COURS DE MAÎTRISE 2003-2004
INTRODUCTION À L'ALGÈBRE COMMUTATIVE ET HOMOLOGIQUE

par

Yves Laszlo

On donne dans un premier temps des bases de la théorie des anneaux commutatifs (anneaux et modules noethériens, factoriels, modules sur les anneaux principaux, produit tensoriel, algèbre extérieure...). Dans un second temps, on aborde l'algèbre homologique (foncteurs dérivés standards Tor et Ext) avec en vue le théorème des syzygies de Hilbert ([**2**]) qui donne des renseignements très précis sur les modules sur les anneaux de polynômes. Une bonne référence est par exemple le livre de Lang [**3**].

On ne suppose aucune connaissance particulière en algèbre, en dehors de l'algèbre linéaire de premier cycle (qu'on éclairera d'ailleurs au jour de la théorie des modules sur les anneaux principaux). On espère malgré tout que le lecteur a déjà rencontré et manipulé des anneaux et des idéaux, même si on revoit ces notions. Sauf mention expresse du contraire, les anneaux considérés sont commutatifs, munis d'une unité notée 1 (pour la multiplication) et les morphismes d'anneaux sont les applications respectant sommes, produits et unités. Rappelons qu'une famille $a_i, i \in I$ d'un ensemble muni d'un 0 est presque nulle si tous ses termes sauf un nombre fini sont nuls. Si on a une addition (commutative) de neutre 0 sur cet ensemble, la somme est $\sum_i a_i$ est bien définie (la somme sur une famille vide est nulle). De même, si un ensemble est muni d'un produit (commutatif) de neutre 1, le produit d'une famille $\prod_i a_i$ d'une famille dont tous les termes sauf un nombre fini sont égaux à 1 est défini (le produit sur une famille vide est égal à 1).

PARTIE I

GÉNÉRALITÉS SUR LES MODULES

On se souvient que se donner une espace vectoriel E sur un corps k, c'est se donner une action à gauche de k sur un groupe abélien E vérifiant les compatibilités usuelles. Autrement dit, c'est se donner une multiplication à gauche de k sur E vérifiant

$$(ab)e = a(be),\ (a+b)e = ae + be \text{ et } a(e+f) = ae + af$$

pour tout $a, b \in k$ et $e, f \in E$.

1. La notion de module

La notion de A-module M est en tout point analogue. On se permet de supposer seulement que A (qui joue le rôle de k) est un anneau, pour nous ceci suppose qu'il est commutatif et unitaire, et que M (qui joue le rôle de E) est un groupe abélien sur lequel A agit de sorte qu'on ait encore

$$(ab)e = a(be),\ (a+b)e = ae + be \text{ et } a(e+f) = ae + af$$

pour tout $a, b \in A$ et $e, f \in M$. De même qu'un sous-espace vectoriel est sous-ensemble contenant 0 et stable par addition et multiplication externe, de même un sous-module est sous-ensemble contenant 0 et stable par addition et multiplication externe.
De même qu'un corps est un espace vectoriel sur lui-même, de même un anneau est un module sur lui-même.

Exercice 1.1. — *Soit A l'anneau des fonctions de $\mathbf{C}$ dans $\mathbf{R}$. On fait opérer A sur le groupe additif $\mathbf{R}$ par la formule $f.x = f(i)x$ pour $f \in A$ et $x \in \mathbf{R}$. Montrer que cette loi externe muni $\mathbf{R}$ d'une structure de A-module.*

2. Groupes abéliens et Z-modules

Observons déjà que tout groupe **abélien** G a une unique structure de $\mathbf{Z}$-module induisant l'addition de G. En effet, si $n \in \mathbf{Z}$ et $g \in G$, on définit ng par la formule

$$ng = signe(n)(g + \cdots + g)\ |n|\ \ fois.$$

Le fait que G soit abélien garantit qu'on a bien (vérifiez !) $n(g+h) = ng+nh$. Par exemple, $M = \mathbf{Z}/4\mathbf{Z}$ est un $A = \mathbf{Z}$-module. Mais observons immédiatement un phénomène nouveau (par rapport aux espaces vectoriels) : celui de la **torsion**, autrement dit la possibilité d'existence d'éléments $m \in M, a \in A$ non nuls tels que $am = 0$. Ici par exemple, l'élément $a = 4$ « tue » tous les éléments de M.

Définition 2.1. — *Un élément m d'un A-module M est dit de torsion si l'idéal annulateur* $\mathrm{Ann}(m) = \{a \in A \text{ tels que } am = 0\}$ *est non réduit à* 0.

Ainsi le $\mathbf{Z}$-module $\mathbf{Z}/4\mathbf{Z}$ a de la torsion alors que $\mathbf{Z}$ n'en a pas -on veut dire par là que seul 0 est de torsion-.

3. Endomorphisme des k-espaces vectoriels et $k[X]$-module

Donnons nous un espace vectoriel E muni d'un endomorphisme f. On munit E d'une structure de $k[X]$-module en faisant opérer X comme f et plus généralement $P(X)$ comme le polynôme d'endomorphisme $P(f)$. Précisément, si $P \in k[X]$ et $e \in E$, on définit $P(X)e$ par la formule

$$P(X)e = P(f)(e).$$

Exercice 3.1. — *Vérifier que E est bien un $k[X]$-module avec cette loi externe. Montrez que si E est de dimension fini, tout élément de E est de torsion [calculer $\mu_f e$ où μ_f est le polynôme minimal de f].*

4. Morphismes

De même qu'on a des morphismes (voire endo, iso)morphismes d'espaces vectoriel, on a les notions analogues pour les morphismes de modules. On note $\mathrm{Hom}_A(M_1, M_2)$ l'ensemble des morphismes du A-module M_1 dans le A-module M_2, voire, si le contexte est clair, $\mathrm{Hom}(M_1, M_2)$. On laisse au lecteur le soin de définir la notion d'isomorphisme, de noyau, d'image dans ce cadre en copiant les définitions d'algèbre linéaire standard.

Exercice 4.1. — *Montrer que la multiplication externe de M_2 induit sur $\mathrm{Hom}_A(M_1, M_2)$ une structure de A-module.*

4.2. Illustrons sur un exemple important la signification de cette notion. Partons de deux espaces vectoriels E_1, E_2 sur un corps k, munis d'endomorphismes f_1, f_2. Comme en 3, ces endomorphismes définissent des structures de $k[X]$-module sur E_i qu'on notera alors $M_i, i = 1, 2$. Un morphisme de modules ϕ de M_1 dans M_2 est donc un morphisme $\phi : E_1 \to E_2$ vérifiant $\phi(f_1(e_1)) = \phi(Xe_1) = X\phi(e_1) = f_2\phi(e_1)$ pour tout $e_1 \in E_1$, autrement dit

$$\mathrm{Hom}_{k[X]}(M_1, M_2) = \{\phi \in \mathrm{Hom}(E_1, E_2) \text{ tels que } \phi \circ f_1 = f_2 \circ \phi\}.$$

En particulier, si $M_1 = M_2$, *ie* $E_1 = E_2$ et $f_1 = f_2$, alors $\mathrm{End}(M_1)$ est le **commutant** de f_1, ensemble des endomorphismes qui commutent avec f.

Exercice 4.3 **(Morphisme de Frobenius)**. — *Soit p un nombre premier. Montrer que pour $0 < n < p$, le coefficient binomial $\binom{n}{p}$ est divisible par p. Soit A un anneau, annulé par p (ie $pa = 0$ pour tout $a \in A$). Montrer que l'application $F : a \mapsto a^p$ définit un morphisme d'anneaux (on l'appelle le morphisme de Frobenius).*

4.4. Diagrammes, diagrammes commutatifs. — Plutôt que de nommer des morphismes de modules $f_1 \in \mathrm{Hom}(M_1, M_2)$, on se contente souvent, quand le contexte est clair d'écrire $M_1 \to M_2$. On aboutit alors à des *diagrammes* du type

$$\begin{array}{ccc} M_1 & \longrightarrow & M_2 \\ \downarrow & & \downarrow \\ M_3 & \longrightarrow & M_4 \end{array}$$

ou, plus compliqué par exemple

$$\begin{array}{ccc} M_1 & \longrightarrow & M_2 \\ & \searrow \downarrow \swarrow & \\ M_4 & \longrightarrow & M_3 \end{array}.$$

Dire qu'un tel diagramme commute, c'est dire que toutes les flèches obtenues par composition des flèches du diagramme partant d'une même source et arrivant à un même but sont égales. Ici, dans le premier cas, ceci signifie simplement que les flèches composées

$$M_1 \to M_2 \to M_4 \text{ et } \ M_1 \to M_3 \to M_4$$

sont égales. Dans le second cas, il suffit de vérifier, comme on s'en convainc facilement, que les deux triangles de gauche et de droite commutent.

5. Sous-modules

Rappelons qu'un sous-module d'un module M est un sous-groupe additif stable par multiplication externe. De même, les noyaux, images d'un morphisme sont des sous-modules. Par exemple, les sous-modules d'un anneau sont les idéaux.

Exercice 5.1. — *Si A intègre, vérifier que* $\mathrm{Tors}(M)$ *est un sous-module de M. Montrer que les idéaux de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$.*

Exercice 5.2. — *Quels sont les sous-modules du $\mathbf{Z}$-module $\mathbf{Z}/n\mathbf{Z}$?*

Avec les notations de 4.2, on se convaincra facilement que se donner un sous-module N_1 de $M_1 = (E_1, f_1)$, c'est se donner un sous-espace vectoriel F_1 de E_1 **stable** par f_1 et que, N_1 est le module associé à $(F_1, f_{1|F_1})$. On verra plus tard comment la théorie générale des $k[X]$-modules donne sans peine les résultats difficiles d'algèbre linéaire tels que la réduction de Jordan des endomorphismes d'espaces vectoriels de dimension finie.
D'ores et déjà, nous avons la correspondance suivante :

(5.2.a)

Algèbre linéaire	modules sur $k[X]$
$(E_1, f_1 \in \mathrm{End}_k(E_1))$	M_1 avec $Xe_1 = f(e_1)$
$(E_1, f_1, f_1' \in \mathrm{End}_k(E_1))$ avec f_1, f_1' semblables	isomorphisme de modules $M_1 = (E_1, f_1) \xrightarrow{\sim} M_1' = (E_1, f_1')$
$F_1 \subset E_1$ stables par f_1	$N_1 = (F_1, f_{1\|F_1}) \subset M_1$
diagrammes commutatifs $\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ E_1 & \xrightarrow{\phi} & E_2 \end{array}$	$\phi \in \mathrm{Hom}(M_1, M_2)$

6. Somme directe de modules-Modules libres

Comme en algèbre linéaire, on se donne une famille (éventuellement infinie) de A-modules $M_i, i \in I$. La somme directe est par définition l'ensemble des familles $(e_i)_{i\in I}$ presque nulles, *ie* telles que l'ensemble des $i \in I$ vérifiant $e_i \neq 0$ est **fini**. On définit les lois + et externe terme à terme comme en algèbre linéaire. On note ce module $\bigoplus_{i\in I} M_i$. Comme d'habitude, on identifie M_j au sous-module de $\bigoplus_{\in I} M_i$ des familles (e_i) tels que e_i nul si $i \neq j$. Avec cette convention, on a $(e_i) = \sum_{i\in I} e_i$ étant entendu que cette somme est finie car tous les termes sauf un nombre fini sont nuls. Si tous les M_i sont égaux à un même espace vectoriel M, on note $\oplus_{i\in I} M_i$ simplement $M^{(I)}$.

Exercice 6.1. — *Montrer que la somme directe $A^{\mathbf{N}}$ est isomorphe au module des polynômes $A[X]$.*

Le module somme directe vérifie la propriété universelle suivante :
pour tout A-module M, on a un bijection

$$h_M : \ F(M) = \mathrm{Hom}(\oplus_i M_i, M) \xrightarrow{\sim} G(M) = \prod_i \mathrm{Hom}(M_i, M) \tag{6.1.a}$$

définie comme suit. À $\Psi \in \mathrm{Hom}(\oplus_i M_i, M)$, on associe la famille de sa restriction aux M_i. L'inverse associe à la famille

$$(\Psi_i), \Psi_i \in \mathrm{Hom}(\oplus_i M_i, M)$$

le morphisme Ψ définit par

$$\Psi(\sum m_i) = \sum \Psi_i(m_i)$$

qui est bien une somme finie.
Si M_i est une famille de sous-modules de M, l'image de l'application canonique $\oplus M_i \to M$ est appelée somme des M_i, ou **module engendré** par les M_i, et se note parfois $+_{i\in I} M_i$.
Plus généralement, un module M sera dit somme directe de $M_i, i \in I$ s'il est isomorphe à la somme directe des M_i.

Définition 6.2 **(Module libre)**. — *On dit qu'un A-module est libre s'il est isomorphe à la somme directe de modules tous isomorphes à A.*

Par exemple, l'existence d'une base pour tout espace vectoriel assure que tout k-module est libre si k est un corps. C'est faux dans le cas général.

Exercice 6.3. — *Soit n un entier > 1. Montrer que $\mathbf{Z}/n\mathbf{Z}$ n'est pas libre. Montrer plus généralement que si tout A-module est libre alors A est un corps.*

Comme en algèbre linéaire, on a les notions de **famille libre** d'un module M ($(m_i)_{\in \mathcal{I}}$ est libre si une combinaison linéaire finie $\sum a_i m_i, a_i \in A$ n'est nulle qu'à condition que tous les coefficients a_i soient nuls), de **famille génératrice** (si tout élément de M est combinaison linéaire (finie) des m_i) et de **base** (libre et génératrice).
Dire qu'un module est libre c'est dire qu'il a une base. Notons que, comme en algèbre linéaire, $A^{(I)}$ a une base canonique e_i : si on voit $A^{(I)}$ comme le modules des applications de I dans A nulles sauf sur un nombre fini d'indices, e_i est l'application qui vaut 1 en i et 0 sinon. On a alors la décomposition $a = \sum a(i)e_i$, qui, contrairement aux apparences trompeuses, est bien une somme finie.

7. Modules quotients

Rappelons la construction du quotient d'un module M_2 par un sous-module M_1. L'idée est de fabriquer un nouveau-module $M_3 = M_2/M_1$ dans lequel on a tué les éléments de M_1. On reprend la construction de $\mathbf{Z}/n\mathbf{Z}$, cas particulier pour $M_1 = n\mathbf{Z}$ et $M_2 = \mathbf{Z}$.
En général, l'ensemble quotient M_2/M_1 est l'ensemble des **translatés**

$$m_2 + M_1 = \{m_2 + m_1, m_1 \in M_1\} \subset M_2.$$

Notons que deux tels translatés $(m_2 + M_1)$ et $(m_2' + M_1)$ sont égaux si et seulement si $m_2 - m_2' \in M_1$.
On définit la somme de deux translatés $(m_2 + M_1) + (m_2' + M_1) = (m_2 + m_2' + M_1)$ qui ne dépend que des translatés $(m_2 + M_1)$ et $(m_2' + M_1)$ et pas du choix de m_2 (exercice). Ceci reflète le caractère distingué du sous-groupe M_1 de M_2 (qui est abélien).

On définit de même le produit externe $a(m_2 + M_1) = am_2 + M_1$. La condition M_1 sous-module est précisément celle qui assure que la **surjection canonique**

$$\pi : \ M_2 \twoheadrightarrow M_2/M_1$$

définie par $m_2 \to m_2 + M_1$ est un **morphisme** de modules.

Exercice 7.1. — *Montrer qu'il existe une unique structure de A-module sur M_2/M_1 telle que π est un morphisme. Vérifier que le noyau de π est M_1.*

L'énoncé suivant est facile, bien connu et... fondamental.

***Proposition 7.2* (Propriété universelle du quotient).** — *L'application de composition par la surjection canonique $M_2 \twoheadrightarrow M_2/M_1$ définit un isomorphisme fonctoriel*

$$\mathrm{Hom}(M_2/M_1, M) \to \{f \in \mathrm{Hom}(M_2, M) \text{ tels que } f(M_1) = 0\}.$$

Preuve : Soit $f \in \mathrm{Hom}(M_2, M)$ tels que $f(M_1) = 0$. Un antécédent $\phi \in \mathrm{Hom}(M_2/M_1, M)$ vérifie $f = \phi \circ \pi$. La valeur de ϕ est déterminée sur $\pi(M_2)$ par f. Comme π est surjectif, ϕ est déterminé sur $M_2/M_1 = \pi(M_2)$, donc un tel ϕ, s'il existe, est unique. D'où l'injectivité. Soit alors $t \in M_2/M_1$: c'est la classe d'un élément m_2, bien déterminé à addition d'un élément $m_1 \in M_1$ quelconque près. Comme $f(M_1) = 0$, les images de tous les éléments m_2 représentant t sont un seul et même élément qu'on baptise $\phi(t)$. Par construction, $\phi \circ \pi = f$ et ϕ est évidemment un morphisme (par exemple, si $a \in A$ et $t = \pi(m_2)$ est un élément arbitraire de M_2/M_1, on a

$$\phi(at) = \phi(a\pi(m_2)) = \phi(\pi(am_2)) = f(am_2) = af(m_2) = a\phi \circ \pi(m_2) = a\phi(t)$$

et de même pour l'addition).■

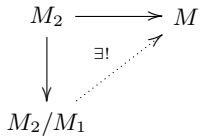
Remarque 7.3. — *Comme dans le cas arithmétique de $\mathbf{Z}/n\mathbf{Z}$, on n'étudie essentiellement jamais les modules quotients en revenant à la définition en termes de translatés, mais en utilisant la propriété universelle caractéristique. On verra cela tout au long du cours.*

Exemple 7.4. — *Le noyau du morphisme $\mathbf{Z} \to A$ défini par $n \mapsto n1_A$ est de la forme $n\mathbf{Z}, n \geq 0$ (5.1) et on dit que A est de caractéristique n. On a alors un plongement canonique $\mathbf{Z}/n\mathbf{Z} \hookrightarrow A$.*

Exercice 7.5. — *Montrer que si A est intègre, l'ensemble $\mathrm{Tors}(M)$ des éléments de M qui sont de torsion est un sous-module. Montrer que c'est en général faux si A n'est pas intègre. Montrer que le quotient $M/\mathrm{Tors}(M)$ est sans torsion. Montrer, en un sens que l'on précisera, que c'est le plus grand module quotient de M qui est sans-torsion.*

8. Diagrammes, complexes, suites exactes

On raisonnera de plus en plus souvent en représentant des suites de morphismes par des diagrammes. Quand le contexte est clair, on ne nommera pas les flèches. Par exemple, la proposition 7.2 se représente sous la forme suivante



et on dira qu'il existe une unique (symbolisé ici par la flèche pointillée avec en exposant $\exists!$) flèche $M_2/M_1 \to M$ qui fait commuter le diagramme précédent, au sens que la flèche composée $M_2 \to M_2/M_1 \to M$ est égale à la flèche $M_2 \to M$. Quand

on a des diagrammes plus compliqués, dire qu'il commute c'est dire que tous les composés possibles sont égaux lorsqu'ils partent d'une même source et arrivent à un même but.

Définition 8.1. — *Soient*

$$M_1 \stackrel{f_1}{\to} M_2 \stackrel{f_2}{\to} M_3 \tag{8.1.a}$$

une suite de morphismes de modules.

- *Le conoyau de f_1 est le quotient* $\mathrm{Coker}(f_1) = M_2/\mathrm{Im}(f_1)$.
- *La suite 8.1.a est un complexe si* $\mathrm{Im}(f_1) \subset \mathrm{Ker}(f_2)$ *ie si* $f_2 \circ f_1 = 0$.
- *La suite 8.1.a est exacte si* $\mathrm{Im}(f_1) = \mathrm{Ker}(f_2)$.

De même que dire que f_1 est injectif c'est dire que son noyau est nul, de même dire que f_1 est surjectif c'est dire que son conoyau est nul. Une suite plus longue

$$M_1 \to \cdots \to M_n, n \geq 3$$

sera dite un complexe (une suite exacte) si chaque sous-suite

$$M_i \to M_{i+1} \to M_{i+2}, 1 \leq i \leq n-2$$

à trois termes consécutifs est un complexe (une suite exacte).
Notons que dire que $0 \to M \to N$ est exact, c'est dire que $M \to N$ est injectif et que dire que $M \to N \to 0$ est exact c'est dire que $M \to N$ est surjectif.

Exercice 8.2. — *Soit $f : M \to N$ un morphisme. Vérifier que la suite*

$$0 \to \mathrm{Ker}(f) \to M \to N \to \mathrm{Coker}(f) \to 0$$

est exacte. Montrer que si $M_0 \to M_1 \to M_2 \to M_3 \to M_4$ est exacte et que $N_2 = \mathrm{Coker}(M_1 \to M_2)$, on a naturellement deux suites exactes

$$M_0 \to M_1 \to N_2 \to 0$$

et

$$0 \to N_2 \to M_3 \to M_4.$$

9. Anneaux quotients

De même, si I est un idéal de A, le A-module quotient A/I est muni d'une structure d'anneau qui est la seule telle que la surjection canonique $A \twoheadrightarrow A/I$ soit un morphisme d'anneaux (et pas seulement de module). De même que plus haut, les homomorphismes d'anneaux de A/I dans un anneau B s'identifient aux morphisme de A dans B nuls sur I (on tue I !). On notera $(a_s, s \in S)$ l'idéal engendré par la famille $(a_s), s \in S$. Si I, J sont des idéaux, on note IJ l'idéal engendré par les produits $ij, i \in I, j \in J$. On parle alors, abusivement, d'*idéal produit* de I et J.

Définition 9.1. — *Soit I un idéal d'un anneau A.*

- *On dit que A est intègre si A est non nul et si le produit de deux éléments non nuls de A est non nul.*
- *On dit que I est premier si A/I est intègre.*
- *On dit que I est maximal si A/I est un corps.*

En particulier, un idéal maximal est premier. Notons que l'idéal A n'est ni premier ni maximal (l'anneau nul n'est pas intègre),

Exercice 9.2. — *Montrer que l'image inverse d'un idéal premier par un morphisme d'anneaux est un idéal premier. Montrer qu'en général l'image inverse d'un idéal maximal n'est pas maximal (considérer par exemple l'inclusion de* $\mathbf{Z}$ *dans* $\mathbf{Q}$*).*

L'ensemble des idéaux premiers de A se note $\mathrm{Spec}(A)$: le spectre de A (rien à voir avec Hamlet, ou James Bond!!!).

Lemme 9.3. — *Un idéal est maximal s'il est maximal pour l'inclusion parmi les idéaux propres de* A*.*

Preuve : Supposons que A/I est un corps. Soit J un idéal contenant I, distinct de I. Montrons que $J = A$, autrement dit $1 \in J$. Soit $j \in J$ non dans I. La classe de j dans A/I est non nulle, donc inversible. Autrement dit, il existe $a \in A$ tel que $aj \equiv 1 \mod I$ ou encore $1 - aj \in I$. Mais $aj \in J$ et $I \subset J$ donc $1 \in J$ et ainsi $J = A$.
Inversons, supposons I propre maximal pour l'inclusion. Montrons que A/I est un corps. Comme $I \neq A$, certainement $A/I \setminus 0$ est non vide. Soit alors $\bar{a} \neq 0$ la classe de a dans A/I, autrement dit $a \notin I$. L'idéal $J = aA + I$ contient I strictement. Par maximalité, il n'est pas propre, donc $A = aA + I$ et donc $1 \in aA + I$. Si $b \in A$ est tel que $1 - ab \in I$, la classe de b est l'inverse de $\bar{a}$.■

Une application facile du lemme de Zorn assure **l'existence d'idéaux maximaux dans tout anneau non nul**. On utilisera librement cette existence.

Exercice 9.4. — *Montrer que dans un anneau principal, les idéaux premiers non nuls sont maximaux, engendrés par les polynômes irréductibles.*

10. Rang d'un module libre de type fini

Un A-module libre est, rappelons le, un module isomorphe à A^n. Rappelons que, sauf mention expresse du contraire, les anneaux que nous considérons sont non nuls. La question est de savoir si le n en question est unique. Autrement dit, l'existence d'un isomorphisme $A^n \xrightarrow{\sim} A^m$ entraîne-t-il $n = m$. Lorsqu'on aura vu l'algèbre extérieure, ceci deviendra évident. Voyons une preuve « élémentaire ». Un tel isomorphisme est défini par une matrice $M \in M_{m,n}(A)$. L'inverse a une matrice $N \in M_{n,m}(A)$. Ces deux matrice vérifient

$$MN = \mathrm{Id}_{m,A} \text{ et } NM = \mathrm{Id}_{n,A}.$$

Soit alors $\mathfrak{m}$ un idéal maximal de A (qui est non nul!) et notons $k = A/\mathfrak{m}$ le corps résiduel. Réduisant ces identités matricielles mod $\mathfrak{m}$, on déduit l'existence de matrices dans k vérifiant

$$\bar{M}\bar{N} = \mathrm{Id}_{m,k} \text{ et } \bar{N}\bar{M} = \mathrm{Id}_{n,k}.$$

La matrice $\bar{M}$ définit donc un isomorphisme de k-espaces vectoriels $k^n \xrightarrow{\sim} k^m$. La théorie de la dimension assure alors $n = m$. Cet entier n s'appelle **le rang** du module libre A^n.

Remarque 10.1. — *Il n'est pas difficile de montrer que si* $A^{(I)} \xrightarrow{\sim} A^{(J)}$*, alors* I *et* J *sont en bijection. À titre d'exercice, on pourra déjà vérifier que si* I *est infini, il en est de même de* J*.*

Cette propriété est complètement fausse si on ne suppose plus l'anneau commutatif.

11. Le lemme Chinois

On sait que les anneaux $\mathbf{Z}/nm\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ sont isomorphes si n et m sont premiers entre eux. Cette dernière condition peut s'écrire aussi $(n) + (m) = A$ d'après l'identité de Bézout. Plus généralement, supposons qu'on ait des idéaux $I_1, \cdots, I_n, n \geq 2$ de A, deux à deux étrangers, *ie* tels que $I_i + I_j = A$ pour $i \neq j$.

***Lemme 11.1* (Lemme Chinois).** — *Sous ces conditions, l'application canonique $A \to \prod A/I_j$ se factorise à travers $\cap I_j$ pour donner un isomorphisme*

$$A/I_1 \cap \cdots \cap I_n \xrightarrow{\sim} \prod A/I_j.$$

De plus, on a

$$I_1 \cap \cdots \cap I_n = I_1. \cdots .I_n.$$

Preuve : Bien entendu, le noyau de $A \to A/I_1 \times \cdots \times A/I_n$ est l'intersection $I_1 \cap \cdots \cap I_n$. Par propriété universelle du quotient, on a donc une application

$$A/I_1 \cap \cdots \cap I_n \xrightarrow{\sim} \prod A/I_j$$

qui est injective (on a tué le noyau de la flèche initiale !). Vérifions la surjectivité. Si on note $I(-j)$ l'idéal

$$I(-j) = I_1 \cdots \widehat{I_j} \cdots I_n$$

produit des idéaux I_i distincts de I_j (*ie* engendré par les produits d'éléments des I_i distincts de I_j), observons qu'on a

$$\sum_j I(-j) = A.$$

En effet, on peut faire une récurrence sur n. Si $n = 2$, c'est l'hypothèse $I_2 + I_1 = A$. Sinon, on applique l'hypothèse de récurrence à $I_1, \cdots, I_{n-1}$. On obtient alors que la somme des $n-1$ idéaux $I_1 \cdots \widehat{I_j} \cdots I_{n-1}$ est A, de sorte que, multipliant par I_n, on a

$$\sum_{j<n} I(-j) = I_n$$

et la somme $\sum_j I(-j)$ contient I_n. En appliquant le même procédé à $I_2, \cdots, I_n$, on obtient que la somme contient I_1. Comme $I_1 + I_n = A$, la somme vaut A.
On écrit alors $1 = \sum_j a_j, a_j \in I(-j)$. Soit alors $\bar{b}_j \in A/I_j$ des classes quelconques. Posons $b = \sum_j a_j b_j$. Observons alors

$$a_j \equiv 0 \mod I_i \text{ si } i \neq j \text{ et } a_j \equiv 1 \mod I_j$$

de sorte que $b \equiv b_j a_j \equiv b_j \mod I_j$ pour tout j.
Reste à se convaincre que le produit des I_i, clairement dans l'intersection des I_i, lui est égale. Soit donc a dans cette intersection. On a $a = \sum_i a a_i$. Comme $a \in I_i$, on a $a \in I_i I(-i) = I_1 \cdots I_n$ pour tout i, ce qu'on voulait.■

Exercice 11.2. — *Montrer que l'anneau quotient $\mathbf{R}[X]/(X^2 + X + 1)$ est isomorphe à $\mathbf{C}$. Montrer que l'anneau $\mathbf{R}[X]/(X(X+1))$ est isomorphes à $\mathbf{R}^2$ (cf. 12.2).*

12. Algèbres

Donnons nous deux anneaux A, B. On dit que B est une A-algèbre (unitaire) si B est de plus muni d'une structure de A-module compatible avec le produit au sens où

$$a.(bb') = (a.b)b' \text{ pour tout } a \in A,\ b, b' \in B.$$

Il revient au même de se donner un morphisme d'anneaux $f : A \to B$ car on définit alors la structure de modules par $a.b = f(a)b$ pour $a \in A,\ b \in B$. Par exemple, $\mathbf{C}$ est une $\mathbf{R}$-algèbre, un anneau est une $\mathbf{Z}$-algèbre.
Un morphisme $f \in \mathrm{Hom}(B, B')$ de A-algèbres B, B' est un morphisme d'anneaux qui est de plus A-linéaire.

Proposition 12.1. — *Soit B une A-algèbre et $b \in B$. Il existe un unique morphisme d'algèbres $A[X] \to B$ qui envoie X sur b. De plus, tous les morphismes sont de ce type.*

Preuve : Soit ϕ un tel morphisme. Alors, nécessairement, $\phi(\sum_i a_i X^i) = \sum_i a_i \phi(X)^i$ et donc est déterminé par $b = \phi(X)$. Inversement, on vérifie que l'application

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

est bien un morphisme d'algèbres. ■

En utilisant l'identification $A[X, Y] = A[X][Y]$, on obtient que les morphismes d'algèbres de $A[X_1, \cdots, X_n]$ dans B s'identifient aux n-uples $b = (b_1, \cdots, b_n) \in k^n$ (à un tel élément est associé le morphisme $(P \mapsto P(b))$).
Notons que si B est une A-algèbre et I un idéal de B, l'anneau quotient B/I est aussi un A-module (car B et I sont des A-modules) et donc B/I est une A-algèbre canoniquement).

Exercice 12.2. — *Décrire un isomorphisme de $\mathbf{R}$-algèbre entre $\mathbf{R}[X]/(X^2+X+1)$ et $\mathbf{C}$ d'une part et entre $\mathbf{R}[X]/(X(X+1))$ et $\mathbf{R}^2$ d'autre part. Comparer avec l'exercice 11.2.*

13. Une application du lemme chinois : l'algorithme de Berlekamp

Nous allons donner un algorithme, qu'on peut implanter sur un ordinateur, permettant de factoriser un polynôme de $\mathbf{F}_p[X]$ en facteurs irréductibles (on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$). On suppose que le lecteur se souvient des propriétés arithmétiques usuelles des anneaux de polynômes sur des corps, essentiellement le fait que ce sont des anneaux euclidiens. Dans le cas contraire, il reportera la lecture de cette section après l'étude des anneaux principaux plus bas. On se donne donc p premier et $P \in \mathbf{F}_p[X]$ non constant, unitaire. Rappelons (petit théorème de Fermat ou théorème de Lagrange comme on veut) que si p ne divise pas $n \in \mathbf{Z}$, on a la congruence $n^{p-1} \equiv 1 \mod p$. On déduit l'égalité

$$x^p = x \text{ pour tout } x \in \mathbf{F}_p.$$

13.1. Où l'on se ramène à P' non nul. — Observons déjà que le polynôme dérivé P' est nul si et seulement si P est une somme de monômes du type $a_n X^{pn}, a_n \in \mathbf{F}_p$ (observer que $(X^m)' = mX^{m-1}$ est nul si et seulement si $p|m$). Comme $a^p = a$ pour tout $a \in \mathbf{F}_p$, on a alors

$$P(X) = \sum a_n X^{pn} = \sum a_n^p X^{pn} = (\sum a_n X^n)^p$$

d'après 4.3. Ainsi, en itérant le processus, visblement parfaitement algorithmique, on arrive à écrire

$$P(X) = Q(X)^{p^m} \text{ avec } Q'(X) \not\equiv 0.$$

On peut donc supposer $P' \neq 0$.

