ALGÈBRE M1

par

Laurent Berger

Table des matières

1. Anneaux et modules

On considère des anneaux commutatifs et pour lesquels $0 \neq 1$.

1.1. Modules et suites exactes. — Un *module* sur un anneau A est l'analogue d'un espace vectoriel sur un corps K, c'est-à-dire que c'est un ensemble M muni d'une loi $+$ telle que $(M,+)$ est un groupe abélien et d'une loi $A \times M \to M$ qui à (a,m) associe am et vérifie :

1. $(a+b)m = am + bm$ et $a(m+n) = am + an$;
2. $a(bm) = abm$ et $1 \cdot m = m$.

Contrairement au cas des espaces vectoriels, le fait que $am = 0$ n'implique pas que $a = 0$ ou que $m = 0$, et les A-modules n'admettent pas de bases en général. La théorie des A-modules est beaucoup plus riche que celle des espaces vectoriels sur un corps.

Sous-modules ; si A est un anneau intègre, et M est un A-module, alors l'ensemble M_{tors} des éléments de torsion est un sous-module de M.

Un morphisme $f : M \to N$ est une application additive et A-linéaire. L'ensemble des morphismes de M dans N est noté $\mathrm{Hom}_A(M,N)$ ou plus simplement $\mathrm{Hom}(M,N)$ et c'est un A-module. Notons que $\mathrm{Hom}(A,M) = M$ pour tout A-module M. Le module dual de M est M^* ou $M^\vee$ et est défini par $M^\vee = \mathrm{Hom}(M,A)$. C'est donc l'ensemble des *formes linéaires* sur M.

Étant donnée une application $f : M \to N$, on note $\ker(f) = \{m \in M \mid f(m) = 0\}$ et $\mathrm{im}(f) = \{f(m), m \in M\}$. Ce sont des sous-modules de M et N respectivement. Si l'on a trois modules L, M et N et $f : L \to M$ et $g : M \to N$, alors on écrit plutôt la *suite* :

$$L \xrightarrow{f} M \xrightarrow{g} N,$$

et on dit que cette suite est *exacte* en M si $\mathrm{im}(f) = \ker(g)$. Cette définition est absolument fondamentale. Si on a une suite :

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to \cdots,$$

alors on dit que cette suite est exacte en M_i si $\mathrm{im}(f_{i-1}) = \ker(f_i)$ et on dit que la suite est exacte si elle est exacte en M_i pour tout i.

Par exemple, la suite $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est exacte si et seulement si :

1. f est injective ;
2. $\mathrm{im}(f) = \ker(g)$;
3. g est surjective.

Si l'on a $f : N_1 \to N_2$, on en déduit $f_* : \mathrm{Hom}_A(M, N_1) \to \mathrm{Hom}_A(M, N_2)$, donnée par $f_* : h \mapsto f \circ h$. Si l'on a $f : M_1 \to M_2$, on en déduit $f^* : \mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N)$, donnée par $f^* : h \mapsto h \circ f$.

Proposition 1.1. —

1. *La suite* $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ *est exacte si et seulement si la suite* $0 \to \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'')$ *est exacte pour tout* M.
2. *La suite* $M' \to M \to M'' \to 0$ *est exacte si et seulement si* $0 \to \mathrm{Hom}_A(M'', N) \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$ *est exacte pour tout* N.

Démonstration. — Rappelons que $\mathrm{Hom}(A, P) = P$ pour tout A-module P. Si la suite $0 \to \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'')$ est exacte pour $M = A$, alors la suite $0 \to N' \to N \to N''$ est exacte. Montrons l'implication réciproque. Tout d'abord, montrons que f_* est injective. Si $f_*(h) = 0$, alors $f(h(m)) = 0$ pour tout $m \in M$ et comme f est injective, on voit que $h(m) = 0$ pour tout m et donc $h = 0$. Ensuite, montrons que $\ker(g_*) = \mathrm{im}(f_*)$. On a $g_*(f_*(h))(m) = g(f(h(m))) = 0$ et donc $\mathrm{im}(f_*) \subset \ker(g_*)$. Si $g_*(h) = 0$, alors $g(h(m)) = 0$ pour tout m et donc $h(m) = f(n')$ pour un $n' \in N'$ qui est unique car f est injective. Si on pose $i(m) = n'$, alors $i \in \mathrm{Hom}(M, N')$ et $h(m) = f(i(m))$ et donc $h = f_*(i)$. Ceci montre le (1). Le (2) se montre de manière analogue : exercice. □

Si M et N sont deux modules, alors on définit $M \oplus N$, et $M \oplus N = M \times N$. Plus généralement, si on a une famille de modules $\{M_i\}_{i \in I}$ on peut définir la somme directe $\oplus_{i \in I} M_i$ et le produit $\prod_{i \in I} M_i$. On a $\oplus_{i \in I} M_i \subset \prod_{i \in I} M_i$ avec égalité si et seulement si I est fini. Notons que $\mathrm{Hom}(\oplus_{i \in I} M_i, N) = \prod_{i \in I} \mathrm{Hom}(M_i, N)$ et que $\mathrm{Hom}(M, \prod_{j \in J} N_j) = \prod_{j \in J} \mathrm{Hom}(M, N_j)$. Plus généralement, on a $\mathrm{Hom}(\oplus_{i \in I} M_i, \prod_{j \in J} N_j) = \prod_{I \times J} \mathrm{Hom}(M_i, N_j)$.

Si M est un sous-module de N, alors on définit une relation d'équivalence sur N par $n_1 \sim n_2$ si et seulement si $n_1 - n_2 \in M$ et on note N/M l'ensemble des classes d'équivalence de $\sim$. On munit cet ensemble des lois $\overline{n}_1 + \overline{n}_2 = \overline{n_1 + n_2}$ et $a \cdot \overline{n} = \overline{an}$. C'est un exercice de vérifier que les lois ne dépendent pas des choix faits, et qu'elles font de N/M un A-module. On a alors une suite exacte :

$$0 \to M \to N \xrightarrow{n \mapsto \overline{n}} N/M \to 0.$$

Si $f : N \to P$ est nulle sur $M \subset N$, alors f se factorise par $\overline{f} : N/M \to P$.

Corollaire 1.2. — *Si l'on a une suite exacte* $0 \to M \xrightarrow{f} N \xrightarrow{g} Q \to 0$, *alors* $Q \simeq N/f(M)$. *Par exemple, étant donné* $f : N \to P$, *on a* $N/\ker(f) \simeq \mathrm{im}(f)$.

Si l'on a $f : M \to N$, on note $\mathrm{coker}(f) = N/\mathrm{im}(f)$ le *conoyau* de f et on a alors une suite exacte :

$$0 \to \ker(f) \to M \xrightarrow{f} N \to \mathrm{coker}(f) \to 0.$$

Enfin, f est injective si et seulement si $\ker(f) = 0$ et f est surjective si et seulement si $\mathrm{coker}(f) = 0$.

Notons que si l'on se donne $f : M \to N$ et $X \subset M$ et $Y \subset N$ deux sous-modules de M et N tels que $f(X) \subset Y$, alors l'application $\overline{f} : M/X \to N/Y$ est bien définie.

Un *diagramme* est une collection de modules $\{M_i\}_i$ et de morphismes f_{ij} entre eux, par exemple :

$$\begin{array}{ccc} M_1 & \xrightarrow{f_{12}} & M_2 \\ {\scriptstyle f_{13}}\downarrow & & \downarrow{\scriptstyle f_{24}} \\ M_3 & \xrightarrow{f_{34}} & M_4. \end{array}$$

On dit qu'un diagramme est *commutatif* si quels que soient i et j et le chemin que l'on choisit de M_i à M_j en suivant les flèches, on obtient le même résultat. Par exemple, le diagramme ci-dessus est commutatif si et seulement si $f_{24} \circ f_{12} = f_{34} \circ f_{13}$.

Nous allons énoncer le *lemme du serpent*. Considérons un diagramme commutatif où les lignes sont exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{u} & B & \xrightarrow{v} & C & \longrightarrow & 0 \\ & & {\scriptstyle a}\downarrow & & {\scriptstyle b}\downarrow & & {\scriptstyle c}\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{u'} & B' & \xrightarrow{v'} & C' & \longrightarrow & 0 \end{array}$$

Construisons une application $\delta : \ker(c) \to \mathrm{coker}(a)$. Si $z \in \ker(c)$, alors on peut écrire $z = v(y)$ avec $y \in B$ et on a $0 = cv(y) = v'b(y)$ ce qui fait que $b(y) \in \ker(v') = \mathrm{im}(u')$ et il existe donc un (et un seul) $x' \in A$ tel que $b(y) = u'(x')$. Si on avait choisi un y différent, disons $\tilde{y}$ tel que $z = v(\tilde{y})$, alors $y - \tilde{y} \in \ker(v) = \mathrm{im}(u)$ et donc $b(y - \tilde{y}) \in b(\mathrm{im}(u)) = u'(\mathrm{im}(a))$ ce qui fait que $\tilde{x}' - x' \in \mathrm{im}(a)$. L'application $\delta : y \mapsto \overline{x}'$ de $\ker(c)$ dans $\mathrm{coker}(a)$ est donc bien définie.

Théorème 1.3. — *La suite :*

$$0 \to \ker(a) \xrightarrow{u} \ker(b) \xrightarrow{v} \ker(c) \xrightarrow{\delta} \mathrm{coker}(a) \xrightarrow{\overline{u}'} \mathrm{coker}(b) \xrightarrow{\overline{v}'} \mathrm{coker}(c) \to 0$$

est exacte.

1.2. Modules noethériens. — On dit qu'un module M est de *type fini* s'il existe $m_1, \ldots, m_r \in M$ tels que $M = \{\sum_{i=1}^r a_i m_i,\ a_i \in A\}$ (on écrit alors $M = (m_1, \ldots, m_r)$), ce qui revient à dire qu'il existe un morphisme surjectif $A^r \to M$.

On dit qu'un A-module M est *noethérien* (d'après Emmy Noether) si tout sous-A-module de M est de type fini (en particulier M lui-même). On dit que A est un anneau *noethérien* si tout idéal I de A est de type fini, c'est-à-dire si A est un A-module noethérien. En particulier, un anneau principal est noethérien (tout idéal étant engendré par un seul élément).

Proposition 1.4. — *Un A-module M est noethérien si et seulement si toute suite croissante $M_1 \subset M_2 \subset \cdots$ de sous-modules de M est stationnaire (constante après un certain rang).*

Démonstration. — Si M est noethérien et si $M_1 \subset M_2 \subset \cdots$ est une telle suite, alors $N = \cup_{i\geq 1} M_i$ est un sous-module de M et est donc de type fini, engendré par $m_1, \ldots, m_r$. Il existe alors $n \gg 0$ tel que $m_i \in M_n$ ce qui fait que $M_n = M_{n+1} = \cdots = N$.

Réciproquement, soit M vérifiant la condition sur les suites de sous-modules et N un sous-module de M, dont on suppose qu'il n'est pas de type fini. Soit $m_1 \in N$ et $M_1 = (m_1)$. Pour $i \geq 1$, on choisit $m_{i+1} \in N \setminus M_i$ ce qui est possible car M_i est de type fini, et on pose $M_{i+1} = (m_{i+1}, M_i)$. La suite des M_i est strictement croissante, contradiction. □

Lemme 1.5. — *Si L, M et N sont trois A-modules et si on a une suite exacte :*

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0,$$

alors M est noethérien si et seulement si L et N le sont.

Démonstration. — Si M est noethérien, alors un sous-module de L est via f un sous-module de M et est donc de type fini ce qui fait que L est noethérien. Si P est un sous-module de N, alors $g^{-1}(P)$ est un sous-module de M qui est donc de type fini et si l'on note $m_1, \ldots, m_r$ des éléments qui l'engendrent, alors $g(m_1), \ldots, g(m_r)$ engendrent P et donc N est noethérien.

Si L et N sont noethériens, soit P un sous-module de M, soient $\ell_1, \ldots, \ell_r$ des éléments de L tels que $f(\ell_1), \ldots, f(\ell_r)$ engendrent $f(L) \cap P$ et soient $p_1, \ldots, p_s$ des éléments de P dont les images dans N engendrent $g(P)$. Si $p \in P$, alors il existe des $a_i \in A$ tels que $g(p) = \sum_{i=1}^s a_i g(p_i)$ ce qui fait que $p - \sum_{i=1}^s a_i p_i \in \ker(g) = \mathrm{im}(f)$ et donc qu'il existe des b_i tels que $p = \sum_{i=1}^s a_i p_i + \sum_{j=1}^r b_j f(\ell_j)$ ce qui fait que P est de type fini engendré par les $f(\ell_j)$ et les p_i. □

Théorème 1.6. — *Si A est un anneau noethérien, alors tout A-module M de type fini est noethérien.*

Démonstration. — Si $r \geq 1$, alors on a une suite exacte $0 \to A \to A^r \to A^{r-1} \to 0$ d'où l'on déduit par récurrence (par le lemme 1.5) que A^r est noethérien pour tout $r \geq 1$.

Si M est un A-module de type fini, alors il existe un morphisme surjectif $g : A^r \to M$ et cela nous donne une suite exacte $0 \to \ker(g) \to A^r \xrightarrow{g} M \to 0$ d'où l'on déduit (par le lemme 1.5) que M est noethérien. □

Les anneaux de polynômes $K[X_1, \ldots, X_n]$ sont noethériens. En fait, beaucoup des anneaux que l'on rencontre le sont. En voici un qui ne l'est pas : soit K un corps et A l'ensemble des suites $(x_n)_{n\geq 1}$ d'éléments de K (l'addition et la mutliplication étant terme à terme). L'idéal I des suites nulles à partir d'un certain rang n'est alors pas de type fini.

1.3. Modules libres de type fini et matrices. — Soit A un anneau et J un ensemble. Rappelons qu'on note $\oplus_{j\in J} A$ l'ensemble des suites $x = (x_j)_{j\in J}$ telles que $x_j = 0$ pour tout j sauf un nombre fini. Si M est un A-module, on dit qu'une famille $\{m_j\}_{j\in J}$ d'éléments de M est une *base* de M si l'application $\oplus_{j\in J} A \to M$ donnée par $(x_j)_{j\in J} \mapsto \sum_{j\in J} x_j m_j$ est un isomorphisme (l'application est bien définie puisque pour chaque x, $x_j = 0$ pour tout j sauf un nombre fini). On dit qu'un A-module M est *libre* s'il admet une base.

