UNIVERSITÉ DE BORDEAUX

Master 1
Modules, algèbre commutative - 4TMA702U

OLIVIER BRINON

Table des matières

Bibliographie sommaire (pour aller plus loin)

M. Atiyah, I. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley (1969)
D. Dummit, R. Foote, *Abstract Algebra*, John Wiley & Sons (2003)
D. Eisenbud, *Commutative Algebra, with a View Toward Algebraic Geometry*, GTM **150**, Springer (1995)
H. Matsumura [1], *Commutative Ring Theory*, Cambridge University Press (1987)

Dans tout ce qui suit, les anneaux seront tous supposés *commutatifs et unitaires*. Rappelons que si A est un anneau et $I \subsetneq A$ un idéal strict, alors il existe un idéal maximal $\mathfrak{m} \subset A$ tel que $I \subset \mathfrak{m}$ (théorème de Krull).

1 Polynômes symétriques

Soient A un anneau, $r \in \mathbf{N}_{>0}$ et $X_1, \dots, X_r, T$ des indéterminées. Rappelons qu'un *monôme* est un élément de la forme $\alpha X^{\underline{n}} := X_1^{n_1} \cdots X_r^{n_r}$ avec $\alpha \in A\backslash\{0\}$ et $\underline{n} = (n_1, \dots, n_r) \in \mathbf{N}^r$; son *degré* (total) est $|\underline{n}| := n_1 + \cdots + n_r$. Tout élément de $A[X_1, \dots, X_r]$ peut s'écrire de façon unique comme somme de monômes. Si $d \in \mathbf{N}$, un élément de $A[X_1, \dots, X_r]$ est *homogène* de degré d lorsque c'est une somme de monômes de degré d. L'ensemble $\mathscr{H}_{r,d}$ des polynômes homogènes de degré d auquel on adjoint 0 est un sous-groupe de $A[X_1, \dots, X_r]$ et $A[X_1, \dots, X_r] = \bigoplus_{d=0}^{\infty} \mathscr{H}_{r,d}$. Explicitement, cela signifie que si $P \in A[X_1, \dots, X_r]$, il existe une unique suite $(P_d)_{d\in\mathbf{N}}$ (les *composantes homogènes* de P) nulle à partir d'un certain rang telle que $P = \sum_{d=0}^{\infty} P_d$ et P_d est homogène de degré d pour tout $d \in \mathbf{N}$.

Définition 1.1. (1) Si $P(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$ et $\gamma \in \mathfrak{S}_r$, on pose

$$(\gamma.P)(X_1, \dots, X_r) = P(X_{\gamma^{-1}(1)}, \dots, X_{\gamma^{-1}(r)}).$$

On munit ainsi $A[X_1, \dots, X_r]$ d'une action (à gauche) du groupe $\mathfrak{S}_r$.
(2) Un polynôme $P(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$ est dit *symétrique* si c'est un point fixe sous cette action (on définit de façon analogue la notion de fraction rationnelle symétrique à coefficients dans un corps).
(3) Pour $k \in \{1, \dots, r\}$, le *k-ième polynôme symétrique élémentaire* est

$$\sigma_k = \sigma_k(X_1, \dots, X_r) = \sum_{i_1<\cdots<i_k} X_{i_1} \cdots X_{i_k}.$$

Exemple 1.2. On a

$$\begin{aligned}
\sigma_1 &= X_1 + X_2 + \cdots + X_r \\
\sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_1X_r + X_2X_3 + \cdots + X_2X_r + \cdots + X_{r-1}X_r \\
\sigma_r &= X_1X_2 \cdots X_r.
\end{aligned}$$

1. 松村 英之

Version du 10 décembre 2024

Proposition 1.3. (RELATIONS COEFFICIENTS-RACINES) *On a*

$$\prod_{i=1}^{r}(T-X_i) = T^r - \sigma_1 T^{r-1} + \sigma_2 T^{r-2} + \cdots + (-1)^k \sigma_k T^{r-k} + \cdots + (-1)^r \sigma_r$$

dans $\mathbf{Z}[T, X_1, \ldots, X_r]$.

Démonstration. On procède par récurrence sur r, en observant que si $1 \leqslant k \leqslant r$, on a

$$\sigma_k(X_1, \ldots, X_{r+1}) = \sigma_k(X_1, \ldots, X_r) + \sigma_{k-1}(X_1, \ldots, X_r) X_{r+1}$$

avec la convention $\sigma_0 = 1$. □

Théorème 1.4. (THÉORÈME FONDAMENTAL DES POLYNÔMES SYMÉTRIQUES) *Si* $P(X_1, \ldots, X_r) \in A[X_1, \ldots, X_r]$ *est symétrique, il existe* $Q(Y_1, \ldots, Y_r) \in A[Y_1, \ldots, Y_r]$ *unique tel que* $P(X_1, \ldots, X_r) = Q(\sigma_1, \ldots, \sigma_r)$.

Dans ce qui suit, on ordonnera l'ensemble $\mathbf{N}^r$ au moyen de l'ordre lexicographique : on a $\underline{n} < \underline{m}$ s'il existe $i \leqslant r$ tel que $n_j = m_j$ pour $j < i$ et $n_i < m_i$. On rappelle que c'est une relation d'ordre total (et même un bon ordre). Cet ordre définit un ordre sur les monômes.

Lemme 1.5. *Un polynôme est symétrique si et seulement si ses composantes homogènes sont symétriques.*

Démonstration. Cela résulte du fait chaque $\mathscr{H}_{r,d}$ est stable par l'action de $\mathfrak{S}_r$, et de l'unicité de la décomposition en somme de composantes homogènes. □

Lemme 1.6. *Le polynôme* $\sigma_1^{a_1} \cdots \sigma_r^{a_r}$ *est symétrique de degré* $a_1 + 2a_2 + \cdots + ra_r$. *Son monôme le plus grand pour l'ordre lexicographique est* $X_1^{a_1+a_2+\cdots+a_r} X_2^{a_2+\cdots+a_r} \cdots X_{r-1}^{a_{r-1}+a_r} X_r^{a_r}$.

Démonstration. Pour $i \in \{1, \ldots, r\}$, le polynôme σ_i est symétrique de degré i. Le polynôme $\sigma_1^{a_1} \cdots \sigma_r^{a_r}$ est donc symétrique, de degré $a_1 + 2a_2 + \cdots + ra_r$ (c'est vrai même lorsque A n'est pas intègre, parce que les coefficients de tous les monômes qui interviennent valent 1). Le monôme le plus grand de σ_i (pour l'ordre lexicographique) est $X_1 X_2 \cdots X_i$. Le monôme le plus grand de $\sigma_1^{a_1} \cdots \sigma_r^{a_r}$ est donc

$$X_1^{a_1} (X_1 X_2)^{a_2} \cdots (X_1 X_2 \cdots X_r)^{a_r} = X_1^{a_1+a_2+\cdots+a_r} X_2^{a_2+\cdots+a_r} \cdots X_{r-1}^{a_{r-1}+a_r} X_r^{a_r}$$

(on retouve le fait que le degré vaut $a_1 + 2a_2 + \cdots + ra_r$). □

Démonstration du théorème 1.4. D'après le lemme 1.5, il suffit de traiter le cas où P est homogène, ce que l'on suppose par la suite. Notons d son degré et soit $\alpha X^{\underline{n}}$ son monôme le plus grand pour l'ordre lexicographique. on a nécessairement $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_r$. En effet, si on avait $n_i < n_j$ avec $i < j$, on pourrait appliquer la transposition $\tau_{(i,j)}$ à f : ce dernier étant symétrique, il contiendrait aussi le monôme $\alpha \tau_{(i,j)} \cdot X^{\underline{n}}$, qui est strictement plus grand que $\alpha X^{\underline{n}}$ pour l'ordre lexicographique.
Posons $P_1 = P - \alpha \sigma_1^{n_1-n_2} \sigma_2^{n_2-n_3} \cdots \sigma_{r-1}^{n_{r-1}-n_r} \sigma_r^{n_r} \in A[X_1, \ldots, X_r]$. C'est encore un polynôme symétrique homogène de degré d. Les monômes qui le composent sont tous strictement plus petits que $X^{\underline{n}}$ (on l'a éliminé dans la différence). En itérant le procédé qui précéde, on peut écrire tout polynôme symétrique comme polynôme en les polynômes symétriques élémentaires (il n'y a qu'un nombre fini d'étapes car $\mathbf{N}^r$ n'admet pas de suite strictement décroissante infinie, vu que l'odre lexicographique est un bon ordre).
Reste à prouver que l'écriture est unique. Par linéarité, il suffit de prouver que si $P = 0$, on a nécessairement $Q = 0$. Prouvons la contraposée : supposons $Q \neq 0$. Soit $\alpha Y_1^{a_1} \cdots Y_r^{a_r}$ son monôme le plus grand (pour l'ordre lexicographique, en les indéterminés $Y_1, \ldots, Y_r$). Le monôme le plus grand de $P = Q(\sigma_1, \ldots, \sigma_r)$ (pour l'ordre lexicographique) est alors $\alpha X_1^{a_1+a_2+\cdots+a_r} X_2^{a_2+\cdots+a_r} \cdots X_{r-1}^{a_{r-1}+a_r} X_r^{a_r}$ d'après le lemme 1.6 : il n'est pas nul, donc $P \neq 0$. □

Remarques. (1) La preuve fournit un procédé algorithmique pour déterminer le polynôme Q. Cela dit, les degrés en chaque indéterminée, ainsi que les poids des monômes qui composent P excluent certains monômes de Q. On peut alors chercher Q avec des coefficients indéterminés : les évaluations de P en des éléments de A^r fournissent des relations linéaires sur les coefficients. Choisies judicieusement, un nombre fini de telles relations permet souvent de déterminer les coefficients en question, en résolvant un système linéaire.
(2) Le théorème 1.4 est très utile (entre autres) en théorie de Galois et en théorie des nombres. Par exemple, si K est un corps et $P \in K[X]$ unitaire a pour racines $\alpha_1, \ldots, \alpha_r$ (dans une extension L de K), l'évaluation d'un polynôme symétrique à coefficients dans K en $\alpha_1, \ldots, \alpha_r$ peut se faire sans connaitre $\alpha_1, \ldots, \alpha_r$, et est un élément de K (et pas seulement de L). C'est notamment le cas du discriminant $\prod_{1 \leqslant i < j \leqslant r} (\alpha_j - \alpha_i)^2$.

(3) Soit k un corps. Comme $k[X_1, \ldots, X_r]$ est factoriel (*cf* corollaire 5.26), le théorème 1.4 s'étend aux fractions rationnelles : le groupe $\mathfrak{S}_r$ agit sur le corps $L := k(X_1, \ldots, X_r)$, et le sous-corps des invariants est $K := k(\sigma_1, \ldots, \sigma_r)$. L'extension L/K est galoisienne de groupe $\mathfrak{S}_r$ (Artin) ; c'est aussi l'extension de décomposition de $T^r - \sigma_1 T^{r-1} + \sigma_2 T^{r-2} + \cdots + (-1)^k \sigma_k T^{r-k} + \cdots + (-1)^r \sigma_r \in K[T]$ (*cf* proposition 1.3). Plus généralement, si G est un groupe d'ordre r, il existe un morphisme de groupes injectif (théorème de Cayley) : ce qui précède fournit une action de G sur L, et donc l'extension galoisienne L/L^G (Artin again). On voit donc que tout groupe fini peut être facilement vu comme un groupe de Galois. La *théorie de Galois inverse* a pour but, un corps de base K (typiquement $\mathbf{Q}$ ou un corps de nombres) et un groupe G étant fixés, de déterminer s'il est possible de trouver (voire d'expliciter) une extension galoisienne de K de groupe G. C'est en général très ardu (c'est un sujet de recherche).

Exemples 1.7. (1) $(X_1 - X_2)^2 = X_1^2 - 2X_1X_2 + X_2^2 = (\sigma_1^2 - 2X_1X_2 - X_2^2) - 2X_1X_2 + X_2^2 = \sigma_1^2 - 4\sigma_2$.
(2) $X_1^2 + X_2^2 + X_3^2 = (\sigma_1^2 - X_2^2 - X_3^2 - 2X_1X_2 - 2X_1X_3 - 2X_2X_3) + X_2^2 + X_3^2 = \sigma_1^2 - 2\sigma_2$.
(3) $\sum_{i \neq j} X_i^2 X_j = \begin{cases} \sigma_1\sigma_2 & \text{si } r = 2 \\ \sigma_1\sigma_2 - 3\sigma_3 & \text{si } r \geqslant 3 \end{cases}$.
(4) $X_1^2X_2^2 + X_1^2X_3^2 + X_2^2X_3^2 = \sigma_2^2 - 2(X_1X_2)(X_1X_3) - 2(X_1X_2)(X_2X_3) - 2(X_1X_3)(X_2X_3) = \sigma_2^2 - 2\sigma_1\sigma_3$.

Exercice 1.8. ∗∗ Montrer que $\sum_{i<j} X_i^2 X_j^2 = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4$.

Remarque. Pour $k \in \mathbf{N}_{>0}$, on pose

$$S_k = S_k(X_1, \ldots, X_r) = X_1^k + \cdots + X_r^k$$

(k-ième polynôme de Newton). Comme ce polynôme est symétrique, c'est un polynôme en $\sigma_1, \ldots, \sigma_r$ en vertu du théorème 1.4.

Proposition 1.9. (FORMULES DE NEWTON) *On a* $\begin{cases} S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - \cdots + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k k\sigma_k = 0 & \text{si } k \leqslant r \\ S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - \cdots + (-1)^{r-1}\sigma_{r-1}S_{k-r+1} + (-1)^r \sigma_r S_{k-r} = 0 & \text{si } k > r \end{cases}$.

Les formules de Newton permettent d'exprimer les S_k en fonction de $\sigma_1, \sigma_2, \ldots, \sigma_r$. Par exemple, on a

$$\begin{aligned} S_1 &= \sigma_1 \\ S_2 &= \sigma_1^2 - 2\sigma_2 \\ S_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \end{aligned}$$

Réciproquement, elles permettent d'exprimer les σ_k en fonction de $S_1, \ldots, S_r$. Remarquons néanmoins qu'il faut alors inverser les entiers $2, 3, \ldots, r$, de sorte que c'est possible si $r!$ est inversible dans l'anneau où l'on travaille.

$$\begin{aligned} \sigma_1 &= S_1 \\ \sigma_2 &= \tfrac{1}{2}(S_1^2 - S_2) \\ \sigma_3 &= \tfrac{1}{6}(S_1^3 - 3S_1S_2 + 2S_3) \end{aligned}$$

On s'en doute, des formules générales existent (ce sont les formules de Waring).

2 Notions de module sur un anneau

Soit A un anneau.

Définition 2.1. Un *A-module*[2] est la donnée d'un triplet $(M, +, \cdot)$ où $(M, +)$ est un groupe abélien et $\cdot : A \times M \to M$ une loi de composition externe vérifiant les propriétés suivantes :
(1) $(\forall a, b \in A)\ (\forall m \in M)\ (a + b) \cdot m = a \cdot m + b \cdot m$;
(2) $(\forall a, b \in A)\ (\forall m \in M)\ (ab) \cdot m = a \cdot (b \cdot m)$;
(3) $(\forall a \in A)\ (\forall m_1, m_2 \in M)\ a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$;
(4) $(\forall m \in M)\ 1 \cdot m = m$.
Les éléments de A s'appellent les *scalaires*. Comme d'habitude, on commettera systématiquement l'abus consistant à désigner un module par l'ensemble sous-jacent, en parlant du A-module M. En outre, on notera souvent am au lieu de $a \cdot m$.

Remarque. (1) Soit $(M, +)$ un groupe abélien. La donnée d'une structure de A-module sur M équivaut à celle d'un morphisme d'anneaux $A \to \mathsf{End}_{\mathsf{gr}}(M)$.
(2) On peut voir la notion de module comme une généralisation de celle d'espace vectoriel sur un corps. Il faut prendre garde toutefois que bon nombre de propriétés agréables des espaces vectoriels (l'existence de bases en particulier) sont compétement fausses pour les modules sur un anneau qui n'est pas un corps.

Exemples 2.2. (0) L'anneau A lui-même est un A-module, la loi externe étant donnée par le produit de A.
(1) Si A est un corps, un A-module n'est autre qu'un A-espace vectoriel.
(2) Un $\mathbf{Z}$-module n'est rien d'autre qu'un groupe abélien.
(3) Si K est un corps, un $K[X]$-module est un K-espace vectoriel muni d'un endomorphisme (qui correspond à la multiplication par X). On reviendra sur cette situation plus tard.
(4) Si $I \subset A$ est un idéal, alors I et A/I sont des A-modules.

Définition 2.3. Soient Λ un ensemble et $(M_\lambda)_{\lambda \in \Lambda}$ une famille de A-modules.
(1) On note $\prod_{\lambda \in \Lambda} M_\lambda$ l'ensemble produit. C'est l'ensemble des applications $f : \Lambda \to \bigcup_{\lambda \in \Lambda} M_\lambda$ telles que $f(\lambda) \in M_\lambda$ pour tout $\lambda \in \Lambda$. C'est un A-module, qu'on appelle le A-module *produit* des $(M_\lambda)_{\lambda \in \Lambda}$.
(2) On note $\bigoplus_{\lambda \in \Lambda} M_\lambda$ le sous-ensemble de $\prod_{\lambda \in \Lambda} M_\lambda$ constitué des fonctions $f : \Lambda \to \bigcup_{\lambda \in \Lambda} M_\lambda$ pour lesquelles l'ensemble $\{\lambda \in \Lambda\ ;\ f(\lambda) \neq 0\}$ est *fini*. C'est un A-module, qu'on appelle la *somme* des $(M_\lambda)_{\lambda \in \Lambda}$.
(3) Si tous de M_λ sont égaux à M, on note M^Λ et $M^{(\Lambda)}$ au lieu de $\prod_{\lambda \in \Lambda} M$ et $\bigoplus_{\lambda \in \Lambda} M$.

Remarque. (1) Si l'ensemble Λ est fini, les A-modules $\prod_{\lambda \in \Lambda} M_\lambda$ et $\bigoplus_{\lambda \in \Lambda} M_\lambda$ coïncident. C'est faux lorsque Λ est infini.
(2) Si $n \in \mathbf{N}$, on note M^n au lieu de $M^{\{1,\ldots,n\}}$.

2. Dans le cas d'un anneau non commutatif, il y a lieu de distinguer les notions de module à gauche et de module à droite. Conformément à la convention fixée en préambule, on ne rentrera pas dans ce genre de considérations. Cela ne signifie pas que la notion soit dépourvue d'intérêt lorsque A n'est pas commutatif, bien au contraire (elle apparaît naturellement, entre autres, dans l'étude des représentations linéaires des groupes).

Définition 2.4. Soit M un A-module. Un *sous-module*[3] de M est une partie $N \subset M$ stable par $+$ et par multiplication par les scalaires, *i.e.* telle que $(\forall a \in A)\ (\forall n_1, n_2 \in N)\ n_1 + an_2 \in N$.

Exemples 2.5. Les sous-modules de A ne sont autres que ses idéaux (à gauche). Si $(M_\lambda)_{\lambda\in\Lambda}$ une famille de A-modules, $\bigoplus_{\lambda\in\Lambda} M_\lambda$ est un sous-A-module de $\prod_{\lambda\in\Lambda} M_\lambda$.

Opérations sur les sous-modules d'un A-module. Soient M un A-module et $(M_\lambda)_{\lambda\in\Lambda}$ une famille de sous-modules de M. Alors l'intersection $\bigcap_{\lambda\in\Lambda} M_\lambda$ est un sous-module de M. Par ailleurs, on pose

$$\sum_{\lambda\in\Lambda} M_\lambda = \Big\{ \sum_{\lambda\in\Lambda} m_\lambda\,;\, (m_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} M_\lambda \Big\}$$

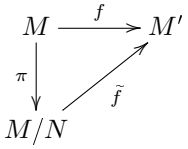
(l'ensemble des sommes *finies* d'éléments de $\bigcup_{\lambda\in\Lambda} M_\lambda$). C'est un sous-module de M, qu'on appelle la *somme* de $(M_\lambda)_{\lambda\in\Lambda}$.

Définition 2.6. Soit M un A-module.
(1) Soit $X \subset M$. Il existe un plus petit (au sens de l'inclusion) sous-A-module N de M tel que $X \subset N$. On l'appelle le sous-module de M *engendré* par X. Ce n'est autre que l'intersection des sous-modules de M qui contiennent X. C'est aussi la somme $\sum_{x\in X} Ax$ (où $Ax = \{ax\}_{a\in A}$).
(2) On dit qu'une partie $X \subset M$ *engendre* M, ou que c'est une *partie génératrice* de M si le sous-module de M engendré par X est M en entier.
(3) Le A-module M est dit *type fini* s'il contient une partie génératrice finie.
(4) Le A-module M est dit *noethérien* si tous ses sous-A-modules sont de type fini.

Remarque. Le fait d'être de type fini n'est pas stable par sous-objet (trouver un exemple), alors que c'est le cas pour la noethérianité : cela suggère que la « bonne » notion de finitude pour les modules (généralisant la notion de dimension finie pour les espaces vectoriels) est la noethérianité.

Définition 2.7. Soient M et N deux A-modules.
• Une *application A-linéaire* de M vers N est un morphisme de groupes $f\colon M \to N$ qui vérifie en outre $f(am) = af(m)$ pour tout $a \in A$ et $m \in M$. On note $\mathsf{Hom}_A(M,N)$ l'ensemble des applications A-linéaires de M dans N. C'est un A-module. On le note $\mathsf{End}_A(M)$ lorsque $M = N$.
• Le *noyau* de f est alors $\mathsf{Ker}(f) = f^{-1}(0)$, c'est un sous-$A$-module de M, et l'*image* de f est $\mathsf{Im}(f) = f(M)$, c'est un sous-A-module de N.
• On dit que f et un *isomorphisme* si f est bijective (l'application f^{-1} est alors A-linéaire). Cela équivaut à $\mathsf{Ker}(f) = \{0\}$ (*i.e.* f injective) et $\mathsf{Im}(f) = N$.

Définition 2.8. Soient M un A-module et N un sous-A-module. On dispose du groupe quotient M/N. Il est naturellement muni d'une structure de A-module (parce que si $m \in M$ et $a \in A$, on a $a(m+N) = am + aN \subset am + N$). Le A-module M/N s'appelle de A-module *quotient* de M par N. L'application canonique $\pi\colon M \to M/N; m \mapsto m+N$ est A-linéaire, et jouit de la propriété universelle suivante : pour toute application A-linéaire $f\colon M \to M'$ telle que $N \subset \mathsf{Ker}(f)$, il existe une unique application A-linéaire $\tilde{f}\colon M/N \to M'$ telle que $f = \tilde{f} \circ \pi$.



En particulier, si $f\colon M \to M'$ est un morphisme de A-modules, on dispose de la *décomposition canonique* $f = \iota \circ \tilde{f} \circ \pi$ où $\iota\colon \mathsf{Im}(f) \to M'$ est l'inclusion, $\tilde{f}$ un isomorphisme et $\pi\colon M \to M/\mathsf{Ker}(f)$ la projection canonique.

