardinality argument that \mathbf{M} is not free¹⁴.

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?
4. Let $u \in \mathbf{M}^*$ and denote by $\mathbf{S} = \{n \mid u(e_n) \neq 0\}$ the support of $\varphi(u)$. Show that there exists $x \in \mathbf{M}$ be an element whose support is \mathbf{S} and such that the mappings $\mathbf{S} \rightarrow |x_s|_2$ and $s \mapsto u(e_s)|x_s|_2$ from \mathbf{S} to \mathbf{R} are strictly decreasing.
5. Let $\mathbf{A} \subset \{0, 1\}^{\mathbf{N}}$ be the set of all sequences with value in $\{0, 1\}$ vanishing outside \mathbf{S} . For $\varepsilon \in \mathbf{A}$, 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 $\Psi : \mathbf{A} \rightarrow \mathbf{Z}$ is injective.
6. Prove $\text{Im}(\varphi) = \mathbf{N}$ by considering the cardinality of \mathbf{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 \mathbf{M}^* .

¹⁴This method of proof of Baer's result comes from [9]

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

Chapter 6

Rings and Modules



6.1 Introduction



Perspective

We will illustrate how modules are an important tool to study rings and... conversely. In particular, we will emphasize the role of matrices which is crucial, the first step towards the advanced notion of *resolution* of a module/ring.

6.2 Quotient rings

Recall that an ideal I of a ring R is a submodule of R , that is an additive subgroup of R such that $\forall r \in R, rI \subset I$. By 5.2.3, there exists a unique group structure on R/I making the projection $\pi : R \rightarrow R/I$ a morphism.

6.2.1 Definition

The main (simple but important) result goes as follows:

Proposition 6.2.1.1. *There exists a unique group structure on R/I making the projection $\pi : R \rightarrow R/I$ a morphism whose kernel is I . One has the following universal property (cf. 5.5.2.1) : for any ring T , the natural sequence*

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

is exact. Moreover, if $f \in \text{Hom}(R, R')$, then f induces a canonical isomorphism of rings $\bar{f} : R/\text{Ker}(f) \simeq \text{Im}(f)$ (cf. 5.2.3.4).

In a diagrammatic way, the main point summarizes as

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

Proof. The proof goes straightforward as in the module case except for the fact that π is multiplicative which follows from the computation

$$\pi(r_1)\pi(r_2) = (r_1 + I)(r_2 + I) + I = r_1r_2 + r_1I + r_2 + I^2 + I = r_1r_2 + I$$

because $r_1I + r_2 + I^2 \subset I$ (recall that if I, J are ideals, IJ denotes the ideal generated by all products ij where $i \in I, j \in J$). \square

Exercise 6.2.1.2. *With the above notations, show that the map $\bar{J} \mapsto J = \pi^{-1}(\bar{J})$ identifies ideals \bar{J} of $\bar{R} = R/I$ and ideals J of R containing I . Show that π induces an isomorphism $R/J \xrightarrow{\sim} \bar{R}/\bar{J}$.*

Definition 6.2.1.3. *An ideal I of R is prime if and only if R/I is an integral domain, maximal if R/I is a field (cf. 6.6.0.5).*

6.2.2 Product Rings

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

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

Lemma 6.2.2.1. *Let I be an ideal of K_T and $S = \{t \in T \mid p_t(I) = \{0\}\}$. Then $I = I_S$ and $K_T/I = K_S$.*

Proof. Let $e_t = (\delta_{t,t'})_{t' \in T} \in K_T$. 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 K_t and therefore is equal to K_t . We can choose $i_t \in I$ such that $p_t(i_t) = 1 \in K_t$ 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

6.2.3 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 6.2.3.1 (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 $I = \text{Ann}_R(M) = \{\lambda \in R \mid \lambda M = \{0\}\}$ and the map $J \supset I \mapsto JM \xrightarrow{\sim} J/I$ identifies the ideals of $J \supset I$ and the submodules of N . In particular, if the ideals of R can be generated by a single element, 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. The last point is the formula $I = \text{Ann}_R(R/I)$ and the fact that the submodules of R/I are in one to one correspondence to ideals of J containing I . \square

Exercise 6.2.3.2. *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 $I = \{0\}$)¹. Prove that the ideal of real $\mathbf{R}[X, Y]$ vanishing at $(0, 0)$ is not cyclic but is a submodule of cyclic module.*

6.3 Algebras

Let us be given two rings A, B . 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

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

¹As we will see, this result is true for all PID.

It 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 which is multiplicative with $f(1_B) = 1_{B'}$.

Proposition 6.3.0.1. *Let B be an A -algebra and $b \in B$. There exists a unique algebra morphism $A[X] \rightarrow B$ that sends X to b . Moreover, all morphisms are of this type.*

Proof. Let φ be such a morphism. Then, necessarily, $\varphi(\sum_i a_i X^i) = \sum_i a_i \varphi(X)^i$ and thus is determined by $b = \varphi(X)$. Conversely, we know (4.1.2.1) that this A -module morphism

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

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 morphism $(P \mapsto P(b))$).

Note that if B is an A -algebra and I an ideal of B , 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.

Exercise 6.3.0.2. *Describe an isomorphism of \mathbf{R} -algebras between $\mathbf{R}[X]/(X^2 + X + 1)$ and \mathbf{C} on one hand, and between $\mathbf{R}[X]/(X(X + 1))$ and \mathbf{R}^2 on the other hand.*

6.4 Integrality

Let us illustrate how the close relation between rings and modules allows to prove stability results for algebraic or integral elements.

6.4.1 An Application of Cayley-Hamilton

Proposition 6.4.1.1 (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 consider a matrix $A = [a_{i,j}]$ of f , i.e. for each j , write (in a non-unique way)

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

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 (4.1.2.2) 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.

Corollary 6.4.1.2 (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 (e.g., if i is nilpotent), then $M = 0$.*

6.4.2 Rings of Integers

Let R' be an R -algebra (in other words, consider a ring morphism $R \rightarrow R'$). An element $x \in R'$ is said to be integral over R if it is annihilated by a monic polynomial with coefficients in R .

Lemma 6.4.2.1. *$x \in R'$ 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 canceled 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 homomethy h_x of ratio x on R'' produces a monic annihilator $P \in R[T]$ and therefore $P(h_x)(1) = h_{P(x)}(1) = P(x) = 0$. □

Corollary 6.4.2.2. *The subset \mathcal{O} of R' of elements which integral over R forms a subring of R' . Moreover, any element of R' which is integral over \mathcal{O} belongs to \mathcal{O} .*

Proof. If $x, y \in \mathcal{O}$ are canceled 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.

If x is integral over \mathcal{O} , the subring of R' generated by x and the coefficients of a monic polynomial of $\mathcal{O}[T]$ canceling x is of finite type over R and therefore $x \in \mathcal{O}$. □

Corollary 6.4.2.3. *Let k be a subfield of a field k' . Then the subset of elements of k' that are algebraic over k forms a subfield of k' .*

Proof. Following 6.4.2.2 applied to $R = k$, 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 $1/x$. \square

Remark(s) 6.4.2.4. For instance, the set $\overline{\mathbf{Q}}$ of complex numbers which are algebraic over \mathbf{Q} is a subfield of \mathbf{C} and the $\overline{\mathbf{Z}}$ of complex numbers which are integral over \mathbf{Z} is a subring of $\overline{\mathbf{Z}}$. One can show without too much difficulty that $\overline{\mathbf{Q}}$ is algebraically closed (6.6.0.9), which is a good news, and that $\overline{\mathbf{Z}}$ is non Noetherian (10.2.2.4), which is bad news in some extent.

Remark(s) 6.4.2.5. 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 π (F. Lindemann, 1883) are transcendental.

Exercise 6.4.2.6. 1. Show that a rational number is integral over \mathbf{Z} if and only if it is an integer.
2. Show that the minimal degree monic polynomial $P \in \mathbf{Q}[T]$ that annihilates $\exp(\frac{2i\pi}{n})$ has integer coefficients.

6.5 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 that more generally that $R/(ab) \xrightarrow{\sim} R/(a) \times R/(b)$ for coprime ideals $(a), (b)$ in a PID R . This 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 (if we have just a ring structure, recall that any ring is uniquely a \mathbf{Z} -algebra). 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.

Proposition 6.5.0.1 (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 .



Terracotta Army
Mausoleum of Emperor Qin

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 $e_j = \varepsilon_j \pmod{I_1 \cdots I_n}$.

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)³.

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

$$\varphi_M: M/(I_1 \cap \cdots \cap I_n)M \simeq \prod M/I_j M$$

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 $m \sum \varepsilon_j m$.

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 φ is onto. We write $1 = \sum_j \varepsilon_j$, $\varepsilon_j \in I(-j)$. Let $x_j \pmod{I_j}$ be arbitrary classes. Set $x = \sum_j \varepsilon_j x_j$. Observe that

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

³Recall that by definition its is the ideal generated by products of $\prod_{i \neq j} x_i$ with $x_i \in I_i$.

³By 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.

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

3. The other items follow directly from (*)

□

Remark(s) 6.5.0.2. 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 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 $\prod_{i \in I} K_i$ of a finite product of fields is isomorphic to $\prod_{j \in J} K_j$ where $J = \{i \in I \mid e_i \text{Ker} = \{0\}\}$.

6.6 Exercises

Exercise 6.6.0.1. TBD

Exercise 6.6.0.2. 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 6.6.0.3 (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. 5.2.4), 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

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

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

5. If Q is monic, show that $\text{Res}(\prod(T - r_i), Q) = \prod Q(r_i)$. 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 6.6.0.4. 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 $d \equiv 2, 3 \pmod{4}$.

Exercise 6.6.0.5. 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 6.6.0.6. 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 $|P(\frac{p}{q})| \geq \frac{1}{q^d}$.

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

1. Show that the $P_m(\mathbb{T})$ 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 6.6.0.8. Existence corps alg clos. TBD

Exercise 6.6.0.9. TBD \bar{k} is algebraically closed.

Exercise 6.6.0.10. Let R be a ring and $P = \sum_{i=0}^n a_i \mathbb{T}^i \in R[\mathbb{T}]$.

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 $R[\mathbb{T}]$ if and only if a_0 is invertible and for all $i \geq 1$, a_i is nilpotent. Hint: if $Q = \sum_{i=0}^m b_i \mathbb{T}^i$ is an inverse of P , one could start by showing that for all $r \geq 0$, $a_n^{r+1} b_{m-r} = 0$.

Chapter 7

Noetherianity



David Hilbert



Emmy Noether

7.1 Introduction



Perspective

We will illustrate how the intertwining between finite type properties of modules (Noetherian conditions) and matrix computations allows to obtain quite general and non trivial result in an easy way like the structure theorem for finite type abelian groups (8.4.0.3) or more generally of finite type modules over PID (8.4.0.1).

The notion of Noetherian ring inevitably leads back to Hilbert's foundational paper from 1890 [14] with its three major theorems, the first being the Basis Theorem 7.2.2.1 in the case of polynomial rings. However, as a student rightly pointed out to me, talking only about this (tremendous) paper¹ is unfair. Indeed, it was Emmy Noether who developed the general vision as early as 1920 ([17]). We will give the basics about Noetherian rings and modules and explain the link with linear algebra.

7.2 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

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

finitely generated R module is still finitely generated when R is a field, this is generally not the case (cf 5.2.4). However, it is the case in a Noetherian setting.

Lemma 7.2.0.1. *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. Then, $\cup M_i$ is a submodule of M , thus 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' : therefore, it is equal to it, so that $n \in N'$. We thus have $N' = N$ and therefore N is finitely generated. □

Definition 7.2.0.2.

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 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) 7.2.0.3. *Submodules of Noetherian modules are Noetherian (tautological), as are the quotients of Noetherian modules (easy exercise). 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 field of fractions which is!).*

7.2.1 Stability under exact sequences

Proposition 7.2.1.1. *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. The direct part has already been observed in the previous example. Conversely, 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 7.2.1.2. *The Noetherian modules over a Noetherian ring are exactly the finitely generated modules.*

Remark(s) 7.2.1.3. *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 K is again of finite type as submodule of the Noetherian module R^n . There exists therefore a surjective morphism $R^m \rightarrow K$ and the composition with the inclusion $K \rightarrow R^n$ 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.*

7.2.2 Hilbert's Basis Theorem

Theorem 7.2.2.1. *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 an immediate consequence of the first (by induction, any polynomial ring over R with n variables is Noetherian, and thus so is any quotient). Let's consider the first point.

Let I be an ideal of $R[T]$ and $I^* = I - \{0\}$. If P is a non-null polynomial, denote $\text{dom}(P)$ its highest degree non-null coefficient. The formula $\text{dom}(T^n P) = \text{dom}(P)$ ensures that $\{0\} \cup \text{dom}(I^*)$ is an ideal of R (exercise). It thus has a finite number of generators of the form $\text{dom}(P_i), P_i \in I^*$ which can be assumed to be of the same degree $d \geq 0$ according to the previous formula. An immediate induction then shows $I \cap R_{\geq d}[T] = \langle P_i \rangle$. But $I \cap R_{\leq d}[T]$ is a sub- R -module of $R_{< d}[T] \simeq R^d$: therefore, it is a Noetherian module like R^d (7.2.1.2). One can thus take a finite number of generators Q_j (as an R -module) and the finite family (P_i, Q_j) generates I . \square

We have in fact reused the argument of Euclidean division used to show that $\mathbf{k}[T]$ is principal, the problem being that one 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 leading coefficients of I .

7.3 Exercises

Exercise 7.3.0.1. *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.*

Exercise 7.3.0.2. *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 $f_n \prod_{k=0}^n (z - k) = \sin(\pi z)$.*
3. *Compute $f_n(k)$ for $k \in \mathbf{Z}$.*
4. *Prove that R is not Noetherian.*

Exercise 7.3.0.3. *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, R^G is Noetherian.

Exercise 7.3.0.4. 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 7.3.0.5. 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 4.2.0.1.
4. Using 7.3.0.4, give another proof of (3) and (4) of 4.2.0.1.

Chapter 8

Matrix and modules over PID



8.1 Introduction



Perspective

As explained in 7.2.1.3, equivalence of matrices is deeply linked to module structure. We will show how this remark yields general and non trivial results like the structure theorem for finite type abelian groups (8.4.0.3) or more generally of finite type modules over PID (8.4.0.1).

We study the equivalence relation \sim on $M_{p,q}(R)$ for R a PID (or if the reader is specifically interested in applications to abelian groups or similarity of matrices over fields (see chapter 9), he can restrict himself to the Euclidean rings $R = \mathbf{Z}$ or $R = \mathbf{k}[T]$). We will explain where the equivalence relation \sim of matrices coincides with the Gauss equivalence \equiv when R is Euclidean giving an efficient algorithm to handle this problem in this case. We have added a "cultural" chapter (8.6) giving some hints about advanced results explaining the deep and subtle differences between these two equivalence relations which already arise in this "simple" case of PID.

We address two questions.

1. Describe $M_{p,q}(R)/\sim$ by giving a canonical representative in each similarity class. This is achieved in 8.3.1.2 (3).

2. Describe the map by giving an algorithmic way to decide when $A \sim B$. This is achieved in 8.3.1.2 (1).

8.2 Survival kit for PID and Euclidean rings

As usual, for $x \neq 0, y$ elements an integral ring R , we say that $x|y$ if there exists $z \in R$ such that $y = xz$. We write $x|y$. Recall that a principal ring is an integral ring whose ideals can be generated by a single element. The usual examples of PID 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 8.2.0.1. *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 exists¹ $q, r \in R$ such that $a = bq + r$ and $r = 0$ or $f(r) < f(b)$.*

Lemma 8.2.0.2. *An Euclidean ring is principal.*

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 $I \subset bR$. \square

Definition 8.2.0.3. *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 R^*/R^\times .

Proposition 8.2.0.4 (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, $1 = \text{GCD}(x_i)$ 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*

¹We do not require the uniqueness of (q, r) .

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 $I = R = R.1$. \square

Proposition 8.2.0.5 (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

Exercise 8.2.0.6. *Prove that any non zero prime ideal of a PID is maximal.*

8.3 Matrix equivalence in PID and Euclidean rings

8.3.1 Invariant ideals of a matrix

In this section, R is a PID, $A = [a_{i,j}] \in M_{n,m}(R)$ is a matrix and $\nu = \min(p, q)$. Let us adapt Gauss elimination method 4.3.1.1 to prove the following proposition. We will need more than Gauss elementary operations in this case.

Definition 8.3.1.1. *Two matrices are if they differ by a series of left and right multiplications by transvections 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 . The main observation is that $(a, b) \simeq (\text{GCD}(a, b), 0)$ for any $(a, b) \in R^2 - \{0\}$. Indeed, by Bézout theorem, there exists $u, v \in R|au + bv = \text{GCD}(a, b)$ and therefore

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

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 8.3.1.2.

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. $\text{Coker}(A) \xrightarrow{\sim} \bigoplus_{j=1}^n \mathbb{R}/I_j$ 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 \mathbb{R} if $i > \nu$.
4. The ideals and I_j depends only on the equivalence class of A . They are called the invariant ideals² of A .
5. Two matrices are equivalent if and only if they have the same invariant ideals.
6. Equivalent matrices are Bézout equivalent. In particular the invariant factors of A are those of Id_n , they are equal to 1.

