M1 2020-2021: Modules over commutative rings

David Harari

Table des matières

1. Introduction to modules

Modules are the natural generalization of vector spaces. They are of absolutely fundamental importance in, for example, algebraic geometry and number theory. In all of the following, A corresponds to a commutative ring, which will occasionally be required to be non-zero.

1.1. First notions

Definition 1.1 An *A-module* $(M, +, .)$ is a set endowed with an internal composition law $+$ and an external one : $A \times M \to M$, $(\alpha, m) \mapsto \alpha.m$ (often abbreviated as αm) satistifying :

— $(M, +)$ is an abelian group.

— The following properties :

1. $\alpha(m + m') = \alpha m + \alpha m'$
2. $(\alpha + \beta)m = \alpha m + \beta m$
3. $(\alpha\beta)m = \alpha(\beta m)$
4. $1.m = m$

hold for all $\alpha, \beta \in A$ and all $m, m' \in M$.

Remark 1.2 As A is supposed commutative, there is no need to distinguish between left and right modules (for noncommutative A the third property is different for right modules).

Definition 1.3 Let M be an A-module. A *submodule* N of M is a subgroup of $(M, +)$ which is also stable with respect to external multiplication by any element of A.

In other words, a subset N of M is a submodule if and only if it contains 0 and if for any x, y in N and α in A, we have : $x + y \in N$ and $\alpha x \in N$.

Example 1.4 a) A is an A-module, where the external operation is the multiplication operation in A itself.

b) Any abelian group M can be seen as a $\mathbf{Z}$-module with external operation : $\alpha.m = \alpha m$.

c) Let $n > 0$ and M be an *n-torsion* abelian group, i.e., one for which $nx = 0$ for all x in M. Then M is a $\mathbf{Z}/n\mathbf{Z}$-module with operation $\bar{\alpha}.x = \alpha x$, where $\alpha \in \mathbf{Z}$ is of the class $\bar{\alpha}$ in $\mathbf{Z}/n\mathbf{Z}$.

d) Let I be a subset of A. Then I is a sub-A-module of A if and only if it is an ideal of A.

e) Let $(M_i)_{i \in I}$ be a (finite or infinite) family of A-modules. Then the product set $\prod_{i \in I} M_i$ is an A-module with the obvious operations ; we call this the *product A-module* of the M_i.

f) Let S be a subset of an A-module M. Then the *submodule generated by* S is the set of linear combinations $\sum_{s \in S} \alpha_s s$, where $(\alpha_s)_{s \in S}$ is an almost zero family of elements of A. This is the smallest submodule of M that contains S. This notion is especially useful when S is finite.

Definition 1.5 A *homomorphism* (or morphism) of A-modules is a map $f : M \to M'$ between two A-modules that satisfies : $f(x+y) = f(x) + f(y)$ and $f(\alpha.x) = \alpha.f(x)$ for all x, y in M and α in A. We call $\ker f := f^{-1}(\{0\})$ the *kernel* of f and $\operatorname{Im} f := f(M)$ its image. These are submodules of respectively M and M'.

Instead of calling this a homomorphism of A-modules, we sometimes call it an A-linear map. We continue to have notions such as isomorphism and automorphism for A-modules, as well as the usual factorization theorem (whose proof is immediate) :

Proposition 1.6 *Let M be an A-module and N a submodule of M. Then the quotient group M/N, endowed with the external operation $\alpha.\bar{m} = \overline{\alpha.m}$ is an A-module, called the quotient module of M by N. If $f : M \to M'$ is a homomorphism of A-modules, there exists a unique homomorphism $\tilde{f} : M/\ker f \to M'$ such that $f = \tilde{f} \circ \pi$, where $\pi : M \to M/\ker f$ is the canonical projection. Furthermore, $\tilde{f}$ is one-to-one and has image* $\operatorname{Im} f$.

Remark 1.7 If $f : M \to M'$ is a homomorphism of A-modules and N a submodule of M contained in $\ker f$, then f can also be factorized by a homomorphism $M/N \to M'$ with image $\operatorname{Im} f$ (though we lose the one-to-one property which holds when $N = \ker f$).

The following definition is analogous to the one we had for vector spaces :

Definition 1.8
- — Let $(M_i)_{i\in I}$ be a family of A-modules. The ("external") *direct sum* of the M_i is the submodule $\bigoplus_{i\in I} M_i$ of the product $\prod_{i\in I} M_i$ of almost zero families $(m_i)_{i\in I}$. If I is finite, the direct sum coincides with the direct product. Note that each M_i is injected into $\bigoplus_{i\in I} M_i$ by mapping m_i to the element for which all of its components are zero except the i-th one, which is equal to m_i. Thus, we can write any element of $\bigoplus_{i\in I} M_i$ uniquely in the form $\sum_{I\in I} m_i$ with $m_i \in M_i$ and almost all m_i are zero.
- — Let $(M_i)_{i\in I}$ be a family of submodules of the A-module M. Then the *sum* submodule $\sum_{i\in I} M_i$ is that generated by the union of the M_i. More explicitly, it is the set of sums $\sum_{i\in I} m_i$, where $(m_i)_{i\in I}$ is an almost zero family with $m_i \in M_i$ for each $i \in I$. If furthermore the condition $\sum_{i\in I} m_i = 0$ implies $m_i = 0$ for all i, we say that the sum of the M_i is *direct*; in this case, $\sum_{i\in I} M_i$ is isomorphic to the external direct sum $\bigoplus_{i\in I} M_i$, and we write $\bigoplus_{i\in I} M_i$ for $\sum_{i\in I} M_i$ ("internal direct sum").

Note that the sum of two submodules M_1 and M_2 of an A-module M is direct if and only if $M_1 \cap M_2 = \{0\}$, but this cannot be generalized to more than two submodules. Also, if $M = M_1 \oplus M_2$, then M/M_1 is isomorphic to M_2 (via the projection onto M_2) but unlike in the vector space case, the converse is not necessarily true[1] (for example, $\mathbf{Z}$ is not isomorphic to the external direct sum of $n\mathbf{Z}$ and $\mathbf{Z}/n\mathbf{Z}$ since $\mathbf{Z}$ has no non-zero element that vanishes under multiplication by n).

Remark 1.9 For any family of homomorphisms of A-modules $f_i : M_i \to N$, there exists a unique homomorphism f from $\bigoplus_{i\in I} M_i$ to N which induces the homomorphism f_i on each M_i (identified with a submodule of $\bigoplus_{i\in I} M_i$) : f is defined by $f(\sum_i m_i) = \sum_i f_i(m_i)$. This is what is known as the universal property of direct sums. We write $f = \bigoplus_{i\in I} f_i$. The direct product $\prod_i M_i$ itself satisfies a universal property "in the other direction" : for any family of homomorphisms $g_i : N \to M_i$, there exists a unique homomorphism $N \to \prod_i M_i$ which induces g_i after composition with the projection on M_i.

1.2. Interlude : the determinant of a matrix with values from a commutative ring

We will need to extend to arbitrary commutative rings classical results on the determinant of a matrix with values from a field. We start by generalizing to modules the notion of n-linear forms :

Definition 1.10 Let A be a commutative ring. An *n-linear form* (bilinear if $n = 2$, trilinear if $n = 3$) on an A-module M is a map $f : M^n \to A$ which satisfies, for any $j \in \{1, \dots, n\}$ and any $(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n)$ in M^n that the map

$$x \mapsto f(x_1, \dots, x_{j-1}, x, x_{j+1}, \dots, x_n)$$

is A-linear from M into A. An n-linear form f is said to be *alternating* if $f(x_1, \dots, x_n) = 0$ whenever there exists $i \neq j$ for which $x_i = x_j$.

We define the ring $M_n(A)$ of (n, n) matrices with coefficients from A in the usual way. The determinant of a matrix $M = (a_{ij})_{1\leq i,j\leq n} \in M_n(A)$ is then defined by the usual formula :

$$\det M := \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i}.$$

1. In other words, an exact sequence of vector spaces is always split, but not an exact sequence of A-modules.

The usual properties of the determinant generally hold when A is a field, via the properties of vector spaces (though some are no longer valid in the general framework we find ourselves in here). It is possible to develop the properties of alternating n-linear forms on A^n and thereby obtain these results. Here we will use another approach, consisting in transporting ourselves to the case where A is a field.

Theorem 1.11 *a) If M and N are matrices in $M_n(A)$, then*

$$\det(MN) = \det M . \det N.$$

b) The map that associates with the n column vectors (resp. row vectors) the determinant of the matrix M formed by these vectors is an alternating n-linear form on A^n. In particular, the determinant of a matrix $M \in M_n(A)$ is unchanged when adding to one of its columns (resp. rows) a linear combination of the others.

c) We can calculate the determinant of any matrix M in $M_n(A)$ via Laplace expansion along a row or a column in the same way as can be done when A is a field.

d) Let $M \in M_n(A)$ and $\widetilde{M}$ be the adjoint of M (i.e., the transpose of its cofactor matrix); then :

$$M\widetilde{M} = \widetilde{M}M = (\det M)I_n.$$

Proof: All of the claims are proved using the same technique : we first note that if A is an integral domain, it can be seen as a subring of its field of fractions K ; the results then follow immediately from the field case. Furthermore, it is clear that if one of these claims is true for a ring A, it is also true for any quotient ring A/I (where I is an ideal of A). In particular, we obtain the result for any ring A which is a quotient of the integral domain $\mathbf{Z}[X_1, \ldots, X_r]$ (where r is an integer), i.e., is of finite type as a $\mathbf{Z}$-algebra.

Now it suffices to note [2] that to prove (a) for instance, all that is needed is to replace A by the subring of A generated by the coefficients of M and N (which is by definition a $\mathbf{Z}$-algebra of finite type). The same can be done for (b)–(d), replacing A with the subring of A generated by the coefficients of M.

□

Note that with this procedure we can also prove the Cayley-Hamilton theorem over any commutative ring A : for any matrix $M \in M_n(A)$ with characteristic polynomial $\chi_M \in A[X]$, we have $\chi_M(M) = 0$.

2. We can also simply observe that A is isomorphic to a quotient of a polynomial ring over $\mathbf{Z}$ (in general with an infinite number of inderterminates).

1.3. Free modules, modules of finite type

Definition 1.12 An A-module M is said to be *of finite type* if there exists a finite subset S of M such that M is generated by S. It is said to be *free* if there exists a basis for it, i.e., a family $(x_i)_{i\in I}$ such that any element x in M can be written $x = \sum_{i\in I} \alpha_i x_i$ in a unique way, where $(\alpha_i)_{i\in I}$ is an almost zero family of elements of A.

