I. ANNEAUX ET MODULES, LOCALISATION (SUITE)

Séances des 2, 3 et 9 octobre

4. Idéaux premiers et localisation (suite)

Remarque 4.8. — Lorsque A n'est pas intègre, l'application $A \to S^{-1}A$ n'est pas nécessairement injective. Voici deux exemples.

1) Soit $A = \mathbb{Z}/6\mathbb{Z}$ et soit $\mathfrak{p} = (\overline{2}) = \{0, \overline{2}, \overline{4}\}$; c'est un idéal maximal de A, puisque $A/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$ est un corps. Donc $S = A \setminus \mathfrak{p} = \{1, -1, \overline{3}\}$, est une partie multiplicative, ce qu'on vérifie directement puisque

$$\overline{3} \cdot \overline{3} = \overline{9} = \overline{3}.$$

Comme $\overline{2}\,\overline{3} = 0$, alors le noyau de $\tau : A \to S^{-1}A$ contient $\overline{2}$, donc égale $\mathfrak{p}$. Donc τ se factorise en un morphisme d'anneaux injectif

$$\overline{\tau} : \mathbb{Z}/2\mathbb{Z} \hookrightarrow S^{-1}A,$$

et tout élément de $S^{-1}A$ s'écrit sous la forme $\overline{\tau}(s)^{-1}\,\overline{\tau}(a)$, avec $a \in A$, $s \in S$. Or, les trois éléments de S ont pour image 1 dans $\mathbb{Z}/2\mathbb{Z}$; il en résulte que $\overline{\tau}$ est surjectif, donc un isomorphisme.

2) Soit $A = \mathbb{C}[X, Y]/(XY)$ et soit $\mathfrak{p}$ l'idéal de A engendré par l'image de Y ; c'est un idéal premier, puisque $A/\mathfrak{p} \cong \mathbb{C}[X]$. Donc $S = A \setminus \mathfrak{p}$ est une partie multiplicative, qui contient X. Comme $XY = 0$, le noyau I de $A \to S^{-1}A$ contient Y, donc $\mathfrak{p}$. On peut montrer que $I = \mathfrak{p}$ et que l'on a un isomorphisme

$$\mathbb{C}[X, X^{-1}] \xrightarrow{\sim} S^{-1}A.$$

[(0)] Version du 11/10/06

***Théorème 4.9* (Propriété universelle des localisés)**. —
1) *Soient* M *un* A*-module,* N *un* $S^{-1}A$*-module et* $f : M \to N$ *un morphisme de* A*-modules. Alors, il existe un* **unique** *morphisme de* $S^{-1}A$*-modules* $g : S^{-1}M \to N$ *tel que* $g \circ \tau_M = f$*.*

2) *Soit* $\phi : A \to B$ *un morphisme d'anneaux, avec* B *non nécessairement commutatif. On suppose que* $\phi(s)$ *est inversible, pour tout* $s \in S$*. Alors, il existe un* **unique** *morphisme d'anneaux* $\Phi : S^{-1}A \to B$ *tel que* $\Phi \circ \tau = \phi$*.*

Démonstration. — 1) S'il existe un morphisme de $S^{-1}A$-modules $g : S^{-1}M \to N$ tel que $g \circ \tau_M = f$, alors nécessairement, pour tout $m \in M, s \in S$, on doit avoir :

$$(*) \qquad g(\frac{m}{s}) = \frac{1}{s} f(m).$$

Il faut vérifier que ceci définit g sans ambiguité. Si $m'/t = m/s$, il existe $u \in S$ tel que $umt = um's$, d'où

$$utf(m) = usf(m'),$$

et donc $(1/s)f(m) = (1/t)f(m')$. Ceci montre que g est bien définie, et alors on vérifie facilement que c'est un morphisme de $S^{-1}A$-modules. Ceci prouve le point 1).

2) Remarquons d'abord que, même si B n'est pas commutatif, $\phi(A)$ est un sous-anneau commutatif de B, puisque

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a).$$

De plus, prenant pour b un élément $s \in S$, et multipliant l'égalité ci-dessus à gauche et à droite par $\phi(s)^{-1}$, on obtient

$$\phi(s)^{-1}\phi(a) = \phi(a)\phi(s)^{-1}.$$

Donc, le sous-anneau de B engendré par $\phi(A)$ et les $\phi(s)^{-1}$ est commutatif. En d'autres termes, on peut écrire les « dénominateurs » $\phi(s)^{-1}$ à gauche ou à droite, de façon indifférente.