Proof.

1. We use induction on $n + m$ starting with the obvious case $n + m = 2$. We can assume $A \neq 0$
 - Transposing if necessary, one can assume $m \leq n = \nu \geq 1$. Recall that the ideal $\wedge^1(A) \wedge^1(A)$ generated by the coefficients of A is invariant by matrix equivalence (5.7.1.3).
 - Assume first $n = 1$ (A is a line matrix). I claim that $A \simeq (d, 0, \dots, 0)$ with $\wedge^1(A) = (d)$. This is true if $m = 1$ and, using the invariance of $\wedge^1(A)$ by equivalence, is reduced by an immediate induction to the $m = 2$ 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 $n = 1$ or $m = 1$.
 - Assume now $n, m > 1$. 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 $d_\nu \text{ not } = 0$ because $A \neq 0$.
 If $a_{1,j}, j > 1$ is not divisible by $a_{1,1}$, then (d_ν) is strictly contained in $(\wedge^1(d_\nu, a_{1,j}))$. But using Bézout replacement, this contradicts the maximality of (d_ν) .
 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.

²By 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.

- 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 $\bar{A} \in M_{n-1, m-1}(\mathbb{R})$ and we conclude by induction.
2. This is the functoriality of the cokernel and the computation of the cokernel in the diagonal case (5.6.0.1).
 3. Direct consequences of the calculations of the Fitting ideals of a direct sum (5.7.2.5).
 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 independence of the number $\rho = n - \nu + N$ 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 \mathbb{R} is an integral domain.
 5. Direct consequence of (1) and (3).
 6. Direct consequence of (4) and (1).

□

Exercise 8.3.1.3. Let K be the fraction field of \mathbb{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 $\text{rank}(\text{Coker}(A)) = n - r$.

8.4 Invariant factors of a module

Let us reap the benefits of our labor.

Theorem 8.4.0.1 (Structure theorem of finite type modules over PID). *Let M be a finite type module over a PID \mathbb{R} .*

1. Every submodule of M is of finite type.
2. There exists an exact sequence $\mathbb{R}^m \xrightarrow{A} \mathbb{R}^n \rightarrow M \rightarrow 0$ and $M \xrightarrow{\sim} \bigoplus \mathbb{R}/I_j$ 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 $M_{\text{tors}} \oplus \mathbb{R}^r$ with $r = \text{rank}(M) = \text{Card}\{j | I_j = (0)\}$ and

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

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 (8.3.1.2).

1. R is Noetherian and so is M (7.2.1.2).
2. The existence of the exact sequence is (7.2.1.3) and the remaining part is (8.3.1.2) taking into account account that $R/I_j = \{0\}$ if I_j is not proper.
3. Cf. (8.3.1.2).
4. Cf. (8.3.1.2).
5. Direct consequence (2).
6. Direct consequence of the previous item and of 4.2.0.1.
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 $A = PDQ$ (8.3.1.2). 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 $D_{i,i} \neq 0$.

□

Exercise 8.4.0.2. *With keep the notation above. Assume that M is not cyclic with infinite cardinality. Prove that there the number of submodules of M is infinite. Prove the converse if $R = \mathbf{k}[T]$ or $R = \mathbf{Z}$ (cf. 6.2.3.2)³.*

Corollary 8.4.0.3 (Structure theorem of finite type abelian groups). *Let G be a finite type abelain group. There exists a unique sequence of integers $2 \leq d_n | \dots | d_1$ and $r \geq 0$ such that $G \cong \bigoplus_i \mathbf{Z}/d_i \mathbf{Z} \oplus \mathbf{Z}^r$.*

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

□

8.4.1 The Euclidean case

³As we will see, this result is true for all PID (10.2.2.2).

Proposition 8.4.1.1. *Assume R is Euclidean. Then*

$$\text{equivalence} \Leftrightarrow \text{Bézout equivalence} \Leftrightarrow \text{Gauss equivalence}$$

Proof. By 8.3.1.2 we just have to show Bézout equivalence \Leftrightarrow Gauss equivalence, Let $L = (a_0, a_1) \in R \times R^*$ and $a_0 = a_1q_0 + a_2$ with $f(a_2) < f(a_1)$ or $a_2 = 0$. Using the Gauss operation $a_0 \mapsto a_0 - q_0a_1$, 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 δ 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. \square

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 following Gauss equivalence is.

Exercise 8.4.1.2. *Write a software 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?*

Corollary 8.4.1.3. *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 (8.3.1.2) that their invariant factors are equal to 1 proving that A is Gauss equivalent to an invertible diagonal matrix and we apply lemma 4.3.2.1. In particular, $\text{SL}_n(R)$ is generated by transvections. \square

8.5 About uniqueness of invariant ideals

This section can be skipped in a first reading not because it is difficult but because the results are more or less rather cultural than useful. In the PID situation, we have seen that any finite type module M is isomorphic to a direct sum $\bigoplus_{i=1}^n M_i$ with $\text{Ann}_R(M_1) \subset \text{Ann}_R(M_2) \subset \dots \subset \text{Ann}_R(M_n)$. In other words, M is isomorphic to $\bigoplus_{i=1}^n R/I_i$ where $I_1 \subset I_2 \subset \dots \subset I_n$ is an increasing sequence of proper ideals which depends only on M . In general, they are a lot of modules that are not of this form. But in the case where such a decomposition exist, let us show that the ideals are uniquely defined as in the PID case⁴

⁴This is well known, and easy, in the Noetherian case, using the existence of enough irreducible elements, see below. With this generality, I learned this nice argument from <https://math.stackexchange.com/q/3147043>.

Assume therefore that M has such a decomposition but that R is no longer assumed to be a PID.

Lemma 8.5.0.1. *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 $R^d \mapsto \oplus R/I_k \oplus (R/I_n)^n$ which factors through a surjection $(R/I_n)^d \rightarrow (R/I_n)^n$ implying $d \geq n$ by 4.2.0.1.
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 $xM \cong \oplus_{k=1}^{n(x)} R/(I_k)_x$ 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 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) 8.5.0.2.

- *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 8.7.0.12).*

8.6 Supplementary Section: Insight into K-Theory



This section is cultural and can therefore be skipped at the first glance. It aims to introduce an important idea in mathematics: how to measure the obstruction to a result being true. Here, the question is how to measure the potential impossibility of *diagonalizing* matrices by means of Gaussian elimination in a ring R .

The precise question one naturally addresses is then: is the group $GL_n(\mathbf{R})$ generated by the elementary matrices of transvections of pivot type (1.2)? We will consider the matrices of permutation and dilatations (because they can be easily handled through the determinant function below).

The first step is to move away from n : for this, we view $GL_n(\mathbf{R})$ as the subgroup of $GL_{n+1}(\mathbf{R})$ consisting of block diagonal matrices of the form $\text{diag}(M, 1)$, where $M \in GL_n(\mathbf{R})$. This allows us to consider their infinite union $GL(\mathbf{R})$, seen as the set of matrices of infinite size, containing all finite-sized linear groups. We then define $E(\mathbf{R}) = \cup E_n(\mathbf{R})$ as the subgroup of $GL(\mathbf{R})$ generated by all transvections (cf. 4.3), *i.e.* the determinant 1 matrices that we can reach by Gauss elimination (even if we allow enlarging the matrices). The first result is both simple and remarkable, especially in the proof provided by [16].

Lemma 8.6.0.1 (Whitehead). *For any ring \mathbf{R} , the group $E(\mathbf{R})$ is the derived group $[GL(\mathbf{R}), GL(\mathbf{R})]$ generated by the commutators $[A, B] = ABA^{-1}B^{-1}$ of matrices in $GL(\mathbf{R})$.*

In particular, $E(\mathbf{R})$ is a normal subgroup, and the quotient $K_1(\mathbf{R}) = GL(\mathbf{R})/[GL(\mathbf{R}), GL(\mathbf{R})]$ is a commutative group, as it is the abelianization of $GL(\mathbf{R})$! 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 (6.2) to define the special group of algebraic K-theory of degree 1:

$$SK_1(\mathbf{R}) = \text{Ker}(GL(\mathbf{R}) \xrightarrow{\det} \mathbf{R}^\times).$$

This group avoids considering dilatations and permutation matrices, which do not play a crucial role in pivoting. The inclusion $\mathbf{R}^\times = GL_1(\mathbf{R}) \hookrightarrow GL(\mathbf{R})$ followed by the quotient projection $GL(\mathbf{R}) \rightarrow K_1(\mathbf{R})$ allows us to define a map:

$$\mathbf{R}^\times \times SK_1(\mathbf{R}) \rightarrow K_1(\mathbf{R}),$$

which is visibly an isomorphism.

Remark(s) 8.6.0.2. *This result is far from being banal. Precisely, $E_2(\mathbf{R})$ is not normal in $GL_2(\mathbf{R})$ for $\mathbf{R} = \mathbf{k}[T_1, T_2]$. Precisely, the matrix $A = \begin{pmatrix} 1 + T_1 T_2 & T_1^2 \\ -T_2^2 & 1 - T_1 T_2 \end{pmatrix} \notin E_2(\mathbf{k}[T_1, T_2])$ and one can show that $AM_{(1,2)}A^{-1} \notin E_2(\mathbf{R})$. More surprising, if $\mathbf{R} = \mathbf{Z}[1/2 + \theta]$ with $\theta = \sqrt{-19}/2$, Cohn (*op. cit.*) has shown that $A = \begin{pmatrix} 3 - \theta & 2 + \theta \\ -3 - 2\theta & 5 - 2\theta \end{pmatrix} \notin E_2(\mathbf{R})$ and again $AM_{(1,2)}A^{-1} \notin E_2(\mathbf{R})$ (Lam, *op. cit.*). And we know that \mathbf{R} is a PID (8.7.0.5)! On the other hand, Suslin has shown that $E_n(\mathbf{k}[T_1, \dots, T_m])$ is normal in $GL_n(\mathbf{k}[T_1, \dots, T_m])$ 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, §I.8*).*

The group $\text{SK}_1(\mathbf{R})$ is evidently the obstruction to the Gauss elimination algorithm (infinite) being able to diagonalize matrices. And our results prove that if \mathbf{R} is Euclidean, $\text{SK}_1(\mathbf{R}) = 0$. It is noteworthy that this obstruction is very sudden. For example, in the case of the non-Euclidean principal ring $\mathbf{R} = \mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, we have $\text{SK}_1(\mathbf{R}) = \{1\}$ (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 when allowing to increase the size of matrices. Finding a principal \mathbf{R} such that $\text{SK}_1(\mathbf{R})$ is non-trivial is difficult. An example is given in [12]: take the subring of $\mathbf{Z}(T)$ generated by $\mathbf{Z}[T]$ and the $(T^m - 1)^{-1}$ for $m \geq 1$. This is a principal ring (!) whose SK_1 is even infinite.

8.7 Exercises

Exercise 8.7.0.1.

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 8.7.0.2. Prove that $\mathbf{R}[T]$ is a PID if and only if \mathbf{R} is a PID.

Exercise 8.7.0.3. Let \mathbf{R} be an integral ring \mathbf{K} its with fraction field . 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 8.7.0.4. 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 8.7.0.5. 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 exist $q, r \in A$ 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 $q, r \in A$ such that $N(r) < N(b)$ and

$$2a = bq + r$$

10. Conclude that R is a PID.

Exercise 8.7.0.6. *Base adaptée et équation diophantienne TBD*

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

Exercise 8.7.0.7. *Transform the proof of 8.4.1.1 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 8.7.0.8. *TBD*

Exercise 8.7.0.9. *TBD 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 8.7.0.10. *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 8.7.0.11. *Let $P, Q \in \mathbf{k}[T]$ 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 8.7.0.12. *Let $R = \mathbf{Q}[T_1, T_2]/(T_1^2 - T_2^2)$. Show that $M_i = R/(T_i, T_1 T_2) \oplus R/(T_1, T_2)$ have the same Fitting ideals but their invariant ideal sequences in the sense of 8.5 are distinct. Can you produce an analogous example with R an integral domain?*

Part II

Linear Algebra over Fields

Chapter 9

Similarity in $M_n(\mathbf{k})$



9.1 Introduction



Perspective

We explain how the understanding of matrices with coefficients in the PID $\mathbf{k}[T]$ allows to completely understand the similarity problem in $M_n(\mathbf{k})$ in a completely algorithmic manner (5.2.4).

The goal of the chapter is the study the similarity equivalence relation \equiv on $M_n(\mathbf{k})$, in other words we would like to understand the quotient map of sets $M_n(\mathbf{k}) \rightarrow M_n(\mathbf{k})/\equiv$. We need to answer two questions

1. Describe $M_n(\mathbf{k})/\equiv$ by giving a canonical representative in each similarity class. This is achieved in 9.2.2.1.
2. Describe the map by giving an algorithmic way to decide when $A \equiv B$. This is achieved in 9.4.0.2.

The main point is the dictionary between \mathbf{k} -endomorphisms and $\mathbf{k}[T]$ -modules (5.2.4) which allow to translate this problem in terms of the equivalence class of $T \text{Id} - A, A \in M_n(\mathbf{k})$ in $M_n(\mathbf{R})$ where $\mathbf{R} = \mathbf{k}[T]$ and then to use our understanding of these classes in this Euclidean situation (cf. 8.3.1.2).

9.2 Similarity in $M_n(\mathbf{k})$

The main theorem 8.4.0.1 has a version for polynomial rings. We use it to classify matrices of $M_n(\mathbf{k})$ up to similarity. The useful version in classical linear algebra come from the use of the $\mathbf{k}[T]$ -module V_a associated to an endomorphism of V .

9.2.1 Similiarity invariants

Let $a, b \in \text{End}_{\mathbf{k}}(V)$ be an endomorphism of an n dimensional vector space V .

Corollary 9.2.1.1 (Similarity invariants of vector space endomorphisms).

1. The torsion $\mathbf{k}[T]$ -module V_a is of finite type and torsion.
2. The rank of V_a is zero and its invariant ideals are nonzero.
3. Let $P_i, 1 \leq i \leq m$ the unique monic generator of the invariant factor I_i of V_a . We have $P_m | \dots | P_1$ and $V_a \xrightarrow{\sim} \bigoplus_{i=1}^m \mathbf{k}[T]/(P_i)$.
4. $m \leq n$. We define $P_i = 1$ for $m < i \leq n$: the similarity invariants of a .
5. If $Q_{m'} | \dots | Q_1$ are monic polynomials such that $V_a \xrightarrow{\sim} \bigoplus_{i=1}^{m'} \mathbf{k}[T]/(Q_i)$, then $m = m'$ and $P_i = Q_i$ for all i .
6. a and b are similar if and only if there similarity invariant are equal¹.

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. There exists a non zero $P \in \mathbf{k}[T]$ such that $P(f) = 0$ (use Cayley-Hamilton theorem or 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 $P(T).V_a = \{0\}$.
2. Use 8.4.0.1 or simpler that if $v \in V_a$ were not torsion, then $\mathbf{k}[T]v = Rv \subset V_a$ which cannot be for dimension reason.
3. This is (5) of the structure theorem 8.4.0.1 taking into account $\text{rank}(V_a) = 0$.
4. Direct consequence of (4) by a dimension argument.
5. This is (4) of 8.4.0.1.
6. Direct consequence of (3) and the dictionary 5.2.4.

□

¹Of course, we still have $V_a \xrightarrow{\sim} \bigoplus_{i=1}^n \mathbf{k}[T]/(P_i)$.

9.2.2 Explicit computations of similarity invariants

We keep in mind the notations and result of 5.3.2. Let $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ be a basis of V and A the matrix of a in this basis. We define the $\mathbf{k}[T]$ -module $V_A = \mathbf{k}^n$ by the rule $P(T)X = P(A)X$ for all $X \in \mathbf{k}^n = M_{n,1}(\mathbf{k})$.

Of course, the isomorphism $\mathbf{k}^n \xrightarrow{\sim} V$ defined by \mathcal{B} induces an isomorphism $V_A \xrightarrow{\sim} V_a$.

The map $(P_i(T) = \sum_j P_{i,j}T^j) \mapsto \sum_{i,j} P_{i,j}e_iT^j$ is an isomorphism of $\mathbf{k}[T]$ -modules $(\mathbf{k}[T])^n \xrightarrow{\sim} V[T]$ and the exact sequence².

$$V[T] \xrightarrow{T\text{Id}-\tilde{a}} V[T] \xrightarrow{\pi_a} V_a \rightarrow 0$$

becomes

$$0 \rightarrow (\mathbf{k}[T])^n \xrightarrow{T\text{Id}-A} (\mathbf{k}[T])^n \xrightarrow{\pi_A} V_A \rightarrow 0$$

or in purely matrix terms

$$0 \rightarrow (\mathbf{k}[T])^n \xrightarrow{T\text{Id}-A} (\mathbf{k}[T])^n \xrightarrow{\pi_A} V_A \rightarrow 0$$

where $\pi_A(\sum X_i T^i) = \sum A^i X_i$.

