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)
松村 英之 (H. Matsumura), *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

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

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

Version du 9 octobre 2024

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

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

avec la convention $\sigma_0 = 1$. □

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

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 $i \in \{1, \dots, r\}$, 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 $X_1X_2 \cdots X_i$. Le monôme le plus grand de $\sigma_1^{a_1} \cdots \sigma_r^{a_r}$ est donc

$$X_1^{a_1}(X_1X_2)^{a_2} \cdots (X_1X_2 \cdots X_r)^{a_r} = X_1^{a_1+a_2+\cdots+a_r} X_2^{a_2+\cdots+a_r} \cdots X_{r-1}^{a_{r-1}+a_r} X_r^{a_r}$$

(on retrouve 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 $P_1 = P - \alpha\sigma_1^{n_1-n_2}\sigma_2^{n_2-n_3} \cdots \sigma_{r-1}^{n_{r-1}-n_r}\sigma_r^{n_r} \in A[X_1, \dots, X_r]$. 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 précède, 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 $Y_1, \dots, Y_r$). Le monôme le plus grand de $P = Q(\sigma_1, \dots, \sigma_r)$ (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 $\alpha_1, \dots, \alpha_r$ (dans une extension L de K), l'évaluation d'un polynôme symétrique à coefficients dans K en $\alpha_1, \dots, \alpha_r$ peut se faire sans connaitre $\alpha_1, \dots, \alpha_r$, 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 $k[X_1, \dots, X_r]$ est factoriel (*cf* corollaire 4.26), le théorème 1.4 s'étend aux fractions rationnelles : le groupe $\mathfrak{S}_r$ agit sur le corps $L := k(X_1, \dots, X_r)$, et le sous-corps des invariants est $K := k(\sigma_1, \dots, \sigma_r)$. 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 $\sum_{i<j} X_i^2X_j^2 = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4$.

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

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

(k-ième polynôme de Newton). Comme ce polynôme est symétrique, c'est un polynôme en $\sigma_1, \dots, \sigma_r$ 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 $\sigma_1, \sigma_2, \dots, \sigma_r$. 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 $S_1, \dots, S_r$. Remarquons néanmoins qu'il faut alors inverser les entiers $2, 3, \dots, r$, 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* [1] 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 $M^{\{1,\dots,n\}}$.

Définition 2.4. Soit M un A-module. Un *sous-module* [2] 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 $\prod_{\lambda\in\Lambda} M_\lambda$.

1. 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).
2. 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.

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

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

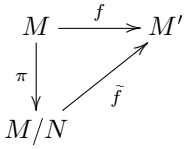
(l'ensemble des sommes *finies* d'éléments de $\bigcup_{\lambda\in\Lambda} M_\lambda$). C'est un sous-module de M, qu'on appelle la *somme* de $(M_\lambda)_{\lambda\in\Lambda}$.

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 $N \subseteq \mathsf{Ker}(f)$, il existe une unique application A-linéaire $\widetilde{f}\colon M/N \to M'$ telle que $f = \widetilde{f} \circ \pi$.



En particulier, si $f\colon M \to M'$ est un morphisme de A-modules, on dispose de la *décomposition canonique* $f = \iota \circ \widetilde{f} \circ \pi$ où $\iota\colon \mathsf{Im}(f) \to M'$ est l'inclusion, $\widetilde{f}$ 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 $(f(e_\lambda))_{\lambda\in\Lambda}$.

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*[3].

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 $(f(e_\lambda))_{\lambda\in\Lambda} \in \left(A^{(\Lambda')}\right)^{\Lambda}$ (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 $\widetilde{\pi}\colon \left(A^{(\Lambda')}\right)^{\Lambda} \to \left((A/\mathfrak{m})^{(\Lambda')}\right)^{\Lambda}$: notons $\overline{f} \in \mathsf{Hom}_{A/\mathfrak{m}}\left((A/\mathfrak{m})^{(\Lambda)}, (A/\mathfrak{m})^{(\Lambda')}\right)$ 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 $m_1, \ldots, m_r \in M$ tels qu'il soit engendré par $\{m_1, \ldots, m_r\}$. Comme la réunion est croissante, il existe $N \in \mathbf{N}$ tel que $\{m_1, \ldots, m_r\} \subset M_N$. On a alors $M_N \subseteq \sum_{n\in\mathbf{N}} M_n \subset M_N$ 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.
• 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 $M'_n \subsetneq M'_{n+1} \subset M'$.

3. 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.

(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 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 $\operatorname{ann}_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z}) = \{0\}$.

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

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 $M_{\text{tors}} = (\mathbf{Z} \times \{0\}) \cup (\{0\} \times \mathbf{Z})$ 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 **??**).

