

Linear and Bilinear Geometry

Yves Laszlo

Yves.Laszlo@universite-paris-saclay.fr

Beta version of February 14, 2025 with typos and mistakes



Contents

1	Introduction	9
1.1	Conventions	10
1.2	Prerequisites	11
1.3	Complement: Zorn's Lemma and application	12
I	Linear Algebra over Rings	15
2	Warm-up: review on basic linear algebra	19
2.1	Perspective	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	26
2.3.1	Minimal polynomial	27
2.3.2	Cyclic vectors	27
2.4	Supplementary exercices	27
3	Matrices without eigenvectors, I	29
3.1	Perspective	29
3.1.1	Algebraic Identities Extension Principle	29
3.1.2	Cayley-Hamilton in $M_n(\mathbb{R})$	30
3.2	Maximal rank matrices	31
3.3	Reminder on Gauss elimination method, field case	32
3.4	Application to subgroups of $GL_n(\mathbf{k})$	33
3.4.1	Transvections	33

3.4.2	Normal subgroups of $GL(V)$	35
3.5	Supplementary exercises	37
4	Modules	39
4.1	Perspective	39
4.2	Vocabulary and first examples	40
4.2.1	Modules	40
4.2.2	Morphisms	42
4.2.3	Quotient, cokernel	43
4.2.4	A key example: the $\mathbf{k}[T]$ -module V_a	45
4.3	Exact sequences and diagrams	45
4.3.1	Exact sequences	46
4.3.2	A key exact sequence	46
4.3.3	Commutative diagrams	47
4.4	Functoriality and diagram chasing	48
4.5	Universal properties	52
4.5.1	Sum and product	52
4.5.2	Kernel and cokernel	53
4.6	Properties to handle with caution	54
4.6.1	Finiteness	55
4.6.2	Free modules	55
4.6.3	Torsion	56
4.6.4	Summary of some specifics of Modules	57
4.7	Supplementary Exercises	57
5	Rings and Modules	61
5.1	Perspective	61
5.2	Quotient rings	61
5.2.1	Definition	61
5.3	Algebras	62
5.3.1	Cyclic modules and quotient rings	63
5.4	Integrality	64
5.4.1	An Application of Cayley-Hamilton	64
5.4.2	Rings of Integers	64
5.5	Cokernel of Diagonal Matrices	66
5.5.1	A fundamental exact sequence	66
5.5.2	Polycyclic modules	67
5.6	The Chinese Remainder Lemma	68

<i>CONTENTS</i>	5
5.7 Supplementary Exercises	70
6 Modules and Matrices	73
6.1 Perspective	73
6.2 Introduction	73
6.3 Noetherian Modules	74
6.3.1 Stability under exact sequences	75
6.3.2 Hilbert's Basis Theorem	76
6.4 Gauss algorithm in PID and Euclidean rings	77
6.4.1 Survival kit for PID and Euclidean rings	77
6.4.2 The general PID case	78
6.4.3 The Euclidean case	80
6.4.4 Minors and invariant ideals	81
6.5 Finite type modules over PID	83
6.6 Similarity in $M_n(\mathbf{k})$	84
6.6.1 Similiarity invariants	84
6.6.2 Explicit computations of similarity invariants	85
6.7 Frobenius Decomposition	87
6.8 Application: Commutant	89
6.9 Summary	90
6.10 Supplementary Section: Insight into K-Theory	91
6.11 Supplementary Exercises	92
II Linear Algebra over Fields	95
7 The Irreducible Toolbox	97
7.1 Perspective	97
7.2 Introduction	97
7.3 An UFD Criterion	97
7.3.1 Uniqueness Condition	98
7.3.2 Existence Criterion	100
7.4 Transfer	101
7.4.1 GCD, LCM in UFD	101
7.4.2 Content	102
7.4.3 The Transfer Theorem	103
7.5 Irreducibility of the Cyclotomic Polynomial Over \mathbf{Q}	103
7.6 Torsion Modules over PID	105
7.6.1 Primary Decomposition	106

7.6.2	Invariant Ideals and Primary Decomposition	107
7.7	Application: Jordan Reduction	108
7.7.1	Examples	110
7.8	An algorithm from \sim to \approx	111
7.9	Supplementary Exercises	112
8	Diagonalization and Semisimplicity	113
8.1	Perspective	113
8.2	Diagonalization	113
8.2.1	115
8.3	Semisimple Modules	115
8.4	«Reminder» on Perfect Fields	117
8.4.1	Criterion for Semisimplicity of V_a	118
8.5	Commuting families of Diagonal Matrices	119
8.6	Jordan-Chevalley Decomposition	120
8.6.1	Hensel's Lemma and Existence	120
8.6.2	Uniqueness	122
8.6.3	Similarity class of the components	122
8.6.4	Appendix: What about the algorithmic nature of the decomposition?	123
8.7	Supplementary Exercises	124
9	The Duality Toolbox	127
9.1	Basic notions	127
9.2	Motivation	129
9.3	Formal Biorthogonality	129
9.4	Ante-dual Basis: Biduality	129
9.5	Orthogonal and Polar in Finite Dimension	130
9.6	Biduality Conventions (Finite Dimension)	131
9.7	Contravariance	132
9.8	Supplementary Exercises	133
10	Topology of Similarity Classes*	135
10.1	Perspective	135
10.2	Introduction	135
10.3	Closure of a Nilpotent Orbit	136
10.3.1	Order and Duality on Partitions	137
10.3.2	Rank and Nilpotent Orbits	139
10.3.3	A Nilpotent Matrix Deformation	139
10.4	Closure of an Arbitrary Orbit	140

<i>CONTENTS</i>	7
10.5 Additional Exercises	141
11 Index et bibliography	143

Chapter 1

Introduction

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" ([11]).



Felix Klein

In these notes on vector, quadratic, and Hermitian geometry, we illustrate this visionary viewpoint by classifying geometric objects via invariants under various group actions (invariant factors, similarity invariants, discriminant, index, signature...).

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 ([2]) 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.

Let us explain our mathematical motivations. We are mainly concerned in properties of matrices, more precisely square matrices in field coefficients. This has two reasons. The first one is that they are of fundamental importance in all mathematics and more generally in all quantitative sciences. The second one is that their study reveals deep insights of a lot of more general subjects (arithmetic, K-theory, algebraic geometry, ...). It is definitely not our pretention to make a study of these advanced topics, but

we have tried to use methods which will be useful later. In particular, we have used the (quite abstract) diagrammatic view of modules together with the (quite concrete) use of matrix computations to obtain deep results on linear algebra.

In the first part, we give an introduction to language theory in order to solve the following problem : how to decide when two square matrices are similar ? We do that without any reduction theory, eigenvalue or irreducible elements. The gain is that we can solve this problem in a perfectly algorithmic way. The cost to pay is that the algorithm is non continuous (even it is semi-continuous in some sense).

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

The material of this book is more or less classical, only the perspective being somehow more original. The titles of the (few) chapters whose content is less classical are followed by an asterisk *..

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.

I extend my warm thanks to Peter Haïssinki who kindly provided his beautiful notes on the quadratic part, notes on which I relied heavily for a first version of the text, and to Olivier Debarre for his examples of endomorphism reduction.

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

1.1 Conventions



Unless expressly stated otherwise, the rings are assumed to be commutative and with an identity, generally denoted R . They are assumed, unless explicitly stated otherwise, to be non-zero, i.e., $1 \neq 0$. Their multiplicative group of units is denoted R^\times .

This grants them the following property: Every ring admits a proper maximal ideal for inclusion, a result we shall consider as an axiom (in this generality, this is equivalent to the axiom of choice).

Otherwise, the reader will easily demonstrate this by applying Zorn's Lemma to the set of proper ideals of R (1.3). In practice, it can often be dispensed with if one really insists. Naturally, it will only be used for existence theorems: it has no algorithmic value. Zorn's Lemma also allows us to demonstrate, essentially formally, that, just as \mathbf{Q} is contained in \mathbf{C} , any field \mathbf{k} is contained in an algebraically closed field Ω .

It will be used without further specification. The key to this result is the elementary fact that every polynomial with coefficients in \mathbf{k} has a root in some possibly larger field K . The existence of Ω then formally follows from the existence of maximal ideals in any non-zero rings. However, readers who dislike the axiom of choice will check that the existence of the aforementioned fields K suffices for us and that the existence of Ω is just a convenience of language, in fact.

1.2 Prerequisites

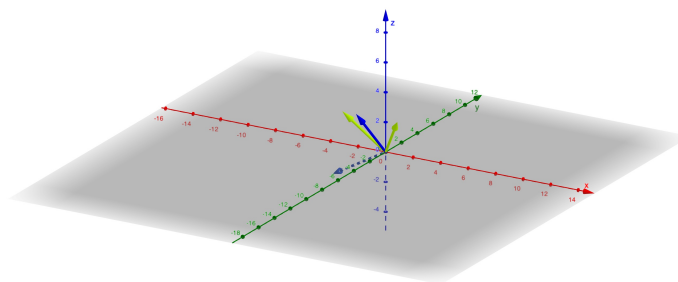
No other knowledge of linear algebra is assumed beyond the basics of dimension theory¹, the relationship between matrices and endomorphisms, and the elementary properties of the determinant. The reader is assumed to be familiar with the Gauss elimination method. Readers who have studied the theory in the context of real or complex vector spaces will make an effort to accept (or verify) that nothing changes on an arbitrary field.

Strictly speaking we 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.

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.

¹Strictly speaking, it is easy following our way to recover all the results just using Gauss elimination and formal properties of determinant

Definition 1.2.0.1. *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 permutation² $\sigma \in S_n$;*
- *dilatation if its of the form $D(r) = \text{Id} + (r - 1)E_{1,1}$ with $r \in \mathbb{R}^\times$;*
- *a Bézout matrix if it 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).

The multiplication of a principal pivot by a scalar r is achieved by product with a elementary dilatation $D(r) = \text{Id} + (r - 1)E_{1,1}$.

Geometrically in classical linear algebra, both transvections and dilatations add to a given vector $\sum x_j e_j$ the vector of constant direction e_i with "algebraic length" a constant multiple of x_j .

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 (5.2).

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 reading easier, a proof of the main results will be given in 6.4.1 and in (7). We just e will use two things for principal rings: Bézout's identity (in the first chapter) and the fact that a principal ring is a Unique Factorization Domain (UFD) (7.3.2.2), which allows us to relate the notion of GCD both to the decomposition into irreducible factors and to Bézout's identity.

1.3 Complement: 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.

Definition 1.3.0.1. *We say that E is inductive if every non-empty totally ordered part has an upper bound in E .*

²where $\delta_{i,j}$ is the Kronecker symbol equal to 1 if $i = j$ and 0 if not.

Example(s) 1.3.0.2. \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 1.3.0.3 (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 1.3.0.4. *[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

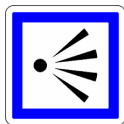
Content and Perspective

Chapter 2

Warm-up: review on basic linear algebra



2.1 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

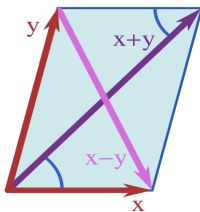
Theorem 2.2.1.2. *The mapping $v \mapsto \|v\|$ is a norm called the Euclidean norm.*

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

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

□

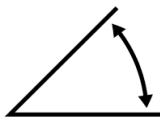
One immediately checks the important property of the Euclidean norm: the median equality



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

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.*

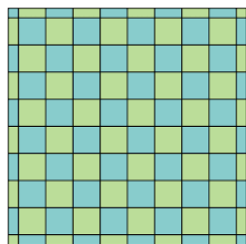
For instance, if we change the order of a basis of the plane, we change the orientation of the plane. Therefore, given a normed vector v of an oriented Euclidean plane, there exists a unique positive orthonormal basis of the plane (v, w) .

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

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

proving (2).

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

We get the well-known formula

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

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

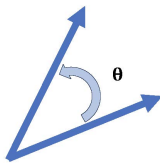
Corollary 2.2.3.4. *Two Euclidean planes are (non canonically) isomorphic.*

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 $\widehat{(v, w)} = |\widehat{(v, w)}|$.



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

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 $\pm w^\perp$ 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 $(1, \mathbf{i})$, the corresponding statement is that rotations are as usual of the form $\theta \mapsto \exp(\mathbf{i}\theta)z$ and symmetries of the form $\theta \mapsto \exp(\mathbf{i}\theta)\bar{z}$.*

Exercise(s) 2.2.5.4. *Show that the application which associates to an 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(s) 2.2.5.5. *Determine the real and complexe eigenvalues and th 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 $\text{SO}_2(E) \simeq \mathbf{R}/2\pi\mathbf{Z}$, 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 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 $M_2(\mathbf{R})$ are exactly orthogonally diagonalizable matrices (with respect to the standard Euclidean structure of \mathbf{R}^2).*

Proof. We identify E with the standard Euclidean plan \mathbf{R}^2 with its standard orthogonal basis \mathcal{B} . If $X, Y \in \mathbf{R}^2$ and $M \in M_2(\mathbf{R})$, 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

2.3 General linear maps of the plane



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 6.6.2.3 and 6.7).

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 6.7.

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 Supplementary exercises

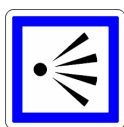
Exercise(s) 2.4.0.1. *Let G act primitively and faithfully on a set X . Assume that for some $x \in X$, the G_x contains an abelian normal subgroup whose conjugate subgroups generate G . Then $D(G) \subset G$ [Adapt the proof of Iwasawa criterium].*

Chapter 3

Matrices without eigenvectors, I



3.1 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.

3.1.1 Algebraic Identities Extension Principle

Proposition 3.1.1.1. *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. \square

Corollary 3.1.1.2. *All integral formulas for the determinant valid for complex square matrices remain valid for square matrices in any commutative ring \mathcal{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 $A \in M_n(\mathcal{R})$.*

Remark(s) 3.1.1.3. *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.*

3.1.2 Cayley-Hamilton in $M_n(\mathcal{R})$

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 multiplicativity.

Lemma 3.1.2.1. *Let $P = \sum_i \pi_i T^i, \bar{P} = \sum_i \bar{\pi}_i T^i \in \mathcal{R}[T]$ 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

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

\square

Corollary 3.1.2.2 (Cayley-Hamilton). *Let $A \in M_n(\mathcal{R})$ 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 3.1.2.1 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

3.2 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 3.2.0.1. *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.

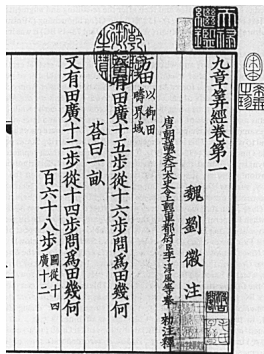
(4). Each (2) or (3) implies (4) (apply to both A and A^{-1} , the latter being defined as usual because A is bijective). \square

Remark(s) 3.2.0.2. • One will give below more natural proofs in some way, but less elementary. Precisely, see 5.7.0.3 for (2) and (4) with an argument using the choice axiom see and 6.11.0.6 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 (1.3.0.4).

- I have learned the nice argument in (3) from the post <https://mathoverflow.net/q/47846> of Balasz Strenner.

3.3 Reminder on Gauss elimination method, field case

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 ([6]).

With definition 1.2.0.1 in mind, we set

Definition 3.3.0.1. Let R be a ring and $p, q \geq 1$ two integers. 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);
- equivalent ($A \sim B$) is the exists invertible 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.

Proposition 3.3.0.2. *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. *$GL_n(\mathbf{k})$ is generated by transvections and dilatations.*
3. *$SL_n(\mathbf{k})$ 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(s) 3.3.0.3. *Give a computer program of 3.3.0.2 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 ?*

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

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)¹.

