L'Enseignement Mathématique (2) 60 (2014), 1–49

ON THE STRUCTURE OF ENDOMORPHISMS OF PROJECTIVE MODULES

by Daniel FERRAND and Dan LAKSOV †)

ABSTRACT. Taking as a model the completed theory of vector space endomorphisms, the present text aims at extending this theory to endomorphisms of finitely generated projective modules over a general commutative ring; now analogous results often require totally different methods of proof.

The first important result is a structure theorem for such modules when the characteristic polynomial of the endomorphism is separable. The second topic deals with the minimal polynomial, whose mere existence is shown to require additional hypotheses, even over a domain. In the third topic we extend the classical notion of 'cyclic modules' as the modules which are invertible over the ring of polynomials modulo the characteristic polynomial.

Regarding the diagonalization of endomorphisms, we show that a classical criterion of being diagonalizable over some extension of the base field can be transferred nearly verbatim to rings, provided that diagonalization is expected only after some faithfully flat base change. Many results that hold over a field, like the fact that commuting diagonalizable endomorphisms are simultaneously diagonalizable, hold over arbitrary rings, with this extended meaning of diagonalization. The Jordan-Chevalley-Dunford decomposition, shown as a particular case of the lifting property of étale algebras, also holds over rings.

Finally, in several reasonable situations, the eigenspace associated with any root of the characteristic polynomial is shown to be given a more concrete description as the *image* of a map. In these situations the classical theory generalizes to rings.

†) Les Éditeurs ont appris le décès de Dan Laksov en novembre 2013, après que cet article eut été accepté pour publication. Son coauteur, Daniel Ferrand, a pris le soin d'en faire une relecture minutieuse et a procédé à quelques remaniements dans le but de perfectionner la présentation.

Achevé de composer le 24 février 2014 à 13 : 48

CONTENTS

1. Preliminaries on idempotents, and open and closed subsets 4
2. Finite étale algebras 8
3. Endomorphisms with a separable characteristic polynomial 14
4. Minimal polynomials 22
5. Cyclic modules 28
6. Diagonalizable endomorphisms 33
7. The Jordan-Chevalley-Dunford decomposition 36
8. Eigenspaces 42

INTRODUCTION

The principal aim of the present text is to extend the theory of endomorphisms of vector spaces to endomorphisms of finitely generated projective modules, as far as possible. Our motivations arise from situations in algebra and geometry which need global properties while the classical theory is too much concentrated above a one-point scheme to be adequate.

For example, we often meet families of linear maps u_s which depend on parameters s, and this situation is usually described as a vector bundle $\pi: E \to S$ over the space S of the parameters, together with a map $u: E \longrightarrow E$ inducing on each fiber $E_s = \pi^{-1}(s)$ a linear map $u_s: E_s \to E_s$ of vector spaces. Roughly speaking, the Gelfand point of view then leads us to associate with the space S a commutative ring A of functions on S (continuous, or algebraic, etc.), and the vector bundle E is similarly described as a projective A-module of finite type, say M. To a point $s \in S$ is thus associated a maximal ideal $\mathfrak{m}$ of A, and the map u_s is equal to the map $M/\mathfrak{m}M \longrightarrow M/\mathfrak{m}M$ induced by u.

The consideration of the generic matrix leads to a situation of the same kind: in this case S is the spectrum of the ring $A = \mathbf{Z}[X_{ij}]$ with n^2 independent variables, and the endomorphism of A^n is given by the matrix with entries the X_{ij}.

In a sense the present work is intended to understand how the classical notions vary in a family of endomorphisms. What we might reasonably expect is not always true even under strong hypotheses. We encounter, for example, square matrices with a constant eigenvalue, whose eigenspace is a projective module of rank 1 *which is not free*. In the above geometric perspective this means that there is no (continuous, algebraic, etc.) section σ of π with $\sigma(s)$ a non-zero eigenvector of u_s for all s.

However, this work adds nothing to the problem of moduli of vector space endomorphisms, which is different (see, for example, [MS]).

The power of the classical theory over a field K comes essentially from two facts:

– every K-module is free,

– every ideal in $K[T]$ is principal,

two obviously missing properties over a general commutative ring.

Concerning the lack of bases, we are led to restrict ourselves, from the outset, to modules of finite type which are *locally* free, that is, which are projective. This restriction ensures us the existence of the characteristic polynomial, which indeed plays a central role in this article. More problematic, as we shall see, is the mere existence of the minimal polynomial because it should be the generator of an ideal in $A[T]$, which is not always principal.

The fact that the ideals in $A[T]$ are as a rule non principal renders it impossible to decompose the module into a direct sum of cyclic modules. However, some results which are usually deduced from this decomposition remain true in general. For example, we show that the characteristic polynomial always divides some power of the minimal polynomial, when the latter exists; but this requires a completely different argument, which rests on the so-called "spectral mapping theorem" (Theorems 3.6 and 5.5; see Corollary 5.6).

Practically all the results over a field which depend on a hypothesis involving some extension of the base field extend verbatim over a ring A under a hypothesis which is analogous, but relative to some faithfully flat algebra $A \to A'$. For example, the classical property of a monic polynomial p to have distinct roots in some extension of the base field, that is to be separable, has to be translated into the property that the A-algebra $A[T]/(p)$ is étale. This explains why étaleness is everywhere recurrent in the text.

Our hypotheses are supported by the following rings attached with an endomorphism $u\colon M \to M$ of a projective module of finite type over a ring A: first we have the ring $B = A[T]/(p_u)$, where p_u is the characteristic polynomial of u, and there is also the sub-A-algebra $A[u] \subset \mathrm{End}_A(M)$ generated by u. The Cayley-Hamilton theorem asserts that there is a surjective morphism of A-algebras

$$\rho\colon B \longrightarrow A[u];$$

in particular, M may be seen as a B-module. The kernel of ρ is a nilpotent ideal.

Achevé de composer le 24 février 2014 à 13:48

The first important result is that the B-module M is invertible when B is finite étale over A. More generally, being an invertible B-module appears to be the appropriate generalization of the classical notion of 'cyclic module'.

Secondly we deal with the existence and properties of the minimal polynomial, defined as the generator of the ideal $\mathrm{Ker}(\rho)$, when it exists, i.e. when $A[u]$ is projective as an A-module. We also indicate some situations where this holds, for example, when A is integrally closed.

Then we work out the analogue of the diagonalization of endomorphisms. Classically it involves the minimal polynomial, which is a priori lacking in our context. Therefore we must rather consider the weaker condition of being "absolutely semi-simple", that is of being diagonalizable over some extension of the base field. This property can be transferred nearly verbatim to rings under the form: $A[u]$ is étale over A. With this meaning of the word 'diagonalizable', two commuting endomorphisms which are "diagonalizable", are shown to be simultaneously "diagonalizable".

We also show that the Jordan-Chevalley-Dunford decomposition holds over rings, simply because it is shown to be a particular case of the lifting property of étale algebras. In fact, the decomposition $u = u_s + u_n$ is here equivalent to the existence of a quotient B/J, étale over A, where J is a nilpotent ideal.

Finally, we discuss eigenvectors and eigenspaces. We show that in several reasonable situations the eigenspace associated to any root λ of the characteristic polynomial of u can be given a concrete description as the *image* of a map close to the cotranspose of $u - \lambda$. In these situations the classical theory generalizes to rings.

One conclusion of this work is that extending over a ring the linear results which are classical over a field forces us to weaken both the hypothesis and the conclusion by restricting them to be true only locally for the Zariski, or étale, or even fpqc topology. After all, we already meet this constraint when working over a field which is not algebraically closed.

In what follows, all rings are supposed to be commutative with unity.

1. Preliminaries on idempotents, and open and closed subsets

In this section we collect for the convenience of the reader some classical results on idempotents and open and closed subsets of the prime spectrum of a ring. We follow the usual notation: see for example [AC], II, 4; in particular, for an ideal I of a ring A, $V(I)$ denotes the set of prime ideals of A containing I; it is closed in $\mathrm{Spec}(A)$.

1.1. LEMMA. *Let* $\pi\colon C \to C_1$ *be a surjective morphism of rings, and let* U *be the closed subset of* $\mathrm{Spec}(C)$ *image of the map* $\pi^\star\colon \mathrm{Spec}(C_1) \to \mathrm{Spec}(C)$. *Then the following properties are equivalent:*

i) *The set* U *is open and, as a morphism of schemes,* $\pi^\star$ *is an open immersion: this means that, for all prime ideals* $\mathfrak{p}$ *containing* $I = \mathrm{Ker}(\pi)$, *the map* $\pi_\mathfrak{p}\colon C_\mathfrak{p} \to (C_1)_\mathfrak{p}$ *is an isomorphism, i.e.* $I_\mathfrak{p} = 0$.

ii) *The ideal* $\mathrm{Ker}(\pi)$ *is generated by an idempotent* e *in* C *and one has* $U = V(e)$*; such an idempotent is unique.*

iii) *The ring* C *has a quotient* $C \to C_0$ *such that the morphism* $C \longrightarrow C_0 \times C_1$ *is an isomorphism of rings.*

iv) *The morphism* π *defines a structure of* projective C*-module on* C_1.

Proof. i) $\Rightarrow$ ii) By definition, one has $U = V(I)$, where $I = \mathrm{Ker}(\pi)$. By assumption, there is an ideal J in C such that $\mathrm{Spec}(C)$ is the disjoint union of $V(I)$ and $V(J)$. Since $\varnothing = V(I) \cap V(J) = V(I + J)$, there are two elements $a \in I$ and $b \in J$ such that $1 = a + b$. Moreover, since $\mathrm{Spec}(C) = V(I) \cup V(J) = V(IJ)$, the elements of IJ are nilpotent, and thus $(ab)^m = 0$ for some integer m.

The element $u = a^m + b^m$ is not contained in any prime ideal of C, and thus it is invertible in C. We let $e = a^m/u$ and $e' = b^m/u$. Then $1 = e + e'$ and $ee' = 0$; thus e is an idempotent contained in I, and $e' = 1 - e$ is an idempotent contained in J. Hence we have inclusions $U = V(I) \subset V(e)$ and $V(J) \subset V(1 - e)$. Since, moreover, both pairs of closed subsets $[V(I), V(J)]$ and $[V(e), V(1 - e)]$ are partitions of $\mathrm{Spec}(C)$, these partitions are equal. In particular one has $V(I) = V(e)$. In order to check that $Ce = I$ we can localize at the prime ideals $\mathfrak{p}$ of C. In fact, $Ce \subset I$ and hence $(Ce)_\mathfrak{p} \subset I_\mathfrak{p}$. If $\mathfrak{p}$ contains I we have $I_\mathfrak{p} = 0$ by assumption, whence $(Ce)_\mathfrak{p} = I_\mathfrak{p} = 0$. If, on the other hand, $\mathfrak{p}$ does not contain I then $e \notin \mathfrak{p}$ is invertible in $C_\mathfrak{p}$ and $C_\mathfrak{p} = (Ce)_\mathfrak{p} = I_\mathfrak{p}$.

Uniqueness of e: starting from an equality $Ce = Ce_1$, the product by $1 - e$ gives $0 = C(1 - e)e_1$, that is $e_1 = ee_1$. By symmetry we get $e = e_1$.

ii) $\Rightarrow$ i) The image of $1 - e$ in C/eC is 1, thus we have a surjective morphism $C_{1-e} \to C/eC$. It is in fact an isomorphism since its kernel $(eC)_{1-e}$ is zero due to the relation $(1 - e)(eC) = 0$. Moreover the morphism $\mathrm{Spec}(C_{1-e}) \to \mathrm{Spec}(C)$ is an open immersion.

ii) $\Rightarrow$ iii) One has $C_1 = C/eC$; let $C_0 = C/(1 - e)C$. Then we obtain a factorization $C = C_0 \times C_1$ such that U is the image of the morphism $\mathrm{Spec}(C_1) \to \mathrm{Spec}(C)$ defined by the projection $C \to C_1$.

iii) $\Rightarrow$ iv) Clear.

iv) $\Rightarrow$ ii) Since C_1 is a projective C-module, the C-linear surjection π admits a C-linear section, that is a map $\sigma\colon C_1 \to C$ such that $\pi\sigma = \mathrm{Id}$. By definition of the action, we have $c\,.\,c_1 = \pi(c)c_1$ for any $c \in C$ and $c_1 \in C_1$. Hence $c\sigma(c_1) = \sigma(\pi(c)c_1)$. This applies in particular to $c = \sigma(1)$ and $c_1 = 1$, from which we see that $\sigma(1)$ is an idempotent. Now applying the equality to $c_1 = 1$ and $c \in \mathrm{Ker}(\pi)$ we get $c\sigma(1) = 0$, and hence $c = ce$, where $e = 1 - \sigma(1)$ is also idempotent. Conversely, the relation $c = ce$ implies that $\pi(c) = 0$ since $\pi(\sigma(1)) = 1$. Thus $\mathrm{Ker}(\pi)$ is generated by e. □

1.2. DEFINITION. A ring C is said to be *connected* if $\mathrm{Spec}(C)$ is connected as a topological space.

The above lemma shows that a ring C is connected if and only if it contains no idempotent other than 0 and 1.

1.3. PROPOSITION. *Let C be a ring, and let P be a projective C-module of finite type. Then the support of P is closed and open in* $\mathrm{Spec}(C)$. *Equivalently there is a unique idempotent e in C such that* $\mathrm{Ann}_C(P) = eC$; *moreover, P is a C/eC-module which is projective. In particular, if the support of P is equal to* $\mathrm{Spec}(C)$, *then* $\mathrm{Ann}_C(P) = 0$.

More generally, for any integer d, the set of prime ideals $\mathfrak{p}$ such that $\mathrm{rk}_{\mathfrak{p}}(P_{\mathfrak{p}}) = d$ *is closed and open. In particular, if C is connected, the map* $\mathfrak{p} \to \mathrm{rk}_{\mathfrak{p}}(P_{\mathfrak{p}})$ *is constant, and thus the rank of P is well defined.*

Proof. Since P is of finite type the formation of the ideal $\mathrm{Ann}_C(P)$ commutes with localization, and the support of P is the closed set $V(\mathrm{Ann}_C(P))$. Let $C_1 = C/\mathrm{Ann}_C(P)$. According to the implication iv) $\Rightarrow$ ii) of Lemma 1.1, we have to prove that C_1 is a projective C-module. For doing so we use twice Theorem 1 of [AC], II, 5.2: P is projective if and only if for every maximal ideal $\mathfrak{m}$ of C, there exists $t \in C \setminus \mathfrak{m}$ such that P_t is a free C_t-module; but for such a t we have $(C_1)_t = C_t/\mathrm{Ann}_{C_t}(P_t) = 0$ if $P_t = 0$, and $(C_1)_t = C_t$ otherwise; in any case it is indeed a free C_t-module.

Finally, the set of primes $\mathfrak{p}$ such that $\mathrm{rk}_{\mathfrak{p}}(P_{\mathfrak{p}}) \geq d$ is the support of the wedge product $\wedge^d(P)$, which is closed. Hence the set of primes $\mathfrak{p}$ such that $\mathrm{rk}_{\mathfrak{p}}(P_{\mathfrak{p}}) = d$ is open and closed. □

1.4. PROPOSITION. *Let $C \longrightarrow C'$ be a morphism of commutative rings such that C' is a non-zero projective C-module of finite type. If C is connected, then there exists a surjection of rings $C' \to C''$ such that C'' is a non-zero projective C-module, and C'' is* connected.

