Chapitre 3

Algèbres, polynômes, algèbres de type fini

Version du 14 octobre 2004

Dans ce chapitre, tous les anneaux considérés sont commutatifs.

3.1 Algèbres et extension des scalaires

3.1.1 Algèbres

Définition 3.1.1 *Soient A, B deux anneaux commutatifs non nuls. On dit que B est une A-algèbre si l'on s'est donné un morphisme d'anneaux $\phi : A \to B$.*

Dans ce cas, B est aussi un A-module, via

$$a \cdot b = \phi(a)b, \qquad \forall a \in A, b \in B.$$

De plus, la multiplication $B \times B \to B$ est A-bilinéaire, donc induit (et est déterminée par) une application A-linéaire $\mu : B \otimes_A B \to B$.

Remarque 3.1.1 Si $A = k$ est un corps, tout morphisme $k \to B$ est injectif et donc, dans ce cas, une k-algèbre est un anneau commutatif contenant k comme sous-anneau.

3.1.2 Extension et restriction des scalaires

Soit B une A-algèbre.

Proposition 3.1.1 *Soit M un A-module. Alors $B \otimes_A M$ est un B-module, appelé le B-module obtenu par extension des scalaires à partir de M. De plus, l'application*

$$\sigma_B : M \longrightarrow B \otimes_A M, \qquad m \mapsto 1 \otimes m,$$

est un morphisme de A-modules.

Démonstration. Fixons $b \in B$. On vérifie que l'application

$$B \times M \longrightarrow B \otimes_A M, \qquad (c, m) \mapsto bc \otimes m,$$

est A-bilinéaire. Elle induit donc une application

$$\theta_b : B \otimes_A M \longrightarrow B \otimes_A M,$$

telle que $\theta_b(c \otimes m) = bc \otimes m$, pour tout $c \in B$, $m \in M$. Ceci définit une structure de B-module sur $B \otimes_A M$. En effet, il est clair que $\theta_1 = \mathrm{id}_{B \otimes_A M}$, et il faut vérifier que

$$\theta_{bb'} = \theta_b \circ \theta_{b'}$$

pour tout $b, b' \in B$. Comme les éléments $c \otimes m$ engendrent le A-module $B \otimes_A M$, il suffit de vérifier que

$$\theta_{bb'}(c \otimes m) = \theta_b \left(\theta_{b'}(c \otimes m)\right),$$

pour tout $c \in B$, $m \in M$. Mais ceci est clair, car les deux membres égalent $bb'c \otimes m$. Ceci prouve la 1ère assertion. La 2ème est facile et laissée au lecteur. □

Définition 3.1.2 *Réciproquement, tout B-module N est muni, via ϕ, d'une structure de A-module définie par*

$$a \cdot n = \phi(a)n,$$

pour tout $a \in A$, $n \in N$. On parle alors de restriction des scalaires. Si l'on veut spécifier que l'on regarde N comme A-module, on écrira $N|_A$.

Proposition 3.1.2 [Propriété universelle de l'extension des scalaires]
Soient M un A-module et N un B-module. L'application

$$\alpha : \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_B(B \otimes_A M, N), \quad \phi \mapsto \widetilde{\phi}$$

où $\widetilde{\phi}$ est le B-morphisme tel que $\widetilde{\phi}(b \otimes m) = b\phi(m)$ pour tout $b \in B$, $m \in M$, est une bijection. Son inverse est l'application $\beta : \psi \mapsto \psi|_M$, où $\psi|_M$ est définie par $\psi|_M(m) = \psi(1 \otimes m)$, pour tout $m \in M$.

Démonstration. Soit $\phi \in \mathrm{Hom}_A(M,N)$. On vérifie que l'application

$$B \times M \longrightarrow N, \qquad (b,m) \mapsto b\phi(m)$$

est A-bilinéaire. Par conséquent, elle induit un morphisme de A-modules $\widetilde{\phi} : B \otimes_A M \to N$, tel que

$$\widetilde{\phi}(b \otimes m) = b\phi(m),$$

pour tout $b \in B$, $m \in M$. De plus, $\widetilde{\phi}$ est un morphisme de B-modules, car pour tout $b, c \in B$ et $m \in M$, on a

$$\widetilde{\phi}(b \cdot (c \otimes m)) = \widetilde{\phi}(bc \otimes m) = bc\phi(m) = b\widetilde{\phi}(c \otimes m).$$

Ceci montre que α est bien définie. On voit alors facilement que

$$(\beta \circ \alpha)(\phi) = \phi \quad \text{et} \quad (\alpha \circ \beta)(\psi) = \psi,$$

pour tout $\phi \in \mathrm{Hom}_A(M,N)$ et $\psi \in \mathrm{Hom}_B(B \otimes_A M, N)$. Ceci prouve la proposition. □

3.1.3 Localisation de modules

Soit S une partie multiplicative de A et soit M un A-module. De la même façon qu'on a défini, dans le paragraphe 1.4.2, l'anneau localisé A_S, noté aussi $S^{-1}A$, on définit un A-module, noté M_S ou $S^{-1}M$, de la façon suivante.