Remark 1.13 a) We will see that if M is free and of finite type, there exists a finite basis for it, though this is far from clear at the moment !

b) Saying that $(x_i)_{i\in I}$ is a basis is equivalent to the family (x_i) being both a generating set and free, the latter signifying that the condition $\sum_{i\in I} \alpha_i x_i = 0$ implies that the almost zero family (α_i) is trivial.

c) An A-module M has a basis of cardinal n if and only if it is isomorphic to A^n. More generally, it has a basis of cardinal I if and only if it is isomorphic to $A^{(I)}$ (the set of almost zero families $(\alpha_i)_{i\in I}$ in A^I). [3]

d) An A-module M is of finite type if and only if it can be written as a quotient of A^n for some $n > 0$. Do not mix up this notion with that of A-algebras of finite type seen in the chapter on rings (which corresponds to being a quotient of the polynomial ring $A[X_1, \ldots, X_n]$). When an A-algebra is of finite type in the A-module sense, we sometimes call it a *finite* A-algebra.

Example 1.14 a) $\mathbf{Z}/n\mathbf{Z}$ is a $\mathbf{Z}$-module of finite type (generated by $\bar{1}$), but not free because in a free $\mathbf{Z}$-module, $\alpha x = 0$ implies $\alpha = 0$ or $x = 0$ if $\alpha \in \mathbf{Z}$, $x \in M$ (such modules are called *torsion-free*. This is more generally the case in any free module over an integral domain).

b) While the $\mathbf{Z}$-module $\mathbf{Q}$ is torsion-free, it is not free since it is *divisible*, i.e., if $n > 0$, any element x of $\mathbf{Q}$ can be written ny with $y \in \mathbf{Q}$, which is not possible in a free $\mathbf{Z}$-module (take an element for which one of its components in the basis is 1, and $n \geq 2$). We will see that for a principal ideal domain, a module of finite type that is torsion-free is also free.

c) It is easy to see that a quotient of a module of finite type is also of finite type.

d) If A is a non-Noetherian ring, an ideal of A which is not generated by a finite number of elements is not of finite type as an A-module, even though it is a submodule of A (which is generated by 1). We will see that if A is Noetherian, a submodule of a module of finite type over A is also of finite type.

e) Let A be a ring and B an A-algebra. Suppose that B is an A-module of finite type. Then any B-module M of finite type is also an A-module of finite

3. Be careful : if I is infinite, it does not necessarily follow that A^I is free.

type. In effect, if $(m_1, \ldots, m_n)$ generates the B-module M and $(b_1, \ldots, b_r)$ generates the A-module B, we see immediately that the family $(b_i m_j)$ (for $1 \leq i \leq r$ and $1 \leq j \leq n$) generates the A-module M.

Thus, the situation is more complicated for modules than for vector spaces. There is however a statement which is true in general : bases of M are finite and have the same cardinality if M is free and of finite type. This is the subject of the following theorem :

Theorem 1.15 *Let A be a non-zero commutative ring. Suppose that there exists an onto homomorphism of A-modules $f : A^r \to A^s$. Then $r \geq s$.*

Proof: We will provide two different proofs. The first consists of linking up with the known result for vector spaces, while the second involves matrix calculations using the properties of determinants.

Proof 1 : Since $A \neq \{0\}$, A possesses at least one maximal ideal I (due to Zorn's theorem in the general case, though obviously true if A is Noetherian). For any A-module M, we define the sub-A-module IM as that generated by the im for $i \in I$ and $m \in M$. Then M/IM is a vector space over the field $K := A/I$ via $\bar{a}\bar{m} := \overline{am}$, $a \in A$, $m \in M$. We apply this to $M = A^r$, $N = A^s$. The onto homomorphism of A-modules $f : M \to N$ induces a homomorphism $\bar{f}$ of K-vector spaces $M/IM \to N/IN$ defined by $\bar{f}(\bar{m}) = \overline{f(m)}$, and it is clear that $\bar{f}$ is still onto. Since M/IM is isomorphic to K^r (we map the class of $(a_1, \ldots, a_r)$ onto $(\bar{a}_1, \ldots, \bar{a}_r)$), we obtain an onto homomorphism of K-vector spaces from K^r to K^s ; thus $r \geq s$ by the classical theorem on the rank of linear maps between vector spaces. [4]

Proof 2 : Let $B \in M_{s,r}(A)$ be the matrix of the A-linear function $f : A^r \to A^s$. Since f is onto, the elements $\varepsilon_1, \ldots, \varepsilon_s$ of the canonical basis of A^s are each mapped to from something by f, this being column vectors $X_1, \ldots, X_s$ of A^r for which $BX_i = \varepsilon_i$. The matrix C of $M_{r,s}(A)$ whose column vectors are the X_i thus satisfies $BC = I_s$. If we had $s > r$, we could consider the matrix B_1 obtained by adding $s - r$ non-zero columns to B, and the matrix C_1 obtained by adding $s - r$ rows of zeros to C, and we would still have $B_1 C_1 = I_s$, with B_1 and C_1 in $M_s(A)$. But then $\det B_1 \det C_1 = 1$ (which is not zero, since A is non-zero !), which is impossible given that according to theorem 1.11, a matrix with a row or columns of zeros has a determinant of zero.

4. After we have seen tensor products, we will be able to reformulate this proof : we tensorize M and N by the A-module $K = A/I$; this operation preserves the onto (but not one-to-one) property of homomorphisms, and turns A^r into K^r. Note that if A is not an integral domain, we cannot do the same thing by using the field of fractions.

□

Corollary 1.16 *Let M be a module over a non-zero ring A. If M is of finite type and possesses a basis, then this basis is finite. In this case we say that M is* free and of finite type*, and all of its bases have the same cardinality, which is called the* rank *of M.*

Proof: Let r be a non-negative integer. First note that if M possesses a basis (finite or otherwise) of cardinality $> r$, then there exists a submodule N of M such that M/N is isomorphic to A^{r+1} (it suffices to take $r+1$ elements $e_1, \ldots, e_{r+1}$ in the basis, and to choose N as the submodule made up of the m of M whose components with respect to e_i are zero for all i in $[1, r+1]$). Now, suppose that M is generated by a finite family $(f_1, \ldots, f_r)$. Then we have an onto homomorphism of A-modules $u : A^r \to M$ defined by $u(a_1, \ldots, a_r) = \sum_{i=1}^{r} a_i f_i$. If M has an infinite basis (and in particular with cardinality $> r$), we would have a quotient M/N such that M/N is isomorphic to A^{r+1}. Under the composition of u with the canonical projection $M \to M/N$, we would obtain an onto A-linear function from A^r to A^{r+1}, which would contradict theorem 1.15. Thus, if M possesses a basis, this basis is finite. The fact that all bases have the same cardinality follows immediately from theorem 1.15.

□

1.4. Submodules over Noetherian rings

Though in a free module of finite type over a non-zero commutative ring A, all bases have the same cardinality, we cannot hope to have results for submodules that are comparable to those for vector spaces :

Example 1.17 We see that $2\mathbf{Z}$ is a strict sub-$\mathbf{Z}$-module of $\mathbf{Z}$, even though both have a rank of 1 (a basis of the former is $\{2\}$, the latter : $\{1\}$). Thus $2\mathbf{Z}$ is not a direct summand of $\mathbf{Z}$, as an N such that $2\mathbf{Z} \oplus N = \mathbf{Z}$ would have to be isomorphic to $\mathbf{Z}/2\mathbf{Z}$, whereas $\mathbf{Z}$ has no submodule isomorphic to $\mathbf{Z}/2\mathbf{Z}$ (since it has no non-zero element x for which $2x = 0$). Therefore, the free family (2) cannot be extended to a basis of $\mathbf{Z}$. On the other hand, if A is not Noetherian, the A-module A is free and of rank 1 but has submodules (= ideals of A) that are not of finite type.

Remark 1.18 It can be shown (using fairly tedious calculations on determinants, see tutorials) that if P is a matrix in $M_r(A)$ and f the A-linear function $A^r \to A^r$ induced by it, f is one-to-one if and only if $\det A$ is non-zero and does not divide zero in the ring A. From this we can deduce that if

$f : A^r \to A^s$ is one-to-one linear (with $A \neq \{0\}$), then $r \leq s$ since if we had $r > s$, the matrix obtained by adding $r - s$ rows of zeros to the matrix of f would still be a linear one-to-one map (as it would represent the composition of f with the one-to-one map $A^s \to A^r$ defined by $x \mapsto (x, 0, 0, \ldots)$) and would have a determinant of 0. Thus, if M is a free submodule of A^s, then its rank r is at most s since $M \simeq A^r$. In particular, an ideal I of a ring A cannot be a free A-module if it is not generated by a single element. We can therefore hope for a positive result only for principal ideal domains, and we will see that this is indeed the case.

Theorem 1.19 *Let A be a Noetherian ring and M an A-module of finite type. Then any submodule of M is of finite type.*

Proof: Since M is of finite type, we can write it as a quotient A^r/M' where M' is a submodule of A^r ; a submodule of A^r/M' is of the form N'/M', with N' a submodule of A^r containing M'. Thus it suffices to prove the result for $M = A^r$ since a quotient of a module of finite type is also of finite type.

We show this by induction on r. For $r = 1$, this corresponds to the definition of Noetherian rings. Suppose that the result is true for all positive integers $< r$, and let N be a submodule of A^r. Denote by M_1 the submodule of A^r made up of the $(a, 0, 0, \ldots, 0)$ with $a \in A$, so M_1 is isomorphic to A. From the $r = 1$ case, $N_1 := N \cap M_1$ is of finite type. Also, the linear map $\pi : N \to A^r/M_1$ which associates $\bar{x}$ with x has the kernel N_1 ; the module A^r/M_1 is isomorphic to A^{r-1}, thus $\operatorname{Im} \pi$ is of finite type by the induction hypothesis. Let $(\bar{x}_1, \ldots, \bar{x}_n)$ be a finite family that generates $\operatorname{Im} \pi$ ($x_i \in N$) and $(y_1, \ldots, y_m)$ a finite family that generates N_1. Then, $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ generates N. [5] In effect, if $x \in N$, we can write $\bar{x} = \sum_{i=1}^{r} \alpha_i \bar{x}_i$ with the α_i in A, which means that

$$x = \sum_{i=1}^{r} \alpha_i x_i + y,$$

with $y \in (N \cap M_1) = N_1$, and then

$$x = \sum_{i=1}^{r} \alpha_i x_i + \sum_{i=1}^{m} \beta_i y_i,$$

with the β_i in A.

□

5. More generally, if $0 \to M_1 \to M \to M_2 \to 0$ is an exact sequence of A-modules, it is clear that M_1 and M_2 being of finite type implies that M is too.

Remark 1.20 a) Note that a submodule of M may need more generators than N does ; e.g., take an ideal of A that is not principal. We will see that this difficulty disappears when the ring A is a PID.

b) A module M over a commutative ring A is said to be *Noetherian* if all of its submodules are of finite type (or equivalently : if every increasing sequence of submodules of M is stationary). Theorem 1.19 means that any module of finite type over a Noetherian ring is a Noetherian module.

2. Tensor products

2.1. Introduction

The notion of a tensor product is a little difficult to grasp at the beginning, but it turns out to be essential when we want to deal with advanced subjects in algebra (especially in number theory and algebraic geometry). We will be content in this introductory course to consider some basic properties and examples. Nevertheless, it seemed important to us not to limit ourselves to the case of vector spaces over fields, which would have been overly restrictive (especially as over a field, we can often use matrix methods without even really needing tensor products).