Définition 2.9. Soient M et N deux A-modules, et $f \in \mathsf{Hom}_A(M,N)$. Le *conoyau* de f est $\mathsf{Coker}(f) := N/\mathsf{Im}(f)$. Notons que f est surjective si et seulement si $\mathsf{Coker}(f) = \{0\}$.

Définition 2.10. (1) Un A-module *libre* est un A-module isomorphe au A-module $A^{(\Lambda)}$ pour un ensemble Λ convenable.
(2) Soit Λ un ensemble. Pour $\lambda \in \Lambda$, on définit $e_\lambda \in A^{(\Lambda)}$ par $e_\lambda(\eta) = \delta_{\lambda,\eta}$ (symbole de Kronecker, qui vaut 1 si $\lambda = \eta$ et 0 sinon). La famille $(e_\lambda)_{\lambda\in\Lambda}$ s'appelle la *base canonique* de $A^{(\Lambda)}$.

Proposition 2.11. *(1) Si $a \in A^{(\Lambda)}$, on a l'égalité $a = \sum_{\lambda\in\Lambda} a(\lambda)e_\lambda$ (la somme est finie).*
(2) Si M est un A-module, l'application A-linéaire

$$\begin{aligned}\mathsf{Hom}_A(A^{(\Lambda)}, M) &\to M^\Lambda \\ f &\mapsto (f(e_\lambda))_{\lambda\in\Lambda}\end{aligned}$$

est un isomorphisme. En d'autres termes, la donnée d'une application A-linéaire $f\colon A^{(\Lambda)} \to M$ équivaut à la donnée de la famille $(f(e_\lambda))_{\lambda\in\Lambda}$.

3. En fait on devrait dire *sous-A-module* (surtout si plusieurs anneaux interviennent). On omet la mention de l'anneau lorsqu'il n'y a pas d'ambiguité, comme ici.

Démonstration. (1) Pour $\eta \in \Lambda$, on a $\Big(\sum_{\lambda\in\Lambda} a(\lambda)e_\lambda\Big)(\eta) = a(\eta)$.

(2) Cela résulte de $f(a) = \sum_{\lambda\in\Lambda} a(\lambda)f(e_\lambda)$ pour tout $f \in \mathsf{Hom}_A(A^{(\Lambda)}, M)$ et $a \in A^{(\Lambda)}$ (égalité qui s'obtient par A-linéarité). □

Définition 2.12. D'après la proposition 2.11, un A-module M est libre si et seulement s'il existe une famille $(m_\lambda)_{\lambda\in\Lambda}$ d'éléments de M telle que tout élément $m \in M$ s'écrit de façon unique $m = \sum_{\lambda\in\Lambda} a_\lambda m_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Un telle famille $(m_\lambda)_{\lambda\in\Lambda}$ s'appelle une *base* de M (dans le cas où A est un corps, on retrouve la définition habituelle de base).

Remarque. Lorsque A est un corps, tout A-module est libre (tout espace vectoriel admet une base). Ce n'est plus du tout le cas pour un anneau quelconque. Par exemple, si $I \subset A$ est un idéal de A distinct de $\{0\}$ et de A, le A-module A/I n'est pas libre (si $e \in A/I$ et $a \in I\backslash\{0\}$, on a $ae = 0$). Par exemple, $\mathbf{Z}/2\,\mathbf{Z}$ est un $\mathbf{Z}/4\,\mathbf{Z}$ module, mais il n'est pas libre. On peut montrer (mais ça n'est pas évident) que $\mathbf{Z}^{\mathbf{N}}$ n'est pas libre sur $\mathbf{Z}$.

Proposition 2.13. *Les bases d'un module libre ont toutes même cardinal*[4].

Démonstration. Il s'agit de montrer que si Λ et Λ' sont des ensembles tels que les A-modules $A^{(\Lambda)}$ et $A^{(\Lambda')}$ sont isomorphes, alors Λ et Λ' ont même cardinal. Soit $f\colon A^{(\Lambda)} \to A^{(\Lambda')}$ un isomorphisme, et $\mathfrak{m} \subset A$ un idéal maximal de A (il en existe en vertu du théorème de Krull), de sorte que $A/\mathfrak{m}$ est un corps. D'après la proposition 2.11 (2), f correspond à la donnée de $(f(e_\lambda))_{\lambda\in\Lambda} \in \big(A^{(\Lambda')}\big)^{\Lambda}$ (où $(e_\lambda)_{\lambda\in\Lambda}$ désigne la base canonique de $A^{(\Lambda)}$). Si I est un ensemble, la surjection canonique $\pi\colon A \to A/\mathfrak{m}$ induit un morphisme A-linéaire surjectif $\pi_I\colon A^{(I)} \to (A/\mathfrak{m})^{(I)}$. De même, elle induit un morphisme A-linéaire surjectif $\widetilde{\pi}\colon \big(A^{(\Lambda')}\big)^{\Lambda} \to \big((A/\mathfrak{m})^{(\Lambda')}\big)^{\Lambda}$: notons $\overline{f} \in \mathsf{Hom}_{A/\mathfrak{m}}\big((A/\mathfrak{m})^{(\Lambda)}, (A/\mathfrak{m})^{(\Lambda')}\big)$ l'application $A/\mathfrak{m}$-linéaire correspondant à $\widetilde{\pi}\big((f(e_\lambda))_{\lambda\in\Lambda}\big)$. Elle s'insère dans le carré commutatif :

$$\begin{array}{ccc} A^{(\Lambda)} & \xrightarrow{\ f\ } & A^{(\Lambda')} \\ {\scriptstyle \pi_\Lambda}\downarrow & & \downarrow{\scriptstyle \pi_{\Lambda'}} \\ (A/\mathfrak{m})^{(\Lambda)} & \xrightarrow{\ \overline{f}\ } & (A/\mathfrak{m})^{(\Lambda')} \end{array}$$

Posons $g = f^{-1}\colon A^{(\Lambda')} \to A^{\Lambda)}$: on dispose du morphisme induit $\overline{g}\colon (A/\mathfrak{m})^{(\Lambda')} \to (A/\mathfrak{m})^{(\Lambda)}$. Comme $g \circ f = \mathsf{Id}_{A^{(\Lambda)}}$ et $f \circ g = \mathsf{Id}_{A^{(\Lambda')}}$, on a $\overline{g} \circ \overline{f} = \mathsf{Id}_{(A/\mathfrak{m})^{(\Lambda)}}$ et $\overline{f} \circ \overline{g} = \mathsf{Id}_{(A/\mathfrak{m})^{(\Lambda')}}$, ce qui montre que $\overline{f}$ est un isomorphisme $A/\mathfrak{m}$-linéaire. Les $A/\mathfrak{m}$-espaces vectoriels $(A/\mathfrak{m})^{(\Lambda)}$ et $(A/\mathfrak{m})^{(\Lambda')}$ sont isomorphes, on a donc $\mathsf{Card}(\Lambda) = \mathsf{Card}(\Lambda')$. □

Définition 2.14. D'après la proposition précédente, si M est isomorphe à A^n avec $n \in \mathbf{N}$, l'entier n est un invariant de M, qu'on appelle le *rang* de M.

Remarque. (1) Si M et N sont deux A-modules libres de rangs respectifs m et n, il résulte de la proposition 2.11 (2), après le choix de bases dans M et dans N, que

$$\mathsf{Hom}_A(M, N) \simeq \mathsf{Hom}_A(A^m, A^n) = \mathsf{M}_{n\times m}(A).$$

Comme pour les espaces vectoriels de dimension finie, après le choix de bases, la donnée d'une application A-linéaire entre deux A-modules libres de rang fini équivaut à celle de sa matrice dans ces bases.
(2) Soient M un A-module et $\{m_\lambda\}_{\lambda\in\Lambda}$ une famille d'éléments de M. D'après la proposition 2.11 (2), il existe une unique application A-linéaire $f\colon A^{(\Lambda)} \to M$ telle que $f(e_\lambda) = m_\lambda$ pour tout $\lambda \in \Lambda$.
Le A-module $\mathsf{Im}(f)$ est le sous-module de M engendré par $\{m_\lambda\}_{\lambda\in\Lambda}$. En particulier, la famille $\{m_\lambda\}_{\lambda\in\Lambda}$ est génératrice si f est surjective, et c'est une base si f est un isomorphisme. Lorsque f est injective, on dit que $\{m_\lambda\}_{\lambda\in\Lambda}$ est *libre*.

Proposition 2.15. *(1) Soit M un A-module. Alors M est noethérien si et seulement si toute suite croissante de sous-modules de M est stationnaire.*
(2) Soient M un A-module et N un sous-A-module de M. Alors M est noethérien si et seulement si les A-modules N et M/N sont noethériens.

Démonstration. (1) • Supposons M noethérien, et soit $(M_n)_{\in\mathbf{N}}$ une suite croissante de sous-modules de M. Comme le sous-module $\sum_{n\in\mathbf{N}} M_n$ est de type fini, il existe $m_1, \dots, m_r \in M$ tels qu'il soit engendré par $\{m_1, \dots, m_r\}$. Comme la réunion est croissante, il existe $N \in \mathbf{N}$ tel que $\{m_1, \dots, m_r\} \subset M_N$. On a alors $M_N \subset \sum_{n\in\mathbf{N}} M_n \subset M_N$ et donc $\sum_{n\in\mathbf{N}} M_n = M_N$, et $M_n = M_N$ pour tout $n \geqslant N$: la suite $(M_n)_{\in\mathbf{N}}$ est stationnaire.

4. Observons que la commutativité de A est cruciale : si R est un anneau commutatif (unitaire), notons $(e_k)_{k\in\mathbf{N}}$ la base canonique que $L := R^{(\mathbf{N})}$ et posons $A = \mathsf{End}_R(L)$. Comme on l'a vu dans la proposition 2.11 (2), la donnée d'un élément $f \in A$ équivaut à celle de $(f(e_k))_{k\in\mathbf{N}} \in L^{\mathbf{N}}$. En particulier, on dispose de $f_1, f_2 \in A$ définis par $f_1(e_k) = \begin{cases} e_{k/2} & \text{si } k \text{ est pair} \\ 0 & \text{sinon} \end{cases}$ et $f_2(e_k) = \begin{cases} e_{(k-1)/2} & \text{si } k \text{ est impair} \\ 0 & \text{sinon} \end{cases}$ respectivement. Il est alors facile (exercice) de voir que $A = Af_1 \oplus Af_2$, ce qui montre que $A \simeq A^2$ comme A-modules à gauche : par induction, on a $A \simeq A^r$ (comme A-modules à gauche) pour tout $r \in \mathbf{N}_{>0}$, ce qui montre que la notion de rang n'a pas de sens dans ce cas.

• Supposons M non noethérien : il existe un sous-A-module M' qui n'est pas de type fini. On construit par récurrence une suite *strictement* croissante de sous-modules de type fini de M' de la façon suivante : on pose $M'_0 = \{0\}$, et si M'_n est construit, il est distinct de M' (puisque M'_n est de type fini et M' ne l'est pas) : soient $m_n \in M' \backslash M'_n$ et $M'_{n+1} = M'_n + Am_{n+1}$. On a $M'_n \subsetneq M'_{n+1} \subset M'$.

(2) • Si M est noethérien, alors N est de type fini. Par ailleurs, si N' est un sous-module de M/N, on a $N' = \widetilde{N}/N$ avec $\widetilde{N} = \pi^{-1}(N')$ (où $\pi\colon M \to M/N$ est la projection canonique). Comme M est noethérien, $\widetilde{N}$ est de type fini, c'est *a fortiori* de cas de $N' = \widetilde{N}/N$, et M/N est noethérien.

• Supposons N et M/N noethériens. Soit $(M_n)_{n\in\mathbf{N}}$ une suite croissante de sous-modules de M. On dispose des suites croissantes $(M_n \cap N)_{n\in\mathbf{N}}$ et $((N + M_n)/N)_{n\in\mathbf{N}}$ de sous-A-modules de N et de M/N respectivement. Comme ces derniers sont noethériens, ces suites sont stationnaires : il existe $n_0 \in \mathbf{N}$ tel que pour $n \geqslant n_0$, on a $M_n \cap N = M_{n_0} \cap N$ et $(N + M_n)/N = (N + M_{n_0})/N$ *i.e.* $N + M_n = N + M_{n_0}$. Si $m \in M_n$, il existe donc $x \in N$ et $y \in M_{n_0} \subset M_n$ tels que $m = x + y$. Comme $x = y - m \in N \cap M_n = N \cap M_{n_0}$, on a $m \in M_{n_0}$, d'où $M_n \subset M_{n_0}$ *i.e.* $M_n = M_{n_0}$. Le A-module M est donc noethérien. □

Corollaire 2.16. *Si M_1 et M_2 sont deux A-modules noethériens, le A-module produit $M_1 \times M_2$ est noethérien.*

Démonstration. Les modules $M_1 \simeq M_1 \times \{0\}$ et $M_2 \simeq (M_1 \times M_2)/(M_1 \times \{0\})$, étant noethériens, cela résulte de la proposition 2.15 (2). □

Définition 2.17. L'anneau A est dit *noethérien* s'il est noethérien vu comme A-module. Par définition, cela signifie que tout idéal de A est de type fini. En vertu de la proposition 2.15, cela équivaut au fait que toute suite croissante d'idéaux de A est stationnaire.

Proposition 2.18. *Si A est noethérien, tout A-module de type fini est noethérien.*

Démonstration. Soit M un A-module de type fini : il existe $n \in \mathbf{N}$ et une application A-linéaire surjective $f\colon A^n \to M$. Comme A est noethérien, il en est de même de A^n (corollaire 2.16), et de $M = A^n/\operatorname{Ker}(f)$ (proposition 2.15 (2)). □

Théorème 2.19. (HILBERT) *Si A est un anneau noethérien, alors $A[X]$ est noethérien.*

Démonstration. Soit $I \subset A[X]$ un idéal : montrons qu'il est de type fini. On peut supposer $I \neq \{0\}$. Pour $n \in \mathbf{N}$, notons $A_{\leqslant n}[X]$ le sous-module de $A[X]$ constitué des polynômes de degré inférieur à n (il est libre de base $(1, X, X^2, \ldots, X^n)$), et J_n l'ensemble des coefficients de X^n des éléments de $I \cap A_{\leqslant n}[X]$: c'est aussi $\{0\}$ union l'ensemble des coefficients dominants des éléments de I qui sont de degré n. Comme $I \subset A[X]$ est un idéal, $I \cap A_{\leqslant n}[X]$ est un sous-module de $A_{\leqslant n}[X]$, donc J_n est un idéal de A. En outre, si $n \leqslant m$ et $\alpha \in J_n \backslash \{0\}$ (de sorte qu'il existe $P \in I$ de degré n de coefficient dominant égal à α), alors $\alpha \in J_m$ (c'est le coefficient dominant du polynôme $X^{m-n}P$). La suite d'idéaux $(J_n)_{n\in\mathbf{N}}$ est donc croissante. Comme A est noethérien, elle est stationnaire : soit $d \in \mathbf{N}_{>0}$ tel que $n \geqslant d \Rightarrow J_n = J_d$. Comme A est noethérien, l'idéal J_d est de type fini : choisissons $\alpha_1, \ldots, \alpha_r$ des générateurs de J_d. Comme $I \neq \{0\}$, on a $J_d \neq \{0\}$, et on peut supposer $\alpha_1, \ldots, \alpha_r$ tous non nuls. Pour tout $i \in \{1, \ldots, r\}$, choisissons $P_i \in I$ de degré d et de coefficient dominant α_i. Par ailleurs, le A-module $A_{\leqslant d-1}[X]$ est de type fini, donc noethérien (*cf* proposition 2.18) : son sous-module $M := I \cap A_{\leqslant d-1}[X]$ est de type fini. Choisissons des générateurs $Q_1, \ldots, Q_s$ de M. On a bien sûr

$$\langle P_1, \ldots, P_r, Q_1, \ldots, Q_s\rangle \subset I.$$

Montrons l'inclusion réciproque, *i.e.* que tout $P \in I$ appartient à $\langle P_1, \ldots, P_r, Q_1, \ldots, Q_s\rangle$. On procède par récurrence sur $n = \deg(P)$. Si $n < d$, on a $P \in M = \langle Q_1, \ldots, Q_s\rangle \subset \langle P_1, \ldots, P_r, Q_1, \ldots, Q_s\rangle$. Supposons $n \geqslant d$. Le coefficient dominant α de P appartient à J_d : il existe $a_1, \ldots, a_r \in A$ tels que $\alpha = a_a\alpha_1 + \cdots + a_r\alpha_r$. Le polynôme $P - \sum_{i=1}^{r} a_i X^{n-d} P_i \in I$ est de degré $< n$, et c'est un élément de I : par hypothèse de récurrence, il appartient à $\langle P_1, \ldots, P_r, Q_1, \ldots, Q_s\rangle$, ce qui prouve que $P \in \langle P_1, \ldots, P_r, Q_1, \ldots, Q_s\rangle$. Ainsi, l'idéal I est de type fini, et $A[X]$ est noethérien. □

Corollaire 2.20. *Soient A un anneau noethérien et B une A-algèbre*[5] *de type fini. Alors B est un anneau noethérien.*

Démonstration. Comme B est de type fini, il existe $b_1, \ldots, b_r \in B$ tels que $B = A[b_1, \ldots, b_r]$: on dispose du morphisme de A-algèbres $f\colon A[X_1, \ldots, X_r] \to B$ défini par $f(X_i) = b_i$ pour $i \in \{1, \ldots, r\}$. Il est surjectif : si $I = \operatorname{Ker}(f)$, on a $B \simeq A[X_1, \ldots, X_r]/I$. Comme A est noethérien, il en est de même de $A[X_1, \ldots, X_r]$ (en appliquant r fois le théorème 2.19), et donc de B (le idéaux de ce derniers sont isomorphes à des quotients d'idéaux de $A[X_1, \ldots, X_r]$). □

Définition 2.21. (1) Soient M un A-module et $m \in M$. On pose $\operatorname{ann}_A(m) = \{a \in A,\ am = 0\}$. C'est un idéal (à gauche) de A, appelé *idéal annulateur* de m. On dit que m est de *torsion* si $\operatorname{ann}_A(m) \neq \{0\}$, *i.e.* s'il existe $a \in A\backslash\{0\}$ tel que $am = 0$. On note M_{tors} l'ensemble des éléments de M qui sont de torsion. On dit que M est *sans torsion* (resp. *de torsion*) si $M_{\text{tors}} = \{0\}$ (resp. $M_{\text{tors}} = M$).

(2) On pose $\operatorname{ann}_A(M) = \{a \in A\,;\ (\forall m \in M)\ am = 0\} = \bigcap_{m\in M} \operatorname{ann}_A(m)$. C'est un idéal de A, appelé *idéal annulateur* de M. On en déduit une structure de $A/\operatorname{ann}_A(M)$-module sur M. Remarquons que M peut-être de torsion même si $\operatorname{ann}_A(M) = \{0\}$: par exemple, on a $\operatorname{ann}_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z}) = \{0\}$.

5. Cela signifie simplement que B est un anneau muni d'un morphisme d'anneaux $A \to B$.

Exemple 2.22. Si $I \subset A$ est un idéal non nul, A/I est de torsion. Par exemple, $\mathbf{Z}/2\,\mathbf{Z}$ est un $\mathbf{Z}/6\,\mathbf{Z}$-module de torsion. De même, $\mathbf{Q}/\mathbf{Z}$ est un $\mathbf{Z}$-module de torsion.

Proposition 2.23. *Supposons A commutatif, intègre et soit M un A-module. Alors M_{tors} est un sous-module de M et le A-module quotient M/M_{tors} est sans torsion.*

Démonstration. Si $m_1, m_2 \in M_{\mathrm{tors}}$ et $\alpha \in A$, il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1 m_1 = 0$ et $a_2 m_2 = 0$. Comme A est intègre, on a $a_1 a_2 \neq 0$ et $a_1 a_2(m_1 + \alpha m_2) = 0$ implique $m_1 + \alpha m_2 \in M_{\mathrm{tors}}$.
Soit $m \in M$ dont l'image $m + M_{\mathrm{tors}}$ est de torsion dans M/M_{tors} : il existe $a \in A\backslash\{0\}$ tel que $am + M_{\mathrm{tors}} = M_{\mathrm{tors}}$ *i.e.* $am \in M_{\mathrm{tors}}$. Il existe donc $b \in A\backslash\{0\}$ tel que $b(am) = 0$. Comme A est intègre, on a $ab \neq 0$, et $m \in M_{\mathrm{tors}}$. □

Remarque. (1) Ce qui précède tombe en défaut si A n'est pas supposé intègre. Par exemple, si $A = M = \mathbf{Z} \times \mathbf{Z}$, alors $M_{\mathrm{tors}} = (\mathbf{Z} \times \{0\}) \cup (\{0\} \times \mathbf{Z})$ n'est pas un sous-module de M.
(2) Un A-module libre est sans torsion, mais la réciproque est fausse en général (elle est valide dans le cas des modules de type fini sur un anneau principal, *cf* corollaire 6.10).

Exercice 2.24. ∗∗∗ Soient A un anneau unitaire, M un A-module noethérien et $f : M \to M$ une application A-linéaire.
(1) On suppose f surjective. Montrer que c'est un isomorphisme (indication : considérer les sous-modules $K_n = \mathsf{Ker}(f^n)$).
(2) Si f est supposée injective, est-ce automatiquement un isomorphisme ?
On suppose désormais que $M = A^n$ et on note $X = (x_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ la matrice de f dans la base canonique.
(3) Montrer que f est surjective si et seulement si $\det(X) \in A^\times$.
(4) Montrer que si $\det(X)$ n'est pas diviseur de zéro dans A, alors f est injective.
(5) Montrer que réciproquement, si $\det(X)$ est diviseur de zéro dans A, alors f n'est pas injective (indication : soient $a \in A\backslash\{0\}$ tel que $a \det(X) = 0$ et $r < n$ le plus grand entier tel qu'il existe une matrice $N \in \mathsf{M}_r(A)$ extraite de M telle que $a \det(N) \neq 0$, construire $V \in A^n\backslash\{0\}$ tel que $XV = 0$ à partir d'une telle matrice N).
On suppose désormais que f est injective.
(6) Lorsque $A = \mathbf{Z}$, montrer que $\#\,\mathsf{Coker}(f) = |\det(X)|$.
(7) Montrer qu'on a $\dim_K(\mathsf{Coker}(f)) = \deg(\det(X))$ lorsque $A = K[X]$ (où K est un corps commutatif).

3 Le produit tensoriel

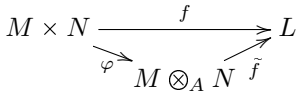
Soient M et N deux A-modules.