Ceci étant dit, si Φ existe alors on a, pour tout $a \in A$ et $s \in S$, $\Phi(a/1) = \phi(a)$ et

$$\phi(a) = \Phi(a/1) = \Phi(\frac{s}{1}\frac{a}{s}) = \phi(s)\Phi(\frac{a}{s}),$$

d'où

$$(1) \qquad \Phi(\frac{a}{s}) = \phi(a)\phi(s)^{-1}.$$

Ceci montre que Φ, s'il existe, est nécessairement unique. Réciproquement, vérifions que la formule (1) définit Φ sans ambiguités. Si $a/s = b/t$, il existe $u \in S$ tel que $(at - bs)u = 0$, d'où

$$\phi(a)\phi(t)\phi(u) = \phi(atu) = \phi(bsu) = \phi(b)\phi(s)\phi(u).$$

Comme $\phi(s), \phi(t)$ et $\phi(u)$ sont inversibles, on obtient $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$. Ceci montre que Φ est bien définie, et alors on voit facilement que c'est un morphisme d'anneaux. Le théorème est démontré. □

Un corollaire standard d'une propriété universelle comme ci-dessus est que $\mathrm{S}^{-1}\mathrm{A}$ est unique à isomorphisme unique près. C.-à-d., on a le corollaire suivant.

Corollaire 4.10. — *Soit $\tau' : \mathrm{A} \to \mathrm{A}'$ un morphisme d'anneaux tel que $\tau'(s)$ soit inversible pour tout $s \in \mathrm{S}$ et vérifiant la propriété universelle précédente. Alors il existe un* **unique** *morphisme d'anneaux*

$$\Phi : \mathrm{S}^{-1}\mathrm{A} \longrightarrow \mathrm{A}',$$

tel que $\Phi \circ \tau = \tau'$, et c'est un isomorphisme.

Démonstration. — Par la propriété universelle de $\mathrm{S}^{-1}\mathrm{A}$, il existe un unique morphisme $\Phi : \mathrm{S}^{-1}\mathrm{A} \to \mathrm{A}'$ tel que $\Phi \circ \tau = \tau'$. De même, par la propriété universelle de A', il existe un unique morphisme $\Psi : \mathrm{A}' \to \mathrm{S}^{-1}\mathrm{A}$ tel que $\Psi \circ \tau' = \tau$.

Alors, $\Psi \circ \Phi \circ \tau = \Psi \circ \tau' = \tau$, donc, par la propriété universelle de $\mathrm{S}^{-1}\mathrm{A}$, appliquée à $\mathrm{B}' = \mathrm{S}^{-1}\mathrm{A}$ et $\tau' = \tau$, on obtient que $\Psi \circ \Phi = \mathrm{id}_{\mathrm{S}^{-1}\mathrm{A}}$. On obtient de même que $\Phi \circ \Psi = \mathrm{id}_{\mathrm{A}'}$. Ceci prouve le corollaire. □

Remarque 4.11. — On prendra garde au fait que dans la propriété universelle, l'hypothèse qu'il existe un **unique** Φ joue un rôle essentiel : on l'a vu dans la démonstration du corollaire. On peut aussi remarquer que le morphisme $\mathrm{A} \to \mathrm{S}^{-1}\mathrm{A} \to \mathrm{S}^{-1}\mathrm{A}[\mathrm{X}]$, vérifie la propriété universelle sans l'unicité, c.-à-d., pour tout $\phi : \mathrm{A} \to \mathrm{B}$ comme dans le théorème, on peut de façon arbitraire étendre le morphisme $\Phi : \mathrm{S}^{-1}\mathrm{A} \to \mathrm{B}$ à $\mathrm{S}^{-1}\mathrm{A}[\mathrm{X}]$, en envoyant X sur un élément arbitraire de B.

Revenons plus longuement sur le corps des fractions d'un anneau intègre A. Dans ce cas, on peut prendre comme partie multiplicative $\mathrm{S} = \mathrm{A} \setminus \{0\}$; alors l'anneau $\mathrm{S}^{-1}\mathrm{A}$, que nous noterons K, est un corps, puisque tout élément non nul de K est de la forme as^{-1}, avec $a \neq 0$, donc admet sa^{-1} pour inverse. De plus, le morphisme $\mathrm{A} \to \mathrm{K}$, $a \mapsto a/1$ est injectif.