Before going into detail, let us first point out some examples (seen previously in this course, or in previous years) where the tensor product is already involved :

— Complexifying a real vector space
— When A is a subring of a commutative ring B, looking at a matrix with coefficients in A as if they were also coefficients in B
— The proof of theorem 1.15.

In the rest of this section, we suppose that A is a commutative ring.

2.2. Tensor products of modules

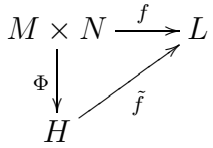
First, recall a previously seen definition for when $L = A$:

Definition 2.1 Let M, N, and L be modules over the commutative ring A. A map $f : M \times N \to L$ is said to be A-*bilinear* (or simply bilinear if A is implied) if for all $m \in M, n \in N$, the maps $f(m, .)$ and $f(., n)$ are A-linear from N (resp. M) to L.

Let M and N be A-modules. We want to construct an A-module H, equipped with a bilinear map $\Phi : M \times N \to H$, which satisfies the following *universal property* :

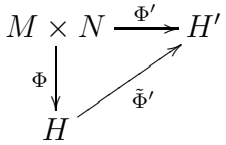
(P) For any A-module L and bilinear map $f : M \times N \to L$, there exists a unique homomorphism of A-modules $\tilde{f} : H \to L$ such that $f = \tilde{f} \circ \Phi$.

More explicitly : given f and Φ, we want there to always be a unique A-linear map $\tilde{f}$ that makes the following diagram commutative :



Theorem 2.2 *Such a module H exists and is unique up to isomorphism. We call it the tensor product of the A-modules M and N, and write it $M \otimes_A N$.*

Proof: If H and H' both satisfy (P) (with bilinear maps Φ and Φ' respectively), we first apply (P) to (H, Φ), taking for f the bilinear map Φ', which gives an A-linear map $\tilde{\Phi}' : H \to H'$ that makes the following diagram commutative :



We can therefore factorize : $\Phi' = \tilde{\Phi}' \circ \Phi$; by symmetry we have also an A-linear map $\tilde{\Phi} : H' \to H$ such that $\Phi = \tilde{\Phi} \circ \Phi'$. Thus,

$$\tilde{\Phi} \circ \tilde{\Phi}' \circ \Phi = \tilde{\Phi} \circ \Phi' = \Phi,$$

which can be rewritten as $\mathrm{Id}_H \circ \Phi = (\tilde{\Phi} \circ \tilde{\Phi}') \circ \Phi$. Uniqueness in the universal property (P) (applied to (H, Φ) with bilinear map $f = \Phi$) then gives $\tilde{\Phi} \circ \tilde{\Phi}' = \mathrm{Id}_H$ and, similarly, $\tilde{\Phi}' \circ \tilde{\Phi} = \mathrm{Id}_{H'}$, and hence an isomorphism between H and H'.

We now show the existence of an (H, Φ) satisfying (P). Consider the A-module $A^{(M \times N)}$ of almost zero families of elements of A indexed by $M \times N$, where we denote by $(e_{x,y})_{(x,y) \in M \times N}$ the canonical basis (all components of $e_{x,y}$ are zero except that of (x, y) which is equal to 1). Let H be the quotient of $A^{(M \times N)}$ by the submodule R generated by elements with one of the following forms :

$$e_{x_1+x_2,y} - e_{x_1,y} - e_{x_2,y}, \quad e_{x,y_1+y_2} - e_{x,y_1} - e_{x,y_2}, \quad e_{ax,y} - a e_{x,y}; e_{x,ay} - a e_{x,y},$$

with $x_1, x_2, x \in M$, $y_1, y_2, y \in N$, and $a \in A$.

Now let $\theta : M \times N \to A^{(M \times N)}$ be the map that sends (x, y) to $e_{x,y}$. It is not a priori bilinear, but if we note $\Phi : M \times N \to H$ the map induced by

θ, which sends (x, y) to the image $\overline{e_{x,y}}$ of $e_{x,y}$ in $H = A^{(M\times N)}/R$, then Φ is bilinear by the definition of R.

If now $f : M \times N \to L$ is a bilinear map, the homomorphism u of A-modules $A^{(M\times N)} \to L$ which sends each $e_{x,y}$ to $f(x, y)$ has a kernel which contains R due to the bilinearity of f, and therefore induces a homomorphism $\tilde{f} : H \to L$ upon taking the quotient. By the definition of θ, we have a commutative diagram :

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & L \\ {\scriptstyle\theta}\downarrow & \nearrow_{u} & \\ A^{(M\times N)} & & \end{array}$$

whence (taking the quotient) a commutative diagram :

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & L \\ {\scriptstyle\Phi}\downarrow & \nearrow_{\tilde{f}} & \\ H & & \end{array}$$

In other words, we have $f = \tilde{f} \circ \Phi$, and it can be immediately seen that $\tilde{f}$ is the only homomorphism of A-modules of H in L that satisfies this property. We have therefore indeed shown that the universal property (P) holds for (H, Φ).

□

Remark 2.3 a) Strictly speaking, we should use the notation $(M \otimes_A N, \Phi)$ for the tensor product, but in general the bilinear map Φ is implicitly known.

b) When M and N are abelian groups, we will often write $M \otimes N$ for $M \otimes_{\mathbf{Z}} N$.

c) For $(x, y) \in M \times N$, we will denote by $x \otimes y$ the image of (x, y) by Φ. Thus, any element of $M \otimes_A N$ can be written (generally non-uniquely) as a finite sum $\sum_i x_i \otimes y_i$ with $(x_i, y_i) \in M \times N$. Hence the map $(x, y) \mapsto x \otimes y$ is A-bilinear on $M \times N$.

The universal property is therefore now : for all bilinear maps $f : M \times N \to L$, there exists a unique linear map $\tilde{f} : M \otimes N \to L$ such that

$$f(x, y) = \tilde{f}(x \otimes y)$$

for all $x \in M$, $y \in N$.

d) The elements of $M \otimes_A N$ of the form $x \otimes y$ with $x \in M$ and $y \in N$ are sometimes known as *decomposable* elements of $M \otimes_A N$. Keep in mind that they generate the A-module $M \otimes_A N$, but seen as a set, they cannot be a submodule of $M \otimes_A N$.

Example 2.4 a) The universal property means that

$$M \otimes_A A = A \otimes_A M = M,$$

where by abuse of notation, we have written "$=$" instead of "$\simeq$". More generally, if $N = Ae_1$ is free and with basis (e_1), then $u : m \mapsto e_1 \otimes m$ is an isomorphism from M to $N \otimes_A M$. Indeed, if we set $f(\lambda e_1, m) = \lambda m$ for all $\lambda \in A$, $m \in M$, this gives us a well-defined bilinear map from $N \times M$ to M (seeing as (e_1) is a basis of N). The universal property therefore means there is a linear map $\tilde{f} : N \otimes_A M \to M$ which makes the following diagram commutative :

$$\begin{array}{ccc} N \times M & \xrightarrow{f} & M \\ {\scriptstyle \Phi}\downarrow & \nearrow_{\tilde{f}} & \\ N \otimes_A M & & \end{array}$$

Thus, $\tilde{f}(e_1 \otimes m) = m$ for all $m \in M$, which implies that f corresponds to an inverse of the linear map u (by noticing that any element of $N \otimes_A M$ is a sum of elements of the form $\lambda e_1 \otimes m$ with $m \in M$ and $\lambda \in A$, which by bilinearity can be written $e_1 \otimes m$ with $m \in M$).

b) Let r and s be two integers that are prime with each other. Then $\mathbf{Z}/r\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/s\mathbf{Z} = 0$. In effect, there exists integers u and v such that $ur + vs = 1$ (Bézout). For $x \in \mathbf{Z}/r\mathbf{Z}$ and $y \in \mathbf{Z}/s\mathbf{Z}$, we therefore have :

$$x \otimes y = (ur + vs)(x \otimes y) = urx \otimes y + x \otimes vsy = 0 \otimes y + x \otimes 0 = 0.$$

c) Let M be an abelian group and suppose $n \in \mathbf{N}^*$. We show using the universal property that

$$M \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \simeq M/nM.$$

For this, we define $\Phi : M \times \mathbf{Z}/n\mathbf{Z} \to M/nM$ by $\Phi(m, \bar{a}) = a.m$ for all $m \in M$ and $a \in \mathbf{Z}$, where $\bar{a}$ is the class of a in $\mathbf{Z}/n\mathbf{Z}$; this makes sense because if we modify a by an element in $n\mathbf{Z}$, we modify $a.m$ by an element in nM. Thus, if $f : M \times \mathbf{Z}/n\mathbf{Z} \to L$ is bilinear, we have for all $m \in M$, $a \in A$:

$$f(m, \bar{a}) = f(m, a\bar{1}) = f(am, \bar{1}),$$

and therefore have the commutative diagram

$$\begin{array}{ccc} M \times \mathbf{Z}/n\mathbf{Z} & \xrightarrow{f} & L \\ {\scriptstyle \Phi}\downarrow & \nearrow_{\tilde{f}} & \\ M/nM & & \end{array}$$

where $\tilde{f}$ is the A-linear map $f(.,\bar{1})$, which is well-defined on M/nM (note that if $y = nz$ is in nM, then $f(y,\bar{1}) = f(z,\bar{n}) = 0$). Also, $\tilde{f}$ is clearly the only A-linear map with this property.

In particular, if M is a divisible abelian group (e.g., $M = \mathbf{Q}$), we have $M \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} = 0$.

Proposition 2.5 *a) (Commutativity) If M and N are A-modules, then*

$$M \otimes_A N \simeq N \otimes_A M.$$

b) (Associativity) If M, N, and P are A-modules, then

$$P \otimes_A (M \otimes_A N) \simeq (P \otimes_A M) \otimes_A N.$$

c) (Distributivity) If (M_i) is a family of A-modules and N an A-module, then[6]

$$(\bigoplus_i M_i) \otimes_A N \simeq \bigoplus_i (M_i \otimes N).$$

In other words, "the tensor product commutes with direct sums".

Proof (sketch): All follows from the universal property (P). Let us prove for example (c) by showing that $\bigoplus_i (M_i \otimes N)$ satisfies the universal property of $(\bigoplus_i M_i) \otimes_A N$. Define

$$\Phi : (\bigoplus_i M_i) \times N \to \bigoplus_i (M_i \otimes N)$$

by mapping $(\sum_i m_i, n)$ onto $\sum_i m_i \otimes n$. Now let $f : (\bigoplus_i M_i) \times N \to L$ be bilinear; this induces for each i a bilinear map $f_i : M_i \times N \to L$, which factorizes (via the universal property of $M_i \otimes N$) through a unique linear map $\tilde{f}_i : M_i \otimes N \to L$. Then, via the universal property of the direct sum (remark 1.9) we have a unique homomorphism $\tilde{f} : \bigoplus_i (M_i \otimes N) \to L$ satisfying $f = \tilde{f} \circ \Phi$ defined by $\tilde{f} = \bigoplus \tilde{f}_i$.