Définition 3.1. Soit L un A-module. Une application $f : M \times N \to L$ est dite *bilinéaire* si elle vérifie les conditions suivantes :

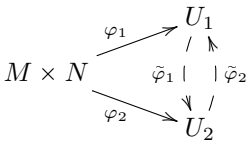
(i) f est linéaire à gauche, *i.e.* $(\forall a \in A)\,(\forall m_1, m_2 \in M)\,(\forall n \in N)\, f(am_1 + m_2, n) = af(m_1, n) + f(m_2, n)$;
(ii) f est linéaire à droite, *i.e.* $(\forall a \in A)\,(\forall m \in M)\,(\forall n_1, n_2 \in N)\, f(m, an_1 + n_2) = af(m, n_1) + f(m, n_2)$.

L'ensemble $\mathsf{Bil}_A(M, N, L)$ des applications bilinéaires $M \times N \to L$ est un A-module.

Proposition 3.2. *Il existe un couple $(M \otimes_A N, \varphi)$ où $M \otimes_A N$ est un A-module et $\varphi : M \times N \to M \otimes_A N$ une application bilinéaire, ayant la propriété universelle suivante : si $f : M \times N \to L$ est une application bilinéaire, il existe une unique application A-linéaire $\tilde{f} : M \otimes_A N \to L$ telle que $f = \tilde{f} \circ \varphi$.*



Démonstration. • Unicité à isomorphisme près [6]. Soient (U_1, φ_1) et (U_2, φ_2) deux couples ayant la propriété universelle requise. Par universalité, il existe $\tilde{\varphi}_1 : U_2 \to U_1$ et $\tilde{\varphi}_2 : U_1 \to U_2$ uniques tels que $\varphi_1 = \tilde{\varphi}_1 \circ \varphi_2$ et $\varphi_2 = \tilde{\varphi}_2 \circ \varphi_1$. On a alors $\varphi_1 = \tilde{\varphi}_1 \circ \tilde{\varphi}_2 \circ \varphi_1$: par universalité, on a $\tilde{\varphi}_1 \circ \tilde{\varphi}_2 = \mathsf{Id}_{U_1}$. On a de même $\tilde{\varphi}_2 \circ \tilde{\varphi}_1 = \mathsf{Id}_{U_2}$, ce qui montre que $\tilde{\varphi}_1$ et $\tilde{\varphi}_2$ sont des isomorphismes inverses l'un de l'autre.



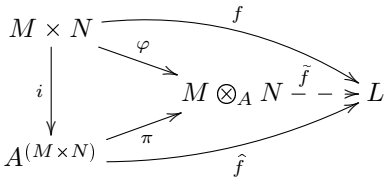
• Considérons le A-module $A^{(M \times N)}$ des fonctions $M \times N \to A$ à support fini. On dispose de la base canonique $\left(e_{(m,n)}\right)_{(m,n) \in M \times N}$. Notons K le sous-module de $A^{(M \times N)}$ engendré par les éléments suivants :

- $e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}$ pour $m_1, m_2 \in M$ et $n \in N$;
- $e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$ pour $m \in M$ et $n_1, n_2 \in N$;
- $e_{(am,n)} - ae_{(m,n)}$ et $e_{(m,an)} - ae_{(m,n)}$ pour $a \in A$, $m \in M$ et $n \in N$.

Posons $M \otimes_A N = A^{(M \times N)}/K$. C'est un A-module. Posons $i : M \times N \to A^{(M \times N)}; (m, n) \mapsto e_{(m,n)}$ (notons que i n'est pas A-linéaire) et notons $\pi : A^{(M \times N)} \to M \otimes_A N$ la surjection canonique. On pose $\varphi = \pi \circ i$: par définition de K, l'application φ est bilinéaire. Si maintenant $f : M \times N \to L$ est bilinéaire, on définit l'application A-linéaire $\widehat{f} : A^{(M \times N)} \to L$ en posant $\widehat{f}(e_{(m,n)}) = f(m, n)$ pour tout $m \in M$ et $n \in N$. Comme f est bilinéaire, on a $K \subset \mathsf{Ker}(\widehat{f})$:

6. La preuve qui suit, formelle, est valable pour toute solution d'un problème universel.

l'application $\widehat{f}$ se factorise par une application $\widetilde{f}\colon M \otimes_A N \to L$, de sorte que $f = \widetilde{f} \circ \varphi$ (on a $\widetilde{f}(\pi(e_{(m,n)})) = f(m,n)$ pour tout $m \in M$ et $n \in N$).



□

Remarque. (1) Une reformulation de la propriété universelle du produit tensoriel est

$$\mathsf{Bil}(M,N,L) \simeq \mathsf{Hom}_A(M, \mathsf{Hom}_A(N,L)) \simeq \mathsf{Hom}_A(M \otimes_A N, L)$$

(2) Si M est un A-module et B une A-algèbre (*i.e.* on a un morphisme d'anneaux $A \to B$, qui fait de B un A-module), alors $B \otimes_A M$ est muni d'une structure de B-module (changement de base).

Notation. Avec les notations de la preuve de la proposition 3.2, on pose $m \otimes n = \pi(e_{(m,n)}) \in M \otimes_A N$ pour tout $m \in M$ et $n \in N$. Les éléments de $M \otimes_A N$ de cette forme s'appellent les *tenseurs simples*. Ils engendrent $M \otimes_A N$, mais en général, les éléments de $M \otimes_A N$ ne sont pas tous des tenseurs simples.

Proposition 3.3. *Si M est libre de base $(e_\lambda)_{\lambda\in\Lambda}$, alors $M \otimes_A N \simeq N^{(\Lambda)}$. En particulier, si N est libre lui aussi, de base $(f_\delta)_{\delta\in\Delta}$, alors $M \otimes_A N$ est libre, de base $(e_\lambda \otimes f_\delta)_{(\lambda,\delta)\in\Lambda\times\Delta}$.*

Démonstration. Fixons un isomorphisme $M \xrightarrow{\sim} A^{(\Lambda)}$. Si L est un A-module, on a des isomorphismes naturels

$$\begin{aligned}\mathsf{Bil}(M,N,L) &\simeq \mathsf{Hom}_A(M, \mathsf{Hom}_A(N,L)) \\ &\simeq \mathsf{Hom}_A(A^{(\Lambda)}, \mathsf{Hom}_A(AN, L)) \\ &\simeq \mathsf{Hom}_A(N,L)^\Lambda \\ &\simeq \mathsf{Hom}_A(N^{(\Lambda)}, L)\end{aligned}$$

(*cf* proposition 2.11 (2)), ce qui prouve que $N^{(\Lambda)}$ a la propriété universelle de $M \otimes_A N$: ils sont isomorphes. Plus précisément, on a $M \otimes_A N \simeq \bigoplus_{\lambda\in\Lambda} Ae_\lambda \otimes_A N$: la deuxième partie de la proposition en résulte. □

Remarque. (1) Fonctorialité du produit tensoriel. Soient $f\colon M \to M'$ et $g\colon N \to N'$ deux applications A-linéaires. Elles induisent l'application $M \times N \to M' \otimes_A N'$; $(m,n) \mapsto f(m) \otimes g(n)$. Cette dernière est bilinéaire : elle se factorise de façon unique par une application A-linéaire

$$f \otimes g\colon M \otimes_A N \to M' \otimes_A N'$$

En particulier, si $f\colon M \to M'$ est A-linéaire et N un A-module, on a une application $M \otimes_A N \xrightarrow{f\otimes 1} M' \otimes_A N$. Un cas particulier important est le changement de base : si B est une A-algèbre, f induit une application B-linéaire $B \otimes_A M \to B \otimes_A M'$.

(2) Bien entendu, si $f\colon M \to M'$ est un isomorphisme, alors $M \otimes_A N \xrightarrow{f\otimes 1} M' \otimes_A N$ est un isomorphisme. Par contre, si f est seulement supposé injectif, alors $M \otimes_A N \xrightarrow{f\otimes 1} M' \otimes_A N$ n'est pas injectif en général (trouver des exemples). Par contre, la surjectivité est conservée, mieux, on a $\mathsf{Coker}(f \otimes 1) \simeq \mathsf{Coker}(f) \otimes_A N$ (exercice).

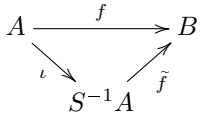
Exercices 3.4. $*$ (1) Montrer que $M \otimes_A N \simeq N \otimes_A M$.
(2) Montrer que $(\mathbf{Z}/a\,\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/b\,\mathbf{Z}) \simeq \mathbf{Z}/\,\mathsf{pgcd}(a,b)\,\mathbf{Z}$.
(3) Montrer que $\mathbf{C} \otimes_{\mathbf{C}} \mathbf{C} \to \mathbf{C}$; $z_1 \otimes z_2 \mapsto z_1 z_2$ et $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \to \mathbf{C}^2$; $z_1 \otimes z_2 \mapsto (z_1 z_2, z_1 \overline{z}_2)$ sont des isomorphismes.
(4) Soient K un corps, V un K-espace vectoriel et $V^\vee = \mathsf{Hom}_K(V,K)$ son dual. L'application $V \otimes_K V^\vee \to \mathsf{End}_K(V)$ qui à $v \otimes \alpha$ (avec $v \in V$ et $\alpha \in V^\vee$) associe l'endomorphisme (de rang 1) donné par $x \mapsto \alpha(x)v$ est un isomorphisme. De plus, l'application $V \otimes_K V^\vee \to K$; $v \otimes \alpha \mapsto \alpha(v)$ correspond, *via* cet isomorphisme, à la trace $\mathsf{Tr}\colon\ \mathsf{End}_K(V) \to K$.

4 Localisation

Définition 4.1. Une partie $S \subset A$ est dit *multiplicative* si $0 \notin S$, $1 \in S$ et si S est stable par multiplication.

Exemple 4.2. (1) $A^\times$.
(2) $\{f^n\}_{n\in\mathbf{Z}_{\geqslant 0}}$ où $f \in A$ n'est pas nilpotent.
(3) $A\backslash\mathfrak{p}$ où $\mathfrak{p} \subset A$ est un idéal premier.

Proposition 4.3. *Soit $S \subset A$ une partie multiplicative. Il existe une A-algèbre $A \xrightarrow{\iota} S^{-1}A$, unique à isomorphisme près, possédant la propriété universelle suivante : si $f\colon A \to B$ est un homomorphisme d'anneaux tel que $(\forall s \in S)\ f(s) \in B^\times$, alors il existe un unique homomorphisme d'anneaux $\widetilde{f}\colon S^{-1}A \to B$ tel que $f = \widetilde{f} \circ \iota$.*



Démonstration. On munit l'ensemble $A \times S$ de la relation binaire $\sim$ définie par

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow (\exists t \in S)\ t(a_1 s_2 - a_2 s_1) = 0$$

Il s'agit d'une relation d'équivalence. Notons $S^{-1}A = (A \times S)/\sim$ l'ensemble quotient. Si $(a, s) \in A \times S$, on note $\frac{a}{s}$ son image dans $S^{-1}A$. Soit $(a_1, s_1), (a_2, s_2) \in A \times S$. On vérifie facilement que les éléments $\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$ et $\frac{a_1}{s_1} . \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}$ dépendent seulement des classes $\frac{a_1}{s_1}$ et $\frac{a_2}{s_2}$ (et pas des représentants (a_1, s_1) et (a_2, s_2)), et que ceci définit deux lois internes $+$ et $.$ sur $S^{-1}A$, faisant de $S^{-1}A$ un anneau commutatif d'unité $\frac{1}{1}$. En outre, l'application

$$\begin{aligned} \iota\colon A &\to S^{-1}A \\ a &\mapsto \tfrac{a}{1} \end{aligned}$$

est un homomorphisme d'anneaux. Notons que si $s \in S$, alors $\iota(s) = \frac{s}{1}$ est inversible dans $S^{-1}A$, d'inverse $\frac{1}{s}$.
Soit $f\colon A \to B$ un homomorphisme d'anneaux tel que $(\forall s \in S)\ f(s) \in B^\times$. L'application

$$\begin{aligned} \widetilde{f}\colon S^{-1}A &\to B \\ \tfrac{a}{s} &\mapsto f(s)^{-1} f(a) \end{aligned}$$

est un homomorphisme d'anneaux bien défini, et c'est l'unique tel que $f = \widetilde{f} \circ \iota$. L'unicité à isomorphisme près de $(S^{-1}A, \iota)$ résulte de la propriété universelle. □

Définition 4.4. La A-algèbre $S^{-1}A$ est la *localisation* de A par rapport à l'ensemble multiplicatif S.

Remarque. (1) Comme d'habitude, si $a \in A$, on écrira a au lieu de $\iota(a)$ son image dans $S^{-1}A$ (c'est un peu abusif, parce que l'application ι n'est pas injective en général).
(2) Dans un certain sens, $S^{-1}A$ est la A-algèbre « minimale » dans laquelle les images des éléments de S sont inversibles.
(3) Lorsque A est intègre, $\sim$ est la relation « habituelle » $(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$. Lorsque A n'est pas intègre, cette dernière n'est pas une relation d'équivalence (pourquoi ?), et le « t » est nécessaire.
(4) $\mathsf{Ker}(\iota) = \{a \in A\,;\ (\exists s \in S)\ sa = 0\}$, donc ι est injectif lorsque A est intègre.
(5) À moins que A ne soit factoriel (*cf* plus bas), il n'y a pas de notion de « fraction irréductible ».

Exemple 4.5. (1) Supposons A soit intègre. Alors $A\backslash\{0\}$ est multiplicatif ($\{0\}$ est premier), et $(A\backslash\{0\})^{-1}A = \mathsf{Frac}(A)$ est le *corps de fractions* de A. Par exemple, $\mathsf{Frac}(\mathbf{Z}) = \mathbf{Q}$, et $\mathsf{Frac}(K[X]) = K(X)$ lorsque K est un corps.
Si de plus $S \subset A$ est un ensemble multiplicatif, la propriété universelle fournit un homomorphisme d'anneau injectif $S^{-1}A \to \mathsf{Frac}(A)$: les localisations de A s'identifient à des sous-anneaux de $\mathsf{Frac}(A)$.
(2) Plus généralement, si on ne suppose pas A intègre, la partie $S = \{f \in A\,;\ f$ n'est pas un diviseur de zéro dans $A\} \subset A$ est multiplicative. Dans ce cas la localisation $Q(A) := S^{-1}A$ est appelée *anneau total des fractions* de A.
(3) Soit $f \in A$. On note $A_{(f)}$ la localisation de A par rapport à l'ensemble multiplicatif $\{f^n\}_{n \in \mathbf{Z}_{\geqslant 0}}$. On montre facilement que $A_{(f)} \simeq A[X]/\langle fX - 1\rangle$. Par exemple, $\mathbf{Z}_{(10)}$ n'est rien d'autre que l'anneau des nombres décimaux.
(4) Si $\mathfrak{p} \subset A$ est un idéal premier, on note $A_\mathfrak{p}$ la localisation de A par rapport à l'ensemble multiplicatif $A\backslash\mathfrak{p}$. Lorsque A est intègre et $\mathfrak{p} = \{0\}$, on retrouve $\mathsf{Frac}(A)$.

Exercice 4.6. Trouver des ensembles multiplicatifs $S \subset \mathbf{Z}$ autres que $\mathbf{Z}\backslash\{0\}$ tels que $S^{-1}\mathbf{Z} = \mathbf{Q}$.

Définition 4.7. Soient $S \subset A$ une partie multiplicative et M un A-module. La *localisation* $S^{-1}M$ de M par rapport à S est définie de façon similaire à $S^{-1}A$: c'est le quotient de l'ensemble $M \times S$ par la relation d'équivalence donnée par $(m_1, s_1) \sim (m_2, s_2) \Leftrightarrow (\exists t \in S)\ t(m_1 s_2 - m_2 s_1) = 0$. C'est un $S^{-1}A$-module pour les lois $\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}$ et $\frac{a}{s} . \frac{m}{s'} := \frac{am}{ss'}$. Toute application A-linéaire $f\colon M \to N$ induit une application $S^{-1}A$-linéaire $f_S\colon S^{-1}M \to S^{-1}N$ (telle que $f_S\left(\frac{m}{s}\right) = \frac{f(m)}{s}$ pour tout $m \in M$ et $s \in S$). Elle a la propriété suivante : pour tout $S^{-1}A$-module N, l'application naturelle

$$\mathsf{Hom}_{S^{-1}A}(S^{-1}M, N) \to \mathsf{Hom}_A(M, N)$$

est un isomorphisme.

En particulier, si $I \subset A$, est un idéal (*i.e.* un sous-module de A), $S^{-1}I$ est un idéal dans $S^{-1}A$.

Proposition 4.8. *(1)* $\big(\mathrm{Id}_M\big)_S = \mathrm{Id}_{S^{-1}M}$.
(2) Si $f\colon M \to M'$ *et* $g\colon M' \to M''$ *sont des applications* A*-linéaires, alors* $(g\circ f)_S = g_S \circ f_S$.
(3) Si $M \subset N$*, alors* $S^{-1}M \subset S^{-1}N$ *et* $S^{-1}(N/M) \simeq S^{-1}N/S^{-1}M$.
(4) Si $f\colon M \to N$ *est* A*-linéaire, alors* $\mathsf{Ker}(f_S) = S^{-1}\,\mathsf{Ker}(f)$ *et* $\mathsf{Coker}(f_S) = S^{-1}\,\mathsf{Coker}(f)$.

Démonstration. (3) Le composé $M \subset N \xrightarrow{\iota} S^{-1}N$ s'étend en une application $S^{-1}A$-linéaire $i\colon S^{-1}M \to S^{-1}N$. Soit $x \in S^{-1}M$: écrivons $x = \frac{m}{s}$ avec $m \in M$ et $s \in S$. Si $i(x) = 0$, il existe $t \in S$ tel que $tm = 0$ dans $M \subset N$, ce qui implique que $x = \frac{m}{s} = 0$ dans $S^{-1}M$: l'application i est injective. On la considère comme une inclusion.
L'application canonique $\pi\colon N \to N/M$ induit une application $S^{-1}A$-linéaire $S^{-1}N \xrightarrow{\pi_S} S^{-1}(N/M)$. Elle est surjective : si $x \in S^{-1}(N/M)$, il existe $\overline{n} \in N/M$ et $s \in S$ tels que $x = \frac{\overline{n}}{s}$. Soit $n \in N$ relevant $\overline{n}$: on a $\pi_S\big(\frac{n}{s}\big) = x$. Bien entendu $S^{-1}M \subset \mathsf{Ker}(\pi_S)$. Inversement, si $x = \frac{n}{s} \in \mathsf{Ker}(\pi_S)$ (avec $n \in N$ et $s \in S$), on a $\frac{\pi(n)}{s} = 0$ dans $S^{-1}(N/M)$: il existe $t \in S$ tel que $t\pi(n) = \pi(tn) = 0$ dans N/M, *i.e.* $tn \in M$, donc $x = \frac{tn}{ts} \in S^{-1}M$. On a donc $\mathsf{Ker}(\pi_S) = S^{-1}M$ et $S^{-1}N/S^{-1}M \xrightarrow{\sim} S^{-1}(N/M)$.
(4) Découle de (3) appliqué à la décomposition canonique de f. □

Proposition 4.9. *Soit* M *un* A*-module et* $S \subset A$ *une partie multiplicative. Alors* $S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$ *comme* $S^{-1}A$*-modules.*

Démonstration. L'application $S^{-1}A \times M \to S^{-1}M$; $\big(\frac{a}{s}, m\big) \mapsto \frac{am}{s}$ est bilinéaire donc se factorise par une application A-linéaire $u\colon S^{-1}A \otimes_A M \to S^{-1}M$, telle que $u\big(\frac{a}{s} \otimes m\big) = \frac{am}{s}$. Son inverse n'est rien d'autre que la préimage de l'application A-linéaire $M \to S^{-1}A \otimes_A M$ donnée par $m \mapsto 1 \otimes m$ sous l'isomorphisme

$$\mathsf{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}A \otimes_A M) \xrightarrow{\sim} \mathsf{Hom}_A(M, S^{-1}A \otimes_A M)$$

(*cf* définition 4.7). Explicitement, supposons que $\frac{m}{s} = \frac{m'}{s'}$ dans $S^{-1}M$: il existe $t \in S$ tel que $t(s'm - sm') = 0$, donc

$$\frac{1}{s} \otimes m = \frac{ts'}{tss'} \otimes m = \frac{1}{tss'} \otimes (ts'm) = \frac{1}{tss'} \otimes (tsm') = \frac{ts}{tss'} \otimes m' = \frac{1}{s'} \otimes m'.$$

Cela implique que l'application $v\colon S^{-1}M \to S^{-1}A \otimes_A M$ donnée par $v\big(\frac{m}{s}\big) = \frac{1}{s} \otimes m$ est bien définie, et que c'est l'inverse de u. □

Soient $S,\ S' \subset A$ des parties multiplicatives. Posons $SS' := \{ss'\ ;\ s \in S,\ s' \in S'\}$. Dans ce qui suit, on suppose que $0 \notin SS'$, alors SS' est aussi une partie multiplicative de A.

Proposition 4.10. *Soit* $\overline{S}$ *l'image de* S *dans* $S'^{-1}A$*, alors* $\overline{S}$ *est une partie multiplicative de* $S'^{-1}A$ *et on a un isomorphisme naturel* $\overline{S}^{-1}(S'^{-1}A) \xrightarrow{\sim} (SS')^{-1}A$.

Démonstration. Supposons que $0 \in \overline{S}$: il existe $s \in S$ et $s' \in S'$ tel que $\frac{s}{s'} = 0$: il existe $t \in S'$ tel que $st = 0$, ce qui contredit l'hypothèse $0 \notin SS'$. Cela prouve que $0 \notin \overline{S}$. Le fait que $1 \in \overline{S}$ et que $\overline{S}$ est stable par produit est trivial.
Soit $f\colon A \to B$ une A-algèbre telle que $f(SS') \subset B^\times$. Comme $f(S') \subset B^\times$, l'application f s'étend de manière unique en un homomorphisme d'anneaux $\tilde{f}\colon S'^{-1}A \to B$. De même, $\tilde{f}(\overline{S}) \subset B^\times$, donc $\tilde{f}$ s'étend de manière unique en un homomorphisme d'anneaux $\hat{f}\colon \overline{S}^{-1}(S'^{-1}A) \to B$. Cela implique que $\overline{S}^{-1}(S'^{-1}A)$ possède la propriété universelle définissant $(SS')^{-1}A$: il existe un isomorphisme naturel d'anneaux $\overline{S}^{-1}(S'^{-1}A) \xrightarrow{\sim} (SS')^{-1}A$. □

Corollaire 4.11. *Si* M *est un* A*-module, il existe un isomorphisme naturel* $S^{-1}(S'^{-1}M) \xrightarrow{\sim} (SS')^{-1}M$.