On considère l'ensemble $C = M \times S$ des couples (m,s), où $m \in M$ et $s \in S$, et sur cet ensemble on considère la relation suivante. On pose

$$(m,s) \sim (m',t)$$

s'il existe $u \in S$ tel que $u(tm - sm') = 0$. On vérifie, comme en 1.4.2, que ceci est une relation d'équivalence.

On note $S^{-1}M$, ou M_S, l'ensemble des classes d'équivalence, et, pour tout $(m,s) \in C$, on désigne par $[m,s]$ son image dans $S^{-1}M$. On définit sur $S^{-1}M$ une addition et une action de $S^{-1}A$ par les formules suivantes. Pour tout $m, m' \in M$, $s, t \in S$ et $a \in A$, on pose :

$$(*) \qquad [m,s] + [m',t] = [tm + sm', st], \qquad [a,s][m,t] = [am, st].$$

On vérifie, comme en 1.4.2, que ceci est bien défini, et munit $S^{-1}M$ d'une structure de $S^{-1}A$-module et donc, a fortiori, de A-module, via l'application $A \to S^{-1}A$.

On obtient ainsi les deux premiers points du théorème suivant.

Théorème 3.1.3 1) *$S^{-1}M$ est un $S^{-1}A$-module, donc a fortiori un A-module via le morphisme d'anneaux $\tau : A \to S^{-1}A$, et l'application*

$$\tau_M : M \to S^{-1}M, \qquad m \mapsto [m, 1]$$

est un morphisme de A-modules. Son noyau est

$$\ker \tau_M = \{m \in M \mid \exists s \in S \text{ tel que } sm = 0\}.$$

Pour tout $m \in M$ et $s \in S$, l'on a $[m, s] = \tau(s)^{-1}m$.

2) *De plus, $S^{-1}M$ vérifie la propriété universelle suivante : pour tout $S^{-1}A$-module N et tout morphisme de A-modules $\phi : M \to N$, il existe un* **unique** *morphisme de $S^{-1}A$-modules $\Phi : S^{-1}M \to N$ tel que $\Phi \circ \tau_M = \phi$.*

3) *Par conséquent, il existe un unique isomorphisme de $S^{-1}A$-modules*

$$\eta : S^{-1}M \xrightarrow{\sim} S^{-1}A \otimes_A M$$

tel que $\eta([m, 1]) = 1 \otimes m$, pour tout $m \in M$.

Démonstration. Les points 1) et 2) se démontrent comme au paragraphe 1.4.2 ; le détail des vérifications est laissé au lecteur. Démontrons le point 3).

D'après la démonstration du corollaire 1.4.2, il suffit de montrer que le morphisme de A-modules

$$\sigma : M \longrightarrow S^{-1}A \otimes_A M, \qquad m \mapsto 1 \otimes m$$

vérifie la propriété universelle énoncée en 2). Mais ceci résulte de la propriété universelle de l'extension des scalaires (proposition 3.1.2). Ceci prouve le théorème. □

3.1.4 Produit tensoriel de A-algèbres

Proposition 3.1.4 *Soient B, C deux A-algèbres. Il existe sur $B \otimes C$ une unique structure de A-algèbre telle que*

$$(*) \qquad (b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc',$$

pour tout $b, b \in B$, $c, c' \in C$.

Démonstration. Si une telle structure existe, elle est uniquement déterminée par $(*)$, puisque le A-module $B \otimes C$ est engendré par les éléments $\beta \otimes \gamma$, pour $\beta \in B$ et $\gamma \in C$. Il suffit donc de montrer l'existence.

On peut démontrer l'existence en introduisant la notion d'application n-linéaire, et en observant que l'application

$$B \times C \times B \times C \longrightarrow B \otimes C, \qquad (b, c, b', c') \mapsto bb' \otimes cc'$$

est 4-linéaire. C'est la méthode adoptée dans les références [AM] et [La]. La démonstration qui suit est tirée de [Laf] (Chap.IV, §I.9).