Proof. Since C is connected, it follows from Proposition 1.3 that each non-zero quotient ring C'' of C' which is C-projective has a strictly positive well-defined rank over C; such a quotient C'' with minimal rank is connected. In fact, by Lemma 1.1, an idempotent of C'' would produce a decomposition of C into a product of rings $C'' = C''_0 \times C''_1$. If they both were non zero, each factor would have a strictly smaller rank. □

1.5. PROPOSITION. *Let $p(T)$ be a monic polynomial in $A[T]$, of degree n. Denote by t the class of T in $B = A[T]/(p)$. Then*

i) *The characteristic polynomial $p_{t,B}(T)$ of multiplication by t on B is equal to $p(T)$. If $p(T)$ splits over A as $p(T) = \prod_{i=1}^{n}(T - \lambda_i)$, then, for all polynomials $f(T)$ in $A[T]$, we have*

$$p_{f(t),B}(T) = \prod_{i=1}^{n}(T - f(\lambda_i)).$$

ii) *Let $A[T] \to C$ be a surjective morphism of rings. Then C is a projective module over A, of constant (finite) rank, if and only if the kernel of this morphism is generated by a monic polynomial $q(T)$; we thus have an isomorphism $A[T]/(q) \simeq C$. The morphism $A[T] \to C$ factors as $A[T] \to B \to C$ if and only if the polynomial $q(T)$ divides $p(T)$.*

iii) *Assume that the ring B decomposes as a product $B = B_0 \times B_1$, with B_i of constant rank over A. Then the polynomial p factors as a product $p(T) = p_0(T)p_1(T)$ of two monic polynomials, with isomorphisms $A[T]/(p_i) \simeq B_i$, and these polynomials are comaximal, that is, $p_0A[T] + p_1A[T] = A[T]$.*

Proof. i) On the A-module basis $1, t, \ldots, t^{n-1}$ of B, multiplication by t is represented by the *companion matrix* of $p(T)$, whose characteristic polynomial is well known to be equal to $p(T)$, as a standard calculation shows. This is also a direct consequence of the Hamilton-Cayley theorem, which states that $p_{t,B}(t) = 0$; hence p divides $p_{t,B}$, and both polynomials have the same degree.

If $p(T) = (T - \lambda_1)\cdots(T - \lambda_n)$ in $A[T]$, an A-module basis for B is given by

$$1,\ t - \lambda_1,\ (t - \lambda_1)(t - \lambda_2),\ \ldots,\ (t - \lambda_1)\cdots(t - \lambda_{n-1}).$$

On this basis multiplication by t is represented by a triangular matrix with the elements $\lambda_1, \ldots, \lambda_n$ on the diagonal. Thus multiplication by $f(t)$ is represented by a triangular matrix with the elements $f(\lambda_1), \ldots, f(\lambda_n)$ on the diagonal.

ii) Let $A[T] \to C$ be a surjective homomorphism, where C is projective of rank m over A, and let $q(T)$ be the characteristic polynomial of the product by the image t_C of T in C. By the Cayley-Hamilton theorem we have a surjective homomorphism of A-algebras $A[T]/(q) \longrightarrow C$. Since these algebras have the same rank m, the morphism is an isomorphism. The last part follows, since $p(t_C) = 0$, and thus the polynomial $q(T)$ divides $p(T)$.

iii) Let $p_i(T)$ be the characteristic polynomial of multiplication by t on B_i. Since we have a direct decomposition of B as a product, the characteristic polynomial of t in B factors as $p_0(T)p_1(T)$. From i) we deduce that $p(T) = p_0(T)p_1(T)$, and from ii) we get isomorphisms $A[T]/(p_i) \simeq B_i$. Finally, it is a general fact that two ideals I and J in a ring R are relatively prime if the morphism $R \to R/I \times R/J$ is bijective, as can be seen by tensoring by R/I. □

2. FINITE ÉTALE ALGEBRAS

In this section we recall some results related to finite étale morphisms. Geometrically they may be seen as étale coverings. In fact, the main example of a finite étale A-algebra is a finite product A^n of copies of A; "locally" it is the only one (see 2.4). In the sequel, finite étale A-algebras will mainly appear as quotients $A[T]/(p)$ where p is a monic polynomial whose discriminant is invertible in A, i.e. a *separable* polynomial (see 2.8).

Proposition 2.9 deserves to be pointed out because it is often used in the text. For a thorough exposition on étale algebras, see of course [EGA], IV, 17.6, 18.3.

2.1. DEFINITION. A morphism of rings $A \longrightarrow B$ is said to be *finite étale* if it makes B into a projective A-module of finite type and if the multiplication $\mu\colon B \otimes_A B \longrightarrow B$ makes B into a projective module over $B \otimes_A B$.

The kernel of μ is the ideal generated by the elements $b \otimes 1 - 1 \otimes b$; due to Lemma 1.1 (whose idempotent, denoted by e, is here $1 - e$), the condition on μ is equivalent to:

2.2. *There exists an element* $e \in B \otimes_A B$ *such that* $\mu(e) = 1$ *and* $e\,.\,(b \otimes 1) = e\,.\,(1 \otimes b)$ *for all* $b \in B$.

An element e with these properties is an idempotent since the first condition implies that $e - 1 \in \mathrm{Ker}(\mu)$, and the second that $e\,.\,\mathrm{Ker}(\mu) = 0$. Such an idempotent e is unique when it exists, and $1 - e$ is a generator of the ideal $\mathrm{Ker}(\mu)$.

For simplicity we sometimes write that a ring homomorphism $A \to B$ 'is' a projective quotient if it is surjective and makes B into a projective A-module. In the next lemma we collect the properties of finite flat algebras used in the sequel.

2.3. LEMMA. i) *A surjective morphism* $A \to B$ *is étale if and only if it is a projective quotient, that is, if its kernel is generated by an idempotent.*

ii) *Let* $f\colon A \longrightarrow B$ *be a homomorphism making* B *into a projective* A*-module of finite type. Then* f *is faithfully flat if and only if* f *is injective. If* A *is connected and* $B \neq 0$ *or, more generally, if for each prime* $\mathfrak{p}$ *of* A, $\mathrm{rank}_{\mathfrak{p}}(B)$ *is non zero, then* f *is faithfully flat.*

iii) *Let* $f\colon A \longrightarrow B$ *and* $g\colon B \longrightarrow C$ *be finite étale algebras. Then* $gf\colon A \longrightarrow C$ *is also a finite étale algebra.*

iv) *Let* $f\colon A \longrightarrow B$ *be a finite étale algebra with* A *connected and* $B \neq 0$. *Then there is a non-zero projective quotient* $B \to B'$ *which is connected and étale over* A.

v) *Let* $f\colon A \longrightarrow B$ *be a homomorphism and* $f'\colon A' \longrightarrow A' \otimes_A B$ *be the morphism obtained by the base change* $A \to A'$. *If* f *is finite étale then so is* f'. *Conversely, if* f' *is finite étale, and* $A \to A'$ *is faithfully flat, then* $A \longrightarrow B$ *is finite étale as well.*

Proof. i) This is clear from Lemma 1.1, since, in this case, $B \otimes_A B = B$.

ii) A faithfully flat morphism is injective ([AC], I, 3.5). Suppose that f is injective. We have to show that $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is surjective ([AC], II, 2.5); this is a consequence of the "going up theorem", but here we may give the following easy proof. Let $\mathfrak{p}$ be a prime ideal of A. The morphism $A_{\mathfrak{p}} \longrightarrow B_{\mathfrak{p}}$ is injective, so that $B_{\mathfrak{p}}$ is non zero. Since $B_{\mathfrak{p}}$ is a finitely generated projective module over the local ring $A_{\mathfrak{p}}$, it is free and non zero. Therefore the ring $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ is non zero, and each of its prime ideals restricts to $\mathfrak{p}$. We have thus shown that $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is surjective.

iii) In the following diagram, where μ_f and μ_g are multiplication maps and m is the natural homomorphism, the square is co-cartesian, that is, it makes $C \otimes_B C$ into a tensor product of the three other rings

$$\begin{array}{ccccc} C \otimes_A C & \xrightarrow{m} & C \otimes_B C & \xrightarrow{\mu_g} & C \\ \uparrow & & \uparrow & & \\ B \otimes_A B & \xrightarrow[\mu_f]{} & B & & \end{array}$$

Since f is étale, μ_f is a projective quotient, and hence the same is true for m. Since g is étale, μ_g is a projective quotient. Therefore $\mu_{gf} = \mu_g m$ is also a projective quotient.

iv) The proof is similar to that of Proposition 1.4, since a projective quotient of B is still étale over A, by i) and iii).

v) The direct statement comes from the fact that projectiveness is preserved under any base change. Conversely, according to [AC], I, 3.6, prop. 12, the hypothesis implies that B is a finitely generated projective A-module. If we apply the latter result to the faithfully flat morphism

$$B \otimes_A B \longrightarrow A' \otimes_A (B \otimes_A B) = (A' \otimes_A B) \otimes_{A'} (A' \otimes_A B)$$

and to the $B \otimes_A B$-module B, we conclude that B is a projective $B \otimes_A B$-module. □

2.4. PROPOSITION. *Let $A \longrightarrow B$ be a morphism. Then the following conditions are equivalent:*

i) *The morphism $A \longrightarrow B$ is finite étale of constant rank d.*

ii) *There exist a finite étale morphism $A \longrightarrow A'$ of constant rank $\leq d!$ and an isomorphism of A'-algebras $A' \otimes_A B \simeq A'^d$. If, moreover, A is connected then there exists such an A' which is also connected.*

iii) *There exist a faithfully flat morphism $A \longrightarrow A'$ and an isomorphism of A'-algebras $A' \otimes_A B \simeq A'^d$.*

Proof. i) ⇒ ii) We argue by induction on the rank d, starting from the case where $d = 1$, which is obvious. Since B is étale, the ring $B \otimes_A B$ contains two idempotents $1 - e$ and e which yield a decomposition as a product of rings $B \otimes_A B \simeq B \times C$. Consider $B \otimes_A B$ as a B-algebra via the first factor. It is a finite étale B-algebra of rank d, and from Lemma 2.3, i) and iii), we see that the composite $B \to B \otimes_A B \to C$ is a finite étale algebra of rank $d - 1$. By the induction hypothesis there exist a finite étale B-algebra $B \to A'$ of

constant rank $\leq (d-1)!$ over B and an isomorphism $A' \otimes_B C \simeq A'^{d-1}$. The composite $A \to B \to A'$ is finite étale by Lemma 2.3 iii), and of constant rank $\leq d!$, and we have the isomorphisms

$$A' \otimes_A B = A' \otimes_B (B \otimes_A B) \simeq A' \otimes_B (B \times C) \simeq A' \times A'^{d-1}.$$

If moreover A is connected, it follows from Lemma 2.3 iv) that there is a non-zero projective quotient of A' which is connected.

The implication ii) $\Rightarrow$ iii) is clear, since by Lemma 2.3 ii) a finite étale morphism of constant rank is faithfully flat.

The implication iii) $\Rightarrow$ i) follows from Lemma 2.3 v). □

2.5. NOTATION. Given a monic polynomial $p(T) \in A[T]$ we introduce the polynomial $\partial p(X,Y) \in A[X,Y]$ defined by the relation

$$p(X) - p(Y) = (X-Y)\,\partial p(X,Y).$$

Then $\partial p(X,X) = p'(X)$, where $p'(X)$ is the formal derivative of $p(X)$. This follows immediately, by linearity, from the case $p(T) = T^n$. See Remark 8.4 3) below for some complements on this polynomial.

The next two propositions develop some consequences of being étale for algebras of the form $A[T]/(p)$.

2.6. PROPOSITION. *Let $p(T) \in A[T]$ be a monic polynomial. Write $B = A[T]/(p)$ and denote by t the class of T in B. Denote further by $\mu\colon B \otimes_A B \to B$ the multiplication map. We assume that $p'(t)$ is invertible in B. Then the following three assertions hold:*

i) *The morphism $A \longrightarrow B$ is étale. More precisely, the element*

$$e = \frac{\partial p(t\otimes 1, 1\otimes t)}{p'(t)\otimes 1}$$

in $B \otimes_A B$ is an idempotent such that $\mu(e) = 1$ and such that, for all $b \in B$, we have $(b\otimes 1)\,.\,e = (1\otimes b)\,.\,e$.

ii) *The map $\varepsilon\colon B \longrightarrow B \otimes_A B$, defined by $\varepsilon(b) = (b\otimes 1)\,.\,e = (1\otimes b)\,.\,e$, induces an isomorphism $B \xrightarrow{\sim} \mathrm{Ann}_{B\otimes_A B}(t\otimes 1 - 1\otimes t)$.*

iii) *The sequence*

$$0 \longrightarrow B \xrightarrow{\varepsilon} B\otimes_A B \xrightarrow{t\otimes 1 - 1\otimes t} B\otimes_A B \xrightarrow{\mu} B \longrightarrow 0 \tag{2.6.1}$$

is exact and split as a sequence of $B\otimes_A B$-modules.

Proof. i) Since B is a free A-module, it is enough to check the conditions of 2.2. Since $\partial p(X,X) = p'(X)$ we obtain that $\mu(e) = \partial p(t,t)/p'(t) = 1$. From the relation $p(t) = 0$ and the definition of $\partial p(X,Y)$, we deduce that

$$(t \otimes 1 - 1 \otimes t) \,.\, e = (\,p(t \otimes 1) - p(1 \otimes t))/(\,p'(t) \otimes 1) = 0\,.$$

Finally, since t is a generator of the A-algebra B, we see that the relation $(t \otimes 1 - 1 \otimes t) \,.\, e = 0$ implies that $(b \otimes 1) \,.\, e = (1 \otimes b) \,.\, e$ for all b in B.

ii) Since the ideal $I = \mathrm{Ker}(\mu)$ is generated by $1 - e$, the ideal $\mathrm{Ann}_{B \otimes_A B}(t \otimes 1 - 1 \otimes t) = \mathrm{Ann}_{B \otimes_A B}(I)$ is generated by e.

iii) Due to ii), the exactness as a sequence of A-modules is clear. The map ε is $B \otimes_A B$-linear when B is endowed with the structure of $B \otimes_A B$-module coming from μ. Indeed we have:

$$\varepsilon(\mu(x \otimes y)) = \varepsilon(xy) = (xy \otimes 1) \,.\, e = (x \otimes 1)(y \otimes 1) \,.\, e = (x \otimes 1)(1 \otimes y) \,.\, e = (x \otimes y) \,.\, e$$

The sequence is split since B is a projective $B \otimes_A B$-module. □

2.7. REMARKS. 1) The formula for e in the proposition appears to be asymmetric, since in general $p'(t) \otimes 1 \neq 1 \otimes p'(t)$. However, the difference $p'(t) \otimes 1 - 1 \otimes p'(t)$ is a multiple of $t \otimes 1 - 1 \otimes t$; hence it is annihilated by $\partial p(t \otimes 1, 1 \otimes t)$, and we have $\partial p(t \otimes 1, 1 \otimes t)(1 \otimes p'(t)) = \partial p(t \otimes 1, 1 \otimes t)(\,p'(t) \otimes 1)$.

2) See 8.3 for a sequence analogous to (2.6.1), but without the assumption that $p'(t)$ is invertible.

We now turn to the *discriminant* of a polynomial (for more information, see for example [A], V, §6 and §7):

Let $p(T)$ in $A[T]$ be a monic polynomial of degree n. Since the algebra $B = A[T]/(p)$ is free over A, we have a norm map

$$\mathrm{N}_{B/A} \colon B \longrightarrow A\,, \quad \text{defined by } \mathrm{N}_{B/A}(b) = \det(b_B)\,, \quad \text{where } \quad b_B(x) = bx\,.$$

An element b in B is invertible in B if and only if $\mathrm{N}_{B/A}(b)$ is invertible in A. The *discriminant* of $p(T)$ is defined as

$$\mathrm{dis}(p) = (-1)^{n(n-1)/2}\, \mathrm{N}_{B/A}(\,p'(t))\,.$$

Thus $p'(t)$ is invertible in B if and only if the discriminant of $p(T)$ is invertible in A. Moreover, if $p(T)$ splits as $p(T) = (T - \mu_1) \cdots (T - \mu_d)$, then

$$\mathrm{dis}(p) = \prod_{i \neq j} (\mu_i - \mu_j)\,.$$

2.8. PROPOSITION. *Let $p(T) \in A[T]$ be a monic polynomial. Write $B = A[T]/(p)$ and denote by t the class of T in B. Then B is finite étale over A if and only if $p'(t)$ is invertible in B, a condition equivalent to the discriminant of $p(T)$ being invertible in A. We then say that the polynomial $p(T)$ is* separable.