□

Corollary 2.6 *Let M be a free A-module with basis $(e_i)_{i \in I}$. Then any element of $M \otimes_A N$ can be written uniquely as $\sum_i e_i \otimes y_i$, where (y_i) is an almost zero family of elements of N. In particular, if K is a field and $(f_j)_{j \in J}$ a basis of the K-vector space N, then $(e_i \otimes f_j)_{i \in I, j \in J}$ is a basis of the K-vector space $M \otimes_K N$. When M and N are both finite-dimensional over K, we have :*

$$\dim(M \otimes_K N) = \dim M . \dim N.$$

6. Warning : this property is not true in general if we replace the direct sum by the direct product of an infinite number of modules; however, it can be extended to what we call a *direct limit* (or colimit) of A-modules—see tutorial.

Proof: We write $M = \bigoplus_i Ae_i$, from which $M \otimes_A N = \bigoplus_i (Ae_i) \otimes_A N$ via proposition 2.5 (c). We then use example 2.4 (a) which says that any element of $(Ae_i) \otimes_A N$ can be written uniquely as $e_i \otimes y_i$ with $y_i \in N$.

□

Remark 2.7 The associativity of the tensor product makes it possible to unambiguously define the tensor product $M_1 \otimes_A \otimes_A \ldots \otimes_A M_n$ of n modules, for which we have a universal property like (P) : there is an n-linear map

$$\Phi : M_1 \times \ldots \times M_n \to M_1 \otimes_A \ldots \otimes_A M_n; \quad (m_1, \ldots, m_n) \mapsto m_1 \otimes \ldots \otimes m_n$$

such that for any n-linear map $f : M_1 \times \ldots \times M_n \to L$, there exists a unique linear map $\tilde{f} : M_1 \otimes_A \otimes_A \ldots \otimes_A M_n \to L$ which makes the following diagram commutative :

$$\begin{array}{ccc} M_1 \times \ldots \times M_n & \xrightarrow{f} & L \\ \Phi \downarrow & \nearrow_{\tilde{f}} & \\ M_1 \otimes_A \ldots \otimes_A M_n & & \end{array}$$

In other words, we have

$$f(m_1, \ldots, m_n) = \tilde{f}(m_1 \otimes \ldots \otimes m_n)$$

for all $m_1, \ldots, m_n$ in M.

Definition 2.8 Let $u : M \to M'$ and $v : N \to N'$ be homomorphisms of A-modules. Then by the universal property (P) applied to the bilinear map $(x, y) \mapsto u(x) \otimes v(y)$, there exists a unique homomorphism of A-modules

$$u \otimes v : M \otimes_A N \to M' \otimes_A N'$$

such that

$$(u \otimes v)(x \otimes y) = u(x) \otimes v(y)$$

for all $x \in M, y \in N$. We call $u \otimes v$ the *tensor product* of the homomorphisms u and v.

2.3. Tensor product with an A-algebra

Let B be an A-algebra, associated with a ring homomorphism $\varphi : A \to B$. Let M be an A-module. Note that a B-module N is automatically also an A-module : define $a.n = \varphi(a).n$ for all $a \in A$, $n \in N$. The tensor product allows us to—in a sense—perform the inverse operation :

Definition 2.9 Let B be an A-algebra, and M an A-module. We define a B-module structure on $M \otimes_A B$ by setting, for each $b \in B$, $b.z := (\mathrm{Id}_M \otimes m_b)(z)$, where $m_b : B \to B$ is multiplication by b. In other words, we have

$$b.(m \otimes b') := m \otimes bb' \tag{1}$$

for all $m \in M$, $b, b' \in B$. We say that the B-module $M \otimes_A B$ is obtained from M by *scalar extension* of A to B.

Note that we can immediately check the axioms for B-module structure via formula (1) and the fact that any element of $M \otimes_A B$ is a sum of elements of the form $m \otimes b'$ with $m \in M$ and $b' \in B$.

Example 2.10 The same procedure allows us to define a B-module structure on $M \otimes_A N$ for any A-module M and B-module N, by setting $b.(m \otimes n) := m \otimes (b.n)$ for all $m \in M, n \in N, b \in B$. Let us show that we have

$$(M \otimes_A B) \otimes_B N \simeq M \otimes_A N$$

as B-modules. For this, let us show directly that the B-module $M \otimes_A N$ satisfies the universal property required to be isomorphic to the tensor product (on the ring B) $(M \otimes_A B) \otimes_B N$. We start by defining a B-linear map $\Phi : (M \otimes_A B) \times N \to M \otimes_A N$ which satisfies

$$\Phi(m \otimes_A b, n) = m \otimes_A bn = b.(m \otimes_A n) \tag{2}$$

for all $m \in M, n \in N, b \in B$. For this, we take (for each fixed $n \in N$) for $\Phi(., n)$ the A-linear map $\mathrm{Id}_M \otimes_A (.n)$ from $M \otimes_A B$ to $M \otimes_A N$. By definition, the map Φ is then A-bilinear, and it is in fact B-bilinear via formula (2) and the definition of the B-module structure on $M \otimes_A B$.

If now $f : (M \otimes_A B) \times N \to L$ is a B-bilinear map, there exists a unique B-linear map $\tilde{f}$ which makes the following diagram commutative :

$$\begin{array}{ccc} (M \otimes_A B) \times N & \xrightarrow{f} & L \\ \Big\downarrow{\scriptstyle \Phi} & \nearrow_{\tilde{f}} & \\ M \otimes_A N & & \end{array}$$

In effect, since f is B-bilinear, we have in particular that

$$f(m \otimes_A 1, bn) = b.f(m \otimes_A 1, n) \tag{3}$$

for all $b \in B, m \in M, n \in N$. Then, by the universal property of the tensor product $M \otimes_A N$, there exists a unique A-linear map $\tilde{f} : M \otimes_A N \to L$ such that

$$\tilde{f}(m \otimes_A n) = f(m \otimes_A 1, n)$$

for all $m \in M, n \in N$. We thus see that $\tilde{f}$ is in fact B-linear via formula (3) since

$$\tilde{f}(b.(m \otimes_A n)) = \tilde{f}(m \otimes_A bn) = f(m \otimes_A 1, bn) = b.f(m \otimes_A 1, n) = b.\tilde{f}(m \otimes_A n),$$

and furthermore, $\tilde{f}$ indeed makes the diagram commutative since

$$\tilde{f}(\Phi(m \otimes_A b, n)) = \tilde{f}(m \otimes_A bn) =$$

$$f(m \otimes_A 1, bn) = f(b.(m \otimes_A 1), n) = f(m \otimes_A b, n).$$

We also see immediately that this is the only map that has this property.

Example 2.11 a) Let L be a field and K a subfield of L. For any K-vector space M, we have the L-vector space $M \otimes_K L$. From corollary 2.6, its dimension as an L-vector space is that of M seen as a K-vector space since if (e_i) is a basis of the K-vector space M, then $(e_i \otimes 1)$ is a basis of the L-vector space $M \otimes_K L$ since any element x of $M \otimes_K L$ can be written uniquely as

$$x = \sum_i e_i \otimes l_i = \sum_i l_i.(e_i \otimes 1),$$

with the l_i in L. This corresponds for example to the notion of complexifying an $\mathbf{R}$-vector space.

b) More generally, the same reasoning shows that if M is a free A-module of rank r, then $M \otimes_A B$ is a free B-module of rank r, and if we suppose simply that M is an A-module of finite type, we again get that $M \otimes_A B$ is a B-module of finite type.

c) Let M and N be free A-modules of finite rank. Let $(e_i)_{1 \leq i \leq r}$ and $(f_j)_{1 \leq j \leq s}$ be the respective bases of M and N. Let $f : M \to N$ be an A-linear map represented by the matrix Q in these bases. Then the map

$$f \otimes \mathrm{Id}_B : M \otimes_A B \to N \otimes_A B$$

is B-linear and its matrix is Q (seen as a matrix with coefficients in B) in the bases $(e_i \otimes 1)_{1 \leq i \leq r}$, $(f_j \otimes 1)_{1 \leq j \leq s}$. We can for example apply this to an A-linear map $A^r \to A^s$ to obtain (after tensorizing by B) a B-linear map $B^r \to B^s$ with the same matrix.

d) If M is an A-module and I an ideal of A, then we have the isomorphism $M \otimes_A A/I \simeq M/IM$, where IM designates the submodule of M generated by the im with $i \in I$ and $m \in M$. The proof of this is basically the same as that for the special case $A = \mathbf{Z}$, $I = n\mathbf{Z}$ (example 2.4 (c)).

If B and C are A-algebras, then we can endow $B \otimes_A C$ with an A-algebra structure in the following way. Consider the quadrilinear map

$$g : B \times C \times B \times C \to B \otimes_A C$$

defined by $g(b, c, b', c') = (bb') \otimes (cc')$ for all $b, b' \in B$ and $c, c' \in C$. By the universal property in remark 2.7, this factorizes via an A-linear map

$$\tilde{g} : B \otimes_A C \otimes_A B \otimes_A C \to B \otimes_A C,$$

which makes it possible to define an internal product on $B \otimes_A C$ which in particular satisfies :

$$(b \otimes c).(b' \otimes c') := \tilde{g}(b \otimes c \otimes b' \otimes c') = (bb') \otimes (cc'),$$

which implies immediately that it is associative, commutative, and distributive with respect to addition. Furthermore, this product is compatible with the A-module structure of $B \otimes_A C$; in other words, it makes $B \otimes_A C$ an A-algebra.

Definition 2.12 The algebra $B \otimes_A C$ is the A-algebra which is the *tensor product of the A-algebras B and C*. It comes with [7] the A-algebra homomorphisms $u_B : B \to B \otimes_A C$ and $u_C : C \to B \otimes_A C$ defined respectively by $b \mapsto b \otimes 1$ and $c \mapsto 1 \otimes c$.

The A-algebra $B \otimes_A C$ has the following universal property :

Proposition 2.13 *For any A-algebra D and homomorphisms of A-algebras $f_B : B \to D$ and $f_C : C \to D$, there exists a unique homomorphism of A-algebras $f : B \otimes_A C \to D$ such that $f_B = f \circ u_B$ and $f_C = f \circ u_C$.*

Proof: We apply the universal property of $B \otimes_A C$ to the A-bilinear map $\varphi : B \times C \to D$ defined by

$$\varphi(b, c) = f_B(b) f_C(c); \quad b \in B, c \in C.$$

This gives us an A-linear map $f : B \otimes_A C \to D$ satisfying

$$f(b \otimes c) = f_B(b) f_C(c) \tag{4}$$

for all $b \in B$, $c \in C$, from which $f(b \otimes 1) = f_B(b)$ and $f(1 \otimes c) = f_C(c)$. From (4) it also follows that f is a ring homomorphism.