Comme B, resp. C, est une A-algèbre, sa multiplication induit une application A-linéaire

$$\mu_B : B \otimes_A B \longrightarrow B, \qquad \text{resp.,} \quad \mu_C : C \otimes_A C \longrightarrow C.$$

Alors, l'application $\mu_B \times \mu_C : (B \otimes B) \times (C \otimes C) \longrightarrow B \otimes C$ est A-bilinéaire, donc induit une application A-linéaire

$$\mu' : B \otimes B \otimes C \otimes C \longrightarrow B \otimes C,$$

telle que $\mu'(b \otimes b' \otimes c \otimes c') = bb' \otimes cc'$, pour tout $b, b' \in B$ et $c, c' \in C$. Ici, on a omis les parenthèses car le produit tensoriel est associatif. Comme il est aussi commutatif, on a un isomorphisme de A-modules

$$\eta : B \otimes C \otimes B \otimes C \xrightarrow{\sim} B \otimes B \otimes C \otimes C$$

tel que $\eta(b \otimes b' \otimes c \otimes c') = b \otimes c \otimes b' \otimes c'$ pour tout b, b' et c, c'. Alors, $\mu = \mu' \circ \eta$ est un morphisme de A-modules

$$B \otimes C \otimes B \otimes C \longrightarrow B \otimes C$$

tel que

$$(*) \qquad \mu(b \otimes c \otimes b' \otimes c') = bb' \otimes cc',$$

pour tout $b, b' \in B$ et $c, c' \in C$. Il reste à voir que la multiplication sur $B \otimes C$ ainsi définie est associative et commutative, et admet $1 \otimes 1$ pour élément neutre. Par bilinéarité, il suffit de vérifier ces propriétés sur des éléments de la forme $b \otimes c$ et $b' \otimes c'$, et alors c'est clair d'après $(*)$. Ceci prouve la proposition. □

3.2 Algèbres de polynômes et algèbres de type fini

3.2.1 Monoïdes et algèbres associées

Définition 3.2.1 *Un monoïde est un ensemble S muni d'une loi associative $S \times S \to S$, notée $(s, t) \mapsto st$. On dit que le monoïde est unitaire s'il possède un élément 1 tel que $1 \cdot s = s = s \cdot 1$ pour tout s, et qu'il est commutatif si la loi est commutative.*

Lemme 3.2.1 *Soient X, Y, Z trois ensembles et soit P un A-module. On a des bijections*

$$\mathrm{Hom}_{Ens}(X \times Y, Z) \cong \mathrm{Hom}_{Ens}(X, \mathrm{Hom}_{Ens}(Y, Z)); \quad (1)$$
$$\mathrm{Hom}_A(AX \otimes_A AY, P) \cong \mathrm{Hom}_{Ens}(X \times Y, P). \quad (2)$$

Démonstration. Le 1er point est laissé au lecteur. Démontrons le second. D'après la propriété universelle du produit tensoriel, et celle du A-module libre associé à un ensmeble, on a des bijections

$$\begin{aligned} \mathrm{Hom}_A(AX \otimes_A AY, P) &\cong \mathrm{Hom}_A(AX, \mathrm{Hom}_A(AY, P)) \\ &\cong \mathrm{Hom}_{\mathrm{Ens}}(X, \mathrm{Hom}_A(AY, P)) \\ &\cong \mathrm{Hom}_{\mathrm{Ens}}(X, \mathrm{Hom}_{\mathrm{Ens}}(Y, P)). \end{aligned}$$

Alors, (2) découle du point (1), appliqué à $Z = P$. Ceci prouve le lemme. □

Exercice 3.2.1 Déduire de la démonstration ci-dessus que l'on a un isomorphisme de A-modules $AX \otimes AY \cong A(X \times Y)$.

On peut maintenant démontrer la proposition suivante.

Proposition 3.2.2 [A-algèbre associée à un monoïde]
Soit S un monoïde commutatif unitaire. Alors l'application A-linéaire $\mu : AS \otimes AS \longrightarrow AS$ définie par

$$\mu(e_s \otimes e_t) = e_{st}, \qquad \forall s, t \in S,$$

fait de AS une A-algèbre commutative.

Démonstration. Il résulte du lemme précédent, appliqué à $X = Y = S$ et $P = AS$, qu'il existe une unique application A-linéaire $\mu : AS \otimes AS \to AS$, telle que

$$\mu(e_s \otimes e_t) = e_{st}$$

pour tout $s, t \in S$. Il reste à montrer que la multiplication ainsi définie est associative et commutative, et que e_1 est élément neutre. Par bilinéarité, il suffit de vérifier ces propriétés sur des éléments de la forme e_u, pour $u \in S$, et c'est alors clair d'après la formule précédente. Ceci prouve la proposition. □

3.2.2 Algèbres de polynômes

Soit A un anneau commutatif. On suppose connue du lecteur la définition de l'anneau de polynômes $A[X]$, où X est une "indéterminée". On va généraliser cela au cas de n indéterminées, de la façon suivante.