Proof. By Proposition 2.6, the only point which remains to be proved is that $p'(t)$ is invertible if B is étale. For doing so we may assume that A is connected; from Proposition 2.4 we see that we can also assume that there is an isomorphism $B = A[T]/(p) \simeq A^n$. The image of t under this isomorphism may be written as $(\mu_1, \ldots, \mu_n)$ with $\mu_i \in A$. Since t is a generator of the A-algebra B, the sequence $(1, t, \ldots, t^{n-1})$ is a basis of this A-module, and thus the Vandermonde matrix

$$\begin{pmatrix} 1 & \mu_1 & \mu_1^2 & \cdots & \mu_1^{n-1} \\ 1 & \mu_2 & \mu_2^2 & \cdots & \mu_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \mu_n & \mu_n^2 & \cdots & \mu_n^{n-1} \end{pmatrix}$$

is invertible, that is $\mu_i - \mu_j$ is invertible in A when $i \neq j$. The discriminant of $p(T)$ is thus invertible. □

2.9. PROPOSITION. *Let B be a finite étale A-algebra, and let M be a B-module of finite type. If M is projective as an A-module, it is also projective as a B-module.*

In particular, if J is an ideal in B such that B/J is isomorphic to A, then B/J is a projective B-module.

Proof. We give two proofs of the proposition:

1) We can assume that A is connected, and hence that B has constant rank, say d. According to 2.4, there exist a faithfully flat morphism $A \longrightarrow A'$ and an isomorphism $A' \otimes_A B \simeq A'^d$. Since $A' \otimes_A M$ is a module over that ring, it splits as a product of A'-modules $M_1 \times \cdots \times M_d$. But, by assumption, $A' \otimes_A M$ is projective over A', and thus each factor M_i is also projective over A'. Hence $A' \otimes_A M$ is projective over $A' \otimes_A B$. The proposition follows by descent of projectiveness under faithfully flat morphisms ([AC], I, 3.6, prop. 12).

2) For the B-module structure coming from the first factor, the module $B \otimes_A M$ is projective. The given B-module structure on M yields a B-linear

map

$$\mu_M \colon B \otimes_A M \longrightarrow M\,, \quad \text{defined by} \quad \mu_M(b \otimes x) = bx\,.$$

To prove the proposition it suffices to show that μ_M admits a B-linear splitting, that is a map

$$\sigma \colon M \longrightarrow B \otimes_A M$$

such that $\mu_M \sigma = \mathrm{Id}_M$ and $\sigma(bx) = (b \otimes 1)\,.\,\sigma(x)$ where $b \otimes 1$ is in $B \otimes_A B$. In fact, the existence of such a B-linear splitting σ shows that M is B-isomorphic to the direct summand $\sigma(M)$ of the projective B-module $B \otimes_A M$, and therefore M is projective as a B-module.

To define $\sigma \colon M \to B \otimes_A M$ we use the idempotent $e \in B \otimes_A B$ coming from the definition of étale morphisms (see 2.2), and we let

$$\sigma(x) = e\,.\,(1 \otimes x)\,.$$

This map is B-linear since $e\,.\,(1 \otimes b) = e\,.\,(b \otimes 1)$. In fact, $\sigma(bx) = e\,.\,(1 \otimes bx) = e\,.\,(1 \otimes b)(1 \otimes x) = e\,.\,(b \otimes 1)(1 \otimes x) = (b \otimes 1)\,.\,\sigma(x)$. Since $\mu(e) = 1$ we have $\mu_M \sigma(x) = \mu_M(e\,.\,(1 \otimes x)) = \mu(e)\mu_M(1 \otimes x) = x$. □

3. Endomorphisms with a separable characteristic polynomial

We first introduce some notation and prove some results used in the proof of Theorem 3.3.

3.1. Notation. In what follows, A will denote a ring and M an A-module of finite type with an A-linear endomorphism $u \colon M \to M$. When M is a projective A-module of rank n we denote by $p_u(T)$ the *characteristic polynomial* of u in $A[T]$, that is, $p_u(T) = \det(T - u)$. By the Cayley-Hamilton theorem, M is also an $A[T]/(p_u)$-module.

We shall on several occasions use that, given a monic polynomial $p(T)$ in $A[T]$, there is an A algebra $A \to A'$ which is free of finite rank as an A-module and such that $p(T)$ splits completely over A' as $p(T) = \prod_{i=1}^{n}(T - \lambda_i)$. The splitting algebra of $p(T)$ provides such an algebra which is also universal for splittings; see e.g. [A], IV, 6.5, [E-L1], and [L-T] (or [F1] for a much more general point of view).

3.2. LEMMA. *Assume that M is a projective A-module of rank n, and let $q(T)$ in $A[T]$ be a monic non-constant divisor of the characteristic polynomial $p_u(T)$ of $u\colon M \to M$. Then* $\det(q(u)) = 0$.

Proof. Let $A \to A'$ be an A-algebra which is free of finite rank as an A-module, and over which $q(T)$ splits as $q(T) = \prod_{i=1}^{m}(T - \lambda_i)$. Since the morphism $A \to A'$ is injective, and since $\det(q(1_{A'} \otimes u))$ is the image in A' of $\det(q(u))$, we can assume from the outset that $q(T)$ splits over A as $q(T) = \prod_{i=1}^{m}(T - \lambda_i)$ with λ_i in A. Then we have

$$\det(q(u)) = \prod_{i=1}^{m} \det(u - \lambda_i)\,.$$

However, since a root λ_i of $q(T)$ is also a root of $p_u(T)$, we obtain

$$\det(u - \lambda_i) = (-1)^n \det(\lambda_i - u) = (-1)^n p_u(\lambda_i) = 0\,.$$

In particular, we have $\det(q(u)) = 0$. □

The following theorem is the first important result of the article.

3.3. THEOREM. *Let M be a projective A-module of rank $n > 0$, and let $u\colon M \to M$ be an A-linear endomorphism with characteristic polynomial $p_u(T)$. Write $B = A[T]/(p_u)$. We suppose that the discriminant of $p_u(T)$ is invertible in A, i.e. that B is étale over A.*
1) *If moreover $p_u(T)$ splits over A as $p_u(T) = \prod_{i=1}^{n}(T - \lambda_i)$, then the following two maps are isomorphisms*

$$\bigoplus_i \operatorname{Ker}(u - \lambda_i) \longrightarrow M \longrightarrow \prod_j M/(u - \lambda_j)\,M$$

and, for each i, the composite map

$$\operatorname{Ker}(u - \lambda_i) \longrightarrow M \longrightarrow M/(u - \lambda_i)\,M$$

is an isomorphism.

2) *The following three equivalent assertions hold:*

i) *The B-module M is invertible, i.e. it is projective of rank 1.*

ii) *If $p_u(T)$ splits over A as $p_u(T) = \prod_{i=1}^{n}(T - \lambda_i)$, then, for each i, the quotient $M/(u - \lambda_i)\,M$ is an invertible A-module.*

iii) *If $p_u(T)$ splits over A as $p_u(T) = \prod_{i=1}^{n}(T - \lambda_i)$, then, for each i, the submodule $\operatorname{Ker}(u - \lambda_i)$ is an invertible A-module.*

Proof of 1). As the characteristic polynomial is supposed to be separable, its factors $(T - \lambda_i)$ are pairwise comaximal, and hence the morphism

$$B \longrightarrow \prod_{i=1}^{n} B/(t - \lambda_i)\, B$$

is an isomorphism. Moreover, for each i, we have the isomorphism $B/(t - \lambda_i)\, B \xrightarrow{\sim} A$, defined by $t \mapsto \lambda_i$. By composition we get an isomorphism $B \xrightarrow{\sim} A^n$; the projection $p_i \colon B \to A$ onto the i-th factor is characterized by $p_i(t) = \lambda_i$. Tensoring with M, we get the isomorphism

$$M = B \otimes_B M \xrightarrow{\sim} \prod_i M_i\,,$$

where M_i denotes the module $(B/(t - \lambda_i)\, B) \otimes_B M = M/(u - \lambda_i)\, M = p_i^{\star} M$. Now we will prove that the composite map

$$(\star)_{i,j} \qquad \mathrm{Ker}(u - \lambda_i) \longrightarrow M \longrightarrow M/(u - \lambda_j)\, M$$

is zero if $i \neq j$, and that it is an isomorphism for $j = i$. This will imply that the composite map

$$\bigoplus_i \mathrm{Ker}(u - \lambda_i) \longrightarrow M \xrightarrow{\sim} \prod_j M/(u - \lambda_j)\, M$$

is an isomorphism, whence the map on the left is also an isomorphism.

Let us fix an index i and let $q(T) = \prod_{j \neq i} (T - \lambda_j)$. There exists a monic polynomial $r(T)$ such that

$$q(\lambda_i) = q(T) + (T - \lambda_i)\, r(T)\,.$$

Since the polynomial $p(T) = (T - \lambda_i)\, q(T)$ is separable, the element $q(\lambda_i)$ is invertible in A. Introducing the endomorphisms $v = q(\lambda_i)^{-1} q(u)$ and $w = q(\lambda_i)^{-1} r(u)$, we get the equality

$$(\star\star) \qquad \mathrm{Id}_M = v + (u - \lambda_i)\, w\,.$$

The Cayley-Hamilton theorem implies that $0 = p(u) = q(u)(u - \lambda_i) = (u - \lambda_i)\, q(u)$. From this we deduce the relations $v(u - \lambda_i) = 0$ and $\mathrm{Im}(v) \subset \mathrm{Ker}(u - \lambda_i)$, and the equality $(\star\star)$ shows that

$$v = v^2 \qquad \text{and} \qquad \mathrm{Im}(v) = \mathrm{Ker}(u - \lambda_i)\,.$$

It is immediate from the definitions that $\mathrm{Im}(v) = \mathrm{Im}(q(u)) \subset \bigcap_{j \neq i} \mathrm{Im}(u - \lambda_j)$, so that $\mathrm{Ker}(u - \lambda_i) \subset \bigcap_{j \neq i} \mathrm{Im}(u - \lambda_j)$. Therefore, for $i \neq j$, the map

$$(\star)_{i,j} \qquad \mathrm{Ker}(u - \lambda_i) \to M \to M/(u - \lambda_j)\, M$$

is zero. Now, the kernel of the map

$$(\star)_{i,i} \qquad \mathrm{Ker}(u-\lambda_i) \to M \to M/(u-\lambda_i)M$$

is $\mathrm{Ker}(u-\lambda_i) \cap \mathrm{Im}(u-\lambda_i)$. But if $x \in \mathrm{Ker}(u-\lambda_i)$ then $x = v(x)$, and if $x \in \mathrm{Im}(u-\lambda_i)$ then $v(x) = 0$. Thus the map $(\star)_{i,i}$ is injective. It is also surjective since the equality $(\star\star)$ shows that $x \equiv v(x) \mod (u-\lambda_i)M$, and we know that $v(x) \in \mathrm{Ker}(u-\lambda_i)$.

Proof of 2). Note first that, according to [AC], I, 3.6, prop. 12, the conclusion of i) is valid if and only if it is established after a faithfully flat base change. Thus we may, and we will, suppose that the characteristic polynomial is split.

Proving the equivalence i) $\Leftrightarrow$ ii) reduces to proving that M is invertible over B if and only if each factor M_i is an invertible A-module. This is clear geometrically: if we allow ourselves to look at M and the M_i as sheaves on $\mathrm{Spec}(B)$ and $\mathrm{Spec}(A)$ respectively, then $M_i = p_i^\star M$ appears as the restriction of M over the open and closed image set of

$$\mathrm{Spec}(A) \xrightarrow{\mathrm{Spec}(p_i)} \mathrm{Spec}(B),$$

and these open sets cover $\mathrm{Spec}(B)$.

The equivalence of ii) and iii) comes from the isomorphism $(\star)_{i,i}$.

We next prove that M is an invertible B-module. Since B is étale over A it follows from Proposition 2.9 that M is a projective B-module. Hence it remains to prove that M is of rank one. This is a consequence of the following slightly more general result:

3.3.1. LEMMA. *Let $u: M \to M$ be an endomorphism of a projective A-module of finite type. Let $q(T)$ be a monic divisor of its characteristic polynomial p_u, such that $q(u) = 0$. We suppose that M is a projective module over $A[T]/(q)$. Then the support of M as an $A[T]$-module is $V(q)$.*

Moreover, if $q = p_u$ then M is invertible over $A[T]/(p_u)$.

It is good to keep in mind the extreme example of the zero endomorphism of A^n, with $n \geq 2$; then $p_0(T) = T^n$, and we can take $q(T) = T$.

Proof. We let $C = A[T]/(q)$; it is a quotient of $B = A[T]/(p_u)$, and M is endowed with a structure of C-module. We first prove that the support of M is equal to $\mathrm{Spec}(C) = V(q)$. To this end, we may clearly assume that $\mathrm{Spec}(A)$ is connected. It follows from Proposition 1.3 that the support of M

is closed and open in $\mathrm{Spec}(C)$. Hence it follows from Lemma 1.1 that we can factor C into a product $C = C_0 \times C_1$ of rings, where $\mathrm{Spec}(C_1)$ is isomorphic to the support of M and $C_0 \otimes_C M = 0$.

Since we assume that $\mathrm{Spec}(A)$ is connected, it follows from Proposition 1.5 ii) that there is a monic divisor $q_0(T)$ of $q(T)$ such that $C_0 = A[T]/(q_0)$. The relation $C_0 \otimes_C M = 0$ can thus be written $M = q_0(u)M$. The latter equality implies [1]) that $q_0(u)$ is an isomorphism of M. Hence it follows from Lemma 3.2 that $q_0(T) = 1$, and consequently that $C_0 = 0$.

We now suppose that $q = p_u$, i.e. that $B = C$. To prove that $\mathrm{rank}_B(M) = 1$, we may assume that A is a field k. Since B is then a finite algebra over a field, we can write B as a product of local rings $B = K_1 \times \cdots \times K_m$, each being a finite k-algebra. Thus $M = M_1 \times \cdots \times M_m$, where $M_i = K_i \otimes_B M$ is a free K_i-module since M is projective over B, and this free module is non zero because $\mathrm{Spec}(K_i)$ is in the support of M, as shown above. We have

$$\dim_k(M) = \sum_{i=1}^{m} \dim_k(M_i) = \sum_{i=1}^{m} \dim_k(K_i)\,\mathrm{rank}_{K_i}(M_i)\,.$$

Moreover, since $B = A[T]/(p_u)$ we have $\dim_k(M) = n = \deg(p_u) = \dim_k(B)$ and thus $\dim_k(M) = \sum_{i=1}^{m} \dim_k(K_i)$. Since, for all i, we have observed that $\mathrm{rank}_{K_i}(M_i) \geq 1$, we obtain that $\mathrm{rank}_{K_i}(M_i) = 1$ for all i. Hence M is an invertible B-module. □

3.4. COROLLARY. *Let M be a projective A-module of rank n, and let $u : M \to M$ be an A-linear endomorphism with characteristic polynomial $p_u(T)$. Write $B = A[T]/(p_u)$. If $p_u(T)$ is separable, that is if the discriminant of $p_u(T)$ is invertible in A, then:*

i) *The only A-module endomorphisms of M that commute with u are the polynomials in u with coefficients in A.*

ii) *A polynomial $q(T)$ in $A[T]$ satisfies $q(u) = 0$ if and only if $q(T)$ is a multiple of $p_u(T)$, i.e. p_u is the minimal polynomial (see §4).*

iii) *Assume that* $\mathrm{Spec}(A)$ *is connected. Let N be an A-submodule of M that is stable under u, that is $u(N) \subseteq N$, and such that M/N is projective over A. Then there exists a unique monic divisor $q(T)$ of $p_u(T)$ such that $N = q(u)M$.*

Conversely, if $q(T)$ in $A[T]$ is a monic divisor of $p_u(T)$, then $q(u)M$ is stable under u, and $M/q(u)M$ is a projective A-module.

[1]) The surjectivity of $q_0(u)$ implies the surjectivity of the endomorphism $\det(q_0(u)) = \wedge^n q_0(u)$ of the invertible module $\wedge^n M$. Hence $\det(q_0(u))$ is bijective, and $q_0(u)$ is an isomorphism.

Proof. The subalgebra of $\mathrm{End}_A(M)$ consisting of A-endomorphisms that commute with u is nothing but $\mathrm{End}_B(M)$. Moreover, M is an invertible B-module by the theorem, so the canonical morphism $B \to \mathrm{End}_B(M)$ is an isomorphism. Hence assertion i) holds.

Assertion ii) is equivalent to having the inclusion $B \simeq \mathrm{End}_B(M) \subseteq \mathrm{End}_A(M)$.