Proposition 1.7. — *Si M est un A-module libre, alors deux bases de M ont même cardinal.*

Démonstration. — Soit $\{m_j\}_{j\in J}$ une base de M et I un idéal maximal de A. Le module quotient M/IM est un A/I-espace vectoriel et les $\{\overline{m}_j\}_{j\in J}$ en forment une base, ce qui fait que $\mathrm{card}(J) = \dim_{A/I} M/IM$. □

On dit qu'un A-module M est *libre de type fini* s'il admet une base finie, ce qui revient à dire qu'il existe $r \geq 1$ et un isomorphisme $f : A^r \to M$.

Si M est un A-module libre de type fini, alors par la proposition 1.7, l'entier r tel que $M \simeq A^r$ est bien défini et on l'appelle le *rang* de M. Si M et N sont deux A-modules libres de rang r et s, dont on choisit des bases $\{m_i\}$ et $\{n_j\}$, et si $f : M \to N$ est un morphisme, alors la matrice de f dans les bases $\{m_i\}$ et $\{n_j\}$ est $\mathrm{Mat}(f) = (f_{i,j})$ où $f(m_j) = \sum_{i=1}^{s} f_{i,j} n_i$. Les règles habituelles de l'algèbre linéaire s'appliquent toujours ; en particulier, on a $\mathrm{Mat}(fg) = \mathrm{Mat}(f)\,\mathrm{Mat}(g)$. On note $\mathrm{M}_{m\times n}(A)$ et $\mathrm{M}_n(A)$ les matrices à m lignes et n colonnes et les matrices carrées $n \times n$.

Si $P = (p_{i,j}) \in \mathrm{M}_n(A)$, on définit $\det(P) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) p_{1,\sigma(1)} \cdots p_{n,\sigma(n)}$ et on a alors $\det(PQ) = \det(P)\det(Q)$ et si ${}^t\mathrm{co}(P)$ désigne la transposée de la comatrice de P, alors ${}^t\mathrm{co}(P) \cdot P = \det(P)\,\mathrm{Id}$. En particulier, la matrice P est inversible dans $M_n(A)$ si et seulement si $\det(P) \in A^\times$; on note $\mathrm{GL}_n(A)$ l'ensemble de ces matrices.

Proposition 1.8. — *Soit M un A-module libre de rang r et $f : M \to M$ linéaire et $P = \mathrm{Mat}(f)$ dans une base $\{m_i\}_i$ de M.*

1. *L'application f est surjective si et seulement si $\det(P) \in A^\times$;*
2. *L'application f est injective si et seulement si $\det(P)$ n'est pas un diviseur de zéro dans A.*

Démonstration. — Si f est surjective, alors $f(m_1), \dots, f(m_r)$ engendrent M et donc il existe $Q \in \mathrm{GL}_r(A)$ telle que $QP = \mathrm{Id}$ et donc $\det(P) \in A^\times$. Si $\det(P) \in A^\times$, alors $\det(P)^{-1} \cdot {}^t\mathrm{co}(P) \cdot P = \mathrm{Id}$ et $f(m_1), \dots, f(m_r)$ engendrent donc M. Ceci montre le (1).

Si f n'est pas injective, alors il existe $v \in A^r$ tel que $Pv = 0$ et ${}^t\mathrm{co}(P) \cdot Pv = \det(P)v = 0$ ce qui fait que $\det(P)$ divise zéro. Supposons enfin que $\det(P)$ divise zéro, c'est-à-dire qu'il existe $h \in A \setminus \{0\}$ tel que $h \cdot \det(P) = 0$. Si $hP = 0$, alors $P(h, 0, \dots, 0) = 0$ et on a fini. Sinon, parmi tous les mineurs de P, il en existe un $\mu = \min_{i_1 \dots i_n}^{j_1 \dots j_n} P$ de taille maximale $n < r$ tel que $h \cdot \mu \neq 0$. Soit $i_0 \neq i_k$ et $x = (x_1 \dots x_r)$ où $x_i = 0$ si $i \neq i_k$ et $x_{i_k} = (-1)^k h \cdot \min_{i_0 \dots \widehat{i_k} \dots i_n}^{j_1 \dots j_n} P$. On a alors $x \neq 0$ et $Px = y = 0$, car $y_j = h \cdot \min_{i_0 \dots i_n}^{j, j_1 \dots j_n} P$, ce qui fait que f n'est pas injective. □

Corollaire 1.9. — *Si $f : A^r \to A^r$ est surjective, alors elle est injective.*

Corollaire 1.10. — *Si $f : A^r \to A^s$ est injective, alors $r \leq s$.*

Démonstration. — Si $s < r$, alors on étend f par 0 en une fonction $f' : A^r \to A^s \oplus A^{r-s}$. Cette nouvelle fonction est injective si f l'est, mais $\det(f') = 0$ ce qui contredit le (2) de la proposition 1.8. □

Si $P \in \mathrm{M}_n(A)$, alors on définit le *polynôme caractéristique* $\Pi_P(X) = \det(X \cdot \mathrm{Id} - P) \in A[X]$ et le *théorème de Cayley-Hamilton* est toujours vrai.

Théorème 1.11. — *Si M est un A-module engendré par n éléments $m_1, \dots, m_n$, si $f : M \to M$ est un endormorphisme de M, et si $P \in \mathrm{M}_n(A)$ est telle que $f(m_i) = \sum_j p_{ij} m_j$, alors $\Pi_P(f)$ est nul sur M.*

Démonstration. — Considérons M comme un module sur $A[X]$ en posant $X \cdot m = f(m)$. On a alors :

$$(X \cdot \mathrm{Id} - P) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

et donc :
$$\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix} = (X\cdot\mathrm{Id}-P)\begin{pmatrix}m_1\\ \vdots\\ m_n\end{pmatrix} = {}^t\mathrm{co}(X\cdot\mathrm{Id}-P)\cdot(X\cdot\mathrm{Id}-P)\begin{pmatrix}m_1\\ \vdots\\ m_n\end{pmatrix} = \det(X\cdot\mathrm{Id}-P)\cdot\mathrm{Id}\begin{pmatrix}m_1\\ \vdots\\ m_n\end{pmatrix},$$
ce qui fait que $\det(X\cdot\mathrm{Id}-P)m_i = 0$ pour tout i et donc que $\Pi_P(f) = 0$ sur M. □

Corollaire 1.12. — *Si M est un A-module de type fini et I est un idéal de A tel que $M \subset I\cdot M$, alors il existe $x \equiv 1 \bmod I$ tel que $xM = 0$.*

Démonstration. — Appliquer le théorème 1.11 à $f = \mathrm{Id}$. □

Rappelons qu'un anneau A est dit *local* s'il admet un unique idéal maximal. Un anneau est donc local si et seulement si l'ensemble de ses non-inversibles en est un idéal. Si A est local d'idéal maximal I, le corps A/I s'appelle le corps résiduel de A. Si A est local d'idéal maximal I, et M est un A-module, alors M/IM est un A/I-espace vectoriel.

Proposition 1.13. — *Soit A un anneau local et I son idéal maximal. Si M est un A-module de type fini et si $m_1,\dots,m_n$ sont tels que leurs images engendrent le A/I-espace vectoriel M/IM, alors M est engendré par $m_1,\dots,m_n$.*

Démonstration. — Soit $N = \sum_i A\cdot m_i$. On a $M = IM + N$ et donc $I(M/N) = (IM + N)/N = M/N$ ce qui fait qu'il existe $x \equiv 1 \bmod I$ tel que $x(M/N) = 0$. Comme $x \in A^\times$, on a $M/N = 0$ et donc $M = N = \sum_i A\cdot m_i$. □

2. Modules de type fini sur un anneau principal

2.1. Facteurs invariants pour un anneau principal. — Il n'est pas vrai, en général, qu'un sous-module d'un module libre est lui-même libre (par exemple $(X,Y) \subset K[X,Y]$) mais sur un anneau principal, c'est vrai.

Théorème 2.1. — *Si A est un anneau principal, si M est un A-module libre de rang r et si N est un sous-A-module de M, alors N est libre de rang $\leq r$.*

Démonstration. — Soit $\{m_i\}$ une base de M et $N_i = N \cap (m_1,\dots,m_i)$. Nous allons montrer par récurrence sur i que N_i est libre de rang $\leq i$. Comme $N_1 \subset (m_1) \simeq A$ et que A est principal, N_1 est de la forme (a_1m_1) avec $a_1 \in A$ et il est donc libre de rang ≤ 1. Soit $i \geq 1$ et I l'ensemble des $a \in A$ tels qu'il existe $x \in N_{i+1}$ qui peut s'écrire $x = b_1m_1 + \cdots + b_im_i + am_{i+1}$. C'est un idéal de A et il est donc engendré par un élément $a_{i+1} \in A$. Si $a_{i+1} = 0$, alors $N_{i+1} = N_i$ et N_{i+1} est bien libre de rang $\leq i+1$. Sinon, soit $x \in N_{i+1}$ tel que $x = b_1m_1 + \cdots + b_im_i + a_{i+1}m_{i+1}$. Si $y \in N_{i+1}$, alors il existe $b \in A$ tel

que $y - bx \in N_i$ et comme $N_i \cap (x) = \{0\}$, on a $N_{i+1} = N_i \oplus (x)$ qui est donc libre de rang $\leq i + 1$. □

Contrairement à ce qui se passe pour les espaces vectoriels sur un corps, il n'existe pas nécessairement $P \subset M$ tel que $M = N \oplus P$, par exemple $N = 2\mathbf{Z}$ n'a pas de « supplémentaire » dans $M = \mathbf{Z}$.

Le résultat ci-dessous précise le théorème 2.1 et est fondamental.

Théorème 2.2. — *Si A est un anneau principal, si M est un A-module libre de rang r et si N est un sous-A-module de M de rang s, alors il existe une base $m_1, \ldots, m_r$ de M et des éléments $d_1, \ldots, d_s$ de $A \setminus \{0\}$ tels que :*

1. *les $d_1 m_1, \ldots, d_s m_s$ forment une base de N ;*
2. *on a $d_1 \mid d_2 \mid \cdots \mid d_s$.*

Démonstration. — Pour que la démonstration soit aussi claire que possible, nous montrons le théorème dans le cas où A est un anneau euclidien (c'est le cas dans les deux applications les plus importantes, $A = \mathbf{Z}$ et $A = K[X]$). La démonstration dans le cas général est assez semblable mais l'une des étapes est plus technique.

Montrons donc le théorème sous l'hypothèse supplémentaire que A est un anneau euclidien. Si l'on choisit des bases de M et N, alors la matrice de la base de N selon celle de M est une matrice $P \in \mathrm{M}_{r\times s}(A)$ et si l'on change les bases de M ou de N, cela revient à remplacer P par XPY avec $X \in \mathrm{GL}_r(A)$ et $Y \in \mathrm{GL}_s(A)$. Pour montrer le théorème, il faut donc montrer qu'il existe $X \in \mathrm{GL}_r(A)$ et $Y \in \mathrm{GL}_s(A)$ telles que XPY a tous ses termes nuls sauf ses s premiers termes diagonaux, et que ceux-ci satisfont la condition (2). Nous allons montrer que l'on peut faire cela en ne modifiant P que par des opérations élémentaires sur les lignes et les colonnes (si A n'est que principal, alors ce n'est justement pas toujours possible).

Si $P = 0$, alors il n'y a rien à faire. Sinon, posons $N(P) = \min\{N(p_{i,j}),\ p_{i,j} \neq 0\}$. Quitte à permuter les lignes et les colonnes, on peut supposer que $N(P) = N(p_{1,1})$. Supposons alors qu'il existe i ou j tels que $p_{1,1}$ ne divise pas $p_{i,1}$ ou $p_{1,j}$. Dans ce cas, considérons les opérations suivantes :

(L) si c'est $p_{i,1}$, alors on fait une division euclidienne de $p_{i,1}$ par $p_{1,1}$: $p_{i,1} = qp_{1,1} + r$ et on remplace la ligne L_i par $L_i - qL_1$ puis on réordonne les lignes et les colonnes pour que $N(P') = N(p'_{1,1})$;

(C) si c'est $p_{1,j}$, alors on fait une division euclidienne de $p_{1,j}$ par $p_{1,1}$: $p_{1,j} = qp_{1,1} + r$ et on remplace la colonne C_j par $C_j - qC_1$ puis on réordonne les lignes et les colonnes pour que $N(P') = N(p'_{1,1})$.

A chaque fois que l'on fait l'une des opérations ci-dessus, on remplace la matrice P par une matrice P' telle que $N(P') \leq N(P) - 1$ ce qui fait qu'après au plus $N(P)$ opérations, on se retrouve forcément avec une matrice qui a la propriété que $p_{1,1}$ divise tous les éléments de la ligne L_1 et de la colonne C_1. Quitte à remplacer L_i par $L_i - (p_{i,1}/p_{1,1})L_1$ et C_j par $C_j - (p_{1,j}/p_{1,1})C_1$, on est alors dans la situation où P est de la forme :

$$\begin{pmatrix} p_{1,1} & 0 \\ 0 & Q \end{pmatrix}.$$

S'il existe i et j tels que $p_{1,1}$ ne divise pas $q_{i,j}$, alors on remplace L_1 par $L_1 + L_i$ et on recommence les opérations (L) et (C) ci-dessus, chacune étant forcée de faire baisser $N(P)$ d'au moins 1. On finit donc par arriver dans la situation où P est de la forme :

$$\begin{pmatrix} p_{1,1} & 0 \\ 0 & Q \end{pmatrix}.$$

avec $p_{1,1} \mid Q$ ce qui permet de démontrer le théorème par récurrence en l'appliquant à la matrice $Q/p_{1,1}$. □

Nous verrons plus loin que les idéaux (d_1), $(d_2), \ldots, (d_s)$ sont déterminés par le module quotient M/N. Ces idéaux s'appellent les *facteurs invariants* de M/N. Si l'anneau A a la propriété que pour toute matrice $P \in \mathrm{M}_{r\times s}(A)$, il existe $X \in \mathrm{GL}_r(A)$ et $Y \in \mathrm{GL}_s(A)$ telles que XPY a tous ses termes nuls sauf peut-être ses s premiers termes diagonaux, et que ceux-ci satisfont la condition (2), alors on dit que A est un *anneau à diviseurs élémentaires*. Dans un tel anneau, tout idéal de type fini est nécessairement principal : c'est un *anneau de Bézout*. Réciproquement, on conjecture que si A est un anneau intègre de Bézout, alors A est un anneau à diviseurs élémentaires. Un exemple d'un tel anneau qui n'est pas principal est celui des fonctions holomorphes sur le disque unité ouvert.