On appelle K **le corps des fractions de** A. D'après le corollaire 4.10, K est unique à isomorphisme unique près. De plus, on a le théorème suivant :

Théorème 4.12. — *Soient* A *un anneau intègre,* K *son corps des fractions, et $\phi : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux tel que $\phi(a)$ soit inversible pour tout $a \neq 0$. (Donc, en particulier, ϕ est injectif.) Alors ϕ se prolonge de façon* **unique** *en un morphisme injectif $\Phi : \mathrm{K} \hookrightarrow \mathrm{B}$ tel que $\Phi(as^{-1}) = \phi(a)\phi(s)^{-1}$, pour tout $a, s \in \mathrm{A}$, $s \neq 0$.*

En particulier, si L *est un corps contenant* A *alors il contient aussi* K.

Démonstration. — D'après le théorème 4.9, ϕ se prolonge de façon unique en un morphisme d'anneaux $\Phi : \mathrm{K} \hookrightarrow \mathrm{B}$ tel que $\Phi(as^{-1}) = \phi(a)\phi(s)^{-1}$, pour tout $a, s \in \mathrm{A}$, $s \neq 0$. Comme K est un corps, l'idéal $\operatorname{Ker}\Phi$ est nul, c.-à-d., Φ est injectif. Ceci prouve le théorème. □

De plus, pour toute partie multiplicative S de A, le localisé $\mathrm{S}^{-1}\mathrm{A}$ s'identifie à un sous-anneau de K contenant A, d'après la proposition suivante.

Proposition 4.13 **(Localisés d'un anneau intègre)**. — *Soit* A *un anneau intègre, soit* K *son corps des fractions, et soit* S *une partie multiplicative de* A*. Alors,* $\mathrm{S}^{-1}\mathrm{A}$ *s'identifie au sous-anneau suivant de* K *:*

$$\mathrm{S}^{-1}\mathrm{A} = \left\{ \frac{a}{s} \in \mathrm{K} \mid a \in \mathrm{A}, s \in \mathrm{S} \right\}.$$

En particulier, si T *est une partie multiplicative contenant* S*, on a*

$$\mathrm{A} \subseteq \mathrm{S}^{-1}\mathrm{A} \subseteq \mathrm{T}^{-1}\mathrm{A} \subseteq \mathrm{K}.$$

Démonstration. — D'après la propriété universelle de $\mathrm{S}^{-1}\mathrm{A}$ (4.9), l'inclusion $\mathrm{A} \subseteq \mathrm{K}$ se prolonge de façon unique en un morphisme

$$\Phi : \mathrm{S}^{-1}\mathrm{A} \longrightarrow \mathrm{K}, \quad as^{-1} \mapsto \frac{a}{s},$$

et ce morphisme est injectif car si $a/s = 0$ alors $a = 0$. Ceci prouve la première assertion, et la deuxième en découle aussitôt. □

Remarque 4.14. — Il existe en général des sous-anneaux B de K, contenant A, qui ne sont pas de la forme $\mathrm{S}^{-1}\mathrm{A}$. Voici trois exemples.

1) Soit $\mathrm{A} = \mathbb{Z}[\mathrm{X}]$, son corps des fractions est le corps des fractions rationnelles $\mathbb{Q}(\mathrm{X})$. Soit B le sous-anneau de $\mathbb{Q}[\mathrm{X}]$ engendré par les $\mathrm{X}^i/i!$, pour $i \in \mathbb{N}$.

2) $\mathrm{A} = \mathbb{Z}[\mathrm{X}]$ et B le sous-anneau de $\mathbb{Z}[\mathrm{X}, \mathrm{X}^{-1}]$ engendré par X et $2/\mathrm{X}$.

3) Soient k un corps et $\mathrm{A} = k[\mathrm{X}, \mathrm{Y}]$. Le corps des fractions de A est le corps des fractions rationnelles $k(\mathrm{X}, y)$. Soit B la sous-k-algèbre de $k(\mathrm{X}, \mathrm{Y})$ engendrée par X et Y/X.

Revenons au cas général. Soient A un anneau commutatif et S une partie multiplicative arbitraire.

Proposition 4.15. — *Un* $\mathrm{S}^{-1}\mathrm{A}$*-module est la même chose qu'un* A*-module* M *tel que, pour tout* $s \in \mathrm{S}$*, l'application*

$$\rho(s) : \mathrm{M} \longrightarrow \mathrm{M}, \qquad m \mapsto sm,$$

soit inversible. Plus précisément, si M *est un* A*-module vérifiant cette propriété, alors le morphisme*

$$\tau_{\mathrm{M}} : \mathrm{M} \longrightarrow \mathrm{S}^{-1}\mathrm{M}, \qquad m \mapsto m/1$$

est bijectif et permet d'identifier M *à* $\mathrm{S}^{-1}\mathrm{M}$.