3.4.1 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 $\tilde{x} \mapsto x + f(x \bmod D)$. The set vector space of V of dimension 1 is

¹At this stage, this is just a notation; cf. chapter ?? for further insights

Proposition 3.4.1.1. *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 $(H(\tau), D(\tau)) \in \mathbf{P}V^* \times \mathbf{P}V$.

Proof. TBD □

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 3.4.1.2. *One has*

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

3.4.2 Normal subgroups of $GL(V)$

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

Definition 3.4.2.1. 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.²
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 3.4.2.2. 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 3.4.2.3 (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.

²Or equivalently (Exercise if the stabilizer G_x of a point $x \in X$ is a maximal subgroup of G).

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 3.4.2.4. *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

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 3.4.2.5. *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 $T_D \xrightarrow{\sim} \text{Hom}(V/D, D)$ be the group of transvections of line D (cf. 3.4.1.1) and apply Iwasawa criterium and 3.4.1.2. \square

3.5 Supplementary exercises

Exercise(s) 3.5.0.1. Prove that the evaluation map of lemma 3.1.2.1 is a (skew)-ring morphism if and only if t commutes with any element of \mathcal{R} .

Exercise(s) 3.5.0.2. Give an example of square matrices $\tau, A \in M_2(\mathbf{C})$ such that the evaluation at τ of ${}^t \text{Com}(\text{T Id} - A)(\text{T Id} - A) = \chi_A(\text{T}) \text{Id}$ is not equal to the products of the evaluation at τ of ${}^t \text{Com}(\text{T Id} - A)$ and of $(\tau - A)$. What is the value of $\chi_A(\tau)$ in this case ?

Exercise(s) 3.5.0.3. With the notation above prove the identity

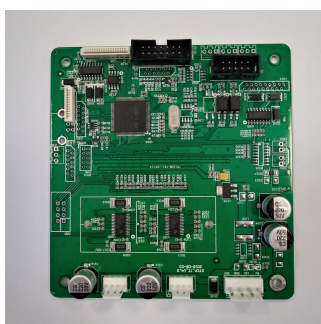
$$\text{T}^n \chi_{AB}(\text{T}) = \text{T}^m \chi_{BA}(\text{T})$$

Hint : Consider the matrices $C = \begin{bmatrix} \text{T Id}_m & B \\ A & \text{I}_n \end{bmatrix}$, $D = \begin{bmatrix} \text{Id}_m & -B \\ 0 & \text{T Id}_n \end{bmatrix}$. Give another proof of 3.1.2.2.(2)

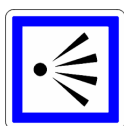
Exercise(s) 3.5.0.4. Let G act primitively and faithfully on a set X . Assume that for some $x \in X$, the G_x contains an abelian normal subgroup whose conjugate subgroups generate G . Then $D(G) \subset G$ [Adapt the proof of Iwasawa criterium].

Chapter 4

Modules



4.1 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 4.3) 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 6.6 and the chapters 8 and 10 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.

4.2 Vocabulary and first examples

4.2.1 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 4.2.1.1. *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) 4.2.1.2. *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 (*exercise*).
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 (*exercise*). This ideal is not finitely generated for example if $\mathbb{T} = \mathbf{R}^n$ (*exercise*).
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. 4.5.1).
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. 4.5.1).

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 \mathbb{R}	$\mathbb{R} = \text{field}$	$\mathbb{R} = \text{ring}$
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	$\oplus N_i = \{(x_i) \in \prod N_i \mid \text{Card}\{i \mid x_i \neq 0\} < \infty\}$	
$\mathbb{R}^{(I)}, \mathbb{R}^n$	$\mathbb{R}^{(I)} = \oplus_I \mathbb{R}, \mathbb{R}^n = \oplus_{i=1}^n \mathbb{R} = \prod_{i=1}^n \mathbb{R}$	

4.2.2 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 4.2.2.1. A morphism of modules $f : M \rightarrow N$ is a linear map: for any $x, y \in M, \lambda \in \mathbb{R}, f(x + y) = f(x) + f(y)$ and $f(\lambda x) = \lambda f(x)$.

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

Specifically, we have, e_j being the "canonical basis" of \mathbb{R}^n

²See 4.5.1.


³See 4.2.3.

Lemma 4.2.2.2. *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	$\text{Hom}_R(R^n, R^m) = M_{m,n}(R)$	

4.2.3 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 4.2.3.1. *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 4.2.3.2. *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 4.5.2.1.

Remark(s) 4.2.3.3. *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. 9.4.0.1), 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 N . We will see other examples.*

The following result is formal but important (compare with 4.5)

Proposition 4.2.3.4. *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 $\overline{m} = 0$. \square

Exercise(s) 4.2.3.5. *Quotient et supplémentaire d'un ev. TBD.*

4.2.4 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

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

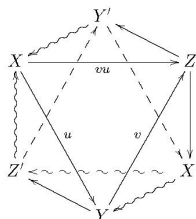
i.e.

(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 4.2.4.1. *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 .

4.3 Exact sequences and diagrams



4.3.1 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 4.3.1.1. 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(s) 4.3.1.2. 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 4.4.0.2 infra.
- Show that the product or direct sum of exact sequences is still exact.

4.3.2 A key exact sequence

Let $a \in \text{End}_{\mathbf{k}}(V)$ and V_a be the associated $\mathbf{k}[T]$ -module (4.2.4). 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 4.3.2.1. *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**. □

4.3.3 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 4.3.3.1. 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.

4.4 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. §4.5).

Proposition 4.4.0.1 (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 4.4.0.2 (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(s) 4.4.0.3. 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) 4.4.0.4. 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.

Exercise(s) 4.4.0.5. 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.

4.5 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.

4.5.1 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

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

and

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

Lemma 4.5.1.1 (Universal properties of sum and product). *The applications $\underline{h}(T)$ and $\underline{h}^\vee(T)$ 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 $f : \oplus M_i \rightarrow T$ is equivalent to giving a collection of morphisms $f_i : M_i \rightarrow T$ (thanks to the formula $f(\sum m_i) = \sum f_i(m_i)$ which is well defined because the sum is actually finite).



4.5.2 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 4.3.1.2 and 4.7.0.3).

If T is a test module we have two tautological applications

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

and

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

Lemma 4.5.2.1 (Universal properties of kernel and cokernel). *The applications $h(T)$ and $h^\vee(T)$ 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 $0 \rightarrow T \xrightarrow{\text{Id}} T \rightarrow 0$. Let then $\psi \in \text{Hom}_0(N, T)$. The condition $\psi \circ f = 0$ precisely ensures the commutativity of the diagram

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

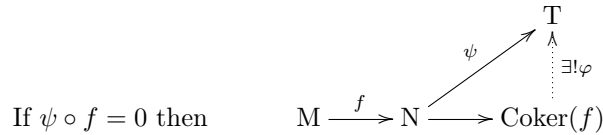
so that 4.4.0.1 ensures the existence of a unique φ making the diagram

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

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

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

The meaning of the lemma is that providing a morphism φ from the cokernel to \mathbb{T} is equivalent to providing a morphism ψ from \mathbb{N} to \mathbb{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:



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

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


and

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

are exact.


4.6 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 $\mathbb{R}^{(I)} \xrightarrow{\lambda_i \mapsto \sum \lambda_i x_i} \mathbb{M}$ injective	
Generating family $(x_i)_{i \in I}$	$\langle x_i \rangle = \mathbb{M}$ or $\mathbb{R}^{(I)} \xrightarrow{\lambda_i \mapsto \sum \lambda_i x_i} \mathbb{M}$ surjective	
Base $(x_i)_{i \in I}$	(x_i) free and generating or $\mathbb{R}^{(I)} \xrightarrow{\lambda_i \mapsto \sum \lambda_i x_i} \mathbb{M}$ bijective	
Free module \mathbb{M}	$\mathbb{M} \simeq \mathbb{R}^{(I)}$ i.e. \mathbb{M} admits a base	
Finite type module \mathbb{M}	finite generating family or $\mathbb{R}^n \rightarrow \mathbb{M}$ surjective	

⁷See 4.6.2.2 for the finite type case and chapter 6 in general.

4.6.1 Finiteness

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 $R^n \rightarrow M$. 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 6, rings for which this pathology does not happen are *Noetherian rings*, a huge generalization of fields containing almost all rings appearing naturally in algebra or number theory. In a first approach⁸, let us explain here how they are defined and what this is relevant for our finiteness problem. 

Definition 4.6.1.1. *A ring is Noetherian if every ideal is finitely generated.*

For instance, fields and PID are Noetherian.

Exercise(s) 4.6.1.2. *Show that the rings of continuous real functions on \mathbf{R} is non Noetherian.*

Proposition 4.6.1.3. *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(s) 4.6.1.4. *Adapt the proof below and prove that if R is a PID, any submodule of R^n is free (we will give a far more general statement in 6.5.0.1).*

4.6.2 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**). 

⁸See 6.3 and 6.3.0.2 below

- Example(s) 4.6.2.1.** 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 $n \in \overline{\mathbf{N}} = \mathbf{N} \cup \{\infty\}$.
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 4.6.2.2. 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 3.2.0.1, n is uniquely determined by M . \square

Exercise(s) 4.6.2.3. Using Krull's theorem, how can you generalize the proposition for general free modules ?

Remark(s) 4.6.2.4.

- This property fails if R is no longer assumed to be commutative (see 4.7.0.4).
- 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 module⁹ (see 4.7.0.6)!

4.6.3 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) 4.6.3.1. *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 3.1.2.2 for instance). More generally¹⁰, 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 domain*¹¹ 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^{6.5} if and only if they have no torsion. Not this not true in general (**exercice TBD**).



4.6.4 Summary of some specifics of Modules

 <p>Bases, Finiteness, Complements</p>		
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

4.7 Supplementary Exercices

Exercise(s) 4.7.0.1. 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 4.2.4), then V is finite-dimensional if and only if V_a is of finite type and torsion.

Exercise(s) 4.7.0.2. Let \mathbf{k} be a field and R a ring.

¹⁰The 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.

¹¹Recall that this means that R is not zero and that the product of two nonzero elements is nonzero.

- Show that the invertibles of $\mathbf{k}[T]$ are the non-zero constant polynomials from \mathbf{k}^* .
- Show that a matrix from $M_n(\mathbf{R})$ is invertible if and only if its determinant is an invertible of \mathbf{R}^\times .
Deduce that $M \in M_n(\mathbf{k}[T])$ is invertible if and only if $\det(M) \in \mathbf{k}^*$.

Exercise(s) 4.7.0.3 (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(s) 4.7.0.4. We will show that if the ring \mathcal{R} is not assumed to be commutative, then it may occur that the \mathcal{R} -modules \mathcal{R}^n , $n \geq 1$ are all isomorphic. To this end, we fix a real vector space V equipped with a countable base $(e_k)_{k \in \mathbf{N}}$ and we denote \mathcal{R} the ring of linear applications on V (equipped with composition), identified as «infinite matrices» of

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

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

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

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

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

Exercise(s) 4.7.0.5. Let $d \geq 1$ be a natural number, \mathcal{R} a principal ring and $M = \mathcal{R}^d$. Let N be a submodule of M . We aim to prove by induction on d that N is isomorphic to \mathcal{R}^δ with $\delta \leq d$. Assume $d \geq 1$ and the theorem proven for submodules of $\mathcal{R}^{d'}$ if $d' < d$.

1. Let $\underline{\nu} = (\nu_1, \dots, \nu_d) \in \mathcal{N}^d - \{0\}$ 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 \mathcal{A} and $K \subset \mathcal{R}^{d-1}$.

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

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

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

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

5. Conclude.

Exercise(s) 4.7.0.6. Let $N = \mathbf{Z}^{(\mathbf{N})}$ (direct sum of countable many copies of \mathbf{Z}). It is a free submodule of $M = \mathbf{Z}^{\mathbf{N}}$ (product of countable many copies of \mathbf{Z}) with basis $e_n = (\delta_{n,p})_{p \in \mathbf{N}}$. Let $\varphi \in \text{Hom}_{\mathbf{R}}(M^*, M)$ be the morphism $u \mapsto (u(e_n))_{n \in \mathbf{N}}$. We will prove that φ defines an isomorphism $M^* \rightarrow N$ and then conclude by a cardinality argument that M is not free¹².

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

Let $d \geq 2$ be an integer.

1. Show that $\text{Ker } \varphi \xrightarrow{\sim} G^*$, where $G = M/N$.

2. Let H_d be the set of elements of G divisible by d^k for all k . Show that H_d is a submodule of G .

3. Show that any linear form $u : G \rightarrow \mathbf{Z}$ vanishes on H_d .

4. Determine $H_2 + H_3$. 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 $x = (x_n)_{n \in \mathbf{N}} \in M$, define $|x|_2 = \sup |x_n|_2$. Show that $|x|_2$ is a real number and $\forall u \in M^*, \forall x \in M, |u(x)|_2 \leq |x|_2$.

¹²This method of proof of Baer's result comes from [7]

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

C. Conclusion

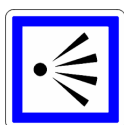
1. Describe M^* .
2. Prove that M is not free by a cardinality argument?
3. Show that the evaluation biduality morphism $\mathbf{N} \rightarrow \mathbf{N}^{**}$ defined by $x \mapsto (\varphi \mapsto \varphi(x))$ is an isomorphism, even though \mathbf{N} is freely generated over \mathbf{Z} with infinite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

Chapter 5

Rings and Modules



5.1 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.

5.2 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 4.2.3, there exists a unique group structure on R/I making the projection $\pi : R \rightarrow R/I$ a morphism.

5.2.1 Definition

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

Proposition 5.2.1.1. *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. 4.5.2.1) : 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. 4.2.3.4).

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(s) 5.2.1.2. *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 5.2.1.3. *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. 5.7.0.3).*

5.3 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

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

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 5.3.0.1. *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 (3.1.2.1) that this A -module morphism

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

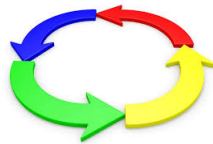
is also an A -algebra morphism. □

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(s) 5.3.0.2. *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.*

5.3.1 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 5.3.1.1 (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 $I = \text{Ann}_R(M) = \{\lambda \in R \mid \lambda M = \{0\}\}$.*

Proof. Let x be a generator of M . Then, the homomorphism $R/I \xrightarrow{x} M$ is an isomorphism. The last point is the formula $I = \text{Ann}_R(R/I)$. □

If it is well known that subgroups of a cyclic groups are cyclic, it is no longer true for submodules of cyclic modules in general. This is true essentially in the principal case where we recover the analogous statement for subgroups of finite groups.

Exercise(s) 5.3.1.2. 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.

5.4 Integrality

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

5.4.1 An Application of Cayley-Hamilton

Proposition 5.4.1.1 (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 $P = \det(TId - A)$ and invoke Cayley-Hamilton theorem (3.1.2.2) 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 5.4.1.2 (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 $M = 0$.*

5.4.2 Rings of Integers

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

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

Theorem 5.4.2.1. *The subset of R' of elements which integral over R forms a subring of R' .*

Proof. 0 and 1 are integral. We must therefore prove that the difference and the product of two integral elements r' and r'' are integral. Let $M = R[r', r'']$ be the ring of polynomial expressions in r' and r'' with coefficients in R . If r' and r'' are annihilated by monic polynomials of degrees n' and n'' , the family $r'^i r''^j \mid 1 \leq i \leq n', j \leq n''$ generates M and contains $r' - r''$ and $r' r''$. But if $\rho \in M$, the homothety of ratio ρ defines an endomorphism h_ρ of M and thus (5.4.1.1) there exists a monic $P \in R[T]$ such that $P(h_\rho) = h_{P(\rho)} = 0$. Applying to $1 \in M$, we obtain $P(\rho) = 0$ so that all elements of M are integral over R . \square

Corollary 5.4.2.2. *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 5.4.2.1 applied to $R = k$, it suffices to show that the inverse of a non-null algebraic element $r' \in k'$ is still nonzero. Suppose therefore P is a unitary annihilator of r' . But then, $T^{\deg(P)} P(1/T)$ is a non-null annihilator of $1/r'$. \square

Remark(s) 5.4.2.3. *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 (5.7.0.6), which is a good news, and that $\overline{\mathbf{Z}}$ is non noetherain (7.3.2.4), which is bad news in some extent.*

Remark(s) 5.4.2.4. *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(s) 5.4.2.5. 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.