Because V_a has no nonzero invariant ideals, we get by 9.2.1.1

the invariant ideals of $T\text{Id} - A$ are the similarity invariants of a characterized by
 $T\text{Id} - A \equiv \text{diag}(P_1, \dots, P_n)$.

Taking this result into account, we can rewrite 9.2.1.1.

Corollary 9.2.2.1. *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
- $T\text{Id} - A \equiv \text{diag}(P_i)$.
- $T\text{Id} - A \sim \text{diag}(P_i)$.
- $V_a \xrightarrow{\sim} \oplus \mathbf{k}[T]/(P_i)$.

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.

²Recall that we have already observed that the left arrows are injective but it is not crucial for us even if this fact is hidden in the next argument



Corollary 9.2.2.2. *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 χ_a and P_1 have the same roots in any extension of \mathbf{k} (hence have the same irreducible factors³).
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 μ_a).

Proof.


1. There exists $Q, Q' \in GL_n(\mathbf{R})$ 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.
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 χ_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.

□

Remark(s) 9.2.2.3.

- Notice that the above proposition 9.2.2.2 reproves the very existence of μ_a without any previous knowledge. By construction, it is the unique monic polynomial of least degree annihilating a .

³Cf. chapter 10

- The interested reader can check that we did not use the Cayley-Hamilton theorem (4.1.2.2) to prove these results. Therefore, the divisibility $P_1 = \mu_a | \chi_a$ is another (too complicated) proof in the field case.
- As we will see later (for example 9.4.0.4), the last P_i are often equal to 1. They contribute by 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 instance, the similarity invariant of $\text{diag}(0, t)$ are $1, T(T - t)$ if $t \neq 0$ and are T, T if $t = 0$. We will discuss this phenomenon in full generality in chapter 14. 

Finally, let us give two classical results.

Corollary 9.2.2.4. *Let $A, B \in M_n(\mathbf{k})$ and K a field containing \mathbf{k} . We have*

1. A and tA 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 $T - \text{Id } {}^tA = {}^tQ' \text{diag}(P_i){}^tQ$.

2. If P_i, \tilde{P}_i are the similarity invariants of A in $M_n(\mathbf{k})$ and $M_n(K)$, we have $T \text{Id} - A \simeq \text{diag}(P_i)$ in $M_n(\mathbf{k}[T])$ and therefore $T \text{Id} - A \simeq \text{diag}(P_i)$ 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 $T \text{Id} - A \simeq \text{diag}(\tilde{P}_i)$ in $M_n(K)$. By uniqueness, we get $P_i = \tilde{P}_i$, hence the result. □

9.3 An important example: diagonalization

Although diagonalizing endomorphisms is not necessary to understand similarity of matrices, let us illustrate our results in this special case. We will denote by \mathbf{k}_λ the $\mathbf{k}[T]$ -module $\mathbf{k}_\lambda = \mathbf{k}[T]/(T - \lambda)$. Its 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 λ characterized by $T.1 = \lambda$.

By definition, let us recall that $a \in \text{End}_k(V)$ is diagonalizable if and only if V has a basis of eigenvectors, *i.e.*if

$$V_a = \bigoplus \text{Ker}(a - \lambda \text{Id})$$

Equivalently, a is diagonalizable if its matrix in an arbitrary matrix is similar to a diagonal matrix. The similarity invariants theory reads as follows in this case.

Proposition 9.3.0.1. *The following assertions are equivalent.*

1. a is diagonalizable.
2. a is canceled by some non zero $P \in \mathbf{k}[T]$ which is split with $\text{GCD}(P, P') = 1$.
3. μ_a is split with $\text{GCD}(\mu_a, \mu'_a) = 1$.
4. V_a is a direct sum of dimension 1 module \mathbf{k}_λ .

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 matrix, then the product $P = \prod (T - d_i)$ 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 Remainder 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 if P cancels a it cancels any restriction of a to a stable subspace. \square

As we will see in chapter 12, diagonalizable endomorphisms is the typical example of semi-simple endomorphisms.

9.4 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 $\overline{\mathbf{A}}$.

Definition 9.4.0.1. 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 χ -type if moreover $\prod P_i = \chi$
2. The companion matrix $C(\chi)$ of χ 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 4.3.2.1 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 4.3.2.1)

$$C(\underline{P}) \equiv \text{diag}(P_1, \dots, P_n)$$

We rewrite the similarity invariant theorem 9.2.2.1 as follows.

Corollary 9.4.0.2 (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) 9.4.0.3 (Frobenius decomposition).

- Using 6.2.3.1, 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 (14.5.2.2).
- The reader will deduce easily (*) from 9.2.2.1 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 6.2.3.1, we get the more or less classical result in the case of a unique companion block $C(P)$

Corollary 9.4.0.4. *Let $a \in \text{End}_{\mathbf{k}}(V)$. The following statements are equivalent⁴:*

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 $(1, \dots, 1, \chi)$.*
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 $\chi_a = \chi$.*

9.5 Applications

9.5.1 Stable subspaces

We know that the stable subspaces by $a \in \text{End}_{\mathbf{k}}(V)$ are its submodules (5.2.4). Therefore if V_a is cyclic they are also cyclic because $\mathbf{k}[T]$ is a PID (6.2.3.1) 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 χ . In particular, they are finite in number. Remarkably, the converse is essentially true.

Proposition 9.5.1.1. *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, their union is not the entire V . Indeed, in the opposite case, their union would be the entire V . Let us then choose for each of these strict subspaces W a non-zero linear form that vanishes on W . The product of these forms is a polynomial function which is identically zero. Since \mathbf{k} is infinite, the ring of polynomial functions on $V = \mathbf{k}^n$ is isomorphic to the ring of polynomials in n variables, a ring that is integral. Thus, one of the forms that is a factor of the product would be identically zero, a contradiction. \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.

⁴This also equivalent for infinite fields that V has a finite number of subspaces stable by a (9.5.1.2).

Remark(s) 9.5.1.2. 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 $P \in \mathbf{Q}[X]$ is irreducible of degree n (take for example $P(X) = X^n - 2$), then the multiplication endomorphism by X on $\mathbf{Q}[X]/(P)$ 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 12 for more results about stable subspaces about the existence of stable complements.

9.5.2 Commutant

It is then easy to study the commutant (see 5.2.4.1)

$$\text{End}_{\mathbf{k}[\mathbf{T}]}(V_a) \simeq \text{End}_{\mathbf{k}[\mathbf{T}]}(\oplus \mathbf{k}[\mathbf{T}]/(P_i)).$$

for example, to calculate its dimension.

Proposition 9.5.2.1. *The dimension of the commutant of a is $\sum (2i - 1) \deg(P_i)$. In particular, $\dim \text{End}_{\mathbf{k}[\mathbf{T}]}(V_a) \geq n$ with equality if and only if a is cyclic.*

Proof. We have

$$\text{End}_{\mathbf{k}[\mathbf{T}]}(\oplus \mathbf{k}[\mathbf{T}]/(P_i)) = \oplus_{i,j} \text{Hom}_{\mathbf{k}[\mathbf{T}]}(\mathbf{k}[\mathbf{T}]/(P_i), \mathbf{k}[\mathbf{T}]/(P_j))$$

Since $\mathbf{k}[\mathbf{T}]/(P_i)$ is cyclic generated by the class of 1, an element of

$$\text{Hom}_{\mathbf{k}[\mathbf{T}]}(\mathbf{k}[\mathbf{T}]/(P_i), \mathbf{k}[\mathbf{T}]/(P_j))$$

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 6.2.1.1). If $i \leq j$, we have $P_j | P_i$, and this condition is automatically satisfied so that

$$\text{Hom}_{\mathbf{k}[\mathbf{T}]}(\mathbf{k}[\mathbf{T}]/(P_i), \mathbf{k}[\mathbf{T}]/(P_j)) \simeq \mathbf{k}[\mathbf{T}]/(P_j) \text{ if } i \leq j$$

If $i > j$, we have $P_i | P_j$ so the condition $(*)$ reads $P \equiv 0 \pmod{P_j/P_i}$ so that

$$\text{Hom}_{\mathbf{k}[\mathbf{T}]}(\mathbf{k}[\mathbf{T}]/(P_i), \mathbf{k}[\mathbf{T}]/(P_j)) \simeq P_j/P_i \mathbf{k}[\mathbf{T}]/(P_j) \simeq \mathbf{k}[\mathbf{T}]/(P_i) \text{ if } i > j$$

We therefore have

$$\begin{aligned} \dim_{\mathbf{k}}(\text{End}_{\mathbf{k}[\mathbf{T}]}(V_a)) &= \sum_{i \leq j} \deg(P_j) + \sum_{i > j} \deg(P_i) \\ &= \sum_j j \deg(P_j) + \sum_i (i-1) \deg(P_i) \\ &= \sum (2i-1) \deg(P_i) \end{aligned}$$

Using $n = \sum \deg(P_i)$, we get $\dim \text{End}_{\mathbf{k}[\mathbf{T}]}(V_a) - n = 2 \sum_{i=1}^n (i-1) \deg(P_i) \geq 0$. 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

9.6 Appendice : Algorithm from equivalence to similarity

We know therefore that if $T\text{Id} - A$ and $T\text{Id} - B$ are equivalent, i.e., if there exist $P(T), Q(T)$ polynomial and invertible matrices such that

$$P(T)(T\text{Id} - A) = (T\text{Id} - B)Q(T)^{-1},$$

then there exists $P \in \text{GL}_n(\mathbf{k})$ such that $B = PAP^{-1}$.

Proposition 9.6.0.1 (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 $\mathcal{R}[\mathbf{T}]$ with $\mathcal{R} = M_n(\mathbf{k}[\mathbf{T}])$

$$\begin{aligned} P(T) &= (T\text{Id} - B)P_1(T) + P_0, \\ Q(T)^{-1} &= \tilde{Q}_1(T)(T\text{Id} - A) + \tilde{Q}_0, \end{aligned}$$

with P_0 and \tilde{Q}_0 in $M_n(\mathbf{k})$ (let's stress that \mathcal{R} is not in a commutative ring⁵). We obtain by substituting

$$((T\text{Id} - B)P_1(T) + P_0)(T\text{Id} - A) = (T\text{Id} - B)(\tilde{Q}_1(T)(T\text{Id} - A) + \tilde{Q}_0)$$

or also

$$(T\text{Id} - B)(P_1(T) - \tilde{Q}_1(T))(T\text{Id} - A) = (T\text{Id} - B)\tilde{Q}_0 - P_0(T\text{Id} - A).$$

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 $(T\text{Id} - B)\tilde{Q}_0 = P_0(T\text{Id} - A)$ (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 $\mathcal{R}[\mathbf{T}]$

$$Q(T) = Q_1(T)(T\text{Id} - B) + Q_0$$

⁵See 1.3.1.1

and we write

$$\begin{aligned}
\text{Id} &= Q(T)^{-1}Q(T) \\
&= (\tilde{Q}_1(T)(T\text{Id} - A) + \tilde{Q}_0)Q(T) \\
&= \tilde{Q}_1(T)(T\text{Id} - A)Q(T) + \tilde{Q}_0Q(T) \\
&= \tilde{Q}_1(T)P(T)^{-1}(T\text{Id} - B) + \tilde{Q}_0(Q_1(T)(T\text{Id} - B) + Q_0) \\
&= (\tilde{Q}_1(T)P(T)^{-1} + \tilde{Q}_0Q_1(T))(T\text{Id} - B) + \tilde{Q}_0Q_0.
\end{aligned}$$

Again, as \tilde{Q}_0Q_0 is constant, the factor of $T\text{Id} - B$ is zero and $\tilde{Q}_0Q_0 = \text{Id}$, hence the conclusion. \square

9.7 Summary on Similiraty Invariants

Collating what we have proved, we have the following results which was wanted in 7.1.

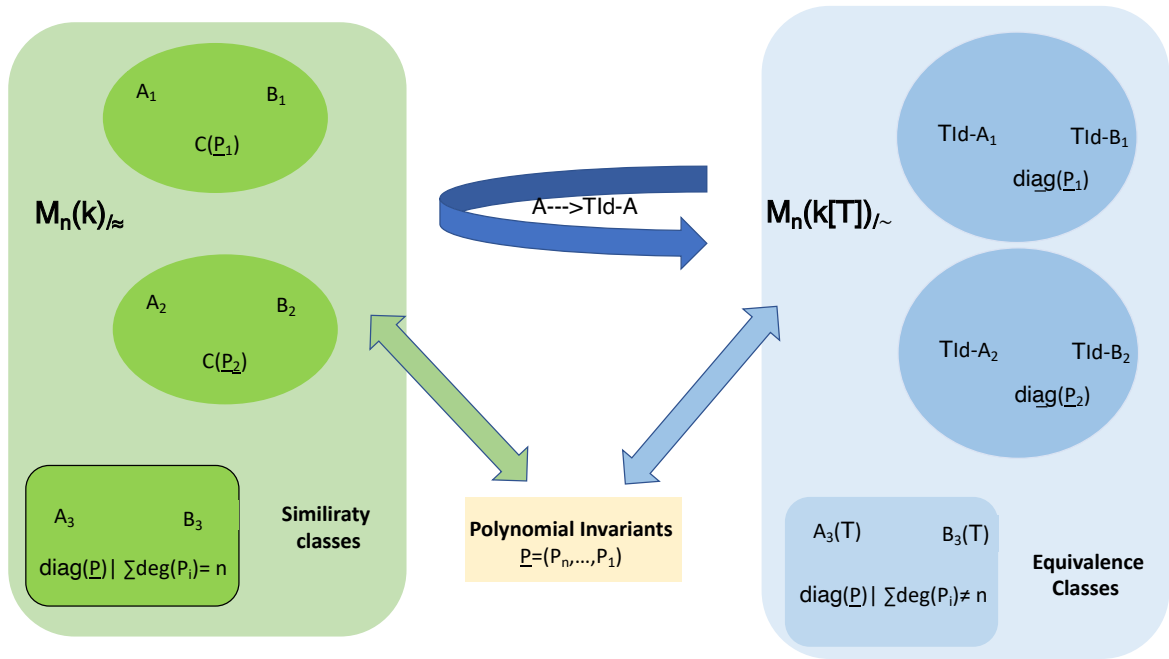
Let $A, B \in M_n(\mathbf{k})$ and $\underline{P} = (P_n | \cdots | P_1)$ a family of monic polynomials.

- 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 $(1, \dots, 1, P)$.

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.



9.8 Exercises

Exercise 9.8.0.1 (difficult). Show that the inclusion $\mathbf{k}[a]$ in his bicommutant, that is the set of endomorphisms that commute with all elements of $\text{End}_{\mathbf{k}[\mathbf{T}]}(V_a)$, is an equality.

Chapter 10

The Irreducible Toolbox



10.1 Introduction



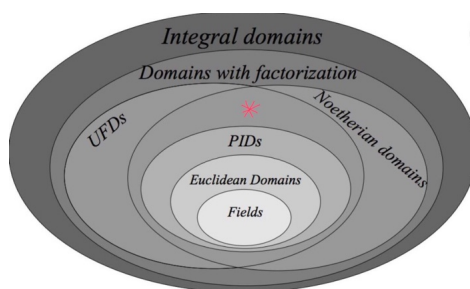
Perspective

Even it is difficult or even 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 computing the eigenvalues of an endomorphism is most often impossible, 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 crucial. We explain the general theory underlying 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(cf. exercice TBD).

10.2 An UFD Criterion

Definition 10.2.0.1. 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, $x \in \mathbf{R}^*$ 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) 10.2.0.2.

- Irreducible elements of \mathbf{Z} are \pm -prime numbers.
- Irreducible polynomials in $\mathbf{k}[T]$ are degree one polynomial for $\mathbf{k} = \mathbf{C}$ and degree one polynomial plus degree two polynomial without real root if $\mathbf{k} = \mathbf{C}$ (*exercise*).

10.2.1 Uniqueness Condition

We know that positive irreducible integers are precisely prime numbers. Generally, we only have one implication

Lemma 10.2.1.1. *Let $x \in \mathbf{R}^*$. If the ideal (x) is prime then x is irreducible.*

Proof. If $x = x_1x_2$, the product x_1x_2 is zero in $\mathbf{R}/(x)$ 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 (integrity), we get $x_2 \in \mathbf{R}^\times$. \square

The converse is the so called Euclid property and is the heart of the uniqueness property of irreducible decomposition.

Definition 10.2.1.2 (Euclid's Property). *We say (by abuse) that \mathbf{R} satisfies Euclid property if the ideal generated by an irreducible element is prime, that is if any irreducible dividing a product divides one of the factors.*

We will use the following proposition at length in the sequel, specially for irreducible polynomials in $\mathbf{k}[T]$.

Proposition 10.2.1.3. *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 $a \not\equiv 0 \pmod{p}$, then 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

Lemma 10.2.1.4. *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, up to R^\times , we 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 (8.2.0.5) and we get $x|x_2$. \square

Definition 10.2.1.5. *Let R be a domain and $x \in R^* - R^\times$.*

1. R is a Unique Factorization Domain (UFD) if

- every nonzero element x has a unique decomposition $x = u \prod_{i=1}^n p_i$ with $u \in R^\times$ and p_i irreducible;
- 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 .