The module M/N of assertion iii) is a B-module since N is stable under u. By assumption, M/N is a projective A-module and the morphism $A \to B$ is étale. We deduce from Proposition 2.9 that M/N is a projective B-module, and it is of rank ≤ 1 as a quotient of the invertible B-module M. By Proposition 1.3 and Lemma 1.1, the support of M/N is the image of a morphism $\mathrm{Spec}(C) \longrightarrow \mathrm{Spec}(B)$, where C is a projective quotient of B. Thus M/N is an invertible C-module. The surjective map of B-modules $M \longrightarrow M/N$ gives rise to a surjective map of invertible C-modules $C \otimes_B M \longrightarrow M/N$, and thus the latter is an isomorphism.

Now, since $\mathrm{Spec}(A)$ is connected by assumption, it follows from Proposition 1.5 ii) that there is a monic divisor $q(T)$ of $p_u(T)$ such that $C = A[T]/(q)$. The above isomorphism $C \otimes_B M \to M/N$ gives an isomorphism $M/q(u)M \simeq M/N$, that is $N = q(u)M$.

Conversely, let $q(T)$ be a monic divisor of $p_u(T)$. Then $M/q(u)M$ is an invertible module over $A[T]/(q) = B/q(t)B$, and in particular, a projective A-module. Finally, it is obvious that $q(u)M$ is stable under u. □

3.5. EXAMPLES. Here are two examples coming from geometry:

1. The first one is an example of an endomorphism of a *free* module with *constant* eigenvalues, whose eigenspaces are projective of rank one but *not free*.

Let $A = \mathbf{R}[X, Y]/(X^2 + Y^2 - 1)$ be the ring of real polynomial functions on the circle, and denote by x and y the classes of X and Y. Consider the A-algebra $M = \mathbf{C} \otimes_{\mathbf{R}} A$ as a free A-module of rank 2, with basis $(1 \otimes 1, i \otimes 1)$. For $a, b \in A$ we shall simply write $a + ib$ instead of the more correct $1 \otimes a + i \otimes b$. The map

$$u\colon \mathbf{C} \otimes_{\mathbf{R}} A \longrightarrow \mathbf{C} \otimes_{\mathbf{R}} A, \qquad a + ib \longmapsto (x + iy)(a - ib) \tag{3.5.1}$$

is A-linear, but of course it is not $\mathbf{C} \otimes_{\mathbf{R}} A$-linear since it involves the complex conjugation. On the specified basis the matrix of u is $\left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right)$, and the characteristic polynomial of u is $p_u(T) = T^2 - 1$. Let L and L' be the two eigenspaces relative to the eigenvalues 1 and -1 respectively (see [F2]

for a thorough but elementary discussion of these eigenspaces and their relation to the Möbius strip). Let $z = x + iy$. For any $\alpha \in \mathbf{C} \otimes_{\mathbf{R}} A$ we have $\alpha + z\bar{\alpha} \in L$ and $\alpha - z\bar{\alpha} \in L'$, whence we get a decomposition as a direct sum of A-modules

$$\mathbf{C} \otimes_{\mathbf{R}} A = A^2 = L \oplus L' .$$

Moreover the A-algebra $B = A[T]/(p_u)$ of Theorem 3.3 is here the product of two copies of A along which the B-module M splits into the product $L \times L'$. Thus, as stated in Theorem 3.3, M is indeed an invertible B-module.

Let us show that the A-module L is invertible *but not free*, and that the same is true for L'. Since an element in A can also be viewed as a real polynomial function on the circle $\mathbf{S}_1$, we consider $f = a + ib$ as a polynomial function $f\colon \mathbf{S}_1 \longrightarrow \mathbf{C}$, in the usual way. Namely, to a point $\zeta \in \mathbf{S}_1$ is attached a morphism of $\mathbf{R}$-algebras $A \longrightarrow \mathbf{C}$, and we denote by $f(\zeta)$ the complex number which is the image of f under this morphism. Thus the image of $x + iy$ is precisely ζ. Hence the elements of L are polynomial functions $f\colon \mathbf{S}_1 \longrightarrow \mathbf{C}$ satisfying, for all $\zeta \in \mathbf{S}_1$, the relation, analogous to (3.5.1),

$$f(\zeta) = \zeta \,.\, \overline{f(\zeta)} . \tag{3.5.2}$$

We will show that any such function f has a zero on $\mathbf{S}_1$ and thus cannot be a generator of L. To do this, we introduce the function $\varphi(\zeta) = f(\zeta) f(\bar{\zeta})$, which is easily seen to have only real values. Since the topological space $\mathbf{S}_1$ is connected and compact, $\varphi(\mathbf{S}_1)$ is a closed interval in $\mathbf{R}$, and we have to show that this interval contains 0. The relation (3.5.2) implies that $f(1)$ is real and that $f(-1)$ is purely imaginary. Hence $\varphi(1) \geq 0$ and $\varphi(-1) \leq 0$, and we are done. □

2. In the second example the A-module M is free of rank 3 but it contains a stable direct factor of rank 2 which is not free. The main point comes from the article [S] by Samuel.

Let $A = \mathbf{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$ be the ring of polynomial functions on the sphere $\mathbf{S}_2$, and denote by x, y, z the classes of X, Y, Z, respectively. In order to define our endomorphism of the free module $M = A^3$, we introduce its canonical basis (e_1, e_2, e_3); attached to it are the usual scalar product, denoted by $(- \mid -)$, and the isomorphism

$$\varphi\colon\ \wedge^2 (A^3) \longrightarrow A^3 , \qquad e_1 \wedge e_2 \mapsto e_3 , \quad e_2 \wedge e_3 \mapsto e_1 , \quad e_3 \wedge e_1 \mapsto e_2 .$$

This isomorphism is characterized by the relation $(\varphi(\alpha \wedge \beta) \mid \gamma)\, e_1 \wedge e_2 \wedge e_3 = \alpha \wedge \beta \wedge \gamma$. The term $\varphi(\alpha \wedge \beta)$ is usually called, for real three-dimensional Euclidean spaces, the *vector product* of α and β, and will be denoted by $\alpha \,\overline{\wedge}\, \beta$. We will use the classical relation

$$\alpha \,\overline{\wedge}\, (\beta \,\overline{\wedge}\, \gamma) = (\alpha \mid \gamma)\beta - (\alpha \mid \beta)\gamma . \tag{3.5.3}$$

Letting $\omega = xe_1 + ye_2 + ze_3$, we define the endomorphism $u\colon A^3 \longrightarrow A^3$ by the relation

$$u(\alpha) = \omega \barwedge \alpha\,.$$

The matrix of u on the canonical basis is

$$\begin{pmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{pmatrix}$$

From the formula (3.5.3) we, at once, deduce that $u^2(\alpha) = (\omega \mid \alpha)\omega - \alpha$, so that $u^3 = -u$, since $u(\omega) = 0$ and $(\omega \mid \omega) = 1$. Hence the characteristic polynomial of u is $p_u(T) = T(T^2 + 1)$.

The eigenspace $\mathrm{Ker}(u)$, relative to the root $T = 0$, is the free submodule $L = A\omega$, as the relation $u^2(\alpha) + \alpha = (\omega \mid \alpha)\omega$ shows. The same relation implies that the submodule $P = \mathrm{Ker}(u^2 + 1)$ of A^3 is the set of α's such that $(\omega \mid \alpha) = 0$, that is the orthogonal of L.

We may interpret P as the bundle of the tangent vectors to the sphere $\mathbf{S}_2$ as follows: let us view $\mathbf{S}_2$ as a subset of $\mathbf{R}^3$; to a point $\zeta \in \mathbf{S}_2$ is associated the morphism of $\mathbf{R}$-algebras $A \longrightarrow \mathbf{R}$ which sends a polynomial $a \in A$ to its value $a(\zeta)$. Its extension $A^3 \longrightarrow \mathbf{R}^3$ sends ω to ζ, and the image of $\alpha \in P$ is a vector $\alpha(\zeta)$ orthogonal to ζ, which therefore has to be seen as a tangent vector to $\mathbf{S}_2$ at the point ζ. Now a deep result of J.L.E. Brouwer (see for example [M], p. 30) asserts that any tangent vector field on the real sphere must vanish somewhere. Therefore no α can be part of a basis of P, and hence the A-module P is not free.

The ring $B = A[T]/(T(T^2 + 1))$ is clearly étale over A, and it splits as the product $A \times C$, where $C = A[T]/(T^2 + 1)$. The B-module $M = A^3$ with its endomorphism splits accordingly as $A\omega \times P$. The factor P is an invertible C-module and it is not free, since C is free over A and P is not.

By its very definition, C is isomorphic to $\mathbf{C} \otimes_{\mathbf{R}} A$. In [S], p. 165, Samuel shows that A is a factorial domain but $\mathbf{C} \otimes_{\mathbf{R}} A$ is not. He also shows that $\mathbf{C} \otimes_{\mathbf{R}} M$ is free of rank 2, over $\mathbf{C} \otimes_{\mathbf{R}} A$. We thus have an exact sequence of $\mathbf{C} \otimes_{\mathbf{R}} A$-modules

$$0 \longrightarrow M' \longrightarrow \mathbf{C} \otimes_{\mathbf{R}} M \longrightarrow M \longrightarrow 0\,,$$

where M and M' are invertible $\mathbf{C} \otimes_{\mathbf{R}} A$-modules which are not free. □

Theorem 3.3 allows us to get a proof of the spectral mapping theorem by specializing from the generic polynomial, which has indeed a separable characteristic polynomial.

3.6. THE SPECTRAL MAPPING THEOREM. *Let M be a projective A-module of rank n, and let $u\colon M \to M$ be an A-linear endomorphism with characteristic polynomial $p_u(T)$. If $p_u(T)$ splits over A as $p_u(T) = \prod_{i=1}^{n}(T - \lambda_i)$, then, for every polynomial $f(T)$ in $A[T]$, we have $p_{f(u)}(T) = \prod_{i=1}^{n}(T - f(\lambda_i))$.*

Proof. When the discriminant of $p_u(T)$ is invertible in A, the assertion is an immediate consequence of Theorem 3.3 ii), since the endomorphism $f(u)$ induces on the quotient $M/(u - \lambda_i)M$ the map $x \mapsto f(\lambda_i)x$.

There is a standard way of reducing to this case, as follows (see also [EL1]). We first note that we can restrict to open affine subschemes of $\mathrm{Spec}(A)$. Therefore we can assume that M is free and we choose a base. Then we represent u by an $n \times n$-matrix with coefficients in A. Specializing the generic $n \times n$-matrix $X = (X_{ij})$ with entries X_{ij} that are algebraically independent over $\mathbf{Z}$, to the matrix representation of u, and splitting $p_X(T)$ in the splitting algebra of $p_X(T)$ over the $\mathbf{Z}$-algebra $\mathbf{Z}[X]$ generated by the entries of X, we see that it suffices to prove the theorem for the generic matrix X. The discriminant d_X of $p_X(T)$ is regular, that is non zero in the domain $\mathbf{Z}[X]$, as can easily be seen, for example by specializing all the non-diagonal entries of X to zero: the discriminant $\prod_{i\neq j}(X_{ii} - X_{jj})$ of the resulting diagonal matrix is regular in $\mathbf{Z}[X_{11}, \ldots, X_{nn}]$. Since d_X specializes to this discriminant, it is non zero and hence regular in $\mathbf{Z}[X]$. It follows that the spectral mapping theorem holds for X over the algebra $\mathbf{Z}[X][1/d_X]$, and thus over its subalgebra $\mathbf{Z}[X]$. □

4. MINIMAL POLYNOMIALS

Let M be a projective A-module of rank n, and let $u\colon M \to M$ be an A-linear map. Denote by

$$\theta_0\colon A[T] \longrightarrow \mathrm{End}_A(M)$$

the morphism defined by $\theta_0(T) = u$. Let t be the class of T in $B = A[T]/(p_u)$. It follows from the Cayley-Hamilton theorem that θ_0 factors through the A-algebra homomorphism

$$\theta\colon B \to \mathrm{End}_A(M)$$

given by $\theta(t) = u$. The image of θ is the A-algebra $A[u]$ in $\mathrm{End}_A(M)$ generated by u.

4.1. LEMMA. *If the ideal* $\mathrm{Ker}(\theta_0)$ *is principal, it can be generated by a monic polynomial, which is then its unique monic generator. Suppose that* A *is a domain with field of fractions* K. *Let* $q \in K[T]$ *be the (monic) minimal polynomial of* $1_K \otimes u$. *Then* $\mathrm{Ker}(\theta_0)$ *is principal if and only if* $q \in A[T]$, *and then* q *is a generator of this ideal.*

When $\mathrm{Ker}(\theta_0)$ is principal its unique monic generator is called the *minimal polynomial* of u. It divides the characteristic polynomial p_u. Note that if $M \neq 0$ the minimal polynomial of the zero endomorphism is equal to T.

Proof of 4.1. A generator q_0 of $\mathrm{Ker}(\theta_0)$ must divide the characteristic polynomial, which is monic. Therefore its leading coefficient, say a, is invertible in A. Then $q = a^{-1}q_0$ is also a generator and it is monic. It is the only one with this property: indeed, let q_1 be another monic generator; the relations $q = q_1 r$ and $q_1 = q r_1$ imply that r and r_1 are monic, and $\deg(r) = \deg(r_1) = 0$; hence $r = r_1 = 1$.

Now suppose that A is a domain with field of fractions K. The isomorphism $K \otimes_A \mathrm{End}_A(M) \to \mathrm{End}_K(K \otimes_A M)$ ([AC], I, 2.10) implies that the map $K \otimes_A A[u] \to K[1_K \otimes u] \subset \mathrm{End}_K(K \otimes_A M)$ is injective; thus the map $K \otimes_A A[u] \to K[1 \otimes u]$ is an isomorphism.

Let $q \in A[T]$ be a monic polynomial such that $q(u) = 0$; and let $f\colon A[T]/(q) \to A[u]$ be the associated morphism. Consider the following commutative square

$$\begin{array}{ccccc} A[T]/(q) & \xrightarrow{f} & A[u] & & \\ \downarrow & & \downarrow & & \\ K[T]/(q) & \xrightarrow[1_K \otimes f]{} & K \otimes_A A[u] & \xrightarrow{\sim} & K[1 \otimes u]\,. \end{array}$$

If q is the minimal polynomial of u, that is if f is an isomorphism, then the same holds for $1 \otimes f$, i.e. q is also the minimal polynomial of $1 \otimes u$. Conversely, if $1 \otimes f$ is an isomorphism, then f is injective (hence bijective) since the vertical map on the left is injective, due to the fact that $A[T]/(q)$ is free over A. □

4.2. PROPOSITION (Existence of the minimal polynomial). *Let, as above,* $u\colon M \to M$ *be an endomorphism of a projective* A*-module of finite type. Assume that* $\mathrm{Spec}(A)$ *is connected. Then:*

i) *The algebra* $A[u]$ *is projective as an* A*-module if and only* u *has a minimal polynomial.*

ii) *If A is an integrally closed domain, then u has a minimal polynomial.*

iii) *Let q be a monic divisor of p_u such that $q(u) = 0$. If the discriminant $d = \mathrm{dis}(q)$ is regular in A, then q is the minimal polynomial of u.*

Proof. The statement i) is given here for the record; a proof has already been given in 1.5 ii).

ii) The morphism $A[T]/(p_u) \longrightarrow A[u]$ is surjective, and the sub-algebra $A[u] \subset \mathrm{End}_A(M)$ is torsion free; thus the conclusion is a particular case of the following variant of a 'Kronecker lemma':

4.3. LEMMA. *Given a monic polynomial $p \in A[T]$, let $f : A[T]/(p) \longrightarrow C$ be a surjective morphism of A-algebras. If A is an integrally closed domain and if C is torsion free then C is a free A-module, of the form $C = A[T]/(q)$ where q is a monic divisor of p.*

A proof is given below.

iii) We have to show that the morphism $A[T]/(q) \to A[u]$ is injective. If the discriminant d is invertible then the module M is projective over $A[T]/(q)$ (by Proposition 2.9), and Lemma 3.3.1 implies that the support of M is the whole spectrum of $A[T]/(q)$; thus, by Proposition 1.3, the minimal polynomial is q. If d is only regular, we again use the commutative square

$$\begin{array}{ccccc} A[T]/(q) & \longrightarrow & A[u] & & \\ \downarrow & & \downarrow & & \\ (A[T]/(q))_d & \longrightarrow & (A[u])_d & \xrightarrow{\sim} & A_d[u]\,, \end{array}$$

whose vertical map on the left is injective, in view of the regularity of d. □

Proof of 4.3. Consider the commutative square associated with the inclusion of A in its field of fractions K:

$$\begin{array}{ccc} A[T]/(p) & \xrightarrow{f} & C \\ \downarrow & & \downarrow \\ K[T]/(p) & \xrightarrow[f_K]{} & K \otimes_A C\,. \end{array}$$

Since K is a field, the ideal $\mathrm{Ker}(f_K)$ is generated by the class of a monic polynomial $q(T)$. It is a divisor of $p(T)$ in $K[T]$, thus $p(T) = q(T)\,r(T)$ with

$r(T)$ in $K[T]$. Since $p(T)$ and $q(T)$ are monic, the polynomial $r(T)$ is also monic. We can then apply the usual Kronecker lemma ([AC], V, 1.3, prop. 11) to deduce that the coefficients of $q(T)$ are integral over A; hence $q(T)$ is in $A[T]$ since A is integrally closed in K. Since C is torsion free, the map $C \to K \otimes_A C$ is injective. Thus the equality $f_K(q) = 0$ implies $f(q) = 0$. From the above square we obtain the diagram

$$\begin{array}{ccc} A[T]/(q) & \longrightarrow & C \\ {\scriptstyle j}\downarrow & & \downarrow \\ K[T]/(q) & \longrightarrow & K \otimes_A C\,. \end{array}$$

The map j is injective since $A[T]/(q)$ is a free A-module, and the lower horizontal map is an isomorphism. Thus the surjective map $A[T]/(q) \to C$ is an isomorphism. □

4.4. EXAMPLES.

4.4.1. Given a monic polynomial $p \in A[T]$, of degree n, we may consider the endomorphism of the free A-module $A[T]/(p)$ defined by the product of the class of T, a.k.a. the "companion matrix". Its minimal polynomial is clearly equal to p, which is also its characteristic polynomial, because both have the same degree n.