Démonstration. Tensorisé avec M, l'isomorphisme $S^{-1}A \otimes_A S'^{-1}A \xrightarrow{\sim} (SS')^{-1}A$ fournit un isomorphisme $(S^{-1}A \otimes_A S'^{-1}A) \otimes_A M \xrightarrow{\sim} (SS')^{-1}A \otimes_A M$ (*cf* proposition 4.9 (1)). Comme il existe des isomorphismes $S'^{-1}A \otimes_A M \xrightarrow{\sim} S'^{-1}M$ et $(SS')^{-1}A \otimes_A M \xrightarrow{\sim} (SS')^{-1}M$ (*cf* proposition 4.9 (1) à nouveau), on en déduit une chaîne d'isomorphismes

$$\begin{array}{ccc}
S^{-1}A \otimes_A (S'^{-1}A \otimes_A M) & \xrightarrow{\sim} & (S^{-1}A \otimes_A S'^{-1}A) \otimes_A M \\
\downarrow\wr & & \downarrow\wr \\
S^{-1}A \otimes_A (S'^{-1}M) & & (SS')^{-1}A \otimes_A M \\
\downarrow\wr & & \downarrow\wr \\
S^{-1}(S'^{-1}M) & \xrightarrow{\sim} & (SS')^{-1}M
\end{array}$$

□

Lemme 4.12. *Soit* M *un* A*-module et* N' *un sous-*$S^{-1}A$*-module de* $S^{-1}M$*. Alors* $N' = S^{-1}N$ *où* N *est l'image inverse de* N' *par l'application naturelle* $M \to S^{-1}M$.

Démonstration. Si $x = \frac{m}{s} \in N'$, alors $sx = \frac{m}{1}$, *i.e.* $m \in N$, donc $x \in S^{-1}N$. Inversement, $x = \frac{n}{s} \in S^{-1}N$ (avec $n \in N$ et $s \in S$), alors $\frac{n}{1} \in N'$, donc $x \in N'$ puisque N' est un $S^{-1}A$-module. □

Corollaire 4.13. *Soit* $S \subset A$ *un ensemble multiplicatif. Les idéaux dans* $S^{-1}A$ *sont des localisations d'idéaux dans* A*. En particulier,* A *est noethérien implique que* $S^{-1}A$ *est noethérien.*

Notation. On note $\mathsf{Spec}(A)$ l'ensemble des idéaux premiers dans A. On l'appelle le *spectre* de A.

Proposition 4.14. *Soit* $S \subset A$ *un ensemble multiplicatif. Les applications*

$$\begin{aligned}
\{\mathfrak{p} \in \mathsf{Spec}(A)\ ;\ \mathfrak{p} \cap S = \varnothing\} &\leftrightarrow \mathsf{Spec}(S^{-1}A) \\
\mathfrak{p} &\mapsto S^{-1}\mathfrak{p} \\
\mathfrak{q} \cap A := \iota^{-1}(\mathfrak{q}) &\hookleftarrow \mathfrak{q}
\end{aligned}$$

sont des bijections croissantes (pour l'inclusion) inverses l'une de l'autre.

Démonstration. Soit $\mathfrak{p} \in \mathsf{Spec}(A)$ tel que $\mathfrak{p} \cap S = \varnothing$. Alors $S^{-1}A/S^{-1}\mathfrak{p} \simeq S^{-1}(A/\mathfrak{p})$ (*cf* proposition 4.8). Soit $\overline{S}$ l'image de S dans $A/\mathfrak{p}$: comme $\mathfrak{p} \cap S = \varnothing$, on a $0 \notin \overline{S}$, et $\overline{S}$ est un ensemble multiplicatif dans $A/\mathfrak{p}$. Comme $A/\mathfrak{p}$ est un ensemble intégral, sa localisation $S^{-1}(A/\mathfrak{p}) = \overline{S}^{-1}(A/\mathfrak{p}) \subset \mathsf{Frac}(A/\mathfrak{p})$ l'est aussi, de sorte que $S^{-1}\mathfrak{p}$ est premier dans $S^{-1}A$.
Inversement, si $\mathfrak{q} \in \mathsf{Spec}(S^{-1}A)$, alors $A/\iota^{-1}(\mathfrak{q}) \hookrightarrow S^{-1}A/\mathfrak{q}$ est un ensemble intégral : on a $\mathfrak{q} \cap A \in \mathsf{Spec}(A)$. Si $s \in (\mathfrak{q} \cap A) \cap S$, alors $s \in \mathfrak{q}$. Comme s est inversible dans $S^{-1}A$, on a $\mathfrak{q} = S^{-1}A$, ce qui n'est pas le cas : on a $(\mathfrak{q} \cap A) \cap S = \varnothing$.
Soit $\mathfrak{p} \in \mathsf{Spec}(A)$ tel que $\mathfrak{p} \cap S = \varnothing$. On a bien sûr $\mathfrak{p} \subset S^{-1}\mathfrak{p} \cap A$. Inversement, soit $a \in S^{-1}\mathfrak{p} \cap A$: écrivons $a = \frac{\alpha}{s}$ avec $\alpha \in \mathfrak{p}$ et $s \in S$. Comme $sa = \alpha \in \mathfrak{p}$ et $s \notin \mathfrak{p}$ (car $\mathfrak{p} \cap S = \varnothing$), on a $a \in \mathfrak{p}$, ce qui prouve l'égalité $\mathfrak{p} = S^{-1}\mathfrak{p} \cap A$.
Soit $\mathfrak{q} \in \mathsf{Spec}(S^{-1}A)$. On a bien sûr $S^{-1}(\mathfrak{q} \cap A) \subset \mathfrak{q}$. Inversement, soit $x \in \mathfrak{q}$: écrivons $x = \frac{a}{s}$ avec $a \in A$ et $s \in S$. On a $sx = a \in \mathfrak{q} \cap A$, donc $x = \frac{a}{s} \in S^{-1}(\mathfrak{q} \cap A)$, ce qui prouve l'égalité $\mathfrak{q} = S^{-1}(\mathfrak{q} \cap A)$. □

Remarque. En particulier on a $\mathsf{Spec}(S^{-1}A) \subset \mathsf{Spec}(A)$. L'ensemble $\mathsf{Spec}(A)$ peut être doté d'une structure d'espace topologique (et même plus...) et la bijection de la proposition 4.14 identifie $\mathsf{Spec}(S^{-1}A)$ à un sous-ensemble ouvert de $\mathsf{Spec}(A)$, ce qui explique la terminologie de « localisation ».

Exercice 4.15. ⁂ Soient A un anneau intègre et M un A-module. On suppose que M peut être engendré par n éléments, et qu'il contient un sous-module qui est libre de rang n. Montrer que M est libre de rang n.

5 Anneaux factoriels

Les anneaux $\mathbf{Z}$ et $K[X]$ (avec K un corps) ont une division euclidienne. Cela implique qu'ils sont principaux, et que tout élément non nul peut s'écrire de façon essentiellement unique comme produit d'éléments irréductibles. Le but de ce chapitre est d'introduire une classe d'anneaux ayant cette propriété de factorisation : les anneaux factoriels.

Dans tout ce numéro, A désigne un anneau *intègre*.

5.1 Généralités

Définition 5.2. (1) Soient $a, b \in A\backslash\{0\}$. On dit que a et b sont *associés* si $a \mid b$ et $b \mid a$ (comme A est intègre, cela équivaut à l'existence de $u \in A^\times$ tel que $b = au$, soit encore à l'égalité $\langle a\rangle = \langle b\rangle$).
(2) Soit $\pi \in A\backslash\{0\}$. On dit que π est *irréductible* (resp. *premier*) dans A si $\pi \notin A^\times$ et

$$(\forall a, b \in A)(\pi = ab \Rightarrow (a \in A^\times \text{ ou } b \in A^\times))$$

(resp. l'idéal $\langle\pi\rangle$ est premier).

Remarques. (1) π est irréductible lorsque les seuls diviseurs de π sont les unités et les éléments associés à π).
(2) Tout élément premier est irréductible, mais la réciproque est fausse en général.

Exercices 5.3. $*$ (1) Soient K un corps, T une indéterminée et $A = K + T^2K[T] \subset K[T]$. Montrer que T^2 est irréductible mais pas premier dans A.
(2) Soient $a, b \in A$ tels que $a \in A^\times$ ou bien a irréductible et $a \nmid b$. Montrer que $aX + b$ est irréductible dans $A[X]$.

Les éléments irréductibles sont donc ceux qui ne peuvent s'exprimer comme un produit non trivial, *i.e.* ce sont les « atomes » pour la multiplication. Les anneaux (intègres) dans lesquels tout élément non nul peut se décomposer de façon « unique » en produit d'éléments irréductibles sont particulièrement agréables.

Définition 5.4. Soit $a \in A\backslash\{0\}$. Une *factorisation en produit d'éléments irréductibles* de a est une écrituture de a sous la forme

$$a = u\pi_1 \cdots \pi_r$$

avec $u \in A^\times$ et $\pi_1, \ldots, \pi_r \in A$ irréductibles. On dit qu'une telle décomposition est *unique* si pour toute autre factorisation $a = vp_1 \cdots p_s$ avec $v \in A^\times$ et $p_1, \ldots, p_s \in A$ irréductibles, alors $r = s$ et il existe $\sigma \in \mathfrak{S}_r$ tel que $\langle\pi_i\rangle = \langle p_{\sigma(i)}\rangle$ (*i.e.* π_i et $p_{\sigma(i)}$ sont associés) pour tout $i \in \{1, \ldots, r\}$. On dit que A est *factoriel* si tout élément non nul admet une unique factorisation en produit d'éléments irréductibles.

Remarque. Tout élément inversible admet une unique factorisation en produit d'éléments irréductibles.

Dans la pratique, si A est factoriel, on se fixe une famille de représentants $\mathbb{P} = \{\pi_\lambda\}_{\lambda\in\Lambda}$ des classes des éléments irréductibles modulo la relation « être associé ». Tout élément $a \in A\backslash\{0\}$ s'écrit alors de façon unique

$$a = u\prod_{\lambda\in\Lambda} \pi_\lambda^{n_\lambda} \qquad (*)$$

avec $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre *fini*).

Définition 5.5. Soit π un élément irréductible de A. Il existe un unique $\lambda \in \Lambda$ tel que $\langle\pi\rangle = \langle\pi_\lambda\rangle$. Si $a \in A\backslash\{0\}$, la multiplicité n_λ dans la factorisation ($*$) s'appelle la *valuation* de a en π. On la note $v_\pi(a)$. On pose $v_\pi(0) = +\infty$. On a $v_\pi(a) = \sup\{k \in \mathbf{N} \cup \{\infty\}\ ;\ \pi^n \mid a\}$.

Proposition 5.6 (PROPRIÉTÉS DES VALUATIONS)**.** *Soient $a, b \in A$. On a*
(1) $v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et $v_\pi(a + b) \geqslant \min\{v_\pi(a), v_\pi(b)\}$ (avec égalité si $v_\pi(a) \neq v_\pi(b)$) pour tout $\pi \in A$ irréductible ;
(2) $a \mid b$ si et seulement si pour tout $\pi \in A$ irréductible, on a $v_\pi(a) \leqslant v_\pi(b)$;
(3) $a \in A^\times$ si et seulement si pour tout $\pi \in A$ irréductible, on a $v_\pi(a) = 0$.

Démonstration. Cela résulte immédiatement des définitions et de l'unicité de la factorisation en produit d'éléments irréductibles. □

Exemples 5.7. (1) Un corps est factoriel (tout élément non nul est inversible).
(2) Étant principal, l'anneau $\mathbf{Z}$ (resp. $K[X]$ où K est un corps) est factoriel, les nombres premiers (resp. le polynômes unitaires et irréductibles) étant un système de représentants des éléments irréductibles (*cf* proposition 5.16). Il en est de même de $A[X]$ si A est factoriel (*cf* théorème 5.25).
(3) Le sous-anneau $\mathbf{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \in \mathbf{C},\ x, y \in \mathbf{Z}\}$ de $\mathbf{C}$ n'est pas factoriel, car 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles, les unités sont ± 1, mais $2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$: on n'a pas unicité de la décomposition de 6 (exercice). De même, si K est un corps et T une indéterminée, le sous-anneau $K + T^2K[T] \subset K[T]$ n'est pas factoriel (parce que $(T^2)^3 = T^6 = (T^3)^2$, exercice).

Proposition 5.8. *Supposons A factoriel et soit $\pi \in A$. Alors π est irréductible si et seulement si π est premier, i.e. si et seulement si on a*

$$(\forall (a,b) \in A^2)\ \pi \mid ab \Rightarrow (\pi \mid a \text{ ou } \pi \mid b).$$

Démonstration. Si π est irréductible et $\pi \mid ab$, on a $v_\pi(a) + v_\pi(b) = v_\pi(ab) \geqslant 1$ et donc $v_\pi(a) \geqslant 1$ ou $v_\pi(b) \geqslant 1$ *i.e.* $\pi \mid a$ ou $\pi \mid b$. La réciproque est triviale. □

Proposition 5.9. *L'anneau A est factoriel si et seulement si tout élément non nul de A admet une factorisation en produit d'éléments irréductibles*[7] *et si tout élément irréductible est premier.*

Démonstration. On sait déjà que si A est factoriel, alors tout élément irréductible est premier (proposition 5.8). Réciproquement, supposons que tout élément admet une factorisation en produit d'éléments irréductibles et que tout élément irréductible est premier : montrons l'unicité. Supposons donc qu'on a une égalité d'idéaux $\langle a \rangle = \langle \pi_1 \cdots \pi_r \rangle = \langle p_1 \cdots p_s \rangle$ avec $\pi_1, \ldots, \pi_r, p_1, \ldots, p_s$ irréductibles : il s'agit de montrer que $r = s$ et que, quitte à renuméroter, on a $\langle \pi_i \rangle = \langle p_i \rangle$ pour tout $i \in \{1, \ldots, r\}$. Quitte à échanger les deux écritures, on peut supposer que $r \leqslant s$: on procède par récurrence sur r. Si $r = 0$, alors $a \in A^\times$, ce qui implique $s = 0$. Supposons $r > 0$. On a $\pi_r \mid p_1 \cdots p_s$: comme π_r est premier, il existe $i \in \{1, \ldots, s\}$ tel que $\pi_r \mid p_i$, et donc $\langle \pi_r \rangle = \langle p_i \rangle$ vu que p_i est irréductible. Quitte à renuméroter, on peut supposer que $i = s$, et on a $\langle \pi_1 \cdots \pi_{r-1} \rangle = \langle p_1 \cdots p_{s-1} \rangle$, et l'hypothèse de récurrence permet de conclure. □

5.10 Pgcd, ppcm

Supposons A factoriel.

Définition 5.11. Soient $a, b \in A$. On appelle *pgcd* (plus grand commun diviseur) –resp. *ppcm* (plus petit commun multiple)– de a et b un plus grand minorant –resp. un plus petit majorant– de $\{a, b\}$ pour la relation de divisiblité. On les note $\mathsf{pgcd}(a,b)$ et $\mathsf{ppcm}(a,b)$ respectivement. On dit que a et b sont *premiers entre eux* si $\mathsf{pgcd}(a,b) = 1$.

Remarques. (1) Rigoureusement, $\mathsf{pgcd}(a,b)$ et $\mathsf{ppcm}(a,b)$ sont des classes d'équivalence pour la relation « être associé ». On commettra systématiquement l'abus de noter de la même façon des *représentants* de ces classes. Dans $\mathbf{Z}$ par exemple, on écrira $\mathsf{pgcd}(6,10) = 2$ au lieu de $\mathsf{pgcd}(6,10) = \{\pm 2\}$. Dans ce qui suit, des égalités impliquant des pgcd et des ppcm doivent donc être comprises à multiplication par une unité près.
(2) Si $a \in A$, on a $\mathsf{pgcd}(a,0) = a$ et $\mathsf{ppcm}(a,0) = 0$.

Comme plus haut, fixons une famille de représentants $\mathbb{P} = \{\pi_\lambda\}_{\lambda \in \Lambda}$ des classes des éléments irréductibles modulo la relation « être associé ».
Soient $a, b \in A\backslash\{0\}$. L'anneau A étant factoriel, il existe $u, v \in A^\times$ et des familles $(n_\lambda)_{\lambda\in\Lambda}$ et $(m_\lambda)_{\lambda\in\Lambda}$ dans $\mathbf{N}^{(\Lambda)}$ telles que les factorisations en produits d'éléments irréductibles de a et b soient

$$a = u \prod_{\lambda\in\Lambda} \pi_\lambda^{n_\lambda} \qquad b = v \prod_{\lambda\in\Lambda} \pi_\lambda^{m_\lambda}$$

alors on a

$$\mathsf{pgcd}(a,b) = \prod_{\lambda\in\Lambda} \pi_\lambda^{\min\{n_\lambda, m_\lambda\}} \qquad \mathsf{ppcm}(a,b) = \prod_{\lambda\in\Lambda} \pi_\lambda^{\max\{n_\lambda, m_\lambda\}}.$$

En d'autres termes, pour tout $\pi \in A$ irréductible, on a

$$\begin{cases} v_\pi(\mathsf{pgcd}(a,b)) = \min\{v_\pi(a), v_\pi(b)\} \\ v_\pi(\mathsf{ppcm}(a,b)) = \max\{v_\pi(a), v_\pi(b)\} \end{cases}$$

On remarque qu'on a $\mathsf{pgcd}(a,b)\,\mathsf{ppcm}(a,b) = ab$.

Remarques. (1) Ce qui précède montre l'existence du pgcd et du ppcm dans un anneau factoriel. Les notions existent dans un anneau quelconque, mais en général, le pgcd et le ppcm n'existent pas.
(2) Par induction, on peut facilement étendre la définition et parler du pgcd et du ppcm d'une famille *finie* d'éléments non nuls.

Proposition 5.12 (LEMME DE GAUSS)**.** *Soient $a, b, c \in A\backslash\{0\}$ tels que $\mathsf{pgcd}(a,b) = 1$. Si $a \mid bc$, alors $a \mid c$.*

Démonstration. Si $\pi \in A$ est irréductible et divise a, on a $v_\pi(b) = 0$ vu que $\pi \nmid b$ (car a et b sont premiers entre eux). On a donc $v_\pi(a) \leqslant v_\pi(bc) = v_\pi(c)$. Comme c'est vrai pour tout π premier divisant a, on a $a \mid c$ (*cf* proposition 5.6 (2)). □

Exercice 5.13. ∗ Soient $a, b, c \in A$. Montrer que $\mathsf{pgcd}(a,b,c) = \mathsf{pgcd}(a, \mathsf{pgcd}(b,c))$.

7. Cette condition est satisfaite lorsque A est noethérien.

5.14 Lien avec les anneaux principaux

Dans ce numéro, on suppose que A est principal (rappelons que cela signifie que A est intègre et que tous ses idéaux sont principaux, *i.e.* engendrés par un élément).

Lemme 5.15. *Soit $\pi \in A$. Les conditions suivantes sont équivalentes :*
(i) π est irréductible ;
(ii) $\langle \pi \rangle$ est un idéal maximal ;
(iii) π est premier.

Démonstration. Supposons π irréductible : on a $\langle \pi \rangle \neq A$. Soit $I \subset A$ un idéal propre tel que $\langle \pi \rangle \subset I$. Il existe $a \in A$ tel que $I = \langle a \rangle$, et on a $a \mid \pi$. Comme π est irréductible, et comme $a \notin A^\times$ (parce que $I \neq A$), cela implique que π et a sont associés, *i.e.* que $I = \langle \pi \rangle$. Cela montre que $\langle \pi \rangle$ est maximal, et donc (i)⇒(ii). Les autres implications sont déjà connues. □

Proposition 5.16. *Tout anneau principal est factoriel.*

Démonstration. D'après la proposition 5.9 et le lemme 5.15, il suffit de montrer que tout élément $a \in A\backslash\{0\}$ admet une factorisation en produit d'éléments irréductibles. Si a est inversible, on a fini. Dans le cas contraire, l'idéal $\langle a \rangle$ est strict : il est contenu dans un idéal maximal. D'après le lemme 5.15, il existe $\pi_1 \in A$ irréductible tel que $\langle a \rangle \subset \langle \pi_1 \rangle$: on peut écrire $a = \pi_1 a_1$ avec $a_1 \in A\backslash\{0\}$. En itérant ce qui précède, on construit des suites $\pi_1, \dots, \pi_n$ et $a_1, \dots, a_n$ telles que $a_{k-1} = \pi_k a_k$ pour tout $k \in \{1, \dots, n\}$ (avec la convention $a_0 = a$). Si on pouvait continuer indéfiniment, cela fournirait une suite strictement croissante d'idéaux $(\langle a_k \rangle)_{k \in \mathbf{N}}$, contredisant le fait que A est noethérien (*cf* définition 2.17) : le processus s'arrête en un nombre fini d'étapes, *i.e.* il existe $n \in \mathbf{N}$ tel que $a_n \in A^\times$. L'écriture $a = \pi_1 \cdots \pi_n a_n$ est une factorisation en produit d'éléments irréductibles. □

Remarque. Si A est un anneau principal, on a une caractérisation importante du pgcd et du ppcm de deux éléments $a, b \in A$. On a $\langle \mathsf{pgcd}(a,b) \rangle = \langle a, b \rangle$ et $\langle \mathsf{ppcm}(a,b) \rangle = \langle a \rangle \cap \langle b \rangle$. Montrons-le pour le pgcd (la preuve pour le ppcm est analogue). Comme A est principal, il existe $d \in A$ tel que $\langle a, b \rangle = \langle d \rangle$. Comme $x \in A$ divise a et b si et seulement si $\langle a \rangle \subset \langle x \rangle$ et $\langle b \rangle \subset \langle x \rangle$ *i.e.* $\langle d \rangle \subset \langle x \rangle$, on a bien $\mathsf{pgcd}(a,b) = d$.
En particulier, si $a, b \in A$, il existe $u, v \in A$ tels que $au + bv = d$ (relation de Bézout).
Il ne faut pas croire que cette caractérisation est valable dans tout anneau factoriel. Par exemple, on verra (*cf* théorème 5.25) que $\mathbf{Q}[X,Y]$ est factoriel. Comme X et Y sont irréductibles et premiers entre eux, on a $\mathsf{pgcd}(X,Y) = 1$, bien que $\langle X, Y \rangle \neq \mathbf{Q}[X,Y]$ (c'est l'idéal des polynômes qui s'annulent en $(0,0)$). Bien sûr, cela vient du fait que l'anneau $\mathbf{Q}[X,Y]$ n'est pas principal.

Exemples 5.17. Si K est un corps et $n \in \mathbf{N}_{>1}$, l'anneau $K[X_1, \dots, X_n]$ est factoriel (*cf* théorème 5.25) mais pas principal (*cf* remarque précédente). De même, l'anneau $\mathbf{Z}[X]$ est factoriel (*cf loc. cit.*) mais pas principal (l'idéal engendré par 2 et X n'est pas principal).

Exercice 5.18. $*$ (1) Soit A un anneau factoriel tel que pour tout $a, b \in A$, l'idéal $\langle a, b \rangle$ est principal. Montrer que A est principal.
$**$ (2) Soient A un anneau et $S \subset A$ une partie multiplicative. Montrer que si A est principal (resp. factoriel), il en est de même du localisé $S^{-1}A$.

5.19 Transfert de la factorialité

Supposons A factoriel et posons $K = \mathsf{Frac}(A)$.