□

7. Note that these homomorphisms have no analogs when B and C are just A-modules.

Example 2.14 Let $F_1, \ldots, F_s$ be polynomials from $A[X_1, \ldots, X_r]$. Take $B = A[X_1, \ldots, X_r]/(F_1, \ldots, F_s)$. Proposition 2.13 then gives that for any A-algebra C :

$$B \otimes_A C \simeq C[X_1, \ldots, X_r]/(F_1, \ldots, F_s).$$

In particular, we have

$$A[X_1, \ldots, X_r] \otimes_A C \simeq C[X_1, \ldots, X_r].$$

For example,

$$A[X_1, \ldots, X_r] \otimes_A A[Y_1, \ldots, Y_s] \simeq A[X_1, \ldots, X_r, Y_1, \ldots, Y_s].$$

2.4. Tensor products and exact sequences

An exact sequence of A-modules does not necessarily remain one when tensorizing by an A-module.

Example 2.15 Consider the one-to-one map f from $\mathbf{Z}$ to $\mathbf{Q}$ (both seen as $\mathbf{Z}$-modules). The $\mathbf{Z}$-linear map

$$\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \to \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z}$$

obtained after tensorizing by the identity of $\mathbf{Z}/n\mathbf{Z}$ gives (cf. example 2.4 (c)) the zero map $\mathbf{Z}/n\mathbf{Z} \to 0$, which is not one-to-one.

It is therefore unrealistic to expect that we will conserve the one-to-one property when tensorizing by any given A-module. [8] Nevertheless, we do have the following result :

Theorem 2.16 *Let*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$$

be an exact sequence of A-modules, and M an A-module. Then the sequence

$$N' \otimes_A M \xrightarrow{f_M} N \otimes_A M \xrightarrow{g_M} N'' \otimes_A M \to 0$$

(obtained by tensorizing the arrows f and g by the identity homomorphism $M \to M$) remains exact.

8. Well-behaved A-modules in this respect are called *flat*. For example, it can be shown that if A is a principal ideal domain, the flat A-modules are those that are torsion-free ; see tutorials.

Proof: Since $N'' \otimes_A M$ is generated by the $x'' \otimes y$ with $x'' \in N'', y \in M$, the onto property of g_M comes directly from that of g and the formula : $g_M(x \otimes y) = g(x) \otimes y$ for all $x \in N, y \in M$. Similarly, the fact that $g \circ f = 0$ immediately implies that $g_M \circ f_M = 0$ since $g_M(f_M(x' \otimes y)) = g(f(x')) \otimes y$ for all $x' \in N', y \in M$. Thus, g_M factorizes through an onto map

$$\tilde{g}_M : (N \otimes_A M)/f_M(N' \otimes_A M) \to N'' \otimes_A M.$$

It now remains to show that $\tilde{g}_M$ is one-to-one.

For any $x'' \in N''$, denote $u(x'') \in N/f(N')$ its antecedent by the isomorphism $N/f(N') \to N''$ induced by g. We therefore have a bilinear map

$$N'' \times M \to (N \otimes_A M)/f_M(N' \otimes_A M)$$

which sends (x'', y) onto the class of $u(x'') \otimes y$ (which is well-defined modulo $f_M(N' \otimes_A M)$ since $u(x'')$ is defined modulo $f(N')$). By the universal property of the tensor product, this map factorizes through an A-linear map

$$\theta : N'' \otimes_A M \to (N \otimes_A M)/f_M(N' \otimes_A M).$$

Note that if $x \in N$, we have $u(g(x)) = x$ in $N/f(N')$ since x is an antecedent of $g(x)$ by g. By construction, we have therefore that for any $x \in N, y \in M$ (and noting $\bar{z}$ the class in $(N \otimes_A M)/f_M(N' \otimes_A M)$ of an element z of $N \otimes_A M$) :

$$(\theta \circ \tilde{g}_M)(\overline{x \otimes y}) = \theta(g(x) \otimes y) = u(g(x)) \otimes y = \overline{x \otimes y},$$

which shows that $\theta \circ \tilde{g}_M$ is the identity of $N \otimes_A M$. In particular, $\tilde{g}_M$ is indeed one-to-one.

□

Example 2.17 a) If $f : A^r \to A^s$ is an onto A-linear map, then for any A-algebra B, the A-homomorphism $B^r \to B^s$ induced by tensorizing by B is onto. By taking $B = A/I$, where I is a maximal ideal, we end up back with the first proof of theorem 1.15.

b) All free A-modules are flat. In effect, if $N' \to N$ is a one-to-one A-linear map, the induced A-homomorphism $N' \otimes_A M \to N \otimes_A M$ remains one-to-one thanks to corollary 2.6. In particular, if K is a field, any module (= vector space) on K is flat.

3. Modules over principal ideal domains

3.1. Main theorems

In this section, A designates a principal ideal domain. The first result considerably refines theorem 1.19 in this setting.

Theorem 3.1 *Let A be a principal ideal domain. Then any submodule N of A^n is free and of finite rank $m \leq n$.*

Remark 3.2 Since A is Noetherian, we already know that N is of finite type. If we knew that N was free, the fact that its rank would be at most n would follow from remark 1.18, so it is indeed the freedom of N that is the difficulty here, and fails when A is not a PID.

Proof: We proceed by induction on n. For $n = 1$, it is the definition of a principal ideal domain. Suppose therefore that the result is true for all positive integers $< n$. Let N be a submodule of A^n, and set $M_1 = Ae_2 \oplus \ldots \oplus Ae_n$, where $(e_1, \ldots, e_n)$ is the canonical basis of A^n. In other words, M_1 is the submodule of A^n made up of elements of the form $(0, \ldots, \ldots)$. If $N \subset M_1$, the result is true by induction since M_1 is isomorphic to A^{n-1}. Therefore, we only need to consider $N \not\subset M_1$. By induction, $(N \cap M_1)$ has a basis $(f_2, \ldots, f_m)$ where $m \leq n$. The difficulty is now in finding an element of N to add to this to make it a basis of N.

Let us consider the subset I of A made up of the $b \in A$ for which there exists some $y \in M_1$ with $be_1 + y \in N$. We have also $I = p(N)$ where $p : N \to A$ is the projection $A^n \to A$ onto the first coordinate. Since p is A-linear, we have that I is an ideal of A, and this ideal is not zero since N contains an element which is not in M_1. Since A is a PID, we can write $I = (d)$ with $d \neq 0$ in A. By the definition of I, we therefore have an element $f_1 = de_1 + y_1$ in N with $y_1 \in M_1$. Note that $f_1 \neq 0$, since otherwise d would be zero as $A^n = Ae_1 \oplus M_1$. We now show that $(f_1, \ldots, f_m)$ is a basis of N.

First let us show that $(f_1, \ldots, f_m)$ generates N. If $x \in N$, we have $x = be_1 + y$ with $b \in A$ and $y \in M_1$. But then $b \in I$, from which $b = ad$ with $a \in A$. This gives $x = af_1 + (y - ay_1)$, and thus $(x - af_1)$ is in $N \cap M_1$, which means we can decompose it in the basis $(f_2, \ldots, f_m)$ of $N \cap M_1$. Hence $x = af_1 + x'$ with $x' \in Af_2 + \ldots + Af_m$, which shows that $(f_1, \ldots, f_m)$ generates N.

We now show finally that $(f_1, \ldots, f_m)$ is free. For this it suffices to show that (f_1) is free and that we have $Af_1 \cap (N \cap M_1) = \{0\}$, since $(f_2, \ldots, f_m)$ is already free by hypothesis. The first point is easy to see : decompose f_1 (which is not zero) in the canonical basis of A^n and use the fact that A is

an integral domain. For the second point, if λf_1 is in M_1 with $\lambda \in A$, then $\lambda d e_1 + \lambda y_1 \in M_1$, from which $(\lambda d)e_1 \in M_1$, but by the definition of M_1 and the canonical basis of A^n, this implies that $\lambda d = 0$ and thus $\lambda = 0$ by the fact that A is an integral domain.

□

To go further in the classification of modules over PID, the following more precise result is required. It is probably the most important theorem in this chapter.

Theorem 3.3 ("'adapted basis") *Let A be a principal ideal domain, M a free A-module of rank n and N a submodule of M. Then there exists a basis $(e_1, \ldots, e_n)$ of M and elements $(d_1, \ldots, d_r)$ of A (with $r \leq n$) such that :*

1. *$(d_1 e_1, \ldots, d_r e_r)$ is a basis of N.*
2. *We have the following divisibilities : $d_1 \mid d_2 \mid \ldots \mid d_r$.*

In particular, the d_i are non-zero, and we can replace each d_i by any element of A it is an associate of. Note that we already knew that N was free and of rank $\leq n$ via theorem 3.1.

The proof of this theorem is long and fairly complex. We start with a lemma that initiates an argument by induction on n.

Lemma 3.4 *Suppose that $N \neq \{0\}$. Then there exists a linear map $f_1 : M \to A$ such that*

1. *$f_1(N)$ is maximal (for inclusion) among the $f(N)$ where $f : M \to A$ is linear.*
2. *If we set $f_1(N) = (d_1)$, then there exists $e_1 \in M$ such that $f_1(e_1) = 1$ and $u_1 := d_1 e_1$ is in N.*

Proof: First we fix a basis $(\varepsilon_1, \ldots, \varepsilon_n)$ for M (which has no reason to be well-adapted for N). We then have (for $1 \leq i \leq n$) the linear form $\varepsilon_i^* : M \to A$ which associates with any $x \in M$ its i-th coordinate in this basis. For any linear form $f : M \to A$, $f(N)$ is an ideal of A. The first result then follows from the fact that A is a PID (and thus Noetherian), which also makes it possible to write $f_1(N) = (d_1)$, with $d_1 \neq 0$ since N is not zero, and so one of the linear forms ε_i^* has a non-null restriction to N.

Now suppose that $u_1 \in N$ such that $f_1(u_1) = d_1$. If $f : M \to A$ is a linear form, we set $d = f(u_1)$ and show that d_1 divides d (be careful since we still do not know whether $f_1(N)$ is the largest element of the $f(N)$ with f a linear form on M ; this will be proved in the following lemma). Set $e = (d, d_1)$; by

Bézout's theorem, there exists α and β in A such that $(\alpha f + \beta f_1)(u_1) = e$. This implies that $(\alpha f + \beta f_1)(N) \supset eA \supset d_1 A$, and by the maximality of $f_1(N) = d_1 A$, we have $(\alpha f + \beta f_1)(N) = d_1 A$, from which $dA = eA$, which signifies that e and d_1 are associates, and thus $d_1 \mid d$.

Finally, $f(u_1) \in d_1 A$ for any linear form $f : M \to A$, and this is true in particular for all linear forms ε_i^*. Thus, all of the coordinates of u_1 in the basis $(\varepsilon_1, \ldots, \varepsilon_n)$ are divisible by d_1, which means we can find $e_1 \in M$ such that $u_1 = d_1 e_1$. Then, $f_1(e_1) = 1$ seeing as $f_1(u_1) = d_1 \neq 0$ and A is integral. □

We now move on to the next lemma.