2. $y^2|x \Rightarrow y \in R^\times$.

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 that $v_p(x)$ is the maximal power of p dividing x and that x is square free if $v_p(x) \leq 1$ for all p (exercise).

Lemma 10.2.1.6 (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 $x = x_1x_2$. We decompose each x_i into irreducibles $x_i = u_i \prod_{j=1}^{n_i} p_{i,j}$ giving $x = u_1u_2 \prod_{i,j} p_{i,j}$. Thus, we have two decompositions of x into irreducibles, 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 ℓ 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 $p_{1,1} \mid \prod_{j=1}^{n_2} p_{2,j}$. 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. \square

Corollary 10.2.1.7. *The number of divisors of a nonzero element of an UFD is, up to multiplication by R^\times , finite.*

10.2.2 Existence Criterion

Lemma 10.2.2.1. *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. But x is not irreducible because otherwise $(x) \notin \mathcal{F}$, so x can be written $x_1 x_2$ 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 irreducibles, and so is their product x . A contradiction. \square

We summarize the main preceding results in the following corollary.

Corollary 10.2.2.2.

- *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 (6.2.2.1), we get

Corollary 10.2.2.3. $P \in \mathbf{k}[T]$ 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 10.2.2.1 implies that the existence of decomposition into irreducible elements is very often automatic, but, unfortunately, 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) 10.2.2.4. The ring $\bar{\mathbf{Z}}$ of complex algebraic integers over \mathbf{Z} has no irreducible element and therefore is neither Noetherian nor UFD. We already know that $\bar{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$ therefore $\bar{\mathbf{Z}}$ is not a field (because $1/2 \notin \bar{\mathbf{Z}}$ for instance). If $\bar{\mathbf{Z}}$ were Noetherian or UFD, there would therefore exist at least one irreducible element p 10.2.2.1. But \sqrt{p} is canceled by $T^2 - p$ in $\bar{\mathbf{Z}}[\mathbf{T}]$ and therefore $\sqrt{p} \in \bar{\mathbf{Z}}$ (6.4.2.2). The formula $p = (\sqrt{p})^2$ contradicts the irreducibility of p .

10.3 GCD, LCM in UFD

Let (x_i) be a finite family of non zero elements of an integral domain R . Recall that an element $x \in R^*$ is a GCD of (x_i) if it is maximal among the common divisors to the x_i . Because R is a domain, a GCD of a family, when it exists, is defined up to multiplication by a unit. Considering minimal common multiples, we obtain the notion of LCM. As with integers, we have

Lemma 10.3.0.1. 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 have¹ $\text{GCD}(xx_i) = x \text{GCD}(x_i)$ and $\text{LCM}(xx_i) = x \text{LCM}(x_i)$

Proof. For each ideal generated by an irreducible element, let us chose one generator 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

$$\text{GCD}(x_i) = \prod_{p \in \mathcal{P}} p^{\min_i(v_p(x_i))} \quad \text{and} \quad \text{LCM}(x_i) = \prod_{p \in \mathcal{P}} p^{\max_i(v_p(x_i))}$$

¹Let's 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. The cautious reader will probably prefer to work in the monoid $R^*/R^\times \dots$

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 $(0, x_i)$ allowing to define the GCD for a finite family with at least one non zero element.

10.4 Transfer of the UFD property

We now demonstrate the following UFD transfer theorem to polynomial rings

Theorem 10.4.0.1. *If R is UFD, then $R[T]$ is UFD.*

We must therefore handle both the uniqueness of decompositions (thus Euclid's property) and their existence. For this, we will compare the notion of irreducibles in $R[X]$ and $\mathbf{k}[X]$ (where \mathbf{k} is the fraction field of R) using the notion of content (due to Gauss). We will look carefully at the irreducible decomposition of $P \in R[T]$ in the UFD ring $\mathbf{k}[T]$ by comparing the irreducibility of P in $R[T]$ and $\mathbf{k}[T]$.

Let us recall the equality $(R[T])^\times = R^\times$ which is true for any domain R (just because in this case we have $\deg(PQ) = \deg(P) + \deg(Q)$, see exercise 6.6.0.10 for the general case).

10.4.1 Gauss' content

In the remainder of this chapter section, R denotes an UFD domain.

Definition 10.4.1.1. *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 like the GCD.

Theorem 10.4.1.2 (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 we must demonstrate that PQ is primitive. Otherwise, let p be an irreducible of R dividing $c(PQ)$. Since R is UFD, it satisfies Euclid's lemma and the quotient $\bar{R} = R/(p)$ is integral. The coefficient 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 integral like \bar{R} , for example $\bar{P} = 0$, i.e. $p|c(P)$, a contradiction because $c(P) = 1$. \square

Corollary 10.4.1.3. *The irreducibles of $R[T]$ are*

1. *The irreducibles of R ;*
2. *Primitive polynomials of $R[T]$ that are irreducible in $k[T]$.*

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 $\tilde{P}_1, \tilde{P}_2 \in k[T]$. 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 $P_1/c(P_1) \in R[T]^\times = R^\times$. Therefore, $\deg(P_1/c(P_1)) = \deg(\tilde{P}_1) = 0$ hence the irreducibility of P in $k[T]$.

The converse is tautological (who can do more can do less) □

10.4.2 The Transfer Theorem

We can now prove the transfer theorem 10.4.0.1.

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 R^\times . We know that $R[T]$ is a domain. We just have to prove the existence and uniqueness of decompositions into irreducible elements.

- Existence. Let $P \in R[X]$ be non-zero. If P is a constant $x \in R^*$, we write the decomposition $x = \prod p_i$ into irreducible factors in R and invoke (10.4.1.3). 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 10.4.1.3, a common denominator argument then allows us to write its decomposition in the principal therefore UFD $k[T]$

$$P = \prod P_i/d_i$$

with $P_i \in R[T]$ irreducible in $k[T]$ and $d_i \in R^*$. 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's demonstrate that $R[T]$ satisfies Euclid's lemma (10.2.1.2). Suppose then P irreducible divides the product of $P_1, P_2 \in R[T]$. If P is of degree > 0 , it is primitive and irreducible

in $\mathbf{k}[T]$ according to (10.4.1.3). As $\mathbf{k}[T]$ is UFD since principal, $P|P_1$ for example (in $\mathbf{k}[T]$) and a common denominator argument allows once more to write $dP_1 = Q_1 \cdot P$ with $d \in R^*$, $Q_1 \in R[T]$. 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 $R[T]$.

□

For example, a polynomial ring in n variables over a field, a principal ring more generally, is UFD. But beware, this remarkable stability of factoriality does not pass to quotients as does the property of being Noetherian. The knowledgeable reader will relate this to the notion of non-singularity in geometry.

10.5 Irreducibility of the Cyclotomic Polynomial Over \mathbf{Q}

From now on, in the rest of this chapter, $k = \mathbf{Q}$ and $\Omega = \mathbf{C}$.

We can take here $\zeta_n = \exp\left(\frac{2\text{Id}\pi}{n}\right)$ so that the primitive n -th roots of unity (in \mathbf{C}) are the complex numbers of the form $\zeta_n^m = \exp\left(\frac{2\text{Id}\pi m}{n}\right)$, where $m \in (\mathbf{Z}/n\mathbf{Z})^*$.

Definition 10.5.0.1. We define the n -th cyclotomic polynomial

$$\Phi_n(T) = \prod_{m \in (\mathbf{Z}/n\mathbf{Z})^*} \left(T - \exp\left(\frac{2\text{Id}\pi m}{n}\right) \right).$$

We will show that Φ_n is irreducible and has integer coefficients.

Lemma 10.5.0.2. 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 ζ 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 parameterized 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 Φ_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 coefficient polynomial is an integer coefficient polynomial (1.3.1.1) to conclude this is also true for $d = n$.

□

But we have in our case the transfert theorem

Lemma 10.5.0.3 (Gauss). *Let $P \in \mathbf{Z}[T]$ be a non-constant 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.*

Proof. It is just an immediate consequence of (10.4.0.1) with $R = \mathbf{Z}$. □

Recall that complex number is said to be an *algebraic integer* if it is the root of a monic polynomial with integral coefficients. For example, ζ_n is an algebraic integer, but $1/2$ is not (cf. Exercise 10.5.0.4).

The consistency of the terminology is ensured by the following result.

Exercise 10.5.0.4. *Show that $x \in \mathbf{Q}$ is an integer over \mathbf{Z} if and only if it is in \mathbf{Z} .*

Gauss's Lemma 10.5.0.3 for polynomials immediately gives the following result.

Corollary 10.5.0.5. *The minimal polynomial of an algebraic integer has integral coefficients.*

Then:

Theorem 10.5.0.6. *The cyclotomic polynomial Φ_n is irreducible over \mathbf{Q} .*

The proof, due to Gauss, is very clever.

Proof. Let P be the minimal polynomial of ζ_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 ζ be a root of P . Then ζ is necessarily a primitive root because $P | \Phi_n$. The key is the following lemma.

Lemma 10.5.0.7. *ζ^p is a root of P .*

Proof. Suppose, by contradiction, the opposite. Write

$$T^n - 1 = P(T)S(T)$$

with $S(T) \in \mathbf{Q}[T]$. Since ζ_n is an integer, we have $P(T) \in \mathbf{Z}[T]$ according to Corollary 10.5.0.5. $P(T)$ being moreover monic, $S(T) \in \mathbf{Z}[T]$. Since $P(\zeta^p)$ is assumed to be non-zero, 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 Π 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. \square

We can now finish the proof of Theorem 10.5.0.6.

Let then ζ be a root of P and ζ' be any root of Φ_n . We write $\zeta' = \zeta^m$ with $\text{GCD}(m, n) = 1$ (because ζ' is primitive). By decomposing m into a product of prime factors, a repeated application of the lemma gives that ζ' is a root of P and therefore $\Phi_n | P$. \square

10.6 Exercises

Exercise 10.6.0.1. Prove that if x, x' are nonzero elements of a UFD R and if p is irreducible

$$v_p(rr') = v_p(x) + v_p(x') \text{ and } v_p(x + x') \geq \min(v_p(x) + v_p(x'))$$

Exercise 10.6.0.2. Show that if R is principal, the $\text{GCD}(x_i)$ is a generator of the ideal generated by the (x_i) . Provide a characterization of the LCM in terms of ideals.

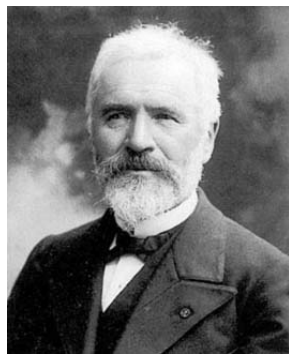
Exercise 10.6.0.3. Let $R = \mathbf{Z}[2i] = \{a + 2bi \mid a, b \in \mathbf{Z}\} \subset \mathbf{C}$ and $P_1 = 2iT + 2$, $P_2 = -2iT + 2$. For $P \in R[T]$, we define its content ideal $c(P) \subset R$ as the ideal generated by its coefficients². Show that $c(P_1P_2) \neq c(P_1)c(P_2)$. Deduce that R is not UFD.

Exercise 10.6.0.4. Show that the ring $\mathbf{R}[X, Y]/(X^2 - Y^3)$ is an integral Noetherian domain but not UFD.

²This example is due to Kaplanski

Chapter 11

Primary decomposition in PID



Camille Jordan

11.1 Introduction



Perspective

We will explain how to decompose torsion modules over PID using its IFD property and the Chinese Remainder Lemma. We will illustrate this result to get the Jordan reduction theorem of $a \in \text{End}_{\mathbf{k}}(V)$ from the Frobenius reduction of V_a immediately leads to the Jordan reduction of endomorphisms under the assumption that the characteristic polynomial χ_a is split.

11.2 Torsion Modules over PID

Let M be a torsion module ($M = M_{tors}$) over a PID R and let \mathcal{P} be the set of nonzero prime ideals of R .



11.2.1 Primary Decomposition

Definition 11.2.1.1. Let $(p) = \mathfrak{p} \in \mathcal{P}$. The \mathfrak{p} -primary part (or p -primary part) of M is the submodule $M[\mathfrak{p}] = M[p] = \{x \in M \mid \exists n \geq 0\} p^n x = 0\}$.

Observe that the primary components are functorial in the following sense. For any $\mathfrak{p} \in \mathcal{P}$, 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 (6.5.0.1) applies to give the following important result.

Proposition 11.2.1.2. Let M be a torsion module and $x = \prod p_i^{v_i}$ be an irredundant¹ prime decomposition of $x \in R^*$.

1. For all j , there exists $\varepsilon_j \in (\prod_{i \neq j} p_i^{v_i})$ such that $\sum_j \varepsilon_j = 1$.
2. If $xM = \{0\}$, the natural map $\bigoplus_{\mathfrak{p} \in \mathcal{P}} M[\mathfrak{p}] \rightarrow M$ is an isomorphism of inverse $m \mapsto \sum \varepsilon_i m$. In particular, the scalar multiplication by ε_i is the projection $\pi_i : M \xrightarrow{\sim} \bigoplus_i M[p_i] \rightarrow M[p_i] \hookrightarrow M$ and $\sum \pi_i = \text{Id}_M$ and $\pi_i \circ \pi_j = \delta_{i,j} p_i$.
3. If M is only torsion, the natural map $\bigoplus_{\mathfrak{p} \in \mathcal{P}} M[\mathfrak{p}] \rightarrow M$ is still an isomorphism.

Proof.

- We just have to check that the Chinese remainder lemma applies for $I_j = (p_j^{v_j})$, that is $I_i + I_j = R$ for $i \neq j$. But in an PID (or more generally in a UFD), we have $\text{GCD}(x, y) = 1 \Rightarrow \text{GCD}(x^n, y^m) = 1$ for any n, m . For instance, in our PID situation, write a Bézout relation $ax + by = 1$ and raise to the $n + m$ -power using the Newton's formula to obtain a Bézout relation $Ax^n + By^m = 1$. This shows that if $i \neq j$, we have $I_i + I_j = R$ and (1)+(2) are just (5) of the Chinese lemma.

¹i.e. $(p_i) \neq (p_j)$ if $i \neq j$ or equivalently $v_i = v_{p_i}(x)$ for all i .

- Because $M = \cup_{x \in R^*} \text{Ann}_M(x)$, we have $M[\mathfrak{p}] = \cup_{x \in R^*} \text{Ann}_M(x)$. Applying (1) and (2) to each $\text{Ann}_M(x)$, the functoriality of primary components gives (3).

□

Example(s) 11.2.1.3. Let $a \in \text{End}_k[V]$.

- Let $P, Q \in k[T]$ coprime polynomials. Applying 11.2.1.2 to V_a , we get the famous "kernel lemma" $\text{Ker}(PQ(f)) = \text{Ker}(P(a)) \oplus \text{Ker}(Q(a))$.
- If $\mu_a(T) = \prod_{\lambda \in \text{Spec}(a)} (T - \lambda)^{v_\lambda}$ is splits, we have $\mu_a(T)V_a = \{0\}$ and

$$V_a[T - \lambda] = \oplus_{\lambda \in \text{Spec}(a)} \text{Ker}(a - \lambda \text{Id})^{v_\lambda}$$

which is the also famous "characteristic spaces decomposition²"

11.2.2 Invariant ideals and primary decomposition

Assume that

$$M \xrightarrow{\sim} R/(d_i)$$

is of finite type and torsion. Its invariant ideals $(d_1) \subset \dots \subset (d_n)$ are proper and non zero (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 the Chinese Remainder Lemma, we get

$$M[p_j] \xrightarrow{\sim} \oplus_i R/(p_j^{d_{i,j}}).$$

Conversely, assume that we have some direct sum decomposition

$$M \xrightarrow{\sim} \oplus_{i,j} R/(p_j^{d_{i,j}}).$$

Reordering if necessary, we can assume that each sequence $(d_{i,j})_{i \geq 1}$ is decreasing with $d_{i,j} = 0$ for i large enough. Then, we define

$$d_i = \prod_j p_j^{d_{i,j}}.$$

The sequence of ideals (d_i) is decreasing and its proper terms are the invariant ideals of M .

²These terminologies are only French Universal.

Graphically, for each prime (p_j) , we order powers that appear in descending order ($d_{i+1,j} \leq d_{i,j}$) in the j^{th} column,

$$\begin{array}{l} d_1 \rightarrow p_1^{d_{1,1}} \quad p_2^{d_{1,2}} \quad \cdots \\ d_2 \rightarrow p_1^{d_{2,1}} \quad p_2^{d_{2,2}} \quad \cdots \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \end{array}$$

and read off the invariant factors d_1, d_2 , etc., from the **rows** (starting from the first one).

11.3 Application: Jordan Reduction

We retain the previous notations (and remind that a matrix of size ≤ 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 χ_A , or equivalently³ μ_A , splits over \mathbf{k} and denote by Λ 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 11.3.0.1. A partition of an integer $n \geq 0$ is a decreasing sequence $\underline{d} = (d_i)_{1 \leq i \leq n}$ of integers ≥ 0 such that $\sum d_i = n$.