Remarquons pour terminer que la démonstration du théorème 2.2 fournit une classification des matrices à coefficients dans un anneau principal A à équivalence près. Une matrice dont tous les termes sont nuls sauf les s premiers termes diagonaux $d_1, \ldots, d_s$ et telle que $d_1 \mid \cdots \mid d_s$ est dite être en *forme normale* et on dit alors aussi que les (d_i) sont les facteurs invariants de la matrice.

2.2. Modules de type fini sur un anneau principal. — Commençons par appliquer directement le théorème 2.2.

Proposition 2.3. — *Si A est un anneau principal, et si M est un A-module de type fini, alors il existe $n \geq 0$ et des éléments non nuls $e_1, \ldots, e_m$ de $A \setminus A^\times$ tels que $e_1 \mid \cdots \mid e_m$ et $M \simeq A^n \oplus (\oplus_{i=1}^m A/e_iA)$.*

Démonstration. — Si M est de type fini, il existe un morphisme surjectif $f : A^r \to M$ et on note $N = \ker(f)$. Par le théorème 2.1, N est libre de rang $s \leq r$ et la proposition suit alors du théorème 2.2 appliqué à $N \subset A^r$, étant donné que si $d_i \in A^\times$, alors $d_i A = A$. □

On voit, en gardant les notations de la proposition 2.3, que l'on a $M_{\text{tor}} \simeq \oplus_{i=1}^m A/d_i A$ et $M/M_{\text{tor}} \simeq A^n$; en particulier n est bien défini et ne dépend que de M. On dit parfois abusivement que n est le rang de M. Si M est sans torsion, alors $M \simeq A^n$ et donc sur un anneau principal, les modules sans torsion et de type fini sont nécessairement libres.

Proposition 2.4. — *Si A est un anneau principal, et si $d_1, \ldots, d_m$ et $e_1, \ldots, e_n$ sont des éléments non nuls de $A \setminus A^\times$ tels que $d_1 \mid \cdots \mid d_m$ et $e_1 \mid \cdots \mid e_n$ et $\oplus_{i=1}^m A/d_i A \simeq \oplus_{j=1}^n A/e_j A$, alors $m = n$ et $(d_i) = (e_i)$ pour tout i.*

Démonstration. — Comme A est un anneau principal, les éléments premiers coïncident avec les éléments irréductibles, et de plus si p est premier, alors l'idéal (p) est maximal et donc A/pA est un corps. Si $d \in A \setminus A^\times$, alors $(A/dA)/p(A/dA) = A/(pA + dA)$ qui vaut 0 si p ne divise pas d et A/pA si p divise d.

On en déduit que si p est un élément premier, alors $(\oplus_{i=1}^m A/d_i A)/p(\oplus_{i=1}^m A/d_i A)$ est un A/pA-espace vectoriel dont la dimension est le nombre de d_i qui sont divisibles par p. En particulier, si p divise d_1, alors ce nombre est égal à m et donc m des e_j sont divisbles par p, et $n \geq m$. Par symétrie, on trouve que $m = n$ et donc que p divise aussi tous les e_j. Enfin, si p divise d, alors on a $p(A/dA) \simeq A/(d/p)A$ et en multipliant $\oplus_{i=1}^m A/d_i A \simeq \oplus_{j=1}^n A/e_j A$ par p, on trouve que :

$$\oplus_{i=1}^m A/(d_i/p)A \simeq \oplus_{j=1}^n A/(e_j/p)A,$$

ce qui permet de démontrer la proposition par récurrence sur le nombre de facteurs premiers (avec multiplicité) de $\text{ppcm}(d_m, e_m)$. □

En rassemblant les résultats du paragraphe, on trouve donc le théorème ci-dessous.

Théorème 2.5. — *Si A est un anneau principal et si M est un A-module de type fini, alors :*

1. *il existe $m \geq 0$ et $n \geq 0$ et des éléments non nuls $d_1, \ldots, d_m$ de $A \setminus A^\times$ tels que $d_1 \mid \cdots \mid d_m$ et :*
$$M \simeq A^n \oplus (\oplus_{i=1}^m A/d_i A);$$
2. *les entiers m et n ainsi que les idéaux (d_i) sont déterminés par M.*

Le module A/dA peut lui-même encore être décomposé. Si $d = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est une décomposition de d en facteurs premiers, alors par le théorème des restes, l'application

$A/dA \to \oplus_{j=1}^{r} A/p_j^{\alpha_j} A$ est un isomorphisme. En revanche, $A/p^{\alpha}A$ ne peut plus être décomposé en somme directe de deux sous-A-modules.

Si M est un A-module et si p est un élément premier, on note $M(p)$ la partie p-primaire de M, c'est à dire l'ensemble des $m \in M$ tels qu'il existe $\alpha \geq 1$ vérifiant $p^{\alpha} m = 0$ ce qui fait que $M(p)$ est un sous-module de M. Si $M = A/dA$, alors $M(p_j) = A/p_j^{\alpha_j} A$ et donc $M = \oplus_{j=1}^{r} M(p_j)$. Le théorème 2.5 peut alors être reformulé de la manière suivante.

Théorème 2.6. — *Si A est un anneau principal et si M est un A-module de type fini, alors $M(p) = 0$ pour presque tout élément premier p et :*

1. *il existe $n \geq 0$ tel que $M = A^n \oplus (\oplus_{p \text{ premier}} M(p))$ et pour tout p premier, il existe des entiers $\alpha_1(p) \leq \cdots \alpha_{m(p)}(p)$ tels que $M(p) = \oplus_{i=1}^{m(p)} A/p^{\alpha_i(p)} A$;*
2. *les entiers n et $m(p)$ et $\alpha_i(p)$ sont déterminés par M.*

2.3. Groupes abéliens de type fini et réduction des endomorphismes. — Dans ce paragraphe, nous appliquons le théorème 2.5 au cas de $A = \mathbf{Z}$ (groupes abéliens de type fini) puis au cas de $A = K[X]$ (réduction des endomorphismes).

Commençons par le cas des groupes abéliens de type fini. L'anneau $A = \mathbf{Z}$ est principal, et on a vu qu'un groupe abélien n'est autre qu'un $\mathbf{Z}$-module. Par suite, le théorème 2.5 nous donne le résultat ci-dessous.

Théorème 2.7. — *Si G est un groupe abélien de type fini, alors il existe $m \geq 0$ et $n \geq 0$ et des entiers $d_1, \ldots, d_m \geq 2$ tels que $d_1 \mid \cdots \mid d_m$ et $G \simeq \mathbf{Z}^n \oplus (\oplus_{i=1}^{m} \mathbf{Z}/d_i\mathbf{Z})$, et les entiers m et n et les d_i sont déterminés par G.*

Passons à présent à la réduction des endomorphismes. Soit K un corps et V un K-espace vectoriel de dimension finie et $f : V \to V$ un endomorphisme. On considère V comme un $K[X]$-module en posant $P(X) \cdot v = P(f)(v)$ et V est alors un $K[X]$-module de type fini, qui est de torsion (par exemple par le théorème de Cayley-Hamilton). Les résultats de la section précédente nous disent que $V \simeq \oplus_{i=1}^{n} K[X]/(d_i)$ en tant que $K[X]$-module où $d_1(X) \mid \cdots \mid d_n(X)$. C'est la *décomposition de Frobenius* de V. Chaque espace vectoriel $K[X]/(d_i)$ est cyclique.

Théorème 2.8. — *Si M est la matrice de f dans une base de V, alors on a $V \simeq \oplus_{i=1}^{d} K[X]/(d_i)$ en tant que $K[X]$-module où $d_1(X) \mid \cdots \mid d_d(X)$ sont les facteurs invariants de la matrice $X \cdot \mathrm{Id} - M \in \mathrm{M}_d(K[X])$.*

Démonstration. — Soit $v_1, \ldots, v_d$ une base de V, $M = (m_{i,j})$ la matrice de f dans la base des v_i, W le module libre $\oplus_{i=1}^{d} K[X] w_i$ et N le sous-module de W engendré par

les $n_i = Xw_i - \sum_{j=1}^d m_{j,i}w_j$ pour $1 \leq i \leq d$. Enfin, soit $\pi : W \to V$ l'application $\pi : \sum_{i=1}^d P_i(X) \cdot w_i \mapsto \sum_{i=1}^d P_i(f)(v_i)$.

Montrons que l'application π induit une suite exacte de $K[X]$-modules : $0 \to N \to W \xrightarrow{\pi} V \to 0$. Il faut vérifier que π est surjective et que $\ker(\pi) = N$. Le fait que π est surjective est évident puisque $\pi(w_i) = v_i$ et que les v_i engendrent V. Montrons donc que $\ker(\pi) = N$. Le fait que M est la matrice de f dans la base des v_i revient à dire que $f(v_i) = \sum_{j=1}^d m_{j,i}v_j$ et donc que $\pi(n_i) = 0$ pour tout i ce qui fait que $N \subset \ker(\pi)$. Enfin, si $\sum_{i=1}^d P_i(X) \cdot w_i \in W$, alors il existe $n \in N$ tel que $\sum_{i=1}^d P_i(X) \cdot w_i - n = \sum_{i=1}^d a_i \cdot w_i$ avec $a_i \in K$ et si $\pi(\sum_{i=1}^d P_i(X) \cdot w_i) = 0$, alors $\pi(\sum_{i=1}^d a_i \cdot w_i) = 0$ et donc $a_i = 0$ pour tout i ce qui fait que $\sum_{i=1}^d P_i(X) \cdot w_i \in N$ et donc $\ker(\pi) = N$.

Comme $V = M/N$, on voit que N est libre de rang d, et donc de base $n_1, \ldots, n_d$. Le théorème 2.2 implique alors notre résultat. □

Dans les notations du théorème, on voit que $d_1(X) \times \cdots \times d_d(X)$ est le polynôme caractéristique de f. Son polynôme minimal est $d_d(X)$.

Corollaire 2.9. — *Si K est un corps et A, $B \in \mathrm{M}_d(K)$, alors A et B sont semblables si et seulement si $A - X \cdot \mathrm{Id}$ et $B - X \cdot \mathrm{Id}$ sont équivalentes dans $\mathrm{M}_d(K[X])$.*

La décomposition en parties p-primaires (théorème 2.6) nous permet de retrouver la décomposition de Jordan. Supposons que K est algébriquement clos. Les éléments premiers de $K[X]$ sont les polynômes irréductibles, qui sont de degré 1 puisque K est algébriquement clos, et tout polynôme premier est donc de la forme $X - \lambda$ avec $\lambda \in K$. Si $\alpha \geq 1$, alors le $K[X]$-module $K[X]/(X-\lambda)^\alpha$ est un K-espace vectoriel de dimension α dont une base est donnée par $\overline{(X-\lambda)}^{\alpha-1}, \overline{(X-\lambda)}^{\alpha-2}, \ldots, \overline{1}$ et dans cette base, la matrice de la multiplication par X est donnée par :

$$\begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}.$$

Le théorème 2.6 nous dit alors que V est une somme directe de V_λ où chaque $V_\lambda = V(X-\lambda)$ est de la forme $\oplus_{i=1}^m K[X]/(X-\lambda)^{\alpha_i}$, c'est-à-dire qu'il existe une base de V dans laquelle la matrice de f est diagonale par blocs, chaque bloc étant un bloc de Jordan. On dit que $\mathrm{Mat}(f)$ est sous *forme de Jordan*. On a donc montré le théorème ci-dessous.

Théorème 2.10. — *Si K est algébriquement clos, alors tout endomorphisme d'un K-espace vectoriel de dimension finie admet une décomposition de Jordan.*

2.4. Modules projectifs. — Rappelons que l'on note $\mathrm{Hom}_A(M,N)$ l'ensemble des applications A-linéaires de M dans N, et que $\mathrm{Hom}_A(M,N)$ est lui-même un A-module. Si l'on a $f : N_1 \to N_2$, on en déduit $f_* : \mathrm{Hom}_A(M,N_1) \to \mathrm{Hom}_A(M,N_2)$, donnée par $f_* : h \mapsto f \circ h$. Rappelons le (1) de la proposition 1.1.

Proposition 2.11. — *La suite* $0 \to N' \to N \to N''$ *est exacte si et seulement si la suite* $0 \to \mathrm{Hom}_A(M,N') \to \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N'')$ *est exacte pour tout* A*-module* M*.*

En revanche, $N \to N''$ surjective n'implique pas forcément que $\mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N'')$ est surjective. Si $N \to N''$ est surjective, alors $\mathrm{Hom}_A(A,N) \to \mathrm{Hom}_A(A,N'')$ est surjective. On en déduit que si L est un A-module libre, alors $\mathrm{Hom}_A(L,N) \to \mathrm{Hom}_A(L,N'')$ est surjective.

Définition 2.12. — On dit qu'un A-module P est *projectif* si $\mathrm{Hom}_A(P,N) \to \mathrm{Hom}_A(P,N'')$ est surjective pour toute application surjective $N \to N''$.

Disons qu'une suite exacte $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ est *scindée* s'il existe $r : P \to N$ telle que $g \circ r = \mathrm{Id}_P$. La suite est donc scindée si et seulement s'il existe $P' \subset N$ tel que $N = f(M) \oplus P'$.

Théorème 2.13. — *Pour un* A*-module* P*, les conditions suivantes sont équivalentes.*

1. P *est projectif ;*
2. *Toute suite exacte* $0 \to M \to N \to P \to 0$ *est scindée ;*
3. *Il existe un* A*-module* R *tel que* $P \oplus R$ *est libre.*

Démonstration. — Montrons que (1) implique (2). Comme P est projectif, $\mathrm{Hom}_A(P,N) \to \mathrm{Hom}_A(P,P)$ est surjectif et Id_P se relève donc en $r : P \to N$, ce qui donne un scindage.

Montrons que (2) implique (3). Le module P est le quotient d'un module libre L, ce qui donne lieu à une suite exacte $0 \to M \to L \to P \to 0$. On a alors $L = f(M) \oplus r(P)$ et on peut donc prendre $R = f(M)$.

Enfin s'il existe un A-module R tel que $L = P \oplus R$ est libre, et si l'on a une application surjective $N \to N''$, alors $\mathrm{Hom}_A(L,N) \to \mathrm{Hom}_A(L,N'')$ est surjective et donc $\mathrm{Hom}_A(P,N) \to \mathrm{Hom}_A(P,N'')$ l'est aussi. □

Remarque 2.14. — Si P est projectif de type fini, alors dans le (3) on peut prendre L de type fini tel que $P \oplus R = L$ est libre (et donc de rang fini).