5.5 Cokernel of Diagonal Matrices

5.5.1 A fundamental exact sequence

Let $d \in R$. Then, the sequence

$$(*) \quad R \xrightarrow{r \mapsto dr} R \xrightarrow{r \mapsto r \pmod{d}} R/(d) \rightarrow 0$$

is exact. More generally, let's consider a "diagonal" rectangular matrix $D \in M_{n,m}(R)$ «diagonal» in the sense that its coefficients $d_{i,j}$ are zero if $i \neq j$. Thus, we have a block decomposition

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

with $\Delta = \text{diag}(d_i) \in M_\nu(R)$, $\nu = \min(m, n)$, $\mu = \sup(m, n)$ 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 (**)

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

or

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

Lemma 5.5.1.1. *The sequence (**) is exact. In particular, one has a canonical isomorphism*

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

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

The arrow $R^n = R^\mu \xrightarrow{r \mapsto (r_i \pmod{d_i})_i} \prod_{i=1}^{\mu} R/(d_i)$ 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 $\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto (d_i x_i \pmod{d_i})_i$ and is therefore zero proving the inclusion $\text{Im} \subset \text{Ker}$.

If $r \in R^m$ maps to zero, we have $r_i \bmod d_i = 0$ for all i and therefore there exists $x_i \in R$ 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 4.4.0.1. \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 $[6] \in M_1(\mathbf{Z})$ is $\mathbf{Z}/6\mathbf{Z}$ but also $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ thanks to the usual Chinese lemma. Let's fix this problem.

5.5.2 Polycyclic modules

Definition 5.5.2.1. A polycyclic module is a finite direct sum of cyclic modules $M = \bigoplus_{i=1}^n M_i$ 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 (eventually zero).

We will show that the I_i 's are uniquely determined by the module²

Proposition 5.5.2.2. Let M a polycyclic module as before. 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 will refer to the I_k 's as the invariant ideals of our polycyclic module and to n as its rank.

Proof. (1). M is a quotient of R^n and has therefore a generating set consisting of n elements. Conversely, if we have a generating family of d elements, we get a surjection $R^d \mapsto \bigoplus R/I_k \oplus (R/I_n)^n$ which factors through a surjection $(R/I_n)^d \rightarrow (R/I_n)^n$ implying $d \geq n$ by 3.2.0.1.(2)] Let $x \in R$, and let $k \leq n$. For any ideal I of R , let $I_x = \{y \in R \mid xy \in I\}$. By construction, the ideal $I_x = R$ if and only if $x \in I$. The multiplication by x defines an isomorphism $xM \cong \bigoplus_{k=1}^{n(x)} R/(I_k)_x$ where $n(x)$ is the largest k such $(I_k)_x \neq R$. Because $(I_k)_x$ is increasing this shows that xM is polycyclic. Moreover, by (1) the module 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 $x \in I_k$. \square

With the example of $M = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, we observe that is polycyclic because it is isomorphic to $\mathbf{Z}/6\mathbf{Z}$ generated by a single element (1 mod 6 for instance) and that xM is generated by less than one element if and only if $x \in 6\mathbf{Z}$, as it has to be.

²This 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>.

Remark(s) 5.5.2.3. *In particular, we recover the fact that \mathbf{R}^n and \mathbf{R}^m are isomorphic if and only if $n = m$.*

5.6 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 $\mathbf{R}/(ab) \xrightarrow{\sim} \mathbf{R}/(a) \times \mathbf{R}/(b)$ for coprime ideals $(a), (b)$ in a PID \mathbf{R} . This latter condition can also be written as $(a) + (b) = \mathbf{R}$ according to Bézout's identity. We will give a useful (fortunately quite straightforward) generalization in the case where \mathbf{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.



Terracotta Army
Mausoleum of Emperor Qin

Proposition 5.6.0.1 (Chinese Remainder Lemma). *Let I_1, \dots, I_n , $n \geq 2$ be ideals of \mathbf{R} which are pairwise coprime, i.e., such that $I_i + I_j = \mathbf{R}$ for $i \neq j$ and let M be an \mathbf{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 ³*

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

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

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)⁴.

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 $(m_j) \mapsto \sum e_j m_j$

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

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

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) 5.6.0.2. 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 $J = \{i \in I \mid e_i \text{Ker} = \{0\}\}$.

Exercise(s) 5.6.0.3. Solve the following systems of equations, with the unknown $x \in \mathbf{Z}$:

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

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

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

5.7 Supplementary Exercises

Exercise(s) 5.7.0.1. TBD

Exercise(s) 5.7.0.2 (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. 4.2.4), 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 $\text{ev}(A) = A(r)$ and $\text{ev}_Q(A, B) = A(r)$. 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(s) 5.7.0.3. 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(s) 5.7.0.4. 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(s) 5.7.0.5. Existence corps alg clos. TBD

Exercise(s) 5.7.0.6. TBD \bar{k} is algebraically closed.

Exercise(s) 5.7.0.7. Let R be a ring and $P = \sum_{i=0}^n a_i X^i \in R[X]$.

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 $R[X]$ if and only if a_0 is invertible and for all $i \geq 1$, a_i is nilpotent. Hint: if $Q = \sum_{i=0}^m b_i X^i$ 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 6

Modules and Matrices



David Hilbert

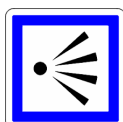


Matrix Equivalence



Emmy Noether

6.1 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 (6.5.0.3) or more generally of finite type modules over PID (6.5.0.1).

6.2 Introduction

The notion of Noetherian ring inevitably leads back to Hilbert's foundational paper from 1890 [10] with its three major theorems, the first being the Basis Theorem 6.3.2.1 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 ([13]). We will give the basics about Noetherian rings and modules and explain the link with linear algebra.

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

The common thread we use to illustrate 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 6.6.2.2.
2. Describe the map by giving an algorithmic way to decide when $A \equiv B$. This is achieved in 6.7.0.2.

To do that we have to study the equivalence class of $T \text{Id} - A$, $A \in M_n(\mathbf{k})$ in $M_n(\mathbf{R})$ where $\mathbf{R} = \mathbf{k}[T]$. To do that, we study the more general equivalence relation \sim on $M_{p,q}(\mathbf{R})$ for \mathbf{R} a PID (or for our concern, more specifically \mathbf{R} Euclidean ring is enough).

As before, we need to answer two questions

1. Describe $M_{p,q}(\mathbf{R})/\sim$ by giving a canonical representative in each similarity class. This is achieved in 6.4.2.2 (3).
2. Describe the map by giving an algorithmic way to decide when $A \sim B$. This is achieved in 6.4.2.2 (1).

6.3 Noetherian Modules

The image of a family of generators of a module through a morphism generates the image module. Thus, *every quotient of a finitely generated module is still finitely generated*. However, while a submodule of a finitely generated \mathbf{R} module is still finitely generated when \mathbf{R} is a field, this is generally not the case (cf 4.2.4). However, it is the case in a Noetherian setting.

Lemma 6.3.0.1. *Let M be an \mathbf{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 contraposition). 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. \square

Definition 6.3.0.2.

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) 6.3.0.3. 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!).

6.3.1 Stability under exact sequences

Proposition 6.3.1.1. 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 6.3.1.2. *The Noetherian modules over a Noetherian ring are exactly the finitely generated modules.*

Remark(s) 6.3.1.3. *Every Noetherian module is of finite presentation, meaning that there exists an exact sequence $R^m \xrightarrow{A} R^n \rightarrow M \rightarrow 0$. 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.*

6.3.2 Hilbert's Basis Theorem

Theorem 6.3.2.1. *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 (6.3.1.2). 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 $\mathbf{k}[T]$ 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 .

6.4 Gauss algorithm in PID and Euclidean rings

6.4.1 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 are cyclic. 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 6.4.1.1. *An integral ring R is said Euclidean if there exists a function $\delta : R^* \rightarrow \mathbf{N}$ such that for any $(a, b) \in R \times R^*$ there exists $q, r \in R$ such that $a = bq + r$ and $r = 0$ or $\delta(r) < \delta(b)$.*

Remark(s) 6.4.1.2. *The reader will check as an exercise that $R[T]$ is Euclidean if and only if \mathbf{k} is a field (exercise). But for any ring³, one can always perform the division of a polynomial by a monic polynomial: the division algorithm only uses that the leading term of the divisor is invertible. And the uniqueness of quotient and rest remain true. This straightforward remark is important as we will see in the sequel.*

Lemma 6.4.1.3. *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 $\delta(b)$ is minimal in $\delta(I - \{0\})$ (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 $\delta(r) < \delta(b)$. Then, $r = a - bq \in I$. By minimality of $\delta(b)$, one has $r = 0$ and $I \subset bR$. \square

Exercise(s) 6.4.1.4.

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

²We do not require the uniqueness of (q, r) .

³The commutativity assumption is even unnecessary in this monic situation. But of course, one has a left and a right division with quotient and rests who have no reason to be the same in this non commutative case.

Definition 6.4.1.5. 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 6.4.1.6 (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 a almost zero family $y_i \in R$ such that $\sum y_i x_i = 1$. We say in this case that the x_i 's are (globally) coprime

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

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

Proposition 6.4.1.7 (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(s) 6.4.1.8. Prove that any non zero prime ideal of a PID is maximal.

6.4.2 The general PID case

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 3.3.0.2 to prove the following proposition. We will need more than Gauss elementary operations in this case.

Definition 6.4.2.1. Two matrices are if they differ by a series of left and right multiplications by transvections and Bézout matrices $\text{diag}(A, \text{Id})$ with $A \in \text{SL}_2(R)$

We denote by \simeq the Bézout equivalence of matrices and by Ω the corresponding equivalence class of A . The main observation is that $(a, b) \simeq (\text{GCD}(a, b), 0)$ for any $a, b \in R$. Indeed, by Bézout theorem, there exists $u, v \in R \mid au + bv = \text{GCD}(a, b)$ 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 $A' = [a'_{i,j}] \in \Omega$ is extremal if one of its coefficient is maximal in the (nonempty) set of ideals $\mathcal{F} = \{(a'_{i,j}), A' \in \Omega\}$, the corresponding coefficient $a'_{i,j}$ being called an extremal coefficient.

Proposition 6.4.2.2.

1. A is Bézout equivalent to a diagonal matrix D with $(d_1) \subset (d_2) \subset \dots \subset (d_\nu)$.
2. The ideals (d_i) depends only on the equivalence classe of A . They are called the invariant ideals⁴ of A .
3. Two matrices are equivalent if and only if they have the same invariant ideals.
4. Equivalent matrices are Bézout equivalent. In particular the invariant factors of A are those of Id_n , they are equal to 1.

Proof.

- By functoriality of the cokernel (4.4.0.1), (2) and (3) are direct consequences of the computation of the cokernel of A 5.5.1.1 and the uniqueness statement 5.5.2.2. Then (4) is a direct consequence of (1) and (3).
- We are reduced to prove (1) by induction on $n + m$ starting with the obvious case $n + m = 2$.
- Transposing if necessary, one can assume $m \leq n = \nu \geq 1$. We define $\text{GCD}(A)$ as the ideal generated by its coefficients (which is precisely generated by a GCD of the coefficients!). We first observe that two equivalent matrices have the same GCD : if $A' = PA$ or $A' = AQ$, we have $\text{GCD}(A') \subset \text{GCD}(A)$ by the product matrix formula and therefore we have equality if P, Q are invertible.
- Assume first $n = 1$ (A is a line matrix). I claim that $A \simeq (d, 0, \dots, 0)$ with $\text{GCD}(A) = (d)$. This is true if $m = 1$ and, using the invariance of GCD by equivalence, is reduced by an immediate induction to the $m = 2$ case whic 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 $m = 1$.

⁴By 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.

- 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 $d_1 = a_{1,1}$ is extremal.

If $a_{1,j}, j > 1$ is not divisible by a_1 , then (d_1) is strictly contained in $(\text{GCD}(d_1, a_{1,j}))$. But using Bézout replacement, this contradicts the maximality of (d_1) .

Therefore, $d_1 | a_{1,j}$ and (same argument $d_1 | a_{i,1}$ for all i, j). By using usual Gauss operations, one can assume that $a_{1,j} = a_{i,1} = 0$ for all $i, j > 1$, without losing extremality as before.

- I claim that in this situation $d_1 | a_{i,j}$. If $i > 1$ say, the change $L_1 \mapsto L_1 + L_i$ changes L_1 to $(d_1, 0, \dots, 0, a_{i,j}, 0, \dots, 0)$ and therefore $d_1 | a_{i,j}$ by the preceding Bézout replacement argument. The matrix A is therefore of the form $d_1 \text{diag}(1, \bar{A})$ with $\bar{A} \in M_{n-1, m-1}(\mathbb{R})$ and we conclude by induction.

□

In this case, invariant ideals can be just computed using Gauss operations. We denote by \equiv the Gauss equivalence.

Let start with a general lemma

Lemma 6.4.2.3. *Let R be any ring and D an invertible diagonal matrix of $M_n(\mathbb{R})$. Then, $D \equiv \text{diag}(\det(D), \text{Id}_{n-1})$.*

Proof. 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 computations⁵)

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

□

6.4.3 The Euclidean case

Proposition 6.4.3.1. *With the notations of 6.4.2 assuming moreover that R is Euclidean, A is Gauss equivalent to a diagonal matrix D with $(d_1) \subset (d_2) \subset \dots \subset (d_\nu)$.*

Proof. Let $L = (a_0, a_1) \in R \times R^*$ and $a_0 = a_1 q_0 + a_2$ with $f(a_2) < f(a_1)$ or $a_2 = 0$. Using the Gauss operation $a_0 \mapsto a_0 - q_0 a_1$, we get $(a_0, a_1) \equiv (a_1, a_2)$ and we know $\text{GCD}(a_0, a_1) \equiv \text{GCD}(a_1, a_2)$. By induction, we construct a_i such that $(a_i, a_i + 1) \equiv (a_{i+1}, a_{i+2})$ with $\text{GCD}(a_i, a_i + 1) \equiv \text{GCD}(a_{i+1}, a_{i+2})$

⁵We indicate the pivot and the bold coefficient is the pivot

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

Corollary 6.4.3.2. *If R is Euclidean, every invertible matrix $M \in \text{GL}_n(R)$ is Gauss equivalent to $(\det(A), \text{Id}_{n-1})$.*

Proof. If M is invertible, we know (6.4.2.2) that there invariant factors are equal to 1 proving that R is Gauss equivalent to an invertible diagonal matrix and we apply lemma 6.4.2.3. In particular, $\text{SL}_n(R)$ is generated by transvections. \square

6.4.4 Minors and invariant ideals

Assume that R is a PID and 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 square matrix $(a_{i,j})_{i \in I, j \in J}$.

We define for $n \geq 1$

$$\delta_n(A) = \text{GCD}(\wedge^n(A))$$

where $\wedge^n A$ is the ideal generated by all minors of order n of A . For instance, if a square matrix A is triangular and invertible, we have $\delta_i(A) = 1$ for all i .

Lemma 6.4.4.1. *If*

$$D(\underline{P}) = \begin{pmatrix} \text{diag}(d_r, \dots, d_1) & 0_{r,q-r} \\ 0_{p-r,r} & 0_{p-r,q-r} \end{pmatrix} d_r | \dots | d_2 | d_1 \text{ monic}$$

then

$$\delta_n(A) = d_r \cdots d_{r-n+1}$$

with the convention here that $d_n = 0$ if $n \leq 0$.