13.2. Points fixes du Frobenius. — On rappelle (on reverra ceci) que P s'écrit de façon unique

$$P = \prod P_i^{n_i}$$

avec $n_i > 0$ et P_i unitaire irréductible. Comme $P_i^{n_i}$ et $P_j^{n_j}$ sont premiers entre eux pour $i \neq j$, la somme des idéaux qu'ils engendrent est tout $\mathbf{F}_p[X]$. Le lemme Chinois assure que le morphisme d'algèbres (de caratéristique p)

$$A = \mathbf{F}_p[X]/(P) \to \oplus \mathbf{F}_p[X]/(P_i^{n_i})$$

est un isomorphisme d'algèbres.

Remarque 13.3. — *L'algèbre A est de dimension $d = \deg(P)$ sur $\mathbf{F}_p$. En effet, si $Q \in P[X]$, la classe de Q est celle de son reste dans la division de Q par P. Comme Q est de degré $< d$, on déduit que les classes de $1, \cdots, X^{d-1}$ engendrent A comme espace vectoriel. Un argument analogue de division prouve qu'elles forment une base. Les éléments de $A \setminus \mathbf{F}_p$ s'identifient alors aux classes des polynômes non constants qui sont de degré $< d$.*

Soit F le morphisme de Frobenius de A (on note de même celui de $A_i = \mathbf{F}_p[X]/(P_i^{n_i})$). Notons que $\mathbf{F}_p \subset A_i$ est contenu dans $A_i^F = \mathrm{Ker}(F - \mathrm{Id})$ (petit théorème de Fermat).

Lemme 13.4. — *L'isomorphisme chinois γ identifie A^F et $\oplus (A_i)^F$. En particulier, A^F contient l'espace vectoriel $\gamma^{-1}(\mathbf{F}_p^r)$ de dimension r avec*

$$\mathbf{F}_p^r = \{(x_1, \cdots, x_r), x_i \in \mathbf{F}_p\} \subset \oplus A_i.$$

Preuve : En effet, si $a \in A$ fixé par F, on a $F(a) = a^p = ax$ et donc $\gamma(a)^p = \gamma(a)$. Mais si $\gamma(a) = (a_i)$, on a $(a_i)^p = (a_i^p) = (F(a_i))$ ce qui prouve que γ est un morphisme (injectif) de A^F dans $\oplus A_i^F$. Inversement, si $(a_i) \in \oplus A_i^F$, soit a l'unique antécédent de a par γ. Lisant le calcul précédent à l'envers, on obtient $a \in A^F$, prouvant la surjectivité. ■

En particulier, on a

$$\dim_{\mathbf{F}_p} A^F = \mathrm{rg}(F - \mathrm{Id}) \geq r.$$

Notons que le calcul de ce rang est parfaitement algorithmique : on calcule la matrice de F dans la base des classes des $X^i, i = 0, \cdots, d-1$ (ce qui se faiut en divisant X^{ip} par P) puis on calcule le rang de $F -$
Id par pivot de Gauss).

13.5. Le cas $\mathrm{rg}(F - \mathrm{Id}) = 1$**.** — On a donc $r = 1$ et $P = P_1^{n_1}$ avec de plus $P' \neq 0$. On a alors $P' = n_1 P_1' P_1^{n_1 - 1} \neq 0$ de sorte que $\mathrm{PGCD}(P, P') = P_1^{n_1 - 1}$ car P_1 irréductible. Le PGCD de P et P' se calcule avec l'algortithme de Bézout ce qui donne P_1 par division euclidienne et le n_1 s'obtient en regardant les degrés : on a terminé dans ce cas.

13.6. Le cas $\mathrm{rg}(F - \mathrm{Id}) > 1$**.** — Dans ce cas, il existe $a \in A$ qui n'est pas dans notre droite $\mathbf{F}_p$ des polynômes constants. Autrement dit (13.3), il existe Q de degré $0 < \deg(Q) < d$ tel que $\bar{Q} \in A^F$, *ie* $P | Q^p - Q$. Le petit théorème de Fermat assure que les p racines de $X^p - X$ sont les éléments de $\mathbf{F}_p$, autrement dit

$$X^p - X = \prod_{i \in \mathbf{F}_p} (X - i)$$

de sorte qu'on a

$$Q^p - Q = \prod_{i=0}^{p-1} (Q - i) \mod P$$

et donc

$$P | \prod_{i \in \mathbf{F}_p} (Q - i).$$

Notons que si $\bar{i} \neq \bar{j}$, l'identité

$$1/(j-i)((Q-i)-(Q-j))=1$$

assure $\mathrm{PGCD}(Q-i, Q-j)=1$ si $i \neq j$ dans $\mathbf{F}_p$. Ainsi, chaque facteur $P_j^{n_j}$ de P divise exactement un des facteurs $Q-i$ de sorte que

$$P=\prod_{i\in\mathbf{F}_p} \mathrm{PGCD}((Q-i),P).$$

Maintenant, chaque polynôme $\mathrm{PGCD}((Q-i),P)$ (qui se calcule grâce à l'algorithme de Bézout) est de degré $<\deg(P)$ par construction et on recommence le processus pour chaque polynôme $\mathrm{PGCD}((Q-i),P)$. Ce processus s'arrête en un nombre fini d'étapes.

Un excellent exercice est de programmer cet algorithme avec un logiciel de calcul formel. Un autre excellent exercice est d'évaluer le nombre d'opérations nécessaire : en effet, comme le nombre de polynômes de degré donné dans $\mathbf{F}_p[X]$ est fini, on aurait pu effectuer tous les produits de deux polynômes et comparer avec P ce qui donne un algorithme de factorisation. Mais, dès que le degré est grand, le nombre d'opérations est énorme et fait exploser n'importe quelle machine. En revanche, pour très petits p, d, il est efficace. Quoi qu'il en soit, l'algorithme de Berlekamp, relativement efficace en général, est théoriquement intéressant.

Remarque 13.7. — *Le lecteur savant généralisera l'algorithme en remplaçant $\mathbf{F}_p$ par $\mathbf{F}_q$, $q=p^n$ simplement en remplaçant F par le composé F^n de n copies de F.*

14. Module des fractions

Donnons un autre exemple de construction universelle. Soit S une partie de l'anneau A, stable par produits. En particulier le produit vide, égal à 1, est dans S.

Les deux exemples fondamentaux sont $S=A\setminus\mathfrak{p}$ le complémentaire d'un idéal premier $\mathfrak{p}$ vérifie cette propriété ou encore l'ensemble $S=\{f^n, n\geq 0\}$ des puissances d'un élément.

On construit le **module des fractions**, ou **localisé** $S^{-1}M$ de M, par rapport à S de la manière suivante.

Lemme 14.1. — *La relation sur $S\times M$ définie par*

$$(s,m)\equiv(s',m') \text{ si et seulement si il existe } \sigma\in S \text{ tel que } \sigma(s'm-sm')=0$$

est une relation d'équivalence.

Preuve : La relation est visiblement réflexive et symétrique. Vérifions la transitivité. Soient donc $s_i\in S, m_i\in M, i=1,2,3$ tels que

$$(s_1,m_1)\equiv(s_2,m_2) \text{ et } (s_2,m_2)\equiv(s_3,m_3).$$

Il existe donc $\sigma_1,\sigma_2\in S$ tel que

$$\sigma_1(s_2m_1-s_1m_2)=0 \text{ et } \sigma_2(s_3m_2-s_2m_3)=0.$$

On cherche à éliminer les termes en m_2 pour obtenir une relation entre m_1 et m_3. On multiplie la première équation par $\sigma_2 s_3$ et la seconde par $\sigma_1 s_1$ et on ajoute pour trouver

$$\sigma_2s_3\sigma_1s_2m_1-\sigma_1s_1\sigma_2s_2m_3=\sigma_1\sigma_2s_2(s_3m_1-s_1m_3)=0,$$

ce qui prouve le lemme car $\sigma_1\sigma_2s_2\in S$.■

Définition 14.2. — *L'ensemble quotient $S\times M/\equiv$ se note $S^{-1}M$.*

La classe de (s, m) dans le quotient se note sous forme de fraction m/s. L'égalité $m/s = m'/s'$ dans $S^{-1}M$ étant par définition obtenue étant obtenue « par réduction formelle au même dénominateur » puis par multiplication du numérateur par s".
L'addition et la loi externe s'imposent alors d'elles-mêmes par analogie au cas des fractions usuelles on pose

$$m/s + m'/s' = (s'm + sm')/ss' \text{ et } a(m/s) = (am)/s.$$

Si M est l'anneau A, on définit de plus une structure d'anneau par la formule

$$(a/s)(a'/s') = (aa')/(ss').$$

On vérifie que $S^{-1}M$ est un $S^{-1}A$-module, la multiplication externe étant définie par

$$a/s.m/s' = (am)/(ss').$$

Notons que la flèche $M \to S^{-1}M$ est un morphisme, en général **ni injectif ni surjectif**. La flèche $A \to S^{-1}A$ est un morphisme d'anneaux qui permet de considérer $S^{-1}M$ comme un A-module.
Si $S = A\backslash\mathfrak{p}$ est le complémentaire de l'idéal premier $\mathfrak{p}$, le localisé correspondant est noté $A_\mathfrak{p}$. Si c'est l'ensemble des puissances de l'élément f, on le note $A[1/f]$.

Exercice 14.3. — *Montrer que* $\mathbf{Z}[1/10]$ *s'identifie à l'ensemble des nombres décimaux (ne pas confondre avec l'anneau des entiers 10-adiques* $\mathbf{Z}_{10}$*).*

Soit $f \in \mathrm{Hom}(M_1, M_2)$ un morphisme de A-modules.

Lemme 14.4. — *Il existe un unique morphisme localisé de* $S^{-1}A$*-modules, encore noté* f *(abusivement), entre* $S^{-1}M_1$ *et* $S^{-1}M_2$ *caractérisé par la formule*

$$f(m_1/s) = f(m_1)/s.$$

Preuve : Il s'agit de vérifier que si on a un autre représentant m_1'/s' de m_1/s, on a $f(m_1/s) = f(m_1'/s')$. Ceci prouvera que f est bien définie par la formule précédente. Le fait que ce soit un morphisme est clair. Vérifions donc. Il existe $\sigma \in S$ tel que $\sigma(s_1'm_1 - s_1m_1') = 0$. Comme f est A-linéaire, on a $\sigma(s_1'f(m_1) - s_1f(m_1')) = 0$ ce qui assure l'égalité $f(m_1)/s = f(m_1')/s$.∎

On laisse au lecteur le soin de vérifier que cette construction est compatible à la composition des morphismes : on a un exemple de foncteur (cf. 16). Quand on a un morphisme $M \to N$, on notera le morphisme localisé $S^{-1}M \to S^{-1}N$ sans plus de commentaire la plupart du temps. C'est même **un foncteur exact**, *ie* qui transforme suite exacte en suite exacte.

Proposition 14.5. — *Si* $M_1 \to M_2 \to M_3$ *est une suite exacte de* A*-modules, il en va de même de*

$$S^{-1}M_1 \to S^{-1}M_2 \to S^{-1}M_3.$$

Preuve : Comme la localisation des morphismes respecte la composition, la suite localisée est certainement un complexe. Soit alors $m_2/s \in S^{-1}M_2$ nul dans $S^{-1}M_3$. Ceci signifie l'existence de $\sigma \in S$ tel que $\sigma m_3 = 0$ où m_3 est l'image de m_2 dans M_3. Mais alors, σm_2 a une image nulle dans M_3 et provient donc de $m_1 \in M_1$. On vérifie que $m_1/(\sigma s)$ s'envoie sur m_2/s.∎

Exemple 14.6. — *Si* A *est un anneau intègre (donc non nul), la partie* $S = A \setminus 0$ *est stable par produit, et le localisé* $K = S^{-1}A$ *est... le* ***corps des fractions*** *de* A *(c'est bien un corps !). Si* S *est une partie stable par produits ne contenant pas zéro,* $S^{-1}A$ *s'identifie au sous-anneau de* K *des fractions de dénominateur dans* S*.*

Exercice 14.7. — *Soit* n *un entier. Calculer les localisés* $(\mathbf{Z}/n\mathbf{Z})_\mathfrak{p}$ *pour* $\mathfrak{p} = p\mathbf{Z}$ *premier. En déduire que l'application* $\mathbf{Z}/n\mathbf{Z} \to \oplus_p(\mathbf{Z}/n\mathbf{Z})_{(p\mathbf{Z})}$ *est un isomorphisme de groupes.*

On reviendra sur ce résultat lorsqu'on étudiera les modules sur les anneaux principaux.

***Proposition 14.8* (Propriété universelle des localisés d'anneaux).** — *Soit S une partie d'un anneau A ne rencontrant pas 0 stable par produit. Pour tout anneau B, l'application canonique $A \to S^{-1}A$ induit une bijection entre l'ensemble des morphismes d'anneaux $\mathrm{Hom}_{ann}(S^{-1}A, B)$ et l'ensemble des $f \in \mathrm{Hom}_{ann}(A, B)$ telle que $f(S)$ est inversible dans B.*

La preuve est laissée au lecteur.

Proposition 14.9. — *Soit $\mathfrak{p} \in \mathrm{spec}(A)$. L'idéal $\mathfrak{p}A_{\mathfrak{p}}$ engendré par $\mathfrak{p}$ est l'unique idéal maximal de $A_{\mathfrak{p}}$.*

Preuve : Observons que tout élément $\alpha = a/s$ qui n'est pas dans

$$\mathfrak{p}A_{\mathfrak{p}} = \{f/s, f \in \mathfrak{p} \text{ et } s \notin \mathfrak{p}\}$$

est inversible. En effet, on a $a \notin \mathfrak{p}$ et donc, la fraction s/a est l'inverse de α. Un idéal propre de $A_{\mathfrak{p}}$ est donc contenu dans $\mathfrak{p}A_{\mathfrak{p}}$, car sinon il contiendrait un inversible.■

Définition 14.10. — *Un anneau A qui possède un unique idéal maximal $\mathfrak{m}$ est dit local. Le quotient $k(\mathfrak{m}) = A/\mathfrak{m}$ est dit corps résiduel.*

Attention, il n'est pas vrai en général que les anneaux $S^{-1}A$ soient locaux.

Exercice 14.11. — *Montrer que $S^{-1}A$ est nul si et seulement si $0 \in S$. En particulier, $A[1/f]$ est non nul, si et seulement si f est* ***non nilpotent****. Montrer que les idéaux premiers de $S^{-1}A$ s'identifient aux idéaux premiers de A ne rencontrant pas S. Montrer que $\mathbf{Z}[1/10]$ n'est pas local.*

15. Radical nilpotent d'un anneau

À titre d'illustration, on va voir que la notion de localisation permet de caractériser les nilpotents d'un anneaux en termes d'idéaux premiers.

Lemme 15.1. — *Si $b \in A$ est nilpotent, $1 - b$ est inversible.*

Preuve : Soit k tel que $b^{k+1} = 0$. La formule de la progression géométrique

$$a^{k+1} - b^{k+1} = (a - b)\sum_{i=0}^{k} a^i b^{k-i}$$

appliquée à $a = 1$ et b donne

$$1 = (1 - b)\sum_{i=0}^{k} b^{k-i}$$

et fournit un inverse de $1 - b$.■

Remarque 15.2. — *L'idée est de développer en série formellement $1/(1 - b)$ en puissance de b et de constater que cette série est ici en fait un polynôme.*

Proposition 15.3. — *L'ensemble des éléments nilpotents de A est l'intersection des idéaux premiers : on l'appelle le radical nilpotent de A.*

Preuve : Soit a un élément nilpotent de A, *ie* tel que $a^n = 0$ pour $n > 0$ et soit $\mathfrak{p} \in \mathrm{Spec}(A)$. Si $n = 1$, alors $a = 0 \in \mathfrak{p}$. Sinon, on prend $m > 0$ minimal tel que $a^m \in \mathfrak{p}$ (qui existe car $a^n = 0 \in \mathfrak{p}$). Si $m > 1$, on a $a^{m-1}a \in \mathfrak{p}$ et donc a^{m-1} ou a est dans $\mathfrak{p}$, contredisant la minimalité de m. Donc, $a \in \mathfrak{p}$.
Inversement, si a n'est pas nilpotent, l'anneau des fractions $A[1/a]$ est non nul (14.11) et donc possède un idéal maximal. Son image inverse par $A \to A[1/a]$ est un idéal premier $\mathfrak{p}$, qui ne contient pas a (14.11). ■

Corollaire 15.4. — *Les inversibles de $A[X]$ sont les polynômes $P = a_0 + \cdots + a_nX^n$ avec $a_i, i > 0$ nilpotents et a_0 inversibles. En particulier, si A est intègre, ce sont les inversibles de A et si A est un corps, les polynômes de degré nul.*

Preuve : Supposons P inversible d'inverse Q. Soit $\mathfrak{p}$ premier. On note $\bar{A}$ le quotient $A/\mathfrak{p}$: c'est un anneau intègre. L'image $\bar{P} = \bar{a}_0 + \cdots + \bar{a}_nX^n$ de P dans $\bar{A}[X]$ est inversible d'inverse $\bar{Q}$. Comme $\bar{A}$ est intègre, on a

$$\deg(\bar{P}) + \deg(\bar{Q}) = \deg(\bar{P}\bar{Q}) = \deg(1) = 0$$

ce qui assure que $\bar{P}, \bar{Q}$ sont constants, *ie* $\bar{a}_i = 0, i > 0$ ou encore $a_i \in \mathfrak{p}, i > 0$. Mais ceci assure que $a_i, i > 0$ est nilpotent. Par ailleurs,

$$1 = P(0)Q(0) = a_0Q(0)$$

ce qui assure que a_0 inversible dans A. Inversement, supposons $P = a_0 + \cdots + a_nX^n$ avec $a_i, i > 0$ nilpotents et a_0 inversible. On peut certainement supposer $n > 0$. Quitte à diviser par a_0 qui est inversible, on peut supposer $a_0 = 1$. Soit N assez grand tel que $a_i^N = 0, i > 0$. Une application facile de la formule du binôme prouve qu'on a

$$(a_1X + \cdots + a_nX^n)^{nN} = 0$$

et on applique le lemme 15.1.■

16. Parenthèse sur les catégories, I

Les correspondances F et G de 6.1.a sont des exemples de foncteurs de la catégorie des ensembles dans celle des modules. Sans rentrer dans les détails, disons qu'une *catégorie* $\mathcal{C}$ est la donnée d'un ensemble (ou d'une classe plus généralement) d'*objets* (ici les modules) et de *flèches* (ici les homomorphismes de modules). Il existe deux applications, dites *source* et *but*, des flèches vers les objets. On note alors une flèche $f : A \to B$, où A est la source et B le but et on note $\mathrm{Hom}_{\mathcal{C}}(A, B)$ ou simplement $\mathrm{Hom}(A, B)$ l'ensemble des flèches (c'est par hypothèse un « vrai » ensemble, pas seulement une classe. On se donne une loi de composition associative qui permet de composer les flèches dont les but et source coïncident respectivement. Enfin, $\mathrm{Hom}(A, A) = \mathrm{End}(A)$ est muni d'un élément marqué noté Id_A (« l'identité de A »), tel que

$$f \circ \mathrm{Id}_A = \mathrm{Id}_B \circ f = f.$$

On dit qu'une flèche $A \to B$ est un *isomorphisme* s'il existe une flèche $B \to A$ telle que les composés

$$A \to B \to A \text{ et } B \to A \to B$$

soient les identités respectives de A et B. Si $\mathcal{C}$ est une catégorie, on note C^{opp} la catégorie opposée de $\mathcal{C}$ dont les objets sont ceux de $\mathcal{C}$, mais telle que

$$\mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A).$$

Par exemple, on a une notion évidente de catégorie des ensembles (notée $\mathcal{E}ns$), des espaces vectoriels sur un corps k...
Un *foncteur* F entre deux catégories C_1 et C_2 associe à tout objet de C_1 un objet de C_2 et à toute flèche $c_1 \to c_1'$ dans C_1 une flèche dans $F(c_1) \to F(c_1')$, de façon compatible avec les compositions. On parle parfois de foncteur covariant de $\mathcal{C}_1$ dans $\mathcal{C}_2$.

***Exemple 16.1* (Foncteur des points).** — *Soit c un objet de $\mathcal{C}$. Le foncteur h_c de $\mathcal{C}$ dans $\mathcal{E}ns$ est défini par*
-Image des objets : $h_c(M) = \mathrm{Hom}(c, M)$.
-Image des flèches : si $M \to N$ est un morphisme, l'image de $(c \to M) \in h_C(M)$ est le composé $(c \to M \to N) \in \mathrm{Hom}(c, N) = h_c(N)$.

Un foncteur de $\mathcal{C}$ dans la catégorie $\mathcal{E}ns$ des ensembles Un foncteur *contravariant* de $\mathcal{C}_1$ dans $\mathcal{C}_2$ est un foncteur de $\mathcal{C}_1$ dans $\mathcal{C}_2^{\mathrm{opp}}$.

Exemple 16.2. — *Si $\mathcal{C}$ une catégorie et c objet, on définit un foncteur contravariant à valeurs dans $\mathcal{E}ns$ de $\mathcal{C}$ dans $\mathcal{C}$ de la manière suivante :*
-Objets : $F(M) = \mathrm{Hom}(M, c)$.
-Flèches : si $M \to N$ est un morphisme, l'image de $N \to c \in F(N) = \mathrm{Hom}(N, c)$ est le composé

$$M \to N \to c \in \mathrm{Hom}(M, c) = F(M).$$

Noter que F est le foncteur des points de c vu comme objet de $\mathcal{C}^{\mathrm{opp}}$.

Si on a deux tels foncteurs F, G, une collection de flèches i_{c_1} entre $F(c_1)$ et $G(c_1)$ compatibles avec la composition dans C_1 est un *morphisme de foncteurs.*

Exemple 16.3. — *Avec les notations précédentes, on observe qu'un morphisme $f : c \to c'$ dans $\mathcal{C}$ induit un morphisme de foncteurs $h_{c'} \to h_c$ noté $h(f)$.*

Si de plus, i_{c_1} est un isomorphisme pour tout c_1, alors on dit que i est un *isomorphisme de foncteurs* et on note $i : c \Rightarrow c'$.

***Exercice 16.4* (Lemme de Yoneda).** — *Montrer que l'application*

$$\mathrm{Hom}(c, c') \overset{f \mapsto h(f)}{\to} \mathrm{Hom}(h_{c'}, h_c)$$

est bijective.

Le sens de l'exercice précédent est que le foncteur h_c caractérise c à isomorphisme unique près. Aussi étrange que cela puisse paraître, cette remarque est fondamentale et... utile (cf. *infra* le produit tensoriel par exemple).

Exercice 16.5. — *Soit C la catégorie dont les objets sont les entiers naturels et les flèches $n \to m$ les matrices réelles de taille (m, n). On associe à n le $\mathbf{R}$-espace vectoriel $F(n) = \mathbf{R}^n$ et à $M \in M_{m,n}$ le morphisme de $F(n)$ dans $F(m)$ défini par M dans les bases canoniques. Vérifier que F est un foncteur dans la catégorie des $\mathbf{R}$-espaces vectoriels.*

17. Un critère d'exactitude universel

On a vu des exemples de caractérisation de certains modules M_1 par le foncteur $M \mapsto \mathrm{Hom}(M_1, M)$. Donnons en ces termes un critère d'exactitude d'un complexe

$$M_1 \overset{j}{\to} M_2 \overset{p}{\to} M_3 \to 0. \tag{17.a}$$

Donnons une condition nécessaire. Tout d'abord, pour tout M, on a un complexe

$$0 \to \mathrm{Hom}(M_3, M) \to \mathrm{Hom}(M_2, M) \to \mathrm{Hom}(M_1, M) \tag{17.b}$$

qui est exact « au bout à gauche » visiblement. Mais, par propriété universelle du quotient, p se factorise à travers $j(M_1)$ et on a une suite exacte $0 \to M_2/j(M_1) \to M_3 \to 0$ *ie* un isomorphisme canonique $M_2/j(M_1) \overset{\sim}{\to} M_3$. Si maintenant

$f_2 \in \mathrm{Hom}(M_2, M)$ a son image nulle dans $\mathrm{Hom}(M_1, M)$, ceci signifie que f_2 est nulle sur $j(M_1)$ et donc se factorise à travers $M_2/j(M_1) \xrightarrow{\sim} M_3$, autrement dit provient de $\mathrm{Hom}(M_3, M)$. Ainsi, la suite 17.b est exacte pour tout M.

Lemme 17.1. — *Le complexe 17.a est exact si et seulement si la suite 17.b est exacte pour tout M.*

Preuve : La partie directe vient d'être prouvée. Supposons donc 17.b exacte pour tout M. Vérifions la surjectivité de p. Posons $M = M_3/\mathrm{Im}(p)$. La surjection canonique $s \in \mathrm{Hom}(M_3, M)$ a une image nulle dans $\mathrm{Hom}(M_2, M)$, et donc est nulle. Mais ceci assure que $s(M_3) = 0$. Or, $M = M_3/p(M_2)$ (surjectivité de s) et donc p est surjective.
Montrons l'exactitude au milieu. Comme plus haut, p se factorise à travers $j(M_1)$ pour donner un morphisme $\bar{p} : \ M_2/j(M_1) \to M_3$. Dire que la suite est exacte, c'est dire que cette flèche est injective (et en fait bijective, puisqu'on sait déjà qu'elle est surjective). On va construire un inverse de $\bar{p}$.
Posons $M = M_2/j(M_1)$ à nouveau. Comme la flèche quotient

$$q : \ M_2 \to M_2/j(M_1) = M$$

a une image nulle dans $\mathrm{Hom}(M_1, M)$, elle provient d'une flèche (unique) $s \in \mathrm{Hom}(M_3, M)$ telle que $q = s \circ p$. Autrement dit,on a un diagramme commutatif

$$\begin{array}{ccc} M_2 & \xrightarrow{q} & M_2/j(M_1) \\ {\scriptstyle q}\swarrow & \downarrow{\scriptstyle p} & \nearrow{\scriptstyle s} \\ M_2/j(M_1) & \xrightarrow{\bar{p}} & M_3 \end{array}$$

Ainsi, on $s\bar{p}q = q$ et donc $s\bar{p} = \mathrm{Id}$ car q est surjectif. Mais ceci assure visiblement l'injectivité de $\bar{p}$, qui est surjectif comme p : c'est un isomorphisme d'inverse s.■

18. Le lemme du serpent

Rappelons qu'un diagramme de modules

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$$

est appelé une suite exacte (à trois termes) si et seulement si le noyau de f_2 est aussi l'image de f_1. Il est important de comprendre que la condition plus faible d'inclusion $\mathrm{Im}(f_1) \subset \ker(f_2)$ signifie que le composé $f_2 \circ f_1$ est nul. On dit dans ce cas que la suite est un **complexe**.
Avec ces notations, si M_1 est nul, dire que la suite est exacte c'est dire que f_2 est injectif et dire que M_3 est nul c'est dire que f_1 est surjectif. On généralise de façon évidente pour des suites plus longues.
Considérons un diagramme commutatif de modules à lignes exacte

$$\begin{array}{ccccccc} & & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 \end{array}$$

Il induit deux diagrammes

$$\ker(f_1) \longrightarrow \ker(f_2) \longrightarrow \ker(f_3)$$

et

$$\mathrm{Coker}(f_1) \longrightarrow \mathrm{Coker}(f_2) \longrightarrow \mathrm{Coker}(f_3) \ .$$

Lemme 18.1. — *Les deux lignes précédentes sont exactes.*

Preuve : Vérifions l'exactitude de la seconde par exemple. Soit donc n_2 un représentant d'une classe de $\mathrm{Coker}(f_2)$ nulle dans $\mathrm{Coker}(f_3)$. Ceci signifie que l'image n_3 de n_2 dans M_3 est en fait dans $\mathrm{Im}(f_3)$ et donc s'écrit $f_3(m_3)$. Comme $M_2 \to M_3$ est surjective, m_3 provient de $m_2 \in M_2$. Ainsi $f_2(m_2)$ et n_2 ont même image dans M_3, donc diffèrent par un élément $n_1 \in N_1$. Mais la classe $f_2(m_2)$ est nulle dans $\mathrm{Coker}(f_2)$ ce qui prouve que la classe de n_2 est l'image de la classe de n_1. Inversement, c'est plus facile. Si n_1 représente une classe de $\mathrm{Coker}(f_1)$, son image dans n_3 est nulle (une suite exacte est un complexe) et donc sa classe dans le conoyau aussi.■

***Proposition 18.2* (Lemme du serpent).** — *Sous les conditions précédentes, il existe un flèche canonique* $\ker(f_3) \to \mathrm{Coker}(f_1)$ *telle que la suite*

$$\begin{array}{ccccccc} \ker(f_1) & \longrightarrow & \ker(f_2) & \longrightarrow & \ker(f_3) & & \\ & & & \overset{\mathrm{d}}{\searrow} & & & \\ \mathrm{Coker}(f_1) & \longrightarrow & \mathrm{Coker}(f_2) & \longrightarrow & \mathrm{Coker}(f_3) & & \end{array}$$

soit exacte.

Preuve : Définissons d. Partons de m_3 nul dans N_3. Choisissons un antécédent m_2 de m_3 dans M_2. L'image de $f_2(m_2)$ dans N_3 est nulle et donc provient d'un élément $n_1 \in N_1$. L'élément m_2 est défini à l'image M_1' de M_1 dans M_2 près. Donc, $f_2(m_2)$ est défini à $f_2(M_1')$ près qui est aussi l'image de $f_1(M_1)$ dans N_2. Ainsi, la classe de n_1 dans $\mathrm{Coker}(f_1)$ ne dépend que de m_3 et pas du choix de l'antécédent. La correspondance $m_3 \mapsto \bar{n}_1$ définit d qui est visiblement un morphisme. Le fait que la suite soit un complexe est clair.
Vérifions par exemple que le noyau de d est le conoyau de $\ker(f_2) \to \ker(f_3)$. Comme on a remarqué que notre suite est un complexe, partons de $m_3 \in \ker(d)$ dont l'image n_1 est nulle dans $\mathrm{Coker}(f_1)$. Ceci signifie qu'un antécédent m_2 de m_3 a une image $f_2(m_2) \in N_1$ (N_1 vu comme sous-module de N_2) nulle dans $\mathrm{Coker}(f_1)$ et donc s'écrit $f_1(m_1)$. Si m_1' est l'image de m_1 dans M_2, on a alors $f_2(m_2 - m_1') = 0$ et $m_2 - m_1'$ se projette sur m_3, qui donc provient de $\ker(f_2)$. L'exactitude en $\mathrm{Coker}(f_1)$ se vérifie de même.■

Comme souvent dans ce genre de preuve, il est fortement conseillé de « suivre » les éléments sur des diagrammes (c'est ce qu'on appelle la *chasse au diagramme*) plutôt que de nommer toutes les flèches et tous les éléments qu'on considère ce qui rend rapidement les preuves illisibles.

***Exercice 18.3* (Lemme des 5).** — *Supposons qu'on a un diagramme commutatif de modules à lignes exactes*

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

Montrer que si

– *si f_1 surjective et f_2, f_4 injectives, alors f_3 injective ;*

– *si f_5 injective et f_2, f_4 surjectives, alors f_3 surjective.*

[on pourra faire une chasse au diagramme ou utiliser le lemme du serpent]

La conséquence à retenir est que si f_1, f_2, f_4, f_5 sont des isomorphismes, il en est de même de f_3.

19. Scindages

Partons de deux A-modules M_1, M_3. La projection $p:\ M_2 = M_1 \oplus M_3 \twoheadrightarrow M_3$ définit une suite exacte

$$0 \to M_1 \to M_2 \xrightarrow{p} M_3 \to 0.$$

Le morphisme $s:\ M_3 \to M_2$ définit par $s(m_3) = (0, m_3)$ vérifie $p \circ s = \mathrm{Id}_{M_3}$.

Définition 19.1. — *Une section d'un morphisme $p:\ M_2 \to M_3$ est un morphisme $s:\ M_3 \to M_2$ qui vérifie $p \circ s = \mathrm{Id}_{M_3}$. Une suite exacte*

$$0 \to M_1 \to M_2 \xrightarrow{p} M_3 \to 0$$

est dite scindée si p admet une section.