Démonstration. — Si N est un $S^{-1}A$-module, c'est aussi, par restriction des scalaires via $A \to S^{-1}A$, un A-module, et tout $s \in S$ agit bijectivement sur N, puisque s est inversible dans $S^{-1}A$.

Réciproquement, soit M un A-module vérifiant la propriété de l'énoncé. Alors le morphisme

$$\tau_M : M \longrightarrow S^{-1}M, \qquad m \mapsto m/1$$

est injectif, car si $m/1 = 0$, il existe $s \in S$ tel que $sm = 0$, et comme s agit bijectivement, $m = 0$. De plus, τ_M est surjectif. En effet, pour tout $m \in M$ et $s \in S$, on a

$$\frac{m}{1} = \tau_M(\rho(s)\rho(s)^{-1}m) = s\tau_M(\rho(s)^{-1}m),$$

d'où $m/s = \tau_M(\rho(s)^{-1}m)$. Ceci montre que τ_M est surjectif ; c'est donc un isomorphisme. □

4.3. Anneaux d'endomorphismes. —

Définition 4.16. — Soit M un groupe abélien, c.-à-d., un $\mathbb{Z}$-module. L'ensemble des **$\mathbb{Z}$-endomorphismes** de M, c.-à-d., des morphismes de groupe abélien $f : M \to M$, est noté $\mathrm{End}_{\mathbb{Z}}(M)$, ou simplement End(M).

Proposition 4.17. — *Pour $f, g \in \mathrm{End}(M)$, on définit $f + g$ par*

$$(f + g)(m) = f(m) + g(m).$$

Ceci munit End(M) *d'une structure de groupe abélien. De plus,* End(M) *est un anneau non commutatif, la multiplication étant la composition des endomorphismes.*

Démonstration. — Il faut d'abord vérifier que $f + g$ est bien un élément de End(M). Mais ceci est clair, car pour $m, n \in M$, on a

$$\begin{aligned}(f + g)(m + n) = f(m + n) + g(m + n) &= f(m) + f(n) + g(m) + g(n)\\ &= (f + g)(m) + (f + g)(n).\end{aligned}$$

Ensuite, on voit facilement que l'addition des endomorphismes est associative, commutative, et admet pour 0 le morphisme nul, et que tout endomorphisme f admet pour opposé le morphisme $-f : m \mapsto -f(m)$.

De plus, la composition des endomorphismes est associative, et admet pour élément neutre l'application identique $\mathrm{id}_M \in \mathrm{End}(M)$. Il reste à vérifier la distributivité. Soient $f, g, h \in \mathrm{End}(M)$. L'égalité $(g + h) \circ f = g \circ f + h \circ f$ résulte de la définition de l'addition. D'autre part, pour tout $m \in M$, on a

$$(f \circ (g + h))(m) = f(g(m) + h(m)) \overset{*}{=} f(g(m)) + f(h(m)),$$

où dans l'égalité $(*)$ on a utilisé le fait que f est un morphisme de groupes abéliens. Ceci prouve que $f \circ (g + h) = f \circ g + f \circ h$. La proposition est démontrée. □

Proposition 4.18. — *Soient* A *un anneau commutatif et* M *un groupe abélien. Se donner une structure de* A*-module*

$$\mu : \mathrm{A} \times \mathrm{M} \longrightarrow \mathrm{M}$$

équivaut à se donner un morphisme d'anneaux $\phi : \mathrm{A} \to \mathrm{End}(\mathrm{M})$.

Démonstration. — Supposons donné μ et définissons $\phi : \mathrm{A} \to \mathrm{End}(\mathrm{M})$ par

$$\phi(a)(m) = \mu(a, m), \qquad \forall\, a \in \mathrm{A},\, m \in \mathrm{M}.$$

L'axiome de bi-additivité assure que ϕ est bien à valeurs dans End(M), et est un morphisme de groupes abéliens. Les deux autres axiomes (associativité et unité) assurent que ϕ est un morphisme d'anneaux.

Réciproquement, supposé donné un morphisme d'anneaux $\phi : \mathrm{A} \to \mathrm{End}(\mathrm{M})$, et posons $\mu(a, m) = \phi(a)(m)$, pour tout $a \in \mathrm{A}$, $m \in \mathrm{M}$. On vérifie facilement que ceci fait de M un A-module. □

La proposition précédente permet « d'expliquer » le résultat obtenu dans la proposition 4.15.