Proof. All minors $D_{I,J}$ of $D = D(\underline{P})$ are triangular with at least one zero diagonal element if $I \neq J$. If $I = (i_1 > \dots > i_n)$, we have $\det(D_{I,I}) = d_{i_n} \cdots d_{i_1}$ if $n \leq r$ and is zero otherwise. If $n \leq r$, we have $i_j \leq r + 1 - j$ so that $d_r \cdots d_{r-n+1} | d_{i_n} \cdots d_{i_1}$ because of the decreasing property of d_i for divisibility. \square

Lemma 6.4.4.2. *Let $A, B \in M_{p,q}(\mathbb{R})$. If A and B are equivalent if and only if*

$$\delta_n(A) = \delta_n(B) \text{ for all } n \geq 0.$$

Proof. Since the determinant of a matrix is equal to that of its transpose, we have $\delta_n(A) = \delta_n({}^tA)$ for all n . It follows that it suffices to show that for any matrix $P \in M_{q,r}(\mathbf{k}[T])$ (whether invertible or not) we have

$$\wedge^n(AP) \subset \wedge^n(A).$$

The learned reader will invoke the general Binet-Cauchy formula

$$\det((AP)_{I,J}) = \sum_{K \mid \text{Card}(K)=n} \det(A_{I,K}) \det(d_{K,J})$$

for computing minors of a product of arbitrary matrices. But we don't need that precision. We can proceed as follows. 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 $\wedge^n(A)$ proving the direct implication.

The previous calculation in the diagonal case (6.4.4.1) is 6.4.2.2 and implies converse implication. \square

Example(s) 6.4.4.3. *Let $A \in M_n(\mathbf{k}[T])$ be a matrix such that $a_{i,j} = 0$ if $i > j + 1$ and $a_{i+1,i} = 1$:*

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

Then, the elementary divisors of A are $(1, \dots, 1, \det(A))$. Indeed, the $(n-1)$ minor A_{1^c, n^c} is upper triangular with diagonal entries equal to 1 showing $\delta_i(A) = 1$ for $i < n$ as already observed

Exercise(s) 6.4.4.4. *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 the pivot.*

Deduce another algorithm than the Gauss elimination algorithm to compute the invariants ideals of a diagonal matrix in $M_{p,q}(\mathbb{R})$.

6.5 Finite type modules over PID

Let us reap the benefits of our labor.

Theorem 6.5.0.1 (Structure theorem of finite type modules over PID). *Let M be a finite type module over a PID R .*

1. *Every submodule of M is of finite type.*
2. *There exists an exact sequence $R^m \xrightarrow{A} R^n \rightarrow M \rightarrow 0$ and M is polycyclic with invariant factors I_k the proper invariant ideals of A .*
3. *Two finite type R -modules are isomorphic if and only if they have the same invariant ideals.*
4. *For any exact sequence $R^m \xrightarrow{A} R^n \rightarrow M \rightarrow 0$, the proper invariant factors of A are the invariant ideals of M .*
5. *M is (non canonically) isomorphic to $M_{tors} \oplus R^r$ with $r = \text{rank}(M)$ and $M_{tors} \oplus_{I_k \neq 0} R/I_k$.*
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 $d_i e_i, i \leq r$ is a (so called adapted) basis of N .*

Proof. All the proofs have been given. Precisely.

1. R is Noetherian and so is M (6.3.1.2).
2. The existence of the exact sequence comes from 6.3.1.3. We know that A is equivalent to a diagonal matrix (6.4.2.2). Its cokernel is therefore polycyclic (5.5.1.1) by functoriality of the cokernel (4.4.0.1).
3. Special case of unicity of invariant ideals of polycyclic modules (5.5.2.2).
4. The proof of (2) is valid for any such exact sequence.
5. If I_k are the invariant factor, we have $M \xrightarrow{\sim} \oplus R/I_k$. Therefore the torsion part M_{tors} is isomorphic to the torsion part of $\oplus R/I_k$ which is $\oplus_{I_k \neq 0} R/I_k$. Then r is the number of zero ideals among the I_k 's.
6. Direct consequence of the preceding point
7. Direct consequence of the previous item and of 3.2.0.1.

8. By choosing basis of M and N , the inclusion $N \rightarrow M$ becomes $R^r \xrightarrow{A} R^n$ with $A \in M_{n,r}(R)$ an injective matrix. Therefore, there exists D diagonal and P, Q invertible with $A = PDQ$ (6.4.2.2). 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 $d_i = D_{i,i}$.

□

Exercise(s) 6.5.0.2. *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. 5.3.1.2)⁶.*

Corollary 6.5.0.3 (Structure theorem of finite type abelian groups). *Let G be a finite type abelian 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. □

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



The main theorem 6.5.0.1 has a version of 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 (4.2.4).

6.6.1 Similarity invariants

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

Corollary 6.6.1.1 (Similarity invariants of vector space endomorphisms).

1. *The torsion $\mathbf{k}[T]$ -module V_a is a torsion module.*
2. *There exists a unique sequence of monic polynomials $P_n | \dots | P_1$ (the similarity invariants of a) such that $V_a \cong \bigoplus_i \mathbf{k}[T]/(P_i)$.*
3. *a and b are similar if and only if there similarity invariant are equal.*

Proof.

⁶As we will see, this result is true for all PID (7.3.2.2).

1. 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 $\text{End}_{\mathbf{k}}(V)$).
2. By the previous theorem applied to $R = \mathbf{k}[T]$ and $M = V_a$, there exists a unique sequence $P_r | \dots | P_1$ or non-constant polynomials such that $V_a \xrightarrow{\sim} \mathbf{k}[T]/(P_i)$. By a dimension (of vector spaces) argument, we have $r \leq n$. We define $P_i, r < i \leq n$ by $P_i = 1$.
3. By 4.2.4.1, the similarity of a and b is equivalent to $V_a \xrightarrow{\sim} V_b$ whose invariant ideals are precisely the non constant similarity invariants of a and b .

□

6.6.2 Explicit computations of similarity invariants

We keep in mind the notations and result of 4.3.2. Let $(e_i), 1 \leq i \leq n$ be a basis of V and A the matrix of a in this basis. The map $(P_i(T) = \sum_j P_{i,j} T^j) \mapsto \sum_{i,j} P_{i,j} e_i T^j$ is an isomorphism of $\mathbf{k}[T]$ -modules $(\mathbf{k}[T])^n \xrightarrow{\sim} V[T]$ and the exact sequence $0 \rightarrow V[T] \xrightarrow{T\text{Id}-a} V[T] \xrightarrow{\pi_a} V_a \rightarrow 0$ becomes

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

Because $\det(T\text{Id}-A) = \chi_a(T)$ is non zero, all the invariant ideals of the size n matrix $T\text{Id}-A$ are non zero and are generated by the non constant diagonal terms of any $D \in M_n(\mathbf{k}[T])$ equivalent to $T\text{Id}-A$ (6.4.2.2).



Exercise(s) 6.6.2.1. If \mathbf{k} is infinite, prove that V_a is cyclic if and only if it V has a finite number of subspaces stable by a (cf. 6.5.0.2).

Corollary 6.6.2.2. Let $A, B \in M_n(\mathbf{k})$ be the matrices of $a, b \in \text{End}_{\mathbf{k}}(V)$ in some basis. If $P_i, 1, \leq i \leq n$ are the similarity invariant of a , then $T\text{Id}-A$ is Gauss equivalent to $\text{diag}(P_i)$ and $V_a \xrightarrow{\sim} \bigoplus \mathbf{k}[T]/(P_i)$. Moreover, the following conditions are equivalent.

1. A and B are similar in $M_n(\mathbf{k})$.
2. $T\text{Id} - A$ and $T\text{Id} - B$ are equivalent in $M_n(\mathbf{k}[T])$.
3. The $\mathbf{k}[T]$ -modules V_a and V_b are isomorphic.

We get then the following relations between the similarity invariants.

Corollary 6.6.2.3. *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 irreducible factors (and hence the same roots in any extension of \mathbf{k}).
3. $P(a) = 0$ if and only if $P_1 | P$. In other words, μ_a is the minimal polynomial of a .

Proof.

1. There exists $Q, Q' \in GL_n(\mathbf{k})$ such that $T\text{Id} - A = Q \text{diag}(P_i) Q'$. Because $\det(P) \in \mathbf{k}^*$, their determinant $\chi_a(T)$ and $\prod P_i(T)$ differ by a multiplication by a scalar which is 1 because both polynomials are monic.
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) 6.6.2.4.

- Notice that the above proposition 6.6.2.3 proves the very existence of μ_a without any previous knowledge. By construction, it is the unique monic polynomial of least degree annihilating a .
- The interested reader can check that we didn't use the Cayley-Hamilton theorem (3.1.2.2) 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 6.7.0.3), the last P_i are often equal to 1. They contribute by the zero module to V_a .

- Unlike the polynomial characteristic, the similarity invariants does 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 $t = 0$.



Finally, let us give two classical results.

Corollary 6.6.2.5. *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, \bar{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 \bar{P}_i , we have also $T \text{Id} - A \simeq \text{diag}(\bar{P}_i)$ in $M_n(K)$. By uniqueness, we get $P_i = \bar{P}_i$, hence the result.

□

6.7 Frobenius Decomposition



Ferdinand Georg Frobenius

We will rephrase the previous results in terms of companion matrices providing a canonical representative $C(\underline{P})$ in each similarity class \bar{A} .

Definition 6.7.0.1. *Let $P = T^n + \sum_{i=0}^{n-1} a_i T^i \in \mathbf{k}[T]$ and $\underline{P} = (P_n, \dots, P_1)$ be a sequence of monic polynomials.*

1. *The companion matrix $C(\underline{P})$ of \underline{P} is*

$$C(\underline{P}) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in M_n(\mathbf{k}).$$

Thus, $C(\underline{P})$ is the empty matrix if $P = 1$

2. The generalized companion matrix $C(\underline{P}) = \text{diag}(C(P_i))$. Its size $\sum \deg(P_i)$.

Theorem 6.7.0.2 (Frobenius Reduction). *Let $\underline{P} = (P_n | \cdots | P_1)$ be a sequence of unitary polynomials of $\mathbf{k}[T]$ with $\sum \deg(P_i) = n$ and $P_n | \cdots | P_1$ and $A \in M_n(\mathbf{k})$. Then, $A \approx C(\underline{P})$ if and only if \bar{P} is the sequence of similarity invariants of A .*

Proof. Let $W = \oplus \mathbf{k}[T]/(P_i)$ and $b \in \text{End}_{\mathbf{k}}(W)$ be the multiplication by T . We have $W_b = \oplus \mathbf{k}[T]/(P_i)$ as $\mathbf{k}[T]$ -module and therefore the similarity family of similarity invariants of b is \underline{P} (5.5.2.2).

Let $V = \mathbf{k}^n$ and $a = C(\bar{P}) \in \text{End}_{\mathbf{k}}(V)$. Let $\mathcal{B} \sqcup \mathcal{B}_i$ where \mathcal{B}_i is the \mathbf{k} -basis $(1, T, \dots, T^{\deg(P_i)-1}) \pmod{(P_i)}$ of $\mathbf{k}[T]/(P_i)$.

We have $\text{Mat}_{\mathcal{B}}(a) = C(\underline{P})$. In other words, if $f \in \text{Hom}_{\mathbf{k}}(V, W)$ mapping \mathcal{B} to the canonical basis of \mathbf{k}^n , we have $a = f^{-1} \circ b \circ f$ and therefore $V_a \xrightarrow{\sim} W_b$ (4.2.4.1). In other words, the family of similarity invariants of $C(\underline{P})$ is \underline{P} . We conclude by 6.6.1.1. \square

Using 5.3.1.1, we get the more or less classical result in the case of a unique companion block $C(P)$

Corollary 6.7.0.3. *Let $a \in \text{End}_{\mathbf{k}}(V)$. The following statements are equivalent⁷:*

1. *The matrix of A in a suitable basis is the companion matrix $C(P)$.*
2. $\mu_a = \chi_a = P$.
3. *The similarity invariants are $1, \dots, 1, P$.*
4. V_a and $\mathbf{k}[T]/(P)$ are isomorphic $\mathbf{k}[T]$ -modules.
5. V_a is cyclic as ($\mathbf{k}[T]$ -module) and $\mu_a = P$.

Using 5.3.1.1 again, an equivalent formulation of the Frobenius reduction theorem 6.7.0.2 is

Theorem 6.7.0.4 (Frobenius Decomposition). *Let $\underline{P} = (P_n | \cdots | P_1)$ be a sequence of unitary polynomials of $\mathbf{k}[T]$ and $a \in \text{End}_{\mathbf{k}}(V)$. Then, if \underline{P} is the sequence of similarity invariants of a , there exists a direct sum decomposition $V_a = \sum V_i$ into cyclic modules with $\text{Ann}_{\mathbf{k}[T]}(V_i) = (P_i)$. Conversely, if such a decomposition exists, then \underline{P} is the similarity invariant sequence of a .*

⁷This also equivalent for infinite fields that V has a finite number of subspaces stable by a (6.6.2.1).

6.8 Application: Commutant

It is then easy to study the commutant (see 4.2.4.1)

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

for example, to calculate its dimension.

Proposition 6.8.0.1. *The dimension of the commutant of a is $\sum (2i - 1) \deg(P_i)$. In particular, $\dim \text{End}_{\mathbf{k}[\mathbb{T}]}(V_a) \geq n$ with equality if and only if a is cyclic.*

Proof. We have

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

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

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

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

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

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

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

We therefore have

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

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

Exercise(s) 6.8.0.2 (Bicommutant, difficult). *Show that the inclusion $\mathbf{k}[a]$ in his bicommutant, that is the set of endomorphisms that commute with all elements of $\text{End}_{\mathbf{k}[\mathbb{T}]}(V_a)$, is an equality.*

6.9 Summary

Collating what we have proved, we have the following results which was wanted in 6.2.

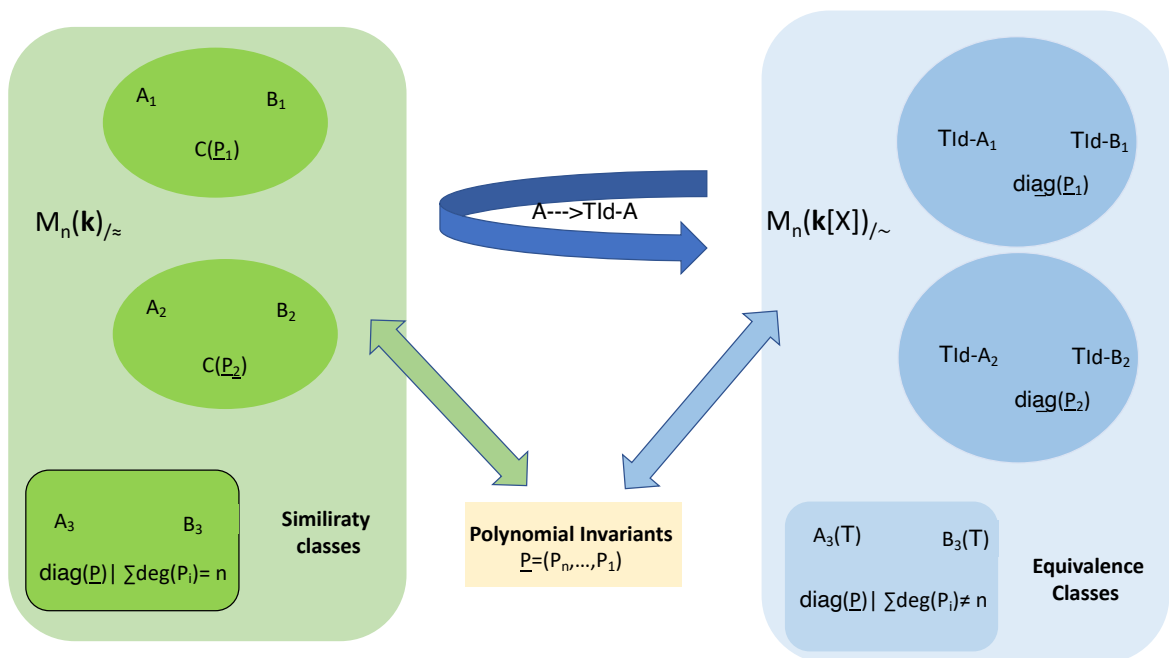
Let $A, B \in M_n(\mathbf{k})$ and $\underline{P} = (P_n | \dots | P_1)$ a family of monic polynomials.