4.4.2. An explicit particular case of 4.2 iii): Suppose that M is free and that u is given, over some basis, by a diagonal matrix $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Let $\mu_1, \ldots, \mu_s$ be the distinct elements from the set $\{\lambda_1, \ldots, \lambda_n\}$. Then $\mathrm{Ker}(\theta_0)$ is the set of polynomials $f(T)$ in $A[T]$ such that $f(\mu_i) = 0$ for all i. If the differences $\mu_i - \mu_j$ are regular for $i \neq j$, in particular if A is a domain, then $\mathrm{Ker}(\theta_0)$ is generated by the polynomial $q(T) = \prod_{i=1}^{s}(T - \mu_i)$.

Proof. The description of the ideal $J = \mathrm{Ker}(\theta_0)$ is clear. Now suppose that the differences $\mu_i - \mu_j$ are regular. Let $f(T)$ in $A[T]$ be a polynomial such that $f(\mu_1) = 0$. Then $f(T)$ is obviously a multiple of $T - \mu_1$. Suppose now that a polynomial $f(T)$ in J is proved to be a multiple of $q_i(T) = (T-\mu_1)\cdots(T-\mu_i)$, say $f(T) = q_i(T)\, g(T)$. The relation

$$0 = f(\mu_{i+1}) = (\mu_{i+1} - \mu_1)\cdots(\mu_{i+1} - \mu_i)\, g(\mu_{i+1})\,,$$

together with the hypothesis that the differences $\mu_{i+1} - \mu_j$ are regular, imply that $g(\mu_{i+1}) = 0$, and thus $q_{i+1}(T)$ divides $f(T)$. We conclude, by induction, that $f(T)$ is a multiple of $q_s(T)$.

Achevé de composer le 24 février 2014 à 13 : 48

4.4.3. Consider the endomorphism u of A^2 given by the matrix $\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)$. By Euclidean division, any element in $\mathrm{Ker}(\theta_0)$ is the sum of a multiple of the characteristic polynomial $p_u(T) = (T-a)(T-b)$ and a polynomial of degree ≤ 1, say $\alpha T + \beta$. The condition $\alpha u + \beta = 0$ is equivalent to

$$\alpha \in \mathrm{Ann}_A(a-b) \cap \mathrm{Ann}_A(c) \qquad \text{and} \qquad \beta = -\alpha a = -\alpha b\,.$$

If this endomorphism has a minimal polynomial q then there are two possibilities:

1) $\deg(q) = 1$; since q is monic this is equivalent to saying that $1 \in \mathrm{Ann}_A(a-b) \cap \mathrm{Ann}_A(c)$, that is, equivalent to $a = b$ and $c = 0$, and then $q = T - a$.

2) $\deg(q) = 2$, i.e. $q = p_u$; since the relation $\alpha u + \beta = 0$ implies $\alpha = 0$, we then have $\mathrm{Ann}_A(a-b) \cap \mathrm{Ann}_A(c) = 0$.

In all other cases, that is if

$$0 \neq \mathrm{Ann}_A(a-b) \cap \mathrm{Ann}_A(c) \neq A\,,$$

the endomorphism $\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)$ does *not* have a minimal polynomial.

In particular, let $A = k[X]$ be the polynomial ring over a field. The endomorphism given by $u = \left(\begin{smallmatrix} 1 & X \\ 0 & 1 \end{smallmatrix}\right)$ has $(T-1)^2$ as minimal polynomial. Its image modulo X^n has a minimal polynomial if and only if $n = 1$.

4.4.4. The following easy remark from commutative algebra leads us to construct endomorphisms over a *domain* which don't possess a minimal polynomial. We have learned this method from the paper [Fr].

Two monic polynomials $p_1, p_2 \in A[T]$ give rise to an *injective* morphism of A-algebras

$$A[T]/(p_1) \cap (p_2) \longrightarrow A[T]/(p_1) \times A[T]/(p_2)\,.$$

In general, the ideal $(p_1) \cap (p_2)$ is not principal; but it *is* principal if A is an integrally closed domain, as can be shown by applying Lemma 4.3 to the morphism $A[T]/(p_1 p_2) \longrightarrow A[T]/(p_1) \cap (p_2)$.

In general, the A-algebra $M = A[T]/(p_1) \times A[T]/(p_2)$ is a free A-module, and the product in M defines an injective morphism of A-algebras $M \longrightarrow \mathrm{End}_A(M)$. Thus, for $t \in M$, the sub-algebra $A[t] \subset M$ is isomorphic to $A[u] \subset \mathrm{End}_A(M)$, where u is the endomorphism $x \mapsto tx$. Let us consider the element $t = (t_1, t_2) \in M$, where t_i is the class of T modulo p_i. The algebra $A[u]$ generated by $x \mapsto tx$ is here isomorphic to $A[T]/(p_1) \cap (p_2)$.

To construct examples where a minimal polynomial does not exist, it is thus enough to find two monic polynomials p_1 and p_2 such that the ideal $(p_1) \cap (p_2)$ of $A[T]$ is not principal. If we restrict to a domain A with field of fractions K, it is enough, according to Lemma 4.1, to produce two monic polynomials in $A[T]$ whose least common multiple in $K[T]$ is not in $A[T]$.

For a simple explicit example consider a domain A whose field of fractions K contains an element x, not in A, such that $x^2 \in A$ and $x^3 \in A$. Let

$$p_1 = T^2 - x^2 \quad \text{and} \quad p_2 = T^2 - x^2T - x^2 + x^3 = (T - x)(T + x - x^2).$$

Then in $K[T]$, one has $\operatorname{lcm}(p_1, p_2) = (T^2 - x^2)(T + x - x^2)$; but the coefficient of T^2 in this polynomial is $x - x^2$, which is not in A.

To be more concrete, we write the matrix coming out of this construction, which therefore does not have a minimal polynomial:

$$\begin{pmatrix} 0 & x^2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x^2 - x^3 \\ 0 & 0 & 1 & x^2 \end{pmatrix}$$

In her paper [Fr], Sophie Frisch gives a characterization of normality along these lines.

Finally, we indicate a special situation where the minimal polynomial exists.

4.4.5. PROPOSITION. *Let A be a domain containing $\mathbf{Q}$. Let u be an endomorphism such that $\operatorname{Spec}(A[T]/(p_u))$ is irreducible. Then the minimal polynomial of u exists, in $A[T]$.*

Let K be the field of fractions of A, and let $q \in K[T]$ be the minimal polynomial of u. It is a classical fact over a field (and it is proved in general in Corollary 5.6) that there exists an integer r for which the following divisibility relations hold in $K[T]$:

$$q \mid p_u \mid q^r.$$

Since the morphism $A[T]/(p_u) \longrightarrow K[T]/(p_u)$ is injective and flat, it induces a bijection between the sets of minimal primes in both rings. Hence the hypothesis implies that $\operatorname{Spec}(K[T]/(p_u)) = \operatorname{Spec}(K[T]/(q))$ is irreducible. Thus the polynomial q is a power $q = q_0^s$ of an irreducible polynomial $q_0 \in K[T]$; and the relation $p_u \mid q_0^{rs}$ implies that p_u is a power of q_0. The following lemma then implies that q_0 is in $A[T]$.

4.4.6. LEMMA. *Let B be a ring, and let $A \subset B$ be a subring containing $\mathbf{Q}$. Let $f \in B[T]$ be a* monic *polynomial of which some power f^m is in $A[T]$, with $m \geq 1$. Then $f \in A[T]$.*

Instead of monic polynomials, it is equivalent to consider polynomials whose constant term is 1, since the transformation

$$f(T) \longmapsto T^{\deg(f)} f(1/T)$$

is multiplicative, as are the hypothesis and the conclusion. Moreover, we will use power series, and so we consider the inclusion $A[[T]] \subset B[[T]]$. Since $\mathbf{Q} \subset A$ one can define exponential and logarithm in $A[[U]]$ (see, for example, [A], IV, 4 and also exercise 8 of §4). More precisely, one has

$$\log(1+U) = \sum_{j \geq 1} (-1)^{j-1} \frac{U^j}{j}, \quad \exp(U) = \sum_{j \geq 0} \frac{U^j}{j!}$$

For a positive rational number $a \in \mathbf{Q}$, let

$$(1+U)^a := \exp(a \log(1+U)) = \sum_{j \geq 0} \binom{a}{j} U^j$$

where $\binom{a}{j}$ is the binomial polynomial $\frac{a(a-1)\cdots(a-j+1)}{j!}$. For a positive integer m, it is easy to check that

$$((1+U)^m)^{\frac{1}{m}} = 1 + U\,.$$

Going back to $A[[T]]$, write the hypothesis $f^m \in A[T]$ as

$$f^m \;=\; 1 + a_1 T + \cdots + a_n T^n \;=\; 1 + g(T)\,,$$

with $g(T) \in TA[T]$. Then, from *loc. cit.* end of §4, we can substitute $g(T)$ for T in $(1+T)^{\frac{1}{m}}$, in the ring $A[[T]]$, and we get

$$f = (f^m)^{\frac{1}{m}} = (1 + g(T))^{\frac{1}{m}} \in A[[T]]\,. \qquad \square$$

5. CYCLIC MODULES

A finite-dimensional vector space V over a field K, equipped with an endomorphism $u\colon V \longrightarrow V$, is said to be *cyclic* (with respect to u) if there exists $x \in V$ such that V is generated by the elements $u^i(x)$. In other words, V is then a monogenous $K[u]$-module, and thus it is isomorphic to $K[T]/(q)$, where $q(T)$ is a monic polynomial. This implies that $\deg(q) = \dim_K V$, whence q is the characteristic polynomial of u. This justifies the following definition.

5.1. DEFINITION. Let $u\colon M \to M$ be an endomorphism of a projective A-module of finite type. We say that M is *cyclic* (with respect to u) if M is an invertible module over $A[T]/(p_u)$.

This property is weaker than the characteristic polynomial p_u being separable, as is shown by Proposition 5.3 below. It may be characterized as follows.

5.2. PROPOSITION. *Under the general hypotheses of* 5.1, *let us write* $B = A[T]/(p_u)$. *Then the following properties are equivalent:*

i) *The* B*-module* M *is invertible, i.e.* M *is cyclic.*

i′) *The* $A[u]$*-module* M *is invertible.*

ii) *The morphism of* A*-algebras* $\theta\colon B \longrightarrow \mathrm{End}_A(M)$ *is universally injective, that is, for any* A*-algebra* $A \to A'$ *the map* $1\otimes\theta\colon A'\otimes_A B \longrightarrow A'\otimes_A \mathrm{End}_A(M) = \mathrm{End}_{A'}(A'\otimes_A M)$ *is injective.*

iii) *After any base change the characteristic polynomial of* u *is also its minimal polynomial.*

Note that, since M is projective of finite type, the canonical map

$$A' \otimes_A \mathrm{End}_A(M) \to \mathrm{End}_{A'}(A' \otimes_A M)$$

is bijective for any algebra A' ([A], II, 5.3). However, in general the map $A' \otimes_A A[u] \longrightarrow A' \otimes_A \mathrm{End}_A(M)$ is not injective, nor is the map $A' \otimes_A A[u] \longrightarrow A'[1 \otimes u]$: the formation of $A[u]$ does not commute with (non-flat) base change.

Proof. i) $\Rightarrow$ ii) The property of M being invertible over B is preserved under any base change $A \to A'$; moreover, it implies the injection $B \xrightarrow{\sim} \mathrm{End}_B(M) \subset \mathrm{End}_A(M)$.

Assertion iii) is a reformulation of ii).

i) $\Leftrightarrow$ i′) We have just seen that i) implies that the morphism $\rho\colon B \longrightarrow A[u]$ is an isomorphism; hence it implies that M is invertible over $A[u]$. Conversely, this condition implies that $A[u]$ is projective over A, with the same rank as M, which is also the rank of B; since ρ is surjective, it is in fact an isomorphism.

iii) $\Rightarrow$ i) If A is a field, the first step of the theory of similarity invariants shows the existence of an $x \in M$ whose annihilator in $A[T]$ is generated by the minimal polynomial of u. By assumption, the latter is also the characteristic polynomial. Therefore the map $B \longrightarrow M$ given by $b \mapsto bx$ is injective, and

hence it is bijective since the vector spaces B and M have the same dimension. The conclusion now follows from the

5.3. PROPOSITION. *Let $u\colon M \to M$ be an endomorphism of a projective A-module of finite type. Let us write $B = A[T]/(p_u)$. Then M is cyclic with respect to u if and only if, for every maximal ideal $\mathfrak{m}$ of A, the vector space $M/\mathfrak{m}M$ is cyclic relative to $\bar{u}\colon M/\mathfrak{m}M \to M/\mathfrak{m}M$. Due to Theorem 3.3, it is even enough that this condition be satisfied for those maximal ideals which contain the discriminant of p_u.*

Proof. We have to prove that for any maximal ideal $\mathfrak{m}$ of A one can find an element $s \notin \mathfrak{m}$ and an isomorphism of B_s-modules $B_s \to M_s$. The above argument shows that $M/\mathfrak{m}M$ is free of rank 1 over $B/\mathfrak{m}B$. By lifting to M a generator of $M/\mathfrak{m}M$, we define an $x \in M$, and thus a B-linear map $\varphi\colon B \longrightarrow M$. From the Nakayama lemma we deduce the surjectivity of the map $\varphi_{\mathfrak{m}}\colon B_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}}$. The A-module $\mathrm{Coker}(\varphi)$ is of finite type and $\mathrm{Coker}(\varphi)_{\mathfrak{m}}$ is zero; therefore there exists $s \in A$, $s \notin \mathfrak{m}$ such that $\mathrm{Coker}(\varphi)_s = 0$, i.e. φ_s is surjective. But B_s and M_s are projective A_s-modules of the same rank; thus φ_s is an isomorphism, which shows that M is locally free of rank 1 over B. □

The following example illustrates a particular case of the hypotheses of Proposition 5.3. For more, related, examples see [F2].

5.4. EXAMPLE. Let $A = \mathbf{R}[X]$ be the polynomial ring over the real numbers, set $M = A^2$, and let u be the endomorphism defined by the matrix

$$\begin{pmatrix} 1 & X \\ -X & -1 \end{pmatrix}$$

The characteristic polynomial is $p_u(T) = T^2 + X^2 - 1$. Let us write $B = \mathbf{R}[X,T]/(T^2 + X^2 - 1)$. Then

- *the module M is invertible over B, although B is not étale over A;*
- *the B-module M is not free.*

The $\mathbf{R}[X]$-algebra B is clearly ramified when $X^2 = 1$, and the discriminant of $p_u(T)$ is here $d = 4(1 - X^2)$.