Définition 5.20. Soit $P = a_0 + a_1 X + \cdots + a_d X^d \in A[X]\backslash\{0\}$. Le *contenu* de P est

$$\mathsf{c}(P) = \mathsf{pgcd}\{a_0, \dots, a_d\}.$$

On dit que P est *primitif* lorsque $\mathsf{c}(P) = 1$.

Remarque. Rappelons que rigoureusement parlant, le pgcd est une classe d'équivalence modulo la relation « être associé ». Dans ce qui suit, on commettra l'abus habituel consistant à voir $\mathsf{c}(P)$ comme un élément de A (n'importe quel représentant de la classe) pour ne pas alourdir la rédaction, et toutes les égalités faisant intervenir des contenus doivent être lues comme des égalités d'idéaux (*i.e.* modulo la relation « être associé »).

Lemme 5.21. *Si $P, Q \in A[X]\backslash\{0\}$, on a*
(1) $\mathsf{c}(aP) = a\,\mathsf{c}(P)$ pour tout $a \in A\backslash\{0\}$;
(2) $P = \mathsf{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif ;
(3) $\mathsf{c}(PQ) = \mathsf{c}(P)\,\mathsf{c}(Q)$.

Démonstration. (1) est évident.
(2) Écrivons $P(X) = a_0 + a_1X + \cdots + a_dX^d$: pour tout $k \in \{0, \dots, d\}$, on peut écrire $a_k = \mathsf{c}(P)b_k$ avec $b_k \in A$. Posons $\widetilde{P}(X) = b_0 + b_1X + \cdots + b_dX^d \in A[X]$: on a $P = \mathsf{c}(P)\widetilde{P}$, et $\mathsf{c}(\widetilde{P}) = \mathsf{pgcd}(b_0, \dots, b_d) = 1$, *i.e.* $\widetilde{P}$ est primitif.
(3) D'après (2), on a $P = \mathsf{c}(P)\widetilde{P}$ et $Q = \mathsf{c}(Q)\widetilde{Q}$ avec $\widetilde{P}, \widetilde{Q} \in A[X]$ primitifs : on a alors $PQ = \mathsf{c}(P)\,\mathsf{c}(Q)\widetilde{P}\widetilde{Q}$. Quitte à remplacer P et Q par $\widetilde{P}$ et $\widetilde{Q}$ respectivement, il suffit donc de montrer que si P et Q sont primitifs, il en est de même de PQ. Supposons au contraire qu'il existe $\pi \in A$ premier tel que $\pi \mid \mathsf{c}(PQ)$. Si on note $\overline{P}$ et $\overline{Q}$ les images dans $(A/\langle\pi\rangle)[X]$ de P et Q respectivement, cela implique que $\overline{P}\overline{Q} = 0$ dans $(A/\langle\pi\rangle)[X]$. Mais comme π est premier, l'anneau $A/\langle\pi\rangle$ est intègre : il en est de même de l'anneau $(A/\langle\pi\rangle)[X]$. On a donc $\overline{P} = 0$ ou $\overline{Q} = 0$, et donc $\pi \mid \mathsf{c}(P)$ ou $\pi \mid \mathsf{c}(Q)$, ce qui contredit $\mathsf{c}(P) = 1$ et $\mathsf{c}(Q) = 1$: absurde. □

Proposition 5.22. *Soit $P \in A[X]$ de degré $\geqslant 1$.*
(1) Si P est irréductible dans $A[X]$, alors il est irréductible dans $K[X]$.
(2) Si P est primitif et irréductible dans $K[X]$, alors il est irréductible dans $A[X]$.

Démonstration. (1) Observons que $\mathsf{c}(P) = 1$, parce que P est irréductible de degré $\geqslant 1$ dans $A[X]$. Supposons P réductible dans $K[X]$: on peut écrire $P = P_1P_2$ avec $P_1, P_2 \in K[X]$ de degrés $\geqslant 1$. Il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1P_1, a_2P_2 \in A[X]$. On a alors $a_1a_2 = \mathsf{c}(a_1a_2P) = \mathsf{c}(a_1P_1)\,\mathsf{c}(a_2P_2)$ d'après le lemme 5.21, vu que $c(P) = 1$. Si on écrit $a_1P_1 = \mathsf{c}(a_1P_1)\widetilde{P}_1$ et $a_2P_2 = \mathsf{c}(a_2P_2)\widetilde{P}_2$ avec $\widetilde{P}_1, \widetilde{P}_2 \in A[X]$ primitifs, on a donc

$$a_1a_2P = \mathsf{c}(a_1P_1)\,\mathsf{c}(a_2P_2)\widetilde{P}_1\widetilde{P}_2$$

soit $P = \widetilde{P}_1\widetilde{P}_2$ en divisant par a_1a_2 (l'anneau A est intègre). Comme P est irréductible dans $A[X]$, on a $\widetilde{P}_1 \in A^\times$ ou $\widetilde{P}_2 \in A^\times$, ce qui contredit $\deg(P_1), \deg(P_2) \geqslant 1$.
(2) Supposons $P = P_1P_2$ avec $P_1, P_2 \in A[X]$. Comme P est irréductible dans $K[X]$, on peut supposer, quitte à échanger P_1 et P_2, que P_1 est constant, *i.e.* $P_1 = \mathsf{c}(P_1)$. D'après le lemme 5.21, on a $1 = \mathsf{c}(P) = \mathsf{c}(P_1)\,\mathsf{c}(P_2)$, donc $P_1 \in A^\times$, et P est irréductible dans $A[X]$. □

Exemples 5.23. (1) Un polynôme non constant et irréductible dans $\mathbf{Z}[X]$ est irréductible dans $\mathbf{Q}[X]$.
(2) Le polynôme $2X + 2$ est irréductible dans $\mathbf{Q}[X]$, mais réductible dans $\mathbf{Z}[X]$.

Remarque. Dans l'énoncé qui précède, il est important de supposer A factoriel. Par exemple, soit $A = \mathbf{Z}\left[\sqrt{-5}\right] \subset \mathbf{C}$. On a $P(X) := 2X^2 - 2X + 3 \in A[X]$. Si $K = \mathsf{Frac}(A)$, on a $P(X) = 2\big(X - \frac{1+\sqrt{-5}}{2}\big)\big(X - \frac{1-\sqrt{-5}}{2}\big)$ dans $K[X]$. Cependant, il est irréductible dans $A[X]$ (exercice).

Exercice 5.24. ∗ Soient $P, Q \in K[X]$ des polynômes unitaires tels que $PQ \in A[X]$. Montrer que $P, Q \in A[X]$.

Théorème 5.25. *(1) Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes primitifs non constants qui sont irréductibles dans $K[X]$.*
(2) L'anneau $A[X]$ est factoriel.

Démonstration. (1) Si $\pi \in A$ est irréductible, alors $A[X]/\langle\pi\rangle = (A/\pi A)[X]$ est intègre, de sorte que le polynôme constant π est premier donc irréductible dans $A[X]$. La proposition 5.22 (2) montre que les polynômes primitifs non constants qui sont irréductibles dans $K[X]$ sont irréductibles dans $A[X]$. Réciproquement, soit P un élément irréductible dans $A[X]$. Si $\deg(P) = 0$, on a $P \in A$, et P est *a fortiori* irréductible dans A. Si $\deg(P) \geqslant 1$, on a $P = \mathsf{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif : comme P est irréductible dans $A[X]$, on a $\mathsf{c}(P) \in A^\times$, donc P est primitif. Par ailleurs, la proposition 5.22 (1) montre que P est irréductible dans $K[X]$.
(2) • Si $\pi \in A$ est irréductible, on a vu ci-dessus que π est premier dans $A[X]$. Si $P \in A[X]$ est non constant, primitif et irréductible dans $K[X]$, et si $Q, R \in A[X]$ sont tels que $P \mid QR$ dans $A[X]$, on a *a fortiori* $P \mid QR$ dans $K[X]$, donc $P \mid Q$ ou $P \mid R$ dans $K[X]$, disons $P \mid Q$. Il existe donc $S \in K[X]$ tel que $Q = PS$. Soit $a \in A\backslash\{0\}$ tel que $aS \in A[X]$: on peut écrire $aS = \mathsf{c}(aS)\widetilde{S}$ avec $\widetilde{S} \in A[X]$ primitif, donc $aQ = \mathsf{c}(aS)P\widetilde{S}$. En prenant les contenus, on a $a\,\mathsf{c}(Q) = \mathsf{c}(aS)$ (parce que $P\widetilde{S}$ est primitif), ce qui montre que $a \mid \mathsf{c}(aS)$: si $\mathsf{c}(aS) = ab$, on a $Q = bP\widetilde{S}$, ce qui montre que $P \mid Q$ dans $A[X]$. Cela prouve que P est premier dans $A[X]$.
• D'après (1), ce qui précède montre que les éléments irréductibles de $A[X]$ sont tous premiers. Pour prouver que $A[X]$ est factoriel il suffit donc de montrer que tout élément $P \in A[X]\backslash\{0\}$ admet une factorisation en produit d'éléments irréductibles (*cf* proposition 5.9). D'après le lemme 5.21 (2), on peut écrire $P = \mathsf{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif. Comme A est factoriel, on peut factoriser $\mathsf{c}(P)$ en produit d'éléments irréductibles dans A (donc dans $A[X]$) : il suffit de montrer $\widetilde{P}$ admet une factorisation. On peut donc se restreindre au cas où P est primitif. Si $P \in A$, on a alors $P = 1$: on peut supposer $\deg(P) \geqslant 1$. Comme l'anneau $K[X]$ est factoriel (parce que principal, *cf* proposition 5.16), on peut écrire $P = P_1P_2 \cdots P_r$ avec $P_1, \dots, P_r$ irréductibles dans $K[X]$. Pour tout $k \in \{1, \dots, r\}$, choisissons $a_k \in A\backslash\{0\}$ tel que $a_kP_k \in A[X]$: le polynôme $\widetilde{P}_k := c(a_kP_k)^{-1}(a_kP_k) \in A[X]$ est primitif. Étant irréductible dans $K[X]$, il est irréductible dans $A[X]$ (proposition 5.22 (2)). Par ailleurs, on a $a_1 \cdots a_rP = \mathsf{c}(a_1P_1) \cdots \mathsf{c}(a_rP_r)\widetilde{P}_1 \cdots \widetilde{P}_r$ donc $a_1 \cdots a_r = \mathsf{c}(a_1P_1) \cdots \mathsf{c}(a_rP_r)$ en prenant le contenu, et donc $P = \widetilde{P}_1 \cdots \widetilde{P}_r$, ce qui achève la preuve. □

Remarque. Réciproquement, il est facile de voir que si $A[X]$ est factoriel, il en est de même de A.

Corollaire 5.26. *L'anneau $A[X_1, \dots, X_n]$ est factoriel.*

Exemple 5.27. Les anneaux $\mathbf{Z}[X_1, \dots, X_n]$ et $K[X_1, \dots, X_n]$ (où K est un corps) sont factoriels.

Exercices 5.28. $\ast\ast\ast$ (1) Montrer que les idéaux premiers de $\mathbf{Z}[X]$ sont de trois sortes :
(a) $\{0\}$;
(b) $\langle P \rangle$ avec $P \in \mathbf{Z}[X]$ irréductible ;
(c) $\langle p, F \rangle$ avec p premier dans $\mathbf{Z}$ et $F \in \mathbf{Z}[X]$ dont le réduction modulo p est irréductible dans $\mathbf{F}_p[X]$.

(2) Soient A un anneau factoriel, $n \in \mathbf{N}_{>0}$ et $\{X_{i,j}\}_{1 \leqslant i,j \leqslant n}$ des indéterminées. Posons $R = A[X_{i,j}]_{1 \leqslant i,j \leqslant n}$ (l'anneau de polynômes en n^2 indéterminées). On dispose de la matrice « générique » $M := (X_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(R)$, et du polynôme $D_n := \det(M) \in R$. Montrer que D_n est irréductible dans R [indication : procéder par récurrence sur n et en développant D_n par rapport à la première colonne].
(3) Soit A un anneau factoriel. Montrer que A est principal si et seulement si ses éléments irréductibles engendrent des idéaux maximaux.
(4) Montrer que $\mathbf{C}[X, Y, Z, T]/\langle XY - ZT \rangle$ est intègre, et qu'il n'est pas factoriel.

6 Modules de type fini sur les anneaux principaux

On suppose désormais A principal. Par définition, A est intègre : on note K son corps des fractions. Rappelons que A est factoriel : on dispose du pgcd et du ppcm. En outre, comme les idéaux de A sont engendrés par un élément, ils sont de type fini, *i.e.* A est noethérien.

Dans ce qui suit, quand on écrit une matrice, les coefficients vides correspondent à des zéros. Si $n \in \mathbf{N}_{>0}$ et $a_1, \dots, a_n \in A$, on pose

$$\operatorname{diag}(a_1, \dots, a_n) = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in \mathsf{M}_n(A).$$

Définition 6.1. Si $n \in \mathbf{N}_{>0}$ on pose $\mathsf{GL}_n(A) = \{M \in \mathsf{M}_n(A) \,;\, \det(M) \in A^\times\}$. D'après les formules de Cramer, c'est le groupe des éléments inversibles de $\mathsf{M}_n(A)$ (prendre garde que lorsque A n'est pas un corps, la condition $\det(A) \neq 0$ est insuffisante). On pose $\mathsf{SL}_n(A) = \{M \in \mathsf{M}_n(A) \,;\, \det(M) = 1\}$. C'est un sous-groupe de $\mathsf{GL}_n(A)$ (c'est le noyau du morphisme déterminant).

Proposition 6.2. *Si $n \in \mathbf{N}_{\geqslant 2}$ et $a_1, \dots, a_n \in A$ engendrent l'idéal unité, il existe une matrice dans $\mathsf{SL}_n(A)$ dont la première ligne est $(a_1, \dots, a_n)$.*

Démonstration. Posons $X = (a_1, \dots, a_n)$: il faut montrer qu'il existe $M \in \mathsf{SL}_n(A)$ telle que $XM^{-1} = (1, 0, \dots, 0)$. On procède par récurrence sur $n \geqslant 2$.
Cas $n = 2$. Comme $\langle a_1, a_2 \rangle = A$, il existe $u, v \in A$ tels que $va_1 - ua_2 = 1$. La matrice $M = \left(\begin{smallmatrix} a_1 & a_2 \\ u & v \end{smallmatrix}\right)$ répond alors à la question.
Cas $n > 2$. Posons $d = \mathsf{pgcd}(a_2, \dots, a_n)$ et soient $b_2, \dots, b_n \in A$ tels que $db_i = a_i$ pour $i \in \{2, \dots, n\}$. On a alors $\langle b_2, \dots, b_n \rangle = A$: par hypothèse de récurence, il existe $M_1' \in \mathsf{SL}_{n-1}(A)$ telle que $(b_2, \dots, b_n)M_1'^{-1} = (1, 0, \dots, 0)$. Soit alors $M_1 = \begin{pmatrix} 1 & \\ & M_1' \end{pmatrix}$. On a $\det(M_1) = \det(M_1') = 1$ et $XM_1^{-1} = (a_1, d, 0, \dots, 0)$. On utilise le cas $n = 2$: comme $\langle a_1, d \rangle = A$, il existe $M_2' \in \mathsf{SL}_2(A)$ avec $(a_1, d)M_2'^{-1} = (1, 0)$. Soit alors $M_2 = \begin{pmatrix} M_2' & \\ & \mathrm{I}_{n-2} \end{pmatrix}$ où $\mathrm{I}_{n-2} \in \mathsf{SL}_{n-2}(A)$ désigne la matrice identité. On a $\det(M_2) = \det(M_2') = 1$ et $XM_1^{-1}M_2^{-1} = (1, 0, \dots, 0)$, *i.e.* $XM^{-1} = (1, 0, \dots, 0)$ avec $M = M_2M_1 \in \mathsf{SL}_n(A)$. □

Remarque. Cette preuve fournit une procédure effective pour construire la matrice si on sait traiter le cas $n = 2$, *i.e.* trouver des relations de Bezout (par exemple lorsque A est un anneau euclidien).

Définition 6.3. Si $n, m \in \mathbf{N}_{>0}$, on fait agir $\mathsf{SL}_n(A) \times \mathsf{SL}_m(A)$ sur le A-module $\mathsf{M}_{n \times m}(A)$ par

$$(P, Q) \cdot M = PMQ^{-1}.$$

Deux matrices $M_1, M_2 \in \mathsf{M}_{n \times m}(A)$ sont dites *équivalentes* si elles sont dans la même orbite pour cette action. On écrit alors $M_1 \sim M_2$ (cela définit une relation d'équivalence). Remarquons qu'on peut aussi faire agir $\mathsf{GL}_n(A) \times \mathsf{GL}_m(A)$ de la même façon.

Remarque. Lorsque $n = m$, on prendra garde à ne pas confondre cette notion avec celle, plus fine, de matrices *semblables* : si $M_1, M_2 \in \mathsf{M}_n(A)$, on dit que M_1 et M_2 sont semblables s'il existe $P \in \mathsf{GL}_n(A)$ tel que $M_2 = PM_1P^{-1}$.

Définition 6.4. Un matrice *réduite* est une matrice de la forme

$$\begin{pmatrix} \alpha_1 & & & \\ & \ddots & & \\ & & \alpha_r & \end{pmatrix} \in \mathsf{M}_{n \times m}(A)$$

avec $r \in \{0, \dots, \min\{m, n\}\}$ et $\alpha_1, \dots, \alpha_r \in A \backslash \{0\}$ tels que $\langle \alpha_{i+1} \rangle \subset \langle \alpha_i \rangle$ (*i.e.* $\alpha_i \mid \alpha_{i+1}$) pour tout $i \in \{1, \dots r-1\}$.

Notation. (1) Fixons une famille $(p_\lambda)_{\lambda \in \Lambda}$ de représentants des éléments irréductibles de A. Tout élément $a \in A \backslash \{0\}$ admet une décomposition unique en facteurs irréductibles :

$$a = u \prod_{\lambda \in \Lambda} p_\lambda^{n_\lambda}$$

où $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ est une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre fini). On pose alors

$$\ell(a) = \sum_{\lambda\in\Lambda} n_\lambda \in \mathbf{N}$$

qu'on appelle *longueur* de a. C'est le nombre de facteurs irréductibles de a (par exemple, on a $\ell(a) = 0 \Leftrightarrow a \in A^\times$ et $\ell(a) = 1$ si et seulement si A est irréductible). Si $M = (m_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} \in \mathsf{M}_{n\times m}(A)\backslash\{0\}$, on pose

$$\ell(M) = \min\big\{\ell(m_{i,j})\,;\, 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m,\ m_{i,j} \neq 0\big\}.$$

(2) Si $\sigma \in \mathfrak{S}_n$, on pose $P_\sigma = \big(\delta_{\sigma(i),j}\big)_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ (où $\delta_{i,j}$ est le symbole de Kronecker). On a $\det(P_\sigma) = \varepsilon(\sigma)$ (où $\varepsilon(\sigma)$ désigne la signature de σ), donc $P_\sigma \in \mathsf{GL}_n(A)$. Posons $\widetilde{P}_\sigma = \operatorname{diag}\big(1,\dots,1,\varepsilon(\sigma)\big)P_\sigma \in \mathsf{SL}_n(A)$.
Si $M \in \mathsf{M}_{n\times m}(A)$, la matrice $P_\sigma M$ est l'élément de $\mathsf{M}_{n\times m}(A)$ dont la i-ième ligne est la $\sigma(i)$-ième ligne de M. De même, si $\gamma \in \mathfrak{S}_m$ est une permutation, la matrice MP_γ est déduite de M en permutant les colonnes suivant γ. En multipliant M par $\widetilde{P}_\sigma$ à gauche (resp. par $\widetilde{P}_\gamma$ à droite), on permute les lignes suivant σ (resp. les colonnes suivant γ) et on multiplie la dernière ligne (resp. colonne) par $\varepsilon(\sigma)$ (resp. $\varepsilon(\gamma)$).

Théorème 6.5. *Tout matrice $M \in \mathsf{M}_{n\times m}(A)$ est équivalente à une matrice réduite.*

Démonstration. On peut supposer $M \neq 0$. On procède par récurrence sur $d = \min\{m, n\}$.

Supposons $d = 1$. Quitte à transposer, on peut supposer $n = 1$, de sorte que M est un vecteur ligne. Si $m = 1$, il n'y a rien à faire : supposons $m \geqslant 2$. Notons α_1 le pgcd des coefficients de M : on a $M = \alpha_1 X$ où X est un vecteur ligne dont les composantes engendrent l'idéal unité. D'après la proposition 6.2, il existe une matrice $Q \in \mathsf{SL}_n(A)$ telle que la première ligne de Q soit égale à X. On a alors $X = (1, 0, \dots, 0)Q$ et donc $MQ^{-1} = (\alpha_1, 0, \dots, 0)$.

Supposons désormais $d > 1$. Rappelons que $M \neq 0$. Soit $\delta = \min\big\{\ell(M')\,;\, M' \sim M\big\} \in \mathbf{N}$. Quitte à remplacer M par une matrice équivalente convenable, on peut supposer que $\ell(M) = \delta$. Il existe $i_0 \in \{1,\dots,n\}$ et $j_0 \in \{1,\dots,m\}$ tels que $\ell(m_{i_0,j_0}) = \delta$. Notons $\tau_{1,i_0} \in \mathfrak{S}_n$ (resp. $\tau_{1,j_0} \in \mathfrak{S}_m$) la transposition de $\{1,\dots,n\}$ (resp. $\{1,\dots,m\}$) échangeant 1 et i_0 (resp. j_0), et posons $M' = \widetilde{P}_{\tau_{1,i_0}} M \widetilde{P}^{-1}_{\tau_{1,j_0}} \in \mathsf{M}_{n\times m}(A)$ (où $\widetilde{P}_{\tau_{1,i_0}} \in \mathsf{SL}_n(A)$ et $\widetilde{P}_{\tau_{1,j_0}} \in \mathsf{SL}_m(A)$ sont les matrices de permutation modifiées, *cf* définition 6.1 (2)). On a $M' \sim M$ et $m'_{1,1} = m_{i_0,j_0}$: quitte à remplacer M par M', on peut supposer que $\ell(m_{1,1}) = \delta$. Posons $\alpha_1 := m_{1,1}$.

• Commençons par montrer que α_1 divise les coefficients de la première ligne et de la première colonne. Quitte à transposer, il suffit de traiter le cas de la première colonne. Raisonnons par l'absurde : supposons qu'il existe $i \in \{2,\dots,n\}$ tel que $\alpha_1 \nmid m_{i,1}$. Quitte à permuter la deuxième et la i-ème ligne, on peut supposer $i = 2$. Soit $\tilde{\alpha}_1 = \mathsf{pgcd}(\alpha_1, m_{2,1})$. Comme $\tilde{\alpha}_1$ divise strictement α_1, on a $\ell(\tilde{\alpha}_1) < \delta$. Par ailleurs, il existe $a, b \in A$ tels que $\tilde{\alpha}_1 = am_{1,1} + bm_{2,1}$. Posons alors

$$P = \begin{pmatrix} \overset{a}{} & \overset{b}{} & & & \\ -m_{2,1}/\tilde{\alpha}_1 & m_{1,1}/\tilde{\alpha}_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

On a $\det(P) = 1$ et le coefficient d'indice $(1,1)$ de $M' = PM$ est $\tilde{\alpha}_1$. On a $M' \sim M$ et $\ell(M') \leqslant \ell(\tilde{\alpha}_1) < \delta$, ce qui contredit la définition de δ.