- A and B are similar if and only if they have the same similarity invariants.
- The family of similarity invariants of $C(\underline{P})$ is \underline{P} .

If \underline{P} is the family of similarity invariants of A , we have:

- A and $C(\underline{P})$ are similar.
- $V_A \simeq \oplus \mathbf{k}[T]/(P_i)$ where A also denotes the endomorphism of $V = \mathbf{k}^n$ associated.
- $T \text{Id} - A$ is equivalent to $\text{diag}(P_1, \dots, P_n)$.
- \underline{P} is calculated by Gauss elimination by "diagonalizing" $T \text{Id} - A$ in $M_n(\mathbf{k}[T])$.
- We have $\chi_A = P_1 \dots P_n$ and $P_1 = \mu_A$.
- The similarity invariants of $C(P)$ are $(1, \dots, 1, P)$.

The proof strategy is illustrated by the following diagram.



6.10 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 $GL_n(R)$ 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 $GL_n(R)$ as the subgroup of $GL_{n+1}(R)$ consisting of block diagonal matrices of the form $\text{diag}(M, 1)$, where $M \in GL_n(R)$. This allows us to consider their infinite union $GL(R)$, seen as the set of matrices of infinite size, containing all finite-sized linear groups. We then define $E(A)$ as the subgroup of $GL(A)$ generated by all transvections with determinant 1 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 [12].

Lemma 6.10.0.1 (Whitehead). *For any ring R , the group $E(R)$ is the derived group $[GL(R), GL(R)]$ generated by the commutators $[A, B] = ABA^{-1}B^{-1}$ of matrices in $GL(R)$.*

In particular, $E(A)$ is a normal subgroup, and the quotient $K_1(R) = GL(R)/[GL(R), GL(R)]$ is a commutative group, as it is the abelianization of $GL(R)$! This is the group of algebraic K-theory of degree 1. As the determinant of any commutator is 1, the determinant map passes to the quotient (5.2) to define the special group of algebraic K-theory of degree 1:

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

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

$$R^\times \times SK_1(R) \rightarrow K_1(R),$$

which is visibly an isomorphism.

The group $SK_1(R)$ is evidently the obstruction to the Gauss elimination algorithm (infinite) being able to diagonalize matrices. And our results prove that if R is Euclidean, $SK_1(R) = 0$. It is noteworthy that this obstruction is very sudden. For example, in the case of the non-Euclidean principal ring $R = \mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$, we have $SK_1(R) = \{1\}$ (this follows from a general deep theorem about so-called Dedekind rings, [1]). 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 R such that $\text{SK}_1(R)$ is non-trivial is difficult. An example is given in [9]: 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.

6.11 Supplementary Exercises

Exercise(s) 6.11.0.1. 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(s) 6.11.0.2. 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(s) 6.11.0.3. 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(s) 6.11.0.4. Transform the proof of 6.4.3.1 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(s) 6.11.0.5. 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(s) 6.11.0.6. 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 $A_0 : R_0^n \rightarrow R_0^m$ defied by A has the same property.
3. Give another proof of (2) and (4) of 3.2.0.1.
4. Using 6.11.0.5, give another proof of (3) and (4) of 3.2.0.1.

Example(s) 6.11.0.7. Prove that $\mathbf{R}[T]$ is a PID if and only if \mathbf{R} is a PID.

Exercise(s) 6.11.0.8. Let \mathbf{R} be an integral ring \mathbf{K} its with fraction field \mathbf{K} . Prove that the \mathbf{R} -module \mathbf{K} is free if and only if \mathbf{R} is a field and therefore if and only if $\mathbf{R} = \mathbf{K}$. Deduce that if \mathbf{R} is a PID, \mathbf{K} is torsion free but not free as a \mathbf{R} -module.

Exercise(s) 6.11.0.9. 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(s) 6.11.0.10. 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 there exist $q, r \in \mathbf{A}$ such that $N(r) < N(b)$ and $a = bq + r$.
9. Prove that if $v \in [n + \frac{1}{3}, n + \frac{2}{3}]$, there exist $q, r \in \mathbf{A}$ such that $N(r) < N(b)$ and

$$2a = bq + r$$

10. Conclude.

Exercise(s) 6.11.0.11. 1. Give an algorithm to solve a finite number of linear equations with integral coefficients and test in a suitable computer language like Python.

2. Solve the system

Base adaptée et équation diophantienne TBD

Exercise(s) 6.11.0.12. 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 π is a projector of image R^G .
2. Show that π is R^G linear.
3. Show that if R is Noetherian, R^G is Noetherian.

Exercise(s) 6.11.0.13. 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 ?].

Part II

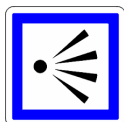
Linear Algebra over Fields

Chapter 7

The Irreducible Toolbox



7.1 Perspective



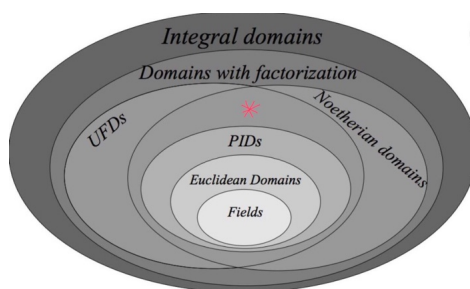
Blabla

7.2 Introduction

In this chapter, R denotes a *domain*, i.e. a ring (commutative with unity as usual) and \mathbf{k} is its field of fractions.

7.3 An UFD Criterion

Definition 7.3.0.1. We say that $r \in R^*$ is *irreducible* if it is non-invertible and if the equation $r = r_1 r_2$ implies r_1 or r_2 is invertible, that is all divisors of d are equal to 1 or d up to multiplication by an invertible.



Notice that whether r is irreducible only depends on (r) , i.e., it is invariant by multiplication by an invertible.

Example(s) 7.3.0.2.

- 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*).

7.3.1 Uniqueness Condition

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

Lemma 7.3.1.1. *Let $r \in R^*$. If the ideal (r) is prime then r is irreducible.*

Proof. If $r = r_1 r_2$, the product $r_1 r_2$ is zero in $R/(r)$ which by definition is integral. Hence, the class $(r_1 \bmod r)$ for example is zero so that $r = \rho_1 r$ and $r = \rho_1 r r_2$. Simplifying by r (integrity), r_2 is invertible. \square

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

Definition 7.3.1.2 (Euclid's Property). *We say (by abuse) that Euclid's lemma is true in R if the ideal generated by an irreducible is prime, that is if any irreducible dividing a product divides one of the factors.*

The following lemma is well known

Lemma 7.3.1.3. *Euclide's lemma is true for PID.*

Proof. Let $r, r_1, r_2 \in R^*$ with $r|r_1r_2$ irreducible and let $d = \text{GCD}(r, r_1)$. Because $d|r$ and r irreducible, up to R^\times , we have $d = 1$ or $d = r$. In the second case, we have done because $r \sim d|r_1$ by definition. In the first case, we apply Gauss lemma for PID (6.4.1.7) and we get $r|r_2$. \square

Definition 7.3.1.4. *Let R be a domain. A domain is said to be a Unique Factorization Domain (UFD) if*

1. *every non-zero element has a unique decomposition $r = u \prod_{i=1}^n p_i$ with $u \in R^\times$ and p_i irreducible;*
2. *if $r = u' \prod_{i=1}^{n'} p'_i$, with $u' \in R^\times$ and p'_i irreducible is another decomposition, then, $n = n'$ and, with renumbering, $(p_i) = (p'_i)$.*

The link with what precedes is

Lemma 7.3.1.5 (Uniqueness Lemma). *Assume every non-invertible 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 r be irreducible. Then (r) is nonzero like r . Suppose we have a decomposition $r = r_1r_2$. We decompose each r_i into irreducibles $r_i = u_i \prod_{j=1}^{n_i} p_{i,j}$ giving $r = u_1u_2 \prod_{i,j} p_{i,j}$. Thus, we have two decompositions of r 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 r_1 is invertible.

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 $p_{1,1} | \prod_{j=1}^{n_2} p_{2,j}$. 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 7.3.1.6. *The number of divisors of a nonzero element of an UFD is, up to multiplication by \mathbf{R}^\times , finite.*

7.3.2 Existence Criterion

Lemma 7.3.2.1. *Every nonzero and non-invertible element in a Noetherian domain \mathbf{R} is a product of irreducible elements.*

Proof. Then, let \mathcal{F} be the set of proper and nonzero principal ideals (r) of \mathbf{R} with r is not a product of irreducible elements. If \mathcal{F} were non-empty, it would have a maximal element $(r) \in \mathcal{F}$ for inclusion. But r is not irreducible because otherwise $(r) \notin \mathcal{F}$, so r can be written $r_1 r_2$ with r_1 and r_2 non-invertible. Thus $(r) \subsetneq (r_i)$. By maximality, $(r_i) \notin \mathcal{F}$ so that each r_i is a product of irreducibles, and so is their product r . A contradiction. \square

Corollary 7.3.2.2. *An integral Noetherian domain is UFD if and only if it satisfies Euclid's Property. In particular, PIDn are UFD and therefore the number of divisors of a nonzero element of an PID is finite up to multiplication by \mathbf{R}^\times (7.3.1.6)*

Corollary 7.3.2.3. *A PID is UFD. .*

Notice that lemma 7.3.2.1 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 $\mathbf{R}[T, Y]/(T^2 - Y^3)$ is Noetherian, obviously integral (exercise). Yet, the element $T^2 = Y^3$ of the quotient has two decompositions (non-equivalent, **exercise**) because both T and Y are irreducible in the quotient .

Corollary 7.3.2.4. *The ring $\overline{\mathbf{Z}}$ of complex algebraic integers over \mathbf{Z} is neither Noetherian nor UFD.*

Proof. We already know that $\overline{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$ therefore $\overline{\mathbf{Z}}$ is not a field (because $1/2 \notin \overline{\mathbf{Z}}$ for instance). If $\overline{\mathbf{Z}}$ were noetherian, there would exist at least one irreducible element p 7.3.2.1. But $\sqrt{(p)} = T^2 - p$ and therefore the subring of $\mathbf{Z}[p, \sqrt{p}]$ of \mathbf{C} is of finite type over \mathbf{Z} proving $\sqrt{p} \in \overline{\mathbf{Z}}$. The formula $p = (\sqrt{p})^2$ contradicts the irreducibility of p . \square

By invoking the existence of decompositions in the Noetherian case (7.3.2.1 and Euclid Property for principal ideal domain (7.3.1.3), we get

7.4 Transfer

We now demonstrate the following UFD transfer theorem to polynomial rings

Theorem 7.4.0.1. *If R is UFD, then $R[T]$ is UFD.*

We must therefore demonstrate the uniqueness of decompositions (thus Euclid's lemma) and their uniqueness. For this, we will compare the notion of irreducibles in $R[X]$ and $\mathbf{k}[X]$ using the notion of content (due to Gauss). We will use 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 5.7.0.7 for the general case).

7.4.1 GCD, LCM in UFD

Let (r_i) be a finite family of elements of R which we will assume are not identically zero. Recall that an element $r \in R^*$ is a GCD of the r_i if it is maximal among the common divisors to the r_i . Two GCDs of the same family, when they exist, are of course associated, which is why we speak of the GCD. Therefore, we can consider the GCD, LCM as elements of the monoid R/\sim . Considering maximal common multiples, we obtain the notion of LCM. As with integers, we have

Lemma 7.4.1.1. *If R is UFD, the GCD and the LCM of the (r_i) exist.*

Proof. Consider decompositions into irreducible factors of each of the $r_i \neq 0$ and let q_j be a family of irreducibles not associated with each other so that all these factors are associated with exactly one of the p_i . We can then write uniquely

$$r_i = u_i \prod_j q_j^{v_{i,j}}, \quad v_{i,j} \geq 0 \text{ and } u_i \in R^\times.$$

We then define

$$\text{GCD}(r_i) = \prod_j q_j^{\min_i(v_{i,j})} \text{ and } \text{LCM}(r_i) = \prod_j q_j^{\max_i(v_{i,j})}$$

which are verified to be suitable. □

Note that GCD and LCM are homogeneous of weight 1 for multiplication by R^* .

Exercise(s) 7.4.1.2. *Show that if R is principal, the $\text{GCD}(r_i)$ is a generator of the ideal generated by the (r_i) . Provide a characterization of the LCM in terms of ideals.*

7.4.2 Content

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

Definition 7.4.2.1. Let $P \in R[T]$ be nonzero. We define the content $c(P)$ of P as the GCD $\in (R/\sim)$ of its coefficients¹. A polynomial with content $c(P) \sim 1$ is said to be primitive.

For example, monic polynomials of $R[T]$ are primitive. The content is homogeneous of weight 1 under multiplication by nonzero element like the GCD.

Theorem 7.4.2.2 (Gauss). Let P, Q be nonzero polynomials of $R[T]$. Then, $c(PQ) \sim c(P)c(Q)$.

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 $R[T] \rightarrow R/(p)$ 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 $c(P) \sim 1$. \square

Corollary 7.4.2.3. The irreducibles of $R[T]$ are

1. The irreducibles of R ;
2. Primitive polynomials of $R[T]$ that are irreducible in $\mathbf{k}[X]$.

Proof. Recall the equality $(R[T])^* = R^\times$. The first point follows immediately for reasons of degree.

If P is irreducible in $R[T]$ of degree > 0 , it is certainly primitive according to the first point.

Suppose it is the product of two polynomials $\tilde{P}_1, \tilde{P}_2 \in \mathbf{k}[T]$. By reducing to a common denominator $d_i \in R^*$ for the coefficients of \tilde{P}_i , we can write $\tilde{P}_i = P_i/d_i$ with $P_i \in R[X]$. 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. As P is irreducible in $R[T]$, we deduce for example $P_1/c(P_1)$ is invertible, thus of degree zero, and therefore the same for \tilde{P}_1 which is proportional to it by a scalar. Hence the irreducibility in $\mathbf{k}[T]$.

The converse is tautological (who can do more can do less) \square

¹Let's emphasize that $c(P)$ belongs to R/\sim , i.e. is only defined up to multiplication by a unit.

7.4.3 The Transfer Theorem

Theorem 7.4.3.1. *If R is UFD, then so is $R[T]$.*

Proof. Because the defining properties of UFD are invariant under multiplication by a unit of R^\times , for simplicity we simply write by an equality an equality up to R^\times .

Existence of decomposition. Let $P \in R[X]$ be non-zero. If P is a constant $r \in R^*$, we write the decomposition $r = \prod p_i$ into irreducible factors in R and invoke (7.4.2.3).

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 7.4.2.3, a common denominator argument then allows us to write its decomposition in the principal therefore UFD $\mathbf{k}[X]$

$$P = \prod P_i/d_i$$

with $P_i \in R[T]$ irreducible in $\mathbf{k}[T]$ 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 of decomposition in $R[T]$. Let's demonstrate that $R[T]$ satisfies Euclid's lemma (7.3.1.2). 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 (7.4.2.3). 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 $R[T]$. \square

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.