In order to apply the above result we consider the quotients $\mathbf{R}[X]/(X-1)$ and $\mathbf{R}[X]/(X+1)$, and we need to check that the $\mathbf{R}$-vector space $\mathbf{R}^2$ is cyclic

for the matrices $\left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & -1 \\ 1 & -1 \end{smallmatrix}\right)$. But, for both these matrices, the vector $\binom{1}{0}$ and its image are independent.

Here is a direct proof which does not use Proposition 5.3. The condition for the B-module M to be free is the existence of $\xi \in M$ such that $(\xi, u(\xi))$ is a basis over A. Consider the base change $\mathbf{R} \to \mathbf{C}$. The module $\mathbf{C} \otimes_{\mathbf{R}} M$ is free over $\mathbf{C} \otimes_{\mathbf{R}} B$: in fact, let $\xi = \binom{i}{1} \in \mathbf{C} \otimes_{\mathbf{R}} M$; then we have $u(\xi) = \binom{i+X}{-iX-1}$. Since

$$\det \begin{pmatrix} i & i+X \\ 1 & -iX-1 \end{pmatrix} = -2i$$

is invertible in $\mathbf{C} \otimes_{\mathbf{R}} A$, the elements $\xi, u(\xi)$ yield a basis over $\mathbf{C} \otimes_{\mathbf{R}} A$, and thus ξ is a basis over $\mathbf{C} \otimes_{\mathbf{R}} B$. By descent from $\mathbf{C}$ to $\mathbf{R}$ we see that M is invertible over B.

Let us check that M is not free over B. Consider a non-zero element $\xi = \binom{a}{b} \in M$, where a and b are real polynomials in X. The determinant of $(\xi, u(\xi))$, over the canonical basis of M, is easily seen to be the polynomial

$$q(X) = -((a^2 + b^2)X + 2ab).$$

Since $\deg(a^2 + b^2) = 2\max(\deg a, \deg b) \geq \deg(ab)$, the degree of $q(X)$ is odd. Since a real polynomial of odd degree has a real root, $q(T)$ cannot be invertible in $A = \mathbf{R}[X]$, and M is not a free B-module. □

The following result is a partial generalization of both the spectral mapping theorem of [LTS] and of 3.6.

5.5. THE SPECTRAL MAPPING THEOREM. *Let M be a projective A-module of rank n, and let $u\colon M \to M$ be an A-linear map. For b in $B = A[T]/(p_u)$ we denote by $p_{b,B}(X)$ the characteristic polynomial of multiplication by b on B, and by $p_{\theta(b),M}(X)$ the characteristic polynomial of the endomorphism $\theta(b)$ of M. Then, in $A[X]$, we have*

$$p_{b,B}(X) = p_{\theta(b),M}(X).$$

In particular, if we assume that p_u splits as $p_u(T) = \prod_{i=1}^{n}(T - \lambda_i)$, then, for all polynomials $f(T)$ in $A[T]$, we have in $A[X]$

$$p_{f(u),M}(X) = \prod_{i=1}^{n}(X - f(\lambda_i)).$$

Proof. First, let us check the equality of the constant terms of the given polynomials, namely

$$\det_B(b) = \det_M(\theta(b)) .$$

The element b can be written as $b = f(t)$, where $f(T)$ is a polynomial in $A[T]$ of degree strictly less than $n = \deg(p_u)$, and we have to prove that $\det_B(f(t)) = \det_M(\theta(f(t))) = \det_M(f(u))$. Since we also have $b = f(t) + p_u(t)$, we can assume that $f(T)$ is monic of degree n. Let $A \to A'$ be a base extension such that A' is free as an A-module, and such that $f(T)$ splits into a product of linear factors $T - \alpha$ over A'. Since $A \to A'$ is injective it is enough to check this equality in A'. As the determinant is multiplicative it suffices to prove that

$$\det_B(t - \alpha) = \det_M(u - \alpha)$$

for all roots α of $f(T)$ in A'. However, by Proposition 1.5 i), the left hand side is equal to $(-1)^n p_u(\alpha)$, and so is the right hand side, by definition.

The expected equality between polynomials in X can be written as

$$\det_{B[X]}(X - b) = \det_{A[X]\otimes M}(X \otimes 1 - 1 \otimes \theta(b)) ,$$

which, one sees, is a particular case of the one above.

The second part of the theorem follows from the first, together with the second part of Proposition 1.5 i). □

5.6. COROLLARY. *The kernel of the homomorphism* $\theta\colon B = A[T]/(p_u) \to \mathrm{End}_A(M)$ *is a nilideal, that is, the support of* M *as a* B*-module is equal to* $\mathrm{Spec}(B)$.

In particular, $p'_u(t)$ *is invertible in* B *if and only if* $p'_u(u)$ *is invertible in* $A[u]$, *and then* θ *is injective.*

If the minimal polynomial $q(T)$ *exists, then we have, in* $A[T]$, *the usual divisibility properties*

$$q(T) \mid p_u(T) \mid q(T)^n .$$

Proof. If $\theta(b) = 0$ we obtain from the theorem above that $p_{b,B}(T) = T^n$. We then deduce from the Cayley-Hamilton theorem that $b^n = p_{b,B}(b) = 0$, which proves the first part of the corollary. Since the support of M is the set of prime ideals of B containing $\mathrm{Ann}_B(M)$, it is equal to $\mathrm{Spec}(B)$.

When the minimal polynomial $q(T)$ exists, we take b to be the class of $q(T)$, to obtain the last assertion of the corollary. □

This proof of the equality $\mathrm{Supp}_B(M) = \mathrm{Spec}(B)$ can be used to shorten the proof of 3.3.1.

6. DIAGONALIZABLE ENDOMORPHISMS

In this section we generalize the diagonalization of endomorphisms of vector spaces to endomorphisms of projective modules over arbitrary commutative rings.

6.1. We first recall the diagonalization property for an endomorphism $u\colon V \to V$ of vector spaces of finite dimension over a field K. The K-algebra $K[u]$ in $\mathrm{End}_K(V)$ generated by u is isomorphic to $K[T]/(q)$, where $q(T)$ is the *minimal* polynomial of u.

The following properties are known to be equivalent (see, for example, [A], VII, 5.8, and [A], V, 7):

(6.1.1) The roots of q, in an extension of K, are distinct.

(6.1.2) The algebra $K[u]$ is étale over K.

(6.1.3) There exists an extension L of K such that the endomorphism $1 \otimes u\colon L \otimes_K V \longrightarrow L \otimes_K V$ is diagonalizable, in the usual sense.

Note that the proper extension to a ring A of the notion of *distinct* elements is *elements with distinct images in each residue field* $\kappa(\mathfrak{p})$ of A, and then they may be called *everywhere distinct*. Let λ and μ be elements in A with distinct images in each $\kappa(\mathfrak{p})$. The factorization

$$A \longrightarrow A/\mathfrak{p} \hookrightarrow \kappa(\mathfrak{p})$$

shows that the condition "everywhere distinct" is equivalent to: "for all prime ideals $\mathfrak{p}$, $\lambda - \mu \notin \mathfrak{p}$". Ultimately, this condition is equivalent to: "$\lambda - \mu$ is invertible in A". Hence, over a ring A, the condition (6.1.1) must be translated as follows: if $(\mu_1, \ldots, \mu_n)$ denote the roots of q in some extension A' of A, then $\mu_i - \mu_j \in A'^{\times}$, for $i \neq j$, a condition equivalent to q being *separable*.

When the above three properties are satisfied, Bourbaki writes that u is *absolutely*[2]) *semi-simple*.

[2]) The translator of Bourbaki into English has forgotten this crucial adjective in the definition of Jordan decomposition [A], VII, 5.9.

6.2. THEOREM. *Let M be a projective module of rank n over a connected ring A. Let $u\colon M \longrightarrow M$ be an endomorphism and let $A[u]$ in $\mathrm{End}_A(M)$ be the algebra generated by u. The following three properties are equivalent:*

i) *The A-algebra $A[u]$ is projective as an A-module and the roots $\mu_1, \dots, \mu_s$ of the minimal polynomial $q(T)$ of u in any faithfully flat extension $A \to A'$ of A are everywhere distinct, that is, $\mu_i - \mu_j$ is invertible in A' when $i \neq j$; in other words, q is separable.*

ii) *The algebra $A[u]$ is finite étale over A.*

iii) *There exists a faithfully flat morphism $A \longrightarrow A'$ such that $A' \otimes_A M$ is free with a basis on which the matrix U of $1_{A'} \otimes u$ is diagonal with the property that distinct diagonal entries are everywhere distinct, that is, if $U = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$, and if $\lambda_i \neq \lambda_j$ then $\lambda_i - \lambda_j$ is invertible in A'.*

Proof. The equivalence i) $\Leftrightarrow$ ii) is established in 2.8.

ii) $\Rightarrow$ iii) According to 2.4, there exist a finite étale morphism $A \longrightarrow A'$, with A' connected, and an isomorphism of A'-algebras $A' \otimes_A A[u] \simeq A'^s$. The image of $1 \otimes u$ may be written as $(\mu_1, \dots, \mu_s)$ with $\mu_i \in A'$, and it follows from 2.8 that $\mu_i - \mu_j$ is invertible in A' if $i \neq j$.

Now, the A'-module $A' \otimes_A M$ decomposes as a product of projective A'-modules $M_1 \times M_2 \times \cdots \times M_s$. Since A' is connected, each module M_i has constant rank. By covering $\mathrm{Spec}(A')$ with a finite number of open sets over which the M_i are free, and by taking the disjoint union of these sets, we can find a faithfully flat map $A' \longrightarrow A''$ such that each $A'' \otimes_{A'} M_i$ is a *free* A''-module, of rank, say, $n(i)$. On $A'' \otimes_{A'} M_i$ the endomorphism $1 \otimes u$ is simply the map $x \mapsto \mu_i x$. Finally, if we choose any basis in each factor, the matrix of $1 \otimes u$ may be written as

$$\mathrm{diag}(\underbrace{\mu_1, \dots, \mu_1}_{n(1)}, \underbrace{\mu_2, \dots, \mu_2}_{n(2)}, \dots, \underbrace{\mu_s, \dots, \mu_s}_{n(s)}).$$

iii) $\Rightarrow$ ii) Let $\mu_1, \dots, \mu_s$ be the distinct elements from the set $\{\lambda_1, \dots, \lambda_n\}$. The free A'-module $A' \otimes_A M$ splits into a direct sum of free A'-modules $A' \otimes_A M = M_1 \oplus \cdots \oplus M_s$ such that $1 \otimes u$ acts as $x \mapsto \mu_i x$ on M_i. Since the differences $\mu_i - \mu_j$ are invertible in A', we deduce from 4.4.2 that $1 \otimes u$ has a minimal polynomial, namely the separable polynomial $q(T) = \prod(T - \mu_i)$. Hence the A'-algebra $A'[1 \otimes u] \simeq A'[T]/(q)$ is finite étale. Since A' is flat over A, the morphism $A' \otimes_A A[u] \to A'[1 \otimes u]$ is injective, hence it is an isomorphism. It follows from Proposition 2.4 that $A[u]$ is finite étale over A. □

6.3. REMARK. We shall not introduce a specific adjective to qualify these morphisms; the choice of Bourbaki ('absolutely semi-simple') is a little cumbersome; we prefer to say: $A[u]$ is étale.

However, the semi-simplicity property itself deserves to be pointed out: *if $A[u]$ is étale then each u-stable submodule N of M such that M/N is projective over A has a u-stable complement*. Indeed, M/N is then projective over $A[u]$, by Proposition 2.9.

Note that the projectiveness (over A) of M/N is necessary. For example, if $A = k[X]$ then the endomorphism $u = \left(\begin{smallmatrix} X & 0 \\ 0 & 1+X \end{smallmatrix}\right)$ of $M = A^2$ is injective, not surjective, and its characteristic polynomial is separable; but the strict sub-module $u(M) \subset M$ is not a direct summand of M, since the quotient $M/u(M)$ is isomorphic to k^2.

A classical result on endomorphisms of vector spaces says that two commuting endomorphisms which are both diagonalizable are simultaneously diagonalizable, that is, there exists a basis on which they both are given by diagonal matrices. In our context, the result states as follows.

6.4. PROPOSITION. *Let u and v be two commuting endomorphisms of a projective A-module M of finite type. If $A[u]$ and $A[v]$ are étale over A, then the sub-algebra $A[u,v]$ of $\mathrm{End}_A(M)$ they generate is étale.*

If A is connected, there exists a faithfully flat morphism $A \to A'$ such that $A' \otimes_A M$ is a free A'-module with a basis with respect to which the matrices of u and v are both diagonal.

Proof. Since u and v commute, the commutative A-algebra $A[u,v]$ is endowed with a surjective map

$$C = A[u] \otimes_A A[v] \longrightarrow A[u,v]\,.$$

This morphism allows us to define a structure of C-module on M, for which we have an isomorphism

$$C/\operatorname{Ann}_C(M) \simeq A[u,v]\,.$$

We thus have to show that $C/\operatorname{Ann}_C(M)$ is étale over A. Lemma 2.3 implies that C is étale over A, as are $A[u]$ and $A[v]$. Therefore M is a projective C-module, by Proposition 2.9. It then follows from Proposition 1.3 that $C/\operatorname{Ann}_C(M)$ is a projective quotient of C; hence it is étale over A.

Proposition 2.4 ensures the existence of a faithfully flat morphism $A \to A'$, with A' connected, such that the algebra $A' \otimes_A A[u,v]$ is split, say $A' \otimes_A A[u,v] \simeq A'^m$. As in the beginning of the proof of Theorem 6.2, we can assume that in the related decomposition of $A' \otimes_A M$ as $M_1 \times \cdots \times M_d$, each M_i is a free A'-module. Moreover, on each factor, $1 \otimes u$ and $1 \otimes v$ act as multiplication by a constant. □

It is perhaps worth recalling that in general there is no relation between the dimensions of the three algebras $A[u]$, $A[v]$ and $A[u,v]$, even over a field. For example, consider the diagonal endomorphisms of A^3 given by

$$u = \mathrm{diag}(1,1,0)\,, \quad v = \mathrm{diag}(0,1,1)\,.$$

Then $A[u]$ and $A[v]$ are of rank 2, and $A[u,v]$ is of rank 3, with basis $(1,u,v)$, since $u^2 = u$, $v^2 = v$ and $uv = u + v - 1$.

7. The Jordan-Chevalley-Dunford decomposition

If u is an endomorphism of a vector space over a field K, the following result is classical:

The endomorphism u has a Jordan decomposition $u = u_s + u_n$, where u_s is absolutely semi-simple and u_n is nilpotent, if and only if the eigenvalues of u are separable over K.

See, for example, [A], VII, 5.8 and 5.9.

Over a ring A, the condition "*u_s is absolutely semi-simple*" has to be replaced by: *the algebra $A[u_s]$ is étale over A*. See §6.

We must find a substitute for the condition "*the eigenvalues of u are separable*" which remains meaningful over rings. For a monic polynomial $p(T)$, the condition that its roots should be separable has to be replaced by:

(1) *There exist a monic separable divisor q of p and an integer s such that p divides q^s.*

Equivalently, if A is connected,

(2) *The A-algebra $B = A[T]/(p)$ has a quotient B/J which is finite étale over A, with J a nilpotent ideal in B.*

In fact, (1) implies (2) with J the ideal generated by $q(T)$ in B. The opposite implication follows from Proposition 1.5 ii), which provides a monic polynomial $q(T)$ in $A[T]$ such that $B/J = A[T]/(q)$; and Proposition 2.8 implies that $q(T)$ is separable.

Actually, the generalization of Jordan decomposition is a special case of the following fundamental result of Grothendieck:

7.1. THEOREM (Lifting property for étale algebras). *Let $A \to B$ be an A-algebra, let J be a nilpotent ideal in B, and let $\pi\colon B \to B/J$ denote the canonical projection. If B/J is finite étale over A, then there exists a unique morphism of A-algebras $\sigma\colon B/J \longrightarrow B$ such that $\pi\sigma = \mathrm{Id}_{B/J}$.*

Two direct proofs are given below. This result can also be found in the EGA as follows: in [EGA], IV, 18.3.1, the definition given in 2.1 is shown to imply "formal étaleness" as defined in [EGA], IV, 17.1. To deduce the statement of Theorem 7.1 from this proposition, take $Y'_0 = X = \mathrm{Spec}(B/J)$, $Y = \mathrm{Spec}(A)$, and $Y' = \mathrm{Spec}(B)$.