Observons d'abord qu'un morphisme p qui admet une section est nécessairement surjectif. Observons ensuite qu'une section n'est en général pas unique : la différence de deux sections est à valeurs dans le noyau M_1 de p et ainsi on peut rajouter à n'importe quelle section s un morphisme de M_3 dans M_1 pour obtenir une autre section. Toutefois, contrairement à l'algèbre linéaire, les morphismes surjectifs n'admettent en général pas de section.

Exercice 19.2. — *Montrer que si $n \geq 1$, la surjection $\mathbf{Z} \twoheadrightarrow \mathbf{Z}/n\mathbf{Z}$ n'admet pas de section.*

Lemme 19.3. — *Si la suite exacte*

$$0 \to M_1 \xrightarrow{j} M_2 \xrightarrow{p} M_3 \to 0$$

est scindée, alors $M_2 \xrightarrow{\sim} M_1 \oplus M_3$.

Preuve : Soit s une section de p. Alors, le morphisme $(m_1, m_3) \mapsto j(m_1) + s(m_3)$ est injectif. En effet, l'image par p d'un élément du noyau vérifie $ps(m_3) = m_3 = 0$ (car $pj = 0$) et donc $j(m_1) = 0$ ce qui entraîne $m_1 = 0$ car j injectif. Mais il est aussi surjectif. En effet, si $m_3 = p(m_2)$, la différence $m_2 - s(m_3)$ est dans le noyau de p donc s'écrit $j(m_1)$.■

20. Conditions de finitude

Comme dans le cas des espaces vectoriels, on dit qu'un A-module est de *type fini* si il existe une surjection $\phi:\ A^n \twoheadrightarrow M$. Autrement dit, ceci signifie qu'il existe $m_1, \cdots, m_n \in M$ tel que tout élément de M soit combinaison linéaire des m_i. En effet, si une telle famille existe, le morphisme

$$(a_i) \mapsto \sum a_i m_i$$

de A^n dans M est surjectif et, inversement, si un tel ϕ existe, la famille $m_i = \phi(0, \cdots, 0, 1, 0, \cdots, 0)$ (1 à la i-ème place) convient.

Exercice 20.1. — *Montrer que tout idéal de $\mathbf{Z}$ est de type fini. Montrer qu'en revanche l'idéal de $\mathcal{F}(\mathbf{R}, \mathbf{R})$ des fonctions à support compact n'est pas de type fini.*

Dans le cas des k-espaces vectoriels, si un espace vectoriel est de type fini (*ie* de dimension finie), il existe une donc une surjection $k^n \twoheadrightarrow E$. Le noyau N est alors un sous-espace vectoriel d'un espace de dimension finie et donc lui aussi est de dimension finie. Il existe donc une surjection $k^m \twoheadrightarrow N$ de sorte qu'on a une suite exacte

$$k^m \to k^n \to E \to 0.$$

Définition 20.2. — *On dit qu'un A-module M est de présentation finie s'il existe des entiers naturels n, m et une suite exacte*

$$A^m \to A^n \to M \to 0.$$

Ainsi, la condition « de présentation finie » est plus forte que celle de « de type fini ». La signification de l'existence d'une présentation finie est la suivante. Se donner une surjection $A^n \twoheadrightarrow M$, c'est se donner des images $m_i \in M$ de la base canonique de A^n qui engendrent M. Autrement dit, ceci signifie qu'on s'est donné une **famille génératrice finie**. Le noyau de la flèche est l'ensemble R des n-uples $r = (a_1, \cdots, a_n)$ de A^n tels que $\sum a_i m_i = 0$, autrement dit c'est le **module des relations** entre les m_i. Se donner une présentation comme plus haut, c'est se donner une surjection $A^m \twoheadrightarrow R$, autrement dit c'est se donner une famille $r_1, \cdots, r_m$ de relations entre les m_i qui engendre R. Autrement dit, toute relation r entre les m_i est combinaison linéaire des relations r_j.

Exercice 20.3 **(Difficile)**. — *Soit A l'anneau des fonctions de $\mathbf{R}^2$ dans $\mathbf{R}$ et M l'idéal engendré par x, y, le fonctions coordonnées. Montrer que le noyau de la surjection*

$$A^2 \xrightarrow{(x,y)} M \longrightarrow 0$$

n'est pas de type fini. [Utiliser l'exercice précédent].

21. Présentation du $k[X]$-module associé à un endomorphisme

On se donne donc un k-espace vectoriel de dimension finie muni d'un endomorphisme f. On note M le $k[X]$-module associé (on rappelle que comme ensemble, il se réduit à E et que X opère comme f). On note $E[X]$ les polynômes à coefficients dans E, somme finies formelles du type $\sum e_i X^i$ où $e_i \in E$. Autrement dit, c'est la somme directe $E^{(\mathbf{N})}$. C'est un k espace vectoriel, et même naturellement un $k[X]$-module, grâce à la règle $X.\sum e_i X^i = \sum e_i X^{i+1}$.

Lemme 21.1. — *Le $k[X]$-module $E[X]$ est libre de rang* $\dim_k(E)$.

Preuve : Soit $\epsilon_1 \cdots, \epsilon_n$ une base de E. Alors, l'application

$$\begin{cases} (k[X])^n & \to & E[X] \\ (P_i(X)) & \mapsto & \sum P_i(X)\epsilon_i \end{cases}$$

est un isomorphisme de $k[X]$ modules.■

On a une surjection k-linéaire canonique $\pi :\ E[X] \twoheadrightarrow E$ qui à $\sum e_i X^i$ associe $\sum f^i(e_i)$ (on remplace X par f et on évalue les coefficients). Par construction, elle est même $k[X]$-linéaire. En effet,

$$\pi(X.\sum e_i X^i) = \pi(\sum e_i X^{i+1}) = \sum f^{i+1}(e_i) = f\sum(f^i(e_i)) = Xf^i(e_i) = X.\pi(\sum e_i X^i),$$

ce qui entraîne la $k[X]$-linéarité.
Notons encore f l'endomorphisme de $E[X]$ défini par $\sum e_i X^i \mapsto \sum f(e_i)X^i$. C'est un morphisme de $k[X]$-modules. Le lecteur réinterprétera cette construction lorsqu'on aura étudié le produit tensoriel. En effet, $E[X]$ s'identifie à $k[X] \otimes_k E$ et on regarde les morphismes $1 \otimes f$ et $X\mathrm{Id}$.

Lemme 21.2. — *La suite*

$$0 \longrightarrow E[X] \xrightarrow{X\mathrm{Id}-f} E[X] \xrightarrow{\pi} M \longrightarrow 0$$

est une présentation finie de M.

Preuve : Vérifions que c'est un complexe. On a en effet

$$\pi \circ (X\mathrm{Id} - f)(\sum e_i X^i) = \pi(\sum (e_i X^{i+1} - f(e_i)X^i)) = \sum f^{i+1}(e_i) - \sum f^i(f(e_i)) = 0.$$

Vérifions l'exactitude au milieu. Soit donc $v = \sum e_i X^i$ un élément de $\ker(\pi)$, *ie* tel que $\sum f^i(e_i) = 0$. On a alors

$$v = v - \sum f^i(e_i) = \sum (X^i\mathrm{Id} - f^i)(e_i)$$

de sorte qu'il reste à se convaincre que $X^i\mathrm{Id} - f^i$ est un multiple de $X\mathrm{Id} - f$ dans $\mathrm{End}(E[X])$. Mais on a la formule de la progression géométrique (valable pour deux éléments d'un anneau qui commutent),

$$a^i - b^i = (a-b)\sum_{j=0}^{i-1}(a^j b^{i-1-j})$$

qui appliquée à $a = X\mathrm{Id}$ et $b = f$ dans l'anneau $\mathrm{End}(E[X])$ donne ce qu'on veut.
La surjectivité de π est claire.
Reste l'injectivité de $X\mathrm{Id} - f$. Mais si $v = \sum e_i X^i$ est dans le noyau, on a

$$\sum (e_i X^{i+1} - f(e_i)X^i) = 0$$

de sorte que pour tout $i \geq 0$ on a $e_i = f(e_{i+1})$. On a donc l'implication $(e_{i+1} = 0) \Rightarrow (e_i = 0)$. Comme e_i est nul pour $i >> 0$, on une récurrence descendante montre la nullité de e_i pour tout i.■

22. Interprétation calculatoire

On a vu que se donner une surjection $A^n \twoheadrightarrow M$ c'est se donner n éléments de M engendrant m. Le noyau N de cette surjection est par définition le sous-module des n-uple $r = (a_1, \cdots, a_n)$ tels que $\sum a_i m_i = 0$, autrement dit c'est l'ensemble des relations entre les m_i. Dire que M est de présentation signifie qu'il existe une surjection $A^m \twoheadrightarrow N$ (exercice), autrement dit qu'il existe m éléments $r_j = (a_{j,1}, \cdots, a_{j,n})$ de A^n qui sont des relations entre les m_i et tels que toute autre relation $r = (a_1, \cdots, a_n)$ entre les m_i s'obtienne à partir des r_i.
Regardons un exemple. Soit A l'anneau de polynôme $\mathbf{C}[x, y]$ et soit P, Q deux polynômes sans facteurs communs. Soit M l'idéal engendré par P, Q. On a une surjection $A^2 \twoheadrightarrow M$ définie par les générateurs P, Q de M. On vérifie sans peine que le noyau de cette surjection est l'ensemble des couples (U, V) tels que $UP + VQ = 0$. Comme P, Q sont sans facteurs commun, ceci n'est possible que si (U, V) s'écrit $a(Q, -P)$ pour $a \in A$. Ceci signifie que la suite

$$A \xrightarrow{\begin{pmatrix} Q \\ -P \end{pmatrix}} A^2 \xrightarrow{(P,Q)} M \longrightarrow 0$$

est exacte et que M est de présentation finie. On va étudier une bonne classe d'anneaux pour lesquels tout sous-module d'un module de type fini est de encore de type fini, et donc en fait de présentation fini : les anneaux **noethériens**.

PARTIE II

MODULES ET ANNEAUX NOETHÉRIENS

En algèbre linéaire, tout sous-espace vectoriel d'un espace vectoriel de dimension finie est de dimension finie. On a vu qu'il existait des anneaux (en l'occurrence celui des fonctions de $\mathbf{R}$ dans $\mathbf{R}$) et des sous-modules d'un module de type fini (en l'occurrence l'idéal des fonctions à support compact) qui ne sont pas de type fini. La condition de noethérianité interdit cette pathologie.

1. Modules noethériens

On dira qu'un A-module M est noethérien si tout sous-module de M est de type fini. En particulier, M est de type fini.

Proposition 1.1. — *On se donne une suite exacte de A-modules*

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

Alors, M_1, M_3 sont noethériens si et seulement si il en est de même de M_2.

En particulier, tout quotient et tout sous-module d'un module noethérien est noethérien. Tout module somme de modules noethérien est noethérien.
Soit F un ensemble de partie d'un ensemble E. Rappelons qu'on dit que $M \in F$ est maximal dans F si on a

$$M' \in F \text{ et } M \subset M' \Rightarrow M = M'.$$

Ainsi, dire que M n'est pas maximal c'est dire qu'il existe $M' \in F$ contenant strictement M. Pour prouver la proposition, prouvons le lemme suivant.

Lemme 1.2. — *Les trois propositions suivantes sont équivalentes :*
i) M est noethérien ;
ii) toute suite croissante de sous-modules de M est stationnaire ;
iii) toute famille non vide de sous-modules de M admet un élément maximal.

Preuve : $i \Rightarrow ii$. Soient $n_1, \cdots, n_n$ une famille finie engendrant le sous-module $\cup M_i$ réunion croissante de la suite $M_i, i \in \mathbf{N}$. Choisissons l assez grand de sorte que $n_i \in M_l, i = 1 \cdots, n$. Alors, $M_i = M_l$ si $i \geq l$.
*$ii \Rightarrow iii$.*Supposons qu'une famille non vide de sous-modules de F soit sans élément maximal. On choisit un module $M_0 \in F$. Comme M_0 non maximal, on choisit $M_1 \in F$ contenant strictement M_0. Par récurrence, on construit une suite M_i strictement croissante, ce qui est absurde.
$iii \Rightarrow i$. Soit N un sous-module de M. Soit F la famille des sous-modules de N qui sont de type fini. Elle est non vide (elle contient le module nul). Soit N' un élément maximal de F. Soit $n \in N$. Comme $N' + An$ est de type fini et est contenu dans N, il est dans F et visiblement contient N'. Ainsi, il est égal à N' et donc $n \in N'$ pour tout $n \in N$ de sorte que $N' = N \in F$ et N de type fini.■

Preuve de la proposition : Supposons les extrêmes noethériens. Si $M_{2,i}$ est une suite croissante de sous-modules de M_2, la suite croissante $p(M_{2,i})$ de sous-modules de M_3 stationne pour $i \geq l$. Le noyau de p restreint à $M_{2,i}$ est un sous-module $M_{1,i}$ de M_1. La suite de ces noyaux stationne pour $i \geq l'$. Et la suite des $M_{2,i}$ stationne pour $i \geq l, l'$.

Inversement, supposons M_2 noethérien. Montrons que M_1 est noethérien. Une suite croissante de sous-modules de M_1 a une image par j qui stationne donc stationne, ce qu'on voulait. Pour M_3, on constate que l'image inverse par p d'une suite croissante de sous-modules de M_3 stationne, donc son image par p également : mais c'est la suite initiale car p est surjectif.■

2. Anneaux noethériens

On dit qu'un anneau est noethérien si tout idéal est de type fini (*ie* engendré par un nombre fini d'éléments). Par exemple les corps, les anneaux principaux sont noethériens. L'hypothèse A noethérien signifie exactement que A, vu comme module sur lui-même, est un module noethérien. En particulier, on a d'après ce qui précède :

Lemme 2.1. — *Les trois propositions suivantes sont équivalentes :*
i) A est noethérien ;
ii) toute suite croissante d'idéaux de A est stationnaire ;
iii) toute famille non vide d'idéaux de A admet un élément maximal.

L'intérêt de ces anneaux réside en particulier dans la proposition suivante.

Proposition 2.2. — *Soit A un anneau noethérien. Alors, un A-module est noethérien si et seulement si il est de type fini. Tout A-module de type fini est de présentation finie.*

Preuve : On sait en général qu'un module noethérien est de type fini. Inversement, supposons M de type fini. Mais on sait alors que A^n est noethérien pour tout n. Soit alors $m_1, \cdots, m_n$ une famille génératrice finie de M, définissant une surjection $A^n \twoheadrightarrow M$. Mais alors, M est un quotient de A^n noethérien, et donc est noethérien. Pour le dernier point, on observe que le noyau de cette surjection est noethérien, donc de type fini.■

3. Construction d'anneaux noethériens : transfert I

Le plus simple pour construire un anneau est sans doute la construction de l'anneau quotient.

Proposition 3.1. — *Tout anneau quotient d'un anneau noethérien est noethérien.*

Preuve : Une suite croissante d'idéaux du quotient A/I donne par image inverse une suite croissante d'idéaux de A qui stationne par noethérianité de A, et donc stationne elle-même.■

Si on n'avait que ce critère, on aurait à notre disposition essentiellement les produits de corps et de quotients d'anneaux principaux, ce qui n'est pas grand-chose. L'énoncé suivant enrichit considérablement notre liste, puisqu'il donne **tous les quotients d'anneaux de polynômes à plusieurs variables sur un anneau noethérien.**

***Théorème 3.2* (Théorème de transfert d'Hilbert)**. — *Si A est noethérien, l'anneau de polynôme $A[X]$ est noethérien.*

Preuve : Soit I un idéal de $A[X]$. Soit J la réunion de 0 et tous les coefficients dominants des éléments non nuls de I. C'est un idéal de A (exercice), qui est donc de type fini. Soient $P_1, \cdots, P_n$ un système fini d'éléments non nuls de J dont les coefficients dominants engendrent J (on peut supposer I non nul et $n > 0$). Soit d le plus grand des degré d_i des P_i. Si P est de degré $\delta \geq d$, son coefficient dominant $dom(P)$ s'écrit sous la forme $\sum a_i dom(P_i)$ et

$$P - \sum a_i x^{\delta - d_i} P_i$$

a un degré $< \deg(P)$. De proche en proche, on trouve que P est somme d'un élément de l'idéal $< P_1, \cdots, P_n >$ engendré par les P_i et d'un élément de I_d, ensemble des éléments de I de degré $< d$. Mais I_d comme un A-sous-module du A-module $A_{<d}[X] \xrightarrow{\sim} A^d$. Comme A noethérien, A^d est un module noethérien et I_d est de type fini (comme A-module). Choisissons $Q_1, \cdots, Q_m$ engendrant I_d comme A-module. Ainsi, I_d est engendré, comme $A[X]$-module, par $Q_1, \cdots, Q_m, P_1, \cdots, P_n$.■

4. Décomposition en facteurs premiers

Supposons dans cette section que A est intègre.

Définition 4.1. — *Un élément non nul p d'un anneau A est dit irréductible s'il est non nul et si on a la propriété suivante : si p s'écrit $p = ab$ dans A, alors a ou b est inversible dans A.*

Par exemple, les irréductibles de $\mathbf{Z}$ sont les nombres premiers et leurs opposés.

Exercice 4.2. — *Montrer que deux idéaux principaux aA et bA sont égaux si et seulement si $a = ub$ u inversible de A (on alors dit que a et b sont associés). Montrer que p est irréductible si les seuls diviseurs de p sont inversibles ou associés à p.*

Faisons le lien entre irréductible et premier.

Lemme 4.3. — *Soit p non nul dans A intègre. Si $(p) = pA$ est premier, alors p est irréductible.*

Preuve : Comme pA est premier, il est différent de A et donc p non inversible. Si $p = ab$, alors $ab \in pA$ qui est premier, donc, par exemple $a \in pA$. Il existe donc $\alpha \in A$ tel que $a = p\alpha$ de sorte que $p = p\alpha b$. Comme p est non nul dans A intègre, on peut simplifier par p ce qui donne $\alpha b = 1$, et donc b inversible.■

La réciproque est fausse en général.

Exercice 4.4. — *On considère l'anneau $A = \mathbf{R}[x, y]/(x^2 - y^3)$. Montrer que A est intègre. Montrer que la classe de x est irréductible mais que pourtant xA n'est pas premier.*

Définition 4.5. — *Soit A un anneau intègre. On dit que le lemme d' Euclide est vrai dans A si l'idéal engendré par un élément irréductible est premier.*

Notons que dire (p) premier c'est dire p non inversible et $p|ab$ entraîne $p|a$ ou $p|b$, ce qui est l'énoncé habituel dans $\mathbf{Z}$ par exemple : le lemme d' Euclide est vrai dans $\mathbf{Z}$.

Proposition 4.6 **(Existence de décomposition en facteurs premiers)**. — *Dans un anneau noethérien intègre, tout élément non nul se décompose en un produit de facteurs irréductibles et d'un inversible.*

Preuve : Soit F la famille des idéaux principaux non nuls aA de A tels que a n'est pas un tel produit. Si F était non vide, cette famille d'idéaux aurait un élément maximal a, qui en particulier n'est pas irréductible. Donc $a = bc$ et ni b ni c ne sont inversibles. De plus, ou b ou c n'est pas un tel produit, Disons b. Mais alors, on a $aA \subset bA$ et $bA \in F$ donc $aA = bA$. Il existe (intégrité) alors un inversible u de A tel que $a = ub$ et donc $c = u$ ce qui n'est pas.■

Tout le problème est qu'en général on n'a **pas de propriété d'unicité** de la décomposition. Par exemple, dans le cas $A = \mathbf{R}[x, y]/(x^2 - y^3)$, la classe de x^2 est le carré de l'irréductible x (vérifier que x est irréductible), mais c'est aussi le cube de l'irréductible y. Pourtant, x et y ne sont pas associés : on a au moins deux décompositions. On reviendra sur les anneaux pour lesquels on a unicité (les anneaux factoriels).

5. Parenthèse sur les catégories, II

Soit $\mathcal{C}$ une catégorie. On reprend les notations de la section I.16

5.1. Équivalence de catégories. — La notion de bijection entre ensembles est remplacée dans le cadre des catégories par celle d'équivalence de catégorie.

Définition 5.2. — *Un foncteur de $\mathcal{C}$ dans $\mathcal{C}'$ est dit une équivalence de catégorie s'il est essentiellement surjectif, ie si tout objet de $\mathcal{C}'$ est isomorphe à l'image par F d'un élément de $\mathcal{C}$ et pleinement fidèle, ie si l'application induite par F*

$$\mathrm{Hom}_{\mathcal{C}}(c, c') \to \mathrm{Hom}_{\mathcal{C}'}(F(c), F(c'))$$

est bijective.

Par exemple, on vérifie sans peine que le foncteur F de l'exercice I.16.5 est une équivalence de catégorie.

Définition 5.3. — *Un foncteur G de $\mathcal{C}'$ dans $\mathcal{C}$ est dit quasi-inverse de F si $F \circ G \Rightarrow \mathrm{Id}_{\mathcal{C}'}$ et $G \circ F \Rightarrow \mathrm{Id}_{\mathcal{C}'}$.*

Exercice 5.4. — *Montrer que F est une équivalence de catégorie si et seulement si F admet un quasi-inverse.*

Définition 5.5. — *On dit qu'une flèche $a \to b$ est un monomorphisme (resp. épimorphisme) si pour tout objet c la flèche* $\mathrm{Hom}(c, a) \to \mathrm{Hom}(c, b)$ *est injective (resp. la flèche* $\mathrm{Hom}(a, c) \to \mathrm{Hom}(b, c)$ *est injective.*

Par exemple, on vérifie sans difficulté que les monomorphismes de la catégorie des ensembles, ou de celle des modules sont les morphismes injectifs alors que les épimorphismes de ces catégories sont les morphismes surjectifs. L'intérêt est que ces notions sont invariantes par équivalence de catégorie.

5.6. Foncteur représentables. — Un foncteur F (covariant) de $\mathcal{C}$ dans $\mathcal{E}ns$ est dit représentable s'il existe un objet c de $\mathcal{C}$ et un isomorphisme de foncteurs $h_c \Rightarrow F$ du foncteur des points h_c de c dans F. L'image de Id_c dans $F(c)$ est dit objet universel.
Notons d'abord que si on a autre isomorphisme $h_{c'} \Rightarrow F$, on a alors un isomorphisme $h_c \Rightarrow h_{c'}$ induit (lemme de Yoneda) par un unique isomorphisme $c \xrightarrow{\sim} c'$ dans $\mathcal{C}$. Autrement dit, si un foncteur est représentable par un objet c, cet objet est unique à isomorphisme unique près. On parlera de l'objet qui représente F.
Par exemple, si $M_i, i \in I$ est une famille de A-modules, le foncteur $M \mapsto \prod_i \mathrm{Hom}(M_i, M)$ est représentable par $\oplus_{in \in I} M_i$.

5.7. Noyau, conoyau de double flèche. — Une double flèche de $\mathcal{C}$ est un couple de flèches (f, g) où f, g sont des flèches de même source c et de même but c'. On note $c \rightrightarrows c'$. Considérons le foncteur K de $\mathcal{C}$ dans $\mathcal{E}ns$ défini comme suit :
Pour tout objet b de c, l'ensemble $F(c)$ est le sous ensemble de $\mathrm{Hom}_{\mathcal{C}}(b, c)$ des morphismes m tels que $f \circ m = g \circ m$.

Définition 5.8. — *Dans le cas où K est représentable par une flèche $k \to c$ de $\mathcal{C}$, on dit, abusivement, que k est le noyau de la double flèche.*

Notons que l'abus de langage consistant à parler de « le » noyau et non « d'un » noyau est justifié car un représentant est unique à isomorphisme unique près. L'objet universel, image de l'identité de k, est donc un homomorphisme $j : k \to c$ tel que $f \circ j = g \circ j$. Par définition, un homomorphisme $u : a \to c$ se factorise à travers j si et seulement si $f \circ u = g \circ u$.

Exemple 5.9. — *La catégorie des ensembles, des A-modules admettent des noyaux pour toute double flèche. Par exemple, si (f, g) est une double flèche d'un module M dans N dans la catégorie des modules, on vérifie que* $\ker(f, g)$ *défini par*

$$\{m \in M \text{ tel que } f(m) = g(m)\}$$

est un noyau de la double flèche.

Définition 5.10. — *On dit que* p; $c' \to d$ *est un conoyau de la double flèche* $c' \rightrightarrows c$ *dans* $\mathcal{C}$ *si* c*'est un noyau dans* $\mathcal{C}^{\mathrm{opp}}$*, la catégorie opposée.*

L'objet universel, image de l'identité de d, est donc un homomorphisme $p : \ c' \to d$ tel que $p \circ f = p \circ g$. Par définition, un homographes $v : c' \to b$ se factorise à travers p si et seulement si $v \circ f = v \circ g$.

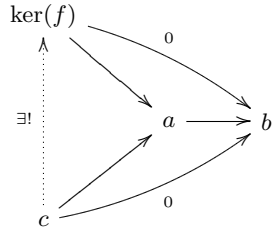
5.11. Objets initiaux, finaux, nuls. — On dit qu'un objet i de $\mathcal{C}$ est initial pour tout objet de $\mathcal{C}$, l'ensemble $\mathrm{Hom}(i, c)$ est un singloton. En passant à la catégorie opposée, on a la notion d'objet final. Un objet initial et final est dit objet nul. On vérifie sans difficulté qu'un objet initial (final, nul), est bien défini à isomorphisme unique près.

Exercice 5.12. — *Vérifier que l'ensemble vide est initial pour* $\mathcal{E}ns$ *et qu'un singloton est final et que* $\mathcal{E}ns$ *n'a pas d'objet nul. Montrer que le module nul est un objet nul de la catégorie des modules.*

On suppose que $\mathcal{C}$ a un objet nul 0. Un morphisme $a \to b$ est dit nul s'il se factorise à travers l'unique morphisme $a \to 0$, ou, ce qui revient au même, à travers l'unique morphisme $0 \to b$. Noter que le morphisme nul est unique, car $\mathrm{Hom}(a, 0)$ et $\mathrm{Hom}(0, b)$ sont des singlotons.

Exercice 5.13. — *Vérifier que composer à gauche ou à droite par un morphisme nul est un morphisme nul.*

On note 0 le morphisme nul bien entendu, un peu abusivement il faut bien l'avouer. Un noyau (conoyau) de $f : a \to b$ est par définition un noyau (conoyau) de $(f, 0)$. On notera ces flèches, quand elles existent $\ker(f) \to a$ et $b \to \mathrm{Coker}(f)$ respectivement. Comme une équivalence envoie 0 sur un objet nul, ces notions sont stables par équivalence.
La propriété universelle du noyau $\ker(f) \to a$ de $f \in \mathrm{Hom}(a, b)$ se traduit par le diagramme suivant



Exercice 5.14. — *Utiliser la propriété d'unicité du relèvement* $c \to \ker(f)$ *pour montrer que* $\ker(f) \to a$ *est un monomorphisme. On suppose donc que* $\mathcal{C}$ *a un objet nul. Montrer que le noyau d'un monomorphisme* $a \to b$ *est nul (* ie $0 \to a$ *est noyau), la réciproque étant fausse en général. Quel est le diagramme décrivant la propriété universelle du conoyau ? Énoncer et démontrer un résultat analogue pour les épimorphismes.*

Supposons que notre catégorie possède des noyaux et des conoyaux. On définit alors l'image $\mathrm{Im}(f) \to b$ de $f : a \to b$ comme le noyau de $b \to \mathrm{Coker}(f)$ et la coimage $a/\ker(f)$ comme conoyau de $\ker(f) \to \mathrm{Im}(a)$. On vérifie sans peine que f induit une flèche canonique $a/\ker(f) \to \mathrm{Im}(a)$.

PARTIE III

ANNEAUX FACTORIELS

On a observé que tout élément d'un anneau noethérien intègre est produit d'irréductibles, non uniquement en général. L'unicité est l'apanage, par définition, des anneaux factoriels.

1. Définition et caractérisation

Définition 1.1. — *On dira qu'un anneau A est factoriel, s'il est intègre et si tout élément non nul a de A s'écrit $a = up_1 \cdots p_n$ avec p_i irréductibles, u inversible et qu'une telle décomposition est unique au sens suivant : si $a = vq_1 \cdots q_m$, avec q_i irréductibles et v inversible, alors $n = m$ et il existe une bijection σ de $\{1..n\}$ telle que $(p_i) = (q_{\sigma(i)})$ soient associés pour $i = 1..n$.*

Rappelons qu'un produit vide est égal à 1 de sorte qu'on a $n = 0$ pour a inversible dans la définition précédente. Rappelons aussi que dire $(a) = (b)$ équivaut à a, b associés.

Proposition 1.2. — *Soit A un anneau dans lequel tout élément non nul admet au moins une décomposition en facteurs irréductibles. Alors, A est factoriel si et seulement si le lemme d'Euclide est vrai dans A.*

Preuve : Supposons A factoriel et soit p irréductible divisant ab. On a donc $ab = pc$ avec $c \in A$. Décomposons a, b, c en facteurs irréductibles :

$$a = \prod \alpha_i, b = \prod \alpha_j, c = \prod \gamma_k$$

où $\alpha_i, \beta_j, \gamma_k$ décrivent un ensemble (fini) d'irréductibles. On a donc

$$\prod \alpha_i \prod \beta_j = p \prod \gamma_k.$$

Comme A est factoriel, le facteur irréductible p doit être associé à un des α_i, β_j, disons α_1 par exemple. Mais ceci entraîne $p|a$, ce qu'on voulait.
Inversement, supposons que le lemme d'Euclide est vrai. Supposons qu'un élément a ait deux décompositions

$$p_1 \cdots p_n = q_1 \cdots q_m.$$

Montrons par récurrence sur n que les décompositions coïncident au sens précédent. On a p_1 divise $q_1 q_2 \cdots q_m$. Le lemme d'Euclide assure que p_1 divise un des facteurs $q_{\sigma(1)}$. Comme les diviseurs d'un irréductible qui sont non inversibles sont lui sont associés, p_1 est associé à $q_{\sigma(1)}$. On écrit alors $q_{\sigma(1)} = up_1$ avec u inversible et on simplifie par p_1 (A intègre) pour trouver

$$p_2 \cdots p_n = (uq_1) \cdots \widehat{q_{\sigma(1)}} \cdots q_m.$$

Par récurrence, on conclut d'une part $n - 1 = m - 1$ et donc $n = m$, et, d'autre part à l'existence d'une bijection

$$\sigma : \{2, \cdots, n\} \to \{1, \cdots, \widehat{\sigma(1)}, \cdots m\}$$

telle que

$$(p_i) = (q_{\sigma(i)}), i = 2, \cdots, n,$$

ce qui prouve la proposition.■

2. Rappels sur les anneaux principaux

Rappelons qu'un module est dit monogène s'il peut être engendré par un seul élément.

Définition 2.1. — *Un anneau est principal s'il est intègre et si tout idéal est monogène.*

Les corps sont principaux par exemple. Notons que l'intégrité de A assure qu'un générateur d'un idéal est bien défini à multiplication par un inversible près (exercice).
Par exemple, supposons qu'un anneau intègre qui n'est pas un corps soit euclidien, *ie* possède une pseudo-division : il existe une fonction de $A \setminus 0 \to \mathbf{N}$ telle que pour tout $a, b \in A$ avec b non nul, il existe q, r tels que

$$a = bq + r \text{ et } r = 0 \text{ ou } f(r) < f(b).$$

Nous dirons alors que $f(a)$ est la taille de $a \neq 0$ (pour cette pseudo-division).
Par exemple, $k[X]$ si k est un corps $\mathbf{Z}$ sont euclidiens (avec la division euclidienne usuelle).

Lemme 2.2. — *Un anneau euclidien est principal.*

Preuve : On répète la preuve du cas des entiers. Soit donc I un idéal non nul de A et J l'ensemble de $f(i), i \in I \setminus 0$. Comme J est non vide dans $\mathbf{N}$, il admet un plus petit élément $f(i_0)$. En faisant une division de $i \in I$ par i_0, on constate $I = Ai_0$.■

Exercice 2.3. — *Montrer qu'un localisé d'un anneau principal est principal dès qu'il est non nul (ce qui n'arrive que si* 0 *est dans la partie multiplicative qu'on inverse).*

Proposition 2.4. — *Soient a, b deux éléments de A non tous deux nuls et $d \neq 0$ un générateur de (a, b). Alors d divise a, b et si d' divise a, b, alors d' divise d.*

Preuve : Comme $a \in (a, b) = Ad$, on a le premier point. Comme $d \in (a, b)$, il existe $u, v \in A$ tels que $au + bv = d$. Si d' divise a, b, on a donc d' divise d. ■

On dit alors que d est un PGCD de a, b, qui est donc bien défini à inversible près, et est bien le plus grand diviseur commun de a, b au sens de la relation de divisibilité ! On écrit abusivement $d = \mathrm{PGCD}(a, b)$.