Since each P_i divides χ_A , we have

$$(i) \quad P_i = \prod_{\lambda \in \Lambda} (T - \lambda)^{d_{\lambda,i}} \text{ where } \underline{d}_\lambda = (d_{\lambda,i})_i \text{ is a partition of } d_\lambda.$$

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 $\text{Mat}_{\mathcal{B}_{\lambda,i}}(T)$ theof multiplication by T on $\mathbf{k}[T]/((T - \lambda)^{d_{\lambda,i}})$ is $\lambda + J_{d_{\lambda,i}}$ where

$$J_m = C(T^m)$$

³see 9.2.2.2

the standard Jordan block

$$J_m = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

is the standard Jordan block of size m . Using 11.2.2, we get

Theorem 11.3.0.2 (Jordan Reduction). *Under the above assumptions and notations above, we have with*

$$\chi_A(T) = \prod_{\lambda} (T - \lambda)^{d_{\lambda}}$$

1. A is similar to a unique diagonal matrix $\text{diag}(\lambda + J_{d_{i,\lambda}})$ with for every λ the sequence $(d_{i,\lambda})_i$ being a partition of d_{λ} .
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 $T^{d_n}, T^{d_{n-1}}, \dots, T^{d_1}$.

11.3.1 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

$$(T - \lambda), \quad (T - \lambda)^2, \quad (T - \lambda)^2(T - \mu).$$

(2) If $M = \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$, we have

$$T\mathbf{I} - M = \begin{pmatrix} T & -4 & -2 \\ 1 & T+4 & 1 \\ 0 & 0 & T+2 \end{pmatrix}.$$

Let's perform elementary operations according to the algorithm - or rather its outline - described in the proof of the proposition 8.3.1.2 :

$$\begin{aligned} & \begin{pmatrix} T & -4 & -2 \\ 1 & T+4 & 1 \\ 0 & 0 & T+2 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} 1 & T+4 & 1 \\ T & -4 & -2 \\ 0 & 0 & T+2 \end{pmatrix} \\ & \xrightarrow{L_2 \rightarrow L_2 - TL_1} \begin{pmatrix} 1 & T+4 & 1 \\ 0 & -4 - T(T+4) & -2 - T \\ 0 & 0 & T+2 \end{pmatrix} \xrightarrow{\begin{matrix} C_2 \rightarrow C_2 - (T+4)C_1 \\ C_3 \rightarrow C_3 - C_1 \end{matrix}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & (T+2)^2 & -2 - T \\ 0 & 0 & T+2 \end{pmatrix} \\ & \xrightarrow{L_2 \rightarrow L_2 + L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & (T+2)^2 & 0 \\ 0 & 0 & T+2 \end{pmatrix} \xrightarrow{\begin{matrix} C_1 \leftrightarrow C_2 \\ L_1 \leftrightarrow L_2 \end{matrix}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & T+2 & 0 \\ 0 & 0 & (T+2)^2 \end{pmatrix}. \end{aligned}$$

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 $T\mathbf{I} - M$ 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.

11.4 Exercises

Exercise 11.4.0.1. 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 11.4.0.2. 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 (13.2.0.2) below).

Chapter 12

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 weaving./ 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.

12.1 Introduction



Perspective

Following Descartes philosophy, we look at stable subspaces of endomorphisms trying to simplify them into more simple peaces. The best situation is the diagonalizable situation, or more generally the semisimple situation as we will explain.

12.2 Semi-simple Modules

Definition 12.2.0.1. Let \mathcal{M} be the set of maximal ideals of R and $(\mu) \in \mathcal{M}$. Let M be an R -module.

1. We define $M(\mu) = \{m \in M \mid (\mu)m = \{0\}\}$ and $\mathbf{k}(\mu) = R/(\mu)$ (which is a field by definition).
2. M is said
 - semi-simple if every submodule of M has a complement;



Ryoan-ji, Kyoto

- simple if M non-zero and has no non-trivial submodules.

3. An endomorphism $a \in \text{End}_{\mathbf{k}}(V)$ is semi-simple if the $\mathbf{k}[T]$ -module V_a is.

In this commutative situation, the theory is very... simple.

Let us observe that, (μ) canceling $M(\mu)$, the R -module structure on M defines a canonical $\mathbf{k}(\mu)$ -vector space structure on $M(\mu)$. The key lemma is the following.

Lemma 12.2.0.2. *Let M be a semi-simple 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 semi-simple.

Proof.

1. Clear.
2. Enough to prove that M/N is semi-simple 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) 12.2.0.3. *Simple modules are certainly semi-simple as all modules if R is a field. On the other hand, if p is irreducible in a UFD say, $R/(p^2)$ is certainly not semi-simple: if $pR/(p^2) \cong R/(p)$ had a complement S , we would have $R/(p^2) \cong R/(p) \oplus S \cong R/(p) \cong R/(p)$. In particular, $R/(p^2)$ would be canceled by p , which is not the case.*

Proposition 12.2.0.4. *Let M be an R -module.*

1. M is semi simple if and only if the natural morphism $\bigoplus_{(\mu) \in \mathcal{M}} M(\mu) \rightarrow M$ is an isomorphism.
2. A direct sum of semi-simple modules is semi-simple.
3. Up to isomorphism, $\{\mathbf{k}(\mu), (\mu) \in \mathcal{M}\}$ is the set of all simple modules.
4. A semi-simple module is a direct sum of simple modules.

Proof.

1. Let us observe that $\bigoplus M(\mu) \rightarrow M$ is always injective. Let $(m_\mu \in M(\mu))_{\mu \in F}$ a finite family such that $\sum_F m_\mu = 0$ (*). Let $e_\mu \in R/I$ be the complete family the Chinese Remainder Lemma where $I = \prod_{\mu \in F} (\mu)$. The action of R on $\bigoplus_{\mu \in F} M(\mu)$ factors through R/I and we have $e_\mu m_\nu = \delta_{\mu\nu} m_\mu$. Multiplying (*) by each e_μ we get $m_\mu = 0$ for all $\mu \in F$ hence the injectivity.

Assume M is semi-simple. Let S be a complement of (the image of) $\bigoplus M(\mu)$ in M . If $S \neq \{0\}$, let s nonzero in S and $\mu \in \mathcal{M}$ containing $I = \text{Ann}_R(s)$ (Krull's lemma 1.3.2.4). Then Rs is semi-simple (12.2.0.2) and isomorphic to R/I which is also semi-simple (12.2.0.2 again). But $\mathbf{k}(\mu) = R/(\mu)$ is a quotient of $R/I = Rs$ and therefore isomorphic a submodule of $Rs \subset S$. But the image of 1 in S is cancelled by (μ) and therefore belongs to $M(\mu)$, a contradiction.

Conversely, assume $\iota : \bigoplus_{(\mu) \in \mathcal{M}} M(\mu) \rightarrow M$ is surjective and let N be a submodule of M . The injection $N(\mu) \rightarrow \bigoplus N$ is surjective because ι is. Let S_μ be a complement of the $N(\mu)$ in $M(\mu)$ as $\mathbf{k}(\mu)$ -vector spaces. Then $S = \bigoplus S_\mu$ is complement of N in M .

2. (2), (3) and (4) follow immediately from (1).

□

Remark(s) 12.2.0.5.

- It follows that every semi-simple module is a torsion module except R is a field.
- If R is a field any module is semi-simple : 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 12.2.0.2. 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).
- If R is a PID, Krull's lemma is elementary once we know that R is an UFD and that nonzero prime ideals are maximal.

Corollary 12.2.0.6. *Let $a \in \text{End}_{\mathbf{k}}(V)$ with V of finite dimension. The following conditions are equivalent.*

- a is semi-simple.
- μ_a is square free in $\mathbf{k}[T]$.
- $\mathbf{k}[a]$ is a (finite) product of fields containing \mathbf{k} .
- $\mathbf{k}[a]$ is reduced¹

Proof.

- (1) \Rightarrow (2). If $P_1 = \mu_a$ is divisible by a square P^2 of some irreducible polynomial P , the quotient $\mathbf{k}[T]/(P^2)$ of V_a is not semi-simple (12.2.0.3) and therefore V_a neither.
- (2) \Rightarrow (3). Because $\mathbf{k}[a] \xrightarrow{\sim} \mathbf{k}[T]/(\mu_a)$, 12.2.0.3 gives the result.
- (3) \Rightarrow (4). A product of fields has no nilpotent elements.
- (4) \Rightarrow (1). If $\mathbf{k}[a] \xrightarrow{\sim} \mathbf{k}[T]/(\mu_a)$ is reduced, then μ_a is square free (if μ_a is divisible by P^2 , then the square of the non zero element $\mu_a/P \pmod{(\mu_a)}$ is zero). Therefore, all similarity invariants P_i are square free because they divide μ_a implying that $\mathbf{k}[T]/(P_i)$ is a product of fields (12.2.0.3), and so is $V_a \xrightarrow{\sim} \oplus \mathbf{k}[T]/(P_i)$ which is therefore semi-simple by 12.2.0.4.

□

Example(s) 12.2.0.7. *If χ_a is split, semi-simple 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 semi-simple. The converse being true for characteristic zero or more generally for fields (12.3.0.2). Semi-simple endomorphisms is the appropriate generalization in the nonsplit case. We will discuss in full details this topic and more generally the diagonalizable endomorphisms in the next chapter.*

12.3 «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 field of fractions of the polynomial ring $\mathbf{F}_2[t]$ [t is assumed to be transcendental over \mathbf{F}_2]. This does not occur in perfect fields. Let p be a

¹A ring is reduced if 0 is the only nilpotent element, i.e. if the only element which has a positive power equal to 0.

prime number and R a ring such that $pR = \{0\}$. The well-known divisibility $p \mid \binom{p}{n}$ for $1 \leq n \leq p-1$ and the binomial formula ensure that the application $F : r \mapsto r^p$ is a ring morphism called the Frobenius morphism. If R is a field, it is additionally injective as any morphism of fields.

Definition 12.3.0.1. *A field of characteristic p is said to be perfect if $p = 0$ or if every element admits a p -th root, i.e. if its Frobenius morphism is an isomorphism.*

Thus, every finite field is perfect since an injection between finite sets is bijective. Therefore, we must prove the following statement.

Lemma 12.3.0.2. *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 \mathbf{k} is perfect and P irreducible, then $\text{GCD}(P, P') = 1$.*
- *If K is a field containing \mathbf{k} , then $A \in M_n(K)$ is semi-simple if and only if it is semi-simple in $M_n(\mathbf{k})$.*

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 $P_i \mid P'_i$. 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 $P_i = (\sum_n a_{np}^{1/p} T^n)^p$ because the Frobenius of $\mathbf{k}[T]$ is a ring morphism. A contradiction with the irreducibility of P_i □

This corollary is false in the imperfect case.

Remark(s) 12.3.0.3. *When the base field K is not perfect, there are semi-simple matrices over K which, considered in a superfield, are no longer so. With the notations of 12.3, 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 $\text{GCD}(\mu_a, \mu'_a) = 1$, stronger than semisimplicity.*

Exercise 12.3.0.4. *Let V be a \mathbf{k} -vector space of finite dimension and φ 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.*

12.3.1 Sums of semi-simple 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 12.3.1.1. *Let $a, b \in \text{End}_{\mathbf{k}}(V)$ which commutes and let $P \in \mathbf{k}[T_1, T_2]$. Assume a is semi-simple and $\text{GCD}(\mu_b, \mu'_b) = 1$ (in the perfect case, this is equivalent to a, b semi-simple by 12.3.0.2). Then $P(a, b)$ is semi-simple. In particular $a + b$ is semi-simple.*

Proof. Because $\mathbf{k}[c] \subset \mathbf{k}[a, b] \subset \text{End}_{\mathbf{k}}(V)$, its enough to show that $\mathbf{k}[a, b]$ is reduced. But the \mathbf{k} -algebra surjective morphism $\mathbf{k}[T_1, T_2]$ defines 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 $\mathbf{k}[T_1]$ is a finite product of fields K_i (containing \mathbf{k}) by 12.2.0.6. Because the GCD does not depends on the subfield where it is calculated by Euclide's algorithm, μ_b is also square free in $K_i[T]$ and $R = \prod K_i[T]/(\mu_b(T))$ is therefore a product of fields and so is its quotient $\mathbf{k}[a, b]$ by 12.2.0.3. \square

12.4 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).

12.4.1 Hensel's lemma and existence

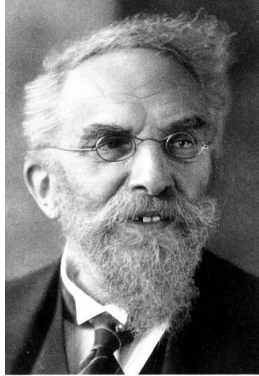
Lemma 12.4.1.1 (Hensel-Newton). *Let I be a nilpotent ideal ($I^N = 0$) of an arbitrary ring R and $P \in R[T]$. Assume there exists $x_0 \in R$ such that $P(x_0) \equiv 0 \pmod{I}$ and $P'(x_0) \pmod{I}$ is invertible. Then, there exists $x \in R$ such that $x \equiv x_0 \pmod{I}$ and $P(x) = 0$.*

Proof. First, observe that if $a \pmod{I}$ is invertible, then a is invertible in a . 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

$$x_k \pmod{I^{2^k}} | P(x_k) \equiv 0 \pmod{I^{2^k}} \text{ and } x_k \equiv x_0 \pmod{I}$$

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 $x_{k+1} = x_k + \varepsilon$, $\varepsilon \in I^{2^k}$ so that x_{k+1} is indeed an approximation of $x_k \pmod{I^{2^k}}$.



Kurt Hensel

Kurt Hensel



Isaac Newton

The entire Taylor formula 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 $P'(x_k) \pmod{I^{2^k}}$ is invertible. We then set $\varepsilon = -P(x_k)/P'(x_k)$. $\varepsilon \in I^{2^k}$ is guaranteed by the construction of x_k . As $\varepsilon^2 \in I^{2^{k+1}}$, this choice is suitable. To conclude, we choose k such that $2^k \geq N + 1$ and set $x = x_k$: the algorithm converges exponentially! \square

Corollary 12.4.1.2 (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 semi-simple, ν nilpotent. In particular, d and ν commute.*

Proof. Let $\pi \in \mathbf{k}[T]$ be the product of the irreducible factors of the minimal μ_a of a . As it is without squared factors, it is coprime with its derivative. Choose $\alpha, \beta \in \mathbf{k}[T]$ such that $\alpha\pi + \beta\pi' = 1$.

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 absolutely semi-simple. Since $\nu = a - P(a) \in I$ and $I^n = 0$, ν is nilpotent. \blacksquare \square

Remark(s) 12.4.1.3. *This is essentially Chevalley's proof. Beyond its algorithmic character (very fast), it is important because it allows the definition of semi-simple and nilpotent parts within the context of Lie algebras and algebraic groups (on a perfect field), see for example the excellent [4].*

12.4.2 Uniqueness

Theorem 12.4.2.1 (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, ν) with d semi-simple, ν nilpotent, d and ν 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, ν as in the theorem and a pair $d', \nu' \in \mathbf{k}[a]$ as in Corollary 12.4.1.2. Since d, ν commute with each other, they commute with $d + \nu = a$. They therefore also commute with d', ν' 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 $d - d'$ semi-simple (as a sum of commuting semi-simples, 12.3.1.1); an endomorphism that is both semi-simple and nilpotent being zero since its minimal polynomial has no squared factors and divides T^n , we indeed have $d = d'$ and $\nu = \nu'$. \square

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 12.3.0.3 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 semi-simple with absolutely semi-simple. The proof is then identical.

12.4.3 Similarity class of the components

We retain the previous notation. $a = d + \nu$. The invariant factors of the semi-simple part d are entirely determined by χ_a since two diagonalizable endomorphisms with the same characteristic polynomials are similar over Ω and the invariants do not depend on the base field (cf. 12.4.4.1). Similarly, the similarity invariants of a determine the nilpotent type \underline{d}_a of ν . 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.

12.4.4 Appendix: What about the algorithmic nature of the decomposition?

On re-examining the proofs *supra*, one easily convinces oneself that finding d and ν is algorithmic once one knows the product π of the distinct 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 that 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 null derivative: the polynomials in T^p . The following exercise provides an «algorithm» to find π for a perfect field of characteristic $p > 0$. The quotes are justified by the assumption that the inverse of the Frobenius² $F : x \mapsto x^p$ of \mathbf{k} is known algorithmically.

Exercise 12.4.4.1. *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 χ_{red} .
5. What is χ_{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 semi-simple endomorphisms with characteristic polynomial χ .
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 .

Regarding Hensel's lemma, the very writing of the proof is an algorithm that lives in $\mathbf{k}[a] \subset M_d(\mathbf{k})$ where $d = \dim(V)$. It involves calculating 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 lighten it is to consider the

²Which is the case, for example, for finite fields.

algebra isomorphism $k[T]/\mu_a \xrightarrow{\sim} k[a]$ that sends T to a (**exercise**) and to work within this quotient, which is less computationally demanding.