• Quitte à multiplier M à gauche par la matrice

$$\begin{pmatrix} 1 & & & \\ -m_{2,1}/\alpha_1 & 1 & & \\ \vdots & & \ddots & \\ -m_{n,1}/\alpha_1 & & & 1 \end{pmatrix} \in \mathsf{SL}_n(A)$$

et à droite par la matrice

$$\begin{pmatrix} 1 & -m_{1,2}/\alpha_1 & \cdots & -m_{1,m}/\alpha_1 \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in \mathsf{SL}_m(A)$$

on peut supposer que $m_{i,1} = 0$ pour $\in \{2,\dots,n\}$ et $m_{1,j} = 0$ pour $j \in \{2,\dots,m\}$. En effet, cela donne une matrice équivalente, et de même longueur (puisqu'on a pas changé le coefficient d'indice $(1,1)$).

• La matrice M est alors de la forme $\begin{pmatrix} \alpha_1 & \\ & M_1 \end{pmatrix}$ avec $M_1 \in \mathsf{M}_{(n-1)\times(m-1)}(A)$. Par hypothèse de récurrence, il existe donc $P_1 \in \mathsf{SL}_{n-1}(A)$, $Q_1 \in \mathsf{SL}_{m-1}(A)$, $r \in \mathbf{N}$, et des éléments $\alpha_2,\dots,\alpha_r \in A\backslash\{0\}$ tels que $\alpha_i \mid \alpha_{i+1}$ pour tout $i \in \{2,\dots,r-1\}$ et

$$P_1^{-1} M_1 Q_1 = \begin{pmatrix} \alpha_2 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

Quitte à multiplier M par $\begin{pmatrix} 1 & \\ & P_1^{-1} \end{pmatrix} \in \mathsf{SL}_n(A)$ à gauche et par $\begin{pmatrix} 1 & \\ & Q_1 \end{pmatrix} \in \mathsf{SL}_m(A)$ à droite, on peut supposer que

$$M = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

Reste à voir que $\alpha_1 \mid \alpha_2$, et on aura fini. Supposons le contraire. Soit $\alpha_1' = \mathsf{pgcd}(\alpha_1, \alpha_2)$. Comme $\alpha_1 \nmid \alpha_2$, on a $\ell(\alpha_1') < \ell(\alpha_1) = \delta$. Il existe $a, b \in A$ tels que $a\alpha_1 + b\alpha_2 = \alpha_1'$. L'égalité $\left(\begin{smallmatrix} 1 & \\ a & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha_1 & \\ & \alpha_2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \\ b & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha_1 & \\ \alpha_1' & \alpha_2 \end{smallmatrix}\right)$ montre qu'il existe $M' = (m_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} \in \mathsf{M}_{n\times m}(A)$ équivalente à M et telle que $m_{2,1}' = \alpha_1'$. On a alors $\ell(M') \leqslant \ell(\alpha_1') < \delta$, ce qui contredit la définition de δ. On a fini. □

Remarques. (1) Dans le cas où A est *euclidien*, il est possible de rendre cet énoncé constructif, à l'aide d'opérations élémentaires.
(2) Dans le cas où A est un corps, on retrouve le fait bien connu que les orbites pour la relation d'équivalence sont caractérisées par le rang : toute matrice M est équivalente à $\left(\begin{smallmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{smallmatrix}\right)$ (où le nombre de 1 est $\mathsf{rg}(M)$).

Exercice 6.6. ∗∗ Soient $n, d \in \mathbf{N}_{>0}$. Montrer que le morphisme de réduction $\mathsf{SL}_d(\mathbf{Z}) \to \mathsf{SL}_d(\mathbf{Z}/n\,\mathbf{Z})$ est surjectif.

Théorème 6.7. (THÉORÈME DE LA BASE ADAPTÉE). *Soit M un sous-A-module d'un A-module L libre de rang n fini. Alors M est libre, et il existe une base $(e_1, \dots, e_n)$ de L, un entier $r \leqslant n$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que*

$$\begin{cases} \langle \alpha_{i+1} \rangle \subset \langle \alpha_i \rangle \text{ (i.e. } \alpha_i \mid \alpha_{i+1}) \text{ pour tout } i \in \{1, \dots r-1\} \\ (\alpha_1 e_1, \dots, \alpha_r e_r) \text{ soit une base de } M. \end{cases}$$

Démonstration. Comme A est principal, il est noethérien. Comme L est libre de rang fini, le A-module L est noethérien (proposition 2.18) : son sous-A-module M est donc lui aussi de type fini. Choisissons $x_1, \dots, x_m \in M$ une famille génératrice. On dispose donc d'une application A-linéaire

$$\begin{aligned} f \colon A^m &\to L \\ (a_1, \dots, a_m) &\mapsto \sum_{j=1}^{m} a_j x_j \end{aligned}$$

dont l'image n'est autre que M. Après le choix d'une base $\mathfrak{B}$ de L, cette application est donnée par une matrice $n \times m$ (dont la j-ième colonne consiste en les coordonnées de x_j dans la base $\mathfrak{B}$). D'après le théorème 6.5, cette dernière est équivalente à une matrice réduite : quitte à effectuer un changement de base de A^m et de L, elle s'écrit

$$\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

avec $r \in \{0, \dots, \min\{m, n\}\}$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que $\langle \alpha_{i+1} \rangle \subset \langle \alpha_i \rangle$ pour tout $i \in \{1, \dots, r-1\}$. Si on note $(e_1, \dots, e_n)$ la nouvelle base de L, l'image de f est donc le sous-A-module libre de base $(\alpha_1 e_1, \dots, \alpha_r e_r)$. □

Remarque. Le résultat qui précède est faux lorsque A n'est pas principal. Par exemple $\mathbf{Z}/2\,\mathbf{Z}$ est un sous-$\mathbf{Z}/4\,\mathbf{Z}$-module non libre de $\mathbf{Z}/4\,\mathbf{Z}$. De même, le sous-$\mathbf{Z} \times \mathbf{Z}$-module $\mathbf{Z} \times \{0\}$ de $\mathbf{Z} \times \mathbf{Z}$ n'est pas libre.

Rappelons que A est factoriel (*cf* proposition 5.16).

Lemme 6.8. *Soient $a \in A\backslash\{0\}$ et $p \in A$ premier. Si $M = A/\langle a \rangle$ et $k \in \mathbf{N}$, on a $p^k M/p^{k+1}M \simeq \begin{cases} A/\langle p \rangle & \text{si } k < v_p(a) \\ \{0\} & \text{sinon} \end{cases}$.*

Démonstration. Soit $i \in \mathbf{N}$. Si $i \leqslant v_p(a)$, on a $\langle a \rangle \subset p^i\rangle$, d'où $p^i M = \langle p^i \rangle / \langle a \rangle$. Si $i > v_p(a)$, on a bien entendu $p^i M \subset p^{v_p(a)} M$. Par ailleurs, on a $\mathsf{pgcd}(p^i, a) = p^{v_p(a)}$: il existe $u, v \in A$ tels que $p^{v_p(a)} = up^i + va$. Modulo $\langle a \rangle$, on en déduit que la classe de $p^{v_p(a)}$ appartient à $p^i M \subset M$, d'où $p^{v_p(a)} M \subset p^i M$, et donc en fait $p^i M = p^{v_p(a)} M$. Finalement, on a [8] $p^k M/p^{k+1}M \simeq \langle p^k \rangle / \langle p^{k+1} \rangle \simeq A/\langle p \rangle$ si $k < v_p(a)$, et $p^k M/p^{k+1}M = \{0\}$ si $k \geqslant v_p(a)$. □

Théorème 6.9. (THÉORÈME DES FACTEURS INVARIANTS). *Soit M un A-module de type fini. Alors il existe des entiers $d, r \in \mathbf{N}$ et $a_1, \dots, a_d \in A\backslash\big(\{0\} \cup A^\times\big)$ tels que*

$$\begin{cases} \langle a_{i+1} \rangle \subset \langle a_i \rangle \text{ pour tout } i \in \{1, \dots d-1\} \\ M \simeq (A/\langle a_1 \rangle) \times \cdots \times (A/\langle a_d \rangle) \times A^r \end{cases}$$

En outre, les entiers d, r et les idéaux $\langle a_1 \rangle \supset \cdots \supset \langle a_d \rangle$ sont uniques. L'entier r s'appelle le rang *de M et si $r = 0$, les éléments $(a_1, \dots, a_d)$ « les »* facteurs invariants *de M.*

8. Autre prenve : écrivons $a = p^{v_p(a)} b$ avec $\mathsf{pgcd}(p, b) = 1$. D'après le théorème des restes chinois, on a $M \simeq (A/\langle p^{v_p(a)} \rangle) \times (A/\langle b \rangle)$: comme la multiplication par p induit un automorphisme de $A/\langle b \rangle$, on peut remplacer M par $A/\langle p^{v_p(a)} \rangle$, auquel cas c'est évident.

Démonstration. • Commençons par montrer l'existence. Comme M est de type fini, choisissons une famile génératrice $m_1, \dots, m_n$: on dispose d'une application surjective

$$f\colon A^n \to M$$
$$(\lambda_1, \dots, \lambda_n) \mapsto \sum_{i=1}^{n} \lambda_i m_i.$$

Comme le A-module A^n est libre, il admet une base $(e_1, \dots, e_n)$ telle que $\mathsf{Ker}(f) = \bigoplus_{i=1}^{s} \langle \alpha_i \rangle e_i$ avec $s \in \{1, \dots, n\}$ et $\alpha_1, \dots, \alpha_s \in A \backslash \{0\}$ tels que $\langle \alpha_{i+1} \rangle \subset \langle \alpha_i \rangle$ pour tout $i \in \{1, \dots s-1\}$ (théorème de la base adaptée). En passant au quotient, f induit un isomorphisme A-linéaire

$$M \simeq A^n / \mathsf{Ker}(f) = \Big(\bigoplus_{i=1}^{s} (A/\langle \alpha_i \rangle) e_i \Big) \oplus \Big(\bigoplus_{i=s+1}^{n} A e_i \Big)$$

Soit $t = \max \big\{ i \in \{1, \dots, s\} \,;\, \alpha_i \in A^\times \big\}$ (on a $t = 0$ si $\alpha_1 \notin A^\times$). Posons $d = s - t$, $r = n - s$ et $a_i = \alpha_{t+i}$ pour $i \in \{1, \dots, d\}$. On a $a_1, \dots, a_d \in A \backslash \big(\{0\} \cup A^\times \big)$ et $\langle a_{i+1} \rangle \subset \langle a_i \rangle$ pour tout $i \in \{0, \dots d-1\}$. En outre, comme

$$A/\langle \alpha_i \rangle = \begin{cases} 0 & \text{si } i \leqslant t \\ A/\langle a_{i-t} \rangle & \text{si } t < i \leqslant s \end{cases}$$

on a bien $M \simeq (A/\langle a_1 \rangle) \times \cdots \times (A/\langle a_d \rangle) \times A^r$.
• Montrons maintenant l'unicité. On a déjà $M_{\mathrm{tors}} \simeq (A/\langle a_1 \rangle) \times \cdots \times (A/\langle a_d \rangle)$ et donc $M/M_{\mathrm{tors}} \simeq A^r$. L'entier r ne dépend donc que de M (proposition 2.13). Il suffit donc de traiter le cas où M est de torsion. On a $M \simeq \bigoplus_{i=1}^{d} (A/\langle a_i \rangle)$ avec $\langle a_1 \rangle \supset \langle a_2 \rangle \supset \cdots \supset \langle a_d \rangle$ dans $A \backslash \{0\}$. Notons $\mathscr{P}$ l'ensemble des éléments irréductibles de A. Si $p \in \mathscr{P}$, l'idéal $\langle p \rangle$ est premier non nul donc maximal (*cf* lemme 5.15) : le A-module M/pM est un $A/\langle p \rangle$-espace vectoriel de dimension finie $d_p(M)$ (on a donc $d_p(M) = \#\{i \in \{1, \dots, d\} \,;\, p \mid a_i\}$). On en déduit déjà que $d = d(M) := \max_{p \in \mathscr{P}} d_p(M)$ ne dépend que de M.
Pour tout $n \in \mathbf{N}$, on a $d_p(p^n M/p^{n+1}M) = \#\{i \in \{1, \dots, d\} \,;\, v_p(a_i) \geqslant n+1\}$ (*cf* lemme 6.8). Il en résulte que pour tout $n \in \mathbf{N}_{>0}$, l'entier

$$\#\{i \in \{1, \dots, d\} \,;\, v_p(a_i) = n\} = d_p(p^{n-1}M/p^n M) - d_p(p^n M/p^{n+1}M)$$

ne dépend que de M et de p. Comme on a $v_p(a_1) \leqslant v_p(a_2) \leqslant \cdots \leqslant v_p(a_d)$, cela implique que pour tout $p \in \mathscr{P}$ et tout $i \in \{1, \dots, d\}$, l'entier $v_p(a_i)$ ne dépend que de M et de p. Cela signifie que les idéaux $\langle a_i \rangle$ ne dépendent que de M. □

Corollaire 6.10. *Un A-module de type fini sans torsion est libre.*

Corollaire 6.11. *Les idéaux $\langle \alpha_1 \rangle \supset \cdots \supset \langle \alpha_r \rangle$ des théorèmes 6.5 et 6.7 sont uniques.*

Démonstration. Si $M = \bigoplus_{i=1}^{r} \langle \alpha_i \rangle e_i \subset \bigoplus_{i=1}^{n} A e_i = L$, on a $L/M \simeq \bigoplus_{i=1}^{r} (A/\langle \alpha_i \rangle) e_i \times A^{n-r}$. Soit s le nombre d'indices $i \in \{1, \dots, r\}$ tels que $\langle \alpha_i \rangle = A$ (*i.e.* $\alpha_i \in A^\times$). On a $L/M \simeq (A/\langle \alpha_{s+1} \rangle) \times \cdots \times (A/\langle \alpha_r \rangle) \times A^{n-r}$. D'après le théorème 6.9, les entiers $r - s$ et $n - r$ et donc s ne dépendent que de L et M (il en est donc de même de r et de s), ainsi que les idéaux $\langle \alpha_{s+1} \rangle \supset \cdots \supset \langle \alpha_r \rangle$, ce qui implique l'unicité pour le théorème 6.7. Cela implique l'unicité dans le théorème 6.5. On a fini. □

Remarque. Comme on l'a vu au cours de la preuve du théorème 6.9, si M est un A-module de type fini, alors M/M_{tors} est libre de rang fini. Il existe donc un isomorphisme $M \simeq M_{\mathrm{tors}} \oplus L$ avec L un A-module libre de rang fini (isomorphe à M/M_{tors}). Bien entendu, un tel module libre L n'a rien d'unique : on peut parler de la « partie de torsion » de M (c'est M_{tors}), mais cela n'a pas de sens de parler de la « partie libre » de M (sauf si M est déjà libre, auquel cas cela n'a aucun intérêt).

Exercice 6.12. ✻✻ Soit A un anneau factoriel tel que tout A-module de type fini sans torsion soit libre. Montrer que A est principal (utiliser le critère fourni par l'exercice 5.28 (3)).

Exercice 6.13. ✻✻✻ Soient A un anneau commutatif unitaire et X un ensemble. On note A^X le A-module des fonctions de X dans A et $A^{(X)}$ son sous-module des fonctions à support fini.
(1) Définir une application bilinéaire naturelle $\varphi\colon A^X \times A^{(X)} \to A$.
(2) Montrer que φ induit un isomorphisme de A-modules $A^X \xrightarrow{\sim} \mathsf{Hom}_{A\text{-lin}}(A^{(X)}, A)$.
(3) Montrer que φ induit une injection $\iota\colon A^{(X)} \hookrightarrow \mathsf{Hom}_{A\text{-lin}}(A^X, A)$.
On suppose désormais que $A = \mathbf{Z}$ et $X = \mathbf{N}$. On pose $E = \mathsf{Hom}_{\mathbf{Z}\text{-lin}}(\mathbf{Z}^{\mathbf{N}}, \mathbf{Z})$ et

$$\psi\colon E \to \mathbf{Z}^{\mathbf{N}}$$
$$f \mapsto (f(\varepsilon_n))_{n \in \mathbf{N}}$$

(où $\varepsilon_n = (\delta_{n,m})_{m \in \mathbf{N}}$ est le n-ième vecteur de la base canonique de $\mathbf{Z}^{(\mathbf{N})}$).
(4) En considérant les images par ψ de suites de la forme $(2^n a_n)_{n \in \mathbf{N}}$ et $(3^n b_n)_{n \in \mathbf{N}}$, montrer que tout élément $f \in E$ qui s'annule sur $\mathbf{Z}^{(\mathbf{N})}$ est identiquement nul.
(5) En regardant les images des suites de la forme $(2^{in})_{n \in \mathbf{N}}$, montrer que $\mathsf{Im}(\psi) \subset \mathbf{Z}^{(\mathbf{N})}$.
(6) En déduire que ι est un isomorphisme de $\mathbf{Z}$-modules.
(7) Conclure que $\mathbf{Z}^{\mathbf{N}}$ n'est pas un $\mathbf{Z}$-module libre.

6.14 Application aux groupes abéliens de type fini

Rappelons qu'un $\mathbf{Z}$-module n'est rien d'autre qu'un groupe abélien.

Théorème 6.15. *Soit G un groupe abélien de type fini. Il existe $r, s \in \mathbf{N}$ et $n_1, \dots, n_s \in \mathbf{N}_{>1}$ uniques tels que*

$$G \simeq \Big(\bigoplus_{k=1}^{s} \mathbf{Z}/n_k\,\mathbf{Z} \Big) \oplus \mathbf{Z}^r$$

et $n_k \mid n_{k+1}$ pour $k \in \{1, \dots, s-1\}$.

Démonstration. Comme $\mathbf{Z}$ est un anneau principal, cela résulte du théorème des facteurs invariants (*cf* théorème 6.9), en observant que si $I \subset \mathbf{Z}$ est un idéal non nul, il existe $n \in \mathbf{N}_{>0}$ unique tel que $I = \langle n \rangle$. □

Si G est un groupe abélien fini, alors il est de type fini, et G/G_{tors} est fini et libre sur $\mathbf{Z}$, donc réduit à $\{0\}$, *i.e.* $G = G_{\mathrm{tors}}$. On en déduit une classification complète des groupes abéliens finis.

Corollaire 6.16. *Si G est un groupe abélien fini, il existe $s \in \mathbf{N}$ et $n_1, \dots, n_s \in \mathbf{N}_{>1}$ uniques tels que*

$$G \simeq \bigoplus_{k=1}^{s} \mathbf{Z}/n_k\,\mathbf{Z}$$

et $n_k \mid n_{k+1}$ pour $k \in \{1, \dots, s-1\}$. En particulier, tout groupe abélien fini est produit de groupes cycliques.

Remarque. En fait, on peut démontrer ce théorème directement sans passer par la théorie des modules.

Exemple 6.17. D'après le théorème des restes chinois, on a

$$(\mathbf{Z}/6\,\mathbf{Z}) \oplus (\mathbf{Z}/10\,\mathbf{Z}) \simeq (\mathbf{Z}/2\,\mathbf{Z}) \oplus (\mathbf{Z}/3\,\mathbf{Z}) \oplus (\mathbf{Z}/10\,\mathbf{Z}) \simeq (\mathbf{Z}/2\,\mathbf{Z}) \oplus (\mathbf{Z}/30\,\mathbf{Z})$$

ce qui montre que les facteurs invariants de $(\mathbf{Z}/6\,\mathbf{Z}) \oplus (\mathbf{Z}/10\,\mathbf{Z})$ sont $(2, 30)$.

Soit p un nombre premier. Rappelons qu'un p-groupe est un groupe d'ordre une puissance de p. Par ailleurs, si $m \in \mathbf{N}_{>0}$, une *partition* de m est une suite décroissante $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_s$ d'entiers naturels non nuls telle que $m_1 + \cdots + m_s = m$. À une telle partition est associée un *diagramme de Young*, *i.e.* une collection finie de cases, ou cellules, organisée en lignes justifiées à gauche, et telle que les longueurs des lignes décroissent au sens large. Par exemple, le diagramme de Young associé à la partition $(4, 3, 1)$ de l'entier 8 est  .

Corollaire 6.18. *Soit G est un p-groupe abélien : écrivons $\#G = p^m$. Il existe une unique partition $(m_1, \dots, m_s)$ de m telle que*

$$G \simeq \bigoplus_{k=1}^{s} \mathbf{Z}/p^{m_k}\,\mathbf{Z}\,.$$

Cela montre que les classes d'isomorphisme de groupes abéliens d'ordre p^m sont en bijection avec les partitions de l'entier m, soit encore avec les diagrammes de Young correspondants

Exemple 6.19. Il y a 3 classes d'isomorphisme de groupes abéliens d'ordre p^3 :

partition	diagramme de Young	groupe
(3)		$\mathbf{Z}/p^3\,\mathbf{Z}$
(2,1)		$(\mathbf{Z}/p^2\,\mathbf{Z}) \oplus (\mathbf{Z}/p\,\mathbf{Z})$
(1,1,1)		$(\mathbf{Z}/p\,\mathbf{Z})^3$

6.20 Application à la réduction des endomorphismes

Soient K un corps commutatif, V un K-espace vectoriel. Rappelons que $\mathsf{End}_K(V)$ est une K-algèbre (la multiplication étant donnée par la composition des endomorphismes). Elle est non commutative si $\dim_K(V) > 1$. Si $f \in \mathsf{End}_K(V)$ et $P \in K[X]$, on dispose donc de $P(f) \in \mathsf{End}_K(V)$. Cela fournit un morphisme d'anneaux

$$\begin{aligned} \alpha_f \colon K[X] &\to \mathsf{End}_K(V) \\ P &\mapsto P(f), \end{aligned}$$

et munit donc V d'une structure de $K[X]$-module : on note V_f le $K[X]$-module ainsi obtenu. Réciproquement, si M est un $K[X]$-module, alors M est en particulier un K-espace vectoriel, et l'action de X sur M est donnée par un endomorphisme f_M. On a bien sûr $f_M = f$ si $M = V_f$. Ainsi $(V, f) \mapsto V_f$ est une bijection de « l'ensemble » des couples constitués d'un K-espace vectoriel V et d'un endomorphisme f de V sur « l'ensemble » des $K[X]$-modules.