Si A est un anneau principal, tout sous-module d'un module libre de type fini est libre de type fini et donc tout module projectif de type fini sur A est en fait libre. Il existe

d'autres types d'anneaux ayant cette propriété, par exemple $K[X_1, \ldots, X_n]$ où K est un corps (théorème de Quillen-Suslin).

Exemple 2.15. — Voici quelques exemples de modules projectifs non libres.

1. $\mathbf{Z}/6\mathbf{Z} = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ et donc $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$ sont projectifs sur $\mathbf{Z}/6\mathbf{Z}$.
2. Plus généralement, si A et B sont deux anneaux et si M est un A-module libre et N est un B-module libre, alors $M \times N$ est un $A \times B$-module projectif, qui est libre si et seulement si M et N ont même rang.
3. Si $A = \mathbf{Z}[\sqrt{-5}]$ et $P = (3, 1 + \sqrt{-5})$ et $R = (3, 1 - \sqrt{-5})$, alors $P \oplus R \simeq A^2$ (on a $0 \to P \cap R \to P \oplus R \to P + R \to 0$ et $P + R = A$ et $P \cap R = 3A$) mais P n'est pas libre (écrire $3 = (a + b\sqrt{-5})x$ et $1 + \sqrt{-5} = (a + b\sqrt{-5})y$ et regarder les normes).
4. Si X est un espace (algébrique, topologique, ...), on a une correspondance entre les fibrés vectoriels sur X et les modules projectifs de type fini sur $C(X)$.

   Par exemple, le fibré tangent de la sphère de dimension n correspond à la situation suivante : soit $A = C^0(S^n, \mathbf{R})$ et $e = (x_0, \ldots, x_n)$ et $P = \{v \in A^{n+1}$ tels que $\langle v, e\rangle = 0\}$. On a $P \oplus Ae = A^{n+1}$ car $\langle e, e\rangle = 1$, et donc P est projectif. Supposons que $P = Av_1 \oplus \cdots \oplus Av_n$. Si $s \in S^n$, alors $\mathbf{R}^{n+1} = \mathbf{R} \cdot v_1(s) + \cdots + \mathbf{R} \cdot v_n(s) + \mathbf{R} \cdot e(s)$ et donc $v_1(s) \neq 0$. Le vecteur v_1 est donc tangent à la sphère et non-nul partout sur celle-ci. Si n est pair, cela contredit le théorème de la boule chevelue. En fait, P n'est libre que si $n = 1$, 3 ou 7 (dimensions qui viennent des nombres complexes, des quaternions et des octonions).

3. Produits tensoriels

La notion de produit tensoriel de modules généralise celle de produit tensoriel d'espaces vectoriels de dimension finie.

3.1. Produits tensoriels de modules. —

Soient M et N deux A-modules.

Théorème 3.1. — *Il existe un A-module $M \otimes N$ et une application bilinéaire $t : M \times N \to M \otimes N$, telle que si P est un A-module, alors $f \mapsto f \circ t$ induit une bijection* $\mathrm{Hom}(M \otimes N, P) \to \mathrm{Bil}(M \times N, P)$.

Le module $M \otimes N$ est caractérisé à isomorphisme près par la propriété ci-dessus.

Démonstration. — Soit L le A-module libre dont une base est l'ensemble des $[m, n]$ avec $m \in M$ et $n \in N$, et soit R le sous-module engendré par les éléments de la forme $[a_1m_1 + a_2m_2, n] - a_1[m_1, n] - a_2[m_2, n]$ et par ceux de la forme $[m, a_1n_1 + a_2n_2] - a_1[m, n_1] -$

$a_2[m, n_2]$. On pose alors $M \otimes N = L/R$ et on note $m \otimes n$ l'image de $[m, n]$ dans $M \otimes N$. Notons que si $m = \sum_{i=1}^{r} x_i m_i \in M$ et $n = \sum_{j=1}^{s} y_j n_j \in N$, alors $m \otimes n = \sum_{i=1}^{r} \sum_{j=1}^{s} x_i y_j \cdot m_i \otimes n_j$. Soit $t : M \times N \to M \otimes N$ l'application $t(m, n) = m \otimes n$.

Le fait que t est bilinéaire est clair. Si $f \in \mathrm{Hom}(M \otimes N, P)$ et si $f \circ t = 0$, alors $f(m \otimes n) = 0$ pour tout m, n et donc $f = 0$ ce qui fait que $f \mapsto f \circ t$ est injective. Montrons qu'elle est surjective. Si $g \in \mathrm{Bil}(M \times N, P)$, soit $f : L \to P$ donnée par $f([m, n]) = g(m, n)$. Comme g est bilinéaire, $g = 0$ sur R et f se factorise par $f : M \otimes N \to P$. On voit alors que $g = f \circ t$.

Soit (X, u) un autre couple, avec $u : M \times N \to X$, tel que $f \mapsto f \circ u$ induit une bijection $\mathrm{Hom}(X, P) \to \mathrm{Bil}(M \times N, P)$. En appliquant la propriété universelle à t, on trouve $f : X \to M \otimes N$ tel que $t = f \circ u$. Réciproquement, on trouve $g : M \otimes N \to X$ tel que $u = g \circ t$ et donc $t = (f \circ g) \circ t$ et $u = (g \circ f) \circ u$. La bijection $\mathrm{Hom}(X, X) \to \mathrm{Bil}(M \times N, X)$ envoie $g \circ f$ sur $(g \circ f) \circ u = u$ et donc $g \circ f = \mathrm{Id}_X$. De même, $f \circ g = \mathrm{Id}_{M \otimes N}$.

Le module X est donc isomorphe à $M \otimes N$ via un isomorphisme qui envoie u sur t. □

La construction de $M \otimes N$ montre que si M est engendré par une famille $\{m_i\}_{i \in I}$ et N par une famille $\{n_j\}_{j \in J}$, alors $M \otimes N$ est engendré par $\{m_i \otimes n_j\}_{I \times J}$. Si M et N sont de type fini, $M \otimes N$ l'est donc aussi.

En général, tout élément de $M \otimes N$ est somme de tenseurs simples et le rang d'un élément x de $M \otimes N$ est le plus petit nombre r tel que x est somme de r tenseurs simples.

Proposition 3.2. — *Le produit tensoriel a les propriétés suivantes.*

1. $M \otimes N \simeq N \otimes M$
2. $A \otimes M = M$
3. $(\oplus_{i \in I} M_i) \otimes N = \oplus_{i \in I} (M_i \otimes N)$
4. $\mathrm{Hom}(M \otimes N, P) = \mathrm{Hom}(M, \mathrm{Hom}(N, P))$
5. $(M \otimes N) \otimes Q = M \otimes (N \otimes Q)$

Démonstration. — Étant donnée la proposition 3.1, cela résulte des isomorphismes :

1. $M \times N \simeq N \times M$
2. $\mathrm{Bil}(A \times M, P) = \mathrm{Hom}(M, P)$ (via $f \mapsto [m \mapsto f(1, m)]$)
3. $\mathrm{Bil}((\oplus_{i \in I} M_i) \times N, P) = \prod_{i \in I} \mathrm{Bil}(M_i \times N, P)$
4. $\mathrm{Bil}(M \times N, P) = \mathrm{Hom}(M, \mathrm{Hom}(N, P))$
5. $\mathrm{Bil}((M \otimes N) \times Q, P) = \mathrm{Mult}(M \times N \times Q, P) = \mathrm{Bil}(M \times (N \otimes Q), P)$

Ici Mult désigne le module des applications multilinéaires. □

Le (5) implique qu'on peut écrire $M \otimes N \otimes Q$, et que ce module a une propriété universelle vis à vis des applications multilinéaires sur $M \times N \times Q$.

On déduit de la proposition que si M et N sont deux A-modules libres, de bases $\{m_i\}_{i\in I}$ et $\{n_j\}_{j\in J}$, alors $M \otimes N$ est libre, de base $\{m_i \otimes n_j\}_{I\times J}$. Plus généralement, si M est quelconque et N est libre de base $\{n_j\}_{j\in J}$, alors tout élément de $M \otimes N$ s'écrit d'une et d'une seule manière sous la forme $\sum_{j\in J} m_j \otimes n_j$ où les $m_j \in M$ sont presque tous nuls.

Corollaire 3.3. — *Si M et N sont deux A-modules projectifs, alors $M\otimes N$ est projectif.*

Démonstration. — Développer $(M \oplus M') \otimes (N \oplus N')$. □

Proposition 3.4. — *Si $M' \to M \to M'' \to 0$ est une suite exacte, alors $M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ est exacte.*

Démonstration. — Soit P un A-module. En appliquant $\mathrm{Hom}(\cdot, P)$ à la suite $M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$, et en appliquant le (4) de la proposition 3.2, on trouve $0 \to \mathrm{Hom}(M'', \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M', \mathrm{Hom}(N, P))$. Cette suite est exacte si $M' \to M \to M'' \to 0$ l'est par la proposition 1.1, et on conclut en réappliquant la proposition 1.1. □

Corollaire 3.5. — *Si I est un idéal de A, alors $A/I \otimes M = M/IM$.*

Démonstration. — Si on tensorise la suite exacte $I \to A \to A/I \to 0$ par M, on trouve $I \otimes M \to M \to A/I \otimes M \to 0$ et l'image de $I \otimes M$ dans M est IM. □

Attention au fait que $I \otimes M$ n'est pas égal à IM en général. En appliquant le corollaire 3.5 à $M = A/J$, on trouve que $A/I \otimes A/J = A/(I + J)$.

Corollaire 3.6. — *Si l'on a deux suites exactes $K \xrightarrow{i} M \to P \to 0$ et $L \xrightarrow{j} N \to Q \to 0$, alors on a une suite exacte $((K \otimes N) \oplus (M \otimes L)) \xrightarrow{i\otimes \mathrm{Id} + \mathrm{Id} \otimes j} M \otimes N \to P \otimes Q \to 0$.*

Démonstration. — La proposition montre que $M/K \otimes N/L = (M \otimes N/L)/\operatorname{im}(K \otimes N/L)$. De même, $M \otimes N/L = M \otimes N/\operatorname{im}(M \otimes L)$. On a donc

$$M/K \otimes N/L = \frac{M \otimes N/L}{\operatorname{im}(K \otimes N/L)} = \frac{M \otimes N}{\operatorname{im}(M \otimes L) + \operatorname{im}(K \otimes N)}.$$

□

Notons que si $M' \to M$ est injective, le morphisme $M' \otimes N \to M \otimes N$ n'est pas injectif en général. Par exemple si $n \geq 2$, alors $n\mathbf{Z} \subset \mathbf{Z}$ et $n\mathbf{Z} \otimes \mathbf{Z}/n\mathbf{Z}$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ par le corollaire 3.5, mais son image dans $\mathbf{Z} \otimes \mathbf{Z}/n\mathbf{Z}$ est nulle. On dit qu'un module P est *plat* si pour tout morphisme injectif $M' \to M$, le morphisme $M' \otimes P \to M \otimes P$ est

injectif. Nous étudierons les modules plats plus tard, mais mentionnons tout de même le résultat suivant.

Proposition 3.7. — *Si P est un A-module projectif, alors P est plat.*

Démonstration. — Il existe Q tel que $L = P \oplus Q$ est libre. Si $M' \to M$ est injectif, le morphisme $M' \otimes L \to M \otimes L$ est injectif et donc $M' \otimes P \to M \otimes P$ est injectif. □

3.2. Produits tensoriels et homomorphismes. — Si $f \in \mathrm{Hom}(M_1, M_2)$ et $g \in \mathrm{Hom}(N_1, N_2)$, on a $f \otimes g \in \mathrm{Hom}(M_1 \otimes N_1, M_2 \otimes N_2)$. On a donc une application $h : \mathrm{Hom}(M_1, M_2) \otimes \mathrm{Hom}(N_1, N_2) \to \mathrm{Hom}(M_1 \otimes N_1, M_2 \otimes N_2)$. Cette application n'est, en général, ni injective ni surjective.

Proposition 3.8. — *Si M_1 et N_1 sont libres de rang fini, ou encore si M_1 et M_2 sont libres de rang fini, alors h est un isomorphisme.*

Démonstration. — En utilisant la commutativité de $\otimes$ et $\oplus$, on se ramène au cas où $M_1 = N_1 = A$ ou bien $M_1 = M_2 = A$. Dans les deux cas, la proposition est évidente. □

Si M_1, M_2, N_1 et N_2 sont libres de rang fini et qu'on en choisit des bases, alors on dispose de $\mathrm{Mat}(f)$ et de $\mathrm{Mat}(g)$. Si l'on pose $A = \mathrm{Mat}(f)$ et $B = \mathrm{Mat}(g)$, alors la matrice de $f \otimes g$ dans des bases appropriées est :

$$\mathrm{Mat}(f \otimes g) = A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots \\ a_{2,1}B & \ddots & \\ \vdots & & \end{pmatrix}.$$

En posant $M_1 = M$ et $M_2 = A$ et $N_1 = A$ et $N_2 = N$, on trouve une application $M^* \otimes N \to \mathrm{Hom}(M, N)$. La proposition 3.8 implique que cette application est un isomorphisme si M est libre de type fini. Si $A = K$ est un corps et si V et W sont deux K-espaces vectoriels de dimension finie, on a donc $V^* \otimes W = \mathrm{Hom}(V, W)$.

Proposition 3.9. — *Si $f \in \mathrm{Hom}(V, W)$, alors le rang de f en tant qu'application linéaire est le rang du tenseur correspondant dans $V^* \otimes W$.*

Démonstration. — Soit $t = \sum_{i=1}^r x_i \otimes w_i$ un tenseur correspondant à f. On a $f(v) = \sum_{i=1}^r x_i(v) w_i$ et donc l'image de f est incluse dans $\mathrm{Vect}(w_1, \ldots, w_r)$: ceci montre que le rang de f est $\leq r$. Réciproquement, soit $w_1, \ldots, w_r$ une base de l'image de f et $x_1, \ldots, x_r$ les formes linéaires définies par $f(v) = \sum_{i=1}^r x_i(v) w_i$. On peut prendre $t = \sum_{i=1}^r x_i \otimes w_i$ et donc $r \leq$ le rang de f. □

Proposition 3.10. — *Si M_1 et N_1 sont projectifs de type fini, ou encore si M_1 et M_2 sont projectifs de type fini, alors h est un isomorphisme.*

Démonstration. — Cela suit de la proposition 3.8. □

Dans le cas où $M = N$ et M est projectif de type fini, on a donc un isomorphisme $M^* \otimes M \to \mathrm{End}(M)$. On a un application $\mathrm{Tr} : M^* \otimes M \to A$, induite par $(f, m) \mapsto f(m)$ de $M^* \times M \to A$, et donc donnée par $\sum f_i \otimes m_i \mapsto \sum f_i(m_i)$. On en déduit $\mathrm{Tr} : \mathrm{End}(M) \to A$, c'est la trace des endomorphismes d'un module projectif de type fini. Si M est libre de rang fini, on retrouve la trace habituelle.