On considère le monoïde

$$\mathbb{N}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{N}\},$$

muni de l'addition coordonnée par coordonnée. C'est un monoïde commutatif unitaire, dont l'élément neutre est $0 = (0, \ldots, 0)$. Pour tout $k = 1, \ldots, n$, notons ε_k l'élément de $\mathbb{N}$ dont toutes les coordonnées sont nulles, sauf la k-ième qui vaut 1 et notons

$$X_k = e_{\varepsilon_k}$$

l'élément de $A\mathbb{N}^n$ qui lui est associé. Pour tout $\nu = (a_1, \ldots, a_n)$, on a $\nu = a_1\varepsilon_1 + \cdots + a_n\varepsilon_n$ et donc, d'après la définition de la multiplication dans $A\mathbb{N}^n$,

$$e_\nu = X_1^{a_1} \cdots X_n^{a_n}.$$

De même, si $\eta = (b_1, \ldots, b_n)$, on a

$$(**) \qquad X_1^{a_1} \cdots X_n^{a_n} \cdot X_1^{b_1} \cdots X_n^{b_n} = e_{\nu+\eta} = X_1^{a_1+b_1} \cdots X_n^{a_+b_n}.$$

On désignera $A\mathbb{N}^n$ par $A[X_1, \ldots, X_n]$. On a ainsi obtenu la proposition suivante.

Proposition 3.2.3 *$A[X_1, \ldots, X_n]$ est le A-module libre de base les monômes*

$$X^\nu := X_1^{\nu_1} \cdots X_n^{\nu_n},$$

pour tout $\nu \in \mathbb{N}^n$, muni de la multiplication A-bilinéaire définie par $(**)$. C'est une A-algèbre, appelée algèbre des polynômes en n indéterminées sur A.

Pour tout $\nu \in \mathbb{N}^n$, on pose $|\nu| = \nu_1 + \cdots + \nu_n$ et on l'appelle le degré (total) du monôme X^ν. Tout élément $P \in A[X_1, \ldots, X_n]$ est une somme finie de termes $a_\nu X^\nu$, avec $a_\nu \in A \setminus \{0\}$, et le plus grand des degrés $|\nu|$ s'appelle le degré de P et se note $\deg P$ *; ainsi P peut s'écrire comme somme finie*

$$P = \sum_{\eta \in \mathbb{N}, |\eta| \leq \deg P} a_\eta X^\eta.$$

De plus, $A[X_1, \ldots, X_n]$ vérifie la propriété universelle suivante.

Théorème 3.2.4 (Propriété universelle de $A[X_1, \ldots, X_n]$)
Pour toute A-algèbre commutative B, et tout n-uplet $(b_1, \ldots, b_n)$ d'éléments de B, il existe un unique morphisme de A-algèbres $\phi : A[X_1, \ldots, X_n] \to B$ tel que $\phi(X_i) = b_i$, pour $i = 1, \ldots, n$.

Démonstration. Un tel morphisme, s'il existe, doit vérifier, pour tout $\nu \in \mathbb{N}^n$,

$$(*) \qquad \phi(X^\nu) = b_1^{\nu_1} \cdots b_n^{\nu_n}.$$

Réciproquement, comme $\mathcal{A} := A[X_1, \ldots, X_n]$ est un A-module libre de base les X^ν, pour $\nu \in \mathbb{N}^n$, on peut définir un morphisme de A-modules $\phi : \mathcal{A} \to B$ par la formule $(*)$ ci-dessus. Alors $\phi(1) = 1$ et il reste à vérifier que $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$, pour tout $\alpha, \beta \in \mathcal{A}$. Par bilinéarité, il suffit de le vérifier lorsque $\alpha = X^\nu$ et $\beta = X^\eta$ sont des monômes. Mais alors c'est clair, car

$$\phi(X^{\nu+\eta}) = b_1^{\nu_1+\eta_1} \cdots b_n^{\nu_n+\eta_n} = b_1^{\nu_1} \cdots b_n^{\nu_n} \cdot b_1^{\eta_1} \cdots b_n^{\eta_n}.$$

Ceci prouve le théorème. □

Exercice 3.2.2 Montrer que l'on a un isomorphisme de A-algèbres

$$A[X_1, \ldots, X_n] \cong (A[X_1, \ldots, X_{n-1}])[X_n].$$

3.2.3 Algèbres de type fini

Soit B une A-algèbre. (On rappelle que, dans ce chapitre, tous les anneaux sont commutatifs).

Définition 3.2.2 *On dit que B est une A-algèbre de type fini si elle est engendrée comme A-algèbre par un nombre fini d'éléments $x_1, \ldots, x_n$. Ceci signifie que tout élément de B peut s'écrire (de façon non unique en général) comme une combinaison A-linéaire finie de monômes $x_1^{\nu_1} \cdots x_n^{\nu_n}$.*

Proposition 3.2.5 *B est une A-algèbre de type fini $\Leftrightarrow$ B est isomorphe à un quotient d'une algèbre de polynômes $A[X_1, \ldots, X_n]$.*

Démonstration. Si B est engendrée comme A-algèbre par $x_1, \ldots, x_n$, alors le morphisme de A-algèbres $\phi : A[X_1, \ldots, X_n] \to B$ défini par $\phi(X_i) = x_i$ est surjectif, donc induit un isomorphisme de A-algèbres

$$(*) \qquad A[X_1, \ldots, X_n]/I \xrightarrow{\sim} B,$$

où $I = \ker \phi$. Réciproquement, si l'on a un isomorphisme $(*)$, notons x_i l'image dans B de X_i. Alors les x_i engendrent B comme A-algèbre. Ceci prouve la proposition. □

Chapitre 4

Anneaux et modules noethériens

Version du 14 octobre 2004

4.1 Modules noethériens

Soit A un anneau et M un A-module à gauche.