Remarque 2.5. — *On pourrait montrer de même qu'un générateur de l'idéal (a_i) engendré par une* ***famille quelconque*** *d'éléments non tous nuls de A* ***principal*** *est un* PGCD *des a_i.*

Définition 2.6. — *On dit que $a, b \in A$ sont étrangers si $(a, b) = A$, autrement dit si* $1 = \mathrm{PGCD}(a, b)$.

Autrement dit, a, b étrangers si et seulement si a, b vérifient une relation de Bézout.

***Lemme 2.7* (Lemme de Gauss)**. — *Supposons que $a \neq 0$ divise bc dans A principal. Si a et b sont étrangers, alors a divise c.*

Preuve : En effet, il existe $u, v, w \in A$ tels que

$$au + bv = 1 \text{ et } bc = aw.$$

On a donc

$$c = cau + cbv = a(uc + wv).$$

■

Corollaire 2.8. — *Un anneau principal est factoriel.*

Preuve : En effet, un anneau principal est noethérien, d'où l'existence des décompositions en facteurs irréductibles (II.4.6). Reste à vérifier que le lemme d'Euclide est vrai (1.2). Soit donc p irréductible divisant ab dans A principal. Comme un PGCD de (a,p) divise p, c'est soit un associé de p, auquel cas $p = \mathrm{PGCD}(a,p)$ et donc $p|a$, et sinon c'est un inversible et alors $1 = \mathrm{PGCD}(a,p)$, et le lemme de Gauss assure $p|c$.■

3. Valuations et anneaux factoriels

Dans cette section, A est un anneau factoriel.

Soit p un irréductible de A factoriel et $a \in A$ qu'on décompose en facteurs irréductibles $a = p_1 \cdots p_n$. Soit v le nombre d'entiers $i \in \{1, \cdots, n\}$ tels que $(p_i) = (p)$. Si on a une autre décomposition en facteurs irréductibles, elle est de la forme $q_1 \cdots q_n$ avec $p_i = q_{\sigma(i)}$ pour $\sigma \in S_n$. Ainsi, σ réalise une bijection entre l'ensemble des indices i tels que $(p) = (p_i)$ et l'ensemble des indices j tels que $(p) = (q_j)$. On note

Définition 3.1. — *La valuation $v_p(a)$ d'un élément non nul de A est le nombre d'irréductibles associés à p qui apparaissent dans une décomposition en facteurs irréductibles de a. On pose $v_p(0) = +\infty$.*

La remarque précédente prouve que ce nombre ne dépend que de a et pas de la décomposition choisie. L'hypothèse de factorialité a été cruciale. Elle est nécessaire : si $A = \mathbf{R}[X,Y]/(X^2 - Y^3)$ comme plus haut, les classes x, y de X, Y dans A sont irréductibles. Mais l'élément $a = x^2 = y^3$ a deux décompositions. Tenant compte de $a = x^2$, on aurait envie d'écrire $v_x(a) = 2$, tenant compte de $a = y^3$ on aurait envie d'écrire $v_x(a) = 0$ car x et y non associés : que choisir...
La factorialité de A permet de montrer sans aucune difficulté les propriétés suivantes, laissées en exercice :

Lemme 3.2. — *Soient $a, b \in A$. On a*
i) $v_p(ab) = v_p(a) + v_p(b)$;
ii) $v_p(a+b) \geq \inf(v_p(a), v_p(b))$ *avec égalité si* $v_p(a) \neq v_p(b)$.
iii) $v_p(a) > 0$ *si et seulement si* $p|a$.

Une fonction $v : A \to \mathbf{Z} \cup \{+\infty\}$ vérifiant *i)* et *ii)* s'appelle une valuation ultramétrique.
Soit K le corps des fractions de A (I.14.6) et $a, b \in A, a \neq 0$. La propriété *i)* assure que $v_p(a) - v_p(b)$ ne change pas si on multiplie a, b par $c \in A$ non nul. Ceci permet de prolonger v_p à K en posant

$$v_p(a/b) = v_p(a) - v_p(b)$$

C'est une valuation ultramétrique de K.

Exercice 3.3. — *Soit t un réel > 1. Posons pour $a, b \in K$*

$$\mathrm{d}(a,b) = t^{-v_p(a-b)}.$$

Montrer que d *est une distance sur K. Trouver toutes les valuations ultramétriques de* $\mathbf{Q}$.

La relation $\diamond$: « a est associé à b » est une relation d'équivalence sur A puisqu'elle s'écrit aussi

$$a \diamond b \text{ si et seulement si } (a) = (b).$$

Elle se restreint en une relation d'équivalence sur l'ensemble $\mathcal{E}$ des éléments irréductibles de A. L'ensemble quotient $\mathcal{P} = \mathcal{E}/\diamond$ (l'ensemble des classes d'équivalence) est l'ensemble des idéaux monogènes engendrés par un irréductible. On choisit dans chaque classe d'équivalence $\pi \in \mathcal{E}/\diamond$ un représentant $p \in \pi$, nécessairement irréductible, autrement dit $\pi = (p)$.

Si $a \in A$ non nul s'écrit $a = p_1 \cdots p_n$ et $p \in \mathcal{P}$, on a $v_p(a) > 0$ si et seulement si $(p) \in \{(p_1), \cdots, (p_n)\}$, ce qui assure qu'il y a un nombre fini de $p \in \mathcal{P}$ tels que $v_p(a) \neq 0$.

Exemple 3.4. — *Prenons $A = \mathbf{C}[X]$. Le théorème de d'Alembert assure que les irréductibles de A sont les polynômes $t(X-z), t \in \mathbf{C}^*$ et $z \in \mathbf{C}$. On peut alors prendre $\mathcal{P} = \{X - z, z \in \mathbf{C}\}$. Le point est qu'on n'a pas envie de prendre à la fois $X - z$ et $2(X-z)$...*

De même qu'on a défini la somme d'une famille presque nulle, de même on définit le produit d'une famille dont presque tous les termes valent 1. Dans ces termes, pour tout $a \in K^*$, on a alors une écriture unique

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \text{ avec } u \text{ inversible dans } A.$$

Exercice 3.5. — *Montrer que v_p est une valuation. Montrer que $a|b$ dans $A \setminus 0$ si et seulement si $v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{P}$.*

Par exemple, si $A = \mathbf{Z}$, on peut prendre $\mathcal{P}$ égal à l'ensembles des nombres premiers et on retrouve l'écriture habituelle d'un rationnel non nul

$$a = \pm \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

car les inversibles de $\mathbf{Z}$ sont ± 1.

4. PGCD,PPCM

Rappelons que dans un anneau intègre, un PGCD, s'il existe, d'une famille d'éléments (a_i) non tous nuls de A est un plus grand (pour la relation de divisibilité) élément de A qui divise tous les (a_i). Il est alors défini à un inversible près. Si d est un PGCD, on écrira encore par abus $d = \mathrm{PGCD}(a_i)$ (on devrait écrire $d \diamond \mathrm{PGCD}(a_i)$, et encore...).

Dans cette section, A est un anneau factoriel.

On choisit un système de représentants des irréductibles $\mathcal{P}$ comme plus haut.

Proposition 4.1. — *Soit a_i une **famille finie** d'éléments de A factoriel, non tous nuls. L'élément*

$$\mathrm{PGCD}(a_i) = \prod_{p \in \mathcal{P}} p^{\inf_i(v_p(a_i))}$$

est un PGCD *des a_i.*

Preuve : Observons déjà d'une part qu'on a $\inf(v_p(a_i)) \neq +\infty$ car un des a_i est non nul et, d'autre part, que la famille de ces inf est presque nulle (car on n'a qu'un nombre fini d'éléments a_i) assurant que presque tous les facteurs du produit sont égaux à 1, assurant sa définition. Comme $v_p(\mathrm{PGCD}) \leq v_p(a_i)$ pour tout $p \in \mathcal{P}$, c'est un diviseur. D'autre part, un diviseur d des a_i vérifie $v_p(d) \leq v_p(a_i)$ et donc $v_p(d) \leq \inf_i(v_p(a_i)) = v_p(\mathrm{PGCD})$, ce qui assure $d|\mathrm{PGCD}$, ce qu'on voulait.■

Lemme 4.2 **(Lemme de Gauss)**. — *Si $a|bc$ dans A et $\mathrm{PGCD}(a,b) = 1$, alors $a|c$.*

Notons que l'hypothèse de divisibilité signifie qu'on suppose en particulier a non nul (on ne divise pas par zéro !).

Preuve : L'hypothèse

$$1 = \mathrm{PGCD}(a,b) = \prod_{p \in \mathcal{P}} p^{\inf(v_p(a), v_p(b))}$$

se traduit en

$$\inf(v_p(a), v_p(b)) = 0 \text{ pour tout } p \in \mathcal{P}.$$

Comme $v_p(a)$ et $v_p(b)$ sont ≥ 0 pour tout p, soit $v_p(a)$ soit $v_p(b)$ est nul. L'hypothèse de divisibilité se traduit en $v_p(a) \leq v_p(b) + v_p(c)$. Si $v_p(b) \neq 0$, on a donc $v_p(a) = 0$ et on a bien $v_p(a) \leq v_p(c)$. Si $v_p(b) = 0$, on a

$$v_p(a) \leq v_p(b) + v_p(c) = v_p(c).$$

Donc, pour tout p, on a $v_p(a) \leq v_p(c)$ et donc $a|c$.■

Donc, comme dans le cas principal, le lemme de Gauss est vrai. **Mais attention, la propriété de Bézout est fausse en général dans les anneaux factoriels** (cf. 5.7 plus bas).
De même, si la famille est **finie**, on l'existence d'un PPCM, avec

$$\mathrm{PPCM}(a_i) = \prod p^{\sup_i(v_p(a_i))}.$$

Cette notion est moins utile que celle de PGCD. Bien entendu, lorsque l'anneau est euclidien, comme $\mathbf{Z}, k[X]$ (donc principal, et donc factoriel comme on l'a vu), en général on calcule le PGCD non pas avec cette formule mais avec l'algorithme d'Euclide (le fameux dernier reste non nul). En effet, décomposer un élément en facteurs irréductibles est un problème extrêmement complexe, la base de la cryptographie RSA.

Exercice 4.3. — *Soit $a, b \in A \setminus 0$. Montrer qu'on a*

$$\mathrm{PPCM}(a,b)\mathrm{PGCD}(a,b) \diamond ab.$$

5. Factorialité des anneaux de polynômes : transfert II

Soit A factoriel, en particulier intègre. Rappelons que les unités de $A[X]$ sont les constantes qui sont inversibles dans A. En particulier, deux polynômes sont associés s'ils se déduisent l'un de l'autre par multiplication par un inversible de A.
On va comparer les irréductibles de $A[X]$ et ceux de $K[X]$ où K est le corps des fractions de A qui est donc vu comme un sous-anneau de K.

Définition 5.1 **(Contenu)**. — *Soit P est un polynôme non nul de $A[X]$. On définit son* ***contenu*** *$c(P)$ comme un* PGCD *de ses coefficients. Un polynôme de contenu* 1 *est dit primitif.*

Il est donc défini à un inversible près, autrement dit c'est un élément du groupe multiplicatif quotient $A' = A \setminus 0/U(A)$, ou, si l'on préfère on peut l'identifier à l'idéal monogène qu'il engendre. Bien entendu, si $a \in A$ non nul, on a $c(aP) = ac(P)$. On écrira, par abus, $a = b$ pour $a \diamond b$: à charge du lecteur de vérifier que ceci ne pose pas de problème.

Lemme 5.2 **(Gauss)**. — *Soient $P, Q \in A[X]$ non nuls. On a $c(PQ) = c(P)c(Q)$.*

Preuve : On a une factorisation dans $A[X]$ de la forme

$$P = c(P)P_1, Q = c(Q)Q_1$$

avec $c(P_1) = c(Q_1) = 1$. Il suffit de prouver l'identité pour P_1, Q_1, de sorte qu'on se ramène à P, Q primitifs. On doit prouver PQ primitif. Si ce n'est pas le cas, choisissons un facteur irréductible p de $c(PQ)$. Comme A est factoriel, il vérifie le lemme d'Euclide de sorte que l'idéal pA est premier. Notons $P \mapsto \bar{P}$ la projection quotient $A[X] \twoheadrightarrow A/pA[X]$ de réduction $\mod p$ des coefficients de P. On a alors $\bar{P}\bar{Q} = 0$ dans $\bar{A}[X]$. Comme pA est premier, $\bar{A}$ et donc également $\bar{A}[X]$ est intègre. On en déduit que $\bar{P}$ ou $\bar{Q}$ est nul, disons $\bar{P}$ par exemple. Mais ceci signifie exactement $p|c(P) = 1$, une contradiction.■

Corollaire 5.3. — *Les polynômes irréductibles de $A[X]$ sont les irréductibles de A (vus comme polynômes de degré nul) et les polynômes de $A[X]$, qui sont primitifs et irréductibles dans $K[X]$.*

Preuve : Supposons $P \in A[X]$ irréductible, non constant. Il est certainement primitif, car sinon on a une écriture $P = pQ$ avec p irréductible dans A divisant $c(P)$ et p non associé à P (car sinon P serait de degré nul), ni inversible, une contradiction. Par ailleurs, s'il était réductible dans $K[X]$, il s'écrirait UV avec $UV \in K[X]$ de degrés non nuls. En prenant des dénominateurs u, v des coefficients de U, V, on écrit $UV = u^{-1}\tilde{U}v^{-1}\tilde{V}$ avec $\tilde{U}, \tilde{V} \in A[X]$. On a alors

$$uvP = \tilde{U}\tilde{V}$$

et donc $uv = c(\tilde{U})c\tilde{(V)}$. On en déduit la formule

$$P = \tilde{U}/c(\tilde{U})\tilde{V}/c(\tilde{V})$$

qui est une écriture dans $A[X]$, donc interdite, puisque P est irréductible ! Par ailleurs, un irréductible de A le reste dans $A[X]$ (degré). La réciproque est claire.■

***Exercice 5.4* (Critère d'Eisenstein).** — *Soit p irréductible de A factoriel et $P = \sum_{i \leq n} a_i X^i \in A[X]$. On suppose que p ne divise pas a_n, mais $p|a_i$ pour tout $i < n$ et p^2 ne divise pas a_0. Montrer que P est irréductible dans $K[X]$ [Indication : se ramener d'abord à P primitif]. Montrer par exemple que le polynôme $X^4 + X^2Y^3 + Y$ est irréductible dans $\mathbf{Q}[X, Y]$. Montrer qu'il existe des polynômes irréductibles dans $\mathbf{Q}[X]$ de tout degré > 0.*

Exercice 5.5. — *Montrer que le polynôme $\sum_{i=1}^{n} X_i^2$ est irréductible dans $\mathbf{R}[X_i]$ si $n > 1$ et dans $\mathbf{C}[X_i]$ si $n > 2$.*

Théorème 5.6. — *Si A est factoriel, alors $A[X]$ est factoriel.*

Preuve : Soit $P \in A[X]$ non nul.
Si P est constant, on le décompose dans A en facteurs irréductibles dans A, donc dans $A[X]$.
Sinon, $\deg(P) > 0$. Il se décompose dans $K[X]$ sous la forme $P = P_1 \cdots P_n$ avec P_i irréductibles de $K[X]$. Chassant les dénominateurs et mettant en facteurs les contenus, on l'écrit $P = a/bQ_1 \cdots Q_n$ avec $Q_i \in A[X]$ primitif et irréductible dans $K[X]$, donc irréductible dans $A[X]$. Prenant les contenus, on a $bc(P) = a$, ce qui donne la formule $P = c(P)Q_1 \cdots Q_n$. Décomposant $c(P)$ en facteurs irréductibles dans A, on obtient l'existence de la décomposition.
Pour l'unicité, montrons que $A[X]$ vérifie le lemme d'Euclide. Soit donc P irréductible dans $A[X]$ divisant QR.
Si P est constant, c'est un irréductible p de A. On a alors $p|c(Q)c(R)$ et donc, d'après le lemme d'Euclide dans A, on a $p|c(Q)$ par exemple. En écrivant $Q = c(Q)Q_1$, on en déduit $p = P|Q$.
Si P est non constant, il est primitif et irréductible dans $K[X]$. Comme $K[X]$ est principal, le lemme d'Euclide dans $K[X]$ assure que par exemple $P|Q$ dans $K[X]$, autrement dit il existe $\bar{S} \in K[X]$ tel que $Q = \bar{S}P$. On écrit $\bar{S} = S/s, \bar{S} \in A[X], s \in A \setminus 0$ et donc $sQ = SP$. Prenant les contenus, on déduit $sc(Q) = c(S)$. On écrit $S = c(S)S_1$ avec S_1 primitif. En remplaçant, on obtient

$$Q = c(Q)S_1P$$

de sorte que $P|Q$ dans $A[X]$. On invoque alors 1.2.■

Ainsi, les anneaux de polynômes à plusieurs variables sont factoriels.

Exercice 5.7. — *Montrer que X, Y sont irréductibles dans $\mathbf{R}[X, Y]$ de* PGCD *égal à* 1. *Montrer qu'on n'a pas de relation de Bézout entre X, Y (évaluer l'identité en $(0, 0)$).*

6. Parenthèse sur les catégories, III

On se donne une catégorie $\mathcal{C}$ avec un objet nul. Si $a \to b$ est un morphisme, on a observé que $0 \to a$ est un noyau si $a \to b$ est un monomorphisme, et, de même, $b \to 0$ un conoyau si $a \to b$ est un épimorphisme. On sait aussi que les noyaux, quand ils existent, sont des monomorphismes tandis que les conoyaux sont des épimorphismes.
Observons que la catégorie des modules a une propriété remarquable : les ensembles de flèches sont des groupes abéliens et la composition est bilinéaire. On connaît la notion de produit d'ensembles (l'ensemble des couples). On va définir alors la notion de produit et de somme « à la Yoneda ».

Définition 6.1. — *Soient a, b deux objets d'une catégorie.*
– *On dit que a, b admettent un produit si le foncteur*

$$c \mapsto \mathrm{Hom}(c, a) \times \mathrm{Hom}(c, b)$$

de $\mathcal{C}^{\mathrm{opp}}$ dans $\mathcal{E}ns$ est représentable. On note alors $a \times b$ un représentant (bien défini à isomorphisme unique près).
– *On dit que a, b admettent un coproduit (ou une somme) si le foncteur*

$$c \mapsto \mathrm{Hom}(a, c) \times \mathrm{Hom}(b, c)$$

de $\mathcal{C}$ dans $\mathcal{E}ns$ est représentable. On note alors $a \oplus b$ un représentant (bien défini à isomorphisme unique près).

Ainsi, on a des isomorphismes fonctoriels

$$\mathrm{Hom}(c, a) \times \mathrm{Hom}(c, b) \xrightarrow{\sim} \mathrm{Hom}(c, a \times b)$$

et

$$\mathrm{Hom}(a, c) \times \mathrm{Hom}(b, c) \xrightarrow{\sim} \mathrm{Hom}(a \oplus b, c).$$

Exercice 6.2. — *Montrer qu'au sens précédent le produit dans $\mathcal{E}ns$ est le produit usuel alors que la somme est la réunion disjointe. Montrer que dans la catégorie des modules, le produit et la somme coïncident et sont égaux à la somme directe.*

On laisse au lecteur le soin de définir les notions de somme, produit d'un nombre fini d'éléments.

Définition 6.3. — *Une catégorie $\mathcal{C}$ est dite additive si les propriétés suivantes sont vérifiées :*
a) les ensembles de flèches sont des groupes abéliens ;
b) la composition est bilinéaire ;
c) $\mathcal{C}$ a un objet nul 0 ;
d) $\mathcal{C}$ a des produits et des sommes directes finies.

On a une notion évidente de foncteur additif.

Exercice 6.4. — *Montrer que dans une catégorie additive $\mathcal{C}$, la somme de deux objets est isomorphe au produit. Vérifier que le neutre $0 \in \mathrm{Hom}(a, b)$ est le morphisme nul au sens des catégories.*

Dans la catégorie des modules, tout morphisme injectif $f : M \to N$ est le noyau de $N \to N/f(M)$ et tout morphisme surjectif $g : M \to N$ est le conoyau de $\mathrm{Ker}(g) \to M$. Ainsi, les épimorphismes sont les morphismes surjectifs et les monomorphismes sont les morphismes injectifs dans ce cas. Par ailleurs, la catégorie des modules admet des produits finis : autrement dit, pour tout a, b objets de $\mathcal{C}$ le foncteur contravariant

$$c \mapsto \mathrm{Hom}(c, a) \times \mathrm{Hom}(c, b)$$

de $\mathcal{C}$ dans la catégorie opposée des groupes abéliens est représentable par un objet $a \times b$, bien défini à isomorphisme unique près (Yoneda). En effet, la somme directe de deux modules est un produit en ce sens.

Définition 6.5. — *Une catégorie additive est dite abélienne, si les les propriétés suivantes sont vérifiées :*
a) toutes les flèches ont des noyaux et conoyaux ;
b) la flèche canonique $a/\ker(f) \to \mathrm{Im}(f)$ *de la coimage de* $f \in \mathrm{Hom}(a,b)$ *dans l'image est isomorphisme.*

Par exemple, la catégorie des modules est une catégorie abélienne. C'est le prototype. On peut montrer que toute catégorie abélienne $\mathcal{C}$ se plonge dans la catégorie des modules sur un anneau, au sens qu'il existe un foncteur fidèle de la première dans la seconde.

Exercice 6.6. — *Soit* $\mathcal{C}$ *une catégorie abélienne et* $f \in \mathrm{Hom}(a,b)$ *une flèche de* $\mathcal{C}$. *Montrer que* $\mathrm{Ker}(f) = 0$ *si et seulement si* f *est monomorphisme,* $\mathrm{Coker}(f) = 0$ *si et seulement si* f *est un épimorphisme. Montrer que* f *est un épimorphisme et un monomorphisme si et seulement si c'est un isomorphisme.*

PARTIE IV

MODULES SUR LES ANNEAUX PRINCIPAUX

On va dans un premier temps s'intéresser aux modules de torsion sur les anneaux principaux. On illustrera les résultats obtenus en expliquant par exemple le lien avec la décomposition des fractions rationnelles en éléments simples. On s'attaquera ensuite aux modules de type fini sur les anneaux principaux. Pour étudier leur structure, on va se ramener à un problème matriciel, qu'on résoudra grâce à une version raffinée du pivot de Gauss. On donnera un théorème de structure complet dans ce cas, ce qui donnera par exemple la structure des groupes abéliens de type fini. On appliquera la théorie au cas du $k[X]$-module associé à un endomorphisme, ce qui donnera des résultats précis et non triviaux d'algèbre linéaires (étude des espaces stables, décomposition de Jordan...).
Dans toute cette partie M désigne un module sur A principal.

1. Une suite exacte fondamentale

Comme A est intègre, le sous-ensemble $\mathrm{Tors}(M)$ des éléments de M de torsion, *ie* annulés par un élément non nul, est un sous-module de A. On a une suite exacte

$$0 \to \mathrm{Tors}(M) \to M \to M/\mathrm{Tors}(M) \to 0 \tag{1.a}$$

Bien entendu, le module $M/\mathrm{Tors}(M)$ est sans torsion. En effet, si la classe de m est tuée par $a \in A$ non nul, ceci signifie que am est de torsion et donc qu'il existe $b \in A$ non nul tel que $b(am) = 0$. Comme ba est non nul (A est intègre), m est de torsion et sa classe est nulle. On verra plus bas le résultat suivant.

Théorème 1.1. — *Un module sans torsion de type fini sur un anneau principal est libre.*

Donc, si M est de type fini, $M/\mathrm{Tors}(M)$ est libre et la suite exacte 1.a est scindée (non canoniquement). En effet, le choix d'une base e_i de $M/\mathrm{Tors}(M)$ et d'antécédents m_i de e_i dans M définit une section $e_i \mapsto m_i$. On a donc un isomorphisme (non canonique, répétons le) $M \xrightarrow{\sim} \mathrm{Tors}(M) \oplus M/\mathrm{Tors}(M)$ dans ce cas. Ceci explique qu'on s'intéresse aux modules de torsion dans un premier temps, *ie* tels que $M = \mathrm{Tors}(M)$.

Exercice 1.2. — *On note M_K le $K = \mathrm{Frac}(A)$-espace vectoriel $M[1/a, a \neq 0]$. Montrer que $\mathrm{Tors}(M)_K$ est nul. En dduire un isomorphisme $M_K \xrightarrow{\sim} (M/\mathrm{Tors}(M)_K$.*

À vrai dire, le théorème 1.1 se généralise de la manière suivante.

***Théorème 1.3* (Facteurs invariants)**. — *Si M est de type fini, il existe une unique suite déroissante $I_n \subset I_{n-1} \cdots \subset I_1$ d'idéaux propres de A, ie distincts de A, telle que $M \xrightarrow{\sim} \oplus A/I_j$. Les I_j s'appellent les facteurs invariants de M.*

Le théorème de structure entraîne le théorème 1.1. En effet, dire que $M/\mathrm{Tors}(M)$ est sans torsion, c'est dire que ses facteurs invariants sont des idéaux nuls d'après le théorème de structure et donc qu'il est libre de rang fini. Attention, si M n'est pas de type fini, c'est faux en général.

Exercice 1.4. — *Montrer que le $\mathbf{Z}$-module $\mathbf{Q}$ est sans torsion mais n'est pas libre.*

***Corollaire 1.5* (Groupes abéliens de type fini).** — *Si G est un groupe abélien de type fini, il existe une unique suite $r, d_1, \cdots, d_n$ d'entiers ≥ 0 avec $2 \leq d_1 | \cdots | d_n$ telle que que*

$$G \xrightarrow{\sim} \mathbf{Z}^r \oplus \oplus_{i=1}^n \mathbf{Z}/d_i\mathbf{Z}.$$

Exercice 1.6. — *Trouver les facteurs invariants du groupe $\mathbf{Z}/18\mathbf{Z} \oplus \mathbf{Z}/15\mathbf{Z} \oplus \mathbf{Z}/25\mathbf{Z}$.*

Exercice 1.7. — *Soit k un corps fini. Montrer que sa caractéristique est un nombre premier p et que k est un $\mathbf{F}_p$ -espace vectoriel de dimension n. En déduire le groupe additif de k est isomorphe à $(\mathbf{F}_p)^n$. Soit d un entier > 0. Montrer que le nombre d'éléments de k^* tels que $x^d = 1$ est plus petit que d. En déduire que le groupe multiplicatif de k^* est cyclique (utiliser 1.5).*

2. Décomposition des modules de torsion

Soit p irréductible dans A. Comme A est principal, le lemme d'Euclide assure que $\mathfrak{p} = pA$ est un idéal premier.

Définition 2.1. — *La composante p-primaire M_p de M est le sous-module de M des éléments annulés par une puissance de p.*

Lemme 2.2. — *Il existe une unique structure de $A_\mathfrak{p}$-module sur M_p compatible avec celle de A-module.*

Preuve : Il suffit de vérifier que la multiplication par a non divisible par p définit un isomorphisme d'inverse α de M (on pose alors $(b/a).m = b\alpha(m)$). Soit $m \in M_p$ annulé par p^n disons. Soit $a \in A$ non divisible par p, donc premier avec p^n (irréductibilité de p). L'identité de Bézout assure qu'il existe $a_m, \pi \in A$ tels que $aa_m + p^n\pi = 1$. On a alors $aa_m.m = m$ et l'inverse cherché est défini par $\alpha(m) = a_m.m$.■

Exercice 2.3. — *Vérifier que les idéaux non nuls de $A_\mathfrak{p}$ sont engendrés par une puissance de p.*

La notation M_p est justifiée par le résultat suivant.

Proposition 2.4. — *Supposons M de torsion. Alors, la flèche de localisation $M_p \to M_\mathfrak{p}$ est un isomorphisme de $A_\mathfrak{p}$-modules.*

Preuve : L'application est bien linéaire. Prouvons l'injectivité. Si m/a est nul dans $M_\mathfrak{p}$, il existe b non divisible par p tel que $bm = 0$ dans $M_p \subset M$. Mais, comme M_p est un $A_\mathfrak{p}$-module, on peut multiplier par $1/b \in A_\mathfrak{p}$ pour trouver $m = 0$ (on n'a pas utilisé M de torsion ici).
Prouvons la surjectivité. Soit donc m/a un élément de $M_\mathfrak{p}$. Choisissons $b \in A$ non nul annulant m. On écrit $b = p^n\beta$ avec $\mathrm{PGCD}(\beta, p) = 1$. Comme β inversible dans $A_\mathfrak{p}$, on a $m/a = \beta m/(\beta a)$ dans $M_\mathfrak{p}$ avec $\beta m \in M_p$ par construction. Mais alors, m/a a pour antécédent $(1/\beta a).\beta m \in M_p$ car M_p est un $A_\mathfrak{p}$-module. ■

Soit $\mathcal{P}$ un système de représentants des irréductibles de A. La somme induit un morphisme

$$\sigma : \oplus_{p \in \mathcal{P}} M_p \to M.$$

Soit $p \in \mathcal{P}$ engendrant l'idéal premier $\mathfrak{p}$ et $m \in M$ de torsion. On note m_p l'image de m dans M_p identifié à $M_\mathfrak{p}$ comme plus haut. Notons que si a non nul annule m, son image m_p dans M_p est nulle si p ne divise pas a car alors a est inversible dans $A_\mathfrak{p}$ et $0 = (1/a)am = m$. Comme A est factoriel, l'ensemble des $p \in \mathcal{P}$ divisant a est fini. Ainsi, la famille des localisés $(m_p), p \in \mathcal{P}$ est presque nulle d'où une application linéaire (de localisation)

$$\lambda : M \to \oplus_{p \in \mathcal{P}} M_p.$$

***Proposition 2.5* (Décomposition primaire).** — *Le morphisme* σ

$$\oplus_{p\in\mathcal{P}} M_p \to M$$

est un isomorphisme d'inverse λ*. Autrement dit, un module de torsion sur un anneau principal est la somme directe de ses composantes p-primaires.*

Preuve : Le composé $\lambda\circ\sigma$ est l'identité. En effet, si $m\in M_p$, son image est la famille des localisés $m_q, q\in\mathcal{P}$. Mais, si q est différents de p, les irréductibles p et q ne sont pas associés ($\mathcal{P}$ est un système de représentants), de sorte que q ne divise pas p. Mais alors, p est inversible dans $A_{\mathfrak{q}}$ (où $\mathfrak{q}=qA$) d'une part, et, d'autre part, une de ses puissances annule m, donc m_q, assurant la nullité de m_q. Si $q=p$, bien entendu, $m_p=m$. L'autre sens se traite de même.■

***Remarque 2.6* (Fonctorialité).** — *Soit* $f\in\mathrm{Hom}_A(M',M)$ *un morphisme de modules et p irréductible. On a* $f({M'}_p)\subset M_p$*. En particulier, si* M' *est un sous-module de* M*, on a* $M'\cap M_p={M'}_p$ *de sorte que*

$$M'=\oplus_{p\in\mathcal{P}}(M\cap {M'}_p)$$

est la décomposition en composantes p-primaires de M'*.*

Lemme 2.7. — *Si* $aM=0$*, on a* $M_p=0$ *si* $v_p(a)=0$ *et en général* $M_p=\mathrm{Ann}_M(p^{v_p(a)})$*.*

Preuve : Pour le second point, on doit prouver que si m est dans M_p, on a $p^{v_p(a)}m=0$. Or, a s'écrit $p^{v_p(a)}b$ avec p ne divise b et donc est inversible dans $A_{\mathfrak{p}}$. Comme $am=0$ et M_p est un $A_{\mathfrak{p}}$-module, on a $p^{v_p(a)}m=0$. Le premier point est conséquence du second ! ■

Exercice 2.8. — *Soit* a,b *premiers entre eux. Montrer qu'on a une somme directe*

$$\mathrm{Ann}_M(ab)=\mathrm{Ann}_M(a)\oplus\mathrm{Ann}_M(b).$$

2.9. Application à l'algèbre linéaire. — On regarde ici $A=k[X]$ et M le $k[X]$-module associé à un endomorphisme f d'un espace vectoriel de dimension finie E, dont on a déjà observé qu'il était de torsion. On peut prendre pour $\mathcal{P}$ l'ensemble des polynômes P irréductibles unitaires.
Le résultat 2.8 est le lemme des noyaux usuel dans ce cas.
Plus précisément, soit μ_f est le **polynôme minimal** de f (générateur unitaire de $\mathrm{Ann}_{k[X]}(M)=\mathrm{Ann}_{k[X]}(f)$. On déduit du théorème de décomposition 2.5 et de 2.7 que M est somme directe des M_P où P divise μ_f. Avec le dictionnaire « sous-module=sous-espace stable », on obtient que E est une somme directe

$$E=\oplus_{P|\mu_f}\mathrm{Ker}(P^{v_P(\mu_f)}(f)) \text{ avec } E_P=\mathrm{Ker}(P^{v_P(\mu_f)}). \tag{2.9.a}$$

On se souvient que E_P est **le sous-espace caractéristique** associé à P, qui est stable par f.
Maintenant, se donner un sous-espace stable E' de E, c'est se donner un sous-module M' de M. Par fonctorialité de la décomposition en facteurs p-primaires (2.6), on a donc

$$E'=\oplus_{P|\mu_f}E'\cap E_P$$

de sorte qu'on peut se ramener aux sous-espaces caractéristiques pour étudier les sous-espaces stables.
Par exemple, si $k=\mathbf{C}$, les polynômes P sont de degré 1 de la forme $P(X)=X-z, z\in\mathbf{C}$. La restriction de f à E_P est donc annulée par une puissance de $(X-z)$ ce qui permet de ramener l'étude des espaces stables au cas nilpotent car $f-z\mathrm{Id}$ est nilpotente sur E_P par construction. On reverra tout ceci plus précisément en 4.7 et 4.10.