Lemma 3.5 *With the hypotheses and notation from the previous lemma, we have :*

1. $M = Ae_1 \oplus \ker f_1$ *and* $N = Au_1 \oplus (\ker f_1 \cap N)$.
2. *For any linear form* $f : M \to A$, $f(N) \subset d_1 A$.

Proof: 1. Since $f_1(e_1) = 1$, $Ae_1 \cap \ker f_1 = \{0\}$ is clear. Any x in M can be written $x = f_1(x)e_1 + (x - f_1(x)e_1)$ with $(x - f_1(x)e_1) \in \ker f_1$, so $M = Ae_1 \oplus \ker f_1$. The same for any x in N satisfying $f_1(x) = ad_1$ with $a \in A$, from which $x = au_1 + (x - au_1)$ with $(x - au_1) \in (\ker f_1 \cap N)$. Finally, $Au_1 \cap \ker f_1 = \{0\}$ results from $f_1(u_1) = d_1 \neq 0$ and A being integral.

2. Let $f : M \to A$ be linear. Via 1., we define the linear $g : M \to A$ by : $g(x) = f(x)$ if $x \in \ker f_1$, and $g(e_1) = 1$. Then, since $g(u_1) = d_1$, we have $g(N) \supset d_1 A$, and thus $g(N) = d_1 A$ by the maximality of $f_1(N) = d_1 A$. In particular the restriction of f to $(\ker f_1 \cap N)$ has its image contained in $d_1 A$; so does also the restriction of f to N, since N is the sum of $(\ker f_1 \cap N)$ and Au_1, while $f(u_1) = d_1 f(e_1)$ is divisible by d_1.

□

End of the proof of the Theorem : The $n = 0$ and $N = 0$ cases are trivial. For $n = 1$, we can suppose that $M = A$ and the result follows from the definition of a principal ideal domain upon taking $e_1 = 1$ and d_1 a generator of the ideal $N \subset A$ (note that (d_1) is therefore then a basis of N due to A being an integral domain). Suppose the result is true for the positive integers $< n$. We then apply lemma 3.5 and the induction hypothesis to the A-module $\ker f_1$ (which is free due to theorem 3.1, and of rank $n - 1$ by corollary 1.16 and the fact that $M = Ae_1 \oplus \ker f_1$, given that the rank of Ae_1 is 1) and its submodule $(\ker f_1 \cap N)$. We obtain a basis $(e_2, \ldots, e_n)$ of $\ker f_1$, and elements $d_2, \ldots, d_r$ of A with $r \leq n$ and $d_2 \mid \ldots \mid d_r$ such that

$M = Ae_1 \oplus \ldots \oplus Ae_n$ and $N = A(d_1e_1) \oplus \ldots \oplus A(d_re_r)$. Finally, d_1 divides d_2 by applying lemma 3.5 to the "second coordinate" linear form (in the basis $(e_1, \ldots, e_n)$) on M.

□

Be careful not to fall into the usual traps : the theorem does not say that N is a direct summand of M nor that we can complete a basis of N with a basis of M (take for instance $A = \mathbf{Z}$, $M = \mathbf{Z}$, $N = 2\mathbf{Z}$).

Theorem 3.6 *Let M be a module of finite type over a principal ideal domain A. Then there exist non-null and non-invertible $d_1, \ldots, d_s$ in A for which M is isomorphic to*

$$A^m \oplus \bigoplus_{i=1}^{s} (A/d_iA)$$

with $m \in \mathbf{N}$ and $d_1 \mid d_2 \mid \ldots \mid d_s$.

Proof: Since M is of finite type, it is generated by n elements, which means that there is an exact sequence of A-modules

$$0 \to N \to A^n \xrightarrow{p} M \to 0$$

(this simply means that M is isomorphic to a quotient of A^n).

We apply Theorem 3.3 to the submodule N of the free A-module A^n. We obtain

$$A^n = \bigoplus_{i=1}^{n} Aei$$

$$N = \bigoplus_{i=1}^{r} A(d_ie_i).$$

Now let z_i be the image of e_i in M (by p). Then $M = \bigoplus_{i=1}^{n} Az_i$. In effect, the z_i generate M (by the onto nature of p), and also if $\sum_{i=1}^{n} \lambda_i z_i = 0$ where $\lambda_i \in A$, then $\sum_{i=1}^{n} \lambda_i e_i \in N$ and so each λ_i is a multiple of d_i for $1 \leq i \leq r$ (resp. is equal to zero for $r < i \leq n$) since $(d_ie_i)_{1 \leq i \leq r}$ is a basis of N; hence each $\lambda_i e_i$ is in N, i.e., $\lambda_i z_i = 0$.

Now, each $A.z_i$ is isomorphic to (A/d_iA) for $1 \leq i \leq r$ and to A for $r < i \leq n$, since the kernel of the onto map $\lambda_i \mapsto \lambda z_i$ from A to $A.z_i$ is d_iA for $1 \leq i \leq r$ (resp. 0 for $r < i \leq n$), still because $(d_ie_i)_{1 \leq i \leq r}$ is a basis of the kernel N of p. We obtain $M \simeq A^{n-r} \oplus \bigoplus_{i=1}^{r} (A/d_iA)$, but for invertible d_i we have $A/d_iA = 0$, so we can just keep the non-invertible d_i's.

□

Definition 3.7 Let M be a module over a commutative ring A. Remember that M is said to be *torsion-free* if $ax = 0$ (with $a \in A$, $x \in M$) implies either $a = 0$ or $x = 0$. We say that M is a *torsion module* if for each x in M, there exists a non-null a in A such that $ax = 0$.

Note that "torsion-free" is not in general the opposite of "torsion". For example, $\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ is neither when seen as a $\mathbf{Z}$-module. Clearly, a free module over an integral domain is torsion-free. We can now prove the reverse is also true for PID :

Corollary 3.8 *Let M be a module of finite type over a principal ideal domain A. Then M is free if and only if it is torsion-free.*

Proof: This results immediately from theorem 3.6, since the condition that M is torsion-free implies that $s = 0$ (for non-invertible d, A/dA is non-null, and all elements of A/dA are killed by d.

□

This corollary is quite specific to principal ideal domains. If A is a Noetherian integral domain, any ideal I of A is a torsion-free A-module of finite type, but from remark 1.18, I is not free if it is not principal. Furthermore, the finite type hypothesis is important since for example, $\mathbf{Q}$ is a torsion-free $\mathbf{Z}$-module and we have already seen that it is not free (example 1.14).

Remark 3.9 If A is a commutative ring, an A-module (of finite type) M is said to be *projective* if it is a *direct factor* of a free module, i.e., if there exists an A-module N such that $M \oplus N$ is free. We have therefore in particular that a projective module (of finite type) over a principal ideal domain is always free. [9] It is also true for any *local* ring, i.e., those with only one maximal ideal, and for $K[X_1, \ldots, X_n]$ when K is a field (the Quillen-Suslin theorem, 1976, formerly known as Serre's conjecture).

3.2. p-primary decompositions

To finish up the classification of modules of finite type over a principal ideal domain A, we require uniqueness results. Surprisingly, it is not easy to directly prove such results using theorem 3.6 ; it is much more usual to work with what are known as p-primary components, which are also useful in their own right.

9. The finite hypothesis is not indispensable, but the proof is much more complex without it ; see the article by Kaplansky in *Ann. Math.* **68** (1958).

Definition 3.10 Let p be an irreducible element in A. We say that an A-module is *p-primary* if it is isomorphic to a module of the form $\bigoplus_{i=1}^{s}(A/p^{v_i}A)$ with $v_i \in \mathbf{N}^*$ for all $i \in [1,s]$.

In particular, a p-primary A-module is a torsion module of finite type (with the notation below, any element x of a p-primary A-module is killed by $p^{\max(v_i)}$).

For any non-zero d in the principal ideal domain A, we as usual denote by $v_p(d)$ the largest power of the irreducible element p that divides d.

Proposition 3.11 *1. Let $d = u\prod_{p\in S} p^{\alpha_p}$ be a decomposition of d into a product over irreducible elements (where S is a finite set of irreducible elements that are not associates pairwise, and $u \in A^*$). Then*

$$A/dA \simeq \bigoplus_{p\in S}(A/p^{\alpha_p}A).$$

2. Let $M = \bigoplus_{i=1}^{s}(A/d_iA)$ with $d_1 \mid d_2 \mid \ldots \mid d_s$. Then for any irreducible element p of A and any integer $k \geq v_p(d_s)$, we have

$$M/p^kM \simeq \bigoplus_{i=1}^{s}(A/p^{v_p(d_i)}A).$$

3. Let M be a torsion A-module of finite type. Let $\mathcal{P}$ be a system of irreducible representatives of A. Then

$$M = \bigoplus_{p\in\mathcal{P}} M_p,$$

where M_p is a p-primary module for which $M_p = M/p^kM$ for large enough k, and almost all of the M_p are equal to zero. We say that the M_p are the p-primary components of M.

Proof: 1. It is simply the Chinese remainder theorem when $A = \mathbf{Z}$. By reasoning by induction on the cardinality of S, it suffices to show that $A/(d_1d_2)A \simeq A/d_1A \times A/d_2A$ when d_1 and d_2 are elements of A that are prime with each other. The map that links $a \in A$ with (a_1, a_2), where a_i is the class of a in A/d_iA for $i = 1, 2$, clearly has the kernel $(d_1d_2)A$ since $(d_1, d_2) = 1$. It is onto via Bézout's theorem : let $b, c \in A$; then there exists $\alpha, \beta \in A$ such that $\alpha d_1 + \beta d_2 = 1$, and so $x := \beta b d_2 + \alpha c d_1$ is in the same class as b in A/d_1A and c is in A/d_2A.

2. As p is fixed, we remark that if q is an irreducible element of A that is not an associate of p, then multiplication by p is onto in A/q^mA for all $m \in \mathbf{N}$, since by writing out Bézout's identity for q^m and p, we see that the class of p is an invertible element of A/q^mA. We deduce that if Q is a q-primary module, then since it is a direct sum of modules of the form A/q^mA, multiplication by p^n is onto in Q for all $n \in \mathbf{N}$, i.e., $Q/p^nQ = 0$.

According to 1., M is isomorphic to $\bigoplus_{q \in S} M_q$ with M_q a q-primary module (since S is a finite sum of irreducible elements that pairwise are not associates, obtained by decomposing all of the d_i). Hence $M/p^kM = M_p/p^kM_p$ since for $q \neq p$ in S, we have $M_q/p^kM_q = 0$. Since from 1. we have that $M_p = \bigoplus_{i=1}^{s}(A/p^{v_p(d_i)}A)$, we obtain $M/p^kM = M_p$ as soon as k is larger than all of the $v_p(d_i)$, i.e., for $k \geq v_p(d_s)$.