Proposition 4.1.1 *Les conditions suivantes sont équivalentes.*

1) *Tout sous-module de M est de type fini ;*

2) *Toute suite croissante de sous-modules de M est stationnaire, c.-à-d., pour toute suite croissante de sous-modules*

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

il existe un entier k tel que $N_k = N_i$ pour tout $i \geq k$.

3) *Toute famille non-vide de sous-modules de M admet un élément maximal.*

Démonstration. 1) $\Rightarrow$ 2) Supposons 1) vérifiée et soit

$$(*) \qquad N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

une suite croissante de sous-modules. Posons $N = \bigcup_{i \geq 0} N_i$. D'après le lemme 2.9.2, N est un sous-module de M. Par hypothèse, il est engendré par un nombre fini d'éléments $x_1, \ldots, x_k$. Alors, il existe un entier r tel que

$x_1, \ldots, x_k$ appartiennent tous à N_r. Donc $N = N_r$ et la suite $(*)$ est stationnaire à partir du cran r.

2) $\Rightarrow$ 3) Supposons qu'une famille non-vide $\mathcal{F}$ de sous-modules de M ne possède pas d'élément maximal. Soit N_0 un élément de $\mathcal{F}$. Comme il n'est pas maximal, il est contenu strictement dans un élément N_1 de $\mathcal{F}$. Ce dernier n'étant pas maximal, par hypothèse, il est contenu strictement dans un élément N_2 de $\mathcal{F}$. On construit ainsi une suite strictement croissante

$$N_0 \subset N_1 \subset N_2 \subset \cdots$$

de sous-modules de M, en contradiction avec l'hypothèse 2).

3) $\Rightarrow$ 1) Soit N un sous-module de M et soit $\mathcal{F}$ la famille des sous-modules de type fini de N. Elle est non-vide, car elle contient le sous-module (0). Donc, elle possède un élément maximal N'. Soit $n \in N$ arbitraire. Alors $N' + An$ est un sous-module de N de type fini (car il est engendré par n et un système de générateurs de N'). Par maximalité de N', on a $N' = N' + An$, d'où $n \in N'$. Ceci montre que $N' = N$, et donc N est de type fini. La proposition est démontrée. □

Définition 4.1.1 *On dit que M est (un module) noethérien s'il vérifie les conditions équivalentes de la proposition précédente. (Ceci entraîne, en particulier, que M soit de type fini).*

Remarque 4.1.1 (qu'on peut ignorer) Pour être très précis, signalons que la preuve de l'implication 2) $\Rightarrow$ 3) utilise une version faible de l'axiome du choix, appelée Axiome du Choix Dépendant (ACD) (voir [Kri, p.167]). Essentiellement, ceci équivaut à dire que si pour tout x_n on peut trouver un x_{n+1}, alors on peut trouver une suite infinie $(x_n)_{n\in\mathbb{N}}$. Cet argument est utilisé si fréquemment, par exemple en analyse lorsqu'on invoque l'existence de suites, et paraît si évident intuitivement, que la plupart du temps on ne relève pas l'usage de (ACD) et l'on construit des suites sans se poser de problème. Pour cette raison, on peut donc oublier cette remarque !

Proposition 4.1.2 *Soient M un A-module, N un sous-module, et $Q = M/N$ le module quotient.*

1) *Si M est noethérien, N et Q le sont aussi.*

2) *Réciproquement, si N et Q sont noethériens, M l'est aussi.*

Démonstration. 1) Supposons M noethérien et soit N', resp. Q', un sous-module de N, resp. Q. Comme N' est un sous-module de M, il est de type

fini. D'autre part, $Q' = M'/N$, où $M' = \pi^{-1}(Q')$ est un sous-module de M. Par hypothèse, M' est de type fini, donc Q' l'est aussi, d'après la proposition 2.3.2.