3.3. Extension des scalaires. — Soit B un anneau, muni d'un morphisme $f : A \to B$. Si N est un B-module, alors c'est un A-module avec la recette $a \cdot n = f(a)n$. C'est la restriction des scalaires.

Si M est un A-module, on peut former $B \otimes M$ et c'est un B-module, qu'on appelle l'extension des scalaires de M. Par exemple, si X est un espace topologique et si $f : X \to \mathbf{C}$ est continue, on peut décomposer f en parties réelles et imaginaires et donc $C^0(X, \mathbf{C}) = \mathbf{C} \otimes_{\mathbf{R}} C^0(X, \mathbf{R})$.

Proposition 3.11. — *Si M est un A-module et N un B-module, alors* $\mathrm{Hom}_A(M, N)$ *est un B-module, et on a un isomorphisme de B-modules* $\mathrm{Hom}_A(M, N) = \mathrm{Hom}_B(B \otimes M, N)$.

Démonstration. — Si $h \in \mathrm{Hom}_A(M, N)$, soit $\tilde{h} : B \otimes M \to N$ l'application définie par $\tilde{h}(b \otimes m) = bh(m)$. Si $g \in \mathrm{Hom}_B(B \otimes M, N)$, soit $\overline{g} : M \to N$ défini par $\overline{g}(m) = g(1 \otimes m)$. Les deux constructions ci-dessus sont inverses l'une de l'autre. □

Proposition 3.12. — *Si M est un A-module et N un B-module, alors on a un isomorphisme de B-modules $M \otimes_A N = (M \otimes_A B) \otimes_B N$.*

Démonstration. — On définit $u : M \otimes_A N \to (M \otimes_A B) \otimes_B N$ comme l'élément correspondant à celui de $\mathrm{Bil}_A(M \times N, (M \otimes_A B) \otimes_B N)$ donné par $(m, n) \mapsto (m \otimes 1) \otimes n$.

Si $n \in N$, alors on a une application $B \to N$ donnée par $b \mapsto bn$ et en tensorisant par M, on trouve une application $M \otimes_A B \to M \otimes_A N$, donnée par $m \otimes b \mapsto m \otimes bn$. L'application qui en résulte de $(M \otimes_A B) \times N \to M \otimes_A N$, donnée par $(m \otimes b, n) \mapsto m \otimes bn$, est B-bilinéaire et donne donc lieu à $v : (M \otimes_A B) \otimes_B N \to M \otimes_A N$. On vérifie que $uv = vu = \mathrm{Id}$. □

Corollaire 3.13. — *Si M est un A-module plat, alors $B \otimes_A M$ est un B-module plat.*

3.4. Produits tensoriels d'algèbres. — Si M et N sont deux A-algèbres, alors $M \otimes N$ est muni d'une structure d'algèbre par $(m_1 \otimes n_1) \cdot (m_2 \otimes n_2) = m_1 m_2 \otimes n_1 n_2$. Plus précisément, l'application $M \times N \times M \times N \to M \otimes N$ donnée par $(m_1, n_1, m_2, n_2) \mapsto m_1 m_2 \otimes n_1 n_2$ est 4-linéaire et donne lieu à une application bilinéaire $(M \otimes N) \times (M \otimes N) \to (M \otimes N)$ qui est la multiplication.

Par exemple, $A[X]$ est un A-module libre engendré par les X^i avec $i \geq 0$ et donc $B \otimes A[X] = B[X]$ et $A[X] \otimes A[Y] = A[X, Y]$. Plus généralement,

$$A[X_1, \ldots, X_r] \otimes A[Y_1, \ldots, Y_s] = A[X_1, \ldots, X_r, Y_1, \ldots, Y_s].$$

Enfin si $P_1, \ldots, P_k \in A[X_1, \ldots, X_r]$ et $Q_1, \ldots, Q_\ell \in A[Y_1, \ldots, Y_s]$, alors (par exemple par le corollaire 3.6)

$$A[X_1, \ldots, X_r]/(P_1, \ldots, P_k) \otimes A[Y_1, \ldots, Y_s]/(Q_1, \ldots, Q_\ell) \\ = A[X_1, \ldots, X_r, Y_1, \ldots, Y_s]/(P_1, \ldots, P_k, Q_1, \ldots, Q_\ell)$$

Si X et Y sont deux espaces métriques, alors on a une application

$$m : C^0(X, \mathbf{R}) \otimes_{\mathbf{R}} C^0(Y, \mathbf{R}) \to C^0(X \times Y, \mathbf{R}),$$

provenant de $(f \otimes g)(x, y) = f(x)g(y)$.

Proposition 3.14. — *Cette application est injective, et si X et Y sont compacts, alors son image est dense.*

Démonstration. — Soit $h = \sum_{i=1}^r f_i \otimes g_i$ tel que $h \neq 0$ et $m(h) = 0$ sur $X \times Y$, avec r minimal (en particulier, $g_i \neq 0$ pour tout i). La fonction $x \mapsto \sum_{i=1}^r f_i(x) g_i(y)$ est nulle sur X pour tout y. Comme il existe y tel que $g_1(y) \neq 0$, la fonction f_1 est combinaison linéaire des autres f_i. Si r est minimal, on a donc $r = 1$ et l'injectivité de m est claire.

Montrons que l'image de m est dense si X et Y sont compacts. Par le théorème de Stone, il suffit de montrer que l'image de m sépare les points. Si (x_1, y_1) et (x_2, y_2) sont deux points de $X \times Y$, supposons que $x_1 \neq x_2$ et soit $f \in C^0(X, \mathbf{R})$ telle que $f(x_1) \neq f(x_2)$. On a alors $(f \otimes 1)(x_1, y_1) \neq (f \otimes 1)(x_2, y_2)$. □

Regardons de plus près le produit tensoriel de deux corps, dans le cas où $A = F$ est un corps de caractéristique 0. Rappelons le théorème de l'élément primitif : si L est une extension finie de F, alors il existe $\alpha \in L$ tel que $L = F(\alpha)$. Comme F est de caractéristique 0, le polynôme $P_{\min,\alpha}(X)$ est à racines simples. On a $L = F[\alpha] = F[X]/P_{\min,\alpha}(X)$. Si K et L sont deux extensions finies de F, alors $K \otimes L = K \otimes F[X]/P_{\min,\alpha}(X) = K[X]/P_{\min,\alpha}(X)$. Soit $P_{\min,\alpha}(X) = P_1(X) \cdots P_r(X)$ la factorisation de $P_{\min,\alpha}(X)$ en produit de facteurs irréductibles dans $K[X]$. L'anneau $K_i = K[X]/P_i(X)$ est un corps, et par le théorème

des restes, on a $K \otimes L = K_1 \times \cdots \times K_r$. Par exemple, $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} = \mathbf{C} \times \mathbf{C}$ ou encore $\mathbf{Q}(\sqrt{2}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

3.5. Platitude. — Rappelons qu'on dit qu'un A-module P est plat si pour tout morphisme injectif $M' \to M$, le morphisme $M' \otimes P \to M \otimes P$ est injectif. Nous avons vu (proposition 3.7) qu'un module projectif est plat, et (corollaire 3.13) que si P est un A-module plat, alors $B \otimes_A P$ est un B-module plat. On voit que si P_1 et P_2 sont plats, alors $P_1 \oplus P_2$ et $P_1 \otimes P_2$ le sont aussi. Si P est plat et si I est un idéal de A, alors $I \otimes P \to IP$ est un isomorphisme. Si $a \in A$ n'est pas un diviseur de 0, alors $0 \to A \xrightarrow{\cdot a} A$ et donc $0 \to P \xrightarrow{\cdot a} P$. Un module plat sur un anneau intègre est donc sans torsion.

Théorème 3.15. — *Un module P est plat si et seulement si $I \otimes P \to P$ est injective pour tout idéal I de A.*

Afin de démontrer ce théorème nous avons besoin de quelques lemmes préparatoires. Si M et P sont deux A-modules, disons que P est plat pour M si pour tout sous-module $M' \subset M$, l'application $M' \otimes P \to M \otimes P$ est injective. Un module P est donc plat s'il est plat pour tout module M. Le théorème dit que si P est plat pour A, alors il est plat.

Lemme 3.16. — *Si P est plat pour M et si N est un quotient de M, alors P est plat pour N.*

Démonstration. — Écrivons $0 \to K \to M \xrightarrow{p} N \to 0$. Soit N' un sous-module de N, et posons $M' = p^{-1}(N')$. On a donc un diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0, \end{array}$$

et en tensorisant par P, on trouve un diagramme

$$\begin{array}{ccccccccc} P \otimes K & \longrightarrow & P \otimes M' & \longrightarrow & P \otimes N' & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ P \otimes K & \longrightarrow & P \otimes M & \longrightarrow & P \otimes N & \longrightarrow & 0. \end{array}$$

La flèche de gauche est une bijection et celle du milieu est injective. Une chasse au diagramme montre que celle de droite est nécessairement injective. □

Lemme 3.17. — *Si P est plat pour M_1 et M_2, alors P est plat pour $M_1 \oplus M_2$.*

Démonstration. — Soit M' un sous-module de $M_1 \oplus M_2$ et $M'_1 = M' \cap M_1$ et M'_2 l'image de M' dans M_2. On trouve un diagramme

$$\begin{array}{ccccccccc} & & P \otimes M'_1 & \longrightarrow & P \otimes M' & \longrightarrow & P \otimes M'_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P \otimes M_1 & \longrightarrow & P \otimes (M_1 \oplus M_2) & \longrightarrow & P \otimes M_2 & \longrightarrow & 0. \end{array}$$

Les flèches verticales de gauche et de droite sont injectives. On en déduit que celle du milieu l'est aussi. □

Lemme 3.18. — *Si P est plat pour chaque module d'une famille $\{M_i\}_{i\in I}$, alors P est plat pour $\oplus_{i\in I} M_i$.*

Démonstration. — Le lemme 3.17 implique ce résultat si I est une famille finie.

Soit M' un sous-module de $\oplus_{i\in I} M_i$ tel que $P\otimes M' \to P\otimes(\oplus_{i\in I} M_i)$ n'est pas injectif. Si $x' \in P \otimes M'$ est dans le noyau de cette application, écrivons $x' = p_1 \otimes m_1 + \cdots + p_r \otimes m_r$. Soit M'' le module engendré par les m_k et $x'' = p_1 \otimes m_1 + \cdots + p_r \otimes m_r \in P \otimes M''$. Le module M'' est de type fini et il existe donc $J \subset I$ fini tel que $M'' \subset \oplus_{i\in J} M_i$.

Comme $\oplus_{i\in J} M_i$ est un facteur direct de $\oplus_{i\in I} M_i$, l'application $P \otimes (\oplus_{i\in J} M_i) \to P \otimes (\oplus_{i\in I} M_i)$ est injective. L'application $P \otimes M'' \to P \otimes (\oplus_{i\in I} M_i)$ est donc injective. Si l'image de x'' est nulle, c'est que $x'' = 0$ et donc $x' = 0$. □

Démonstration du théorème 3.15. — Soit M un A-module. Montrons que P est plat pour M. On peut écrire M comme quotient d'un module libre $\oplus_{i\in I} A$. Par le lemme 3.18, P est plat pour $\oplus_{i\in I} A$. Par le lemme 3.16, P est donc plat pour M.

Comme P est plat pour tout module M, il est plat. □

Si M est un A-module, une *relation* dans M est une équation $f_1 m_1 + \cdots + f_r m_r = 0$ avec $f_i \in A$ et $m_i \in M$. On dit que la relation est *triviale* s'il existe des $a_{ij} \in A$ pour $1 \leq i \leq r$ et $1 \leq j \leq s$ des et $y_1, \ldots, y_s \in M$ tels que $m_i = a_{i1} y_1 + \cdots + a_{is} y_s$ pour tout i et $f_1 a_{1j} + \cdots + f_r a_{rj} = 0$ pour tout j.

Par exemple, si $A = K[X, Y]$, la relation $X \cdot Y - Y \cdot X = 0$ est triviale dans A mais pas dans $M = (X, Y)$.

Proposition 3.19. — *Le module M est plat si et seulement si toute relation dans M est triviale.*

Démonstration. — Supposons que toute relation dans M est triviale. Par le théorème 3.15, il suffit de montrer que si I est un idéal de A, alors l'application $I \otimes M \to M$ est

injective. Supposons que $f_1m_1 + \cdots + f_rm_r = 0$ avec $f_i \in I$. C'est une relation dans M, qui est donc triviale. Si $m_i = a_{i1}y_1 + \cdots + a_{is}y_s$, alors

$$\sum_{i=1}^{r} f_i \otimes m_i = \sum_{i=1}^{r} f_i \otimes \sum_{j=1}^{s} a_{ij}y_j = \sum_{j=1}^{s} \left(\sum_{i=1}^{r} a_{ij}f_i \right) \otimes y_j = 0,$$

et donc $I \otimes M \to M$ est injective.