Despite this, 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 14.2.0.3). Therefore, approximating the values of the coefficients becomes perilous. When 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. Even though 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 14.

12.4.5 d -th roots in GL_n

If $A \in M_n(\mathbf{k})$ with $\chi_A(T) = \prod (X - \lambda)^{v_\lambda}$ split, we thus find the usual definition encountered in linear algebra. If $\text{pr}_\lambda = e_\lambda(A)$ is as above, the spectral projector on $V[T - \lambda] = \text{Ker}(A - \lambda)^{v_\lambda(x)}$, the Jordan-Chevalley decomposition $A = D + N$ is simply calculated by

$$d = \sum \lambda e_\lambda(A) \text{ and } N = A - D$$

as we have just seen. An immediate and useful application is the existence of polynomial d -th roots in the algebraically closed case.

Proposition 12.4.5.1. *Let d be an integer > 0 and assume \mathbf{k} is algebraically closed with characteristic prime to d . Let χ be unitary of degree n . There exists $P_{d,\chi} \in \mathbf{k}[T]$ such that for any matrix $A \in GL_n(\mathbf{k})$ with $\chi_A = \chi$ we have $P_{d,\chi}(A)^d = A$.*

Proof. Since $\chi(0) \neq 0$, the polynomials χ 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 χ 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 χ and d evaluated in A as are D^{-1} and N , which is what we wanted. \square

We cannot hope for better. On 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. Indeed, it would be nilpotent so that its n -th power would be zero but also equal to $n!$

12.5 Exercises

Exercise 12.5.0.1. Let λ be an eigenvalue of a and d_λ its multiplicity as root of χ_a . Prove $\dim(a - \lambda \text{Id}) \leq d_\lambda$ (*). Prove that a is diagonalizable if and only if χ_a splits over \mathbf{k} with equality in (*) for all eigenvalues.

Exercise 12.5.0.2. 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 $\exp(M)_{\text{nil}}$ in terms of M_{nil} and M .
2. Show that $\exp(M)_{\text{nil}} = 0$ if and only if $M_{\text{nil}} = 0$. 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 $M \mapsto M_{\text{nil}}$ is not continuous on $M_n(\mathbf{C})$.
5. What is the set of points of continuity of the map $M \mapsto M_{\text{nil}}$ (Difficult)?

Exercise 12.5.0.3. 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 12.5.0.4. Let p be prime, K the field of fractions 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 semi-simple, commute but their difference is nilpotent (this is exercise 14 chapter VII.5 [6] rewritten without tensor product).

Exercise 12.5.0.5. 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 6.5.0.2 that if the minimal of A, B and their respective derivatives are coprime, any element C of $\mathbf{k}[A, B]$ is semi-simple (without using 12.3.1.1). Is μ_C necessary coprime with its derivative?

Exercise 12.5.0.6. Let d be the semi-simple part of a in its Chevalley-Jordan decomposition. Prove $\chi_a = \chi_d$.

Exercise 12.5.0.7. 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 ?

Chapter 13

Simultaneous reduction

FURTHER REDUCTION

13.1 Introduction



Perspective

This chapter give criteria to simultaneous reduce matrices in simpler form (diagonal, triangular). These are fundamental tools to understand the general linear group $GL_n(\mathbf{k})$.

We will use the important notion of irreducible action.

Definition 13.1.0.1. 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 irreducibly¹.

The reason to be interest 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 $a \in \mathcal{A}$

$$\text{Mat}_{\mathcal{B}}(a) = \begin{pmatrix} \text{Mat}(a_W) & * \\ 0 & \text{Mat}(a_{V/W}) \end{pmatrix}$$

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) 13.1.0.2. *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: 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 13.1.0.3. *$\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$ 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 ${}^t\mathcal{A}$ (3.8.0.2). □

13.2 Commuting family of matrices

The main observation is the following.

Lemma 13.2.0.1. *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 13.2.0.2. *Let $\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$ be an arbitrary set of commuting endomorphism.*

1. *If χ_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 trigonalization basis \mathcal{B} for \mathcal{S} .*

Proof.

1. Induction on $\dim(V)$: by the "valuable stable space tool", one can assume \mathcal{S} acts irreducibly. By 13.2.0.1, any eigenspace of a is invariant under \mathcal{S} 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 . For each λ , we then choose a common diagonalization base for the $a_j(\lambda)$ and the union of these bases suits.

□

Remark(s) 13.2.0.3. *These results are of fundamental importance in group theory. This shows that commutative subgroups of $\text{GL}_n(\mathbf{C})$ of diagonalizable matrices are conjugate to subgroups of the groups of invertible diagonal matrices the converse being obviously true (this (2) above (1)). For (1), this shows that commutative subgroups of $\text{GL}_n(\mathbf{C})$ are conjugate to subgroups of the groups of upper triangular matrices the converse being obviously false. The good generalization of abelian groups is the notion of solvable groups. In this case, one can show that connected solvable subgroups of $\text{GL}_n(\mathbf{C})$ are exactly connected subgroups of $\text{GL}_n(\mathbf{C})$ (see 13.5). But the connectedness assumption cannot be dropped (see exercise ??).*

13.3 The Burnside-Wedderburn theorem

This result is important and classical²

Theorem 13.3.0.1. *Let $\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$ acting irreducibly on V . Assume moreover that χ_{α} is split and that \mathcal{A} is stable by product. Then $\mathcal{A} = \{0\}$ or \mathcal{A} generates $\text{End}_{\mathbf{k}}(V)$.*

Proof. We can assume $\mathcal{A} \neq \{0\}$ and, changing \mathcal{A} to $\text{Span}(\mathcal{A})$ that \mathcal{A} is a \mathbf{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 $\alpha(x), \alpha(y)$ are independent. But $\mathcal{A}.\alpha(x)$ is invariant under \mathcal{A} and therefore $\mathcal{A}.\alpha(x) = V$ or $\mathcal{A}.\alpha(x) = \{0\}$. In the first case, we would have $\mathbf{k}.\alpha(x)$ invariant under \mathcal{A} and therefore $\alpha(x) = 0$ because $\mathbf{k}.x = V$ is prohibited by $d > 1$. Thus $\mathcal{A}.\alpha(x) = \{0\}$ and we can choose $a \in \mathcal{A}$ such that $a(\alpha(x)) = y$ implying $\alpha a \alpha(x), \alpha(x)$ independent. If $\lambda \in \mathbf{k}$, we have therefore $\beta = \alpha a \alpha(x) - \lambda \alpha(x) \neq 0$. But $\alpha(V)$ is invariant under αa and we choose an eigenvalue of its restriction to $\alpha(V)$ ($\chi_{\alpha a}$ is split so is the characteristic polynomial of the

²Our 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.

restriction $\alpha a|_{\alpha(V)}$. Therefore, we have

$$0 < \text{rk}((a\alpha a - \lambda\alpha) = \dim(a\alpha - \lambda \text{Id})|_{\alpha(V)} < \dim(\alpha(V)) = d$$

and $a\alpha a - \lambda\alpha \in \mathcal{A}$, a contradiction and therefore $d = 1$.

If $\mathbf{k}x = \text{Im}(\alpha)$, there exists a non zero elements $\varphi \in V^*, x \in V$ such that $\alpha(v) = \varphi(v)x$ for all $v \in V$. By 13.1.0.3, we have ${}^t\mathcal{A}.\varphi = V^*$. 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 $\Psi \in V^*, y \in V$ and hence the theorem because it is a generating family of $\text{End}_{\mathbf{k}}(V)$ [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]. \square

13.4 Stable family of nilpotent and unipotent matrices

Theorem 13.4.0.1 (Kolchin). *Let $\varepsilon \in \{0, 1\}$. Assume³ $\mathcal{A} \subset \text{End}_{\mathbf{k}}(V)$ 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

$$(*) \quad \bigcap_{a \in \mathcal{A}} \text{Ker}(a - \text{Id}) \neq \{0\}$$

Let Ω be an algebraically closed field containing \mathbf{k} . Choosing an arbitrary basis, (*) is equivalent to the existence of a non zero solution of the linear systems with \mathbf{k} -coefficients $\text{Mat}_{\mathcal{B}}(a)X = 0$ in n the n unknown $X = (x_i)$ (n equations for each a). But (*) has a solution if and only if it has a solution in Ω (by a dimension argument, one can assume that the equations are in finite number and we know that the ranks of a matrix in \mathbf{k} computed in \mathbf{k} or Ω are the same). In other words, we can assume $\mathbf{k} = \Omega$, *i.e.* we can assume that \mathbf{k} is algebraically closed.

Using the "valuable stable space tool" again, we can assume that \mathcal{A} acts irreducibly on V .

If $\mathcal{A} = \{0\}$ ($\varepsilon = 0$ case), we are done. If not, we have $\varepsilon = 1$ and \mathcal{A} generates $\text{End}_{\mathbf{k}}(V)$ by 13.3.0.1 (because \mathbf{k} is now assumed algebraically closed). But $\text{tr}(a) = n = \text{tr}(ab)$ for any $a, b \in \mathcal{A}$. Therefore, $\text{tr}(a(\text{Id} - b)) = 0$ for any $a \in \mathcal{A}$ and therefore for 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. \square

A subgroup of $\text{GL}_n(\mathbf{k})$ whose elements g satisfy $\text{Spec}(g) = \{1\}$ is called unipotent.

³See 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.

Corollary 13.4.0.2. *Every unipotent subgroup of $GL_n(\mathbf{k})$ is contained in a maximal unipotent subgroup which is conjugate to the group of upper triangular matrices with 1 in the diagonal.*

13.5 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.

13.5.1 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 13.5.1.1. 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) 13.5.1.2. *Any commutative group is solvable. Any sous-group of the group of invertible upper-triangular matrices is solvable (see 13.5.1.4 and 13.6.0.4). The groups S_3 and S_4 are non-commutative and solvable (13.6.0.1).*

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 13.5.1.3. *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 13.5.1.4. *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) 13.5.1.5. *Therefore, the class of solvable groups is the smallest class of subgroups stable by isomorphism and exact sequence. 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.

13.5.2 The Lie-Kolchin theorem

In this section, we assume that \mathbf{k} is a subfield of \mathbf{C} induces a metric topology on $M_n(\mathbf{k})$. The following theorem is both classical and important.

Theorem 13.5.2.1 (Lie-Kolchin). *Let $G \subset GL_n(V)$ be a solvable subgroup such that χ_g is split for every $g \in G$. and assume If G is connected, then 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 Γ is any connected group, then $D(\Gamma)$ is connected. Indeed, the set Γ^i of products of i commutators $[\gamma_1 \gamma_2 \gamma_1^{-1} \gamma_2^{-1}]$ is a continuous (product and inverse are polynomial maps and therefore are continuous) image of the connected set Γ^{2i} and is therefore connected. Then $D(\Gamma)$ is a union of connected set having 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 (13.2.0.2).
- 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(13.2.0.2), 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 eigenvector for H , hg and gh coincides on each such vector. By $(*)$, $g(v)$ is such a vector proving $hg - gh = 0$ on $\text{Span } Gv \stackrel{\text{irreducibility}}{=} V$: g and h commute. An eigenspace of h is nonzero and invariant by G and therefore is equal to V proving that each $h = \lambda(h)\text{Id}$. Because $\ell > 1$, $H \subset DG \subset \text{SL}(V)$ proving that $\lambda(h)$ is a $n = \dim(V)$ root of 1. Therefore H is finite hence $H = \{\text{Id}\}$ because it is connected.

□

Corollary 13.5.2.2. *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.*

13.6 Exercises

Exercise 13.6.0.1.

- 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 13.6.0.2.

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 13.6.0.3. 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 13.6.0.4. 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.

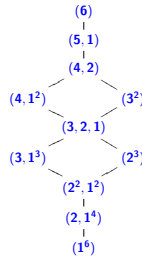
5) Deduce that U is solvable. Conclude.

Part III

About continuity of matrix reduction

Chapter 14

Topology of similarity classes



Hasse Diagram of M_6

14.1 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 $M_n(\mathbf{k})$ with \mathbf{k} any subfield of \mathbf{C} endowed with the metric topology¹ deduced from any norm on $M_n(\mathbf{C})$. We have chosen to keep our module theoretic method in high details even the proofs could be a little bit shorten. The reason is to produce "natural proofs" and, more important, to illustrate the modern notion of deformation/ family of modules.

We will investigate the topology of the set of matrices up to similarity. In other terms, 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 $P.A = PAP^{-1}$. In concrete terms, $f(M) = O(M)$ where $O(M)$ is its conjugation class.

¹As mentioned above, in the case of a general infinite field, the Zariski topology should be considered, which adds no real difficulty once its definition is known (cf. exercice 14.6.0.6). 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 infinitude of the field comes into play in the case of the Zariski topology.

Because the action $GL_n(\mathbf{k}) \times M_n(\mathbf{k}) \rightarrow GL_n(\mathbf{k})$ 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. The reader will verify the following universal property of this topology, natural generalization of the quotient map universal property in our context. Be cautious that even this topology is very natural, it comes not from any metric as we will see in detail. But the reader can convince himself right now of this fact.

Exercise 14.1.0.1. Assume $n \geq 2$. Show that the image of $f(tE_1, 2)$, $t \in \mathbf{k}$ is constant except for $t = 0$. Deduce that $M_n(\mathbf{k})/GL_n(\mathbf{k})$ is not separated.

Exercise 14.1.0.2. 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

$$\text{Hom}_{inv}(M_n(\mathbf{k}), T) = \{\varphi \in \text{Hom}_{cont}(M_n(\mathbf{k}), T) \mid \forall (P, A) \in GL_n(\mathbf{k}) \times M_n(\mathbf{k}), \varphi(P.A) = \varphi(P)\}.$$

In particular, because the characteristic polynomial is invariant by conjugation, the map $A \mapsto \det(T \text{Id} - A)$ defines a continuous (polynomial!) map $\gamma : M_n(\mathbf{k}) \rightarrow \mathbf{k}^n$ which is invariant and by the above universal property defines

$$\mu : M_n(\mathbf{k})/GL_n(\mathbf{k}) \rightarrow \mathbf{k}^n$$

where we identify a monic degree n polynomial with its first n coefficients.

Exercise 14.1.0.3. Let $g : M_n(\mathbf{k}) \rightarrow \mathbf{k}$ be a continuous $GL_n(\mathbf{k})$ -invariant function. Show that there exists a unique continuous function \bar{g} on \mathbf{k}^n such that $g = \bar{g} \circ f$.

Because the image of μ 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 14.5.1.4.

14.2 χ -types

Let $\chi \in \mathbf{k}[T]$ be a degree n monic polynomial and recall (9.4.0.1) that a χ -type is a sequence $\underline{P} = (P_n \mid \cdots \mid P_1)$ of monic polynomials of $\mathbf{k}[T]$ such that $\prod P_i = \chi$.

Definition 14.2.0.1. 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 $\deg(\underline{P}) = n = \sum \deg(P_i)$.

Thus, $O(\underline{P})$ 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 $O(\underline{P})$ as \underline{P} covers all the n -types (9.7). In the perspective of the introduction 14.1, 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 orbits $O(\underline{P})$.

We define a (topological) relation \preceq on χ -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 χ -types for a given χ . The relation \preceq is reflexive and transitive relation on types². 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 (combinatorial³) 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 χ , 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) 14.2.0.2. 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 14.2.0.3. Let $\underline{P}, \underline{Q}$ be two χ -types. Then, $\underline{P} \preceq \underline{Q}$ if and only $\underline{P} \leq \underline{Q}$. In other words, the topological and combinatorial orders on n -types coincide.

²At this stage, the anti-symmetry is not clear (cf. 14.3.0.2).

³Compare with cf. 14.4.2.

Remark(s) 14.2.0.4. *This theorem is a reformulation, more transparent in my opinion, of Theorem 4 from [11]. Indeed, to my knowledge, it was Gerstenhaber who fully elaborated the structure of orbit closures, although I have not been able to find this statement stricto sensu.*

14.3 $\underline{P} \preceq \underline{Q} \Rightarrow \underline{P} \leq \underline{Q}$

This implication follows from the continuity of determinants using the calculation of similarity invariants using minors (9.7).

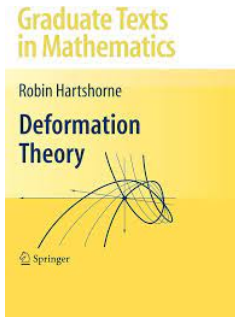
Lemma 14.3.0.1. *Let $\alpha = (\alpha_k)$ be a converging sequence of degree d complex polynomials⁴. Assume that each α_k is a multiple of some monic polynomial $\beta \in \mathbf{k}[T]$. Then, $\beta \mid \lim(\alpha)$.*

⁵Because all norms on $\mathbf{k}_{\leq d}[T]$ are equivalent, we can use any norm to define the convergence notion. Notice that convergence of a sequence of polynomials is equivalent to the convergence of each coefficient sequence.