2.10. Applications aux fractions rationnelles. — Soit $A = k[X]$ comme plus haut, K le corps des fractions rationnelles et $M = K/A$. C'est un module de torsion, car si m est la classe de $a/b \in K$, on a $bm = 0$. Les éléments de $M_P, P \in \mathcal{P}$ sont de la forme Q/P^n. En effet, dire que la classe de la fraction irréductible a/b (avec b unitaire disons) est tuée par P^n, c'est dire $P^n a/b$ polynôme, autrement dit b divise aP^n. Comme $\mathrm{PGCD}(a, b) = 1$ par hypothèse, le lemme de Gauss dans $k[X]$ donne b divise P^n, et donc b est associé à une puissance de P, ce qu'on voulait.

Lemme 2.11. — *Tout élément de M_P s'écrit de façon unique*

$$\sum A_j/P^j \text{ avec } \deg(A_j) < \deg(P).$$

Preuve : Pour l'unicité, supposons qu'on a

$$\sum_{j=0}^{n} A_j/P^j$$

nul dans M avec A_n non nul. Multipliant par P^n, on déduit, que P divise A_n, et donc $\deg(P) \leq \deg(A_n)$, une contradiction. Pour l'existence, on fait une récurrence sur le plus petit entier n tel que $P^n m = 0$. Si $n = 0$, on a $m = 0$ et c'est clair. Sinon, supposons que c'est prouvé au rang n. Un élément m tué par P^{n+1} s'écrit Q/P^{n+1} d'après ce qui précède. Divisant Q par P, on trouve $m = Q_1/P^n + R_1/P^{n+1}$ avec $\deg(R_1) < \deg(P)$. On applique l'hypothèse de récurrence à Q_1/P^n.■

Corollaire 2.12. — *Toute fraction rationnelle $R \in K$ s'écrit de manière unique*

$$E + \sum_{P\in\mathcal{P}} \sum_j A_{P,j}/P^j \text{ avec } \deg(A_{P,j}) < \deg(P) \text{ et } E \in k[X].$$

Preuve : On écrit $M = \oplus_{P\in\mathcal{P}} M_P$ et on décompose (de façon unique) la classe m de R dans M grâce au lemme sous la forme

$$m = \sum_{P\in\mathcal{P}} \sum_j A_{P,j}/P^j \text{ avec } \deg(AP, j) < \deg(P).$$

La différence

$$E = R - \sum_{P\in\mathcal{P}} \sum_j A_{P,j}/P^j$$

est donc nulle dans M : c'est un polynôme.■

3. Modules de type fini sur un anneau principal

Dans toute la suite, M est un module de type fini sur A principal. On fixe un système de représentants $\mathcal{P}$ des irréductibles de A.

3.1. La stratégie. — Comme A est de noethérien, il est de présentation finie. Explicitement, on choisit n générateurs de M qui définissent une surjection $A^n \twoheadrightarrow M$. Le choix de m générateurs du noyau de cette surjection définit une suite exacte

$$A^m \xrightarrow{f} A^n \to M \to 0$$

qui induit un isomorphisme

$$\mathrm{Coker}(f) \xrightarrow{\sim} M.$$

On identifie matrice et morphismes de modules libres grâce aux base canoniques. Si f est nulle en dehors de la diagonale -on dira simplement f diagonale, même dans ce cas rectangulaire-, donc de la forme

$$\begin{pmatrix} a_1 & & \cdots & & 0 \\ \vdots & \ddots & & & \vdots \\ 0 & \cdots & a_n & \cdots & 0 \end{pmatrix}, \tag{3.1.a}$$

la projection

$$A^n \mapsto \oplus_{i=1}^n A/a_iA$$

définit un isomorphisme

$$M \xrightarrow{\sim} \mathrm{Coker}(f) \xrightarrow{\sim} \oplus_{i=1}^n A/a_iA.$$

Supposons que $g \in \mathrm{Hom}(A^m, A^n)$ soit **équivalente** à f, autrement dit qu'il existe des isomorphismes a, b de A^m, A^n tels que $f = b^{-1}ga$. Alors, b induit un isomorphisme

$$\mathrm{Coker}(f) \xrightarrow{\sim} \mathrm{Coker}(g).$$

Plus visuellement, on a un diagramme commutatif à lignes exactes et flèches verticales bijectives

$$\begin{array}{ccccccc} A^m & \xrightarrow{f} & A^n & \to & \mathrm{Coker}(f) & \to & 0 \\ a\downarrow\wr & & b\downarrow\wr & & \downarrow\wr & & \\ A^m & \xrightarrow{g} & A^n & \to & \mathrm{Coker}(g) & \to & 0 \end{array}$$

Ainsi, si f est non plus égale mais seulement équivalente à une matrice diagonale comme en 3.1.a, on a encore un isomorphisme

$$M \xrightarrow{\sim} \oplus_{i=1}^n A/a_iA. \tag{3.1.b}$$

Par exemple, si A est un corps k, on sait (pivot de Gauss) que f est équivalente à une telle matrice diagonale, avec de plus $a_i = 0$ ou 1 ; ainsi, $M \xrightarrow{\sim} k^r$ où r est le nombre coefficients a_i nuls : on retrouve ainsi que tout espace vectoriel de dimension finie admet une base.

Dans le cas général, on va raffiner la méthode du pivot de Gauss pour montrer que f est équivalente à une matrice diagonale, bien particulière. Précisément, nous allons prouver l'énoncé purement matriciel suivant.

Proposition 3.2. — *Toute matrice $f \in \mathrm{Hom}(A^m, A^n)$ est équivalente à une matrice diagonale dont les coefficients diagonaux a_i vérifient $(a_n) \subset (a_{n-1}) \cdots \subset (a_1)$.*

Bien entendu, ce lemme suffit à prouver le versant « existence »du théorème 1.3 en posant $I_j = (a_j)$ si $(a_j) \neq A$.

Exercice 3.3. — *En admettant par exemple le théorème 1.3 d'unicité des facteurs invariants, prouver que les idéaux (a_i) ne dépendent que de la casse d'équivalence de f.*

3.4. Quelques opérations matricielles. — Comme pour le pivot de Gauss, on va considérer des matrices particulières de $\mathbf{GL}_n(A)$ nous permettant de modifier f en restant dans sa classe d'équivalence. Rappelons que $\mathbf{GL}_n(A)$ est le groupe des isomorphismes de A^n, identifié au groupe des matrices de **déterminant inversible** (et pas seulement non nul !).

a) Type 1. — Les matrices de permutation nous autorisent à permuter les lignes et colonnes.

Dans la théorie du pivot sur les corps, on rajoute les matrices de transvections

$$\begin{pmatrix} T(a) & 0 \\ 0 & \mathrm{Id} \end{pmatrix}$$

où $T(a) \in \mathbf{SL}_2(A)$ est la matrice

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Par multiplication par des matrices de permutation, on obtiendrait toutes les transvections qui permettent de faire les opérations de ligne et de colonne habituelles.

Si l'anneau était euclidien (comme $\mathbf{Z}$ ou $k[X]$), ce serait suffisant (cf. TD) pour ramener toute matrice à la forme diagonale cherchée, de façon purement algorithmique. En général, ce n'est pas le cas.

b) Type 2. — Dans le cas général, on se permet de rajouter les matrices de Bézout

$$\begin{pmatrix} E & 0 \\ 0 & \mathrm{Id} \end{pmatrix}$$

où $E \in \mathbf{SL}_2(A)$, n'importe quelle matrice $(2,2)$ de déterminant 1. La dénomination est due à la remarque suivante. Soient a, b non tous deux nuls de PGCD égal à δ. On a une relation de Bézout

$$\alpha a/\delta + \beta b/\delta = 1$$

et on a

$$E\begin{pmatrix} \delta \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

avec

$$E = \begin{pmatrix} a/\delta & -\beta \\ b/\delta & \alpha \end{pmatrix} \in \mathbf{SL}_2(A).$$

On a alors

$$\begin{pmatrix} E & 0 \\ 0 & \mathrm{Id} \end{pmatrix} \begin{pmatrix} \binom{\delta}{0} & * \\ * & * \end{pmatrix} = \begin{pmatrix} \binom{a}{b} & * \\ * & * \end{pmatrix} \tag{3.4.a}$$

Ainsi, on déduit que $\binom{a}{b}$ non nul est équivalente à $\binom{\delta}{0}$, et, par transposition, (a, b) équivalente à $(\delta, 0)$.

Donc, dans les **opérations permises**, on peut remplacer deux coefficients d'une ligne ou d'une colonne par leur PGCD ou 0 suivant qu'ils sont tous deux non nuls ou 0. On a, du point de vue matriciel, la notion de **matrice permise**, à savoir un produit de matrices de type 1 et 2.

On notera par commodité gén(a_i) un générateur, bien défini à un inversible près, de l'idéal engendré par les a_i : si les a_i sont non tous nuls, c'est un PGCD des a_i.

Lemme 3.5. — *Soit $f \in \mathrm{Hom}(A^m, A^n)$ et $\delta = \text{gén}(f_{i,1})$ un des coefficients de la première colonne de f . Alors, il existe une matrice permise $M \in \mathbf{GL}_n(A)$ telle que*

$$Mf = \begin{pmatrix} \delta & * \\ 0 & * \end{pmatrix}.$$

Preuve : Pour éviter les trivialités, supposons $n, m > 0$ (l'énoncé est trivialement vrai pour des matrices vides...). On fait une récurrence sur n. Pour $n = 1$, la matrice de f est une ligne et de première colonne un scalaire qui est δ : l'énoncé est trivialement vrai dans ce cas.

Passons de $n \geq 1$ à $n + 1$. La première colonne C de f est de la forme $C = \binom{f_{1,1}}{C'}$. Par récurrence, on peut trouver une matrice permise $M' \in \mathbf{GL}_{n-1}(A)$ telle que

$$M'C' = \begin{pmatrix} \delta' \\ 0 \end{pmatrix} \text{ avec } \delta' = \text{gén}(f_{i,1}, i > 1)$$

de sorte que

$$\begin{pmatrix} 1 & 0 \\ 0 & M' \end{pmatrix} (f) = \begin{pmatrix} \binom{f_{1,1}}{\delta'} & * \\ 0 & * \end{pmatrix}.$$

Utilisant 3.4.a, avec $a = f_{1,1}, b = \delta'$, on trouve une matrice permise M" $\in \mathbf{GL}_n(A)$ telle que

$$M\text{"} \begin{pmatrix} \binom{f_{1,1}}{\delta'} & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} \binom{\delta}{0} & * \\ 0 & * \end{pmatrix} \text{ avec } \delta = \text{gén}(f_{1,1}, \delta').$$

On observe alors

$$\delta = \text{gén}(f_{i,1}, i \geq 1) = \text{gén}(f_{1,1}, f_{i,1}, i > 1) = \text{gén}(f_{1,1}, \delta').$$

■

Exercice 3.6. — *Supposons A euclidien. Montrer que dans l'énoncé précédent on peut uniquement utiliser des matrices permises de type 1 (utiliser l'algorithme de Bézout pour calculer un* PGCD*).*

3.7. Taille. — Pour finir, on a besoin d'une notion de longueur des coefficients des éléments permettant de mesurer l'avancement de notre algorithme de simplification. Dans le cas euclidien, il serait donné par la fonction f d'une pseudo-division euclidienne.

Définition 3.8. — *La longueur $l(a)$ d'un élément $a \in A$ non nul est le nombre de facteurs irréductibles de intervenant dans sa décomposition en facteurs irréductibles. La longueur d'une matrice non nulle à coefficients dans A est la plus petite longueur de ses coefficients non nuls.*

Par exemple, $l(a)$ est nul si et seulement si a est inversible, et vaut 1 si et seulement si a est irréductible.

Lemme 3.9. — *Soient $a, b \in A$ non nuls. Alors, $l(\mathrm{PGCD}(a,b)) \leq l(a)$, avec égalité si et seulement si a divise b.*

Preuve : C'est une conséquence immédiate des formules

$$l(a) = \sum_{p \in \mathcal{P}} v_p(a) \text{ et } v_p(\mathrm{PGCD}(a,b)) = \inf(v_p(a), v_p(b)).$$

■

C'est la seule propriété de la taille que nous utiliserons.

Exercice 3.10. — *Supposons que A soit $\mathbf{Z}$ ou $k[X]$ et notons L la taille associée à la division euclidienne (cf. III.2). Montrer que L vérifie le lemme 3.9.*

3.11. Équivalence de matrice : existence des facteurs invariants. — On est en mesure de prouver le résultat matriciel annoncé.

Preuve de la proposition 3.2 : prouvons l'existence par récurrence sur $n+m$, le cas $n+m=2$ étant trivial (on laisse au lecteur le cas des matrices vides...).

Supposons donc f de taille (n,m) et le lemme prouvé en taille (n',m') si $n'+m' < n+m$. D'après le lemme 3.5, **on peut supposer n et m strictement plus grands que 1.**

Lemme 3.12. — *Si f et g sont équivalentes, les idéaux I_f, I_g engendrés par les coefficients de f ou de g sont les mêmes.*

Preuve : Si $f = b^{-1}ga$, tous les coefficients de f sont multiples d'un générateur de I_g, prouvant $I_f \subset I_g$. L'inclusion inverse s'obtient en écrivant $g = bfa^{-1}$.■

Ainsi, $I_f = (\text{gén}(f_{i,j}))$ est invariant par équivalence.

Réductions. On peut supposer f non nulle, puis, quitte à diviser f par $\text{gén}(f_{i,j})$, **on peut supposer** $\text{gén}(f_{i,j}) = 1$**, autrement dit** $I_f = A$. On peut ensuite supposer f **de longueur minimale** l dans sa classe d'équivalence -on dira f minimal-, et, quitte à permuter lignes et colonnes, supposer que le coefficient $a_1 = f_{1,1}$ d'indice $(1,1)$ de f est de longueur l (notons que a_1 est non nul) .

La preuve. Grâce à 3.5, on peut grâce à des opérations permises changer f en une matrice du type

$$g = \begin{pmatrix} d & * \\ 0 & * \end{pmatrix} \quad \text{avec} \quad d = \text{gén}(f_{i,1})$$

Comme $d | a_1$, on a

$$l(g) \leq l(d) \leq l(a_1) = l(f),$$

ce qui impose $l(g) = l(f)$ par minimalité de f et donc $l(d) = l(a_1)$ (ce qui signifie $a_1|f_{i,1}$). On déduit alors du cas d'égalité de 3.9 que d et a_1 sont associés. **On peut donc supposer** $d = a_1$, *ie*

$$f = \begin{pmatrix} a_1 & * & \cdots & * \\ 0 & & & \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \text{ avec } l(a_1) = l(f).$$

Le même argument sur la première ligne de notre nouvelle matrice minimale prouve que les divisibilités $a_1|f_{j,1}$.
En retranchant successivement $f_{j,1}/a_1$ fois la colonne 1 à la ligne $j > 1$, on obtient une matrice, encore minimale puisque $l(a_1) = l$, du type

$$f = \begin{pmatrix} a_1 & 0 \\ 0 & \phi \end{pmatrix}$$

(on a bien des zéros à côté et au dessus de $\phi = (f_{1+i,1+j})$ car $n, m > 1$). Maintenant, en ajoutant la ligne $i > 1$ à la première, on ne change pas a_1 car $n > 1$ -, de sorte qu'on reste minimal et la première ligne est changée en

$$(a_1, f_{i,2}, \cdots, f_{i,n}).$$

Le même argument que précédemment prouve alors que $f_{i,j}$ est divisible par a_1 si $i > 1$, de même si $j > 1$. Ainsi, $I_\phi \subset (a_1)$. Par hypothèse de récurrence, ϕ est équivalente à une matrice diagonale de coefficients diagonaux $a_2, \cdots, a_n$ avec $(a_n) \subset \cdots \subset (a_2)$. Grâce encore au lemme 3.12, on a alors $I_\phi = (a_2)$, de sorte que f est équivalente à

$$\begin{pmatrix} a_1 & & \cdots & & 0 \\ \vdots & \ddots & & & \vdots \\ 0 & \cdots & a_n & \cdots & 0 \end{pmatrix}, \tag{3.12.a}$$

(utiliser des blocs encore) avec $(a_n) \subset \cdots \subset (a_1)$. Ceci achève la preuve de 3.2, et donc de l'existence dans 1.3 et donc la preuve de 1.1 car la torsion de M est l'idéal engendré par les I_j qui sont non nuls visiblement.■

Exercice 3.13. — *Supposant que l est donnée, écrire la preuve précédente sous forme d'un algorithme. Pouvez-vous écrire un algorithme qui n'utilise pas l dans le cas $\mathbf{Z}, k[X]$ (cf. 3.6), dans le cas euclidien (cf. TD) ?*

3.14. Unicité des facteurs invariants. — Soit M un module de type fini sur A principal. On sait qu'il existe une suite décroissante finie $I_n \cdots I_1$ d'idéaux **propres** de A telle que

$$M \xrightarrow{\sim} \oplus A/I_j.$$

On veut prouver que la suite des I_j ne dépend que de M. Pour montrer l'unicité, il est plus commode de prouver l'énoncé suivant (équivalent par renumérotation).

Proposition 3.15. — *Soit M un A-module. Il existe au plus une suite croissante d'idéaux $I_i, i \geq 0$ telle*

$$M \xrightarrow{\sim} \oplus_{i \geq 0} A/I_k.$$

Preuve : Donnons nous deux telles suites I_i, J_i. Le module $M/\mathrm{Tors}(M)$ est isomorphe à la somme des A/I_i tels que I_i est non nul, de sorte que le K-espace vectoriel $(M/\mathrm{Tors}(M))_K$ est de dimension $d(I) = \inf\{i, \text{ tels que } I_i \neq 0\}$ (cf. 1.2). On a donc $d(I) = d(J)$. Si on a $d(I) = +\infty$, c'est terminé car alors

$$I_i = I_j = 0 \text{ pour tout } i.$$

Sinon, on a

$$I_i = J_i = 0 \text{ si } i < d \text{ et } I_i, J_i \neq 0 \text{ si } i \geq d.$$

Quitte à changer i en $i-d$ et M en $\mathrm{Tors}(M)$, **on peut donc supposer de plus M de torsion** et donc $I_i, J_i \neq 0$ pour tout i.
Si $p \in \mathcal{P}$ engendrant l'idéal premier $\mathfrak{p}$. On a encore $A_\mathfrak{p}$ principal comme on a vu en TD (cf. III.2.3 ou encore plus simplement 2.3), ce qui est facile d'ailleurs et $k = A/\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est un corps. Par localisation, on a

$$M_\mathfrak{p} = \oplus_i A_\mathfrak{p}/(I_{i,\mathfrak{p}})$$

avec $I_{i,\mathfrak{p}}$ suite croissante d'idéaux de $A_\mathfrak{p}$. Si on a prouvé l'unicité dans le cas des modules $A_\mathfrak{p}$-modules, on aura l'unicité.
On peut donc en outre supposer M de torsion sur $A = A_\mathfrak{p}$.
Dans ce cas, on a alors (2.3) $\mathcal{P} = \{p\}$, et

$$I_j = p^{e_j}A \text{ avec } \ e_1 \geq \cdots \geq e_n \geq \cdots \geq 0.$$

On a une **filtration décroissante** de M par des sous-modules

$$0 = p^{e_1}M \subset p^{e_1-1}M \cdots \subset pM \subset p^0 M = M$$

de **gradué**

$$\mathrm{gr}^d M = p^d M/p^{d+1}M.$$

Bien entendu, la filtration et ses gradués sont invariants par isomorphismes au sens que si $\phi : \ M \to M'$ est un isomorphisme de module de p^n torsion, ϕ induit un isomorphisme

$$\mathrm{gr}^d M \xrightarrow{\sim} \mathrm{gr}^d M'$$

pour tout d. L'avantage de ce gradué est qu'il est tué par pA et donc que c'est un $k = A/pA$ espace vectoriel de dimension finie, car M est de type fini !

Lemme 3.16. — *On a la formule*

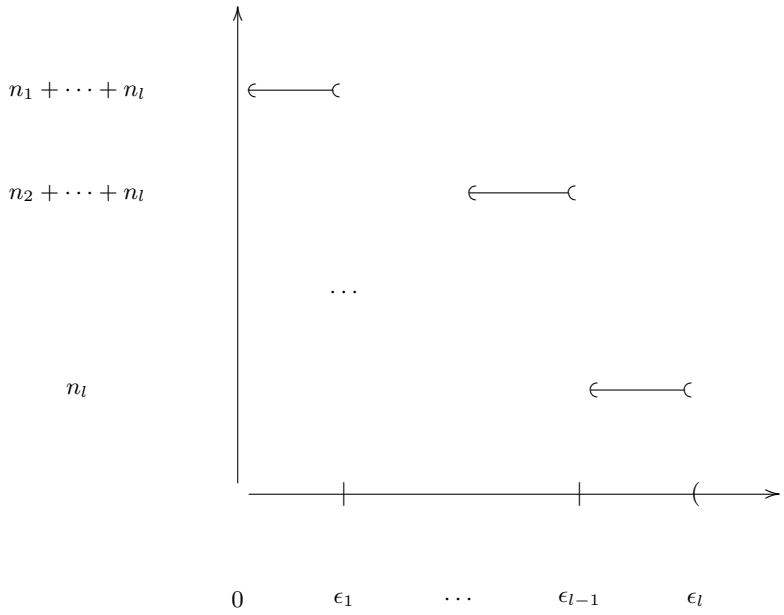
$$\dim_k \mathrm{gr}^d(A/p^e) = \begin{cases} 1 & \text{si } d < e \\ 0 & \text{si } d \geq e \end{cases}$$

Preuve : Le morphisme de multiplication par p^d de A dans $\mathrm{gr}^d(A/p^e)$ se factorise à travers pA, puisque les multiples de p^{d+1} sont nuls dans le gradué. Il est surjectif par construction. Si $d \geq e$, tout multiple de p^d est multiple de p^e donc est nul dans A/p^e. Ainsi, le gradué est nul. Si $d < e$, l'image de 1 dans le gradué serait nulle si on avait une écriture $p^d = p^{d+1}a + p^e B$ dans A ce qui entraînerait $p|1$, ce qui n'est pas.■

Certains des e_j se répètent éventuellement. On écrit M sous la forme

$$\oplus_{j=1}^{l}(A/p^{e_j}A)^{n_j}$$

avec les ϵ_j strictement croissants. Dessinons alors le graphe de $\dim_k \mathrm{gr}^d(M)$, qui a l'allure suivante



et permet donc de récupérer les n_j et les ϵ_j, d'où l'unicité cherchée.■

La preuve du théorème 1.3 est maintenant complète.

4. Algèbre linéaire et facteurs invariants

4.1. Endomorphismes semblables et invariants de similitude. — Soit f un endomorphisme d'un k-espace vectoriel E de dimension finie $d > 0$ donnant lieu à un $A = k[X]$-module M dont on va étudier les invariants de similitude.
D'après le lemme I.21.2, on a une présentation de M

$$0 \longrightarrow E[X] \xrightarrow{X\mathrm{Id}-f} E[X] \xrightarrow{\pi} M \longrightarrow 0$$

où $E[X]$ est libre de rang d. Plus précisément, fixons une base B de E, qui définit à son tour (I.21.1) une base BX de $E[X]$. Soit F la matrice de f dans B. La matrice de $X\mathrm{Id} - f$ dans BX est $X\mathrm{Id} - F$. Mais on sait que $X\mathrm{Id} - F$ est équivalente **une matrice diagonale**

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & P_1 & & & \\ & & & & P_2 & & \\ & & & & & \ddots & \\ & & & & & & P_n \end{pmatrix}$$

où $(P_n) \subset \cdots \subset (P_1)$ où $P_j \neq 1$ sont les générateurs unitaires des facteurs invariants I_j de M, qui sont non nuls, car M est de torsion). Autrement dit, on a $P_1 | \cdots | P_n$.

Définition 4.2. — *Les polynômes P_i s'appellent les invariants de similitude de f.*

Ils se calculent d'après ce qui précède par une méthode de pivot de Gauss raffinée sur la matrice $X\mathrm{Id} - F$. On sait que se donner un automorphisme de $k[X]$-module de M c'est se donner un endomorphisme g de E et un automorphisme u de E tels que $f = ugu^{-1}$ (cf. I.5.2.a).

Théorème 4.3. — *Deux endomorphismes de E sont semblables si et seulement si ils ont mêmes invariants de similitude.*

Exercice 4.4. — *Montrer que $F \in M_d(k)$ est semblable à sa transposée. Calculer les invariants de similitude d'une matrice diagonale.*

***Proposition 4.5* (Invariance par extension de corps)**. — *Soit k' un surcorps de k. Alors, les invariants de similitude de F vue comme matrice de k ou de k' sont les mêmes.*

Preuve : En effet, on sait qu'il existe $P, Q \in GL_d(k[X])$ tels que

$$X\mathrm{Id} - F = P \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & P_1 & & & \\ & & & & P_2 & & \\ & & & & & \ddots & \\ & & & & & & P_n \end{pmatrix} Q.$$

Mais cette formule est aussi valable dans $M_d(k'[X])$, ce qu'on voulait.■

Corollaire 4.6. — *Si k est un sous-corps de k', deux matrices de $M_d(k)$ semblables dans $M_d(k')$ sont semblables dans $M_d(k)$.*

4.7. Une autre façon de voir Cayley-Hamilton. — Il existe donc $P, Q \in GL_d(k[X])$ tels que

$$X\mathrm{Id} - F = P \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & P_1 & & & \\ & & & & P_2 & & \\ & & & & & \ddots & \\ & & & & & & P_n \end{pmatrix} Q.$$

Mais les déterminants de P, Q sont des inversibles de $k[X]$, donc des scalaires non nuls de k. Ainsi, on a la formule

$$P_1 \cdots P_n = \det(X\mathrm{Id} - F) = \chi_f \tag{4.7.a}$$

et donc on a

$$P_n | \chi_f | P_n^n$$

reliant facteurs invariants et polynômes caractéristique (a priori, les deux membres sont multiples l'un de l'autre, mais on a égalité car ils sont unitaires) .

***Corollaire 4.8* (Théorème de Cayley-Hamilton)**. — *Le polynôme minimal μ_f de f est P_n. Le polynôme caractéristique χ_f caractéristique annule f. Plus précisément, les polynômes caractéristique et minimal de f ont mêmes facteurs irréductibles.*

Preuve : En effet $\mathrm{Ann}(M) = (P_n)$ et les annulateurs de f sont les annulateurs de M. Il suffit alors d'invoquer la relation $P_n|\chi_f|P_n^n$.■

Exercice 4.9. — *Montrer qu'on a l'égalité* $\dim_k E_P = v_P(\chi_f)\deg(P)$ *(cf. 2.9.a). Calculer les invariants de similitude d'une matrice diagonale. Retrouver ainsi qu'un endomorphisme est diagnalisable si et seulement si son polynôme minimal est scindé à racines simples.*

4.10. Réduction de Jordan des endomorphismes. — Donc, explicitement, il existe un isomorphisme d'espaces vectoriels $\phi : E \xrightarrow{\sim} \oplus_i k[X]/(P_i)$ tel que $\phi \circ f \circ \phi^{-1}$ soit la multiplication par X dans le $k[X]$-module f, et donc, dans une base convenable, la matrice de f est la matrice de la multiplication par X dans une base, qu'on choisira habilement !

Exercice 4.11. — *Montrer que la dimension du commutant de* f *est* $\geq d$.

a) Le cas nilpotent. — C'est le cas μ_f (ou χ_f) étant une puissance de f. On pose $n_i = \deg(P_i)$. C'est une suite décroissante d'entiers > 0 de somme n. Dans chaque $k[X]/(X^{n_i})$, on choisit les classes de $1, \cdots, X^{n_{i-1}}$ comme base, et on les rassemble dans cet ordre. Comme $X.X^a = X^{a+1}$, on a une matrice diagonale $\mathrm{diag}(J(n_i))$ où $J(n_i)$ est le bloc de Jordan standard de taille n_i

$$J(n_i) = \begin{pmatrix} 0 & 0 & & \cdots \\ 1 & 0 & 0 & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$$

b) Le cas $\chi = \chi_f$ *scindé.* — D'après Cayley-Hamilton, le module M est tué par χ. Soit χ_i ses facteurs irréductibles (unitaires). On a alors $M = \oplus M_{\chi_i}$ et évidemment M_{χ_i} est **l'espace caractéristique** associé à χ_i (on retrouve le lemme des noyaux si on veut).

Exercice 4.12. — *Montrer que la suite des dimensions* d_i *des des noyaux de* f^i *est strictement croissante puis stationnaire. Montrer que la suite des différences* $d_{i+1} - d_i$ *est monotone.*

Exercice 4.13. — *Soit* p *un nombre premier. Combien y a-t-il de matrices nilpotentes dans* $M_2(\mathbf{Z}/p\mathbf{Z}), M_3(\mathbf{Z}/p\mathbf{Z})$ *?*

Exercice 4.14. — *Étudier les sous-espaces stables d'un endomorphisme nilpotent. À quelle condition un endomorphisme de* k^n *n'a-t-il qu'un nombre fini de sous espaces stables ?*

Supposons $\chi_i = (X - \lambda_i)^{m_i}$ avec $\lambda_i \in k$ (le cas scindé). Alors, chaque M_{χ_i} est de la forme

$$\oplus k[X]/(X - \lambda_i)^{n_{i,j}}$$

où comme tout à l'heure $(n_{i,j})_j$ est une suite décroissante d'entiers > 0. En choisissant cette fois ci comme base les classes des monômes $(X - \lambda_i)^d$ en degré $< n_{i,j}$, on s'aperçoit que f à une matrice (dans une base convenable) de la forme $\mathrm{diag}(J(\lambda_i, n_{i,j}))$ où $J(\lambda_i, n_{i,j})$ est la matrice de taille $n_{i,j}$

$$J(\lambda_i, n_{i,j}) = \begin{pmatrix} \lambda_i & 0 & 0 & \cdots \\ 1 & \lambda_i & 0 & 0 \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

Les applications de cet énoncé sont très nombreuses (voir TD) en algèbre, comme en analyse (stabilité de Lyapounov des équations différentielles par exemple). Le lecteur pourra s'amuser à regarder ce qui se passe dans le cas réel.

On verra en TD d'autres applications (décomposition en somme de matrices cycliques qui commutent...) et comment la version algorithmique de la décomposition des matrices dans le cas polynômial permet de calculer les invariants de similitude. Dans le chapitre suivant, on va étudier les notions relatives au produit tensoriel. Il permettra en particulier -ce n'est pas sa seule vertu, loin s'en faut !- de donner une version intrinsèque du « passage aux complexes pour une matrice », ou, plus généralement, de passer à un corps plus gros.