Exercise(s) 7.4.3.2. *Show that the ring $\mathbf{R}[X, Y]/(X^2 - Y^3)$ is integral, Noetherian but not UFD.*

7.5 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 7.5.0.1. *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 7.5.0.2. *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 coefficients polynomial is an integer coefficient polynomial (6.4.1.2) to conclude this is also true for $d = n$. \square

But we have in our case the transfert theorem

Lemma 7.5.0.3 (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 (7.4.3.1) with $R = \mathbf{Z}$. \square

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 7.5.0.4).

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

Exercise(s) 7.5.0.4. *Show that $x \in \mathbf{Q}$ is an integer over \mathbf{Z} if and only if it is in \mathbf{Z} .*

Gauss's Lemma 7.5.0.3 for polynomials immediately gives the following result.

Corollary 7.5.0.5. *The minimal polynomial of an algebraic integer has integral coefficients.*

Then:

Theorem 7.5.0.6. *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 7.5.0.7. *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 7.5.0.5. $P(T)$ 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 7.5.0.6.

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

7.6 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 .



7.6.1 Primary Decomposition

Definition 7.6.1.1. Let $(p) = \mathfrak{p} \in \mathcal{P}$. The \mathfrak{p} -primary part (or p -primary part) of M is the submodule $M[\mathfrak{p}] = M[p] = \{x \in M \mid \exists n \geq 0\} p^n x = 0\}$.

Proposition 7.6.1.2. Let $f : M \rightarrow N$ be a morphism of torsion modules and $\prod p_i^{n_i}$ be the decomposition of $x \in R^*$ into distinct primes ($(p_i) \neq (p_j)$ if $i \neq j$).

1. For all j , there exists $\varepsilon_j \in (\prod_{i \neq j} p_i^{n_i})$ such that $\sum_j \varepsilon_j = 1$.
2. The natural map $\bigoplus_{\mathfrak{p} \in \mathcal{P}} M[\mathfrak{p}] \rightarrow M$ is an isomorphism.
3. For any $\mathfrak{p} \in \mathcal{P}$, we have functoriality of primary components meaning that the natural diagram

$$\begin{array}{ccc} \bigoplus_{\mathfrak{p} \in \mathcal{P}} M[\mathfrak{p}] & \longrightarrow & M \\ \downarrow & & \downarrow \\ \bigoplus_{\mathfrak{p} \in \mathcal{P}} N[\mathfrak{p}] & \longrightarrow & N \end{array}$$

4. If $xM = \{0\}$, the scalar multiplication by ε_i is the projection $\pi_i : M \xrightarrow{\sim} \bigoplus_i M[p_i] \rightarrow M[p_i] \hookrightarrow M$. Moreover $\sum \pi_i = \text{Id}_M$ and $\pi_i \circ \pi_j = \delta_{i,j} p_i$.

Proof. This is a direct consequence of the "more general" statement.

Lemma 7.6.1.3 (PID Splitting Lemma). Let $f : M \rightarrow N$ be a morphism of modules. Assume that M and N are canceled by $x = \prod x_i$ with $\text{GCD}(x_i, x_j) = 1$ if $i \neq j$.

1. If $x, y \in R^*$ are coprime then for any $n, m > 0$, $\text{GCD}(x^n, y^m)$.
2. For all j , there exists $\varepsilon_j \in (\prod_{i \neq j} x_i)$ such that $\sum_j \varepsilon_j = 1$.
3. The natural map $\bigoplus_i \text{Ann}_M(x_i) \rightarrow M$ is an isomorphism.

4. For any i , the natural diagram

$$\begin{array}{ccc} \oplus_i \text{Ann}_M(x_i) & \longrightarrow & M \\ \downarrow & & \downarrow \\ \oplus_i \text{Ann}_N(x_i) & \longrightarrow & M \end{array}$$

5. The scalar multiplication by ε_j is the projection $\pi_j : M \xrightarrow{\sim} \oplus_i \text{Ann}_M(x_i) \rightarrow \text{Ann}_M(x_i) \hookrightarrow M$.
Moreover $\sum \pi_i = \text{Id}_M$ and $\pi_i \circ \pi_j = \delta_{i,j} x_i$.

Proof.

1. By the Newton formula in \mathbb{R} , $(au + bv)^{n+m}$ can be written $a^n U + b^m V$ which proves (1) by Bézout's theorem.
2. This is (1) of the Chinese Remainder Lemma because $\text{GCD}(x_i, x_j)$ if $i \neq j$.
3. Let $m_i \in \text{Ann}_M(x_i)$. With the notation of (2), $m_i = \sum_j \varepsilon_j m_i = \varepsilon_i m_i$ because $x_i | \varepsilon_j$ if $j \neq i$. For the same reason, $\varepsilon_j m_i = 0$ if $j \neq i$.

Injectivity. If $\sum m_i = 0$, by multiplying by ε_j , we have $m_j = \varepsilon_j m_j = -\sum_{i \neq j} \varepsilon_j m_i = 0$ hence the injectivity.

Surjectivity. Let $m \in M$ and define $m_i = \varepsilon_i m$. Because $x_i | \varepsilon_i x_i$, we have $m_i \in \text{Ann}_M(x_i)$ and m is the wanted preimage..

4. Clear.

5. Direct consequence of the previous relations $\varepsilon_j m_i = \delta_{i,j} m_i$ for $m_i \in \text{Ann}_M(x_i)$ and $1 = \sum \varepsilon_i$.

□

□

Example(s) 7.6.1.4. Let $a \in \text{End}_{\mathbf{k}}[V]$ and $P, Q \in \mathbf{k}[T]$ coprime polynomials. Applying lemma 7.6.1.3 to V_a , we get the famous "kernel lemma²" $\text{Ker}(PQ(f)) = \text{Ker}(P(a)) \oplus \text{Ker}(Q(a))$.

7.6.2 Invariant Ideals and Primary Decomposition

Assume moreover that M is of finite type with (non zero) invariant ideals $(d_1) \subset \cdots \subset (d_n) \neq R$ and let

$$d_1 = \prod_{j=1}^r p_j^{d_{1,j}}$$

²This terminology is only French Universal.

a prime decomposition with $(p_i) \neq (p_j)$ if $i \neq j$. Then, up to unit, each d_i can be uniquely written

$$d_i = \prod_{j=1}^r p_j^{d_{i,j}} \text{ with } d_{1,j} \geq d_{2,j} \cdots \geq d_{r,j} \geq 0.$$

By the Chinese Remainder Lemma, we get

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

Conversely, assume that we have some direct sum decomposition

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

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

$$d_i = \prod_{j=1}^r p_j^{d_{i,j}}.$$

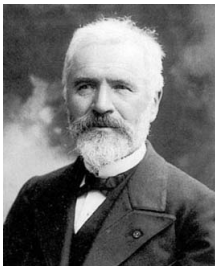
The sequence of ideals (d_i) is decreasing and its proper terms are the invariant ideals of M .

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,

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

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

7.7 Application: Jordan Reduction



Camille Jordan

Let us explain why the Frobenius reduction and the primary decomposition of V_a immediately leads to the Jordan reduction of endomorphisms $a \in \text{End}_{\mathbf{k}}(V)$ under the assumption that the characteristic polynomial χ_a is split. 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 $\sum d_i = n$.

³see 6.6.2.3

Definition 7.7.0.1. 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

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

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

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

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 7.6.2, we get

Theorem 7.7.0.2 (Jordan Reduction). Under the assumptions and notations above, we have:

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 $T^{d_n}, T^{d_{n-1}}, \dots, T^{d_1}$.

7.7.1 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

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

Let's perform elementary operations according to the algorithm - or rather its outline - described in the proof of the proposition 6.4.2.2 :

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

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 $T\text{Id} - M$ 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.

7.8 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 7.8.0.1 (Thanks to O. Debarre). *There exists an algorithm for computing such a P .*

Proof. We can perform the divisions by monic (here of degree one) in $\mathcal{R}[T]$ with $\mathcal{R} = M_n(\mathbf{k}[T])$

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

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

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

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 $(\text{TId} - B)\tilde{Q}_0 = P_0(\text{TId} - A)$ (argue by contradiction and look at the highest degree term). The equality of the coefficients of T gives $\tilde{Q}_0 = P_0$, that of the constant coefficients gives $B\tilde{Q}_0 = P_0A$. It remains to show that \tilde{Q}_0 is invertible. We perform another division in $\mathcal{R}[T]$

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

and we write

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

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

7.9 Supplementary Exercises

Exercise(s) 7.9.0.1. 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 $M_n(\mathbf{R})$)?

Chapter 8

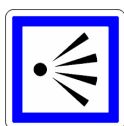
Diagonalization and Semisimplicity



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.

8.1 Perspective



8.2 Diagonalization

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, $a \in \text{End}_k(V)$ si 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 if diagonalizable if its matrix in an arbitrary matrix is similar to a diagonal matrix. The invariant similarity theory allows to quickly recover the following facts.

Proposition 8.2.0.1. *The following assertions are equivalent.*

1. a is diagonalizable.
2. a is cancelled by some non zero $P \in \mathbf{k}[T]$ which is split with $\text{GCD}(P, P') = 1$.
3. 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 .
5. The primary components $V_a[T - \lambda] = \text{Ker}(a - \lambda \text{Id})^{d_\lambda}$ of V_a are (7.7) are the eigenspaces $\text{Ker}(a - \lambda \text{Id})^{d_\lambda}$.

Proof. We prove $(1) \Rightarrow (2) \cdots \Rightarrow (5) \Rightarrow (1)$.

- $(1) \Rightarrow (2)$. 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 .
- $(2) \Rightarrow (3)$. $\mu_a | P$.
- $(3) \Rightarrow (4)$. Each similarity invariant of P_i divides P and therefore is a product of distinct linear factors. The primary decomposition of V_a is therefore isomorphic to a direct sum $\oplus \mathbf{k}_\lambda$ (7.6.2) (one factor for each factor $T - \lambda$ dividing a P_i).
- $(4) \Rightarrow (5)$. By definition, $1 \in \mathbf{k}_\lambda$ is an eigenvector of T with eigenvalue 1 and therefore the some of these dimension 1 spaces for a given λ is the eigenspace $\text{Ker}(a - \lambda \text{Id})$. It is by definition the $(T - \lambda)$ -primary component because $T - \lambda$ acts by $\mu - \lambda \neq 0$ on \mathbf{k}_μ if $\mu \neq \lambda$.
- $(5) \Rightarrow (1)$. V_a is always the direct sum of its primary components.

□

Corollary 8.2.0.2. *Let W be a subspace of V which is stable by a which is diagonalizable.*

1. Then, the restriction $a|_W$ is diagonalizable and W has a complement which is stable by a .
2. Conversely, if χ_a is split and if any stable subspace has a stable complement then a is diagonalizable.

Proof.

1. $a|_W$ is cancelled by μ_a which is split without square factors by (3) of 8.2.0.1 implying it is diagonalizable by (2) of 8.2.0.1. By functoriality of the primary decomposition, we have $W_a[p] = W \cap V_a[p]$ for any irreducible polynomial p and $W_a = W \cap V_a = \oplus W \cap V_a[p] = W_a[p]$. But because $V_a[p]$ is an eigenspace by 8.2.0.1 (5), so is $W_a[p]$.

2. Induction on $\dim(V)$.

□

8.2.1

This splitness condition on χ_a is too restrictive (when the field is not algebraically close), in particular because it is extremely difficult to verify in general! We have two interesting directions to generalize

1. the condition $\text{GCD}(\mu_a, \mu'_a) = 1$ of 8.2.0.1.
2. the existence of stable complement of stable subspaces of 8.2.0.2.

(1) is easy to verify (Euclid's algorithm), has nice diagonalization properties for the matrice of a but unfortunately only over Ω .

(2) has nice geometric properties for the matrice of a on \mathbf{k} itself, but seems difficult to check (except for diagonalizable endomorphism or some cyclic morphisms like for instance a rotation in an Euclidean plane of angle $\neq 0 \pmod{\pi}$ (it has no non trivial invariant supspace!)).

We would like know to look at (1) -absolute semisimplicity- and (2) -semi simplicity and to compare these notions. Fortunately, these conditions are often equivalent (in \mathbf{k} is of zero characteristic or more generally if \mathbf{k} is perfect, sec-perfect). But in general, (2) is delicate to check and not so well behaved.

Because these notions of semismplicity are important in general, we have chosen not to restrict ourself to the linear algebra situation. The good news is that the proofs are not more complicated in this setup.

8.3 Semisimple Modules



Ryoan-ji, Kyoto

Definition 8.3.0.1. 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

- semisimple if every submodule of M has a complement;
- simple if M non-zero and has no non-trivial submodules.

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

In this commutative situation, the theory is very... simple. Observe first that simple modules are certainly semisimple as all modules if R is a field. Moreover, (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 8.3.0.2. *Let M be a semisimple module and N a submodule and S a complement of N .*

1. N is isomorphic to the quotient M/S and $\overline{M} = M/N$ is isomorphic to the submodule S .
2. Submodules and quotient modules of M are semisimple.

Proof.

1. Clear.
2. Enough to prove that M/N is 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!).

□

Proposition 8.3.0.3. *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 semisimple modules is semisimple.
3. Up to isomorphism, $\{\mathbf{k}(\mu), (\mu) \in \mathcal{M}\}$ is the set of all simple modules.
4. A semisimple 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 semisimple. Let S be a complement of (the image of) $\oplus M(\mu)$ 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 1.3.0.4). Then Rs is semisimple (8.3.0.2) and isomorphic to R/I which is also semisimple (8.3.0.2 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 $\iota : \oplus_{(\mu) \in \mathcal{M}} M(\mu) \rightarrow M$ is surjective and let N be a submodule of M . The injection $N(\mu) \rightarrow \oplus N$ 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 $S = \oplus S_\mu$ is complement of N in M .

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

□

Remark(s) 8.3.0.4.

- It follows that every semisimple module is a torsion module except R is a field.
- If R is a field any module is semisimple : this the existence of complement of vector spaces which is at the earth of the preceding proof and depends on Zorn's lemma.
- If M is of finite type, semisimple modules are Noetherian modules thanks to 8.3.0.2. 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 8.3.0.5. *Let $a \in \text{End}_k(V)$ with V of finite dimension. Then a is semisimple if and only if μ_a is square free in $\mathbf{k}[T]$.*

Proof. The maximal ideals of $\mathbf{k}[T]$ are the principal ideals generated by irreducible polynomials. By 8.3.0.3, if a is semisimple, a is cancelled by the products of $\prod P$ where P is monic irreducible such that $V_a(P) \neq \{0\}$. Conversely, we have the decomposition in primary component $V_a = \oplus_{P|\mu_a} V_a[P]$ and $V_a[P] = V_a(P)$ if μ_a is square free (Chinese Remainder Lemma) and we conclude by 8.3.0.3 again. □

8.4 «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 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 8.4.0.1. *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 8.4.0.2. *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 $\text{GCD}(P, P') = 1$.*

Proof. 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 \square

Exercise(s) 8.4.0.3. *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.*

8.4.1 Criterion for Semisimplicity of V_a

The calculation of GCD of polynomials does not depend on the base field (for example because Euclid's algorithm does not depend on it) nor does that of the minimal of the matrix. According to 8.2.0.1, the condition $\text{GCD}(\mu_a, \mu'_a) = 1$ therefore means that the matrix of a is diagonalizable in $M_n(\Omega)$. In the case of V_a , this can be summarized as follows.

Proposition 8.4.1.1. *Let $a \in \text{End}_{\mathbf{k}}(V)$ (with \mathbf{k} perfect) whose matrix $A \in M_n(\mathbf{k})$ is in a given base. The following propositions are equivalent:*

1. *A is diagonalizable in $M_n(\Omega)$.*

2. $\text{GCD}(\mu_a, \mu'_a) = 1$.