2) Supposons N et $Q = M/N$ noethériens. Notons π la projection $M \to Q$. Soit M' un sous-module de M. Par hypothèse, le sous-module $\pi(M)$ de Q est de type fini donc il existe $x_1, \ldots, x_n \in M'$ dont les images engendrent $\pi(M)$. Ceci entraîne que pour tout $m \in M'$, il existe $a_1, \ldots, a_n \in A$ tels que

$$m - (a_1x_1 + \cdots + a_nx_n) \in N \cap M'. \tag{1}$$

D'autre part, le sous-module $N \cap M'$ de N est lui aussi de type fini, donc engendré par des éléments $y_1, \ldots, y_s$. Donc, il existe $b_1, \ldots, b_s \in A$ tels que

$$m - (a_1x_1 + \cdots + a_nx_n) = b_1y_1 + \cdots + b_sy_s. \tag{2}$$

Ceci montre que M' est engendré par $x_1, \ldots, x_r$, $y_1, \ldots, y_s$. La proposition est démontrée. □

Corollaire 4.1.3 *Soit $M_1, \cdots, M_n$ un nombre fini de modules noethériens. Alors $M_1 \oplus \cdots \oplus M_n$ est noethérien.*

Démonstration. Supposons d'abord $n = 2$. Alors M_1 est un sous-module de $M_1 \oplus M_2$ et le module quotient $(M_1 \oplus M_2)/M_1$ est isomorphe à M_2 (exercice : s'en convaincre !). Dans ce cas, le corollaire résulte du point 2) de la proposition précédente.

Enfin, le cas général s'en déduit par récurrence, puisque pour tout $n \geq 3$ l'on a

$$M_1 \oplus \cdots \oplus M_n \cong (M_1 \oplus \cdots \oplus M_{n-1}) \oplus M_n.$$

Le corollaire est démontré. □

4.2 Anneaux noethériens

Soit A un anneau.

Définition 4.2.1 *On dit que A est noethérien à gauche (resp. à droite) s'il est noethérien comme A-module à gauche (resp. à droite). On dira que A est noethérien s'il est à la fois noethérien à gauche et à droite. Bien sûr, si A est commutatif ces trois notions coïncident.*

Proposition 4.2.1 *Supposons A noethérien à gauche et soit M un A-module à gauche. Alors M est noethérien $\Leftrightarrow$ M est de type fini.*

Démonstration. L'implication $\Rightarrow$ est claire. Réciproquement, dire que M est de type fini équivaut à dire que c'est un quotient de A^n, pour un certain $n \geq 1$. Or A^n est noethérien, d'après le corollaire 4.1.3, et tout module quotient de A^n l'est aussi, d'après la proposition 4.1.2. □

4.3 Le théorème de transfert de Hilbert

Dans cette section, A est un anneau commutatif.

Théorème 4.3.1 (Théorème de transfert de Hilbert) *Si A est noethérien, $A[X]$ l'est aussi.*

Démonstration. Soit I un idéal non nul de $A[X]$. Soit D le sous-ensemble de A formé de 0 et des coefficients dominants des polynômes appartenant à I. On voit facilement que D est un idéal de A. Par hypothèse, il est engendré par des éléments $\alpha_1, \ldots, \alpha_r$.

Pour tout $i = 1, \ldots, r$, soit P_i un élément de I dont le coefficient dominant est α_i, et soit $d_i = \deg P_i$. Soit d le plus grand des d_i, soit M le sous-A-module de $A[X]$ engendré par les monômes $1, X, \ldots, X^{d-1}$ et soit $N = M \cap I$. Comme A est noethérien et M de type fini, alors N est de type fini, donc engendré comme A-module par des éléments $Q_1, \ldots, Q_s$. Alors, I est égal à l'idéal J engendré par

$$P_1, \ldots, P_r, Q_1, \ldots, Q_s.$$

En effet, montrons par récurrence sur n que tout élément $P \neq 0$ de I, de degré n, appartient à J. C'est clair si $n < d$, car dans ce cas $P \in N$ donc est combinaison A-linéaire de $Q_1, \ldots, Q_s$. Soit donc $n \geq d$ et supposons l'assertion établie pour $n' < n$. Soit $P \in I \setminus \{0\}$, de degré n, et soit α son coefficient dominant. Alors $\alpha \in D$ donc il existe $a_1, \ldots, a_r \in A$ tels que

$$\alpha = a_1\alpha_1 + \cdots + a_r\alpha_r.$$

Alors,

$$a_1\alpha_1 X^{n-d_1} P_1 + \cdots + a_r\alpha_r X^{n-d_r} P_r$$

a pour terme dominant αX^n. Par conséquent,

$$P - \sum_{i=1}^{r} a_i\alpha_i X^{n-d_i} P_i$$

est un élément de I de degré $< n$. Il appartient donc à J, par hypothèse de récurrence, et donc l'on a aussi $P \in J$. Ceci prouve le théorème. □

Remarque 4.3.1 En anglais, le théorème précédent est appelé “Hilbert's Basis Theorem".

Corollaire 4.3.2 *Si A est noethérien, toute A-algèbre de type fini l'est aussi.*

Démonstration. Ceci résulte du théorème précédent et de la proposition 4.1.2. □

4.4 Un résultat d'Artin et Tate

On déduit du théorème précédent la proposition suivante, dûe à Artin et Tate. Elle sera utilisée plus loin dans la preuve du Théorème des zéros de Hilbert.