PARTIE V

CONSIDÉRATIONS TENSORIELLES, OU COMMENT REMPLACER DU BILINÉAIRE PAR DU LINÉAIRE

On se donne deux modules M et N sur un anneau A.

1. Existence

On se propose d'étudier le foncteur qui à un module T associe l'ensemble $Tens(T)$ des applications A-bilinéaires de $M \times N$ dans T. Bien entendu, si $f \in \mathrm{Hom}(T, T')$, une application bilinéaire $b \in Tens(T)$ définit par composition une application bilinéaire $f \circ b \in Tens(T')$.

Proposition 1.1. — *Le foncteur $Tens$ de $\mathcal{M}od_A$ dans $\mathcal{E}ns$ est représentable par un A-module $M \otimes_A N$, défini à isomorphisme unique près, appelé produit tensoriel de M et N.*

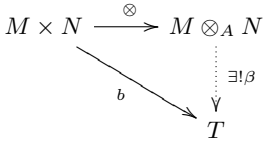
Autrement dit, on a une bijection, fonctorielle en T,

$$Tens(T) \xrightarrow{\sim} \mathrm{Hom}_A(M \otimes N, T), \tag{1.1.a}$$

ie se donner une application b *bilinéaire* à valeurs dans T c'est se donner une application β *linéaire* de $M \otimes N$ dans T. Bien entendu, faisant $T = M \otimes_A N$ et $\beta = \mathrm{Id}$, on en déduit l'existence d'une application bilinéaire canonique

$$\otimes : \left\{ \begin{array}{ccc} M \times N & \to & M \otimes_A N \\ (m,n) & \mapsto & m \otimes n \end{array} \right.$$

On se souviendra du diagramme commutatif résumant la propriété universelle



Preuve : On considère l'énorme module libre $L = A^{(M \times N)}$ de base $[m,n], m \in M, n \in N$. Soit K le sous-module de L engendré par

$$[m+m',n]-[m,n]-[m',n],[m,n'+n]-[m,n]-[m,n'],[am,n]-a[m,n],[m,an]-a[m,n], a \in A, m,m' \in M, n,n' \in N.$$

Se donner une application A-linéaire β de L dans T, c'est se donner une application b de $M \times N$ dans T (propriété universelle du module libre). Dire que b est bilinéaire, c'est dire que β se factorise à travers K (propriété universelle du quotient). Il suffit alors de poser $M \otimes_A N = L/K$. L'unicité est toujours vérifiée pour le représentant d'un foncteur comme on l'a observé. ■

Il va sans dire qu'il est rarissime de dire quoi que ce soit sur le produit tensoriel avec sa construction. On se sert de la propriété universelle.

Remarque 1.2. — *Si on répugne à manipuler des objets définis à isomorphisme unique près, on pourra penser à $M \otimes_A N$ comme étant égal à L/K comme plus haut.*

Exercice 1.3. — *Montrer que la multiplication externe $A \times M \to M$ définit un isomorphisme canonique*

$$A \otimes_A M \xrightarrow{\sim} M.$$

2. Fonctorialité en M, N

Donnons nous deux morphismes de modules $\mu : \ M \to M'$ et $\nu : \ N \to N'$. On a évidemment une application bilinéaire

$$M \times N \to M' \otimes_A N'$$

qui à (m, n) associe $\mu(m) \otimes \nu(n)$. Elle se factorise donc à travers $M \otimes_A N$ définissant

$$\mu \otimes \nu : \ M \otimes_A N \to M' \otimes_A N'$$

caractérisée par

$$\mu \otimes \nu(m \otimes n) = \mu(m) \otimes \nu(n) \text{ pour tout } m \in M, \ n \in N.$$

Ces applications se composent, de sorte qu'on peut voir la correspondance $M \mapsto M \otimes_A N$ comme en foncteur en N (et idem de l'autre côté, en faisant varier N cette fois).

3. Tenseurs purs

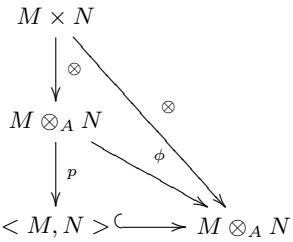
Un élément de la forme $m \otimes n$ s'appelle un **tenseur pur**. La structure de module est donnée par définition par

$$a.m \otimes n = (am) \otimes n = m \otimes (an).$$

On prendra garde qu'en général un **tenseur** (*ie* un élément de $M \otimes N$) n'est pas un tenseur pur, mais une combinaison linéaire de tels tenseurs comme l'assure le lemme suivant.

Lemme 3.1. — *Le module engendré par l'image de $M \times N$ dans $M \otimes_A N$ est $M \otimes_A N$.*

Preuve : En effet, soit $< MN >$ cette image. L'application $\otimes : \ M \times N \to M \otimes_A N$ est à valeurs dans ce sous-module $< MN >$, donc se factorise à travers le produit tensoriel en une application linéaire $p : \ M \otimes_A N \to < MN >$. Autrement dit, on a un diagramme commutatif



où ϕ est le composé de p et de l'inclusion, donc est linéaire. Mais l'identité de $M \otimes_A N$ fait commuter le triangle de droite, et donc, par unicité de la factorisation de l'application bilinéaire $\otimes$, on a $\phi = \mathrm{Id}$ et donc p surjectif.■

On aurait pu aussi remarquer que les classes $m \otimes n$ de $[m, n]$ dans L/K engendrent par construction le produit tensoriel.

4. Commutativité du produit tensoriel

L'application $(m,n) \mapsto n \otimes m$ est bilinéaire, donc définit une application canonique

$$s_{M,N} : \ M \otimes_A N \to N \otimes_A M.$$

Lemme 4.1. — *L'application précédente est un isomorphisme.*

Preuve : Il suffit de vérifier que $s_{M,N}$ et $s_{N,M}$ sont inverses l'une de l'autre.Il suffit de le faire sur les tenseurs purs (qui engendrent) et là, c'est clair car, par définition,

$$s_{M,N} \circ s_{N,M}(n \otimes m) = s_{M,N}(m \otimes n) = n \otimes m$$

et, du coup,

$$s_{N,M} \circ s_{M,N}(m \otimes n) = s_{N,M}(n \otimes m) = m \otimes n.$$

■

Ceci nous permettra d'identifier ces deux modules (on dit que le produit tensoriel est commutatif).

5. Produit tensoriel et somme directe

On se donne une famille de modules A-modules $M_i, i \in I$ et un module N. L'application bilinéaire

$$\begin{cases} (\oplus_i M_i) \times N & \to & \oplus_i (M_i \otimes_A N) \\ (\sum_i m_i, n) & \mapsto & \sum_i m_i \otimes n \end{cases}$$

définit une application linéaire

$$(\oplus_i M_i) \otimes_A N \to \oplus_i (M_i \otimes_A N).$$

Notons qu'on a abusivement noté de la même manière les application bilinéaires canoniques des divers produits cartésiens vers les produits tensoriels.

Lemme 5.1. — *L'application précédente est un isomorphisme.*

Preuve : Construisons une application dans l'autre sens. Il suffit de construire une application

$$M_j \otimes_A N \to (\oplus_j M_j) \otimes_A N$$

pour chaque j, autrement dit une application bilinéaire

$$M_j \times N \to (\oplus_j M_j) \otimes_A N.$$

On considère alors l'application évidente $(m_j, n) \mapsto (m_j \otimes n)$ où m_j est l'image dans $\oplus_i M_i$ de m_j. On doit vérifier que les deux applications précédentes sont inverses l'une de l'autre. Il suffit de le faire sur des générateurs. Or c'est évident sur les tenseurs purs.■

On identifiera sans plus de précaution ces deux modules (on dit que le produit tensoriel commute à la somme directe).
En particulier, si $M = A^{(I)}$, le foncteur produit tensoriel par N s'identifie à $N \mapsto N^{(I)}$, une flèche $f \in \mathrm{Hom}(N,P)$ induisant la flèche diagonale $\mathrm{diag}(f) : N^{(I)} \to P^{(I)}$.

Corollaire 5.2. — *Si M, N sont libres de base m_i, n_j, alors $M \otimes_A N$ est libre de base $m_i \otimes n_j$.*

Exercice 5.3. — *Soient E, F deux espaces vectoriels de dimension finie sur $\mathbf{C}$ et f, g des endomorphismes de E, F. Calculer les valeurs propres de $f \otimes g$ en fonction de celles de f et g. Comparer les déterminants.*

Exercice 5.4. — *Retrouver l'unicité du rang d'un module libre de la manière suivante : supposer qu'on a un isomorphisme* $i : A^n \xrightarrow{\sim} A^m$ *(*A *anneau non nul), choisir* $\mathfrak{m}$ *maximal dans* A *et tensoriser* i *et conclure.*

6. Exactitude à droite du produit tensoriel

Donnons nous une suite exacte

$$M_1 \xrightarrow{f} M_2 \xrightarrow{f} M_3 \to 0$$

de A-modules. On en déduit un complexe (fonctorialité)

$$M_1 \otimes_A N \xrightarrow{f\otimes \mathrm{Id}} M_2 \otimes_A N \xrightarrow{g\otimes \mathrm{Id}} M_3 \otimes_A N \to 0. \tag{6.a}$$

En général, on n'écrit pas les flèches (on sous-entend qu'on a tensorisé par l'identité de N).

Proposition 6.1. — *La suite 6.a est exacte.*

Preuve : D'après le lemme I.17.1, il suffit de prouver que pour tout module T, la suite

$$0 \to \mathrm{Hom}(M_3 \otimes_A N, T) \to \mathrm{Hom}(M_2 \otimes_A N, T) \to \mathrm{Hom}(M_1 \otimes_A N, T)$$

est exacte. On sait que c'est un complexe. On identifie ces homomorphismes aux applications bilinéaires associées.
Comme on sait que la suite est un complexe, il s'agit de vérifier qu'une application bilinéaire $b : M_2 \times N \to T$, nulle sur $f(N_1) \times N$, provient d'une unique application bilinéaire de $M_3 \times N = M_2/f(M_1) \times N$. À n fixé, c'est la propriété universelle du quotient. Il suffit ensuite de faire varier n.■

Remarque 6.2. — *On peut procéder directement. La surjectivité à droite est claire. Par fonctorialité, le composé*

$$M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N$$

est nul de sorte qu'il s'agit de montrer que la surjection

$$M_2 \otimes_A N/(f \otimes \mathrm{Id})(M_1 \otimes_A N) \twoheadrightarrow M_3 \otimes_A N$$

est injective. En fait on construit l'inverse comme suit : on a une application bilinéaire

$$M_2 \times N \to M_2 \otimes_A N/(f \otimes \mathrm{Id})(M_1 \otimes_A N)$$

qui se factorise en une application bilinéaire

$$M_3 \times N \to M_2 \otimes_A N/(f \otimes \mathrm{Id})(M_1 \otimes_A N)$$

car $M_1 \otimes N$ *est tué. Elle définit donc une application linéaire*

$$M_3 \otimes N \to M_2 \otimes_A N/(f \otimes \mathrm{Id})(M_1 \otimes_A N)$$

dont on vérifie que c'est l'inverse cherché.

Si I est un idéal de A, l'application linéaire $m \mapsto 1 \otimes m$ de M dans $A/I \otimes_A M$ est nulle sur IM et donc définit une application

$$c_M : M/IM \to A/I \otimes_A M.$$

Corollaire 6.3. — *Le morphisme* c_M *est un isomorphisme (fonctoriel en* M*).*

Preuve : En effet, si on tensorise la suite

$$0 \to I \to A \to A/I \to 0$$

par M, on trouve une suite exacte

$$I \otimes_A M \to A \otimes_A M = M \to A/I \otimes_A M \to 0.$$

L'image de $I \otimes_A M \to M$ est IM et ainsi on a un isomorphisme

$$M/IM \xrightarrow{\sim} A/I \otimes_A M$$

qui évidemment est c.■

Ce résultat est fondamental, et à base de nombreux calculs de produits tensoriels. On identifiera sans plus de précaution M/IM et $A/I \otimes_A M$.

Exercice 6.4. — *Soient n, m deux entiers > 0 et d leur PGCD. Montrer l'égalité*

$$m\mathbf{Z}/n\mathbf{Z} = d\mathbf{Z}/n\mathbf{Z}.$$

En déduire un isomorphisme

$$\mathbf{Z}/n\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/m\mathbf{Z} = \mathbf{Z}/d\mathbf{Z}.$$

7. Défaut d'exactitude du produit tensoriel

Le produit tensoriel ne conserve pas l'exactitude à gauche du produit tensoriel. Par exemple, considérons la suite

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

pour $n > 0$. Si on tensorise par $\mathbf{Z}/n\mathbf{Z}$, on obtient la suite exacte

$$\mathbf{Z}/n\mathbf{Z} \xrightarrow{n} \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \to 0$$

et la flèche

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

est très loin d'être injective, puisqu'elle est... nulle. On verra que le défaut d'exactitude est contrôlé par des modules « dérivés » du produit tensoriel, les modules $\mathrm{Tor}_i^A(M, N), i > 0$.

Exercice 7.1. — *Supposons qu'on ait une suite exacte*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

de A-modules libres. Montrer que si M_3 est libre, la suite est scindée. En déduire que la suite reste exacte après tensorisation par tout module N. Montrer que si A est principal, on peut supposer seulement M_3 sans torsion (pas nécessairement de type fini) : M_3 est un exemple de module plat.

Exercice 7.2. — *Montrer que si S est une partie multiplicativement stable de A alors on un isomorphisme canonique $S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$. En déduire, si A est intègre, que la tensorisation par le corps des fractions de A est un foncteur exact (transforme suite exacte en suite exacte).*

8. Extension des scalaires

On se donne une A-algèbre B et un A-module M. Le produit $B \otimes_A M$ est naturellement muni d'une structure de B-module caractérisée sur les tenseurs purs par

$$b'(b \otimes m) = (b'b) \otimes m \text{ pour tout } b, b' \in B, m \in M.$$

On dit qu'on a étendu les scalaires de A à B. Si M est libre de rang n, on a vu que $B \otimes_A M$ est libre de même rang (commutation du produit tensoriel et de la somme directe et isomorphisme $B \otimes_A A \xrightarrow{\sim} B$). Regardons ce qu'il advient des endomorphismes dans ce cas $M = A^n$. Un tel endomorphisme f est défini par une matrice F à coefficients dans A (qui représente f dans la base canonique notée e_i de A^n). Dans l'isomorphisme canonique $B \otimes_A (A^n) \xrightarrow{\sim} B^n$, l'image de $1 \otimes e_i$ est le i-ème vecteur de la base canonique et (vérifier !) la matrice de $1 \otimes F$ est l'image de $F \in M_n(A)$ dans $M_n(B)$.
Un cas particulier important où A, B sont des corps. C'est la version canonique de regarder une matrice dans un corps plus gros. Dans le cas d'un $\mathbf{R}$-espace vectoriel de dimension finie E, on dit que $\mathbf{C} \otimes_{\mathbf{R}} E$ est le complexifié de E.
Si maintenant on a une seconde A-algèbre B', le produit tensoriel $B \otimes_A B'$ est muni canoniquement d'une structure d'algèbre caractérisée au niveau des tenseurs purs par

$$(b \otimes b')(\beta \otimes \beta') = (bb') \otimes (\beta\beta').$$

Mais attention, le produit tensoriel de deux corps est souvent non intègre voire non réduit (*ie* avec des nilpotents), ce que le lecteur comprendra mieux avec la théorie de Galois (cf. l'exercice 10.4).

9. Associativité du produit tensoriel

On se donne une A-algèbre B et une B algèbre C. On se donne un A-module M_3, un B-module M_2 et un C-module M_1, qui, bien entendus peuvent être vus comme des A-modules (*restriction des scalaires*). Le produit tensoriel $M_2 \otimes_A M_3$ hérite de la structure de B-module provenant de celle de M_2 tandis que le C-module $M_1 \otimes_B M_2$ peut aussi être vu comme un B-module, soit par restriction des scalaires, soit grâce à la structure de B-module de M_2 : c'est la même chose (vérifier !).
Pour tout $m_1 \in M_1$, on a une application A-bilinéaire

$$\begin{cases} M_2 \times_A M_3 & \to & (M_1 \otimes_B M_2) \otimes_A M_3 \\ (m_2, m_3) & \mapsto & (m_1 \otimes m_2) \otimes m_3 \end{cases}$$

et définit un morphisme A-linéaire $c(m_1) :\ M_2 \otimes_A M_3 \to (M_1 \otimes_B M_2) \otimes_A M_3$. On a

$$c(m_1)(bm_2 \otimes m_3) = (m_1 \otimes bm_2) \otimes m_3 = (b(m_1 \otimes m_2)) \otimes m_3$$

et donc $c(m_1)$ est même B-linéaire (il est suffisant de le vérifier sur les tenseurs purs). Comme l'application

$$\begin{cases} M_1 \times (M_2 \otimes_A M_3) & \to & (M_1 \otimes_B M_2) \otimes_A M_3 \\ (m_1, m_2 \otimes m_3) & \mapsto & c(m_1)(m_2 \otimes m_3) \end{cases}$$

est bilinéaire, elle définit un morphisme

$$c :\ M_1 \otimes_B (M_2 \otimes_A M_3) \to (M_1 \otimes_B M_2) \otimes_A M_3$$

dont on vérifie qu'il est C-linéaire.

Lemme 9.1. — *Le morphisme c est un isomorphisme de C-modules.*

Le preuve est facile et laissée au lecteur (on construit comme d'habitude un inverse) et, comme d'habitude, on identifiera les deux membres de l'isomorphisme.

10. Produit tensoriel d'algèbres de polynômes

On se donne une A-algèbre B (autrement dit un morphisme d'algèbre de A dans B).

Lemme 10.1. — *Le morphisme de B-algèbres $B[X] \to B \otimes_A A[X]$ caractérisé par $X \mapsto 1 \otimes X$ est un isomorphisme.*

Preuve : Comme d'habitude, on construit une application dans l'autre sens. On doit donc construire une application A-bilinéaire $B \times A[X] \to B[X]$. Considérons simplement le produit $(b, P_A(X) \mapsto bP_B(X)$ où $P_B(X)$ est l'image de $P_A(X) \in A[X]$ dans $B[X]$. Il est bilinéaire, se factorise à travers $B \otimes_A A[X]$. On vérifie que la factorisation est bien un inverse.■

En appliquant à B une algèbre de polynômes, on déduit immédiatement

Corollaire 10.2. — *Soient $X_1, \cdots, X_n, Y_1, \cdots, Y_m$ des indéterminées. Alors, on a un isomorphisme de A-algèbres*

$$A[X_i] \otimes_A A[Y_j] \xrightarrow{\sim} A[X_i, Y_j]$$

caractérisé par

$$X_i \otimes 1 \mapsto X_i \text{ et } 1 \otimes Y_j \mapsto Y_j.$$

Exercice 10.3. — *Avec les notations du corollaire, supposons qu'on ait en outre deux idéaux $I = (P(X_i))$ et $J = (Q(Y_j))$. Montrer qu'on a un isomorphisme canonique*

$$(A[X_i]/I) \otimes_A (A[Y_j]/J) \xrightarrow{\sim} A[X_i, Y_j]/(P(X_i), Q(Y_j)).$$

Exercice 10.4. — *Montrer qu'on a $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \xrightarrow{\sim} \mathbf{C}^2$ [Écrire un des deux $\mathbf{C}$ sous la forme $\mathbf{R}[X]/(X^2+1)$. Plus généralement (pour le lecteur féru d'extensions de corps), montrer que si L est une extension finie séparable d'un corps K et L' est une extension de K, alors $L \otimes_K L'$ est réduit (sans nilpotent) et en général pas un corps [Utiliser le théorème de l'élément primitif]. Montrer que ce n'est pas le cas sans hypothèse de séparabilité.*

11. Produit tensoriel et module d'homomorphismes

On se donne trois A-modules M_1, M_2, M_3. Si on a un morphisme $\phi \in \mathrm{Hom}_A(M_1, M_2)$ et un élément de M_3, on associe un morphisme de $\mathrm{Hom}(M_1, M_2 \otimes_A M_3)$ défini par $m_1 \mapsto \phi(m_1) \otimes m_3$ qui définit (vérifier !) un morphisme

$$\mathrm{Hom}(M_1, M_2) \otimes_A M_3 \to \mathrm{Hom}(M_1, M_2 \otimes_A M_3).$$

Lemme 11.1. — *Supposons M_1 libre de rang fini n. Alors, le morphisme précédent est un isomorphisme.*

Preuve : Choisissons un isomorphisme $i : M_1 \xrightarrow{\sim} A^{(I)}$ avec I fini. On a alors la suite d'isomorphismes (on met « = » quand l'isomorphisme est canonique)

$$\begin{aligned}\mathrm{Hom}(M_1, M_2) \otimes_A M_3 \xrightarrow{\sim} &\mathrm{Hom}(A^{(I)}, M_2) \otimes M_3\\ &= \prod_{i\in I} \mathrm{Hom}(A, M_2) \otimes_A M_3\\ &= \oplus_{i\in I} \mathrm{Hom}(A, M_2) \otimes_A M_3 \text{ car I fini}\\ &= M_2^{(I)} \otimes_A M_3 (\text{on remarque } \mathrm{Hom}(A, M_2) = M_2)\\ &= (M_2 \otimes_A M_3)^{(I)}\\ &= \mathrm{Hom}(A^{(I)}, M_2 \otimes_A M_3)\\ \mathrm{Hom}(M_1, M_2 \otimes_A M_3) \xleftarrow{\sim} &\end{aligned}$$

Il suffit alors de constater que cette suite d'isomorphismes est le morphisme précédent pour conclure (il ne dépend pas de i).■

Exercice 11.2. — *Montrer que si on suppose seulement que M_1 est facteur direct d'un module libre de rang fini alors la conclusion du lemme demeure (un tel module est dit projectif).*

12. Algèbre tensorielle

On peut définir la puissance tensorielle n-ième $T^n(M)$ de M, par exemple par récurrence en posant

$$T^0(A) = A \text{ et } T^{n+1}(M) = T^n(M) \otimes_A M \text{ si } n \geq 0.$$

On définit alors

$$T(M) = \oplus_{n\geq 0} T^n(M).$$

On définit par récurrence une application $b_n : M^n \to T^n(M)$ en posant $b_0 = \mathrm{Id}_A$ et $b_{n+1}(m_1, \cdots, m_{n+1}) = b_n(m_1, \cdots, m_n) \otimes m_{n+1}$. On vérifie que b_n est linéaire en chacune des variables (on dit alors n-linéaire). On note alors bien entendu

$$b(m_1, \cdots, m_n) = m_1 \otimes \cdots \otimes m_n.$$

Une récurrence immédiate permet de prouver le résultat suivant.

Lemme 12.1. — *Soit $g : M^n \to N$ une application n-linéaire. Il existe une unique application linéaire $g : T^n(M) \to N$ telle que $g = \gamma \circ b_n$.*

Exercice 12.2. — *Montrer qu'il existe une unique opération de S_n sur $T^n(M)$ qui opère par permutation des indices des tenseurs purs.*

L'isomorphisme d'associativité du produit tensoriel se généralise en un isomorphisme canonique

$$p_{n,m} : T^n(M) \otimes_A T^m(M) \xrightarrow{\sim} T^{n+m}(M).$$

On définit alors une application, visiblement bilinéaire

$$p : T(M) \times T(M) \to T(M)$$

définie par

$$p(\sum t_n, \sum \tau_m) = \sum p_{n,m}(t_n, \tau_m).$$

Le lemme suivant est laissé au lecteur.

Lemme 12.3. — *L'application p fait de $T(M)$ une A-algèbre graduée associative, de neutre $1 \in A = T^0(M)$.*

On dit que $T(M)$ est l'algèbre tensorielle de M. Attention toutefois, $T(M)$ n'est en général pas commutative.

Exercice 12.4. — *Vérifier que $T^+(M) = \oplus_{n>0} T^n(M)$ est un idéal bilatère de $T(M)$. Quel est le quotient $T(M)/T^+(M)$?*

Bien entendu, la construction $M \mapsto T(M)$ est fonctorielle en M : si $f \in \mathrm{Hom}(M, N)$, il existe un unique morphisme de A-algèbres graduées

$$T(f) : T(M) \to T(N)$$

qui induit f sur $T^1(M) = M$ (exercice).

PARTIE VI

ALGÈBRE EXTÉRIEURE

On s'intéresse ici aux applications n-linéaires **alternées** a de M^n dans un module T, *ie* qui vérifient $a(m_1, \cdots, m_n) = 0$ dès qu'il existe $i < j$ tels que $m_i = m_j$. Le lecteur est invité à aller regarder le cas symétrique, analogue, mais en fait plus simple, et qui ne nous servira pas.

1. Définition

Soit $\mathfrak{a}$ l'idéal bilatère engendré par les tenseurs purs $m \otimes m, m \in M$. C'est un idéal homogène, somme directe de ses composantes homogènes $\mathfrak{a}_n = \mathfrak{a} \cap T^n(M)$. Si on veut préciser M, on notera $\mathfrak{a}_n(M)$.

Lemme 1.1. — *Soit $t \in T^n(M)$ et $\sigma \in S_n$ une permutation. Alors,*

$$\sigma.t \equiv \epsilon(\sigma)t \mod \mathfrak{a}_n.$$

Preuve : Il suffit de le montrer pour une transposition $\sigma = (i, i+1)$ car ces transpositions engendrent S_n. Mais on a

$$(m+n) \otimes (n+m) \equiv n \otimes m + m \otimes n \mod \mathfrak{a}_2$$

de sorte qu'on a

$$t_{i-1} \otimes m \otimes n \otimes t'_{n-i-1} \equiv -t_{i-1} \otimes n \otimes m \otimes t'_{n-i-1} \mod \mathfrak{a}_n$$

avec $t_i \in T^{i-1}(M), t'_{n-i-1} \in T^{n-i-1}(M)$, ce qu'on voulait.■

Corollaire 1.2. — *On a $m_1 \otimes \cdots \otimes m_n \equiv 0 \mod \mathfrak{a}$ dès qu'il existe $i < j$ tels que $m_i = m_j$.*

Preuve : On applique la permutation envoyant le couple (i, j) sur $(1, 2)$ par exemple.■

Définition 1.3. — *L'algèbre quotient $\bigwedge M = T(M)/\mathfrak{a}$ s'appelle l'algèbre extérieure de M et son produit se note $\wedge$. Sa partie $\bigwedge^n(M) = T^n(M)/\mathfrak{a}_n$ de degré n s'appelle la puissance extérieure n-ième.*

Exemple 1.4. — *Comme $\mathfrak{a}_0$ et $\mathfrak{a}_1$ sont nuls, on a $\bigwedge^0(M) = A$ et $\bigwedge^1(M) = M$.*

Le lemme précédent assure que le morphisme dit canonique,

$$M^n \to \bigwedge^n(M)$$

qui à $(m_1, \cdots, m_n)$ associe $m_1 \wedge \cdots \wedge m_n$ est alterné. La proposition suivante est immédiate (propriété universelle du quotient)

Proposition 1.5. — *Le foncteur qui à N associe les applications n-alternées de M^n dans N est représentable par le morphisme canonique $M^n \to \bigwedge^n(M)$.*

Exemple 1.6. — *Le déterminant est une application n-linéaire alternée de $(A^n)^n = M_n(A)$ dans A. On a donc une application linéaire* $\det : \bigwedge^n(A^n) \to A$ *caractérisée par* $\det(e_1 \wedge \cdots \wedge e_n) = 1$.

Bien entendu, la **fonctorialité** en M du produit tensoriel induit une **fonctorialité** en M de la puissance extérieure : il suffit pour cela de constater que si $f \in \mathrm{Hom}(M,N)$, alors $T(f)$, envoie $\mathfrak{a}(M)$ dans $\mathfrak{a}(N)$, ce qui est immédiat, et donc passe au quotient. On notera $\bigwedge(f)$ l'application quotient. On a donc

$$\bigwedge(f\circ g)=\bigwedge(f)\circ\bigwedge(g) \tag{1.6.a}$$

pour f, g linéaires composables.

2. Cas d'un module libre

On s'intéresse au cas $M=A^n$. On note $(e_1,\cdots,e_n)$ la base canonique de M. Si I est une partie de $[1,\cdots,n]$ à k éléments, on note e_I le produit extérieur $e_I=e_{i_1}\wedge\cdots\wedge e_{i_k}$ où $i_1<\cdots<i_k$ est la suite ordonnée des éléments de I. On convient que $e_\emptyset=1\in A=\bigwedge^0 A$. Comme $\bigwedge^k(M)$ est un quotient de $M^{\otimes k}$, et que $\sigma.e_I=\pm e_I$, la famille des e_I engendre M.

Proposition 2.1. — *Le module $\bigwedge^k(A^n)$ est libre de base e_I où I décrit les parties à k éléments de $[1,\cdots,n]$.*

Preuve : Supposons qu'on ait une relation $\sum_I a_I e_I$ dans $\bigwedge^k(A^n)$. Montrons que tous les a_I sont nuls. Soit J le complémentaire de I dans $[1,\cdots,n]$. Si I' de cardinal k est distinct, il rencontre J et donc $e_{I'}\wedge e_J=0$. Donc, en multipliant par e_J la relation, on obtient $a_I e_1\wedge\cdots\wedge e_n=0$ dans $\bigwedge^n(A^n)$. En appliquant det (exemple 1.6), on obtient $a_I=0$.■

Par exemple, la matrice dans les bases précédentes de $\bigwedge^k(f)$ pour $f\in\mathrm{Hom}_A(A^n,A^m)=M_{m,n}(A)$ est la matrice des **cofacteurs** de f de taille k.

Corollaire 2.2. — *Si $u,v\in M_n(A)$, on a $\det(uv)=\det(u)\det(v)$.*

Preuve : En effet, c'est la formule $\bigwedge^n(u\circ v)=\bigwedge^n(u)\circ\bigwedge^n(v)$.■

Exercice 2.3. — *Donner une nouvelle preuve de l'unicité du rang d'un module libre de type fini.*

Exercice 2.4. — *Soit $f: A^n\to A^m$ un morphisme et k un entier. On se donne des parties I,J à k éléments de $[1,\cdots,n],[1,\cdots,m]$. Montrer que le coefficient d'indice I,J de la matrice de $\wedge^k f$ dans les bases canoniques est le mineur d'indice I,J de la matrice de f. En déduire que si A est principal, le PGCD des mineurs d'ordre k de f est le produit $d_1\cdots d_k$ des facteurs invariants de f [Faire d'abord le calcul dans le cas diagonal, puis passer à une matrice équivalente].*

2.5. Produit extérieur et famille libre. — Si $x_1,\cdots,x_n$ sont des éléments du module libre $M=A^N$ de base $e_1,\cdots,e_N$, la coordonnée de $x_1\wedge\cdots\wedge\cdots x_n$ relativement à $e_I\in\bigwedge^n M$ est le cofacteur obtenue par extraction des lignes d'indice $i\in I$ de la matrice (N,n) des coordonnées de x_i dans (e_i). Si A est un corps, le cours d'algèbre linéaire nous apprend que les x_i sont liés si et seulement si $x_1\wedge\cdots\wedge x_n=0$. En général, on a

Proposition 2.6. — *Si M est libre de rang fini, alors les x_i sont liés si et seulement si il existe un scalaire $\lambda\neq 0$ tel que $\lambda x_1\wedge\cdots\wedge x_n=0$.*

Comme d'habitude, on note $x_1\cdots\wedge\widehat{x_i}\wedge\cdots\wedge x_n$ le produit extérieur des $x_j, j\neq i$ calculé dans l'ordre.
La partie directe est claire. En effet, si on a une relation de liaison

$$a_1x_1+\cdots+a_ix_i+\cdots+a_nx_n=0$$

avec a_i non nul, on en prenant le produit extérieur avec $x_1\wedge\cdots\wedge\widehat{x_i}\wedge\cdots\wedge x_n$ la relation

$$a_ix_1\wedge\cdots\wedge x_n \text{ avec } a_i\neq 0.$$

La réciproque est plus délicate.

Montrons d'abord un lemme (c'est essentiellement le développement du déterminant par rapport à une ligne).

Lemme 2.7. — *Soit $n \geq 1$ un entier. Alors, l'application*

$$a : \left\{ \begin{array}{ccc} M^n & \to & M \otimes \bigwedge^{n-1} M \\ (x_1, \cdots, x_n) & \mapsto & \sum_{i=1}^n (-1)^i x_i \otimes x_1 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_n \end{array} \right.$$

est alternée.