3. V_a is semisimple.

4. Every submodule of V_a is semisimple.

If these equivalent conditions are met, a is said to be semisimple (ditto for a matrix of a).

Proof. The equivalence (1) \Leftrightarrow (2) follows from 8.2.0.1.

- (2) \Rightarrow (3). The minimal μ_a is certainly square free and 8.3.0.3 gives (3).
- (3) \Rightarrow (4) This is 8.3.0.2.
- (4) \Rightarrow (2) V_a is semi simple and therefore μ_a is square free. But \mathbf{k} is perfect, therefore $\text{GCD}(\mu_a, \mu'_a) = 1$ by 8.4.0.2 (the only place where perfectness matters) hence (12)

□

8.5 Commuting families of Diagonal Matrices

Diagonal matrices commute. We have a converse.

Lemma 8.5.0.1. *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 $b(v) \in \text{Ker}(a - \lambda \text{Id})$. □

Corollary 8.5.0.2. *Let (a_i) be an arbitrary family of diagonalizable endomorphisms of V . Then, if $f_i \circ f_j = f_j \circ f_i$ for all i, j , there exists a common diagonalization basis for all the f_i .*

Proof. 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 f_i are homotheties $\lambda_i \text{Id}$, any basis is suitable. Otherwise, let i such that f_i is not a homothety. Then, f_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 f_j and their restrictions $f_j(\lambda)$ to each $E_i(\lambda)$ are diagonalizable for all j . For each λ , we then choose a common diagonalization base for the $f_j(\lambda)$ and the union of these bases suits. □

Corollary 8.5.0.3. *Let $a, b \in \text{End}_{\mathbf{k}}(V)$ with a, b semisimple that commute (\mathbf{k} perfect) and $P \in \mathbf{k}[X, Y]$. Then, $P(a, b)$ is semisimple.*

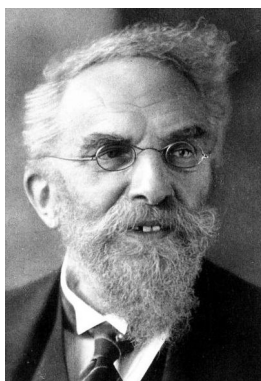
This corollary is false in the imperfect case.

Remark(s) 8.5.0.4. *When the base field K is not perfect, there are semisimple matrices over K which, considered in a superfield, are no longer so. With the notations of 8.4, 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.*

8.6 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).

8.6.1 Hensel's Lemma and Existence



Kurt Hensel

Kurt Hensel



© Gotlib

Isaac Newton

Lemma 8.6.1.1 (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 $x_{k+1} + \varepsilon$, $\varepsilon \in I^{2^k}$ so that x_{k+1} is indeed an approximation of $x_k \pmod{I^{2^k}}$.

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 8.6.1.2 (Existence). *Let $a \in \text{End}_{\mathbf{k}}(V)$ (with \mathbf{k} a perfect field). There exist $d, \nu \in \mathbf{k}[a] \subset \text{End}_{\mathbf{k}}[a]$ such that $a = d + \nu$ and d semisimple, 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 semisimple. Since $\nu = a - P(a) \in I$ and $I^n = 0$, ν is nilpotent. \blacksquare \square

Remark(s) 8.6.1.3. *This is essentially Chevalley's proof. Beyond its algorithmic character (very fast), it is important because it allows the definition of semisimple and nilpotent parts within the context of Lie algebras and algebraic groups (on a perfect field), see for example the excellent [3].*

8.6.2 Uniqueness

Theorem 8.6.2.1 (Jordan-Chevalley). *We still assume \mathbf{k} is a perfect field.*

1. *Let $a \in \text{End}_{\mathbf{k}}(V)$. There exists a unique pair (d, ν) with d semisimple, ν nilpotent, d and ν commuting with $a = d + \nu$.*
2. *Let $\chi \in \mathbf{k}[T]$ be a monic polynomial of degree n . There exists $P \in \mathbf{k}[X]$ (depending only on χ) such that if $\chi_a = \chi$, then $d = P(a)$ and in particular $d, \nu \in \mathbf{R} = \mathbf{k}[a] \subset \text{End}_{\mathbf{k}}[a]$.*

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 8.6.1.2. 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, 8.5.0.3); 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 8.5.0.4 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.

8.6.3 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. 8.6.4.1). 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.

8.6.4 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 Frobenius¹ $F : x \mapsto x^p$ of \mathbf{k} is known algorithmically.

Exercise(s) 8.6.4.1. 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 semisimple 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

¹Which 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 10.2.0.2). 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 10.

8.7 Supplementary Exercises

Exercise(s) 8.7.0.1. 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(s) 8.7.0.2. 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(s) 8.7.0.3. 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(s) 8.7.0.4. 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 semisimple, commute but their difference is nilpotent (this is exercise 14 chapter VII.5 [5] rewritten without tensor product).

Exercise(s) 8.7.0.5. 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 5.6.0.2 that if the minimals of A, B and their respective derivatives are coprime, any element C of $\mathbf{k}[A, B]$ is semi-simple (without using 8.5.0.3). Is μ_C necessary coprime with its derivative?

Chapter 9

The Duality Toolbox



René Magritte

9.1 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 $V^* \times V \rightarrow \mathbf{k}$.

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).

¹Unless otherwise stated.

²Be careful, the dual acts to the right on vectors, cf. [4].

Proposition 9.1.0.1. *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 of the φ_i is zero, a contradiction. If \mathbf{k} is a finite field (of characteristic $p \geq 2$), the cardinality of V is p^n . The union of two hyperplanes has cardinality at worst $2p^{n-1} - 1 \leq p^n - 1$ (because 0 belongs to both 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 $\mathbf{k}^n = M_{n,1}(\mathbf{k}) = V$, its dual basis \mathcal{B}^* is formed from the rows $e_i^* = {}^t e_i$, which is the canonical basis ($E_{1,i} = e_i^*$) of $M_{1,n}(\mathbf{k}) = \mathbf{k}^n = V^*$.

If \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 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) 9.1.0.2. *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.

9.2 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 $eq_i \in V^*$: $W = \{v \mid \langle eq_i, v \rangle = 0\}$ with

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

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 $W^\perp = \{\varphi \in V^* \mid \varphi(W) \equiv 0\}$ and then to the link with the first point of view.

9.3 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

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

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

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

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.

9.4 Ante-dual Basis: Biduality

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

Proposition 9.4.0.1. *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

9.5 Orthogonal and Polar in Finite Dimension

Proposition 9.5.0.1. *Let W, W_* be two subspaces of V, V^* respectively. We have*

1. $\dim(W) + \dim(W^\perp) = n$.

2. $\dim(W_*) + \dim(W_*^\circ) = n$.

3. $W_* = (W_*^\circ)^\perp$.

4. $W = (W^\perp)^\circ$.

5. $ev(W_*^\circ) = W_*^\perp$.

6. $ev(W) = W^{\perp\perp}$.

Proof. 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 $\mathcal{B}^* = (e_i^*, 1 \leq i \leq n)$ 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 $ev(w)(\varphi) = \varphi(w)$ 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) 9.5.0.2. 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 $W \mapsto W^*$. 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) 9.5.0.3. Note that orthogonality and polarity are strictly decreasing applications for inclusion.

Corollary 9.5.0.4. Let $\varphi_i \in V^*$, $i = 1, \dots, m$. Then, the rank of $\text{Vect}\{\varphi_i\}$ is that of the evaluation application $\left\{ \begin{array}{l} V \rightarrow k^m \\ v \mapsto (\varphi_i(v))_i \end{array} \right.$

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(s) 9.5.0.5. 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.

9.6 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 9.1.0.2).

Exercise(s) 9.6.0.1. 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 9.6.0.2. Let φ and φ_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(s) 9.6.0.3. 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) 9.6.0.4 (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, $\bigcap_i H_i^+ \subset H^+$ if and only if φ is a linear combination with positive coefficients of the φ_i . See ??.

9.7 Contravariance

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

Definition 9.7.0.1. If $f \in \text{Hom}_{\mathbf{k}}(V_1, V_2)$, we note ${}^t f \in \text{Hom}_{\mathbf{k}}(V_2^*, V_1^*)$ the transpose of f defined by ${}^t f(\varphi_2) = \varphi_2 \circ f$, in other words, $\langle {}^t f(\varphi_2), v_1 \rangle = \langle \varphi_2, f(v_1) \rangle$ for every $\varphi_2 \in V_2^*, v_1 \in V_1$.

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

We have the following (formal) proposition

Proposition 9.7.0.2. *If $f \in \text{Hom}_{\mathbf{k}}(V_1, V_2)$ and \mathcal{B}_i are bases of V_i .*

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

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

3. *We have $\text{Mat}_{\mathcal{B}_2^*, \mathcal{B}_1^*}({}^t f) = {}^t \text{Mat}_{\mathcal{B}_1, \mathcal{B}_2}(f)$.*
4. *$\text{rk}(f) = \text{rk}({}^t f)$.*
5. *With the identifications (9.6), the transposition is involutive.*
6. *$\text{Im}({}^t f) = \text{Ker}(f)^\perp$ and $\text{Ker}({}^t f) = \text{Im}(f)^\perp$.*
7. *If $V_1 = V_2 = V$, a subspace W of V is stable by f if and only if W^\perp is stable by ${}^t f$.*

Proof. Let'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 9.5.0.1, it suffices to prove $\text{Im}({}^t f) \subset \text{Ker}(f)^\perp$. Now, if $f(v_1) = 0$, then $\langle {}^t f(\varphi_2), v_1 \rangle = \langle \varphi_2, f(v_1) \rangle = 0$.

□

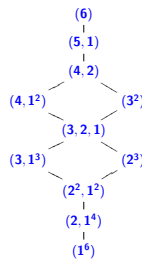
9.8 Supplementary Exercises

Exercise(s) 9.8.0.1. *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?*

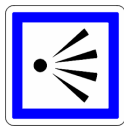
Chapter 10

Topology of Similarity Classes*



Hasse Diagram of GL_6

10.1 Perspective



Here we provide a perspective on the geometry of similarity classes through their topology. To avoid formalism, we restrict ourselves to the usual topology on complex matrices even though the so called Zariski topology whose closed sets are defined by families of polynomial equations would have been more natural¹.

10.2 Introduction

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. 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.

Definition 10.2.0.1. An n -type is a sequence $\underline{P} = (P_n | P_{n-1} | \cdots | P_1)$ of monic polynomials of $\mathbf{k}[T]$ such that $\sum \deg(P_i) = n$. We denote $O(\underline{P})$ the set of matrices in $M_n(\mathbf{k})$ similar to the companion matrix $C(\underline{P})$.

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 (6.7.0.2).

Our goal is to study the closure $\overline{O(\underline{P})}$ of the orbits $O(\underline{P})$. We will therefore assume in the remainder of this chapter that \mathbf{k} is the field of complex numbers \mathbf{C} , with matrix spaces equipped with some norm (let's recall that all matrix norms are equivalent).

We then define a (topological) relation on complex n -types by

$$\underline{P} \preceq \underline{Q} \text{ if and only if } O(\underline{P}) \text{ is contained in the closure } \overline{O(\underline{Q})}.$$

It is clearly a order. Since $\overline{O(\underline{Q})}$ is invariant by conjugation, it is a union of orbits and we have $\overline{O(\underline{Q})} = \cup_{\underline{P} \preceq \underline{Q}} O(\underline{P})$. We will characterize this order in a combinatorial manner as follows.

We define a (combinatorial²) relation on complex n -types by

$$\underline{P} \leq \underline{Q} \text{ if and only if we have the divisibility } \prod_{j \leq i} P_j | \prod_{j \leq i} Q_j \text{ for every } i = 1, \dots, n.$$

It is also a (partial) order. Note that necessarily then $\prod_{i=1}^n P_i = \prod_{i=1}^n Q_i$ for degree reasons.

Theorem 10.2.0.2. Let $\underline{P}, \underline{Q}$ be two complex n -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.

Remark(s) 10.2.0.3. This theorem is a reformulation, more transparent in my opinion, of Theorem 4 from [8]. 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*.

We will proceed by reduction to the nilpotent case using topological results from ???. Let's start with the crucial case.

10.3 Closure of a Nilpotent Orbit

Thus, we have again a topological order on the partitions of n defined by

²Compare with cf. 10.3.



Nilpotent orbits are classified by partitions \underline{d} of n (7.7.0.2), the dictionary between type and partition being given by $\underline{d} \mapsto T^{\underline{d}} = (T_{d_n}, \dots, T_{d_1})$. We then denote $O(\underline{d})$ the orbit $O(T^{\underline{d}})$ accordingly.

$$\underline{d} \preceq \underline{\delta} \text{ if and only if } O(\underline{d}) \text{ is contained within the closure } \overline{O(\underline{\delta})}$$

and a combinatorial order

$$\underline{d} \leq \underline{\delta} \text{ if and only if for every } i = 1, \dots, n \text{ we have the inequality } \sum_{j \leq i} d_j \leq \sum_{j \leq i} \delta_j.$$

In the nilpotent case, the theorem 10.2.0.2 then becomes

Theorem 10.3.0.1 (Nilpotent Case). *Let $\underline{d}, \underline{\delta}$ be two partitions of n . Then, $\underline{d} \preceq \underline{\delta}$ if and only if $\underline{d} \leq \underline{\delta}$.*

Thus, we aim to show that the topological order \preceq and the combinatorial order \leq on the partitions coincide.

Remark(s) 10.3.0.2. *A partition is always defined by indicating the number of times an integer is repeated, often in ascending order. For $n = 6$, for example, the partition $(3, 1, 1, 1, 0, 0)$ is then denoted $(1^3, 3)$ while the partition $(6, 0, 0, 0, 0, 0)$ is noted as (6) . The diagram describing the order is then called a Hasse diagram. We will not use these notations except in the picture at the beginning of this chapter.*

10.3.1 Order and Duality on Partitions



We use notations and results on nilpotent matrices from ???. We will demonstrate that the duality of partitions is decreasing for the combinatorial order \leq . For this, and what follows, the key is the classic lemma of disassembling whose proof I reproduce from [14].

We say that $\underline{d} \leq_e \underline{\delta}$ (\underline{d} elementarily inferior to $\underline{\delta}$) if there are indices $i < j$ such that

$$(\delta_1, \dots, \delta_n) = (d_1, \dots, d_{i-1}, d_i + 1, \dots, d_j - 1, \dots, d_n).$$

Obviously

$$\underline{d} \leq_e \underline{\delta} \Rightarrow \underline{d} \leq \underline{\delta}$$

Lemma 10.3.1.1. *Let $\underline{d}, \underline{\delta}$ be two partitions of n . Then, $\underline{d} \leq \underline{\delta}$ if and only if there exists a series of elementary inequalities $\underline{d} = \nu_0 \leq_e \nu_1 \leq_e \dots \leq_e \nu_{N-1} \leq_e \nu_N = \underline{\delta}$.*

Proof. It suffices to prove the existence of a partition $\underline{\nu}$ such that $\underline{d} \leq_e \underline{\nu} \leq_e \underline{\delta}$ when $\underline{d} \neq \underline{\delta}$ and to iterate the process (which stops when $\underline{\nu}_N = \underline{\delta}$.) We thus seek $i < j$ such that $\underline{\nu} \leq_e \underline{\delta}$ with

$$\underline{\nu} = (d_1, \dots, d_{i-1}, d_i + 1, \dots, d_j - 1, \dots, d_n).$$

If $\underline{\nu} = \underline{\delta}$, we are done. Otherwise, $\underline{\nu} < \underline{\delta}$.