3. The structure theorem 3.6 means we can write $M \simeq \bigoplus_{i=1}^{s}(A/d_iA)$. According to 1., we then have

$$M = \bigoplus_{p \in \mathcal{P}} M_p,$$

with M_p a p-primary module, and from 2., we therefore have $M/p^kM = M_p/p^kM = M_p$ for large enough k. Furthermore, $M_p = 0$ when p divides none of the d_i, which is true for almost all $p \in \mathcal{P}$.

□

From this we can deduce the wished-for uniqueness result :

Theorem 3.12 *Let M be a module of finite type over a principal ideal domain A, and write it as*

$$M \simeq A^m \oplus \bigoplus_{i=1}^{s}(A/d_iA)$$

with non-null and non-invertible $d_1, \ldots, d_s$ such that $d_1 \mid \ldots \mid d_s$. Then m, s, and the d_i up to association depend only on M.

In other words, if we have another decomposition :

$$M \simeq A^{m'} \oplus \bigoplus_{i=1}^{s'}(A/d'_iA),$$

then $m = m'$, $s = s'$, and d'_i is an associate of d_i for all i.

Proof: Let M_{tors} be the *torsion submodule* of M, i.e., the set of x in M for which there exists $a \neq 0$ in A for which $ax = 0$. Then $M_{\text{tors}} \simeq \bigoplus_{i=1}^{s}(A/d_iA)$ and $M/M_{\text{tors}} \simeq A^m$. By the rank invariance of free modules of finite type, m depends only on M so we can assume that M is a torsion module.

It therefore suffices to show that for any irreducible p, the sequence of $v_p(d_i)$ is uniquely defined. Since a torsion A-module M is the direct sum of its p-primary components $M_p = \bigoplus_{i=1}^{s}(A/p^{v_p(d_i)}A)$, which are characterized by $M_p = M/p^kM$ for large enough k, we find ourselves in the setting where M is p-primary.

Suppose therefore that $M = \bigoplus_{i=1}^{s}(A/p^{\alpha_i}A)$, where (α_i) is an increasing sequence of strictly positive integers. Since A is a PID and p irreducible, A/pA is a field and furthermore, for any $k \in \mathbf{N}$, the A-module with p-torsion $p^kM/p^{k+1}M$ is canonically equipped with an A/pA-vector space structure (like in example 1.4 (c)). We see that if $M_i := (A/p^{\alpha_i}A)$, we have for all integers k : $p^kM_i/p^{k+1}M_i = 0$ if $k \geq \alpha_i$ (since then $p^kM_i \subset p^{\alpha_i}M_i = 0$) ; but if $k < \alpha_i$, then $p^kM \supset p^{k+1}M \supset p^{\alpha_i}A$, from which

$$p^kM_i/p^{k+1}M_i = (p^kA/p^{\alpha_i}A)/(p^{k+1}A/p^{\alpha_i}A) \simeq p^kA/p^{k+1}A.$$

However, A/p is isomorphic to $p^kA/p^{k+1}A$ via $\bar{a} \mapsto p^k\bar{a}$, so finally we obtain that $p^kM_i/p^{k+1}M_i \simeq A/pA$ if $k < \alpha_i$. In particular, for any $k \in \mathbf{N}$, the number of $\alpha_i > k$ is none other than the *dimension of the A/pA-vector space* $p^kM/p^{k+1}M \simeq \bigoplus_{i=1}^{s} p^kM_i/p^{k+1}M_i$, so $\sum_{\alpha_i>k} 1$. Hence this number depends only on M, and the same is also true for the increasing sequence of integers (α_i).

□

3.3. Applications

We now present three important examples of the application of the theorems we have just seen.

Abelian groups of finite type.

In the $A = \mathbf{Z}$ case, the general structure theorem (theorems 3.6 and 3.12) gives :

Theorem 3.13 *Let M be an abelian group of finite type (i.e., generated by a finite number of elements). Then M is isomorphic to*

$$\mathbf{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbf{Z}/d_i\mathbf{Z},$$

where $r \in \mathbf{N}$, and the d_i are integers ≥ 2 satisfying $d_1 \mid \ldots \mid d_s$. Furthermore, r and the d_i are entirely determined by M.

Of course, M is finite if and only if $r = 0$. If it is, we obtain the p-Sylow M_p of M via the p-primary decomposition.

Equivalence of matrices with coefficients in a principal ideal domain.

Let A be a commutative ring. We note $\mathrm{GL}_n(A)$ the group of invertible elements of the (non-commutative if $n \geq 2$) ring $M_n(A)$. According to the comatrix identity, this is simply the matrices of $M_n(A)$ with invertible determinants in A, where the inverse of such a matrix M is given by $M^{-1} = (\det M)^{-1}.\widetilde{M}$ (in the other direction : if there exists a matrix $N \in M_n(A)$ with $MN = I_n$, then $(\det M).(\det N) = 1$ and so $\det M$ is invertible).

Definition 3.14 Let p and q be positive integers. We say that the matrices B and C of $M_{p,q}(A)$ are *equivalent* if there exists $U \in \mathrm{GL}_p(A)$ and $V \in \mathrm{GL}_q(A)$ such that $C = UBV$. This is the same as saying that there exists respective bases $\mathcal{B}$ and $\mathcal{B}'$ of A^q and A^p such that if u is the linear map represented by B in the canonical bases of A^q and A^p, we have : $\mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(u) = C$.

When A is a field, this falls back to the classical definition (which we should be careful not to mix up with the more subtle relation of similarity when $p = q$). The following theorem characterizes the equivalence classes under this notion of equivalence when A is a PID.

Theorem 3.15 *Let A be a principal ideal domain. Then :*

1. *Any matrix B of $M_{p,q}(A)$ is equivalent to a block matrix of the form*

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

   where $D = \mathrm{Diag}(d_1, \ldots, d_r)$, $r \leq \min(p, q)$, and $d_1, \ldots, d_r$ are non-null elements of A satisfying $d_1 \mid \ldots \mid d_r$.

2. *The matrices $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix}$ with $D = \mathrm{Diag}(d_1, \ldots, d_r)$, $D' = \mathrm{Diag}(d'_1, \ldots, d'_{r'})$ in the form described above are equivalent if and only if : $r = r'$ and for all i, d_i and d'_i are associates. In other words, the sequence $(d_1, \ldots, d_r)$ in 1. only depends (up to association) on the equivalence class of B.*

The $d_1, \ldots, d_r$ are called the *invariant factors* of B, and sometimes the quotients $d_2/d_1, \ldots, d_r/d_{r-1}$ are known as their *elementary divisors*. Note that r is none other than the *rank* of B seen as a matrix of $M_{p,q}(K)$, where $K := \operatorname{Frac} A$.

Proof: We first prove 1. Let $u : A^q \to A^p$ be the map defined by B in the canonical bases. We must find respective bases $\mathcal{B}$ and $\mathcal{B}'$ of A^q and A^p so that the matrix of u in these bases has the required form. Let us apply Theorem 3.3 to the submodule $\operatorname{Im} u$ of the free module A^p of finite type. We obtain a basis $(e_1, \ldots, e_p)$ of A^p and a sequence $(d_1, \ldots, d_r)$ of elements of $A \setminus \{0\}$, with $d_1 \mid \ldots \mid d_r$, such that $(d_1 e_1, \ldots, d_r e_r)$ is a basis of $\operatorname{Im} u$. We then choose $\varepsilon_1, \ldots, \varepsilon_r$ in A^q such that $u(\varepsilon_i) = d_i e_i$ for $i = 1, \ldots, r$. Then $(u(\varepsilon_1), \ldots, u(\varepsilon_r))$ is free, and therefore $(\varepsilon_1, \ldots, \varepsilon_r)$ is free. We also have that

$$A^q = \ker u \oplus \bigoplus_{i=1}^{r} A\varepsilon_i$$

since $(u(\varepsilon_1), \ldots, u(\varepsilon_r))$ is free (which gives $\ker u \cap \bigoplus_{i=1}^{r} A\varepsilon_i = \{0\}$), and any element x in A^q satisfies : $u(x)$ is a linear combination of the $d_i e_i = u(\varepsilon_i)$, so x can be written as the sum of an element in $\ker u$ and a linear combination of the ε_i. We can then (thanks to theorems 3.1 and 1.16) take a basis $(\varepsilon_{r+1}, \ldots, \varepsilon_q)$ of $\ker u$, and we obtain a basis $\mathcal{B} = (\varepsilon_1, \ldots, \varepsilon_q)$ of A^q. It then suffices to take $\mathcal{B}' = (e_1, \ldots, e_p)$ to obtain the required form. Note that if B is the matrix of a one-to-one map from A^q to A^p, the d_i associated with it are the same as those given by Theorem 3.3 for the submodule $\operatorname{Im} u \simeq A^q$ of A^p.

To prove 2., the major step consists of proving the following lemma :

Lemma 3.16 *For any matrix B in $M_{p.q}(A)$ and any positive integer s (less than or equal to $\min(p, q)$ or to rank(B)), we denote $m_s(B)$ the smallest common divisor of the minors of length s of B. Then :*

a) If B and C are equivalent, $m_s(B)$ and $m_s(C)$ are associates.

b) If $B = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ with $D = \operatorname{Diag}(d_1, \ldots, d_r)$ and $d_1 \mid \ldots \mid d_r$, then :

$$m_s(B) = d_1 ... d_s$$

for all $s \in \{1, \ldots, r\}$.

Proof: a) It suffices to notice that if $U \in M_p(A)$, then the rows of UB are linear combinations of the rows of B and if $V \in M_q(A)$, the columns of BV are linear combinations of the columns of B. From this we deduce (with the help of theorem 1.11 (b)) that any minor of size s of UBV is a linear combination with coefficients in A of minors of size s of B, which implies that $m_s(B)$ divides $m_s(UBV)$. By symmetry, $m_s(B)$ and $m_s(C)$ are associates if B and C are equivalent.

b) When B has this particular form, any minor m of size s is the sum of products $e_1...e_s$, where the e_i are pairwise distinct in the set $\{d_1, \ldots, d_r\}$. From the divisibility property of the d_i, $e_1...e_s$ is divisible by $d_1...d_s$. Since also the principal minor of order s of B is $d_1...d_s$, we obtain the desired result.

□

End of the proof of theorem 3.15 (2). We already have $r = r'$ by the rank invariance of equivalent matrices. From lemma 3.16 (a), we have $m_s(D) = m_s(D')$ (up to association), and then also with part (b) of the same lemma we have

$$d_1...d_s = d'_1...d'_s$$

for all s with $1 \leq s \leq r$. By induction on s, we then see that $d_s = d'_s$ (up to association) for all s in $[1, r]$.

□

Remark: It is much more difficult to determine the similarity classes of matrices in $M_n(A)$. In fact, we only know how to do so when A is a field, since as we will now see, this is linked to the classification of modules over the ring $A[X]$—which is not a PID if A is not a field.

The reduction of endomorphisms of a finite dimensional K-vector space.

Let K be a field, E a K-vector space of (finite) dimension n, and u an endomorphism of E. We want to find a basis in which the matrix of u has a pleasant form, and more precisely : determine the similarity classes in $M_n(K)$. This is the subject of the main theorem in this section. Let us begin by recalling some notation.