Supposons que M est plat. Soit $f_1m_1 + \cdots + f_rm_r = 0$ une relation et $I = (f_1, \ldots, f_r)$. On a une application $A^r \to I$ donnée par $(a_i) \mapsto \sum a_i f_i$ et donc une suite exacte $0 \to N \to A^r \to I \to 0$. En tensorisant par M, on trouve $0 \to N \otimes M \to M^r \to I \otimes M \to 0$. L'élément $\sum f_i \otimes m_i$ est nul dans $I \otimes M = IM$ et l'image de $(m_1, \ldots, m_r) \in M^r$ dans $I \otimes M$ est donc nulle. Il existe donc un élément $\sum_j (a_{1j}, \ldots, a_{rj}) \otimes y_j$ de $N \otimes M$ dont l'image dans M^r est $(m_1, \ldots, m_r)$, c'est à dire que $m_i = a_{i1}y_1 + \cdots + a_{is}y_s$ pour tout i avec $f_1a_{1j} + \cdots + f_ra_{rj} = 0$ pour tout j. □

3.6. Produits symétriques. — Soit M un A-module, $k \geq 0$, et $T^k(M) = M \otimes \cdots \otimes M$ pris k fois. On a une bijection $\mathrm{Mult}(M^k, P) = \mathrm{Hom}(T^k(M), P)$. On dit qu'une application multilinéaire $f : M^k \to P$ est symétrique si $f(m_1, \ldots, m_k) = f(m_{\sigma(1)}, \ldots, m_{\sigma(k)})$ pour tous $m_1, \ldots, m_k \in M^k$ et tout $\sigma \in \mathfrak{S}_k$. Soit S le sous-module de $T^k(M)$ engendré par les $m_1 \otimes \cdots \otimes m_k - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}$ avec $m_1, \ldots, m_k \in M^k$ et $\sigma \in \mathfrak{S}_k$. On pose $\mathrm{Sym}^k(M) = T^k(M)/S$.

Proposition 3.20. — *On a une bijection* $\mathrm{Mult\,Sym}(M^k, P) = \mathrm{Hom}(\mathrm{Sym}^k(M), P)$.

Démonstration. — On a une bijection $\mathrm{Mult}(M^k, P) = \mathrm{Hom}(T^k(M), P)$, notée $f \mapsto \tilde{f}$, et f est symétrique si et seulement si $\tilde{f}$ est nulle sur S. □

On note $m_1 \cdots m_k$ l'image de $m_1 \otimes \cdots \otimes m_k$ dans $\mathrm{Sym}^k(M)$. L'application $(v, w) \mapsto vw$ donne lieu à une application $\mathrm{Sym}^k(M) \times \mathrm{Sym}^j(M) \to \mathrm{Sym}^{k+j}(M)$ et $\mathrm{Sym}(M) = \oplus_{k \geq 0} \mathrm{Sym}^k(M)$ est alors un anneau, l'algèbre symétrique de M.

Si M est un A-module de type fini engendré par $m_1, \ldots, m_n$, alors $\mathrm{Sym}^k(M)$ est engendré par les $\binom{n+k-1}{k}$ éléments $\{m_1^{a_1} \cdots m_n^{a_n}$ avec $a_1 + \cdots + a_n = k\}$.

Théorème 3.21. — *Si M est un A-module libre de rang n, de base $m_1, \ldots, m_n$, alors* $\mathrm{Sym}^k(M)$ *est libre de rang* $\binom{n+k-1}{k}$, *de base* $\{m_1^{a_1} \cdots m_n^{a_n}$ *avec* $a_1 + \cdots + a_n = k\}$.

Démonstration. — Soit $a = (a_1, \ldots, a_n)$ et $f_a \in \mathrm{Mult}(M^k, A)$ l'application déterminée par $f_a(m_{i_1}, \ldots, m_{i_k}) = 1$ si a_j des indices i valent j pour tout j, et 0 sinon. Cette application est symétrique et $\tilde{f}_a(\sum_b x_b m^b) = x_a$, ce qui fait que la famille des m^b est libre. □

Corollaire 3.22. — *Si M est un A-module libre de rang n, alors l'anneau* $\mathrm{Sym}(M)$ *est isomorphe à $A[X_1, \dots, X_n]$, l'élément $m_1^{a_1} \cdots m_n^{a_n}$ correspondant à $X_1^{a_1} \cdots X_n^{a_n}$.*

3.7. Produits alternés. — On dit qu'une application multilinéaire $f : M^k \to P$ est alternée si $f(m_1, \dots, m_k) = 0$ dès qu'il existe $i \neq j$ avec $m_i = m_j$.

Lemme 3.23. — *Si f est alternée, alors $f(m_1, \dots, m_k) = \varepsilon(\sigma) f(m_{\sigma(1)}, \dots, m_{\sigma(k)})$ pour tous $m_1, \dots, m_k \in M^k$ et tout $\sigma \in \mathfrak{S}_k$.*

Démonstration. — On a $f(*, m_i+m_j, *, m_i+m_j, *) = f(*, m_i, *, m_i, *)+f(*, m_i, *, m_j, *)+ f(*, m_j, *, m_i, *) + f(*, m_j, *, m_j, *)$ et donc $f(*, m_i, *, m_j, *) + f(*, m_j, *, m_i, *) = 0$. Le lemme résulte de ceci et du fait que $\mathfrak{S}_k$ est engendré par les transpositions. □

Si $f \in \mathrm{Mult}(M^k, P)$ est alternée, l'application correspondante $\tilde{f} : T^k(M) \to P$ est alors nulle sur le module L engendré par les $m_1 \otimes \cdots \otimes m_k$ où deux des m_i sont égaux. On définit $\Lambda^k(M) = T^k(M)/L$ et on note $m_1 \wedge \ldots \wedge m_k$ l'élément de $\Lambda^k(M)$ qui est l'image de $m_1 \otimes \cdots \otimes m_k$.

Proposition 3.24. — *On a une bijection* $\mathrm{Mult\,Alt}(M^k, P) = \mathrm{Hom}(\Lambda^k(M), P)$.

Démonstration. — On a une bijection $\mathrm{Mult}(M^k, P) = \mathrm{Hom}(T^k(M), P)$ et celles qui sont alternées à gauche correspondent précisément à celles qui sont nulles à droite sur L. □

Lemme 3.25. — *Si M est engendré par n éléments, alors $\Lambda^k(M) = 0$ dès que $k \geq n+1$.*

Démonstration. — Soit $m_1, \dots, m_n$ qui engendrent M. Tout élément de $T^k(M)$ peut s'écrire comme combinaison linéaire $\sum \lambda_{i_1,\dots,i_k} m_{i_1} \otimes \cdots \otimes m_{i_k}$ et si $k \geq n+1$, alors deux des indices $i_j \in \{1, \dots, n\}$ sont nécessairement égaux et donc $L = T^k(M)$ ce qui fait que $\Lambda^k(M) = 0$. □

Théorème 3.26. — *Si M est libre de rang n, alors $\Lambda^k(M)$ est libre de rang $\binom{n}{k}$.*

Démonstration. — Étant donné le lemme 3.25, on suppose que $k \leq n$. Les éléments de la forme $m_{i_1} \otimes \cdots \otimes m_{i_k}$ forment une base de $T^k(M)$. Si deux des i_j sont égaux, alors l'image de cet élément est nul dans $\Lambda^k(M)$ et sinon on a $m_{\sigma(i_1)} \wedge \cdots \wedge m_{\sigma(i_k)} = \varepsilon(\sigma) m_{i_1} \wedge \cdots \wedge m_{i_k}$ ce qui fait que les éléments de la forme $m_{i_1} \wedge \cdots \wedge m_{i_k}$ avec $i_1 < i_2 < \cdots < i_k$ engendrent $\Lambda^k(M)$. Comme il y en a exactement $\binom{n}{k}$, il suffit de montrer que ces éléments sont libres.

Commençons par le cas où $k = n$. Dans ce cas, il s'agit de montrer que $\Lambda^n(M)$ est libre de rang 1, sachant qu'il est engendré par $m_1 \wedge \cdots \wedge m_n$. L'application multilinéaire $\det : M^n \to A$ (le déterminant dans la base $m_1, \dots, m_n$) correspond à une application

linéaire $\widetilde{\det} : T^n(M) \to A$ qui est manifestement nulle sur L et égale à 1 sur $m_1 \wedge \cdots \wedge m_n$. Ceci montre le théorème pour $k = n$.

Supposons maintenant que $k < n$. Si $j_1 < \cdots < j_k$ sont des entiers compris entre 1 et n et si l'on appelle $j_{k+1}, \ldots, j_n$ les autres entiers compris entre 1 et n et $y = m_{j_{k+1}} \wedge \cdots \wedge m_{j_n}$, alors on a une application linéaire $\Lambda^k(M) \to \Lambda^n(M)$ donnée par $x \mapsto x \wedge y$. Cette application envoie $\sum_{i_1<\cdots<i_k} \lambda_{i_1,\ldots,i_k} m_{i_1} \wedge \cdots \wedge m_{i_k}$ sur $\pm\lambda_{j_1,\ldots,j_k} m_1 \wedge \cdots \wedge m_n$ ce qui fait que si l'on a dans $\Lambda^k(M)$ une relation du type :

$$\sum_{i_1<\cdots<i_k} \lambda_{i_1,\ldots,i_k} m_{i_1} \wedge \cdots \wedge m_{i_k} = 0,$$

alors $\lambda_{j_1,\ldots,j_k} = 0$ et comme ceci est vrai pour toute suite $j_1 < \cdots < j_k$, les éléments de la forme $m_{i_1} \wedge \cdots \wedge m_{i_k}$ avec $i_1 < i_2 < \cdots < i_k$ sont donc libres dans $\Lambda^k(M)$. □

Si $f \in \mathrm{End}(M)$, alors on en déduit pour tout $k \geq 1$ une application $T^k(f) : T^k(M) \to T^k(M)$. On voit que $T^k(f)(L) \subset L$ et on en déduit par passage au quotient une application $\Lambda^k(f) : \Lambda^k(M) \to \Lambda^k(M)$.

Proposition 3.27. — *Si M est libre de rang n de base $m_1, \ldots, m_n$ et si $f \in \mathrm{End}(M)$ et P est la matrice de f, alors la matrice de $\Lambda^k(f)$ dans la base des $\{m_{i_1} \wedge \cdots \wedge m_{i_k}\}_{1\leq i_1<\cdots<i_k\leq n}$ est la matrice des mineurs $k \times k$ de P.*

Démonstration. — Comme $f(m_i) = \sum_{j=1}^n p_{j,i} m_j$, on a :

$$T^k(f)(m_{i_1} \otimes \cdots \otimes m_{i_k}) = \left(\sum_{j_1=1}^n p_{j_1,i_1} m_{j_1}\right) \otimes \cdots \otimes \left(\sum_{j_k=1}^n p_{j_k,i_k} m_{j_k}\right).$$

Si on choisit $\ell_1 < \cdots < \ell_k$, alors pour $\sigma \in \mathfrak{S}_k$ le coefficient de $m_{\ell_{\sigma(1)}} \otimes \cdots \otimes m_{\ell_{\sigma(k)}}$ dans le développement de la formule ci-dessus est $p_{\ell_{\sigma(1)},i_1} \cdots p_{\ell_{\sigma(k)},i_k}$. Dans $\Lambda^k(M)$, on a $m_{\ell_{\sigma(1)}} \wedge \cdots \wedge m_{\ell_{\sigma(k)}} = \varepsilon(\sigma) m_{\ell_1} \wedge \cdots \wedge m_{\ell_k}$ et le coefficient de $m_{\ell_1} \wedge \cdots \wedge m_{\ell_k}$ quand on a regroupé les termes est donc :

$$\sum_{\sigma\in\mathfrak{S}_k} \varepsilon(\sigma) p_{\ell_{\sigma(1)},i_1} \cdots p_{\ell_{\sigma(k)},i_k}.$$

C'est le mineur de P correspondant aux lignes $\ell_1, \ldots, \ell_k$ et aux colonnes $i_1, \ldots, i_k$. □

Si $k = n$, alors $\Lambda^n(M)$ est de dimension 1 et l'application $\Lambda^n(f) : \Lambda^n(M) \to \Lambda^n(M)$ est la multiplication par $\det(f)$. Plus généralement, on pourra montrer :

$$\det(X \cdot \mathrm{Id} - f) = \sum_{k=0}^n (-1)^k X^{n-k} \operatorname{Tr}(\Lambda^k(f)).$$

4. Localisation

4.1. Anneaux locaux. — Rappelons qu'un anneau A est dit *local* s'il admet un unique idéal maximal, et qu'un anneau est local si et seulement si l'ensemble de ses éléments non-inversibles en est un idéal. Si A est local d'idéal maximal I, le corps A/I s'appelle le corps résiduel de A. Si M est un A-module, alors $M/IM = M \otimes A/I$ est un A/I-espace vectoriel. On a vu (corollaire 1.12 et proposition 1.13).

Proposition 4.1. — *Soit A un anneau local d'idéal maximal I.*

1. *Si M est un A-module de type fini tel que $M \subset I \cdot M$, alors $M = 0$.*
2. *Si M est un A-module de type fini et si $m_1, \ldots, m_n$ sont tels que leurs images engendrent le A/I-espace vectoriel M/IM, alors M est engendré par $m_1, \ldots, m_n$.*

Théorème 4.2. — *Si M est un A-module plat de type fini, alors M est libre.*

Démonstration. — Soient $x_1, \ldots, x_n$ qui donnent une base du A/I-espace vectoriel M/IM, de sorte que M est engendré par $x_1, \ldots, x_n$ par la proposition 4.1. On va montrer que les x_i forment une famille libre. Montrons par récurrence sur r que r éléments $m_1, \ldots, m_r$ dont les images sont libres dans M/IM sont eux-mêmes libres dans M.

Par la proposition 3.19, on sait que toute relation dans M est triviale : si $f_1 m_1 + \cdots + f_r m_r = 0$, alors il existe des $a_{ij} \in A$ pour $1 \leq i \leq r$ et $1 \leq j \leq s$ des et $y_1, \ldots, y_s \in M$ tels que $m_i = a_{i1} y_1 + \cdots + a_{is} y_s$ pour tout i avec $f_1 a_{1j} + \cdots + f_r a_{rj} = 0$ pour tout j.

Si $r = 1$ et $f_1 m_1 = 0$, alors $m_1 = a_1 y_1 + \ldots + a_s y_s$ avec $f_1 a_j = 0$ pour tout j. Comme $m_1 \notin I \cdot M$, l'un des $a_j \notin I$ et donc $a_j \in A^\times$ ce qui fait que $f_1 = 0$.