Before giving proofs of this theorem we translate it into the "Jordan decomposition" we have in mind.

7.2. THEOREM (Jordan decomposition). *Let u be an endomorphism of a finitely generated projective A-module M. We assume that A is connected.*

i) *If $A[u]$ has an étale quotient defined by a nilpotent ideal I, then there exists a couple of endomorphisms u_s and u_n in $A[u]$ such that*

$$u = u_s + u_n\,,$$

where $A[u_s]$ is étale over A and where u_n is nilpotent. This decomposition is unique if u_n is specified to be in I.

ii) *Suppose that the ring $B = A[T]/(p_u)$ has an étale quotient B/J defined by a nilpotent ideal J. Then, as in* i), *there exists a couple of endomorphisms u_s and u_n in $A[u]$ such that*

$$u = u_s + u_n\,,$$

where $A[u_s]$ is étale over A and where u_n is nilpotent, but in general without the uniqueness assertion.

iii) *If A is reduced, the hypotheses in* i) *and in* ii) *are equivalent.*

The hypothesis in ii) is the direct translation of the classical one; it is weaker than the hypothesis in i).

If A is not reduced, uniqueness is lacking without some additional assumption; if fact, for a nilpotent element $a \in A$, $1+a$ is invertible and we get another decomposition

$$u = u_s + u_n = (1+a)u_s + (u_n - au_s)\,.$$

Proof. i) Let $\pi\colon A[u] \to A[u]/I$ be the projection onto the étale quotient. Since I is nilpotent, from the lifting property 7.1 one has a unique morphism of A-algebras $\sigma\colon A[u]/I \to A[u]$ such that $\pi\sigma = \mathrm{Id}_{A[u]/I}$. Let $u_s = \sigma(\pi(u))$. This morphism σ induces an isomorphism onto its image $A[u]/I \simeq A[u_s]$, which shows that $A[u_s]$ is étale over A. Finally, $u_n = u - u_s$ is nilpotent since it is in I.

Now we prove that the obtained decomposition is unique. Let $u = s + n$ be a decomposition where $A[s]$ is étale, and $n \in I$. The composite morphism

$$f\colon A[s] \longrightarrow A[u] \longrightarrow A[u]/I$$

is then surjective, with a nilpotent kernel. It is in fact an isomorphism. To see this, it is enough to show that f is faithfully flat, and hence injective, as follows from Lemma 2.3 ii). It is flat by Proposition 2.9 because $A[s]$ is étale over A, and $A[u]/I$ is projective over A by assumption. Finally $\mathrm{Spec}(f)$ is surjective since the kernel of f is nilpotent.

The inverse isomorphism f^{-1} composed with the inclusion $A[s] \subseteq A[u]$ gives a section of π, which coincides with σ in view of the uniqueness assertion in 7.1.

ii) Let t denote the class of T in $B = A[T]/(p_u)$. Applying 7.1 to the quotient $B \to B/J$, we get, in B, a decomposition

$$t = s + n$$

where $A[s]$ is an étale sub-algebra of B, and where n is nilpotent. From 2.9 we derive that M is projective over $A[s]$. Since the kernel of $A[s] \subset B \longrightarrow A[u]$ is a nilideal, the support of M as a module over $A[s]$ is the whole spectrum of that ring. Hence $\mathrm{Ann}_{A[s]}(M) = 0$ and the morphism $A[s] \subset B \longrightarrow A[u]$ is injective. Therefore, taking the images u_s of s, and u_n of n, in $A[u]$, we get the expected decomposition in $A[u]$.

iii) Since the kernel of the morphism $B \longrightarrow A[u]$ is nilpotent, the hypothesis in i) implies the hypothesis in ii).

Conversely, let J be a nilpotent ideal in B; denote by I its image in $A[u]$; we have the following commutative square of surjective morphisms

$$\begin{array}{ccc} B & \longrightarrow & A[u] \\ \downarrow & & \downarrow \\ B/J & \xrightarrow[f]{} & A[u]/I\,. \end{array}$$

Suppose that A is reduced and that B/J is étale over A. Then B/J is reduced: this is trivial if B/J is split as a product A^m, and the general case comes from 2.4. But the kernel of f is nilpotent; thus f is injective, i.e. it is an isomorphism. We conclude that $A[u]/I$ is étale over A, as B/J is. □

Proof of 7.1. a) We first prove uniqueness. Let $C = B/J$. Given two A-algebras sections of π, say $\sigma, \tau\colon C \longrightarrow B$, we introduce the morphism of A-algebras $\omega\colon C \otimes_A C \longrightarrow B$ defined by $\omega(x \otimes y) = \sigma(x)\tau(y)$. We have $\omega(x \otimes 1) = \sigma(x)$, and $\omega(1 \otimes x) = \tau(x)$. Thus, to prove uniqueness we have to check that $\omega(x \otimes 1 - 1 \otimes x) = 0$, that is $\omega(I) = 0$, where I denotes the kernel of the morphism $\mu\colon C \otimes_A C \longrightarrow C$. Since

$$\pi\sigma = \pi\tau = \mathrm{Id}_C$$

the following triangle is commutative:

$$\begin{array}{ccc} C \otimes_A C & \xrightarrow{\omega} & B \\ & {\scriptstyle\mu}\searrow \quad \swarrow{\scriptstyle\pi} & \\ & C & \end{array}$$

The kernel I' of ω is contained in I, and a power I^m of I is contained in I' since the kernel of π is nilpotent. Since C is étale over A, the ideal I is generated by an idempotent e. We thus have $e = e^m \in I'$, which shows that $I = I'$. In particular $\omega(I) = 0$, as we wished to prove.

b) We now prove the existence of σ under the additional assumption that the A-algebra B is monogenous: $B = A[t]$. (This is enough for the applications in 7.2.)

We can assume that A is connected. By induction on the least integer m such that $J^m = 0$, we can assume that $J^2 = 0$. Since B/J is a projective A-module, it follows from Proposition 1.5 ii) that there exist a monic polynomial $q(T) \in A[T]$ and an isomorphism $A[T]/(q) \simeq B/J$ which sends T to the image $\bar{t}$ of t in B/J. The expected section σ is determined

by the image $\sigma(\bar{t})$, which has to be a root b in B of the minimal polynomial $q(T)$ of $\bar{t}$. We try $b = t + x$ with $x \in J$. Since $x^2 = 0$, we have

$$q(t+x) = q(t) + x\,q'(t)\,.$$

By Proposition 2.8 the image of $q'(t)$ in $B/J = A[T]/(q)$ is invertible since $A[T]/(q)$ is étale. As $J^2 = 0$, the element $q'(t)$ is invertible in B as well. Moreover, by definition of $q(T)$, the image of $q(t)$ in B/J is zero, so $q(t)$ is in J. Finally, if we let $x = -q(t)\,q'(t)^{-1}$, we have $q(t+x) = 0$.

This proof is very close to the Newton approximation procedure; it is due to Chevalley ([C], I, 8, thm 7), and it can be made effective.

c) We now explain another particular case which shows clearly what is going on. Suppose that the étale algebra B/J is split as a product of copies of A, say $B/J = A^s$. Since J is nilpotent, the map $\mathrm{Spec}(B/J) \longrightarrow \mathrm{Spec}(B)$ is a homeomorphism. Thus $\mathrm{Spec}(B)$ is the disjoint union of s open and closed sets, each of them being homeomorphic to $\mathrm{Spec}(A)$. From Lemma 1.1 we deduce a factorization $B = B_1 \times \cdots \times B_s$ and s surjective morphisms of A-algebras $B_i \to A$ inducing the bijections $\mathrm{Spec}(A) \to \mathrm{Spec}(B_i)$. Then the product of the s canonical inclusions $A \subseteq B_i$ gives the section $\sigma\colon A^s \longrightarrow B = \prod B_i$ we were looking for.

REMARK. Instead of the topological argument used in the above proof and of Lemma 1.1, we could as well use the lifting to B of the idempotents associated with the decomposition of B/J. This is due to the following result:

7.3. LEMMA. *Let a be an element in a ring R such that $a - a^2$ is nilpotent. Then there is an idempotent $b \in R$ such that $b - a \in (a - a^2)R$.*

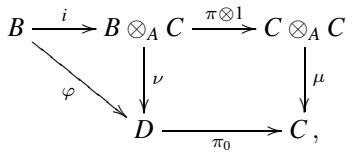
For a proof, see for example, [A], VIII, 9.4.

d) Second proof of the existence: Let $C = B/J$. Consider the composite morphism

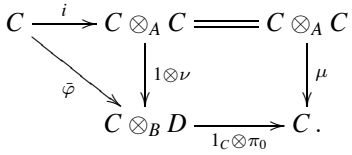
$$B \xrightarrow{\ i\ } B \otimes_A C \xrightarrow{\ \pi\otimes 1\ } C \otimes_A C\,,$$

with $i(b) = b \otimes 1$. Since C is étale over A, the kernel of the multiplication $\mu\colon C \otimes_A C \longrightarrow C$ is generated by an idempotent e. The kernel of $\pi \otimes 1$ is $J \otimes_A C$, a nilpotent ideal. According to the above lemma there exists an idempotent $\varepsilon \in B \otimes_A C$ such that $(\pi \otimes 1)(\varepsilon) = e$. Let $\nu\colon B \otimes_A C \longrightarrow D$ be the morphism to the quotient $D = B \otimes_A C/\varepsilon(B \otimes_A C)$. We get a surjective

homomorphism $\pi_0 \colon D \to C$ with nilpotent kernel making the following diagram commutative:



where $\varphi = \nu i$, and where the square is co-cartesian, i.e. it makes C into a tensor product of the three other rings. The commutativity shows that $\pi_0 \varphi = \pi$. The map i is finite étale by base change from $A \to C$, and ν is a projective quotient by definition, thus ν is an étale morphism, by Lemma 2.3 i). Hence the composite map $\varphi = \nu i$ is finite étale. In fact, it is an isomorphism: by tensoring with C over B, the diagram becomes



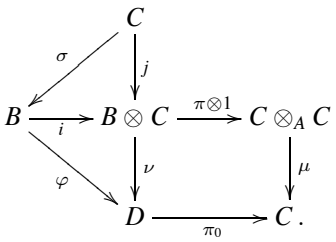
Since the square is cocartesian, the map $1_C \otimes \pi_0$ is an isomorphism; finally we get that $\bar{\varphi} \colon C = B/J \longrightarrow D/JD = C \otimes_B D$ is an isomorphism.

As the ideal J is nilpotent, we first deduce from this that φ is surjective. We also deduce that the map $\mathrm{Spec}(D) \longrightarrow \mathrm{Spec}(B)$ is surjective, i.e. that φ is faithfully flat; hence it is also injective. This allows us to conclude that φ is an isomorphism.

We can now define the required section $\sigma \colon C \longrightarrow B$ by the condition

$$\varphi\sigma = \nu j\,,$$

where $j \colon C \longrightarrow B \otimes_A C$ is the canonical injection $j(c) = 1 \otimes c$:



It remains to calculate $\pi\sigma$. We have

$$\pi\sigma = \pi_0\,\varphi\,\sigma = \pi_0\,\nu\,j = \mu\,(\pi \otimes 1)\,j = \mathrm{Id}_C\,. \qquad \square$$

8. EIGENSPACES

We use the words *eigenvalue* and *eigenspace* with their classical meaning: an eigenvalue λ is a root of the characteristic polynomial, and the eigenspace relative to λ is the submodule $\mathrm{Ker}(u-\lambda)$ of M. If the base ring is not a domain, it may happen that $\mathrm{Ker}(u-\lambda)$ is non zero even if λ is not an eigenvalue. For example, if $ab=0$ with a and b non zero in A, the map $x \mapsto ax$ has a non-zero kernel but its determinant a is not equal to zero, that is 0 is not an eigenvalue.

In this section we show that the eigenspace is often definable as an *image*, essentially the image of (a variant of) the *cotranspose* $(u-\lambda)^c$ of $u-\lambda$; see also [L]. Without any additional hypothesis on u, this description as an image is efficient for the *generic* eigenvalue alone, that is for λ equal to the class of T in $B = A[T]/(p_u)$. To obtain this type of description for all the eigenvalues, we must restrict ourselves to particular classes of endomorphisms for example those for which $A[u]$ is étale.

8.1. LEMMA. *Let C be a ring, let L and L' be C-modules, and let $f: L \to L'$ and $f': L' \to L$ be C-linear maps such that*

$$ff' = d_{L'} \quad \text{and} \quad f'f = d_L\,, \tag{8.1.1}$$

where $d_{L'}(x') = dx'$ and $d_L(x) = dx$ for some element $d \in C$. Finally, let $M = \mathrm{Coker}(f)$. We asssume that the maps d_L and $d_{L'}$ are injective. Then

i) *The module M is annihilated by d, and it is thus a C/dC-module.*

ii) *The following sequence is exact, where $\eta: M \to L/dL$ is induced by f',*

$$0 \longrightarrow M \xrightarrow{\eta} L/dL \xrightarrow{\bar{f}} L'/dL' \xrightarrow{\mathrm{can}} M \longrightarrow 0\,.$$

Proof. To prove assertion i) we note that, if $x' \in L'$, then $dx' = f(f'(x)) \in \mathrm{Im} f$, and hence the image of dx' in M is zero.

In order to prove assertion ii), we first check that the sequence

$$L'/dL' \xrightarrow{\overline{f'}} L/dL \xrightarrow{\bar{f}} L'/dL'$$

is exact, that is $\mathrm{Im}(\overline{f'}) = \mathrm{Ker}(\bar{f})$. If $x \in L$ is such that $f(x) \in dL' = f(f'(L'))$ then $x \in f'(L')$ since $d_{L'}$, and thus f, are injective. The same argument, using the injectivity of d_L, shows that the sequence

$$L/dL \xrightarrow{\bar{f}} L'/dL' \xrightarrow{\overline{f'}} L/dL$$

is exact, that is, $\overline{f'}$ induces an isomorphism from $\mathrm{Coker}(\bar{f}) = M$ onto $\mathrm{Im}(\overline{f'}) = \mathrm{Ker}(\bar{f})$. □

8.2. NOTATION. We shall apply the previous lemma in the following situation :

Let M be an A-module with an A-linear map $u\colon M \to M$, and let $p(T)$ be a monic polynomial of degree n such that

$$p(u) = 0\,. \tag{8.2.1}$$

Moreover, let $C = A[T]$ and $L = L' = A[T] \otimes_A M$, let $f = T \otimes 1 - 1 \otimes u$, and let $f' = \partial p(T \otimes 1, 1 \otimes u)$, where ∂p is the polynomial, introduced in 2.5, which is defined in the polynomial ring $A[T, U]$ by

$$(T - U)\,\partial p(T, U) = p(T) - p(U)\,. \tag{8.2.2}$$

For simplicity we often write $T - u$ and $\partial p(T, u)$ instead of $T \otimes 1 - 1 \otimes u$ and $\partial p(T \otimes 1, 1 \otimes u)$.

Due to the hypothesis $p(u) = 0$, the endomorphism $\partial p(T, u)$ of $A[T] \otimes_A M$ satisfies the relation

$$(T - u)\,\partial p(T, u) = \partial p(T, u)(T - u) = p(T)\,.$$

This corresponds to the condition (8.1.1) of the previous lemma, with $f = T - u$, $f' = \partial p(T, u)$ and $d = p(T)$. The equality $\mathrm{Coker}(f) = M$ from the lemma becomes here the well-known exact sequence (see for example [A], III, 8.10)

$$A[T] \otimes_A M \xrightarrow{T \otimes 1 - 1 \otimes u} A[T] \otimes_A M \xrightarrow{\mu} M \longrightarrow 0$$

where $\mu(\sum T^i \otimes x_i) = \sum u^i(x_i)$.

Denote by t the class of T in $B = A[T]/(p)$; the ring B corresponds to the ring C/dC of the lemma. The condition $p(u) = 0$ gives a structure of B-module on M. On $B \otimes_A M = L/dL$, the maps $\overline{f}$ and $\overline{f'}$ becomes, respectively, $t \otimes 1 - 1 \otimes u$ and $\partial p(t, u)$.