Proposition 4.4.1 *Soient $A \subseteq B \subseteq C$ des anneaux commutatifs. On suppose que A est noethérien, que C est une A-algèbre de type fini, et que C est de type fini comme $\underline{B\text{-module}}$. Alors, B est une A-algèbre de type fini. En particulier, B est noethérien.*

Démonstration. Soient $x_1, \ldots, x_m$ des générateurs de C comme A-algèbre, et soient $y_1, \ldots, y_n$ des générateurs de C comme $\underline{B\text{-module}}$. Alors, on a des expressions de la forme

$$x_r = \sum_{j=1}^{n} b_{rj} y_j \qquad (b_{ij} \in B); \tag{1}$$

$$y_i y_j = \sum_{k=1}^{n} b_{ijk} y_k \qquad (b_{ijk} \in B). \tag{2}$$

Soit B_0 la sous-A-algèbre de B engendrée par les éléments b_{ri} et b_{ijk}. C'est un anneau noethérien, d'après le corollaire précédent.

D'autre part, en procédant par récurrence sur $|\nu|$, on déduit de (1) et (2) que tout monôme

$$x_1^{\nu_1} \cdots x_n^{\nu_n}$$

s'écrit comme combinaison linéaire $\beta_1 y_1 + \cdots + \beta_n y_n$, avec β_k dans B_0. Comme tout $c \in C$ est une combinaison A-linéaire finie de ces monômes, on en déduit que C est engendré comme B_0-module par $y_1, \ldots, y_n$.

Donc, C est un B_0-module de type fini. Puisque B_0 est noethérien et que B est un sous-module de C, alors B est engendré comme B_0-module par un

nombre fini d'éléments $z_1, \ldots, z_p$. Donc, tout élément de B s'écrit comme une combinaison A-linéaire finie de termes

$$\beta_t z_t,$$

pour $t = 1, \ldots, p$, où chaque β_t est un monôme en les b_{ri} et les b_{ijk}. Ceci montre, en particulier, que B est engendrée comme A-algèbre par les b_{ri}, les b_{ijk}, et les z_t. La proposition en découle. □

4.5 Divisibilité, éléments irréductibles

Soit A un anneau commutatif intègre.

Définition 4.5.1 *1) Un élément $p \in A$ est dit irréductible s'il est non nul, non inversible, et vérifie la propriété suivante : si $p = ab$, avec $a, b \in A$, alors a ou b est inversible.*

2) On dit que deux éléments non nuls $a, a' \in A$ sont associés s'il existe un élément inversible $u \in A^\times$ tel que $a' = ua$.

3) On peut donc reformuler la définition 1) en disant que p est irréductible ssi ses seuls diviseurs sont les éléments qui lui sont associés, et les inversibles.

Définition 4.5.2 *Un idéal I de A est principal s'il est engendré par un seul élément, c.-à-d., si $I = (a)$, pour un certain $a \in A$. Un tel a n'est pas unique en général ; en effet, on a le lemme suivant.*

Lemme 4.5.1 *Soient $a, b \in A \setminus \{0\}$. Alors a et b sont associés $\Leftrightarrow$ ils engendrent le même idéal.*

Démonstration. $\Rightarrow$ est clair. Réciproquement, si $(a) = (b)$, il existe $\alpha, \beta \in A$ tels que $b = \alpha a$ et $a = \beta b$. Alors, $b = \alpha\beta a$ et comme A est intègre il vient $\alpha\beta = 1$. Donc α et β sont inversibles. Ceci prouve le lemme. □

Définition 4.5.3 *Notons $\mathcal{P}$ la famille des idéaux principaux de A distincts de (0) et A. Si A n'est pas un corps, $\mathcal{P}$ est non vide, car elle contient (a) pour tout $a \in A$ non nul et non inversible.*

Proposition 4.5.2 *Soit $I \in \mathcal{P}$. Les conditions suivantes sont équivalentes :*

1) *I est engendré par un élément irréductible p ;*

2) *I est un élément maximal de $\mathcal{P}$;*

3) *tout générateur p de I est irréductible.*

Démonstration. Supposons p irréductible et (p) contenu dans un idéal principal $(b) \neq A$. Alors b n'est pas inversible, et il existe $a \in A$ tel que $p = ab$. Comme p est irréductible, ceci entraîne que a est inversible, d'où $(b) = (p)$. Ceci prouve l'implication 1) $\Rightarrow$ 2).

Montrons que 2) $\Rightarrow$ 3). Soit (p) maximal parmi les idéaux principaux $\neq A$. Supposons $p = ab$. Alors $(p) \subseteq (a)$ et deux cas sont possibles. Si $(a) = A$, alors a est inversible et b associé à p. D'autre part, si $(a) = (p)$, alors $p = ua$, avec $u \in A^\times$ (d'après le lemme), et donc $ab = p = ua$, d'où $b = u$ puisque A est intègre. Ceci montre que p est irréductible. L'implication 2) $\Rightarrow$ 3) est démontrée.