Proof. Let \mathcal{R} be the \mathbf{k} -subalgebra of the algebra of complex sequences generated by the $d+1$ -sequences of coefficients of α . 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 $\beta \mid \alpha_k$ 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 14.3.0.2. *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 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 $T \text{Id} - A_k$ (9.7). In particular, $\delta_i(\underline{Q})$ divides the determinant of each of these minors $M_{I,J}(A_k)$ which are converging to the corresponding $\det(M_{I,J}(A_\infty))$ of A_∞ by continuity of the determinant. By the lemma above, $\delta_i(\underline{Q}) \mid \delta_i(\underline{P})$. Using $\prod_{j \geq 1} P_j = \prod_{j \geq 1} Q_j$, we get $\prod_{j \leq n-i} P_j \mid \prod_{j \leq n-i} Q_j$, $i = 1, \dots, n$ 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 ε 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 14.4.1.1. 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.

14.4 $\underline{P} \leq \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$

14.4.1 An elementary deformation

Let $R = \mathbf{k}[\tau]$ be the polynomial ring in the variable τ .

Lemma 14.4.1.1. *Let $(P_2, P_1) = \underline{P} \leq \underline{Q} = (Q_2, Q_1)$ two χ -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.

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 φ be the natural composition $\varphi : \mathbf{R}_{<d_2}[\mathbf{T}] \oplus \mathbf{R}_{<d_1}[\mathbf{T}] \rightarrow \mathbf{R}[\mathbf{T}] \oplus \mathbf{R}[\mathbf{T}] \rightarrow \text{Coker}(A(\tau))$ with $d_i = \deg(P_i)$. Let us show that φ is an \mathbf{R} -linear isomorphism.

Surjectivity. Let $(X_2, X_1) \in \mathbf{R}[\mathbf{T}]^2$. We write $X_1 = Y_1 P_1 + R_1$ 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 $(X_2, X_1) \in \mathbf{R}_{<d_2}[\mathbf{T}] \oplus \mathbf{R}_{<d_1}[\mathbf{T}]$ 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 $(Y_2, Y_1) \in \mathbf{R}[\mathbf{T}]^2$. 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 14.4.1.2. $\underline{P} \leq \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$.

Proof. Let \mathcal{B} be the basis $(1, \dots, T^{d_2-1}) \sqcup (1, \dots, T^{d_1-1})$ of $\mathbf{R}_{<d_2}[\mathbf{T}] \oplus \mathbf{R}_{<d_1}[\mathbf{T}] \xrightarrow{\sim} \mathbf{R}^n$ and $H(\tau) = \text{Mat}_{\mathcal{B}}(\varphi^{-1} \circ h_T \circ \varphi) \in M_n(\mathbf{R})$ where h_T is the multiplication by T on $C(\tau)$. By just rephrasing the lemma 14.4.1.1 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 $\mathbf{k}[\mathbf{T}]$ -modules $C(\varepsilon)$, $\varepsilon \in \mathbf{k}$ is the typical example of an (algebraic) *deformation* of our module $C(0)$.

14.4.2 $\underline{\leq} = \underline{\preceq}$

Definition 14.4.2.1. Let $\underline{P}, \underline{Q}$ be χ -types and \mathcal{P} is the (finite) set of irreducible divisors of χ . 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

$$\underline{P} = (\tilde{P}_n, \dots, \pi \tilde{P}_j, \dots, \tilde{P}_i, \dots, \tilde{P}_1), \quad \text{and} \quad \underline{Q} = (\tilde{P}_n, \dots, \tilde{P}_j, \dots, \pi \tilde{P}_i, \dots, \tilde{P}_1)$$

i.e.

$$P_k = Q_k = \tilde{P}_k \text{ if } k \neq i, j \text{ and } P_j = \pi Q_j = \pi \tilde{P}_j, \quad Q_i = \pi P_i = \pi \tilde{P}_i.$$

We write in this case $\underline{P} \preceq_e \underline{Q}$

The definition is justified by

Lemma 14.4.2.2. *With the notation above, $\underline{P} \preceq_e \underline{Q} \Rightarrow \underline{P} \preceq \underline{Q}$.*

Proof. Apply lemma 14.4.1.1 to $(P_i, \pi Q_j) \leq (\pi P_i, Q_j)$. □

The main theorem 14.2.0.3 is now a consequence of the following proposition.

Proposition 14.4.2.3. *Let $\underline{P} \preceq \underline{Q}$ be two distinct χ -types.*

1. *There exists a finite series of elementary deformations $\underline{P} = \underline{R}^0 \underset{e}{\preceq} \underline{R}^1 \underset{e}{\preceq} \dots \underset{e}{\preceq} \underline{R}^{N-1} \underset{e}{\preceq} \underline{R}^N = \underline{Q}$.*
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 χ -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 χ 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 $\mathbf{R} = (R_k)_{1 \leq k \leq n}$ be the family

$$R_k = P_k \text{ if } k \neq i, j \text{ and } R_i = \pi P_i, R_j = P_j / \pi \stackrel{(2')}{\in} \mathbf{k}[T].$$

We have $\prod R_i = \chi$. Let us verify that R is divisibility decreasing which will prove that R is a χ -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 $R_{i+1} = R_j = P_j / \pi | P_j \mid^{j>i} P_i | R_i$.
- 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 14.2.0.3.



14.5 Topological applications

We want to study $M_n(\mathbf{k}) / GL_n(\mathbf{k})$ using our continuous μ to \mathbf{k}^n defined by the characteristic polynomial (14.1). 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 χ .

14.5.1 Topology of the fibers $\mu^{-1}(\chi)$

We keep the notations above and we denote by \mathcal{T} be the set of χ -types ordered by $\leq = \preceq$. Let

$$M_\chi = \{A \in M_n(\mathbf{k}) \mid \chi_A = \chi\} \stackrel{14.1}{=} \gamma^{-1}(\chi).$$

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 case, $P_{red} = P / \text{GCD}(P, P')$ and can be algorithmically computed (cf. 12.4.4.1 for the general case).

Lemma 14.5.1.1.

1. There exists⁶ 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 π , 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 $v_\pi(Q) \geq v_\pi(P)$ for any irreducible π , 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 π^d is $(1, \dots, 1)$ which is certainly $\leq \underline{\delta}$ and therefore $\chi_{ss} \leq \underline{Q}$.

(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 14.5.1.2. $\underline{\chi}_{cycl} = (1, \dots, 1, \chi)$ is called the cyclic χ -type and $\chi_{ss} = (\chi_{r,n}, \dots, \chi_{r,1})$ the semi-simple type. The corresponding similarity classes are called the cyclic (resp. semi-simple) orbits.

Remark(s) 14.5.1.3. The cyclic type $\underline{\chi}_{cycl}$ is the χ -type of the companion matrix $C(\chi)$ and the semi-simple type χ_{ss} is the χ -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.

⁶See 14.6.0.3 for an alternative algorithmic definition

By definition, the cyclic orbit is the subset of M_χ of cyclic elements the semi-simple orbit is the subset of M_χ of semi-simple elements.

Corollary 14.5.1.4.

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_χ .
4. The semi-simple orbit is the only closed orbit in M_χ (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 cyclic⁷ 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 9.7).

2. $\leq = \preceq$.

3. Use (2) and (3) of Lemma 14.6.0.3.

4. Use (2) and (4) of Lemma 14.6.0.3.

5. Use (3) and (4).

6. Use (2).

7. $\leq = \preceq$.

□

14.5.2 Global properties of $M_n(\mathbf{k})/GL_n(\mathbf{k})$

Let us start with a general lemma.

Lemma 14.5.2.1. *Let $\emptyset \neq \Omega \subset \mathbf{k}^n$ which is defined by the non vanishing of a finite number of polynomials. Then, Ω is dense in \mathbf{k}^n .*

⁷If 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 Ω 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 14.5.2.2.

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 14.5.2.1.
3. Because a matrix in $M_n(\mathbf{k})$ is cyclic if and only if is 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 $\mathrm{Res} \in \mathbf{k}[T_{i,j}]$ (6.6.0.3). We conclude by 14.5.2.1 again.
4. Apply the determinant characterization $\delta_r(A) \neq \{0\}$ of 5.7.1.4.

\square

Remark(s) 14.5.2.3. *It's easy and useful to prove openness and density of regular matrices without using the resultant (see 15.3.1.1) 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).*

14.6 Exercises

Exercise 14.6.0.1. 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 14.6.0.2. 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 Ω .

Exercise 14.6.0.3. With the notations of , prove that $P_{r,1} = P_{\text{red}}$ and $P_{r,i+1} = (P/P_{r,i})_{\text{red}}$ for $i \geq 1$. Deduce an effective algorithm to compute these polynomials (see 12.4.4.1). Can you generalize to the perfect case?

Exercise 14.6.0.4. The semi-simple part of the Jordan-Chevalley decomposition of $a \in M_\chi$ is χ_{ss} (cf. 12.4.2.1).

Exercise 14.6.0.5. 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 $\text{Card}(\mu^{-1}(\chi)) = 1$. 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 14.6.0.6. Prove that $\overline{O(\underline{P})}$ is the zero set of a finite family of polynomials⁸ in $\mathbf{k}[T_{i,j}]$.

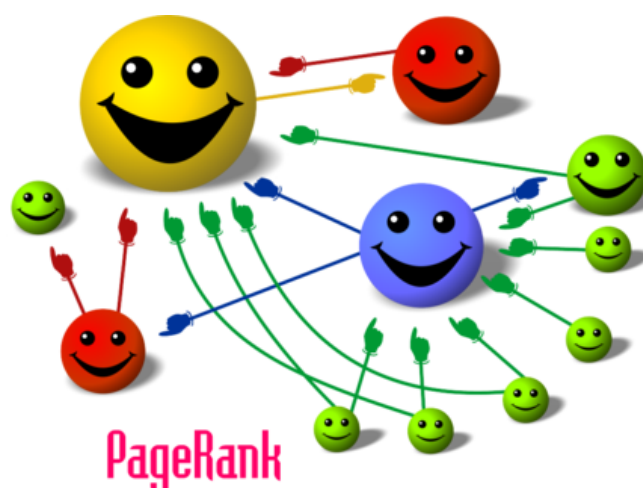
Exercise 14.6.0.7. Prove that the set of regular matrices of size $n \geq 2$ is not open. What is its topological interior ?

Exercise 14.6.0.8. Show that any continuous GL_n -invariant (by conjugation) function on $M_n(\mathbf{C})$ factors through γ (14.1). Deduce that $\mu : M_n(\mathbf{k})/\text{GL}_n(\mathbf{k}) \rightarrow \mathbf{k}^n$ induces an isomorphism of there algebra of numerical functions although μ is not an homemoprhism.

⁸The advance 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 15

Eigenvalues and primary components



15.1 Introduction



Perspective

We focus our attention to eigenvalues of complex and real matrices with a special attention of matrices with non negative coefficients. Our goal is to understand their continuity properties with respect to the matrix coefficients which is a necessary condition to be able to approximate them suitably.

In this chapter, we consider $\mathbf{k} \subset \mathbf{C}$ and $a \in \text{End}_{\mathbf{k}}(V)$, $A \in M_n(\mathbf{k})$ as always with characteristic polynomial χ . The set $\text{Spec}(A)$ of the eigenvalues of A is called its spectrum.

15.2 Continuity of primary components

We know from the chapter 14 that the similarity invariants do not vary continuously with the coefficients of the matrix even when the characteristic polynomial is a given monic polynomial χ . The counterpart

of this bad news is that they can effectively be computed in an exact way, but with an algorithm which is numerically very unstable by nature. But, for instance if the matrix has \mathbf{Q} -coefficients or more generally when the field is "fully computable", we can perform exact calculations with a computer.

In summary, Frobenius decomposition is exactly computable but in general is difficult if not impossible to approximate because it is not continuous even χ_a has been fixed.

On the other hand, we have in hand another decomposition (11.2.1.2) of V_a which in our case reads as follows. We write the irredundant prime decomposition

$$\chi = \prod P_i^{v_i}$$

of χ in monic irreducible polynomials and, remembering $\chi(a) = 0$ hence $\chi/V_a = \{0\}$ 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 χ -torsion module. We denote by $\pi_i(a)$ the projection onto $V_a[P_i]$ parallel to $\bigoplus_{j \neq i} V_a[P_j]$.

Lemma 15.2.0.1. *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 $\dim V_a[P_i] = \deg(\chi_i) = w_i \deg(P_i)$. 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 15.2.0.2. *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 if χ_a is split and we have $v_\lambda(\chi_a) = \dim \text{Ker}(a - \lambda \text{Id})$ for all λ .*

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 15.2.0.3. *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 $e_i \in \mathbf{k}[T_{i,j}]$ depending on χ (and not on α) 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.

2. A polynomial is continuous, so is its composition its α . Apply then the preceding lemma.

□

In summary, the prime decomposition of χ are not exactly computable in general. But we will see that a prime decomposition of χ being given, the primary parts vary continuously with a provided $\chi_a = \chi$ has been fixed. In particular, contrary to the Frobenius decomposition, these primary parts well behave by approximation.

If χ is split (for instance if $\mathbf{k} = \mathbf{C}$), we have $P_i(T) = T - \lambda_i$ where λ_i is an eigenvalue of a and

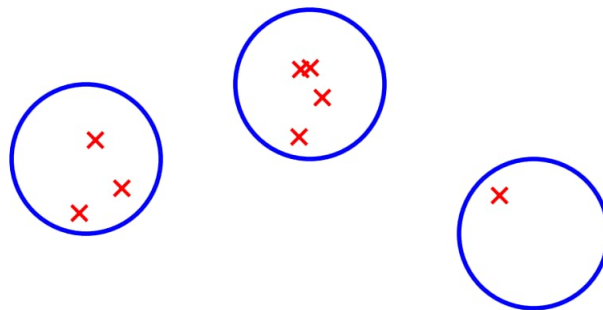
$$V_i[P_i] = \text{Ker}(a - \lambda_i)^{v_i}.$$

If we want to vary χ and understand P_i , we therefore have to look at the continuity of the eigenvalues.

15.3 Regularity of polynomial roots

15.3.1 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 converging¹ to P and Z_n Z be set of complex roots of P_n .



$$P(T) = T^3(T - 2 - i)(T - 4 + i)$$

Proposition 15.3.1.1. *Let λ be a root of P with multiplicity m_λ .*

1. *For any $\varepsilon > 0$, there exists N such that for all $n > N$ the number of roots of P_n in $B(\lambda, \varepsilon)$ counted with multiplicity is m_λ .*

¹With respect to an arbitrary norm on $\mathbf{C}_d[T]$.

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 .

Proof. 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 λ . We have $P_n(T) = \prod (T - \mu_i)$ where $\mu_i \in Z_n$ 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) 15.3.1.2. The following statement, although equivalent, is sometimes useful. Let $X \subset \mathbf{C}$ 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 Ω is open in \mathbf{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 ,

$$\{P \in \mathcal{M}_d \mid \deg_\Omega(P) \geq n\} \text{ is open in } \mathcal{M}_d.$$

Corollary 15.3.1.3. Let $\pi : \mathbf{C}^d \rightarrow \mathcal{M}$ be the continuous map $(\lambda_i) \rightarrow \prod (T - \lambda_i)$ 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 π is surjective (\mathbf{C} is algebraically closed) and therefore π is onto. This give the uniqueness. Moreover, $\pi(\lambda) = P$ exactly means that λ_i are the roots of P and therefore P determines (λ) up to reordering. This gives the existence of \bar{f} as a map of sets. Let $(P_n \stackrel{15.3.1.1}{=} \prod_i (T - \lambda_{i,n}))$ be a sequence \mathcal{M} converging to $P \in \mathcal{M}$. We have

$$\lim \bar{f}(P_n) = \lim f((\lambda_{i,n})) = f(\lim(\lambda_{i,n})) \stackrel{\text{invariance}}{=} f((\lambda_i)) = \bar{f}(P).$$

□

15.3.2 Smoothness of simple roots

Let $\varphi : \mathbf{C}^d \times \mathbf{C} \rightarrow \mathbf{C}$ be the "universal" polynomial function $(a_i, z) \mapsto z^n + \sum_{i < d} a_i z^i$. By smoothness we mean C^∞ (or even holomorphic for the advanced reader).