Supposons à présent que $f_1 m_1 + \cdots + f_r m_r = 0$ et que $m_i = a_{i1} y_1 + \cdots + a_{is} y_s$ pour tout i avec $f_1 a_{1j} + \cdots + f_r a_{rj} = 0$ pour tout j. Quitte à permuter les indices, on peut supposer que $a_{11} \notin I$, c'est-à-dire que $a_{11} \in A^\times$. On a donc

$$f_1 = -\frac{a_{21}}{a_{11}} f_2 - \cdots - \frac{a_{r1}}{a_{11}} f_r,$$

ce qui fait que

$$f_2 \left(m_2 - \frac{a_{21}}{a_{11}} m_1 \right) + \cdots + f_r \left(m_r - \frac{a_{r1}}{a_{11}} m_1 \right) = 0.$$

La famille des $m_i - a_{i1}/a_{11} \cdot m_1$ est libre dans M/IM et donc libre dans M par récurrence. On en déduit que les f_i sont tous nuls. □

Corollaire 4.3. — *Un module projectif de type fini sur un anneau local est libre.*

4.2. Localisation d'anneaux. — Si A est un anneau intègre, on sait construire son corps des fractions K, obtenu en inversant tous les éléments non nuls de A. Cette construction peut se faire de manière partielle. Soit A un anneau (pas nécessairement intègre) et S une partie de A stable par multiplication (qui contient le produit vide 1). On définit une relation d'équivalence sur $A \times S$ par $(a_1, s_1) \sim (a_2, s_2)$ s'il existe $t \in S$ tel que $ta_1s_2 = ta_2s_1$. Soit $S^{-1}A$ le quotient de $A \times S$ par $\sim$. On note a/s la classe de (a, s).

Proposition 4.4. — *Les formules* $a_1/s_1 \cdot a_2/s_2 = a_1a_2/s_1s_2$ *et* $a_1/s_1 + a_2/s_2 = (a_1s_2 + a_2s_1)/s_1s_2$ *font de* $S^{-1}A$ *un anneau, qui est une* A*-algèbre via le morphisme* $\phi_S : a \mapsto a/1$.

Si B *est un anneau et* $f : A \to B$ *est un morphisme tel que* $f(s) \in B^\times$ *pour tout* $s \in S$*, alors il existe un unique* $g : S^{-1}A \to B$ *tel que* $f = g \circ \phi_S$.

Notons que ϕ_S n'est pas nécessairement injectif. Par exemple, si K et L sont deux corps et si $A = K \times L$ et $S = K \times L^\times$, alors $S^{-1}A = L$.

Lemme 4.5. — *On a* $\ker(\phi_S) = \{a$ *tels qu'il existe* $s \in S$ *avec* $as = 0\}$.

Démonstration. — On a $(a, 1) \sim (0, 1)$ si et seulement s'il existe $s \in S$ avec $as = 0$. □

Si A est intègre, alors $S = A \setminus \{0\}$ est une partie multiplicative, $S^{-1}A$ est le corps des fractions de A, et ϕ_S est injective. Plus généralement, si $\mathfrak{p}$ est un idéal premier, alors $S = A \setminus \mathfrak{p}$ est une partie multiplicative et $S^{-1}A$ est le localisé de A en $\mathfrak{p}$, noté $A_\mathfrak{p}$. Enfin si $f \in A$ et $S = \{f^n, n \geq 0\}$, alors $S^{-1}A$ est noté A_f et est isomorphe à $A[1/f]$.

Proposition 4.6. — *Si* $\mathfrak{p}$ *est un idéal premier de* A*, alors* $A_\mathfrak{p}$ *est un anneau local, d'idéal maximal* $\mathfrak{m} = \{a/s$ *avec* $a \in \mathfrak{p}\}$. *On a* $A_\mathfrak{p}/\mathfrak{m} = \mathrm{Frac}(A/\mathfrak{p})$.

Démonstration. — Si $a/s \in A_\mathfrak{p}$ et $a \notin \mathfrak{p}$, alors $a \in S$ et $a/s \cdot s/a = 1$ et donc $a/s \in A_\mathfrak{p}^\times$. Si $a/s \in A_\mathfrak{p}^\times$ alors $a/s \cdot b/t = 1$ et il existe donc $u \notin \mathfrak{p}$ tel que $uab = ust$. En particulier, $a \notin \mathfrak{p}$. L'ensemble $\mathfrak{m}$ est donc le complémentaire de $A_\mathfrak{p}^\times$ et comme c'est un idéal de $A_\mathfrak{p}$, cet anneau est local.

La projection $A \to A/\mathfrak{p}$ donne lieu à $f : A \to \mathrm{Frac}(A/\mathfrak{p})$ si $x \in A \setminus \mathfrak{p}$, alors $f(x)$ est inversible. On en déduit $g : A_\mathfrak{p} \to \mathrm{Frac}(A/\mathfrak{p})$, donnée par $g(a/s) = f(a)f(s)^{-1}$, et qui est surjective. Le noyau de g est l'unique idéal maximal de $A_\mathfrak{p}$, et donc $A_\mathfrak{p}/\mathfrak{m} = \mathrm{Frac}(A/\mathfrak{p})$. □

4.3. Localisation de modules. — Si M est un A-module, on peut définir $S^{-1}M$ de la même manière, c'est le quotient de $M \times S$ par $\sim$, et on note m/s la classe de (m, s). Le module $S^{-1}M$ est alors un $S^{-1}A$-module. L'analogue du lemme 4.5 est vrai : le noyau de $M \to S^{-1}M$ est l'ensemble des $m \in M$ tels qu'il exste $s \in S$ avec $sm = 0$. Si $u : M \to N$ est un morphisme de A-modules, on en déduit un morphisme $S^{-1}u : S^{-1}M \to S^{-1}N$.

Proposition 4.7. — *Si on a une suite exacte $M' \xrightarrow{f} M \xrightarrow{g} M''$, alors la suite $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ est exacte.*

Démonstration. — Il faut montrer que $\mathrm{im}(S^{-1}f) = \ker(S^{-1}g)$. L'inclusion $\subset$ est claire ; soit $m/s \in S^{-1}M$ tel que $S^{-1}g(m/s) = 0$. Il existe donc $t \in S$ tel que $tg(m) = 0$, et donc $tm \in \ker(g) = \mathrm{im}(f)$. On a $tm = f(m')$ et alors $m/s = tm/ts = S^{-1}f(m'/ts)$. □

Corollaire 4.8. — *Si N et P sont deux sous A-modules d'un module M, alors dans $S^{-1}M$, on a $S^{-1}(N+P) = S^{-1}N + S^{-1}P$ et $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.*

Démonstration. — On a une suite exacte $0 \to N \cap P \to N \oplus P \to N + P \to 0$, et le corollaire suit alors de la proposition 4.7. □

Théorème 4.9. — *Il existe un unique morphisme $S^{-1}A \otimes_A M \to S^{-1}M$ qui envoie $a/s \otimes m$ sur am/s, et c'est un isomorphisme.*

Démonstration. — L'existence et l'unicité viennent de l'application bilinéaire $S^{-1}A \times M \to S^{-1}M$ donnée par $(a/s, m) \mapsto (am/s)$. Le morphisme $S^{-1}A \otimes_A M \to S^{-1}M$ qu'on en déduit est surjectif, montrons qu'il est injectif. Soit $a_1/s_1 \otimes m_1 + \cdots + a_r/s_r \otimes m_r \in S^{-1}A \otimes_A M$. Posons $s = s_1 \cdots s_r$ et $t_i = s_1 \cdots \hat{s}_i \cdots s_r$. On a

$$\frac{a_1}{s_1} \otimes m_1 + \cdots + \frac{a_r}{s_r} \otimes m_r = \frac{1}{s} \otimes (a_1 t_1 m_1 + \cdots + a_r t_r m_r)\,,$$

et donc tout élément de $S^{-1}A \otimes M$ est de la forme $1/s \otimes m$. Si son image m/s dans $S^{-1}M$ est nulle, alors il existe $t \in S$ tel que $tm = 0$ et $1/s \otimes m = 1/st \otimes tm = 0$. □

Corollaire 4.10. — *Le A-module $S^{-1}A$ est plat.*

Notons aussi la propriété suivante.

Proposition 4.11. — *Si M et N sont deux A-modules, alors il existe un unique isomorphisme $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ qui envoie $m/s \otimes n/t$ sur $(m \otimes n)/st$.*

4.4. Localisation d'idéaux. — Ce qu'on a fait à la section précédente s'applique en particulier aux idéaux de A. Si I est un idéal de A, alors $S^{-1}I$ est un idéal de $S^{-1}A$.

Soit E (extension) l'application de l'ensemble des idéaux de A vers l'ensemble des idéaux de $S^{-1}A$ donnée par $I \mapsto S^{-1}I$. Soit C (contraction) l'application qui à un idéal J de $S^{-1}A$ associe l'idéal $\phi_S^{-1}(J) = \{a \in A \text{ tels que } a/1 \in J\}$ de A.

Proposition 4.12. — *Si J est un idéal de $S^{-1}A$, alors $J = E \circ C(J)$.*

Démonstration. — Si $a/s \in J$, alors $a/1 \in J$ et donc $a \in C(J)$ ce qui fait que $a/s = 1/s \cdot a \in S^{-1}C(J)$. Réciproquement, si $a/s \in S^{-1}C(J)$, alors il existe $t \in S$ tel que $at \in C(J)$ et donc $at/1 \in J$ et $a/s = at/1 \cdot 1/st \in J$. □

Corollaire 4.13. — *Si A est noethérien, alors $S^{-1}A$ l'est aussi.*

4.5. Localisation de morphismes. — Soit M un A-module.

Proposition 4.14. — *Les propriétés suivantes sont équivalentes :*

1. $M = 0$ *;*
2. $M_{\mathfrak{p}} = 0$ *pour tout idéal premier* $\mathfrak{p}$ *de* A *;*
3. $M_{\mathfrak{m}} = 0$ *pour tout idéal maximal* $\mathfrak{m}$ *de* A*.*

Si en plus M est de type fini, alors ces propriétés sont équivalentes à $M \otimes_A A/\mathfrak{m} = 0$ pour tout idéal maximal $\mathfrak{m}$.

Démonstration. — Il suffit de montrer que (3) implique (1). Si $x \in M$, considérons l'idéal $\mathrm{Ann}(x) = \{a \in A \text{ tels que } ax = 0\}$. Si $\mathrm{Ann}(x) \neq A$, alors il existe un idéal maximal $\mathfrak{m}$ qui contient $\mathrm{Ann}(x)$. Si l'image de x est nulle dans $M_{\mathfrak{m}}$, il existe $a \in S = A \setminus \mathfrak{m}$ tel que $ax = 0$, contradiction.

On a $M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}} = M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} A_{\mathfrak{m}}/\mathfrak{m} = (M \otimes_A A/\mathfrak{m})_{\mathfrak{m}} = 0$. Si M est de type fini sur A, alors $M_{\mathfrak{m}}$ est de type fini sur $A_{\mathfrak{m}}$ et le lemme de Nakayama (proposition 4.1) implique alors que $M_{\mathfrak{m}} = 0$. □

Corollaire 4.15. — *Soit $f \in \mathrm{Hom}_A(M, N)$ et P la propriété d'être injectif ou surjectif ou bijectif. Les propriétés suivantes sont équivalentes :*

1. f *a la propriété* P *;*
2. $f_{\mathfrak{p}}$ *a la propriété* P *pour tout idéal premier* $\mathfrak{p}$ *de* A *;*
3. $f_{\mathfrak{m}}$ *a la propriété* P *pour tout idéal maximal* $\mathfrak{m}$ *de* A*.*

Démonstration. — Comme la localisation est exacte, il suffit d'appliquer la proposition 4.14 à $\ker(f)$ ou à $\mathrm{coker}(f)$. □

Si M est un A-module, on dit que M est de présentation finie s'il existe une suite exacte $0 \to K \to L \to M \to 0$ où L est libre de rang fini et K est de type fini. Comme K est de type fini, il existe L' libre de rang fini et une surjection $L' \to K$, et donc une suite exacte $L' \to L \to M \to 0$. Notons que si A est noethérien, un module de type fini est de présentation finie.

Proposition 4.16. — *Si M et N sont deux A-modules, il y a un unique morphisme de $S^{-1}A$-modules $\alpha : S^{-1}\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ qui envoie f/s sur $[m/t \mapsto f(m)/st]$. Si M est de présentation finie, alors α est un isomorphisme.*

Démonstration. — L'existence de α_S vient plus généralement de l'existence, pour une A-algèbre B, d'un unique morphisme $B \otimes_A \operatorname{Hom}_A(M,N) \to \operatorname{Hom}_B(B \otimes_A M, B \otimes_A N)$ qui envoie $b \otimes f$ sur $[c \otimes m \mapsto bc \otimes f(m)]$.

Supposons maintenant que M est de présentation finie, $L' \to L \to M \to 0$. Soit B une A-algèbre plate. En tensorisant $L' \to L \to M \to 0$ par B et en prenant $\operatorname{Hom}(\cdot, N)$, et vice versa, on trouve un diagramme

$$\begin{array}{ccccc} 0 \to B \otimes \operatorname{Hom}(M,N) & \longrightarrow & B \otimes \operatorname{Hom}(L,N) & \longrightarrow & B \otimes \operatorname{Hom}(L',N) \\ \downarrow{\scriptstyle \alpha_M} & & \downarrow{\scriptstyle \alpha_L} & & \downarrow{\scriptstyle \alpha_{L'}} \\ 0 \to \operatorname{Hom}(B \otimes M, B \otimes N) & \longrightarrow & \operatorname{Hom}(B \otimes L, B \otimes N) & \longrightarrow & \operatorname{Hom}(B \otimes L', B \otimes N) \end{array}$$

Comme L et L' sont libres de rang fini, α_L et $\alpha_{L'}$ sont des isomorphismes. On en déduit que α_M est aussi un isomorphisme. □

Disons qu'un A-module M est localement libre si $M_{\mathfrak{p}}$ est libre sur $A_{\mathfrak{p}}$ pour tout idéal premier $\mathfrak{p}$ de A.

Théorème 4.17. — *Si M est de présentation finie, alors M est projectif si et seulement s'il est localement libre.*

Démonstration. — Si M est projectif de type fini, alors $M_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_A M$ est projectif sur $A_{\mathfrak{p}}$ et donc libre par le corollaire 4.3.