Proposition 6.21. *Le K-espace vectoriel V est de dimension finie si et seulement si V_f est de type fini et de torsion.*

Démonstration. • Supposons V de dimension finie sur K. Le $K[X]$-module V_f est *a fortiori* de type fini. Par ailleurs, si $v \in V$, la famille $\big(f^n(v)\big)_{n\in\mathbf{N}}$ est liée : il existe $N \in \mathbf{N}_{>0}$ et $(\lambda_0, \dots, \lambda_N) \in K^{N+1}\backslash\{0\}$ tels que $\sum_{n=0}^{N} \lambda_n f^n(V)$, de sorte que si $P = \sum_{n=0}^{N} \lambda_n X^n$, on a $P(f)(v) = 0$: le $K[X]$-module V est de torsion.
• Réciproquement, soit $v_1, \dots, v_d$ une famille génératrice du $K[X]$-module V. Pour tout $i \in \{1, \dots, d\}$, il existe $P_i \in K[X]\backslash\{0\}$ tel que $P_i(f)(v_i) = 0$. On a donc un morphisme K-linéaire surjectif $\bigoplus_{i=1}^{d} (K[X]/\langle P_i\rangle) \to V$, d'où

$$\dim_K(V) \leqslant \dim_K\left(\bigoplus_{i=1}^{d} (K[X]/\langle P_i\rangle)\right) = \sum_{i=1}^{d} \deg(P_i) < \infty.$$

□

Remarque. On peut aussi invoquer le théorème 6.9 (c'est un peu plus rapide).

Exemple 6.22. Soit $V = K^{(\mathbf{N})}$. Soit $(e_n)_{n\in\mathbf{N}}$ la base de V définie par $e_n = (\delta_{m,n})_{m\in\mathbf{N}}$, et $f \in \mathsf{End}_K(V)$ défini par $f(e_n) = e_{n+1}$. Alors V_f est le $K[X]$-module libre de rang 1 engendré par e_0.

Définition 6.23. Supposons V de dimension finie d sur K et soit $f \in \mathsf{End}_K(V)$.
(1) L'endomorphisme f est dit *cyclique* s'il existe $v \in V$ tel que V est engendré par la famille $\big(f^n(v)\big)_{n\in\mathbf{N}}$. Cela signifie que le $K[X]$-module V_f est mongène (engendré par un élément).
(2) On note $\chi_f(X) = \det\big(X\,\mathsf{Id}_V - f\big)$ le *polynôme caractéristique* de f. C'est un polynôme de degré d à coefficients dans K.
(3) Comme $\dim_K\big(\mathsf{End}_K(V)\big) = d^2$, l'homorphisme $\alpha_f \colon K[X] \to \mathsf{End}_K(V)$ n'est pas injectif : il existe un unique polynôme unitaire $\mu_f \in K[X]$ tel que $\mathsf{Ker}(\alpha_f) = \langle\mu_f\rangle$. On l'appelle le *polynôme minimal* de f.

Proposition 6.24. *Soit $f \in \mathsf{End}_K(V)$ cyclique. Alors il existe $v \in V$ tel que la famille $\big(v, f(v), \dots, f^{d-1}(v)\big)$ soit une K-base de V, où $d = \dim_K(V)$. Dans ce cas, on a $\mu_f = \chi_f$ et $V_f \simeq K[X]/\langle\mu_f\rangle$.*

Démonstration. Soient $v \in V$ tel que $\big(f^n(v)\big)_{n\in\mathbf{N}}$ engendre le K-espace vectoriel V, et

$$\begin{aligned} \alpha_{f,v} \colon K[X] &\to V \\ P &\mapsto P(f)(v). \end{aligned}$$

C'est une application K-linéaire surjective, et $\mathsf{Ker}(\alpha_{f,v}) = \langle P_v\rangle$ avec $P_v \in K[X]$ unitaire (parce que V est de dimension finie sur K). En passant au quotient, on en déduit un isomorphisme de $K[X]$-modules $K[X]/\langle P_v\rangle \xrightarrow{\sim} V_f$. En particulier, on a $\deg(P_v) = d = \dim_K(V)$. Écrivons $P_v = X^d - \sum_{n=1}^{d} \lambda_n X^{d-n}$: on a $d = \dim_K(V)$ et $\big(v, f(v), \dots, f^{d-1}(v)\big)$ est une K-base de V.
Si $k \in \mathbf{N}$, on a $P_v(f)(f^k(v)) = f^k(P_v(f)(v)) = 0$: par K-linéarité on a $P_v(f) = 0$ et donc $\mu_f \mid P_v$. Réciproquement, comme $\mu_f(f) = 0$, on a $\mu_f \in \mathsf{Ker}(\alpha_v)$ donc $P_v \mid \mu_f$. Les polynômes P_v et μ_f étant unitaires, on a $\mu_f = P_v$.
La matrice de f dans la base $\big(v, f(v), \dots, f^{d-1}(v)\big)$ est donnée par

$$C(\lambda_1, \dots, \lambda_d) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_d \\ 1 & \ddots & & \vdots & \lambda_{d-1} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & 1 & 0 & \lambda_2 \\ 0 & \cdots & 0 & 1 & \lambda_1 \end{pmatrix}$$

(une matrice de cette forme s'appelle une *matrice compagnon*). On a

$$\det\big(X\,\mathrm{I}_n - C(\lambda_1, \dots, \lambda_d)\big) = \begin{vmatrix} X & \cdots & \cdots & 0 & -\lambda_d \\ -1 & \ddots & & \vdots & -\lambda_{d-1} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & -1 & X & -\lambda_2 \\ 0 & \cdots & 0 & -1 & X-\lambda_1 \end{vmatrix} = X \begin{vmatrix} X & \cdots & \cdots & 0 & -\lambda_{d-1} \\ -1 & \ddots & & \vdots & -\lambda_{d-2} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & -1 & X & -\lambda_2 \\ 0 & \cdots & 0 & -1 & X-\lambda_1 \end{vmatrix} + (-1)^d \lambda_d \underbrace{\begin{vmatrix} -1 & X & & 0 \\ 0 & \ddots & \ddots & \\ \vdots & \ddots & -1 & X \\ 0 & \cdots & 0 & -1 \end{vmatrix}}_{=(-1)^{d-1}}$$

$$= X\det\big(X\,\mathrm{I}_n - C(\lambda_1, \dots, \lambda_{d-1})\big) - \lambda_d = \cdots = X^d - \sum_{n=1}^{d} \lambda_n X^{d-n} = P_v$$

et donc $\chi_f = P_v = \mu_f$. □

Exemple 6.25. Si f est cyclique et $\mu_f = X^d$, alors f est nilpotent, d'indice de nilpotence d (*i.e.* $f^d = 0$ mais $f^{d-1} = 0$). Dans une base convenable, la matrice de f est de la forme

$$J_d := C(0, \dots, 0) = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

On l'appelle *bloc de Jordan de taille d*.

Théorème 6.26. (DÉCOMPOSITION DE FROBENIUS). *Soient V un K-espace vectoriel et $f \in \mathsf{End}_K(V)$. Alors il existe $r \in \mathbf{N}_{>0}$ et $V_1, \dots, V_r$ des sous-K-espaces vectoriels de V stables par f et tels que*

(1) $V = \bigoplus_{i=1}^{r} V_i$;

(2) $f_i := f_{|V_i}$ *est cyclique ;*

(3) $P_1 \mid P_2 \mid \cdots \mid P_r$ *où P_i est le polynôme minimal de f_i.*

En outre, l'entier r et les polynômes $P_1, \dots, P_r$ sont uniques.

Démonstration. Le $K[X]$-module V_f est de type fini de torsion : on peut lui appliquer le théorème des facteurs invariants (théorème 6.9). Il existe $r \in \mathbf{N}_{>0}$ et $P_1, \dots, P_r \in K[X]$ unitaires uniques tels que

$$V_f \simeq \big(K[X]/\langle P_1\rangle\big) \oplus \cdots \oplus \big(K[X]/\langle P_r\rangle\big).$$

En termes de K-espaces vectoriels, cela correspond à une décomposition $V = \bigoplus_{i=1}^{r} V_i$ en somme directe de sous-espaces stables par f, telle que si $f_i = f_{|V_i}$, on ait $V_{f_i} = V_i \simeq K[X]/\langle P_i\rangle$ pour tout $i \in \{1, \dots, r\}$. L'endomorphisme f_i est alors cyclique, et $\mu_{f_i} = P_i = \chi_{f_i}$ en vertu de la proposition 6.24. □

Remarque. (1) Il n'est pas très difficile (mais un peu long) de démontrer ce résultat directement.
(2) En termes matriciels, le théorème précédent se traduit ainsi : si $A \in \mathsf{M}_d(K)$, il existe $r \in \mathbf{N}_{>0}$, $C_1, \dots, C_r$ des matrices compagnons telles que $\chi_{C_1} \mid \cdots \mid \chi_{C_r}$ et $P \in \mathsf{GL}_d(K)$ tels que

$$P^{-1}AP = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & C_r \end{pmatrix}$$

Définition 6.27. (1) Les polynômes $P_1, \dots, P_r$ du théorème 6.26 s'appellent les *invariants de similitude* de f.
(2) Soient V_1, V_2 deux K-espaces vectoriels de dimension finie, $f_1 \in \mathsf{End}_K(V_1)$ et $f_2 \in \mathsf{End}_K(V_2)$. On dit que (V_1, f_1) et (V_2, f_2) sont *semblables* lorsqu'il existe un isomorphisme $\varphi\colon V_1 \xrightarrow{\sim} V_2$ tel que $f_2 = \varphi \circ f_1 \circ \varphi^{-1}$. Bien sûr, traduit en termes matriciels, on retrouve la notion habituelle de similitude.

Remarque. (V_1, f_1) et (V_2, f_2) sont semblables si et seulement si les $K[X]$-modules V_{1,f_1} et V_{2,f_2} sont isomorphes (si $\varphi\colon V_1 \to V_2$ est une application K-linéaire, l'application $\varphi\colon V_{1,f_1} \to V_{2,f_2}$ est $K[X]$-linéaire si et seulement si $X \cdot \varphi(v) = \varphi(X \cdot v)$ pour tout $v \in V_1$, ce qui équivaut à $f_2 \circ \varphi = \varphi \circ f_1$).

Proposition 6.28. *Soient V un K-espace vectoriel de dimension finie et $f \in \mathsf{End}_K(V)$. Notons $P_1, \dots, P_r$ ses invariants de similitude.*

(1) L'endomorphisme f est cyclique si et seulement si $r = 1$. On a alors $\mu_f = \chi_f = P_1$.

(2) On a $\chi_f = \prod_{i=1}^{r} P_i$ (en particulier, $\dim_K(V) = \sum_{i=1}^{r} \deg(P_i)$).

(3) On a $\mu_f = P_r$.

Démonstration. (1) Si f est cyclique, on a $r = 1$ par unicité de r, et donc $\mu_f = \chi_f = P_1$ en vertu de la proposition 6.24. La réciproque est évidente.

(2) Avec les notations du théorème 6.26, on a $\chi_f = \prod_{i=1}^{r} \chi_{f_i}$ vu que $V = \bigoplus_{i=1}^{r} V_i$. Mais f_i est cyclique : on a $\chi_{f_i} = \mu_{f_i} = P_i$, et on a bien $\chi_f = \prod_{i=1}^{r} P_i$.

(3) Si $P \in K[X]$, on a $P(f) = 0 \Leftrightarrow (\forall i \in \{1, \dots, r\})\ P(f_i) = 0$ (car $V = \bigoplus_{i=1}^{r} V_i$). Cela implique donc que $\mu_f = \operatorname{ppcm}_{1 \leqslant i \leqslant r}(\mu_{f_i}) = \operatorname{ppcm}_{1 \leqslant i \leqslant r}(P_i) = P_r$ vu que $P_1 \mid P_2 \mid \cdots \mid P_r$. □

Corollaire 6.29. (THÉORÈME DE CAYLEY-HAMILTON). *On a $\mu_f \mid \chi_f$, i.e. $\chi_f(f) = 0$.*

Proposition 6.30. *Soient V_1, V_2 deux K-espaces vectoriels de dimension finie, $f_1 \in \mathsf{End}_K(V_1)$ et $f_2 \in \mathsf{End}_K(V_2)$, $P_1, \dots, P_r$ et $Q_1, \dots, Q_s$ leurs invariants de similitude respectifs. Alors (V_1, f_1) et (V_2, f_2) sont semblables si et seulement si $r = s$ et $P_i = Q_i$ pour $i \in \{1, \dots, r\}$.*

Démonstration. On a $V_{1,f_1} \simeq \bigoplus_{i=1}^{r} K[X]/\langle P_i\rangle$ et $V_{2,f_2} \simeq \bigoplus_{j=1}^{s} K[X]/\langle Q_j\rangle$. Les couples (V_1, f_1) et (V_2, f_2) sont semblables si et seulement si les $K[X]$-modules $\varphi\colon V_{1,f_1}$ et V_{2,f_1} sont isomorphes : cela équivaut au fait que les $K[X]$-modules de type fini $\bigoplus_{i=1}^{r} K[X]/\langle P_i\rangle$ et $\bigoplus_{j=1}^{s} K[X]/\langle Q_j\rangle$ sont isomorphes. Par unicité dans le théorème 6.9, cela équivaut à $r = s$ et $P_i = Q_i$ pour tout $i \in \{1, \dots, r\}$. □

Exercice 6.31. Soient L/K une extension de corps et $M \in \mathsf{M}_d(K)$. Montrer que les invariants de similitude de M sont égaux à ses invariants de similitude vue comme élément de $\mathsf{M}_d(L)$. En déduire que si $M_1, M_2 \in \mathsf{M}_d(K)$ sont semblables dans $\mathsf{M}_d(L)$, alors elles sont semblables dans $\mathsf{M}_d(K)$.

Corollaire 6.32. (DÉCOMPOSITION DE JORDAN). *Soit $N \in \mathsf{M}_d(K)$ une matrice nilpotente. Alors il existe une unique suite d'entiers $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_r$ et $P \in \mathsf{GL}_d(K)$ tels que*

$$P^{-1}NP = \begin{pmatrix} J_{d_1} & 0 & \cdots & 0 \\ 0 & J_{d_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_{d_r} \end{pmatrix}$$

(où J_d désigne le bloc de Jordan de taille d).

Démonstration. Si N est nilpotente, son polynôme minimal est une puissance de X : il en est de même de ses invariants de similitude. Avec les notations du théorème 6.26, on a donc $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_r$ tels que $P_i = X^{d_i}$. Il suffit alors d'appliquer le théorème 6.26. □

Remarque. Avec les notations du corollaire 6.32, on a $d_1 + \cdots + d_r = d$, ce qui montre que $d_r \geqslant \cdots \geqslant d_1$ est une *partition* de l'entier d. Ce qui précède montre qu'il y a une bijection entre l'ensemble des classes de similitude d'endomorphismes nilpotents en dimention d et l'ensemble des partitions de d, soit encore l'ensemble des tableaux de Young correspondants (*cf* corollaire 6.18).

Définition 6.33. Soient V un K-espace vectoriel et $f \in \mathsf{End}_K(V)$. On dispose du dual $V^\vee = \mathsf{Hom}_K(V, K)$ de V (le K-espace vectoriel des formes linéaires sur V). L'endomorphisme f induit un endomorphisme

$$\begin{aligned} f^\vee : V^\vee &\to V^\vee \\ \eta &\mapsto \eta \circ f \end{aligned}$$

appelé *transposée* de f.

Proposition 6.34. *Soient V un K-espace vectoriel de dimension finie, $f \in \mathsf{End}_K(V)$ et $\mathfrak{B} = (e_1, \ldots, e_d)$ une base de V. Notons M la matrice de f dans la base $\mathfrak{B}$ et $\mathfrak{B}^* = (e_1^*, \ldots, e_d^*)$ la base duale[9] de $\mathfrak{B}$. La matrice de $f^\vee$ dans $\mathfrak{B}^*$ est la transposée de M.*

Démonstration. Écrivons $M = (a_{i,j})_{1 \leqslant i,j \leqslant d} \in \mathsf{M}_d(K)$. Si $j \in \{1, \ldots, d\}$, on a $f^\vee(e_j^*) = e_j^* \circ f$: si $i \in \{1, \ldots, d\}$, on a

$$f^\vee(e_j^*)(e_i) = e_j^*(f(e_i)) = e_j^*\Big(\sum_{k=1}^{d} a_{k,i} e_k\Big) = a_{j,i}$$

ce qui montre que $f^\vee(e_j^*) = \sum_{i=1}^{d} a_{j,i} e_i^*$. Cela signifie précisément que la matrice de $f^\vee$ dans la base $\mathfrak{B}^*$ est ${}^tM$. □

Corollaire 6.35. *Supposons V de dimension finie. Alors (V, f) et $(V^\vee, f^\vee)$ sont semblables.*

Démonstration. D'après le théorème 6.9, on a $V = \bigoplus_{i=1}^{r} V_i$ avec $f_i := f_{|V_i}$ cyclique. Comme $V^\vee = \bigoplus_{i=1}^{r} V_i^\vee$, il suffit donc de traiter le cas où f est cyclique. Soit alors $v \in V$ tel que $\mathfrak{B} = \big(v, f(v), \ldots, f^{d-1}(v)\big)$ soit une K-base de V. Écrivons $\chi_f = \mu_f = X^d - \sum_{k=1}^{d} \lambda_k X^{d-k}$, de sorte que $f^d(v) = \sum_{k=1}^{d} \lambda_k f^{d-k}(v)$. La matrice de f dans la base $\mathfrak{B}$ est la matrice compagnon $C(\lambda_1, \ldots, \lambda_d)$: d'après la proposition 6.34, cette de $f^\vee$ dans la base duale $\mathfrak{B}^*$ est

$${}^tC(\lambda_1, \ldots, \lambda_d) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ \lambda_d & \cdots & \cdots & \lambda_2 & \lambda_1 \end{pmatrix}$$

Comme les polynômes caractéristiques (resp. minimaux) d'une matrice et de sa transposée sont les mêmes, on a en particulier $\chi_{f^\vee} = \chi_f = \mu_f = \mu_{f^\vee}$ et donc $f^\vee$ est cyclique (*cf* proposition 6.28), de même invariants de similitude que f : les endomorphismes f et $f^\vee$ sont donc semblables d'après la proposition 6.30. □

Remarque. Bien sûr, cela implique que pour tout $A \in \mathsf{M}_d(K)$, les matrices A et ${}^tA$ sont semblables. Notons que lorsque K est algébriquement clos, cela peut se démontrer directement en utilisant la décomposition de Dunford. Pour traiter le cas général, on peut alors invoquer le résultat de « descente » classique suivant : si L/K est une extension de corps et si $A_1, A_2 \in \mathsf{M}_d(K)$ sont semblables dans $\mathsf{M}_d(L)$, alors elles sont déjà semblables dans $\mathsf{M}_d(K)$ (*cf* exercice 6.31).

Exercice 6.36. Soient K un corps. Montrer que si $A, B \in \mathsf{M}_3(K)$ ont même polynôme minimal et même polynôme caractéristique, alors elles sont semblables. Montrer parr un exemple que cette implication est fausse dans $\mathsf{M}_4(K)$.

9. Caractérisée par $e_i^*(e_j) = \delta_{i,j}$ pour $i, j \in \{1, \ldots, d\}$.

7 Compléments

7.1 Le lemme de Nakayama

Définition 7.2. Soit A un anneau. Le *radical* $\mathsf{rad}(A)$ de A est l'intersection des idéaux maximaux de A (c'est donc un idéal de A).

Exercice 7.3. Soit $a \in \mathbf{N}_{>0}$. Calculer $\mathsf{rad}(\langle a\rangle) \subset \mathbf{Z}$ en termes des diviseurs premiers de a.

Lemme 7.4. $1 + \mathsf{rad}(A) \subset A^\times$.

Démonstration. Soient $x \in \mathsf{rad}(A)$ et $a = 1 + x$: pour tout idéal maximal $\mathfrak{m} \subset A$, on a $a \notin \mathfrak{m}$, et donc $\langle a\rangle \not\subset \mathfrak{m}$: d'après le théorème de Krull, on a $\langle a\rangle = A$, *i.e.* $a \in A^\times$. □

Théorème 7.5. (LEMME DE NAKAYAMA [10]). *Soient A un anneau, $I \subset A$ un ideal et M un A-module de type fini. Si $IM = M$, il existe $a \in 1 + I$ tel que $aM = \{0\}$. En particulier, si $I \subset \mathsf{rad}(A)$, on a $M = \{0\}$.*

Démonstration. • Soit $\{x_1, \dots, x_r\}$ une famille génératrice du A-module de type fini M. Si $i \in \{1, \dots, r\}$, on a $x_i \in IM$: il existe $\lambda_{i,1}, \dots, \lambda_{i,r} \in I$ tels que $x_i = \sum_{j=1}^{r} \lambda_{i,j} x_j$, *i.e.* $\sum_{j=1}^{r} (\delta_{i,j} - \lambda_{i,j}) x_j = 0$. Posons $N = (\delta_{i,j} - \lambda_{i,j})_{1\leqslant i,j\leqslant r} \in \mathsf{M}_r(A)$ et $a = \det(N)$: on a $a \in 1 + I$. Écrivons ${}^t\mathsf{com}(N) = (\mu_{i,j})_{1\leqslant i,j\leqslant r} \in \mathsf{M}_r(A)$: comme $aI_r = {}^t\mathsf{com}(N)N$, on a $\delta_{i,j} a = \sum_{k=1}^{r} \mu_{i,k}(\delta_{k,j} - \lambda_{k,j})$ pour tout $i, j \in \{1, \dots, r\}$. En multipliant par x_j et en sommant sur $j \in \{1, \dots, r\}$, on en déduit que $ax_i = \sum_{k=1}^{r} \mu_{i,k} \sum_{j=1}^{r} (\delta_{k,j} - \lambda_{k,j}) x_j = 0$. Comme c'est vrai pour tout $i \in \{1, \dots, r\}$, cela montre que $aM = \{0\}$.
• Si $I \subset \mathsf{rad}(A)$, on a $a \in 1 + I \subset 1 + \mathsf{rad}(A) \subset A^\times$ (*cf* lemme 7.4) : l'égalité $aM = \{0\}$ implique $M = \{0\}$. □

Remarque. (1) Une reformulation de la deuxième partie du théorème est $(A/\mathsf{rad}(A)) \otimes_A M = \{0\} \Rightarrow M = \{0\}$.
(2) On s'en doute, l'énoncé tombe en défaut sans l'hypothèse de finitude sur M. Par exemple, soit p un nombre premier et $A = \mathbf{Z}_{(p)}$ la localisation de $\mathbf{Z}$ en l'idéal premier $\langle p\rangle$: c'est un anneau dont l'unique idéal maximal est $\langle p\rangle$ et de corps résiduel $\mathbf{F}_p$. Soit $M = \mathbf{Q}/\mathbf{Z}$: c'est un A-module non nul, et $\mathbf{F}_p \otimes_A M = \{0\}$.

Exercices 7.6. (1) Soient A un anneau, et M un A-module de type fini tel que $\mathfrak{m}M = M$ pour tout idéal maximal $\mathfrak{m} \subset A$. Montrer que $M = \{0\}$.
(2) Soient A un anneau et $I \subset A$ un idéal tel que $I^2 = I$. Montrer que I est engendré par un élément e tel que $e^2 = e$.