8.3. PROPOSITION. *Let M be an A-module with an A-linear map $u\colon M \to M$, and let $p(T)$ be a monic polynomial such that*

$$p(u) = 0\,.$$

Denote by t the class of T in $B = A[T]/(p)$. Then the following sequence is exact

$$0 \longrightarrow B \xrightarrow{\eta} B \otimes_A B \xrightarrow{t \otimes 1 - 1 \otimes t} B \otimes_A B \xrightarrow{\mu} B \longrightarrow 0\,, \tag{8.3.1}$$

where η *is defined as* $\eta(b) = \partial p(t,t)(1 \otimes b)$. *On tensoring this sequence on the right by* M *over* B, *exactness is preserved and we obtain the sequence*

$$0 \longrightarrow M \xrightarrow{\eta_M} B \otimes_A M \xrightarrow{t\otimes 1 - 1\otimes u} B \otimes_A M \xrightarrow{\mu_M} M \longrightarrow 0\,, \tag{8.3.2}$$

where now the first arrow is defined as $\eta_M(x) = \partial p(t,u)(1\otimes x)$. *In other words, the subspace* $\mathrm{Im}(\partial p(t,u))$ *of* $B \otimes_A M$ *is the eigenspace of* $1 \otimes u$ *relative to the eigenvalue* $t \otimes 1$.

Proof. The exactness of these two sequences is merely a translation of Lemma 8.1. □

8.4. REMARKS. 1) The main application of Proposition 8.3 is to the case where M is projective of finite type over A and $p(T)$ is the characteristic polynomial $p_u(T)$. The endomorphism $\partial p_u(T,u)$ is then equal to the *cotranspose* $(T-u)^c$ of $T-u$ (in [A], III, 8.6, the cotranspose of v is denoted by $\tilde{v}$). In fact, we have the two relations

$$(T-u)\circ(T-u)^c = p_u(T) \qquad \text{and} \qquad (T-u)\circ\partial(T,u) = p_u(T)\,,$$

and the endomorphism $(T-u)$ of $A[T]\otimes_A M$ is injective.

2) On $B \otimes_A M$ there are *two* B-module structures, called, for simplicity, the *left* and the *right* structure. It is important to note that the sequence (8.3.2) is exact for both these structures, even though, in general, it is *not* split for the left B-module structure. It is obvious that the sequence

$$B \otimes_A M \xrightarrow{t\otimes 1 - 1\otimes u} B \otimes_A M \xrightarrow{\mu} M \longrightarrow 0$$

is exact as a sequence of $B \otimes_A B$-modules. It remains to check that the map $\eta_M\colon M \longrightarrow B \otimes_A M$ is linear for the left structure. Since $t \in B$ acts on M as $tx = u(x)$, we have to show that $\eta_M(u(x)) = (t\otimes 1)\,\eta_M(x)$. We already know that η_M is linear for the right structure, so we have $\eta_M(u(x)) = (1\otimes u)\eta_M(x)$. Moreover, the definition (8.2.2) gives

$$(t\otimes 1 - 1\otimes u)\partial p(t,u) = p(t)\otimes 1 - 1\otimes p(u) = 0\,.$$

Thus we have $(1\otimes u)\,\partial p(t,u) = (t\otimes 1)\,\partial p(t,u)$.

3) The polynomial $\partial p(T,U)$ can be given an explicit expression in terms of the coefficients of

$$p = T^n + a_{n-1}T^{n-1} + \cdots + a_0\,.$$

In fact, if we write $\partial p(T,U) = \sum_{i=0}^{n-1} T^i\, p_i(U)$, then $p_{n-1} = 1$, and for $j > 0$ we have $p_{j-1}(U) = a_j + U\, p_j(U)$. Denoting by $p^{\geq m}$ the sum of the monomials of degree $\geq m$, we get

$$p_j(U) = \frac{p^{\geq j+1}}{U^{j+1}} = U^{n-j-1} + a_{n-1}U^{n-j-2} + \cdots + a_{j+1}\,.$$

With the notation of the above proposition we may write

$$\eta_M(x) = t^{n-1} \otimes p_{n-1}(u)(x) + \cdots + 1 \otimes p_0(u)(x) \in B \otimes_A M\,.$$

4) The endomorphism $\mu_M\,\eta\colon M \longrightarrow B \otimes_A M \longrightarrow M$ is equal to $p'(u)$. This remark "explains" the analogy between the sequences (2.6.1) and (8.3.1). In fact, we have $\eta = p'(t)\,\varepsilon$.

8.5. We now wish to describe the eigenspace relative to a general eigenvalue λ. Giving a root λ of $p(T)$ in some A-algebra A' is the same thing as giving a morphism of A-algebras

$$f\colon B \longrightarrow A'\,, \qquad f(t) = \lambda\,.$$

Hence a root gives rise to the following commutative diagram, obtained from (8.3.2) by the base change f:

$$\begin{array}{ccccc} A' \otimes_B M & \xrightarrow{1\otimes\eta_M} & A' \otimes_B (B \otimes_A M) & \xrightarrow{1\otimes(t\otimes 1 - 1\otimes u)} & A' \otimes_B (B \otimes_A M) \\ \| & & \| & & \| \\ A' \otimes_B M & \xrightarrow[1\otimes\eta_M]{} & A' \otimes_A M & \xrightarrow[\lambda\otimes 1 - 1\otimes u]{} & A' \otimes_A M\,. \end{array} \tag{8.5.1}$$

The submodule $\mathrm{Ker}(\lambda \otimes 1 - 1 \otimes u)$ in $A' \otimes_A M$ is the eigenspace relative to λ. It contains $\mathrm{Im}(1 \otimes \eta_M)$ but, unfortunately, it may be different from it. In other words, the lower row is not exact in general; for example, consider the case where $u = 0$, $\lambda = 0$, and $M \neq 0$. (See 8.7 below for a less trivial example.)

Achevé de composer le 24 février 2014 à 13 : 48

8.6. PROPOSITION. *Let M be an A-module with an A-linear map $u\colon M \to M$, and let $p(T)$ be a monic polynomial such that $p(u) = 0$. Moreover, denote by t the class of T in $B = A[T]/(p)$. Let $f\colon B \longrightarrow A'$ be a morphism of A-algebras, and let $\lambda = f(t)$. Then the sequence*

$$0 \longrightarrow A' \otimes_B M \xrightarrow{1\otimes\eta_M} A' \otimes_A M \xrightarrow{\lambda\otimes 1 - 1\otimes u} A' \otimes_A M \tag{8.6.1}$$

is exact, under each of the following hypotheses:

i) *the morphism $f\colon B \longrightarrow A'$ is flat;*

ii) *M is a projective B-module;*

iii) *B is finite étale over A.*

Proof. The commutativity of (8.5.1) reduces the proof to verifying that, under each of the hypotheses, the following sequence, obtained by tensoring (8.3.2) by A' on the left over B, remains exact:

$$0 \to A'\otimes_B M \xrightarrow{1\otimes\eta_M} A'\otimes_B (B\otimes_A M) \xrightarrow{1\otimes(t\otimes 1 - 1\otimes u)} A'\otimes_B (B\otimes_A M) \xrightarrow{1\otimes\mu} A'\otimes_B M \to 0\,.$$

This is obvious when f is flat.

Assume now that M is a projective B-module. Then it is also projective over A, and thus $B\otimes_A M$ is projective over B for the left B-module structure. The sequence (8.3.2) is exact as a sequence of B-modules for the left structure, by virtue of Remark 8.4 (2). As each term is projective over B, it is split for the same structure. Hence it remains exact by tensoring on the left by A' over B.

If B is finite étale over A then $p'(t)\otimes 1$ is invertible in $B \otimes_A B$, by Proposition 2.8, and thus the maps ε and $\eta = (p'(t)\otimes 1)\,\varepsilon$ have the same image. Moreover, we observed in 2.6 that the sequence (2.6.1), which begins with ε, is split as a sequence of $B \otimes_A B$-modules. Hence the sequence

$$0 \longrightarrow B \xrightarrow{\eta} B \otimes_A B \xrightarrow{t\otimes 1 - 1\otimes t} B \otimes_A B \xrightarrow{\mu} B \longrightarrow 0$$

is also split as a sequence of $B \otimes_A B$-modules. Therefore it remains exact when tensoring over $B \otimes_A B$ by the $B \otimes_A B$-module $A' \otimes_A M$. The last point to be checked is the isomorphism

$$B \otimes_{B\otimes_A B} (A' \otimes_A M) \xrightarrow{\sim} A' \otimes_B M\,.$$

Now, it is a general fact that the kernel of the surjective map $A'\otimes_A M \to A'\otimes_B M$ is generated by the elements $ba' \otimes x - a' \otimes bx$; hence it is the sub-module $\mathrm{Ker}(\mu)\,(A' \otimes_A M)$. □

8.7. EXAMPLE. In this example the situation is simple enough to make the maps in the above results explicit.

Let A be a ring containing two elements a and b such that $ab = 0$. Consider the endomorphism u of A^2 given by the matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. The characteristic polynomial $p_u(T) = T^2 - (a+b)T$ admits two factorizations $p_u(T) = (T-a)(T-b) = T(T-(a+b))$. We have $\partial p_u(X,Y) = X+Y-(a+b)$, and hence the map $\eta_M : M \longrightarrow B \otimes_A M$ of (8.3.2) is

$$\eta_M(x) = t \otimes x + 1 \otimes u(x) - 1 \otimes (a+b)\,x\,.$$

For the canonical basis (e_1, e_2) of M we thus have

$$\eta_M(e_1) = (t-b) \otimes e_1\,, \qquad \eta_M(e_2) = (t-a) \otimes e_2\,.$$

An element $b_1 \otimes e_1 + b_2 \otimes e_2$ in $B \otimes_A M$ is inside the *generic* eigenspace $\mathrm{Ker}(t \otimes 1 - 1 \otimes u)$ if $(t-a)\,b_1 = 0$ and $(t-b)\,b_2 = 0$. An immediate verification confirms that such a b_1 is of the form $(t-b)\,c_1$, and b_2 is of the form $(t-a)\,c_2$ with $c_i \in A$, as the exactness of the sequence (8.3.2) predicts.

For *special* eigenvalues the situation is more difficult. Let λ be a root of $p_u(T)$ in A, and let $f : B \to A$ be the morphism it defines, that is, $f(t) = \lambda$. Then $A \otimes_{f,B} M = M/(u-\lambda)\,M$, and $A \otimes_{f,B} (B \otimes_A M) = B/(t-\lambda)\,B \otimes_A M = M$. The map $1 \otimes \eta_M$ of (8.5.1) can now be written as

$$\eta_\lambda : M/(u-\lambda)\,M \longrightarrow M\,, \qquad \eta_\lambda(x) = \lambda x + u(x) - (a+b)x\,.$$

To determine the eigenspaces and discuss the exactness of the sequence (8.6.1) we must introduce the ideals: $\mathfrak{a} = \mathrm{Ann}_A(a)$, $\mathfrak{b} = \mathrm{Ann}_A(b)$ and $\mathfrak{c} = \mathrm{Ann}_A(a-b)$.

i) For the eigenvalue $\lambda = a$, we find the inclusion

$$\mathrm{Im}(\eta_a) = \mathrm{Im}(u-b) = (a-b)\,Ae_1 \subseteq \mathrm{Ker}(u-a) = Ae_1 + \mathfrak{c}e_2\,.$$

It is an equality if and only if $a-b$ is invertible in A, that is if B is étale. The same conclusion holds for the associate other eigenvalue $\mu = b$.

ii) For the eigenvalue $\lambda = 0$ we get the inclusion

$$\mathrm{Im}(\eta_0) = bAe_1 + aAe_2 \subseteq \mathrm{Ker}(u) = \mathfrak{a}e_1 + \mathfrak{b}e_2\,.$$

It is an equality if and only if $\mathfrak{a} = bA$ and $\mathfrak{b} = aA$.

For the ring $A = \mathbf{Z}[a,b]/(ab)$ the relations $\mathfrak{a} = bA$ and $\mathfrak{b} = aA$ are satisfied, but $a-b$ is not invertible; thus the inclusion in i) is strict, whereas the second one, in ii), is an equality. In the ring $\mathbf{Z}[a,b]/(a^2, ab, b^2)$, both inclusions are strict.

Achevé de composer le 24 février 2014 à 13 : 48

This remark shows that in general the exactness of the sequence (8.6.1) depends not only on u and on the polynomial p, but it also depends on the choice of the eigenvalue.

About the possible decompositions of M into a sum of eigenspaces, the same example shows that it depends on the choice of a factorization of the characteristic polynomial:

• If we use the decomposition $p_u = (T-a)(T-b)$, the eigenspaces are $\mathrm{Ker}(u-a) = Ae_1 + \mathfrak{c}e_2$ and $\mathrm{Ker}(u-b) = \mathfrak{c}e_1 + Ae_2$, and their sum is equal to the whole module M. However, their intersection is trivial if and only if $a-b$ is regular.

• If we now use the decomposition $p_u = T(T-(a+b))$, we find $\mathrm{Ker}(u) = \mathfrak{a}e_1 + \mathfrak{b}e_2$ and $\mathrm{Ker}(u-(a+b)) = \mathfrak{b}e_1 + \mathfrak{a}e_2$. The image of the map

$$\mathrm{Ker}(u) \times \mathrm{Ker}(u-(a+b)) \longrightarrow M$$

is the submodule $(\mathfrak{a}+\mathfrak{b})M$, and its kernel is isomorphic to $(\mathfrak{a}\cap\mathfrak{b})M$. This map is not even surjective without some strong conditions.

REFERENCES

[A] BOURBAKI, N. *Algèbre*, chap. IV–VII. Masson, Paris, 1981. (Translated into English as *Algebra II*. Springer, Berlin, 1990 and 2003.) *Algèbre*, chap. VIII. Springer, Berlin, 2012.

[AC] —— *Algèbre Commutative*. Translated into English as *Commutative Algebra*, Chap. 1–7. Springer, 1989.

[Al] ALMKVIST, G. Endomorphisms of finitely generated projective modules over a commutative ring. *Ark. mat. 11* (1973), 263–301.

[C] CHEVALLEY, C. *Théorie des groupes de Lie*. Hermann, Paris, 1968.

[EGA] GROTHENDIECK, A. Éléments de géométrie algébrique, chap. IV. *Publ. Math. Inst. Hautes Études Sci. 32* (1967).

[EL1] EKEDAHL, T. and D. LAKSOV. Two "generic" proofs of the spectral mapping theorem. *Amer. Math. Monthly 111* (2004), 572–585.

[EL2] EKEDAHL, T. and D. LAKSOV. Splitting algebras, symmetric functions and Galois theory. *J. Algebra Appl. 4* (2005), 59–75.

[F1] FERRAND, D. Un foncteur norme. *Bull. Soc. Math. France 126* (1998), 1–49.

[F2] —— Un module inversible associé au ruban de Möbius, et quelques autres. arXiv:0704.2483 (2007).

[Fr] FRISCH, S. Integrally closed domains, minimal polynomials, and null ideals of matrices. *Comm. Algebra 32* (2004), 2015–2017.

[L] LAKSOV, D. Diagonalization of matrices over rings. *J. Algebra 376* (2013), 123–138.

[LT] LAKSOV, D. and A. THORUP. Splitting algebras and Schubert calculus. *Indiana Univ. Math. J. 61* (2012), 1253–1312.

[LST] LAKSOV, D., L. SVENSSON and A. THORUP. The Spectral Mapping Theorem, norms on rings, and resultants. *L'Enseignement Math. (2) 46* (2000), 349–358; 359–360.

[M] MILNOR, J.W. *Topology from the Differentiable Viewpoint*. Univ. Press of Virginia, Charlottesville, 1965.

[MS] MUMFORD, D. and K. SUOMINEN. Introduction to the theory of moduli. In: *Algebraic Geometry, Oslo 1970* (F. Oort, ed.), 171–222. Wolters-Noordhoff, 1972.

[S] SAMUEL, P. Sur les anneaux factoriels. *Bull. Soc. Math. France 89* (1961), 155–173.

(Reçu le 4 mars 2013; version révisée reçue le 27 novembre 2013)

Daniel Ferrand

Institut Mathématique de Jussieu
F-75005 Paris
France
e-mail: dferrand@math.jussieu.fr

Dan Laksov

Department of mathematics
KTH
Stockholm
Sweden

Achevé de composer le 24 février 2014 à 13:48