Preuve : Supposons qu'on ait deux indices distincts $1 \leq k < l \leq n$ tels que $x_k = x_l$. On a alors certainement

$$a(x_1, \cdots, x_n) = (-1)^k x_k \otimes x_1 \wedge \cdots \wedge \widehat{x_k} \wedge \cdots \wedge x_l \wedge \cdots \wedge x_n + (-1)^l x_l \otimes x_1 \wedge \cdots \wedge x_k \wedge \cdots \wedge \widehat{x_l} \wedge \cdots \wedge x_n.$$

Mais on a d'une part

$$x_1 \wedge \cdots \wedge \widehat{x_k} \wedge \cdots \wedge x_l \wedge \cdots \wedge x_n = (-1)^{l-2} x_l \wedge x_1 \wedge \cdots \wedge \widehat{x_k} \wedge \cdots \wedge \widehat{x_l} \wedge \cdots \wedge x_n$$

(il y a $(l-2)$ termes avant x_l dans le produit), et, d'autre part, on a

$$x_1 \wedge \cdots \wedge x_k \wedge \cdots \wedge \widehat{x_l} \wedge \cdots \wedge x_n = (-1)^{k-1} x_k \wedge x_1 \wedge \cdots \wedge \widehat{x_k} \wedge \cdots \wedge \widehat{x_l} \wedge \cdots \wedge x_n$$

(il y a $(k-1)$ termes avant x_k dans le produit).

On a donc

$$a(x_1, \cdots, x_n) = x_k \otimes ((-1)^k (-1)^{l-2} x_l + (-1)^l (-1)^{k-1} x_k) \wedge x_1 \wedge \cdots \wedge \widehat{x_k} \wedge \cdots \wedge \widehat{x_l} \wedge \cdots \wedge x_n = 0.$$

■

On en déduit donc une unique application linéaire

$$\alpha : \bigwedge^n M \to M \otimes \bigwedge^{n-1} M \tag{2.7.a}$$

induisant a.

Preuve de la proposition : on fait une récurrence sur n. Le cas $n = 1$ est clair.

Supposons donc la propriété prouvée au rang $n - 1 \geq 1$ et $\lambda x_1 \wedge \cdots \wedge x_n = 0$. Deux cas.

Si $\lambda x_2 \wedge \cdots \wedge x_n$ est nul, par récurrence, $x_2, \cdots, x_n$ sont liés.

Si on a $w = \lambda x_2 \wedge \cdots \wedge x_n$ non nul. On sait que $\bigwedge^{n-1} M$ est libre. Dans une base de ce module, une des coordonnées w_i de w est donc non nulle. Notons f la forme linéaire $\bigwedge^{n-1} M \to A$ qui à un tenseur associe sa i-ième coordonnée de sorte que $f(w) \neq 0$. On a alors

$$(\mathrm{Id} \otimes f) \circ \alpha(x_1 \wedge \lambda x_2 \wedge \cdots \wedge x_n) = (\mathrm{Id} \otimes f) \circ \alpha(0) = 0$$

d'une part, et, d'autre part

$$\alpha(x_1 \wedge \lambda x_2 \wedge \cdots \wedge x_n) = \lambda \sum_{i=1}^n (-1)^i x_i \otimes x_1 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_n$$

de sorte que

$$0 = \lambda \sum_{i=1}^n (-1)^i x_i \otimes f(\lambda x_1 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_n).$$

En identifiant $M \otimes_A A$ et M, ceci donne une relation

$$f(\lambda x_2 \wedge \cdots \wedge x_n) x_1 + \sum_{i>1} \lambda_i x_i = 0$$

avec $f(\lambda x_2 \wedge \cdots \wedge x_n) \neq 0$: une relation de liaison.■

Corollaire 2.8. — *Soit $f \in \mathrm{Hom}(A^n, A^m)$ une application linéaire de modules libres (de type fini).*
i) f est injective si et seulement si $\bigwedge^n(f) : A \to \bigwedge^n(A^m)$ est injective ;
ii) en particulier, une matrice f de $M_n(A)$ est injective si et seulement si son déterminant est non diviseur de zéro ;
iii) si f est injective, $\bigwedge(f)$ est injective.

Preuve : Pour le premier point, f est injective si et seulement si elle envoie une base $x_1 \wedge \cdots \wedge x_n$ de A^n sur une famille libre. Comme $x_1, \cdots, x_n$ est une base de $\bigwedge^n A^n$, c'est le cas si et seulement si $\bigwedge^n(f)$ est injective d'après 2.6.
Le second est le cas particulier du premier avec $n = m$.
Pour le dernier point, on prend notre base $x_1, \cdots, x_n$ de A^n, induisant une base x_I de $\bigwedge^l A^n, l \leq n$. Si on a une relation $\sum a_I \bigwedge f(x_I) = 0$, montrons $a_I = 0$ pour tout I. Choisissons une famille (ordonnée) $J = \{1, \cdots, n\} \setminus I$. On a alors $a_I f(x_I \wedge x_J) = \pm a_I f(x_1) \wedge \cdots f(x_n) = 0$ et donc $a_I = 0$ car $f(x_i)$ famille libre puisque f injective (2.6).■

Notons que l'injectivité de $\bigwedge^n(f)$ signifie exactement que le seul scalaire annulant simultanément tous les mineurs maximaux de f est 0. On peut donner une preuve toute différente de ces énoncés d'injectivité en utilisant la notion d'*idéal associé* (cf. TD).

Exercice 2.9. — *Montrer que $f \in M_n(A)$ est surjective si et seulement si f est bijective ou encore si et seulement si* $\det(f)$ *inversible.*

Remarque 2.10. — *Le lecteur pourra généraliser cette procédure d'antisymétrisation comme suit. Supposons que $n = n_1 + \cdots + n_k$ est une somme de k entiers > 0. Il correspond un plongement de groupes*

$$H = S_{n_1} \times \cdots \times S_{n_k} \hookrightarrow G = S_n.$$

Pour $\sigma \in G$, on note encore encore σ l'isomorphisme de M^n obtenu par permutation des indices. En écrivant

$$M^n = M^{n_1} \times \cdots \times M^{n_k}$$

on définit un morphisme « de produit extérieur partiel »

$$w_H : \ M^n \to \bigwedge^{n_1} M \otimes \cdots \otimes \bigwedge^{n_k} M.$$

On a (vérifier !)

$$w_H \circ \sigma = \epsilon(\sigma) w_H \text{ pour tout } \sigma \in H$$

de sorte que

$$\epsilon(\sigma) w_H \circ \sigma = \epsilon(\tau) w_H \circ \tau \text{ si } \tau \in H\sigma.$$

On pose alors $a_H = \sum_{\sigma \in H \setminus G} \epsilon(\sigma) w_H \circ \sigma$. On vérifie comme plus haut que a_H est alternée et définit une antisymétrisation

$$\alpha_H : M^n \to \bigwedge^{n_1} M \otimes \cdots \otimes \bigwedge^{n_k} M.$$

Si $n_1 = 1, n_2 = n - 1$, on retrouve a. Si $n_1 = \cdots = n_n = 1$, on trouve le procédé d'antisymétrisation habituel (si

$$M \otimes \cdots \otimes M \to A$$

est l'application produit des coordonnées dans une base $\mathcal{B}$, on retrouve le déterminant $\det_{\mathcal{B}}$ *d'un système de vecteurs).*

3. Produit extérieur et somme directe

Supposons que M est une somme directe $M_1 \oplus M_2$ libre de rangs finis.

Lemme 3.1. — *L'application produit extérieur*

$$\bigwedge^{i} M_1 \otimes \bigwedge^{k-i} M_2 \to \bigwedge^{k} M$$

définit un isomorphisme

$$\bigoplus_{i=0}^{k} (\bigwedge^{i} M_1 \otimes \bigwedge^{k-i} M_2) \xrightarrow{\sim} \bigwedge^{k} M \tag{3.1.a}$$

qui nous permet d'identifier ces espaces.

Preuve : Il suffit de tester sur une base de M, réunion d'une base de M_1 et d'une base de M_2. ■

Plus généralement, donnons nous une suite exacte courte de modules

$$0 \to M_1 \to M \to M_2 \to 0.$$

On identifie M_1 à son image dans M. Soit n un entier naturel. Pour $0 \leq i \leq n$, on a un morphisme

$$p_i : \bigwedge^{i} M_1 \otimes \bigwedge^{n-i} M \to \bigwedge^{n}(M)$$

défini par le produit extérieur.

Lemme 3.2. — *Si les M_i sont libres, tous les p_i sont injectifs. La suite des images des p_i est croissante et le morphisme $\bigwedge^{n-i} M \to \bigwedge^{n-i} M_2$ induit un isomorphisme*

$$\mathrm{Im}(p_i)/\mathrm{Im}(p_{i+1}) \xrightarrow{\sim} \bigwedge^{i} M_1 \otimes \bigwedge^{n-i} M_2.$$

Preuve : Il suffit de le vérifier sur les bases canoniques adaptées à la suite exacte (exercice).■

Exercice 3.3. — *Supposons M libre de rang n. Montrer qu'on a une application bilinéaire non dégénérée définie par le produit extérieur*

$$\bigwedge^{k} M \otimes \bigwedge^{n-k} M \to \bigwedge^{n} M.$$

En déduire que le choix d'une orientation $\bigwedge^{n} M \xrightarrow{\sim} A$ identifie $\bigwedge^{n-k} M$ et le dual de $\bigwedge^{k} M$ et, que sans choix d'une telle orientation, on un isomorphisme canonique

$$\bigwedge^{n-k} M \xrightarrow{\sim} \bigwedge^{k} M^* \otimes_A \bigwedge^{n} M.$$

4. Produit intérieur par une forme linéaire

Soit M un A-module projectif de rang n. L'application déterminant δ

$$\delta : \begin{cases} M^k \times (M^*)^k & \to & A \\ ((\underline{e}), (\underline{\phi})) & \mapsto & \det(\phi_i(e_j)) \end{cases}$$

est alternée en chacune des variables et se factorise donc en une application bilinéaire

$$\bigwedge^k M \times \bigwedge^k M^* \to A$$

qui est *non dégénérée* comme on le vérifie sur des bases locales. Ainsi on a un isomorphisme canonique

$$\bigwedge^k M \xrightarrow{\sim} \bigwedge^k M^* \tag{4.a}$$

Si $e \in \bigwedge^k M$ et $\phi \in M^*$, on définit alors le produit intérieur droit $e \lrcorner \phi \in \bigwedge^{k-1} M$ par la condition

$$< e \lrcorner \phi, \psi >= \delta(e, \phi \wedge \psi) \text{ pour tout } \psi \in \bigwedge^{k-1} M^*.$$

En testant sur des bases, on obtient que le produit est une anti-dérivation, *ie*

$$(e_a \wedge \epsilon_b) \lrcorner \phi = (e_a \lrcorner \phi) \wedge \epsilon_b + (-1)^a (e_a) \wedge (\epsilon_b \lrcorner \phi) \tag{4.b}$$

pour tout $e_a \in \bigwedge^a M$ et $\epsilon_b \in \bigwedge^b M$.
On déduit la formule

$$e_1 \wedge \cdots \wedge e_k \lrcorner \phi = \sum_{i=1}^{k} (-1)^{(i-1)} \phi(e_i) e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_k \tag{4.c}$$

où le symbole $\widehat{e_i}$ signifie qu'on a omis e_i.
Dans le cas où $M = M_1 \oplus M_2$ et où ϕ s'écrit $\phi_1 + \phi_2$ avec $\phi_i \in M_i^*$ (qu'on comprend comme ϕ_i est nulle sur M_{3-i}), les formules 4.b et 4.c donnent immédiatement

$$(\omega_1 \wedge \omega_2) \lrcorner \phi = (\omega_1 \lrcorner \phi_1) \wedge \omega_2 + (-1)^i \omega_1 \wedge (\omega_2 \lrcorner \phi_2) \text{ pour tout } \omega_1 \in \bigwedge^i M_1 \text{ et } \omega_2 \in \bigwedge^{k-i} M_2. \tag{4.d}$$

Bien entendu, on a $(e \lrcorner \phi) \lrcorner \phi = 0$ de sorte qu'on a un complexe dit de Koszul

$$K(\phi) = (K^j(\phi) = \bigwedge^{-j} M)_{j \leq 0}$$

$$0 \to \bigwedge^n M \xrightarrow{\lrcorner \phi} \cdots \bigwedge^k M \xrightarrow{\lrcorner \phi} \cdots \bigwedge^1 M = M \xrightarrow{\phi} A \to 0,$$

où $d : K^j \to K^{j+1}$ est le produit intérieur par ϕ.

5. Parenthèse sur les modules projectifs

On dit qu'un module P est projectif si le foncteur $M \mapsto \mathrm{Hom}(P, M)$ est exact. Ceci est aussi équivalent au fait que P est facteur direct d'un module libre. Par exemple, un module libre est projectif. Mais il y a des modules projectifs non libres (voir TD). On peut montrer (cf. TD) que si tous les localisés $M_{\mathfrak{p}}, \mathfrak{p} \in \mathrm{spec}(A)$ d'un module M sont libres de rang constant, alors M est projectif, la réciproque étant presque exacte (il faut remplacer rang constant par localement constant en un sens adéquat pour la réciproque, cf. TD). Le lecteur vérifiera sans peine que les isomorphismes 4.a et le lemme 3.1 sont valables sous l'hypothèse plus faible projectif de type fini au lieu de libre de type fini.

6. Complexe de Koszul

Soit $\phi : E \to A$ une forme linéaire sur un module projectif (libre par exemple) de type fini E de rang n. Le produit intérieur définit un complexe, dit complexe de Koszul,

$$K^{-j-1}(E,\phi) = \bigwedge^{j+1} E \xrightarrow{\lrcorner\phi} K^{-j}(E,\phi) = \bigwedge^{j} E \xrightarrow{\lrcorner\phi} K^{-j+1}(E,\phi) = \bigwedge^{j-1} E \tag{6.a}$$

nul en degré $i \notin [-n, 0]$. On notera d_{-j} la différentielle en degré $-j$, par définition le morphisme

$$K^{-j}(E,\phi) \xrightarrow{\lrcorner\phi} K^{-j+1}(E,\phi)$$

ou, si aucune confusion n'est à craindre, simplement d.

6.1. Un exemple important. — Par exemple, si $P_1, \cdots, P_n$ sont des polynômes de $A = B[X_0, \cdots, X_m]$, on peut regarder le module libre $E = A^n$ et ϕ de matrice $(P_1, \cdots, P_n)$. On sait alors que $\bigwedge^k E$ est libre avec une base canonique e_I indexée par les parties à k éléments de $[1, \cdots, n]$. Si on ordonne les éléments de I sous la forme $i_1 < \cdots < i_k$, on a alors

$$\mathrm{d}(e_I) = \sum_{j=1}^{k} (-1)^{(j-1)} P_{i_j} e_{I \setminus i_j}. \tag{6.1.a}$$

Le paragraphe suivant va nous permettre de développer des méthodes pour étudier l'exactitude de ce complexe.

PARTIE VII

COHOMOLOGIE DES COMPLEXES

Pour nous, le mot complexe désignera une suite de modules $M^i, i \in \mathbf{Z}$ et de morphismes $\mathrm{d}_i : M^i \to M^{i+1}$ tels que $d_{i+1} \circ d_i = 0$. Les complexe sont les objets d'une catégorie dont les morphismes sont les diagrammes commutatifs

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & M^{i-1} & \longrightarrow & M^i & \longrightarrow & M^{i+1} & \longrightarrow & \cdots . \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & N^{i-1} & \longrightarrow & M^i & \longrightarrow & M^{i+1} & \longrightarrow & \cdots \end{array}$$

***Exemple 0.2* (Produit tensoriel total).** — *Si M, N sont deux complexes, on définit le produit tensoriel total $M \otimes_A N$ comme suit :*

-

$$(M \otimes_A N)^n = \oplus_{i+j=n} M^i \otimes_A N^j;$$

-sur $M^i \otimes_A N^j$, on pose

$$\mathrm{d} = \mathrm{d}_M \otimes 1 + (-1)^i 1 \otimes \mathrm{d}_N.$$

carré nul et on a bien un complexe.

1. Parenthèse sur les modules gradués

On dit qu'un module M est $\mathbf{Z}$-gradué (ou simplement pour nous gradué) si M est somme directe de sous-modules $M^n, n \in \mathbf{Z}$. Si a est un entier, on note $M[a]$ le module gradué qui, en tant que module sans graduation est M, et, tel que $M[a]^n = M^{n+a}$. Cette opération est appelée **décalage**.

Un morphisme f de modules gradués $M \to N$ est dit gradué de degré a si $f(M^n) \subset N^{n+a}$ pour tout n. Si $a = 0$, on dit que f est un morphisme gradué. Un sous-module M' de M est dit gradué s'il est somme directe des $M^n \cap M'$. Il revient au même de dire que si on décompose un élément de M' en composantes de degré n, toutes les composantes sont dans M'. Par exemple, le noyau, l'image d'un morphisme gradué sont des sous-modules gradués. Il existe alors une unique graduation sur M/M' telle que le morphisme quotient soit gradué. Toutes les preuves de ces assertions sont laissées au lecteur.

Avec ces définitions, une autre manière de voir un complexe (M^i, d^i) est de considérer l'endomorphisme d du module $\mathbf{Z}$-gradué $M = \oplus_{i \in \mathbf{Z}} M^i$ qui vaut d^i sur M^i. Il est de degré $+1$. La condition $d^{i+1} \circ d^i = 0$ pour tout i se résume en $\mathrm{d} \circ \mathrm{d} = 0$. Un morphisme de complexe est alors simplement un morphisme gradué commutant à d. Inversement, se donner un tel d de degré $+1$ de carré nul définit un tel complexe. On utilisera librement les deux langages. Ceci permet de parler de suites exactes de complexes, ou de toute autre notion de module, simplement par oubli de la graduation. Notons que le module associé au produit tensoriel total de deux complexe M et N est canoniquement isomorphe au produit tensoriel des modules associés à M et N. Toutefois, il faudrait un peu modifier, et ce serait raisonnable, la définition du produit tensoriel de morphismes gradués pour tenir compte des signes plus haut. On ne le fera pas ici.

2. Cohomologie des complexes

La condition $\mathrm{d} \circ \mathrm{d} = 0$ se réécrit $\mathrm{Im}(\mathrm{d}) \subset \mathrm{Ker}(\mathrm{d})$ nul, tandis que la condition « être exact en degré i »se traduit par

$$H^i(\mathrm{d}) = \mathrm{Ker}(\mathrm{d}^i)/\mathrm{Im}(\mathrm{d}^{i-1})$$

nul (noter que $H^i(\mathrm{d})$ est la partie de degré i de $H(\mathrm{d}) = \mathrm{Ker}(\mathrm{d})/\mathrm{Im}(\mathrm{d})$). Si le module $H^i(\mathrm{d})$ est nul, on dit que le complexe est acyclique en degré i. Dire qu'il est acyclique en tout degré (ou simplement acyclique) c'est dire que la suite

$$\cdots \to M^{i-1} \to M^i \to M^{i+1} \to \cdots$$

est exacte. Le module gradué $H(\mathrm{d}) = \oplus H^i(\mathrm{d})$ s'appelle le module de **cohomologie** du complexe. On le note aussi $H(M)$ si aucune confusion n'est à craindre.
Par exemple, on a $H^j(M[a]) = H^{j+a}(M)$ pour tout j, ou, si on préfère, $H(M[a]) = H(M)[a]$.
Le noyau de d est noté $Z(\mathrm{d})$ (module des cocycles) tandis que l'image est noté $B(\mathrm{d})$ (module des cobords) de sorte que

$$H(\mathrm{d}) = Z(\mathrm{d})/B(\mathrm{d}).$$

.
Si $f \in \mathrm{Hom}(M, N)$ est un morphisme gradué (ou de complexes, comme on veut), f induit un morphisme gradué

$$H(f) : H(M) \to H(N)$$

qui à la classe du cocycle $m \in Z(M) \subset M$ associe la classe de l'élément $f(m)$ qui se trouve être un cocycle, bien défini à un cobord près.
On vérifie que H est un foncteur additif de la catégorie des complexes dans celle des modules gradués et on dira que $H(f)$ est la flèche de fonctorialité (associée à f) en cohomologie.

3. Suite exacte de cohomologie

On se donne une suite exacte de modules gradués (ou de complexes, comme on veut)

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

On déduit deux complexes de modules gradués

$$M_1/B(M_1) \to M_2/B(M_2) \to M_3/B(M_3) \to 0 \tag{3.a}$$

et

$$0 \to Z(M_1) \to Z(M_2) \to Z(M_3) \tag{3.b}$$

Lemme 3.1. — *Les deux suites 3.a et 3.b sont exactes.*

Preuve : Vérifions pour la première par exemple. La surjectivité découle de la surjectivité de $M_2 \to M_3$. Soit alors $m_2 \in M_2$ dont l'image dans M_3 soit un cobord $\mathrm{d}(m_3)$. Choisissons un antécédent m_2' de m_3. Alors, l'image de $m_2 - \mathrm{d}(m_2')$ dans M_3 est nulle, et donc provient de $m_1 \in M_1$. La classe m_1 s'envoie sur la classe de m_2 par construction. La seconde est analogue.■

La différentielle d est degré $+1$ et tue les cobords $B(M_j)$. Elle induit donc pour tout i un morphisme

$$\delta_j^i : \ M_j^i/B^i(M_j) \xrightarrow{\mathrm{d}^i} Z^{i+1}(M_j)$$

pour $j = 1, 2, 3$.
Le lemme suivant est clair.

Lemme 3.2. — *Avec les notations précédentes, on*

– *La flèche canonique*

$$Z^i(M_j) \hookrightarrow M_j^i \twoheadrightarrow M_j^i/B^i(M_j)$$

induit un isomorphisme

$$\mathrm{Ker}(\delta_j^i) \xrightarrow{\sim} H^i(M_j).$$

– *La flèche canonique*

$$Z^{i+1}(M_j) \twoheadrightarrow H^{i+1}(M_j)$$

induit un isomorphisme

$$\mathrm{Coker}(\delta_j^i) \xrightarrow{\sim} H^{i+1}(M_j).$$

De plus, les flèches naturelles entre les noyaux des δ_j^i d'une part et conoyaux d'autre part s'identifient aux flèche de fonctorialité en cohomologie.

Maintenant, on a un diagramme commutatif,

$$\begin{array}{ccccccc} & & M_1^i/B^i(M_1) & \longrightarrow & M_2^i/B^i(M_2) & \longrightarrow & M_3^i/B^i(M_3) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \delta_1^i} & & \downarrow{\scriptstyle \delta_2^i} & & \downarrow{\scriptstyle \delta_3^i} \\ 0 & \longrightarrow & Z^{i+1}(M_1) & \longrightarrow & Z^{i+1}(M_2) & \longrightarrow & Z^{i+1}(M_3) \end{array}$$

diagramme dont les lignes sont exactes.
Compte tenu du lemme précédent, le lemme du serpent I.18.2 assure l'existence d'un morphisme canonique ∂^i de **liaison** tel que la suite, dite **suite exacte de cohomologie**,

$$\begin{array}{ccccccc} \cdots\cdots & & H^i(M_1) & \longrightarrow & H^i(M_2) & \longrightarrow & H^i(M_3) \\ & & & & & \swarrow{\scriptstyle \partial^i} & \\ H^{i+1}(M_1) & \longrightarrow & H^{i+1}(M_2) & \longrightarrow & H^{i+1}(M_3) & & \cdots\cdots \end{array}$$

soit exacte.
Explicitement, l'image d'une classe $\bar{m}_3$ de $H(M_3)$ s'obtient comme suit. On relève m_3 en $m_2 \in M_2$. L'image de sa différentielle dans M_3 est nulle, donc $\mathrm{d}(m_2) = m_1 \in M_1 \subset M_2$. Mais m_1 est évidemment un cocycle : sa classe dans la cohomologie est le cobord cherché.

Exercice 3.3. — *Soient M_1, M_3 gradués et $M_2 = M_1 \oplus M_3$ (muni de la graduation évidente). On suppose qu'on s'est donné $\mathrm{d}_2 = \begin{pmatrix} \mathrm{d}_1 & \delta \\ 0 & \mathrm{d}_3 \end{pmatrix}$ un endomorphisme gradué de M_2 de carré nul et de degré 1 qui laisse stable M_1. Il induit donc un endomorphisme de carré nul d_3 de M_3. On note δ le composé*

$$\delta : \ M_3 \hookrightarrow M_2 \xrightarrow{\mathrm{d}} M_2[1] \twoheadrightarrow M_1[1].$$

C'est un morphisme de degré 1. Montrer que l'homomorphisme de liaison associé à la suite exacte canonique de complexes correspondantes

$$0 \to (M_1, \mathrm{d}_1) \to (M_2, \mathrm{d}_2) \to (M_3, \mathrm{d}_3) \to 0$$

est $H(\delta)$.

Le lecteur se convaincra facilement que la suite exacte de cohomologie est fonctorielle en M au sens suivant. Si on a un diagramme commutatif de morphismes gradués à lignes exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0\ , \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

le on a alors le diagramme commutatif

$$\begin{array}{ccccccccccccc} \cdots\cdots & H^i(M_1) & \longrightarrow & H^i(M_2) & \longrightarrow & H^i(M_3) & \xrightarrow{\partial^i} & H^{i+1}(M_1) & \longrightarrow & H^{i+1}(M_2) & \longrightarrow & H^{i+1}(M_3) & \cdots\cdots \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ \cdots\cdots & H^i(N_1) & \longrightarrow & H^i(N_2) & \longrightarrow & H^i(N_3) & \xrightarrow{\partial^i} & H^{i+1}(N_1) & \longrightarrow & H^{i+1}(N_2) & \longrightarrow & H^{i+1}(N_3) & \cdots\cdots \end{array}$$

où les flèches verticales sont les flèches de fonctorialité et les lignes les suites exactes de cohomologie.

4. Application au complexe de Koszul

Rappelons qu'à la section VI.6, on a associé à toute forme linéaire ϕ sur un module projectif E de rang n un complexe $K(E,\phi)$ concentré en degré $d \in [-n, 0]$. Par définition, on $H^0(K(E,\phi)) = \mathrm{Coker}(\phi) = A/\mathrm{Im}(\phi)$. Ce qui nous intéresse serait d'avoir une condition assurant que ce complexe est acyclique en degré négatif. Supposons que E se décompose en une somme directe $E = E' \oplus L$ où L est libre de rang 1, de base e_n. Le produit extérieur $\bigwedge^j E$ se décompose (lemme VI.3.1) alors canoniquement en

$$\bigwedge^j E = \bigwedge^j E' \oplus (\bigwedge^{j-1} E' \otimes Ae_n) \xrightarrow{\sim} \bigwedge^j E' \oplus \bigwedge^{j-1} E'.$$

Notons ϕ' la restriction de ϕ à E'. On a alors la formule (VI.4.d)

$$(\omega' \wedge e_n) \lrcorner \phi = (\omega' \lrcorner \phi') \wedge e_n + (-1)^{j-1}\phi(e_n)\omega' \text{ pour tout } \omega' \in \bigwedge^{j-1} E'. \tag{4.a}$$

On déduit immédiatement que le diagramme de modules gradués

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K(E',\phi') & \longrightarrow & K(E,\phi) & \longrightarrow & K(E',\phi')[1] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{d}'} & & \downarrow{\scriptstyle \mathrm{d}} & & \downarrow{\scriptstyle \mathrm{d}'} & & \\ 0 & \longrightarrow & K(E',\phi') & \longrightarrow & K(E,\phi) & \longrightarrow & K(E',\phi')[1] & \longrightarrow & 0 \end{array}$$

induit par la décomposition précédente et les différentielles de Koszul d, d' associées à ϕ, ϕ' commutent. La suite exacte de cohomologie (et l'exercice 3.3) assure que la suite

$$\cdots H^j(K(E',\phi')) \to H^j(K(E,\phi)) \to H^{j+1}(K(E',\phi')) \xrightarrow{\pm\phi(e_n)} H^{j+1}(K(E',\phi')) \cdots \tag{4.b}$$

est exacte.

4.1. Une suite exacte fondamentale. — Reprenons l'exemple VI.6.1, en le particularisant. On s donne donc l'anneau $A = B[X_0, \cdots, X_m]$, un entier naturel $n \leq m$, le module $E = A^{n+1}$ et la forme $\phi = (X_0, \cdots, X_n)$. Les modules $K^{-j} = \bigwedge^j E, j \leq 0$ sont libres. On a déjà observé que

$$H^0(K(E,\phi) = \mathrm{Coker}(\phi) = B[X_0, \cdots, X_n]/(X_0, \cdots, X_m) \xrightarrow{\sim} B[X_{n+1}, \cdots, X_m].$$

Proposition 4.2. — *Avec les notations précédentes, le complexe de Koszul $K(E,\phi)$ est acyclique en degré < 0.*

Preuve : Montrons par récurrence sur n la nullité de $H^j(E,\phi)$ dans ce cas. Si $n=0$, on le complexe concentré en degré 0 et -1

$$B[X_0,\cdots,X_m] \overset{X_0}{\to} B[X_0,\cdots,X_m]$$

qui visiblement est acyclique en degré <0.

Si c'est vrai au rang $n-1, n>0$, on écrit $E=E'\oplus Ae_n$ avec $E'=A^n$ (les n premières composantes d'un n-uple) et $e_n=(0,\cdots,0,1)$. Comme $\phi'=(X_0,\cdots,X_{n-1})$, on a $H^j(E',\phi')=0$ pour $j<0$. La suite exacte 4.b donne alors une suite exacte

$$H^j(K(E',\phi')) \to H^j(K(E,\phi)) \to H^{j+1}(K(E',\phi')).$$

-Si $j<-1$, les deux extrêmes sont nuls donc $H^j(K(E,\phi))=0$.

-Si $j=-1$, compte tenu de

$$H^{j+1}(K(E',\phi')) = A/(X_0,\cdots,X_{n-1}) \overset{\sim}{\to} B[X_n,\cdots,X_m],$$

on a une suite exacte

$$0 \to H^{-1}(K(E,\phi)) \to B[X_n,\cdots,X_m] \overset{\pm X_n}{\to} B[X_n,\cdots,X_m].$$

La multiplication par X_n dans $B[X_n,\cdots,X_m]$ a donc pour noyau $H^{-1}(K(E,\phi))$. Cette multiplication étant injective, ce noyau est nul, ce qu'on voulait.■

Définition 4.3. — *On dit qu'un module M admet une résolution de longueur n s'il existe $n+1$ modules $L^{-j}, j=0,\cdots,n$ et une suite exacte*

$$0 \to M^{-n} \to \cdots \to M^0 \to M \to 0.$$

Si $\mathcal{P}$ est une propriété de modules (comme de rang fini, libre, projectif...) on dira que la résolution est $\mathcal{P}$.

On retiendra de cet énoncé le résultat suivant

Corollaire 4.4. — *que le $B[X_0,\cdots,X_m]$-module*

$$B[X_0,\cdots,X_m]/(X_0,\cdots,X_m) \overset{\sim}{\to} B$$

admet une résolution libre de rang fini de longueur $m+1$.

PARTIE VIII

FONCTEUR Tor

On a déjà observé que le foncteur produit tensoriels $.\otimes_A N$ était exact à droite mais pas à gauche en général. On va mesurer le défaut d'exactitude.

1. Résolutions libres

On va construire une résolution libre canonique $L(M)$ de tout module M. Pour tout module M, on note $e_m, m \in M$ la base canonique du module libre $A^{(M)}$. On note $l_M : A^{(M)} \to M$ le morphisme qui envoie e_m sur m pour tout $m \in M$. C'est une surjection. On pose alors

$$L^0(M) = A^{(M)}, \text{ et } \mathrm{d}_0 = l_M.$$

On définit $L(M)$ inductivement grâce aux formules

$$L^{-n-1}(M) = L^0(\mathrm{Ker}(\mathrm{d}_{-n})) \text{ et } \mathrm{d}_{-n-1} = j_n \circ l_{(\mathrm{Ker}(\mathrm{d}_{-n}))} \text{ pour } n \geq 0.$$

où j_n est l'inclusion $\mathrm{Ker}(\mathrm{d}_n) \hookrightarrow L_n(M)$. Par construction, $L^j, d_j, j \leq 0$ est une résolution de M, dite résolution canonique libre de M. Elle est fonctorielle en M par construction.