Définition 7.7. Un anneau est dit *local* s'il n'a qu'un seul idéal maximal.

Corollaire 7.8. *Soient A un anneau local, de corps résiduel k, et soient M un A-module de type fini, N un A-module.*
(1) Si N est de type fini sur A et $M \otimes_A N = \{0\}$, alors $M = \{0\}$ ou $N = \{0\}$.
(2) Soit $f\colon N \to M$ une application A-linéaire telle que $\mathsf{Id}_k \otimes f\colon k \otimes_A N \to k \otimes_A M$ soit surjective. Alors f est surjective.

Démonstration. (1) On a $\{0\} = k \otimes_A \otimes M \otimes_A N \simeq M \otimes_A k \otimes_A N \simeq (M \otimes_A k) \otimes_k (k \otimes_A N)$. Comme on a $\dim_k \big((M \otimes_A k) \otimes_k (k \otimes_A N)\big) = \dim_k(k \otimes_A M) \dim_k(k \otimes_A N)$, on a $\dim_k(k \otimes_A M) = 0$ ou $\dim_k(k \otimes_A N) = 0$. Comme M et N sont de type fini, le lemme de Nakayama implique que $M = \{0\}$ ou $N = \{0\}$.
(2) Par exactitude à droite du produit tensoriel, on a $k \otimes_A \mathsf{Coker}(f) = \{0\}$: comme $\mathsf{Coker}(f)$ est de type fini (étant un quotient de M qui est de type fini), le lemme de Nakayama implique que $\mathsf{Coker}(f) = \{0\}$, *i.e.* que f est surjectif. □

Corollaire 7.9. *Soit A un anneau, M un A-module de type fini et $f \in \mathsf{End}_A(M)$. Si f est surjectif, alors f est injectif.*

Démonstration. Considérons M comme un $A[X]$-module (l'action de X étant donnée par f) : comme il est de type fini comme un A-module, il est *a fortiori* de type fini comme un $A[X]$-module. Comme f est surjectif, on a $XM = M$: par le lemme de Nakayama, il existe $P \in A[X]$ tel que $P \in 1 + XA[X]$ et $PM = 0$, *i.e.* $P(f) = 0$ sur M. Écrivons $P(X) = 1 - XQ(X)$ avec $Q \in A[X]$: on a $\mathsf{Id}_M = f \circ Q(f)$, donc f est un automorphisme, d'inverse $Q(f)$. □

7.10 Extensions entières

Dans tout ce qui suit, A est un anneau et B une A-algèbre (*i.e.* un anneau B muni d'un morphisme d'anneaux $A \to B$).

Définition 7.11. (1) Un élément $b \in B$ est dit *entier* sur A s'il existe $P \in A[X]$ *unitaire* tel que $P(b) = 0$. L'égalité $P(b) = 0$ s'appelle alors une *relation de dépendance intégrale*.
(2) On dit que B est *entière* sur A si tous ses éléments sont entiers sur A.

10. 中山

Exemples 7.12. (1) L'élément $\sqrt{2} \in \mathbf{C}$ (resp. $\alpha = \frac{1+\sqrt{5}}{2} \in \mathbf{C}$) est entier sur $\mathbf{Z}$, une relation de dépendance intégrale étant donnée par $(\sqrt{2})^2 - 2 = 0$ (resp. $\alpha^2 - \alpha - 1 = 0$).
(2) On verra plus tard que $\frac{\sqrt{2}}{2} \in \mathbf{C}$ n'est pas entier sur $\mathbf{Z}$.
(3) Si A et B sont des corps, alors $b \in B$ est entier sur A si et seulement si b est algébrique sur A, et B est entière (resp. finie) sur A si et seulement si elle est algébrique (resp. de degré fini).

Proposition 7.13. *Soit $b \in B$. Les conditions suivantes sont équivalentes :*
(i) b est entier sur A ;
(ii) la A-algèbre $A[b]$ est finie [11] *;*
(iii) il existe un sous-A-module $B' \subset B$ de type fini, contenant un élément non diviseur de zéro et stable par la multiplication par b (i.e. tel que $bB' \subset B'$).

Démonstration. $(i) \Rightarrow (ii)$ Soient $P \in A[X]$ unitaire tel que $P(b) = 0$. Si $\deg(P) = n$, le A-module $A[b]$ est engendré par $\{1, b, \dots, b^{n-1}\}$ (division euclidienne), donc de type fini.
$(ii) \Rightarrow (iii)$ On prend $B' = A[b]$ (il contient 1 qui n'est pas diviseur de zéro).
$(iii) \Rightarrow (i)$ Soit $(\beta_1, \dots, \beta_n)$ une famille génératrice du A-module B'. Pour tout $i \in \{1, \dots, n\}$, on a $b\beta_i \in B'$: il existe $M = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ telle que $b\beta_i = \sum_{j=1}^{n} a_{i,j}\beta_j$. Posons $X = (\beta_i)_{1 \leqslant i \leqslant n} \in \mathsf{M}_{n\times 1}(B)$: on a $MX = bX$, *i.e.*

$$(b\mathrm{I}_n - M)X = 0. \qquad (*)$$

Posons $P(X) = \det(X\mathrm{I}_n - M)$. C'est un polynôme unitaire de degré n, à coefficients dans A. En multipliant l'égalité $(*)$ par la transposée de la comatrice de $b\mathrm{I}_n - M$, il vient $P(b)X = 0$: on a $P(b)B' = 0$, et donc $P(b) = 0$ (car B' contient un élément non diviseur de zéro). Comme le polynôme $P(X) \in A[X]$ est unitaire, l'élément b est entier sur A. □

Lemme 7.14. *Soient $b_1, \dots, b_n \in B$ tels que b_i soit entier sur $A[b_1, \dots, b_{i-1}]$ pour tout $i \in \{1, \dots, n\}$. Alors la A-algèbre $A[b_1, \dots, b_n]$ est finie.*

Démonstration. On procède par récurrence sur n, le cas $n = 1$ résultant de la proposition 7.13. Supposons $n > 1$ et posons $A' = A[b_1, \dots, b_{n-1}] \subset B$. Par hypothèse de récurrence, la A-algèbre A' est finie, et comme b_n est entier sur A', la A'-algèbre $A'[b_n]$ est finie. Il en résulte que la A-algèbre $A[b_1, \dots, b_n] = A'[b_n]$ est finie. □

Corollaire 7.15. *Soient $b, b' \in B$ entiers sur A. Alors $b - b'$ et bb' sont entiers sur A.*

Démonstration. D'après le lemme 7.14, l'extension $A \subset A[b, b']$ est finie donc entière : comme $b - b', bb' \in A[b, b']$, ils sont entiers sur A. □

Proposition 7.16. *La A-algèbre B est finie si et seulement si elle est entière et de type fini.*

Démonstration. Si B est finie sur A, elle est entière en vertu de la proposition 7.13 (c'est $(iii) \Rightarrow (i)$ avec $B' = B$). Par ailleurs, si $\{b_1, \dots, b_n\}$ est une partie génératrice du A-module B, le morphisme de A-algèbres $A[X_1, \dots, X_n] \to B$ qui envoie X_i sur b_i est surjectif, de sorte que B est de type fini sur A.
Réciproquement, supposons B entière et de type fini sur A. On peut écrire $B = A[b_1, \dots, b_n]$, et comme $b_1, \dots, b_n$ sont entiers sur A, le A-module B est de type fini d'après le lemme 7.14. □

Proposition 7.17. *Si B est une A-algèbre entière et C une B-algèbre entière, alors C est une A-algèbre entière.*

Démonstration. Soient $c \in C$ et $P(c) = 0$, avec $P(X) = X^n + b_1X^{n-1} + \cdots + b_n \in B[X]$, une relation de dépendance intégrale. Comme B est entière sur A, les éléments $b_1, \dots, b_n$ sont entiers sur A : d'après le lemme 7.14, $B' = A[b_1, \dots, b_n]$ est finie sur A. Comme $B'[c]$ est finie sur B, elle est finie sur A, ce qui implique que c est entier sur A (proposition 7.13, en notant que $1 \in B'[c]$). □

Exercice 7.18. $***$ Soient A un anneau noethérien, B une A-algèbre de type fini et G un groupe fini qui agit par automorphismes de A-algèbre sur B. Montrer que la sous-algèbre des points fixes B^G est de type fini sur A.

Remarque. Si B est une A-algèbre et $b \in B$ est inversible et entier sur A, l'inverse $b^{-1} \in B$ n'est pas entier sur A en général.

Définition 7.19. (1) D'après le corollaire 7.15, l'ensemble des éléments de B qui sont entiers sur A est une sous-A-algèbre de B. On l'appelle la *clôture intégrale* de A dans B.
(2) Supposons A intègre et notons K son corps des fractions. La *clôture intégrale* de A est la clôture intégrale de A dans K. On dit que A est *intégralement clos* s'il est égal à sa clôture intégrale, c'est-à-dire lorsque les seuls éléments de K entiers sur A sont les éléments de A.

Proposition 7.20. *Tout anneau factoriel est intégralement clos. En particulier, tout anneau principal est intégralement clos.*

11. *Ie.* de type fini vue comme A-module.

Démonstration. Soient A un anneau factoriel, K son corps des fractions et $x \in K$ entier sur A. Écrivons $x = a/b$ avec $a \in A$ et $b \in A\backslash\{0\}$ premiers entre eux. Soit $x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = 0$ une relation de dépendance intégrale (avec $\alpha_1, \ldots, \alpha_n \in A$). En la multipliant par b^n, on a $a^n + \alpha_1 a^{n-1} b + \cdots + \alpha_n b^n = 0$, de sorte que b divise a^n. Comme a et b sont premiers entre eux, cela implique $b \in A^\times$, et donc $x = ab^{-1} \in A$. □

Exemple 7.21. Soient K un corps, t une indéterminée et $A = K[t^2, t^3] \subset B = K[t]$. Alors A et B ont même corps des fractions $K(t)$. Comme B est factoriel (car principal), il est intégralement clos d'après la proposition 7.20. L'élément t est entier sur A, mais $t \notin A$, de sorte que A n'est pas intégralement clos (et donc non factoriel d'après la proposition 7.20).

Proposition 7.22. *Soient A un anneau intègre, K son corps des fractions et L/K une extension algébrique de corps. Notons B la clôture intégrale de A dans L. Alors pour tout $x \in L$, il existe $a \in A\backslash\{0\}$ tel que $ax \in B$. En particulier, on a*[12] *$L = \mathsf{Frac}(B)$ et B est intégralement clos.*

Démonstration. Soient $x \in L$ et $X^d + \alpha_1 X^{d-1} + \cdots + \alpha_d \in K[X]$ son polynôme minimal. Il existe $a \in A\backslash\{0\}$ tel que $a\alpha_i \in A$ pour tout $i \in \{1, \ldots, d\}$. Le polynôme minimal de ax est alors $X^d + a\alpha_1 X^{d-1} + \cdots + a^d\alpha_n \in A[X]$, donc $ax \in B$. Cela implique que $\mathsf{Frac}(B) = L$. Si $x \in L$ est entier sur B, alors il est entier sur A (proposition 7.17), de sorte que $x \in B$, et B est intégralement clos. □

Proposition 7.23. *Sous les hypothèses de la proposition 7.22, soit $S \subset A$ une partie multiplicative. Alors la clôture intégrale de $S^{-1}A \subset K$ dans L est $S^{-1}B$ (« la clôture intégrale commute aux localisations »).*

Démonstration. Soient $b \in B$ et $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ une relation de dépendance intégrale sur A. Si $s \in S$ et $x = \frac{b}{s} \in S^{-1}B$, on a $x^n + \frac{a_1}{s} x^{n-1} + \cdots + \frac{a_n}{s^n} = 0$, ce qui montre que x est entier sur $S^{-1}A$. Réciproquement, soient $x \in L$ entier sur $S^{-1}A$ et $x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = 0$ une relation de dépendance intégrale sur $S^{-1}A$. Il existe $s \in S$ tel que $a_i := s\alpha_i \in A$ pour tout $i \in \{1, \ldots, n\}$ (on prend pour s un dénominateur commun aux α_i). Posons $b = sx \in L$: on a $b^n + a_1 b^{n-1} + sa_2 b^{n-2} + \cdots + s^{n-2} a_{n-1} b + s^{n-1} a_n = 0$, ce qui montre que b est entier sur A. On a donc $b \in B$, et $x \in S^{-1}B$. □

Définition 7.24. Un *corps de nombres* est une extension finie de $\mathbf{Q}$ (généralement, on la voit comme un sous-corps de $\mathbf{C}$). Si K est un corps de nombres, l'*anneau des entiers* de K est la clôture intégrale de $\mathbf{Z}$ dans K. On la note $\mathcal{O}_K$. D'après la proposition précédente, c'est un anneau intégralement clos et $K = (\mathbf{Z}\backslash\{0\})^{-1}\mathcal{O}_K$.

Proposition 7.25. *Soient A un anneau intègre et intégralement clos, $K = \mathsf{Frac}(A)$ et L/K une extension algébrique. Un élément de L est entier sur A si et seulement si son polynôme minimal est à coefficients dans A.*

Démonstration. Soient $x \in L$ et $P \in K[X]$ son polynôme minimal. Si $P \in A[X]$, l'égalité $P(x) = 0$ est une relation de dépendance intégrale, et x est entier sur A. Réciproquement, supposons $x \in L$ entier sur A. Fixons $\overline{L}$ une clôture algébrique de L, et soient $x_1, \ldots, x_n \in \overline{L}$ les racines de P dans $\overline{L}$ (*i.e.* les conjugués de x, comptés avec multiplicités). Si $i \in \{1, \ldots, n\}$, il existe un K-isomorphisme de corps $f\colon K(x) \to K(x_i)$ qui envoie x sur x_i (théorème de prolongement des isomorphismes). Si $Q(x) = 0$ est une relation de dépendance intégrale (avec $Q \in A[X]$), on a $Q(x_i) = Q(f(x)) = f(Q(x)) = 0$, si bien que x_i est entier sur A pour tout $i \in \{1, \ldots, n\}$. D'après le corollaire 7.15, il en est donc de même des coefficients de P (qui sont, au signe près, des polynômes symétriques en $x_1, \ldots, x_n$). Comme ces coefficients appartiennent à K et A est intégralement clos dans K par hypothèse, on a $P \in A[X]$. □

Exemple 7.26. $\frac{\sqrt{2}}{2}$ n'est pas entier sur $\mathbf{Z}$ (son polynôme minimal sur $\mathbf{Q}$ est $X^2 - \frac{1}{2} \notin \mathbf{Z}[X]$).

Proposition 7.27. *Soient $d \in \mathbf{Z}\backslash\{0, 1\}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$. Alors*

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \mod 4\,\mathbf{Z} \\ \mathbf{Z}[\sqrt{d}] & \text{si } d \not\equiv 1 \mod 4\,\mathbf{Z} \end{cases}$$

Démonstration. Soit $x = \lambda + \mu\sqrt{d} \in K$ avec $\lambda, \mu \in \mathbf{Q}$. Les conjugués de x sont x et $y = \lambda - \mu\sqrt{d}$: son polynôme minimal est $P(X) = X^2 - 2\lambda X + \lambda^2 - d\mu^2$. Comme $\mathbf{Z}$ est factoriel, il est intégralement clos : d'après la proposition 7.25, x est entier sur $\mathbf{Z}$ si et seulement si $2\lambda \in \mathbf{Z}$ et $\lambda^2 - d\mu^2 \in \mathbf{Z}$. On a en particulier $(2\lambda)^2 - d(2\mu)^2 \in 4\,\mathbf{Z}$. Cela implique déjà $d(2\mu)^2 \in \mathbf{Z}$, et donc $2\mu \in \mathbf{Z}$ (parce que d est dans facteur carré). Si $2\mu \notin 2\,\mathbf{Z}$, alors 2μ a une image inversible dans $\mathbf{Z}/4\,\mathbf{Z}$, et d est un carré modulo 4. Ce n'est possible que si $d \equiv 0, 1 \mod 4\,\mathbf{Z}$. On n'a pas $d \in 4\,\mathbf{Z}$ (parce que d est sans facteur carré). Il en résulte que si $d \not\equiv 1 \mod 4\,\mathbf{Z}$, on a $2\mu \in 2\,\mathbf{Z}$, *i.e.* $\mu \in \mathbf{Z}$, et donc $\lambda^2 \in \mathbf{Z}$ *i.e.* $\lambda \in \mathbf{Z}$, ce qui implique que $\mathcal{O}_K \subset \mathbf{Z}[\sqrt{d}]$ dans ce cas. L'inclusion réciproque est évidente.

Supposons désormais que $d \equiv 1 \mod 4\,\mathbf{Z}$, et posons $\alpha = \frac{1+\sqrt{d}}{2}$. On a $\alpha^2 = \frac{1+d+2\sqrt{d}}{4} = \frac{d-1}{4} + \alpha$, de sorte que $\alpha \in \mathcal{O}_K$, donc $\mathbf{Z}[\alpha] \subset \mathcal{O}_K$. On a $x = \lambda - \mu + 2\mu\alpha$. Si $x \in \mathcal{O}_K$, on a vu que $2\mu \in \mathbf{Z}$, donc $\lambda - \mu = x - 2\mu\alpha \in \mathcal{O}_K$. Comme $\lambda - \mu \in \mathbf{Q}$ et $\mathbf{Z}$ est intégralement clos, cela implique $\lambda - \mu \in \mathbf{Z}$, et $x = \lambda - \mu + 2\mu\alpha \in \mathbf{Z} + \mathbf{Z}\,\alpha \subset \mathcal{O}_K$: on a $\mathcal{O}_K = \mathbf{Z}[\alpha]$. □

12. Comme le montre la preuve, on a en fait $L = (A\backslash\{0\})^{-1}B$.

Exercices 7.28. (1) Trouver un contre-exemple à l'énoncé du théorème 7.25 lorsque A n'est pas supposé intégralement clos.
(2) Soient A un anneau factoriel dans lequel 2 est inversible, $\alpha \in A$ sans facteur carré (*i.e.* non divisible par le carré d'un élément premier) et $B = A[\sqrt{\alpha}]$. Montrons que B est intégralement clos.

Proposition 7.29. *Soient $A \to B$ un morphisme* injectif *avec B intègre*[13] *et entier sur A. Alors A est un corps si et seulement si B est un corps.*

Démonstration. Supposons que A soit un corps, et soit $b \in B\backslash\{0\}$. Comme B est entière sur A, on a une relation de dépendance intégrale $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, avec $a_1, \ldots, a_n \in A$. Comme B est supposé intègre, on peut supposer $a_n \neq 0$ (sinon on divise l'égalité par b). On a alors $bc = 1$ avec $c = -a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) \in B$, donc b est inversible dans B, et B est un corps.
Réciproquement, supposons que B soit un corps. Si $a \in A\backslash\{0\}$, alors a a une image non nulle donc inversible dans B : on note $a^{-1} \in B$ son inverse. Comme B est entière sur A, on dispose d'une relation de dépendance intégrale $(a^{-1})^n + \alpha_1 (a^{-1})^{n-1} + \cdots + \alpha_n = 0$ avec $\alpha_1, \ldots, \alpha_n \in A$: on a $a^{-1} = -\alpha_1 - \alpha_2 a - \cdots - \alpha_n a^{n-1} \in A$, et A est un corps. □

Proposition 7.30. *Soit B une A-algèbre entière. Si $\mathfrak{M} \subset B$ est un idéal maximal, alors $\mathfrak{M} \cap A$ est un idéal maximal de A. Réciproquement, si $\mathfrak{m} \subset A$ est un idéal maximal, il existe un idéal premier $\mathfrak{M} \subset B$ tel que $\mathfrak{m} = \mathfrak{M} \cap A$, et les tels $\mathfrak{M}$ sont maximaux dans B.*

Démonstration. • Supposons $\mathfrak{M} \subset B$ maximal, et posons $\mathfrak{m} = \mathfrak{M} \cap A$. On dispose du morphisme injectif $A/\mathfrak{m} \to B/\mathfrak{M}$. La $A/\mathfrak{m}$-algèbre $B/\mathfrak{M}$ est entière parce que B l'est sur A (si $b \in B$ et $P(b) = 0$ est une relation de dépendance intégrale, avec $P \in A[X]$, on a $\overline{P}(\overline{b}) = 0$ où $\overline{P} \in (A/\mathfrak{m})[X]$ et $\overline{b} \in B/\mathfrak{M}$ désignent la réduction de P modulo $\mathfrak{m}A[X]$ et la réduction de b modulo $\mathfrak{M}$ respectivement). Comme $B/\mathfrak{M}$ est un corps, il en est de même de $A/\mathfrak{m}$ en vertu de la proposition 7.29, et $\mathfrak{m}$ est maximal dans A.

• Soit $\mathfrak{m} \subset A$ maximal. Commençons par montrer que $\mathfrak{m}B \neq B$. Supposons au contraire que $\mathfrak{m}B = B$, *i.e.* $1 \in \mathfrak{m}B$: on peut écrire

$$1 = \sum_{i=1}^{r} \alpha_i b_i \qquad (*)$$

avec $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}$ et $b_1, \ldots, b_n \in B$. Comme B est entière sur A, il en est de même de $B' = A[b_1, \ldots, b_n]$. Comme B' est de type fini sur A, la A-algèbre B' est en fait finie (*cf* proposition 7.16) : on peut écrire $B' = A\beta_1 + \cdots + A\beta_n$. Par ailleurs, l'égalité $(*)$ implique que $\mathfrak{m}B' = B'$. Le Lemme de Nakayama (*cf* théorème 7.5) implique qu'il existe $a \in 1 + \mathfrak{m}$ tel que $aB' = 0$. Comme $1 \in B'$, cela implique que $a = 0$, *i.e.* que $1 \in \mathfrak{m}$, ce qui est absurde : on a nécessairement $\mathfrak{m}B \neq B$.
Comme l'idéal $\mathfrak{m}B \subset B$ est propre, il existe $\mathfrak{M} \subset B$ maximal tel que $\mathfrak{m}B \subset \mathfrak{M}$ (théorème de Krull). On a bien sûr $\mathfrak{m} \subset \mathfrak{M} \cap A$, et donc $\mathfrak{m} = \mathfrak{M} \cap A$ vu que $\mathfrak{m}$ est maximal dans A.
• Si $\mathfrak{P} \subset B$ est premier et tel que $\mathfrak{m} = \mathfrak{P} \cap A$, on dispose du morphisme injectif $A/\mathfrak{m} \to B/\mathfrak{P}$. Il fait de $B/\mathfrak{P}$ une $A/\mathfrak{m}$-algèbre entière vu que B l'est sur A, et $B/\mathfrak{P}$ est intègre : comme $A/\mathfrak{m}$ est un corps, il en est de même de $B/\mathfrak{P}$ d'après la proposition 7.29, si bien que $\mathfrak{P}$ est en fait maximal dans B. □

13. Ce qui implique que A est intègre.