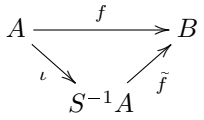
Exercice 2.24. ✻✻✻ Soient A un anneau unitaire, M un A-module noethérien et $f : M \to M$ une application A-linéaire.
(1) On suppose f surjective. Montrer que c'est un isomorphisme (indication : considérer les sous-modules $K_n = \mathsf{Ker}(f^n)$).
(2) Si f est supposée injective, est-ce automatiquement 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 Localisation

Définition 3.1. Une partie $S \subset A$ est dit *multiplicative* si $0 \notin S$, $1 \in S$ et si S est stable par multiplication.

Exemple 3.2. (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 3.3. *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 $f : A \to B$ est un homomorphisme d'anneaux tel que $(\forall s \in S)\ f(s) \in B^\times$, alors il existe un unique homomorphisme d'anneaux $\widetilde{f} : S^{-1}A \to B$ 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 $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}$ 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

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

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 $f : A \to B$ un homomorphisme d'anneaux tel que $(\forall s \in S)\ f(s) \in B^\times$. L'application

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

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 3.4. 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 3.5. (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 3.6. Trouver des ensembles multiplicatifs $S \subset \mathbf{Z}$ autres que $\mathbf{Z}\backslash\{0\}$ tels que $S^{-1}\,\mathbf{Z} = \mathbf{Q}$.

Définition 3.7. 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 $\frac{a}{s}\cdot\frac{m}{s'} := \frac{am}{ss'}$. 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 $f_S\big(\frac{m}{s}\big) = \frac{f(m)}{s}$ 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 3.8. *(1)* $\big(\mathsf{Id}_M\big)_S = \mathsf{Id}_{S^{-1}M}$.
(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. □

4 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*.

4.1 Généralités

Définition 4.2. (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 4.3. $*$ (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 4.4. 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 4.5. 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 4.6 (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 4.7. (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 4.16). Il en est de même de $A[X]$ si A est factoriel (*cf* théorème 4.25).
(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 4.8. *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 4.9. *L'anneau A est factoriel si et seulement si tout élément non nul de A admet une factorisation en produit d'éléments irréductibles*[4] *et si tout élément irréductible est premier.*

Démonstration. On sait déjà que si A est factoriel, alors tout élément irréductible est premier (proposition 4.8). 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. □

4. Cette condition est satisfaite lorsque A est noethérien.

4.10 Pgcd, ppcm

Supposons A factoriel.

Définition 4.11. 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 4.12 (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 4.6 (2)). □

Exercice 4.13. ∗ Soient $a, b, c \in A$. Montrer que $\mathsf{pgcd}(a, b, c) = \mathsf{pgcd}(a, \mathsf{pgcd}(b, c))$.

4.14 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 4.15. *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 4.16. *Tout anneau principal est factoriel.*

Démonstration. D'après la proposition 4.9 et le lemme 4.15, 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 4.15, 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 $\pi_1, \ldots, \pi_n$ et $a_1, \ldots, a_n$ telles que $a_{k-1} = \pi_k a_k$ pour tout $k \in \{1, \ldots, n\}$ (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 4.25) 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 4.17. Si K est un corps et $n \in \mathbf{N}_{>1}$, l'anneau $K[X_1, \ldots, X_n]$ est factoriel (*cf* théorème 4.25) 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 4.18. $*$ 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.

4.19 Transfert de la factorialité

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

Définition 4.20. Soit $P = a_0 + a_1X + \cdots + a_dX^d \in A[X]\backslash\{0\}$. Le *contenu* de P est

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

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 4.21. *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 $k \in \{0, \ldots, d\}$, 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 $\mathsf{c}(\widetilde{P}) = \mathsf{pgcd}(b_0, \ldots, b_d) = 1$, *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 4.22. *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 4.21, 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 4.21, 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 4.23. (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 4.24. $*$ Soient $P, Q \in K[X]$ des polynômes unitaires tels que $PQ \in A[X]$. Montrer que $P, Q \in A[X]$.

Théorème 4.25. *(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 4.22 (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 4.22 (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 4.9). D'après le lemme 4.21 (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 4.16), on peut écrire $P = P_1P_2\cdots P_r$ avec $P_1, \ldots, P_r$ irréductibles dans $K[X]$. Pour tout $k \in \{1, \ldots, r\}$, 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 4.22 (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 4.26. *L'anneau $A[X_1, \ldots, X_n]$ est factoriel.*

Exemple 4.27. Les anneaux $\mathbf{Z}[X_1, \ldots, X_n]$ et $K[X_1, \ldots, X_n]$ (où K est un corps) sont factoriels.

Exercices 4.28. $***$ (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.