2. Les modules $\mathrm{Tor}_j(M, N)$

Si bien entendu le complexe $(L(M), \mathrm{d})$ est acyclique, le complexe $L(M) \otimes_A N, \mathrm{d} \otimes 1$ ne l'est pas en général, car le produit tensoriel n'est pas exact.

Définition 2.1. — *Soit j un entier naturel. On définit le module $\mathrm{Tor}_j^A(M, N)$ par la formule*

$$\mathrm{Tor}_j^A(M, N) = H^{-j}(L(M) \otimes_A N).$$

On peut calculer $\mathrm{Tor}_0^A(M, N)$.

Lemme 2.2. — *Le module $\mathrm{Tor}_0^A(M, N)$ est canoniquement isomorphe à $M \otimes_A N$.*

Preuve : On a une suite exacte canonique

$$L^{-1}(M) \to L^0(M) \to M \to 0$$

qui donne une suite exacte

$$L^{-1}(M) \otimes N \overset{d^{-1}}{\to} L^0(M) \otimes N \to M \otimes N \to 0,$$

et donc

$$\mathrm{Coker}(\mathrm{d}^{-1}) \overset{\sim}{\to} M \otimes_A N.$$

Mais, par définition, $H^0(L(M) \otimes_A N) = \mathrm{Coker}(\mathrm{d}^{-1})$, d'où le lemme.■

Comme $L(M) \otimes A^{(I)}$ s'identifie canoniquement à $L(M)^{(I)}$ qui est visiblement acyclique en degré < 0 comme $L(M)$, on a $\mathrm{Tor}_j^A(M, N) = 0$ si $j > 0$ et N libre.

Exercice 2.3. — *Montrer que si M, N sont de type fini et A noethérien, les $\mathrm{Tor}_j^A(M, N)$ sont de type fini.*

3. Fonctorialité

Si $f \in \mathrm{Hom}(M, M'), g \in \mathrm{Hom}(N, N')$, on a un morphisme de complexes

$$L(f) : L(M) \to L(M')$$

induisant un morphisme de complexes

$$L(f) \otimes g : L(M) \otimes N \to L(M') \otimes N'.$$

On pose alors

$$\mathrm{Tor}_j(f, g) = H^{-j}(L(f) \otimes g) : \mathrm{Tor}_j(M, N) \to \mathrm{Tor}_j(M', N').$$

On vérifie sans peine que $\mathrm{Tor}_0(f, g)$ s'identifie à $f \otimes g$. Ceci permet de définir deux foncteurs (en M et N), compatibles en un sens évident : c'est ce qu'on appelle un bi-foncteur. L'identification $\mathrm{Tor}_0(M, N) \xrightarrow{\sim} M \otimes_A N$ est bifonctorielle (exercice).

3.1. Changement de résolution. — En fait, on peut utiliser n'importe quelle résolution projective pour calculer les Tor. Donnons une définition.

Définition 3.2. — *Deux morphismes de complexes*

$$f, g : \ P \to L$$

sont dit homotopes s'il existe $h : \ P \to L[-1]$ *tel que* $f - g = h \circ \mathrm{d}_P + \mathrm{d}_L \circ h$.

Autrement dit, on doit avoir une collection $h_n : P^n \to L^{n-1}$ tels que

$$f^n - g^n = h^{n+1} \circ \mathrm{d}_P^n + \mathrm{d}_L^{n-1} \circ h^n \text{ pour tout } n.$$

L'importance de cette notion vient de ce qu'on a $H(f) = H(g)$ dans ce cas. En effet, si p est un cocycle de P définissant une classe dans $H(L)$, on a $f(p) - g(p) = \mathrm{d}_L(h(p))$ (car $\mathrm{d}_P(p) = 0$) et donc $f(p)$ et $g(p)$ ont la même classe dans $H(P)$.
On dira que $f : P \to L$ est un **homotopisme** s'il existe $g : L \to P$ tel que $f \circ g$ homotope à Id_L et gf homotope à Id_P. Si on suppose seulement $H(f)$ isomorphisme, on dit que f est un quasi-isomorphisme (ou homologisme). En particulier, un homotopisme est un quasi-isomorphisme car si g est un inverse (à homotopie près), on a

$$H(f) \circ H(g) = H(\mathrm{Id}) = \mathrm{Id}_H$$

et de même pour $H(g) \circ H(f)$.

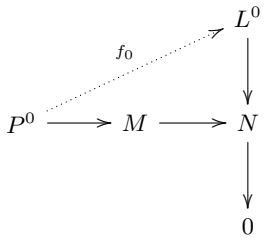
Proposition 3.3. — *Soit $M \to N$ un morphisme de modules et P, L des résolutions de M, N. On suppose que P est une résolution projective. Alors, il existe un morphisme de complexes $f : P \to L$, unique à homotopie près, tel que le diagramme*

$$\begin{array}{ccc} P & \xrightarrow{f} & L \\ \downarrow & & \downarrow \\ M & \longrightarrow & N \end{array}$$

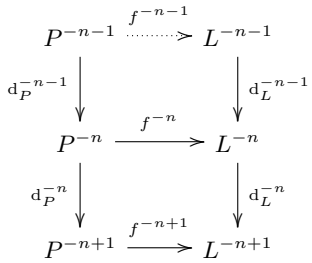
commute.

Preuve : On construit $f_i, i \leq 0$ de proche en proche.

Par définition, f_0 doit faire commuter le diagramme



Elle existe car P_0 est projectif.Si on a une autre flèche g_0, la différence $f_0 - g_0$ est à valeurs dans l'image de d_L^{-1} puisqu'elle est nulle dans N, et donc, P^0 étant projectif s'écrit $\mathrm{d}_L^{-1} \circ h^0$ où $h^0 \in \mathrm{Hom}(P_0, L^{-1})$. Supposons qu'on a construit f^{-i} en rang $\leq n$, et que l'assertion d'unicité est vraie en rang $\leq n$. Construisons f^{-n-1} : on cherche à compléter le diagramme commutatif



Le composé de $P^{-n-1} \to P^{-n} \to L^{-n}$ par d_L^{-n} est la flèche

$$P^{-n-1} \to P^{-n} \to P^{-n+1} \to L^{-n+1}$$

et donc est nul comme

$$P^{-n-1} \to P^{-n} \to P^{-n+1}.$$

Il est donc à valeurs dans $\mathrm{Ker}(\mathrm{d}_L^{-n}) = \mathrm{Im}(\mathrm{d}_L^{-n-1})$. Comme P^{-n-1} est projectif, il existe $f^{-n-1} : P^{-n-1} \to L^{-n-1}$ faisant commuter le diagramme. Si un autre système de $g^{-i}, i \leq n+1$ convient, on a par récurrence construit h^{-i} pour $i \leq n$ et on a

$$\mathrm{d}_L^{-n-1} \circ (f^{-n-1} - g^{-n-1}) = f^{-n} \circ d_P^{-n-1} - g^{-n} \circ d_P^{-n-1} = (h^{-n+1} \circ \mathrm{d}_P^{-n} + \mathrm{d}_L^{-n-1} \circ h^{-n}) \circ d_P^{-n-1} = \mathrm{d}_L^{-n-1} \circ h^{-n} \circ d_P^{-n-1}$$

de sorte que

$$\mathrm{d}_L^{-n-1} \circ (f^{-n-1} - g^{-n-1} - h^{-n} \circ d_P^{-n-1}) = 0.$$

Ainsi,

$$(f^{-n-1} - g^{-n-1} - h^{-n} \circ d_P^{-n-1})$$

est à valeurs dans $\mathrm{Im}(\mathrm{d}_L^{-n-2})$ et s'écrit, $\mathrm{d}_L^{-n-2} \circ h^{-n-1}$ où $h^{-n-1} \in \mathrm{Hom}(P^{-n-1}, L^{-n-2})$. Ceci achève la preuve.■

Corollaire 3.4. — *Soient L et P deux résolutions projectives. Alors, il existe un homotopisme de L dans P, unique à homotopie près.*

Preuve : En effet, on a des morphismes $f : P \to L$ et $g : L \to P$. Par unicité, $f \circ g$ et Id_L sont homotopes, ainsi que $g \circ f$ et Id_P.■

On aurait visiblement eu intérêt à considérer la catégorie des complexes à homotopie près, dont les objets sont les complexes disons nuls en degré assez grands et les morphismes sont les morphismes de complexes modulo les homotopismes. Dans cette

catégorie, deux complexes homotopes sont canoniquement isomorphes. C'est le premier pas (la moitié du chemin) à franchir pour atteindre la notion de catégorie dérivée.

Corollaire 3.5. — *Si $P(M)$ est une résolution projective de M, la cohomologie de $P(M)\otimes N$ est canoniquement isomorphe à* $\mathrm{Tor}^A(M,N)$.

Preuve : En effet, on a une homotopisme f de $L(M)$ dans $P(M)$ qui induit un homotopisme $f\otimes 1$ de $L(M)\otimes N$ dans $P(M)\otimes N$ et donc un isomorphisme en cohomologie.■

Exercice 3.6. — *Montrer que si $f,h\in \mathrm{Hom}(M,M')$ et $g\in \mathrm{Hom}(N,N')$, alors $L(f)+L(h)$ et $L(f+h)$ sont homotopes. En déduire la formule* $\mathrm{Tor}_j(f+h,g)=\mathrm{Tor}_j^A(f,g)+\mathrm{Tor}_j^A(h,g)$. *Avec des notations évidentes, que vaut* $\mathrm{Tor}_j^A(f,g+k)$ *?*

Exercice 3.7. — *Montrer que* $\mathrm{Tor}_j(M,N)$ *est canoniquement, et fonctoriellement, isomorphe à* $\mathrm{Tor}_j(N,M)$ *[Indication : montrer que $L(M)\otimes N$ est isomorphe au produit tensoriel total (cf. l'exemple VII.0.2) $L(M)\otimes_A L(N)$.]*

4. Une annulation fondamentale

Rappelons que le complexe de Koszul fournit une résolution libre du $B=A[X_1,\cdots,X_n]$ module $A=B/(X_1,\cdots,X_n)$, nulle en degré $\leq -n-1$. Le corollaire 3.5 assure que la cohomologie de ce complexe tensorisé avec N calcule $\mathrm{Tor}^B(A,N)$. Comme les différentielles sont nulles en degré $\leq -n-1$, on a

$$\mathrm{Tor}_j^B(A,N)=0 \text{ pour } j\geq n+1 \tag{4.a}$$

Exercice 4.1. — *Montrer que pour tout j, le module* $\mathrm{Tor}_j^B(A,A)$ *est libre et calculer son rang. En déduire qu'il n'existe pas de résolution projective*

$$0\to P^{-m}\to\cdots P^0\to A\to 0$$

de A avec $m<n$.

5. La suite exacte des Tor

Supposons qu'on a une suite exacte

$$0\to N_1\xrightarrow{a} N_2\xrightarrow{b} N_3\to 0.$$

Remarquons que tensoriser par un module libre est un foncteur exact. Rappelons d'abord que le produit tensoriel commute à la somme directe (lemme V.5.1). Compte tenu de l'identification $A\otimes_A M\xrightarrow{\sim} M$ pour tout M, le produit tensoriel de l'injection $j:\ N\to N'$ par le module libre $A^{(I)}$ s'identifie à

$$\mathrm{diag}(j):\ N^{(I)}\to N'^{(I)}$$

où $\mathrm{diag}(j)(n_i)=j(n_i)$ est visiblement injective comme j.
Comme $L(M)$ est un complexe de modules libres, on a une suite exacte de complexes

$$0\to L(M)\otimes_A N_1\to L(M)\otimes_A N_2\to L(M)\otimes_A N_3\to 0.$$

La suite exacte de cohomologie (VII.3) associée s'écrit

$$\cdots\to \mathrm{Tor}_{j+1}^A(M,N_3)\to \mathrm{Tor}_j^A(M,N_1)\to \mathrm{Tor}_j^A M,N_2)\to \mathrm{Tor}_j^A(M,N_3)\to \mathrm{Tor}_{j-1}^A(M,N)\to\cdots \tag{5.a}$$

qui est certainement fonctorielle, en un sens évident, en M et N_i. En fait, cette preuve est miraculeuse, au sens qu'elle ne se généralise pas quand on remplace le foncteur exact à droite $F(N) = M \otimes_A N$ par un foncteur F exact à droite quelconque. On a alors besoin du résultat suivant, pas très difficile et laissé en exercice.

Exercice 5.1. — *Supposons qu'on a une suite exacte*

$$0 \to N_1 \to N_2 \to N_3 \to 0.$$

Alors, il existe des résolutions projectives $P(N_i)$ de $N_i, i = 1, 2, 3$ et un diagramme commutatif à lignes exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P(N_1) & \longrightarrow & P(N_2) & \longrightarrow & P(N_3) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array} .$$

Retrouver la suite exacte des Tor.

PARTIE IX

LE THÉORÈME DES SYZYGIES DE HILBERT

On est en mesure de prouver très simplement le théorème des syzygies de Hilbert. On se donne un corps k, un anneau de polynômes $B = k[X_1, \cdots, X_n]$ et M un B-module de type fini.
Mais B a une structure supplémentaire : c'est une **k-algèbre graduée**. Précisons ce que cela signifie. Si B^d est l'espace vectoriel des polynômes homogènes de degré d (engendré par les monômes

$$X_1^{d_1} \cdots X_n^{d_n}, d_1 + \cdots + d_n = d$$

on a

$$B = \oplus B^d \text{ et } B^d B^\delta \subset B^{d+\delta}.$$

Définition 0.2. — *On dit qu'un anneau A est* **Z***-gradué s'il est muni d'une décomposition $A = \oplus A^d$ telle que*

$$A^d A^\delta \subset A^{d+\delta}$$

pour tout d, δ. De même, un A-module M est dit gradué s'il est muni d'une décomposition $M = \oplus M^d$ telle que

$$A^d M^\delta \subset M^{d+\delta}$$

pour tout d, δ.

On retrouve les notions de VII.1 où l'anneau A était simplement vu comme gradué en degré nul (*ie* $A^d = 0$ si $d \neq 0$). On a alors de mêmes les notions de décalage, de morphisme gradué, de suite exacte... On identifiera toujours k au B-module gradué (concentré en degré 0)

$$k[X_1, \cdots, X_n]/(X_1, \cdots, X_n) \xrightarrow{\sim} k.$$

La structure de module est donc donnée par

$$P.\lambda = P(0)\lambda$$

pour $P \in B, \lambda \in k$.

Définition 0.3. — *On dira qu'un module scindé s'il est isomorphe (comme module gradué) à une somme finie de modules $B[m_i]$ où m_i est une famille finie d'entiers.*

Se donner un morphisme de B-modules gradués de

$$B[m] \to B[m + d],$$

c'est se donner l'image de $1 \in B^0 = B[m]^{-m}$, donc c'est se donner un élément de degré $-m$ de $B[m + d]$, autrement dit un élément de degré d de B, *ie* un *polynôme homogène* de degré d.Se donner un morphisme gradué de modules scindés

$$\oplus B[m_j] \to \oplus B[n_i]$$

c'est donc se donner une **matrice** $(P_{i,j})$ où $P_{i,j}$ est homogène de degré $n_i - m_j$ pour tout i, j.

1. Construction d'une résolution infinie

Construire une résolution infinie n'est pas difficile. On choisit un système de générateurs finis $m_1, \cdots, m_n$ de M. On décompose chaque m_i en somme $\sum_j m_{i,j}$ où chaque $m_{i,j}$ est dans M et est homogène de degré $d_{i,j}$ (possible, car M gradué). Chaque $m_{i,j}$ définit un morphisme gradué

$$B[-d_{i,j}] \overset{m_{i,j}}{\to} M$$

et finalement une surjection

$$L^0 = \oplus_{i,j} B[-d_{i,j}] \twoheadrightarrow M$$

qui est graduée (*ie* de degré 0). Mais le noyau K^0 de cette surjection est alors gradué, comme on l'a déjà observé. Comme B est noethérien, il est de type fini car L^0 est de type fini sur B, donc est un module noethérien. On réapplique ce qui précède à K^0 pour trouver une surjection graduée de L^{-1} libre gradué de rang fini sur K^0. En itérant le procédé, on construit une résolution infinie

$$\cdots L^{-m} \to \cdots\cdots\cdots L^0 \to M \to 0.$$

1.1. Étude d'un noyau. — Soit K^{-m} le noyau de $L^{-m} \to L^{-m+1}$ (on pose $L^1 = M$). On a une suite exacte

$$0 \to K^{-m} \to L^{-m} \to \cdots\cdots\cdots L^0 \to M \to 0.$$

Lemme 1.2. — *On a* $\mathrm{Tor}^B_{n-m}(k, K^{-m}) = 0$. *pour tout* m *tel que* $0 \leq m < n$.

Preuve : On fait une récurrence sur m. Si $m = 0$, on a une suite exacte

$$0 \to K^0 \to L^0 \to M \to 0$$

La suite des Tor donne

$$\mathrm{Tor}_{n+1}(k, M) \to \mathrm{Tor}_n(k, K^0) \to \mathrm{Tor}_n(k, L^0).$$

Comme $n > 0$ et L^0 libre, on a $\mathrm{Tor}_n(k, L^0) = 0$ et $\mathrm{Tor}_{n+1}(k, K^0)$ est toujours nul (formule VIII.4.a) de sorte que $\mathrm{Tor}_n(k, K^0) = 0$.

Supposons la propriété vraie au rang $m - 1, 0 \leq m < n$ et prouvons là au rang m. Comme l'image de $L^{-m} \to L^{-m+1}$ est le noyau K^{-m+1} de $L^{-m+1} \to L^{-m+2}$, on a une suite exacte

$$0 \to K^{-m} \to L^{-m} \to K^{-m+1} \to 0.$$

La suite des Tor donne

$$\mathrm{Tor}_{n-m+1}(k, K^{-m+1}) \to \mathrm{Tor}_{n-m}(k, K^{-m}) \to \mathrm{Tor}_{n-m}(k, L^{-m}).$$

Comme $n - m > 0$ et L^{-m} libre, on a d'une part $\mathrm{Tor}_n(k, L^{-m}) = 0$ et, d'autre part, $\mathrm{Tor}_{n-m+1}(k, K^{-m+1})$ est nul par hypothèse de récurrence. On en déduit l'égalité cherchée $\mathrm{Tor}_{n-m}(k, K^{-m}) = 0$ (comparer avec l'exercice I.8.2). ■

En appliquant le lemme à la suite précédente, on obtient

(1.2.a) $$\mathrm{Tor}^B_1(k, K^{-n+1}) = 0.$$

2. Le lemme de Nakayama gradué

On se donne un module M gradué de type fini sur B notre algèbre de polynôme. On a un analogue gradué du lemme de Nakayama (qui est valable dans les anneaux locaux rappelons le).

Lemme 2.1. — *Si $k \otimes_B M \xrightarrow{\sim} M/(X_1, \cdots, X_n)M$ est nul, alors $M = 0$.*

Preuve : Supposons $M \neq 0$. Soit m_i un famille finie de générateurs non nuls. Quitte à prendre comme nouveau système de générateurs leurs composantes homogènes, on peut supposer qu'ils sont homogènes. Soit m de degré δ minimal. Comme $M = (X_1, \cdots X_d)M$, on peut écrire $m = \sum P_i m_i$ avec P_i homogènes non constants, donc de degré > 0. Comme δ est minimal, on a nécessairement $m = 0$, une contradiction.■

Corollaire 2.2. — *Si M est gradué de type fini sur B. Alors, M est scindé si et seulement $\mathrm{Tor}_1^B(k, M)$ est nul.*

Preuve : Soit m_i une famille finie de générateurs homogènes de M. Les vecteurs $1 \otimes m_i \in k \otimes_B M \xrightarrow{\sim} M/(X_1, \cdots, X_n)M$ engendrent $k \otimes_B M$, qui est en particulier un espace vectoriel de dimension finie. Extrayons une base : on peut supposer que $1 \otimes m_1, \cdots, 1 \otimes m_n$ est une base de $k \otimes_B M$. Soit d_i les degrés de m_i. On a donc un morphisme f gradué

$$L = \oplus_{i=1}^n B[-d_i] \xrightarrow{(m_i)} M.$$

Par construction, la flèche

$$1 \otimes f : \ k \otimes_B L \xrightarrow{\sim} k^n \to k \otimes_B M$$

envoie la base canonique de k^n sur la base $1 \otimes \mathfrak{m}_i$ de $k \otimes_B M$: c'est un isomorphisme d'espaces vectoriels.
Montrons que f est un isomorphisme. Soit Q le conoyau de f : c'est un module gradué de type fini. Par exactitude à droite du produit tensoriel, la suite

$$k \otimes_B L \xrightarrow{1 \otimes f} k \otimes_B M \to k \otimes_B Q \to 0$$

est exacte. Or $1 \otimes f$ est un isomorphisme, en particulier est surjective, de sorte qu'on a $k \otimes_B Q = 0$. Le lemme de Nakayama gradué assure la nullité de Q et donc la surjectivité de f. Soit alors K le noyau de f. On a une suite exacte

$$0 \to K \to L \to M \to 0$$

qui donne une suite exacte

$$0 = \mathrm{Tor}_1^B(k, M) \to k \otimes_B K \to k \otimes_B L \xrightarrow{1 \otimes f} k \otimes_B M$$

qui assure que $k \otimes_B K$ est le noyau de $1 \otimes f$ qui est un... isomorphisme : $k \otimes_B K = 0$. Comme K est gradué de type fini sur B (rappelons que B est noethérien et L de type fini), le lemme de Nakayama assure que K est nul et donc que M est scindé.■

3. Le théorème des syzygies de Hilbert

On est en mesure de prouver le théorème des syzygies.

***Théorème 3.1* (Hilbert).** — *Soit M un $k[X_1, \cdots, X_n]$ module gradué de type fini. Alors, M a une résolution de longueur n par des modules scindés.*

Preuve : On reprend les notations de la section 1.1. On a d'après 1.2.a la nullité de $\mathrm{Tor}_1^B(k, K^{-n+1})$ et d'après le corollaire 2.2 appliqué à K^{-n+1}, ce module est scindé.■

Notons que l'exercice VIII.4.1 prouve qu'on ne peut faire mieux, *ie* trouver en général des résolution plus courtes. D'une certaine manière, on peut considérer que cet énoncé code un module gradué de type fini par une suite de matrices à coefficients polynomiaux, celles-la même qui définissent les morphismes dans la résolution. C'est grâce à ce genre de résolutions que l'on étudie les modules.

PARTIE X

GÉNÉRALISATION DES FONCTEURS Tor

L'objet de cette partie est de montrer comment les techniques développées pour définir les foncteurs Tor permettent de dériver des foncteurs plus généraux.

1. Foncteurs exacts à droite généraux

On se donne F un foncteur de la catégorie des modules $\mathcal{M}od$ sur un anneau A dans une catégorie abélienne $\mathcal{B}$, additif au sens que l'application induite au niveau des morphismes est additive. On suppose qu'il est exact à droite, *ie* transforme la suite exacte

$$N_1 \to N_2 \to N_3 \to 0$$

en la suite exacte

$$F(N_1) \to F(N_2) \to F(N_3) \to 0.$$

Par exemple, le foncteur $F_0(M) = M \otimes_A N$ vérifie ces propriétés ainsi que foncteur $F_1(M) = \mathrm{Ext}^1(M, N)$ de $\mathcal{M}od$ dans $\mathcal{M}od^{opp}$. On définit les foncteurs dérivés $L^jF(M)$ par la formule

$$L^jF(M) = H^{-j}(L(M) \otimes_A N)$$

où $L(M)$ est la résolution libre canonique de M. Par exemple, pour F_0, on retrouve les Tor. Exactement comme précédemment, On a un isomorphisme de foncteurs $L^0F \Rightarrow F$, une suite exacte longue de cohomologie

$$L^jF(N_1) \to L^jF(N_2) \to \cdots \to L^1F(N_1) \to L^1F(N_2) \to L^1F(N_3) \to F(N_1) \to F(N_2) \to F(N_3) \to 0$$

associée à toute suite exacte courte, fonctorielle en un sens évident.

En étant un tout petit peu prudent avec des problèmes de logique du style ensemble de tous les ensembles, on peut même remplacer la catégorie des modules par une catégorie abélienne qui a assez de projectif, *ie* tel que tout objet b est la source d'un épimorphisme $a \to b \to 0$ avec a projectif. On remplace $L(M)$ par une résolution projective. Elle n'est pas unique, mais l'est à homotopie près. Les modules de cohomologie sont bien définis à isomorphisme unique près : ce sont les foncteurs dérivés.

2. Foncteurs exacts à gauche généraux

On se donne G un foncteur de la catégorie des modules $\mathcal{M}od$ sur un anneau A dans une catégorie abélienne $\mathcal{B}$, additif au sens que l'application induite au niveau des morphismes est additive. On suppose qu'il est exact à gauche, *ie* transforme la suite exacte

$$0 \to N_1 \to N_2 \to N_3$$

en la suite exacte

$$0 \to G(N_1) \to G(N_2) \to G(N_3).$$

Par exemple, $G_0(N) = \mathrm{Hom}(M, N)$ est un tel foncteur.

Le foncteur G peut être vu aussi comme un foncteur

$$G^{opp} : \mathcal{M}od^{opp} \to \mathcal{B}^{opp},$$

qui est exact... à droite!!! On peut donc le dériver, pourvu qu'on ait assez de projectifs dans $\mathcal{M}od^{opp}$. Cette précision est importante. Car être projectif dans $\mathcal{M}od^{opp}$ n'est pas du tout être projectif dans $\mathcal{M}od$. On vérifie que la condition I projectif dans $\mathcal{M}od^{opp}$ signifie exactement que le foncteur $M \to \mathrm{Hom}(M, I)$ est exact dans $\mathcal{M}od$, *ie* que tout morphisme d'un sous-module M' de M dans I se prolonge à I. Un tel module I est dit *injectif*.

Une résolution projective de M dans $\mathcal{M}od^{opp}$ est simplement alors une suite exacte

$$0 \to M \to I^0(M) \to I^1(M) \to \cdots$$

avec $I^n(M)$ onjectif pour tout n. De même que tout module a une résolution projective (libre en fait) dans $\mathcal{M}od$, on montre que tout module M a une résolution injective canonique $I(M)$ canonique. Il suffit bien entendu de plonger tout module dans un injectif $I[M]$.

On montre alors que le A-module $I[M] = E^{\mathrm{Hom}_A(M,E)}$ avec $E = \mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z})$ est injectif est injectif et que l'application (bidualité)

$$m \mapsto (\phi(m))_{\phi \in \mathrm{Hom}(M,E)}$$

est injective (cf. [**1**]). Ceci permet de définir comme plus haut le foncteur dérivé $R^jG(M) = H^j(I(M)$. Il est isomorphe en degré 0 à F, et on a une suite exacte de cohomologie

$$0 \to G(N_3) \to G(N_2) \to G(N_1) \to R^1G(N_3) \to R^1G(N_2) \to \cdots$$

associée à la suite exacte courte plus haut (grâce à l'exercice VIII.5.1), fonctorielle. Bien entendu, on peut calculer les foncteurs dérivés avec n'importe quelle résolution injective, de sorte que $R^jG(I) = 0$ pour $j > 0$ et I injectif.

On peut montrer dans le cas de G_0, l'existence d'un isomorphisme fonctoriel $R^jG_0(N) = \mathrm{Ext}^j(M, N)$. Autrement dit, on peut calculer les Ext soit par résolution projective de M soit par résolution injective de N. Une façon de procéder (exercice) est de prouver, comme pour la preuve de la symétrie des foncteurs Tor, qu'on peut calculer les foncteurs dérivés LF_1 et RG_0 en utilisant en même temps une résolution projective de M et une résolution injective de N, *ie* , en mettant des signes convenables sur le complexe total $\mathrm{Hom}(L(M), I(N))$ de montrer que les flèches homologismes $M \to L(M)$ et $N \to I(N)$ induisent des homologismes

$$\mathrm{Hom}(L(M), N) \to \mathrm{Hom}(L(M), I(N))$$

et

$$\mathrm{Hom}(L(M), I(N)) \to \mathrm{Hom}(M, I(N)).$$

Table des matières

Partie I. Généralités sur les modules ... 2
I.1. La notion de module ... 2
I.2. Groupes abéliens et **Z**-modules ... 2
I.3. Endomorphisme des k-espaces vectoriels et $k[X]$-module ... 3
I.4. Morphismes ... 3
I.5. Sous-modules ... 4
I.6. Somme directe de modules-Modules libres ... 4
I.7. Modules quotients ... 5
I.8. Diagrammes, complexes, suites exactes ... 6
I.9. Anneaux quotients ... 7
I.10. Rang d'un module libre de type fini ... 8
I.11. Le lemme Chinois ... 9
I.12. Algèbres ... 10
I.13. Une application du lemme chinois : l'algorithme de Berlekamp ... 10
I.14. Module des fractions ... 12
I.15. Radical nilpotent d'un anneau ... 14
I.16. Parenthèse sur les catégories, I ... 15
I.17. Un critère d'exactitude universel ... 16
I.18. Le lemme du serpent ... 17
I.19. Scindages ... 19
I.20. Conditions de finitude ... 19
I.21. Présentation du $k[X]$-module associé à un endomorphisme ... 20
I.22. Interprétation calculatoire ... 21

Partie II. Modules et anneaux noethériens ... 22
II.1. Modules noethériens ... 22
II.2. Anneaux noethériens ... 23
II.3. Construction d'anneaux noethériens : transfert I ... 23
II.4. Décomposition en facteurs premiers ... 24
II.5. Parenthèse sur les catégories, II ... 25

Partie III. Anneaux factoriels ... 27
III.1. Définition et caractérisation ... 27
III.2. Rappels sur les anneaux principaux ... 28
III.3. Valuations et anneaux factoriels ... 29
III.4. PGCD,PPCM ... 30
III.5. Factorialité des anneaux de polynômes : transfert II ... 31
III.6. Parenthèse sur les catégories, III ... 33

Partie IV. Modules sur les anneaux principaux ... 35
IV.1. Une suite exacte fondamentale ... 35
IV.2. Décomposition des modules de torsion ... 36
IV.3. Modules de type fini sur un anneau principal ... 38
IV.4. Algèbre linéaire et facteurs invariants ... 44

Partie V. Considérations tensorielles, ou comment remplacer du bilinéaire par du linéaire ... 48
V.1. Existence ... 48
V.2. Fonctorialité en M, N ... 49
V.3. Tenseurs purs ... 49
V.4. Commutativité du produit tensoriel ... 50
V.5. Produit tensoriel et somme directe ... 50
V.6. Exactitude à droite du produit tensoriel ... 51
V.7. Défaut d'exactitude du produit tensoriel ... 52
V.8. Extension des scalaires ... 53
V.9. Associativité du produit tensoriel ... 53
V.10. Produit tensoriel d'algèbres de polynômes ... 54
V.11. Produit tensoriel et module d'homomorphismes ... 54
V.12. Algèbre tensorielle ... 55

Partie VI. Algèbre extérieure ... 57
VI.1. Définition ... 57
VI.2. Cas d'un module libre ... 58

VI.3. Produit extérieur et somme directe 61
VI.4. Produit intérieur par une forme linéaire 62
VI.5. Parenthèse sur les modules projectifs 62
VI.6. Complexe de Koszul 63

Partie VII. Cohomologie des complexes 64
VII.1. Parenthèse sur les modules gradués 64
VII.2. Cohomologie des complexes 64
VII.3. Suite exacte de cohomologie 65
VII.4. Application au complexe de Koszul 67

Partie VIII. Foncteur Tor 69
VIII.1. Résolutions libres 69
VIII.2. Les modules $\mathrm{Tor}_j(M,N)$ 69
VIII.3. Fonctorialité 70
VIII.4. Une annulation fondamentale 72
VIII.5. La suite exacte des Tor 72

Partie IX. Le théorème des syzygies de Hilbert 74
IX.1. Construction d'une résolution infinie 75
IX.2. Le lemme de Nakayama gradué 76
IX.3. Le théorème des syzygies de Hilbert 76

Partie X. Généralisation des foncteurs Tor 78
X.1. Foncteurs exacts à droite généraux 78
X.2. Foncteurs exacts à gauche généraux 78
Références 81

Références

[1] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1980. Algèbre. Chapitre 10. Algèbre homologique. [Algebra. Chapter 10. Homological algebra].

[2] D. Hilbert. Über die theorie der algebraischen formen. *Math. Ann.*, (36) :473–534, 1890.

[3] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

9 décembre 2003

YVES LASZLO, Université Paris VI • *E-mail :* laszlo@math.jussieu.fr