Enfin, 3) $\Rightarrow$ 1) est clair, d'où la proposition. □

Supposons que A soit intègre et noethérien, et ne soit pas un corps. Alors, $\mathcal{P}$ est non vide, donc admet au moins un élément maximal, d'après la proposition 4.1.1. Donc, A possède au moins un élément irréductible. En fait, on a le résultat plus précis suivant.

Théorème 4.5.3 [Existence d'une décomposition en facteurs irréductibles]
Soit A un anneau intègre noethérien. Alors, tout élément de $\mathcal{P}$ est un produit d'éléments maximaux de $\mathcal{P}$. Par conséquent, tout élément non nul et non inversible de A se décompose en un produit d'éléments irréductibles.

Démonstration. Rappelons que si $I_1, \ldots, I_n$ sont des idéaux de A, leur produit $I_1 \cdots I_n$ est l'idéal engendré par les produits $x_1 \cdots x_n$, où $x_k \in I_k$ pour tout k. Plus précisément, on voit que $I_1 \cdots I_n$ est l'ensemble des sommes finies de tels produits.

Dans le cas où chaque $I_k = (a_k)$ est principal, on voit facilement que

$$(a_1) \cdots (a_n) = (a_1 \cdots a_n).$$

Supposons maintenant que la sous-famille $\mathcal{P}_0$ formée des éléments de $\mathcal{P}$ qui ne sont pas produits d'éléments maximaux soit non vide. Elle admet alors un élément maximal (a). Bien sûr, (a) n'est pas un élément maximal de $\mathcal{P}$ (sinon, il ne serait pas dans $\mathcal{P}_0$!). D'après la proposition 4.5.2, a n'est pas irréductible, donc il existe une décomposition

$$a = bc$$

où ni b ni c ne sont inversibles ou associés à a. Ceci entraîne que (a) est strictement contenu dans (b) et (c). Alors, (b) et (c) n'appartiennent pas à

$\mathcal{P}_0$, puisque (a) en était un élément maximal. Donc, il existe des éléments irréductibles $p_1, \ldots, p_m$ et $q_1, \ldots, q_n$ tels que

$$(b) = (p_1) \cdots (p_m) \quad \text{et} \quad (c) = (q_1) \cdots (q_n).$$

Alors, $(a) = (b)(c)$ est produit d'éléments maximaux de $\mathcal{P}$, contrairement à l'hypothèse $(a) \in \mathcal{P}_0$. Cette contradiction montre que $\mathcal{P}_0$ est vide. Ceci prouve la 1ère assertion du théorème.

La 2ème en découle. En effet, soit $a \in A$ non nul et non inversible. Alors (a) appartient à $\mathcal{P}$ donc est égal à un produit

$$(p_1) \cdots (p_m) = (p_1 \cdots p_m),$$

où $m \geq 1$ et les p_k sont des éléments irréductibles. Donc, il existe un inversible $u \in A^\times$ tel que

$$a = up_1 \cdots p_m = (up_1)p_2 \cdots p_m.$$

Or, up_1 est, comme p_1, irréductible. Ceci achève la preuve du théorème. □

Remarque 4.5.1 1) En général, on n'a pas unicité de la décomposition en facteurs irréductibles. Par exemple :

a) Dans $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z}[X]/(X^2+5)$, on a

$$(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9 = 3 \cdot 3,$$

et l'on peut montrer que $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ et 3 sont irréductibles mais deux à deux non associés (voir [Pe1, p.II.8]).

b) Dans $A = \mathbb{C}[X, Y]/(X^2 - Y^3)$, notons x et y les images de X et Y. On a $x^2 = y^3$, et l'on peut montrer que x et y sont irréductibles et non associés.

2) Dans les deux cas précédents, il n'est pas si facile de montrer que les éléments en question sont irréductibles et non associés. Ceci peut se faire, par exemple, en considérant la norme associée à une extension quadratique, et en étudiant les factorisations possibles de la norme $N(\alpha)$ d'un élément α. Voir par exemple [Sa], §§II.5 et IV.5.

3) Les anneaux intègres pour lesquels la décomposition en facteurs irréductibles existe et est unique (aux inversibles près), sont appelés anneaux factoriels. On les étudiera dans le prochain chapitre.

Table des matières

Bibliographie

[] Voici une bibliographie provisoire (elle aussi en évolution au fil du texte).

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[Bla] A. Blanchard, Les corps non commutatifs, P.U.F., 1972.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, tome 1/Algèbre, Cedic Fernand Nathan, 1977.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[Kri] J.-L. Krivine, Théorie des ensembles, Cassini, 1998.

[Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.

[La] S. Lang, Algebra, Addison-Wesley, 1965.

[Laf] J.-P. Lafon, Les formalismes fondamentaux de l'algèbre commutative, Hermann, 1974.

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[SD] H.P.F. Swinnerton-Dyer, A brief guide to algebraic number theory, C.U.P., 2001.