Montrons l'implication inverse : il faut montrer que si $P \to Q$ est un morphisme surjectif de A-modules, alors $\operatorname{Hom}_A(M,P) \to \operatorname{Hom}_A(M,Q)$ est surjectif. Par le corollaire 4.15, il suffit de montrer que $\operatorname{Hom}_A(M,P)_{\mathfrak{p}} \to \operatorname{Hom}_A(M,Q)_{\mathfrak{p}}$ est surjectif pour tout idéal premier $\mathfrak{p}$. Comme M est de présentation finie, par la proposition 4.16, on a $\operatorname{Hom}_A(M,P)_{\mathfrak{p}} = \operatorname{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, P_{\mathfrak{p}})$, et de même pour $\operatorname{Hom}_A(M,Q)$. L'application $\operatorname{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, P_{\mathfrak{p}}) \to \operatorname{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, Q_{\mathfrak{p}})$ est surjective car $M_{\mathfrak{p}}$ est libre, et M est donc projectif. □

Corollaire 4.18. — *Un module plat de présentation finie est projectif.*

Démonstration. — Par le théorème 4.2, un module plat de présentation finie sur $A_{\mathfrak{p}}$ est libre, donc un module plat de présentation finie est localement libre. □

Remarque 4.19. — Si M est de présentation finie, alors M est localement libre si et seulement s'il existe $f_1, \ldots, f_n \in A$ tels que $(f_1, \ldots, f_n) = A$ et tels que $M[1/f_i]$ est un $A[1/f_i]$-module libre pour tout i.

5. Entiers

5.1. Éléments entiers. — Soit B un anneau et A un sous-anneau de B. Si $x \in B$, on dit que x est entier sur A s'il existe $P(X) \in A[X]$ unitaire tel que $P(x) = 0$.

Proposition 5.1. — *Si $x \in B$, alors les propriétés suivantes sont équivalentes :*

1. *x est entier sur A ;*
2. *$A[x]$ est un A-module de type fini ;*
3. *il existe un sous-anneau C de B qui est de type fini comme A-module et contient x.*

Démonstration. — Il est évident que (1) implique (2) implique (3). Montrons que (3) implique (1). Soit f l'endomorphisme de C donné par la multiplication par x. Le théorème de Cayley-Hamilton (théorème 1.11) nous donne un polynôme unitaire qui annule x. □

Corollaire 5.2. — *L'ensemble C des éléments x de B qui sont entiers sur A est un sous-anneau de B.*

Démonstration. — Si x, $y \in C$, alors y est entier sur A et donc sur $A[x]$ (par le (1)) et donc $A[x, y]$ est un $A[x]$-module de type fini. On en déduit que $A[x, y]$ est un A-module de type fini, qui contient $x + y$ et xy. □

L'anneau C est la clôture intégrale (normalisation) de A dans B. Si $C = A$, on dit que A est intégralement clos dans B. Si $C = B$, on dit que B est entier sur A. On dit qu'un anneau intègre A est intégralement clos (normal) s'il l'est dans son corps des fractions.

Si K est une extension finie de $\mathbf{Q}$, on note $\mathcal{O}_K$ la clôture intégrale de $\mathbf{Z}$ dans K. L'étude des propriétés de $\mathcal{O}_K$ relève de la théorie algébrique des nombres. Notons par exemple que si $K = \mathbf{Q}(\sqrt{d})$ où d est un entier sans facteur carré, alors $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de rang 2 : on a $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\sqrt{d}$ si $d \not\equiv 1 \bmod 4$ et $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}(1 + \sqrt{d})/2$ sinon.

L'anneau $\mathcal{O}_K$ n'est plus nécessairement factoriel, par exemple dans $\mathbf{Z}[\sqrt{-5}]$, on a $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, et les éléments 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles.

Exemple 5.3. — Un anneau intègre factoriel est intégralement clos.

Démonstration. — Soit a/b dans le corps des fractions de A, tel que a/b est entier sur A. On a $(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0$ et donc $a^n + a_{n-1}ba^{n-1} + \cdots + a_0 b^n = 0$. Si p est un élément premier de A qui divise b, alors il divise a^n et donc a. □

Proposition 5.4. — *Soit B un anneau et A un sous-anneau de B et S une partie multiplicative de A. Si B est entier sur A, alors $S^{-1}B$ est entier sur $S^{-1}A$.*

Démonstration. — Soix $x = b/s \in S^{-1}B$ et $P \in A[X]$ un polynôme unitaire de degré d qui annule b. Si $Q(X) = s^{-d}P(sX)$, alors $Q(b/s) = s^{-d}P(b) = 0$, et $Q(X) \in (S^{-1}A)[X]$ est unitaire. □

5.2. Finitude des invariants. — On dit que A est une K-algèbre de type fini s'il existe $a_1, \ldots, a_n \in A$ tels que $A = K[a_1, \ldots, a_n]$, c'est à dire si l'application $P \mapsto P(a_1, \ldots, a_n)$ de $K[X_1, \ldots, X_n] \to A$ est surjective. Notons qu'une sous algèbre de $K[X_1, \ldots, X_n]$ n'est pas nécessairement de type fini (prendre la sous-algèbre de $K[X, Y]$ engendrée par les monômes $X^a Y^b$ avec $a \leq \sqrt{2}b$).

Soit A un anneau muni d'une action d'un groupe fini G. Que peut-on dire de A^G ? La démonstration du théorème ci-dessous est due à Noether.

Théorème 5.5. — *Si A est une K-algèbre de type fini, et G est un groupe fini qui agit K-linéairement sur A, alors A^G est aussi une K-algèbre de type fini.*

Il existe donc un nombre fini d'invariants tels que tout autre invariant est un polynôme en ceux-ci. Par exemple, $K[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est engendré par les fonctions symétriques élémentaires.

Lemme 5.6. — *L'anneau A est entier sur A^G.*

Démonstration. — Si $a \in A$, alors a est annulé par $\prod_{g \in G}(X - g(a))$ qui est unitaire et à coefficients dans A^G. □

Lemme 5.7. — *Si B/A est entier et de type fini, alors B est un A-module de type fini.*

Démonstration. — Cela suit immédiatement de la proposition 5.1. □

Proposition 5.8. — *Si B est une K-algèbre de type fini, et A est une sous K-algèbre de B telle que B est un A-module de type fini, alors A est une K-algèbre de type fini.*

Démonstration. — Écrivons $B = K[x_1, \ldots, x_n]$ et $B = Ay_1 + \cdots + Ay_m$. Soient a_{ij} et a_{ijk} les éléments de A tels que $x_i = \sum a_{ij}y_j$ et $y_i y_j = \sum a_{ijk}y_k$ et $A_0 = K[a_{ij}, a_{ijk}]$. Montrons que $B = A_0 y_1 + \cdots + A_0 y_m$. Si $b \in B$, on a $b = P(x_1, \ldots, x_n) = P(\sum a_{1j}y_j, \ldots, \sum a_{nj}y_j) \in A_0 y_1 + \cdots + A_0 y_m$.

L'anneau B est donc un A_0-module de type fini, et comme A_0 est noethérien et $A \subset B$, l'anneau A est aussi un A_0-module de type fini. C'est donc une K-algèbre de type fini. □

Démonstration du théorème 5.5. — L'anneau A est une A^G-algèbre de type fini et est entier sur A^G, donc c'est un A^G-module de type fini par le lemme 5.7. La proposition 5.8 implique alors que A^G est une K-algèbre de type fini. □

5.3. Normalisation de Noether. — Soit K un corps et A une K-algèbre. On dit que des éléments $a_1, \ldots, a_n \in A$ sont algébriquement indépendants sur K si l'application $P \mapsto P(a_1, \ldots, a_n)$ de $K[X_1, \ldots, X_n] \to A$ est injective.

Théorème 5.9. — *Si A est une K-algèbre de type fini, alors il existe des éléments algébriquement indépendants $x_1, \ldots, x_n \in A$ tels que A est un $K[x_1, \ldots, x_n]$-module de type fini.*

De plus, si A est engendré par m éléments sur K, alors $n \leq m$.

Afin de simplifier la preuve, on suppose que K est infini. On dispose alors du lemme suivant (noter que le polynôme $X^p - X$ est nul sur $\mathbf{F}_p$).

Lemme 5.10. — *Si $P \in K[T_1, \ldots, T_k]$ est non nul, alors il existe $t_1, \ldots, t_k \in K$ tels que $P(t_1, \ldots, t_k) \neq 0$.*

Démonstration. — Si $k = 1$, cela suit du fait qu'un polynôme en une variable n'a qu'un nombre fini de racines. Si $k \geq 2$, écrivons $P = a_0 + a_1 T_k + \cdots + a_d T_k^d$ avec $a_i \in K[T_1, \ldots, T_{k-1}]$. Par récurrence, il existe $t_1, \ldots, t_{k-1}$ tels que l'un des $a_i(t_1, \ldots, t_{k-1})$ est non nul. On est alors ramené au cas d'une variable. □

Lemme 5.11. — *Si $R \in K[T_1, \ldots, T_m]$ est un polynôme non nul et homogène de degré d, alors il existe $t_1, \ldots, t_{m-1} \in K$ tels que $R(t_1, \ldots, t_{m-1}, 1) \neq 0$.*

Démonstration. — On vérifie facilement que $R(T_1, \ldots, T_{m-1}, 1) \neq 0$ et le lemme suit alors du lemme 5.10. □

Lemme 5.12. — *Soit $a_1, \ldots, a_m \in A$ tels que $A = K[a_1, \ldots, a_m]$. S'il existe un polynôme $P \in K[X_1, \ldots, X_m]$ tel que $P(a_1, \ldots, a_m) = 0$, alors il existe $a'_1, \ldots, a'_{m-1} \in A$ tels que a_m est entier sur $K[a'_1, \ldots, a'_{m-1}]$ et $A = K[a'_1, \ldots, a'_{m-1}, a_m]$.*

Démonstration. — Soient $t_1, \ldots, t_{m-1} \in K$ et $a'_i = a_i - t_i a_m$ pour $1 \leq i \leq m-1$. Soit $B = K[a'_1, \ldots, a'_{m-1}]$. Il est clair que $A = K[a'_1, \ldots, a'_{m-1}, a_m] = B[a_m]$. Soit $Q(X) = P(a'_1 + t_1 X, \ldots, a'_{m-1} + t_{m-1} X, X) \in B[X]$ et $d = \deg(P)$. On a $Q(a_m) = 0$, et le coefficient de X^d vaut $P_d(t_1, t_2, \ldots, t_{m-1}, 1)$ où P_d est la partie homogène de degré d de P.

Par le lemme 5.11, il existe $t_1, \dots, t_{m-1} \in K$ tels que $P_d(t_1, \dots, t_{m-1}, 1) \neq 0$. Le polynôme $Q(X)$ correspondant a un coefficient dominant inversible, et a_m est donc entier sur $B = K[a'_1, \dots, a'_{m-1}]$. □

Démonstration du théorème 5.9. — Procédons par récurrence sur le nombre m de générateurs de A comme K-algèbre. Si $m = 0$, alors $A = K$ et le théorème est trivial. Supposons donc que $A = K[a_1, \dots, a_m]$ avec $m \geq 1$. Si $a_1, \dots, a_m$ sont algébriquement indépendants, alors on peut prendre $x_i = a_i$ et on a terminé. Sinon, il existe un polynôme P tel que $P(a_1, \dots, a_m) = 0$ et le lemme 5.12 nous donne $a'_1, \dots, a'_{m-1}$ dans A tels que a_m est entier sur $B = K[a'_1, \dots, a'_{m-1}]$ et $A = B[a_m]$. L'hypothèse de récurrence appliquée à B nous donne $x_1, \dots, x_{n-1} \in B$ avec $n \leq m$, algébriquement indépendants sur K, tels que B est un $K[x_1, \dots, x_{n-1}]$-module de type fini. Comme $A = B[a_m]$ avec a_m entier sur B, l'anneau A est lui-même un $K[x_1, \dots, x_{n-1}]$-module de type fini. □

5.4. Le théorème des zéros de Hilbert. — Le but de cette section est de montrer l'un des énoncés connus sous le nom de "nullstellensatz".

Théorème 5.13. — *Si K est un corps algébriquement clos, alors les idéaux maximaux de $K[X_1, \dots, X_n]$ sont de la forme $(X_1 - a_1, \dots, X_n - a_n)$ avec $(a_1, \dots, a_n) \in K^n$.*

Corollaire 5.14. — *Si K est un corps algébriquement clos, et I est un idéal propre de $K[X_1, \dots, X_n]$, alors les idéaux maximaux de $K[X_1, \dots, X_n]/I$ sont de la forme $(X_1 - a_1, \dots, X_n - a_n)$ où $(a_1, \dots, a_n) \in K^n$ sont tels que $P(a_1, \dots, a_n) = 0$ pour tout $P \in I$.*

Corollaire 5.15. — *Si $P_1, \dots, P_m \in K[X_1, \dots, X_n]$ n'ont pas de solution commune dans K, alors il existe $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ tels que $f_1P_1 + \cdots + f_mP_m = 1$.*

Corollaire 5.16. — *Si $P_1, \dots, P_m \in K[X_1, \dots, X_n]$ ont une solution commune dans une extension quelconque de K, alors ils ont une solution commune dans K.*

Lemme 5.17. — *Si B est un anneau intègre, qui est entier sur un sous-anneau A, alors B est un corps si et seulement si A est un corps.*

Démonstration. — Si A est un corps et $x \neq 0 \in B$, alors x est entier sur A et donc $A[x]$ est un A-espace vectoriel de dimension finie. La multiplication par x sur $A[x]$ est injective car B est intègre, et donc surjective, ce qui fait que x est inversible.

Si B est un corps et $x \neq 0 \in A$, alors x est inversible dans B et x^{-1} est entier sur A. On a donc $a_0 + a_1x^{-1} + \cdots + a_{n-1}x^{-(n-1)} + x^{-n} = 0$ et donc $x^{-1} = -a_0x^{n-1} - \cdots - a_{n-1} \in A$. □

Lemme 5.18. — *Soit K un corps et A une K-algèbre de type fini. Si A est un corps, alors c'est une extension finie de K.*

Démonstration. — Par le théorème de normalisation de Noether (théorème 5.9), A est entier sur $K[X_1, \ldots, X_n]$ pour un $n \geq 0$. Par le lemme 5.17, si A est un corps, alors $K[X_1, \ldots, X_n]$ est un corps. Ceci ne se produit que pour $n = 0$. □

Démonstration du théorème 5.13. — Soit I un idéal maximal de $K[X_1, \ldots, X_n]$ et $A = K[X_1, \ldots, X_n]/I$. C'est une K-algèbre de type fini qui est un corps, et donc c'est une extension finie de K par le lemme 5.18. Comme K est algébriquement clos, on a $A/I = K$. Soit a_i l'image de X_i. L'idéal I contient $(X_1 - a_1, \ldots, X_n - a_n)$ et lui est donc égal. □

Laurent Berger, UMPA, ÉNS de Lyon, UMR 5669 du CNRS
E-mail : laurent.berger@ens-lyon.fr • *Url :* http://perso.ens-lyon.fr/laurent.berger/