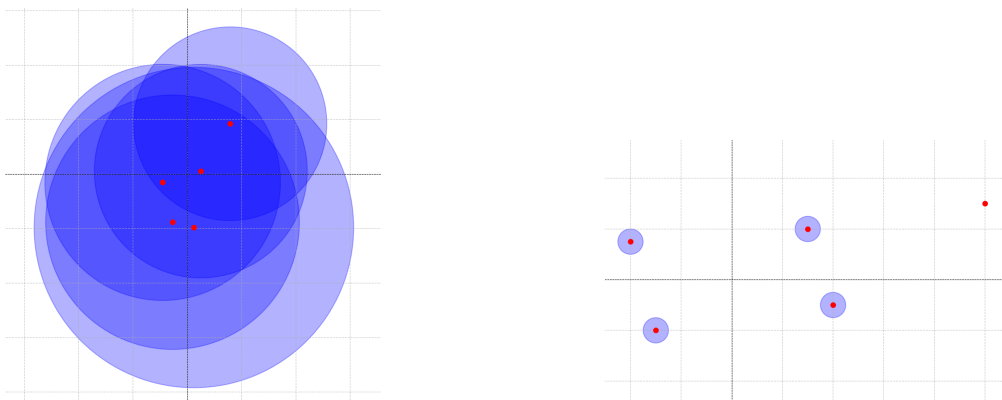
Proposition 15.3.2.1. *Let $\alpha = (\alpha_i) \in \mathbf{C}^d$ and λ_0 is a simple root of the polynomial $P(\cdot) = \varphi(\alpha, \cdot)$. There exists a smooth function λ defined in a neighborhood $U \subset \mathbf{C}^d$ of α and a neighborhood $D \subset \mathbf{C}$ of λ_0 such that $\lambda(a)$ is the only root of $\varphi(a, \cdot)$ belonging to D for any $a \in U$. Moreover, this root is simple.*

Proof. Because φ is smooth, we just have to verify that the hypothesis of the implicit function theorem are fulfilled, namely that the differential of $(x, y) \mapsto \varphi(\alpha, x + iy)$ is not zero at λ_0 . But the (polynomial) Taylor expansion $P(\lambda_0 + h) = P(\lambda_0) + hP'(\lambda_0) + o(h)$ shows that the differential of P is the complex similarity $h \mapsto P'(\lambda_0)h$ which is invertible because $P'(\lambda_0) \neq 0$. □

Remark(s) 15.3.2.2. *We could also use this proposition to show that the locus of polynomials with distinct roots is open.*

15.4 Localizing eigenvalues

15.4.1 Gershgorin disks



Gershgorin disks

We denote by $D(z_0, R)$ the closed disk $D(z_0, R) = \{z \in \mathbf{C} \mid |z - z_0| \leq R\}$.

Proposition 15.4.1.1. Let $A \in M_n(\mathbf{C})$ and $R_i = \sum_{j \neq i} |a_{ij}|$, $i = 1, \dots, n$.

- (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.

- (Gershgorin I) In general,

$$\text{Spec}(A) \subseteq \bigcup_{i=1}^n D(a_{ii}, R_i).$$

- (Gershgorin II)² If F is a connected component³ 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. Hadamard. Let $x = (x_i)$ be a nonzero vector of some $A \in M_n(\mathbf{C})$ and let i such that $|x_i|$ is maximal among the modulus of the coordinates of x . The i^{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 $|x_i| > 0$.

Gershgorin I. Apply Hadamard to $A - \lambda \text{Id}$ with $\lambda \in \text{Spec}(A)$.

Gershgorin II. Let F' be the (finite) union of the connected components of Γ and $d \in [0, \dots, n]$. They are closed in Γ as any connected component and therefore are closed in \mathbf{C} because Γ 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 (15.3.1.2)

$$\{t | \deg_F(\chi_{A_t}) \geq d\} = \{t | \deg_{\Omega'}(\chi_{A_t}) \geq d\}$$

is open in $[0, 1]$. But $\text{Spec}(A_t) \subset F \sqcup F'$ and therefore,

$$\{t | \deg_F(\chi_{A_t}) \leq d\} = \{t | \deg_{F'}(\chi_{A_t}) \geq n - d\}$$

is also open and so is $U_d = \{t | \deg_F(\chi_{A_t}) = d\}$ and $[0, 1] = \sqcup_{d \leq n} U_d$. By connectedness $[0, 1]$ only one is nonempty and equal to $[0, 1]$. But for $d = \text{Card}\{i | a_{i,i} \in F\}$, we have $0 \in U_d$ because $A_0 = \text{diag}(a_{i,i})$. \square

Observe that one can shrink Γ using $\text{Spec}(A) = \text{Spec}(^t A)$.

²This 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.

³The reader will observe that a disk being connected, F is an union of some of the D_i 's.

15.4.2 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 15.4.2.1. 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 15.4.2.2. Let $A \in M_n(\mathbf{C})$.

- ρ 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 $\rho(A) = \lim_{k \rightarrow +\infty} \|A^k\|^{\frac{1}{k}}$.

Let us start with a lemma. Although it is a straightforward of Jordan reduction theorem, let us give a more elementary proof.

Lemma 15.4.2.3. 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 $A \in M_n(\mathbf{C})$ is triangularizable, one can assume $A = ((t_{i,j})_{1 \leq i, j \leq n})$ is upper triangular. For $\delta > 0$, we have:

$$A_\delta = D_\delta^{-1} A D_\delta = \begin{pmatrix} a_{1,1} & \delta a_{1,2} & \dots & \delta^{n-1} a_{1,n} \\ 0 & a_{2,2} & \dots & \vdots \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & a_{n,n} \end{pmatrix} \quad \text{where } D_\delta = \text{diag}(1, \delta, \dots, \delta^{n-1})$$

Then A_δ makes the job for δ small enough. \square

Proof. (Continuity) Use 15.3.1.3.

(Householder) Let $x \in \mathbf{C}^n$ be a unit eigenvector of A whose eigenvalue has maximum modulus. We have $\rho(A)\|x\| = \|Ax\| \leq \|A\|$ which gives: $\rho(A) \leq \inf_{\|x\| \in \mathcal{N}} \|A\|$.

Let us prove the reverse inequality. Let $\varepsilon > 0$, and, thanks to the preceding lemma, let us choose $P_\varepsilon \in \text{GL}_n(\mathbf{C})$ such that $A = P_\varepsilon^{-1}T_\varepsilon P_\varepsilon$ with T_ε 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 $\rho(A) = \inf_{\|x\| \in \mathcal{N}} \|A\|$.

(Gelfand) Assume first $\|\cdot\| \in \mathcal{N}$. With the above notation, or $k \in \mathbf{N}^*$:

$$\|A^k\| = \|P_\varepsilon T_\varepsilon^k P_\varepsilon^{-1}\|_\infty \leq \gamma_\varepsilon \|A^k\|_\infty \leq \gamma_\varepsilon (\rho(A) + \varepsilon)^k$$

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 \mathcal{N} is any norm on $M_n(\mathbf{C})$, there exists $a, b > 0$ such that $a\|A^k\| \leq \mathcal{N}(A^k) \leq b\|A^k\|$ (equivalence of norms in finite dimension). Because $\lim a^{1/k} = \lim b^{1/k} = 1$, we get the result. \square

15.4.3 Smoothness of simple eigenspaces

Let $A_0 \in M_d(\mathbf{C})$ and assume $\lambda_0 \in \text{Spec}(A)$ a simple root of χ_{A_0} . Using the smoothness of simple roots (15.3.2.1) and the smoothness of $A \mapsto \chi_A$, we know that there exists a neighborhood Ω of A_0 and $V \subset \mathbf{C}$ of λ_0 and a smooth function $\lambda : \Omega \rightarrow \mathbf{C}$ such that $\lambda(A_0) = \lambda_0$ and $\lambda(A)$ is the unique eigenvalue 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 15.4.3.1. *The projector π_λ is smooth.*

Proof. Let R be the ring of complex smooth functions on Ω . 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 λ , 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 Ω where these columns $\pi_\lambda(A)$ are independent (semi-continuity of the rank).

Exercise 15.4.3.2. Let $A(a, b, c) = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$ and Ω 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 Ω . 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 $A(a, b, c)$.

15.4.4 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 ≥ 0 and positive $A > 0$ if they are > 0 .

Theorem 15.4.4.1 (Perron-Frobenius I). *Let $A \in M_n(\mathbf{R}^+)$ an irreducible matrix. Then:*

1. $\rho = \rho(A)$ is a simple root of χ_A and is nonzero.
2. The eigenspace of ρ 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 λ . 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

$$\|A^{m+1}\|_1 \|x\|_1 \geq \|A^{m+1}|x|\|_1 \geq r^m \|A|x|\|_1.$$

or because both x and Ax are non zero, $r^m \leq C\|A^{m+1}\|_1$ for some $C > 0$. By Gelfand's theorem (15.4.2.2), 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 ρ . 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 (2.4.0.1) $\alpha \in \mathbf{C}$ 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 ρ and λ which proves (3).

For (2), let us choose x_0 a non zero real vector of A for ρ and let y another such non-zero real eigenvectors for ρ . By (*), $|x_0|$ is an eigenvector for ρ 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 ρ , 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 ${}^tyA = \rho^t y$. 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 3 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 ρ 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 λ_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 λ_1 is a simple root of χ_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 15.4.4.2. *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 ρ) $Ax = \rho x$. \square

15.4.5 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.

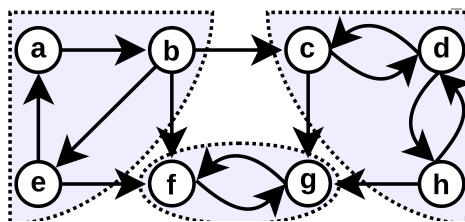
Lemma 15.4.5.1. *The shortest length of a path from v to v' is $\leq n$ where n is the number of vertices of G . In particular, matrix terms, if $G_{v,v'}^k \neq 0$ for some $k > 0$, then $G_{v,v'}^k \neq 0$ for some k with $0 < k < n$.*

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 $0 < k \leq n$.

15.4.6 Irreducible matrices

Definition 15.4.6.1. 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 15.4.6.2. 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 15.4.6.3 (Perron-Frobenius II). Let $A \in M_n(\mathbf{R}^+)$ be an irreducible matrix. Then:

1. $\rho = \rho(A)$ is a simple root of χ_A .
2. The eigenspace of ρ 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 $1 + \lambda \in \rho(\text{Id} + A)$. We have $\lambda \in \rho(A)$ and by triangle inequality $\leq 1 + |\lambda| \leq 1 + \rho(A)$ showing $\rho(\text{Id} + A) \leq 1 + \rho(A)$. Conversely, by 15.4.4.2, $\rho(A)$ 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 15.4.4.1 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 15.4.4.2, 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 15.4.4.1 (2) applied to $\text{Id} + A$, we get $x > 0$.
3. Follows directly from 15.4.4.1 (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 λ of $A \in M_n(\mathbf{C})$ is called a *dominant eigenvalue* if λ has multiplicity 1 in χ_A and $|\lambda| > |\mu|$ for all eigenvalues $\mu \neq \lambda$.

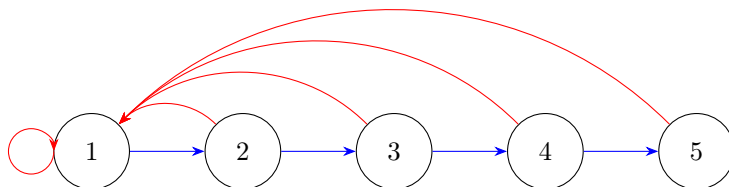
15.4.7 A classical illustration

Rather than classically choosing the historical (and nowadays quite old-fashioned) PageRank algorithm of Google⁴, let us explain how primitive matrices are used in population dynamics through the so called Leslie model⁵.

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 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



⁴Cf. 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

⁵P. H. Leslie. On the Use of Matrices in Certain Population Mathematics. Biometrika 33, no. 3 (1945): 183–212. <https://doi.org/10.2307/2332297>.

and is certainly strongly connected. Using the Perron-Frobenius II theorem 15.4.6.3, we show immediately that the normalized histogram of the population defined the normalized vector $N(t)/\|N(t)\|$ where $N(t) = (N_1(t), \dots, N_n(t))$ will converge when t goes to ∞ to the unique positive eigenvector of A for $\rho(A)$ of 1-norm 1.

15.4.8 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 Ω . 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

$$p_{t+1} = P p_t.$$

If we assume that P is moreover irreducible, the Perron-Frobenius II theorem 15.4.6.3 shows that p_t converges when the discrete time t goes to ∞ 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.

15.5 Exercices

Exercice 15.5.0.1. *Continuité avec P'/P .*

Exercice 15.5.0.2. *Généralités sur la topo quotient*

Exercice 15.5.0.3. $\mathbf{C}^n/S_n = \mathbf{C}^n$ comme métrique

Exercice 15.5.0.4. *distance Hausdorff*

Exercice 15.5.0.5. *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 λ_i is a continuous function on \mathcal{R} .*
2. *Prove that the restriction of λ_i to Ω is a smooth function.*
3. *If $n \geq 2$, prove that there exists no continuous function λ on $M_2(\mathbf{C})$ such that $\lambda(A) \in \text{Spec}(A)$ for all $A \in \text{Spec}(A)$.*

Exercise 15.5.0.6. 1. Prove that the closure in $M_n(\mathbf{R})$ of diagonalizable matrices is the set of trigonizable matrices.

2. What is its interior ?

3. Same questions replacing \mathbf{R} by any subfield of \mathbf{C} .

Exercise 15.5.0.7. Let $\Omega \subset M_2(\mathbf{C})$ be the set of rank 1 matrices. Show

1. Ω 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 15.5.0.8. 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 15.5.0.9 (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 $\lim z_n^n A^n$ is a rank 1 projector. Can you give a way to approximate the corresponding eigenvalue?

Exercise 15.5.0.10. 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 χ_A is split over \mathbf{R} is $1/2$. How can you generalize?

Exercise 15.5.0.11. 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.

Chapter 16

Index et bibliography

Index

- adapted basis, 96
- Algebraic Identities Permanence Principle, 37
- basis,
 - ante-dual, 32
 - dual, 30
- bicommutant, 116
- Bézout equivalence, 93
- Bézout matrix, 13
- Cayley-Hamilton Theorem, 38, 39
- Chinese remainder lemma, 80
- cokernel, 51
- commutant, 113
- commutative diagram, 56
- commutator, 43
- companion matrices, 111
- complex of modules, 54
- content, 122
- decomposition,
 - Frobenius, 111
- derived subgroup, 43
- determinant trick, 78
- diagram, 56
- dilatation, 13
- dominant eigenvalue, 181
- duality bracket, 29
- duality,
 - contravariance, 35
 - convention of biduality, 33
 - differential, 31
 - Jacobian, 31
 - orthogonal, 30
 - polar, 30
 - transpose, 34
- endomorphism,
 - cyclic, 112
 - absolutely semi-simple, 139
- equivalent matrices, 40
- Euclidean division in $\mathcal{R}[T]$, 14
- exact sequence, 54
- factorial, 119
- finite presentation modules, 67
- Fitting ideals, 66
- flatness, 161
- functor, 59
- functoriality,
 - of the cokernel, 56
 - of the kernel, 58
- Gauss equivalent, 40
- Gauss,
 - elimination, 40
- GCD, 121
- Gershgorin disks, 173
- graph,
 - strongly connected, 179
- Greatest Common Divisor GCD, 92
- group
 - solvable, 151
- idempotent, 81
- inductive set, 15
- inequality, Cauchy-Schwarz,

- real, 20
- integer
 - algebraic, 125
- integers,
 - rings of, 79
- integral domain, 70
- integral element, 79
- irreducibility of Φ_n over \mathbf{Q} , 125
- irreducible matrix, 180
- irreducibles,
 - existence, 120
 - of $\mathbf{R}[T]$, 123
 - uniqueness of the decomposition into, 119
- Jordan-Chevalley decomposition, 140
- LCM, 121
- lemma
 - of Zorn, 15
- lemma,
 - five, 59
 - Gauss lemma for PID, 93
 - Hensel, 140
 - Krull, 15
 - Nakayama, 79
 - of Euclid, 118
- Leslie matrix, 181
- minor of a matrix, 63
- module, 48
- module,
 - V_a , 53
 - torsion, 70
 - associated with an endomorphism, 53
 - cyclic, 77
 - free, 68
 - Noetherian, 85
 - quotient, 51
 - semi-simple, 135
- morphism,
 - Frobenius, 139
- Noetherian,
 - Hilbert's basis theorem, 88
 - module, 85
 - ring, 86
- operator norm, 175
- order,
 - \leq on types, 159
 - \leq on partitions, 162
 - \preceq on types, 159
- orientation, 22
- orientation,
 - direct basis, 22
 - positively oriented basis, 22
- partition,
 - of an integer, 130
- perfect group, 43
- permutation matrix, 13
- Perron-Frobenius Matrices, 177
- polynomial
 - cyclotomic, 124
- primary decomposition, 127
- primitive, 122
- quotient, 51
- reduced ring, 138
- reduction,
 - Jordan, 130
 - Frobenius, 111
- ring,
 - Euclidean, 92
 - Noetherian, 86
 - Noetherian UFD, 120
 - UFD, 122
 - UFD or factorial, 119

semi-continuity of the rank, 167

semi-simple,

 module, 135

similar matrices, 53

similarity invariants, 106, 108

similarity invariants, 106

Snake lemma, 71

space,

 stable, 53

spectral radius, 175

theorem,

 structure of finite type modules over PID, 95

torsion, 69

transvection, 13, 44

type, 158

UFD, 119, 122

universal property,

 of the cokernel, 60

 of the kernel, 60

 of the product of modules, 59

 of the sum of modules, 59

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] J. Milnor. Whitehead torsion. *Bull. Amer. Math. Soc.*, 72:358–426, 1966.
- [17] E. Noether. Idealtheorie in Ringbereichen. *Math. Ann.*, 83(1-2):24–66, 1921.
- [18] W. Rudin. *Real and complex analysis*. McGraw-Hill Book Co., New York, third edition, 1987.