Definition 3.17 Let $P = X^d + \sum_{i=0}^{d-1} a_i X^i$ be a monic polynomial whose

coefficients are from K. We denote $C(P)$ the matrix :

$$\begin{pmatrix} 0 & ... & ... & ... & -a_0 \\ 1 & 0 & ... & ... & -a_1 \\ 0 & 1 & 0 & ... & -a_2 \\ ... & ... & ... & ... & ... \\ 0 & ... & ... & 1 & -a_{d-1} \end{pmatrix}$$

which is known as the *companion matrix* associated with P.

If u is the endomorphism associated with $C(P)$ in a basis $\mathcal{B}$ and x is the first vector of this basis, then $\mathcal{B} = (x, u(x), \ldots, u^{d-1}(x))$. In particular, a polynomial Q such that $Q(u) = 0$ is of degree at least d; since $P(u) = 0$ (seeing as $u^d(x) = -\sum_{k=0}^{d-1} a_k u^k(x)$), the minimal polynomial of $C(P)$ is P. From the Cayley-Hamilton theorem, this is also its characteristic polynomial (this can also be checked directly) Such an endomorphism u is said to be *cyclic*.

Theorem 3.18 *1. For any endomorphism u of a finite dimensional K-vector space E, there exists a basis of E in which the matrix of u is block diagonal of the form ("Frobenius normal form") :*

$$\begin{pmatrix} C(P_1) & & & \\ & C(P_2) & & \\ & ... & & \\ & & & C(P_s) \end{pmatrix}$$

where the P_i are monic polynomials from $K[X]$ of degree at least 1, satisfying : $P_1 \mid P_2 \mid \ldots \mid P_s$.

2. The P_i are entirely determined by u ; we call them the invariants of tensors of u. Two matrices in $M_n(K)$ are similar if and only if they have the same invariants of tensors. [10]

3. Let $B \in M_n(K)$ and let $C := XI_n - B$ be the characteristic matrix of B (it is a matrix of rank n in $M_n(K[X])$). Then the sequence of invariant factors of C is $(1, \ldots, 1, P_1, \ldots, P_s)$, where $P_1, \ldots, P_s$ are the invariants of tensors of B. In particular, these invariants are given by the formula :

$$P_1 ... P_h = m_{h+n-s}(C)$$

for $h = 1, \ldots, s$, where $m_i(C)$ designates the greatest common divisor of the minors of size i of C in $K[X]$. [11]

10. Of course, the invariants of tensors of a matrix are by definition the invariants of the endomorphism it represents in the canonical basis.

11. Beware of the shift in indices due to the invertible invariant factors of C.

Note that the minimal polynomial of u is P_s (be careful : this is the "largest" P_i, not the smallest !) and the characteristic polynomial of u is $P_1...P_s$. We can iteratively calculate the P_i starting with P_s, using the formulas $P_s = m_n(C)/m_{n-1}(C)$, $P_{s-1} = m_{n-1}(C)/m_{n-2}(C)$, etc.

The proof of this theorem is based on the theory of modules over the PID $A := K[X]$. More precisely, we define an A-module structure M over the K-vector space E via : $P.v := P(u)(v)$ for $P \in K[X]$ and $v \in E$. We immediately note that this is a torsion A-module since if $\pi(u) = 0$ (ex. π is the characteristic polynomial of u) we have $\pi.v = 0$ for all v in M. Also, it is generated by any basis of the K-vector space E since A contains all of the constants of K. To connect the invariants linked to M with those of the characteristic matrix C, we need the following lemma :

Lemma 3.19 *Let $(\varepsilon_1, \ldots, \varepsilon_n)$ be a fixed basis of E, $B = (a_{ij})$ the matrix of u in this basis, and $(e_1, \ldots, e_n)$ the canonical basis of the A-module $K[X]^n$. Let φ be the (onto) A-linear map from $K[X]^n$ to M that sends e_i to ε_i for all $i = 1, \ldots, n$. Set $f_j = Xe_j - \sum_{i=1}^n a_{ij}e_i$ for $j = 1, \ldots, n$. Then $(f_1, \ldots, f_n)$ is a basis of the A-module* $\ker\varphi$.

Proof: We already have $f_j \in \ker\varphi$ seeing as $\varphi(f_j) = X.\varepsilon_j - \sum_{i=1}^n a_{ij}\varepsilon_i = u(\varepsilon_j) - \sum_{i=1}^n a_{ij}\varepsilon_i = 0$ by the definition of the matrix B.

We now show that $(f_1, \ldots, f_n)$ generates the A-module $\ker\varphi$. Any element $\mathbf{Y}$ of $K[X]^n$ can be written $\mathbf{Y} = \sum_{j=1}^n \lambda_j e_j$ with $\lambda_j \in K[X]$. We then see that we can rewrite $\mathbf{Y}$ in the form $\mathbf{Y} = \sum_{j=1}^n \mu_j f_j + \sum_{j=1}^n b_j e_j$ with $\mu_j \in K[X]$ and b_j a constant in K : in effect, by K-linearity, it suffices to see this when $\mathbf{Y} = X^k e_j$ with $k \in \mathbf{N}$; in this case, this can be deduced by induction on k with the formula $f_j = Xe_j - \sum_{i=1}^n a_{ij}e_i$

If now $\mathbf{Y}$ is also in $\ker\varphi$, then $\sum_{j=1}^n b_j e_j$ is too, and the following holds : $\sum_{j=1}^n b_j\varepsilon_j = 0$, and finally all of the b_j are equal to zero since $(\varepsilon_1, \ldots, \varepsilon_n)$ is a basis of the K-vector space E.

Let us now subsequently show that the family $(f_1, \ldots, f_n)$ is free in the A-module $\ker\varphi$. If $\sum_{j=1}^n \lambda_j f_j = 0$ with $\lambda_j \in A$, then

$$\sum_{j=1}^n (\lambda_j X)e_j = \sum_{1\le i,j\le n} \lambda_j a_{ij} e_i = \sum_{j=1}^n (\sum_{i=1}^n a_{ji}\lambda_i)e_j,$$

and since $(e_1, \ldots, e_n)$ is a basis for the A-module $K[X]^n$, we obtain for all $j = 1, \ldots, n$: $X\lambda_j = \sum_{i=1}^n a_{ji}\lambda_i$, which implies that all of the λ_j are equal to zero, since otherwise there would be a contradiction when taking j such that λ_j has maximal degree (say d) within $\lambda_1, \ldots, \lambda_n$, since then $X\lambda_j$ would be of degree $d+1$ and $\sum_{i=1}^n a_{ji}\lambda_i$ of degree at most d.

□

Proof of theorem 3.18 : With the notation from the previous lemma, let ψ be the inclusion map from $\ker\varphi$ to $K[X]^n$. Its matrix in the bases $(f_1,\dots,f_n)$ and $(e_1,\dots,e_n)$ is by definition $C = XI_n - B$, whose determinant is non-zero (it is indeed the characteristic polynomial of u). The sequence of its invariant factors is thus of the form $(1,\dots,1,P_1,\dots,P_s)$ with $P_1 \mid \dots \mid P_s$, and we can choose the P_i to be monic of degree at least 1. As we saw in the proof of the first point of theorem 3.15 (on the equivalence of matrices with coefficients in A), the A-module $M \simeq (K[X]^n/\ker\varphi)$ is therefore isomorphic to $\bigoplus_{i=1}^s (A/P_i.A)$, and $M = \bigoplus_{i=1}^s A.z_i$, where z_i is the image in M (via φ) of the i-th vector of an adapted basis for the inclusion ψ. The ideal generated by P_i is then the annihilator of z_i in the A-module M, i.e.,

$$(P_i) = \{P \in A, P.z_i = 0\}.$$

Let E_i be the submodule $A.z_i$ of M. Then in particular E_i is a vector subspace of E and is stable by u; more precisely, it is the image of the k-linear map $P \mapsto P.z_i = P(u)(z_i)$ from A to M. Thus E_i is isomorphic to $A/P_i.A$, which is a K-vector space of dimension $d_i := \deg P_i$ (a basis is made up of classes of $(1, X, \dots, X^{d_i-1})$, via Euclidean division by P_i). Now the family $\mathcal{B}_i := (z_i, u(z_i), \dots, u^{d_i-1}(z_i))$ is a basis of the K-vector space E_i (of cardinality d_i and free, still because the annihilator of z_i is $P_i.A$). The matrix of the restriction of u to E_i in $\mathcal{B}_i$ is $C(P_i)$ by the definition of $C(P_i)$ and since $(P_i(u))(z_i) = 0$. Since $E = \bigoplus_{i=1}^s E_i$ (as an A-module or a K-vector space), we deduce the first point by concatenating the bases $\mathcal{B}_i$.

If now u has a matrix in the above form with polynomials $(Q_1,\dots,Q_{s'})$ in another basis, then the A-module M is the direct sum of the submodules N_i, where each N_i corresponds to an endomorphism $v = u_{|N_i}$ whose matrix in a certain basis $(y, u(y), \dots, u^{m-1}(y))$ is $C(Q_i)$, where $m = \deg Q_i$. As above, the A-module N_i is isomorphic to $(A/Q_i.A)$ via the A-linear map $\psi : P \mapsto P.y = P(u)(y)$ from A to N_i, since the kernel of ψ is $Q_i.A$ via the fact that Q_i is the minimal polynomial of $C(Q_i)$, and thus of v. Finally the A-module M is isomorphic to $\bigoplus_i (A/Q_i.A)$. The fact that the P_i are entirely determined by u then comes from the uniqueness theorem 3.12. The second point is thus proved.

To conclude, we saw that $(1,\dots,1,P_1,\dots,P_s)$ was the sequence of invariant factors of C. The end of the third point therefore results from lemma 3.16.

□

Remark 3.20 a) In the special case where the characteristic polynomial of

u is split, we end up with the Jordan normal form as a decomposition in p-primary components of M, seeing as the irreducible factors of each P_i are of the form $(X-\lambda)$ with $\lambda \in K$. In effect, the p-primary component associated with λ corresponds to a matrix of the form $\lambda I + N$ with nilpotent N ; however since a companion matrix of the form $C(X^k)$ is none other than a Jordan matrix [12]

b) Theorem 3.18 for example allows us to see immediately that if two matrices in $M_n(K)$ are similar on a field extension of K, they are already similar on K, a result that is not at all obvious (in particular if K is finite). Other applications will be seen in the tutorials.

Références

[1] R. Godement : Cours d'algèbre. Hermann, Paris, 1987.

[2] N. Jacobson : *Basic Algebra*. W. H. Freeman and Company, New York, 1985.

[3] Q. Liu : *Algebraic geometry and arithmetic curves*. Oxford Graduate Texts in Mathematics, **6**, Oxford Science Publications, Oxford University Press, Oxford, 2002.

12. Up to transposition, but it suffices to write the basis in the other direction to get the classical Jordan form.