There exists therefore k such that

$$(1) \quad d_1 + \dots + d_k < \delta_1 + \dots + \delta_k$$

Let i be the smallest integer k satisfying (1)

Furthermore, as $\sum d_k = \sum \delta_k$, there must exist $k > i$ such that

$$(2). \quad d_1 + \dots + d_k \geq \delta_1 + \dots + \delta_k$$

Let j be the smallest integer $k > i$ satisfying (2).

We have

$$(3) \quad d_1 + \dots + d_k + 1 \leq \delta_1 + \dots + \delta_k \text{ for all } k \in [i, j-1]$$

and

$$(4) \quad d_1 + \dots + d_j = \delta_1 + \dots + \delta_j$$

With these values of i and j , we demonstrate that $\underline{\nu}$ is a partition, *i.e.* $d_{i-1} > d_i$ (or $i = 1$) on one hand and $d_j > d_{j+1}$ on the other.

By construction, i is the smallest integer such that $d_i < \delta_i$ and thus $d_i < \delta_i \leq \delta_{i-1} = d_{i-1}$ (or $i = 1$).

Furthermore, since $d_1 + \dots + d_{j-1} < \delta_1 + \dots + \delta_{j-1}$ and $d_1 + \dots + d_j = \delta_1 + \dots + \delta_j$ $d_j > \delta_j$; since furthermore and $d_1 + \dots + d_{j+1} \leq \delta_1 + \dots + \delta_{j+1}$ we also have $d_{j+1} \leq \delta_{j+1}$. Combining both, we get $d_{j+1} \leq \delta_{j+1} \leq \delta_j < d_j$, which is what we wanted.

We then observe that the inequality $\underline{\nu} \leq_e \underline{\delta}$ is equivalent to (3). □

Corollary 10.3.1.2. *The duality of partitions is strictly decreasing.*

Proof. It suffices to show the decrease in the elementary case $\underline{d} \leq_e \underline{\delta}$. For this, we observe that $\underline{\delta}^*$ satisfies

$$\delta_k^* = \begin{cases} d_k & \text{if } k \neq d_i, d_j \\ d_k - 1 & \text{if } k = d_i \\ d_k + 1 & \text{if } k = d_j \end{cases}$$

so that $\underline{\delta}^* \leq_e \underline{d}^*$. To see this, we note that $d_i > d_j$ and consider the following table

k	\underline{d}^*	$\underline{\delta}^*$	comparison	$\text{Card}(\underline{\delta}^*) - \text{Card}(\underline{d}^*)$
[1,i-1]	$d_k \geq \alpha$	$d_k \geq \alpha$	same	0
i	$d_k \geq \alpha$	$d_k \geq \alpha + 1$	same except if $\alpha = d_i$	-1
[i-1,j-1]	$d_k \geq \alpha$	$d_k \geq \alpha$	same	0
j	$d_k \geq \alpha$	$d_k \geq \alpha - 1$	same except if $\alpha = d_j$	+1
[j+1,n]	$d_k \geq \alpha$	$d_k \geq \alpha$	same	0

using the formula for calculating the dual partition $d_\alpha^* = \text{Card}\{k | d_k \geq \alpha\}$ (??). The proof also provides strict decrease (even though the strict character follows from the fact that duality is involutive) \square

10.3.2 Rank and Nilpotent Orbits



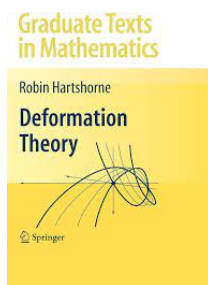
Let M be a nilpotent matrix with associated partition \underline{d} . According to the formula (??) from ??, we have for all $n - \text{rk}(M^i) = \sum_{j \leq i} d_j^*$. However, the rank is lower semi-continuous: there exists a neighborhood U of M where all matrices $N \in U$ satisfies $\text{rk}(N) \geq \text{rk}(M)$. If M is in the closure of $O(\underline{\delta})$, this neighborhood intersects $O(\underline{\delta})$: thus, let $N \in U \cap O(\underline{\delta})$. Then $n - \text{rk}(N^i) \leq n - \text{rk}(M^i)$ for all i , meaning $\underline{\delta}^* \leq \underline{d}^*$ and therefore $\underline{\delta} \leq \underline{d}$.

Corollary 10.3.2.1. *Let $\underline{d}, \underline{\delta}$ be partitions of n . Then,*

$$\underline{d} \preceq \underline{\delta} \Rightarrow \underline{d} \leq \underline{\delta}.$$

Let us demonstrate the reciprocal implication.

10.3.3 A Nilpotent Matrix Deformation



Following Lemma 10.3.1.1, we simply need to demonstrate the implication in the elementary case. Thus, let $\underline{d} \leq_e \underline{\delta}$ and let us show that $\underline{d} \preceq \underline{\delta}$. It therefore exists indices $i < j$ such that

$$(\delta_1, \dots, \delta_n) = (d_1, \dots, d_{i-1}, d_i + 1, \dots, d_j - 1, \dots, d_n).$$

We consider $J_{\underline{d}}$ which we want to show is in the closure of $O(\underline{\delta})$, therefore, we want to demonstrate that $J_{\underline{d}}$ is a limit of matrices from $O(\underline{\delta})$.

As \underline{d} and $\underline{\delta}$ only differ at indices i and j , we can assume without loss of generality that we have only two indices. We must therefore show that $J_{(d_i, d_j)}$ is in the closure of $O((d_i - 1, d_j + 1))$. Let us set for example $N(x) = J_{(d_i, d_j)} + xE_{d_i+d_j, d_i}$. This is a triangular block matrix of size $d_i + d_j$ and rank $d_i + d_j - 2$ with $d_i > d_j$. Its type is characterized by its nilpotency index which is $d_i - 1$ (7.9.0.1) for non-zero x so that $N(x)$ is of type $d_i - 1, d_j + 1$. Thus, $N(0) = \lim_{x \rightarrow 0} N(x) \in \overline{O(\underline{\delta})}$ and $\underline{d} \preceq \underline{\delta}$. Hence, recalling 10.3.2.1

$$\underline{d} \preceq \underline{\delta} \iff \underline{d} \leq \underline{\delta}$$

We have therefore proved the theorem 10.3.0.1 in the nilpotent case.

Remark(s) 10.3.3.1. *It is for this argument sequence (and the one in the following paragraph) that the knowledgeable reader wanting to generalize to the Zariski topology of general fields will use the assumption that the field is infinite.*

Let us move to the general case.

10.4 Closure of an Arbitrary Orbit



All work has been done to reduce the general case to the nilpotent case. Let's explain. We consider two n -types $\underline{P}, \underline{Q}$ and study the inclusion $O(\underline{P}) \subset \overline{O(\underline{Q})}$. In other words, we consider a sequence of matrices A_m in $O(\underline{Q})$ converging towards $A_\infty \in O(\underline{P})$. We then freely use the notations and results from ??.

By the continuity of the characteristic polynomial, it already ensures that $\chi_{A_m}, m \in \overline{\mathbf{N}}$ is a constant polynomial χ whose set of complex roots we denote by Λ . It follows that the characteristic spaces of A_m have a constant dimension d_λ : the multiplicity order of the root λ of χ .

Then (??), we have

$$\lim A_m = A_\infty \text{ if and only if for all } \lambda \in \Lambda, \quad \lim A_{m,\lambda} = A_{\infty,\lambda}$$

But, for each λ , the matrix $A_{m,\lambda} - \lambda \text{Id} \in M_{n,\mathbf{C}}$ is nilpotent and its n -type is (??) is

$$\underline{\delta}_\lambda = 1, \dots, 1, (X - \lambda)^{v_\lambda(Q)}, \quad i = d_\lambda, \dots, 1 \text{ if } n < \infty$$

and

$$\underline{d}_\lambda = 1, \dots, 1, (X - \lambda)^{v_\lambda(P)}, \quad i = d, \dots, 1 \text{ otherwise}$$

where the 1s are repeated $d_\lambda - v_\lambda(\chi)$ times in all cases. But according to the characterization of nilpotent orbits - necessary condition - (10.3.0.1), the existence of this sequence of matrices leads to

(i) $\text{For all } \lambda \in \Lambda, \underline{d}_\lambda \leq \underline{\delta}_\lambda$

Conversely, assuming this condition is satisfied. We denote p_λ the spectral projectors of A_∞ of type \underline{P} . Following the sufficient part of the characterization of nilpotent orbits (10.3.0.1), for every λ there exist nilpotent matrices $N_{m,\lambda}$ that converge to $N_{\infty,\lambda} = A_{\infty,\lambda} - \lambda p_\lambda$. By setting $A_m = \sum_\lambda (N_{m,\lambda} + \lambda p_\lambda)$, we have $\lim A_m = A_\infty$. Thus,

$$\underline{P} \preceq \underline{Q} \iff \text{for all } \lambda \in \Lambda, \underline{d}_\lambda \leq \underline{\delta}_\lambda.$$

Moreover, for two polynomials P, Q whose roots are in Λ , we have

$$P|Q \iff \text{for all } v_\lambda(P) \leq v_\lambda(Q)$$

The condition (i) can therefore be rewritten as

$$\text{for all } i = 1, \dots, n, \text{ we have } \prod_{j \leq i} P_j | \prod_{j \leq i} Q_j$$

This concludes the proof of theorem 10.2.0.2.



10.5 Additional Exercises

Exercise(s) 10.5.0.1. Let \underline{Q} be an n -type and $\chi = \prod Q_i$ the corresponding characteristic polynomial.

1. Show that $O(\underline{\chi}_{red})$ (cf. 8.6.4.1) is the only closed orbit contained in $\overline{O(\underline{Q})}$. Deduce that closed orbits are semi-simple orbits and that $\chi_{red} = (\chi_n, \dots, \chi_1)$ is a minimal type for \preceq .
2. Show that the closure of $O(\underline{\chi}_{red})$ is the set of matrices A such that $\chi_1(A) = 0$ and $\chi_A = \chi$.
3. Generally, show that minimal n -types are of the form $\underline{\chi}_{red}$ for χ monic of degree n . Can you prove this result directly?
4. Conversely, show that maximal n -types are of the form $(1, \dots, 1, \chi)$. Deduce that maximal orbits are those of companion matrices $C(\chi)$.

5. Show that the closure of $O(\mathbb{C}(\chi))$ is the set of matrices A whose $\chi_A = \chi$.

Exercise(s) 10.5.0.2. Let \mathbf{k} be a subfield of \mathbb{C} . Here we consider only n -types \mathbf{k} -rational \underline{d} , i.e. verifying $P_i \in \mathbf{k}[T], i = 1, \dots, n$. We denote $O_{\mathbf{k}}(\underline{d})$ the conjugacy class of $C(\underline{d})$ under $GL_n(\mathbf{k})$. Show in this case $O_{\mathbf{k}}(\underline{P}) = O_{\mathbb{C}}(\underline{P}) \cap M_n(\mathbf{k})$. Using ?? and the main theorem 10.2.0.2, show $\overline{O_{\mathbf{k}}(\underline{Q})} = \cup_{\underline{P} \leq \underline{Q}} O_{\mathbf{k}}(\underline{P})$.

Chapter 11

Index et bibliography

Index

- adapted basis, 83
- Algebraic Identities Permanence Principle, 29
- basis,
 - ante-dual, 129
 - dual, 128
- bicommutant, 89
- Bézout equivalence, 78
- Bézout matrix, 12
- Cayley-Hamilton Theorem, 30, 31
- cokernel, 43
- commutant, 89
- commutative diagram, 48
- commutator, 34
- Companion matrices, 87
- complex of modules, 46
- content, 102
- decomposition,
 - Frobenius, 88
- derived subgroup, 34
- determinant trick, 64
- diagram, 48
- diagram,
 - Hasse diagram, 137
- dilatation, 12
- duality bracket, 127
- duality,
 - contravariance, 133
 - convention of biduality, 131
 - differential, 128
 - Jacobian, 128
 - orthogonal, 128
 - polar, 128
 - transpose, 132
- endomorphism,
 - cyclic, 88
 - absolutely semisimple, 120
 - semisimple, 119
- equivalent matrices, 32
- exact sequence, 46
- factorial, 99, 103
- functor, 52
- functoriality,
 - of the cokernel, 48
 - of the kernel, 50
- Gauss equivalent, 32
- Gauss,
 - elimination, 32
- GCD, 101
- Greatest Common Divisor GCD, 78
- idempotent, 68
- inductive set, 12
- inequality, Cauchy-Schwarz,
 - real, 20
- integer
 - algebraic, 104
- integers,
 - rings of, 64
- integral domain, 57
- integral element, 64
- irreducibility of Φ_n over \mathbf{Q} , 105

- irreducibles,
 - existence, 100
 - of $R[T]$, 102
 - uniqueness of the decomposition into, 99
- Jordan-Chevalley decomposition, 120
- LCM, 101
- lemma
 - of Zorn, 13
- lemma,
 - five, 51
 - Gauss lemma for PID, 78
 - Hensel, 120
 - Krull, 13
 - Nakayama, 64
 - of Euclid, 98
 - PID splitting, 106
- minor of a matrix, 81
- module, 40
- module,
 - V_a , 45
 - torsion, 57
 - associated with an endomorphism, 45
 - cyclic, 63
 - free, 55
 - noetherian, 74
 - quotient, 43
 - semi-simple, 115
- morphism,
 - Frobenius, 118
- Noetherian,
 - Hilbert's basis theorem, 76
 - ring, 75
- noetherian,
 - module, 74
- order,
 - \leq on partitions, 136
 - \leq on types, 136
 - \preceq on partitions, 137
 - \preceq on types, 136
- orientation, 22
- orientation,
 - direct basis, 22
 - positively oriented basis, 22
- partition,
 - of an integer, 109
- perfect group, 34
- permutation matrix, 12
- polycyclic module,
 - invariant ideals, 67
 - rank, 67
- polycyclic modules, 67
- polynomial
 - cyclotomic, 103
- primary decomposition, 105
- primitive, 102
- quotient, 43
- reduction,
 - Jordan, 108
 - Frobenius, 88
- ring,
 - Euclidean, 77
 - Noetherian, 75
 - Noetherian UFD, 100
 - UFD or factorial, 99, 103
- semi-simple,
 - module, 115
- semisimple,
 - endomorphism, 119
- similar matrices, 45
- similarity invariants, 86

similarity invariants, 84

Snake lemma, 58

space,

 stable, 45

theorem,

 structure of finite type modules over PID, 83

torsion, 56

transvection, 12, 33

type, 136

UFD, 99, 103

universal property,

 of the cokernel, 53

 of the kernel, 53

 of the product of modules, 52

 of the sum of modules, 52

Bibliography

- [1] 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.
- [2] Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill Book Co., New York-Toronto-London, 1967.
- [3] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.
- [4] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 1 à 3*. Hermann, Paris, 1970.
- [5] N. Bourbaki. *Algebra. Chapters 4–7*. Springer-Verlag, Berlin, 2007.
- [6] Karine Chemla and Shuchun Guo. *The Nine Chapters: A Mathematical Classic of Ancient China and its Commentaries*. Dunod, Paris, 2005.
- [7] Régine Douady and Adrien Douady. *Algèbre et théories galoisiennes. 1*. CEDIC, Paris, 1977.
- [8] Murray Gerstenhaber. On dominance and varieties of commuting matrices. *Ann. of Math. (2)*, 73:324–348, 1961.
- [9] Daniel R. Grayson. Sk1 of an interesting principal ideal domain. *Journal of Pure and Applied Algebra*, 20:157–163, 1981.
- [10] David Hilbert. Ueber die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890.
- [11] Felix 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.
- [12] J. Milnor. Whitehead torsion. *Bull. Amer. Math. Soc.*, 72:358–426, 1966.
- [13] Emmy Noether. Idealtheorie in Ringbereichen. *Math. Ann.*, 83(1-2):24–66, 1921.
- [14] Hjalmar Rosengren. Proof of the duality of the dominance order on partitions. <https://math.stackexchange.com/q/3429855>, 2020.