Corollaire 4.19. — *Soit* M *un* A*-module* M *sur lequel l'action de tout* $s \in \mathrm{S}$ *est inversible. Alors* M *est un* $\mathrm{S}^{-1}\mathrm{A}$*-module.*

Démonstration. — Soit $\rho : \mathrm{A} \to \mathrm{End}(\mathrm{M})$ le morphisme d'anneaux donnant la structure de A-module. Par hypothèse, $\rho(s)$ est inversible, pour tout $s \in \mathrm{S}$. Donc, d'après le point 2) du théorème 4.9, ρ se factorise à travers $\mathrm{S}^{-1}\mathrm{A}$, c.-à-d., il existe un (unique) morphisme d'anneaux $\rho' : \mathrm{S}^{-1}\mathrm{A} \to \mathrm{End}(\mathrm{M})$ tel que $\rho' \circ \tau_{\mathrm{A}} = \rho$. Donc M est un $\mathrm{S}^{-1}\mathrm{A}$-module. □

Remarque 4.20. — C'est précisément en vue de l'application ci-dessus, qu'on a autorisé, dans le point 2) du théorème 4.9, l'anneau B à être éventuellement non commutatif.

Soient A un anneau commutatif et I un idéal de A. Notons π la projection $\mathrm{A} \to \mathrm{A}/\mathrm{I}$. Tout A/I-module N est, par « restriction des scalaires » via π, un A-module, c.-à-d.pour l'action

$$a \cdot n = \pi(a)n \qquad \forall\, a \in \mathrm{A},\, n \in \mathrm{N}.$$

Alors, pour tout $x \in \mathrm{I}$ on a $x\mathrm{N} = 0$ et donc, comme A-module, N est annulé par I.

Maintenant, soit M un A-module.

Définition 4.21. — On note IM le sous-module de M engendré par les éléments xm, pour $x \in \mathrm{I}$ et $m \in \mathrm{M}$. C.-à-d., IM est l'ensemble des sommes finies $x_1m_1 + \cdots + x_nm_n$, où $n \in \mathbb{N}^*$, $x_i \in \mathrm{I}$, $m_i \in \mathrm{M}$.

On peut donc former le A-module quotient M/IM. Il est annulé par I puisque I$m \subseteq$ IM pour tout $m \in$ M.

Théorème 4.22. — *L'action de* A *sur* M/IM *se factorise en une action de* A/I *sur* M*, telle que*

$$(*) \qquad (a + \mathrm{I})(m + \mathrm{IM}) = am + \mathrm{IM}, \qquad \forall\, a \in \mathrm{A}, m \in \mathrm{M}.$$

Démonstration. — D'après la proposition 4.18, la structure de A-module sur M/IM équivaut à la donnée du morphisme d'anneaux

$$\phi : \mathrm{A} \longrightarrow \mathrm{End(M)}$$

défini par $\phi(a)(m) = am$. Par hypothèse, ce morphisme est nul sur I. Donc d'après la propriété universelle de A/I, appliquée à l'anneau non-commutatif B = End(M), cf. pont 2) du théorème 2.16, ϕ se factorise en un morphisme d'anneaux

$$\overline{\phi} : \mathrm{A/I} \longrightarrow \mathrm{End(M)},$$

et l'action $\overline{\mu}$: (A/I) × (M/IM) associée vérifie $(*)$. □

Corollaire 4.23. — *Un* A*-module annulé par* I *est la même chose qu'un* A/I*-module.*

Démonstration. — On a déjà vu qu'un A/I-module peut être vu comme un A-module annulé par I. Réciproquement, si M est un A-module annulé par I, alors IM = (0) et donc M = M/IM est un A/I-module. □

4.4. La localisation est un foncteur additif exact. — Soient A un anneau commutatif et S une partie multiplicative de de A.

***Théorème 4.24* (Fonctorialité de la localisation)**. — 1) *Pour tout morphisme de* A*-modules* f : M → N*, il existe un* **unique** *morphisme de* S^{-1}A*-modules* $\mathrm{S}^{-1}f : \mathrm{S}^{-1}\mathrm{M} \to \mathrm{S}^{-1}\mathrm{N}$ *rendant commutatif le diagramme suivant :*

$$\begin{array}{ccc} \mathrm{M} & \xrightarrow{f} & \mathrm{N} \\ {\scriptstyle \tau_{\mathrm{M}}}\big\downarrow & & \big\downarrow{\scriptstyle \tau_{\mathrm{N}}} \\ \mathrm{S}^{-1}\mathrm{M} & \xrightarrow{\mathrm{S}^{-1}f} & \mathrm{S}^{-1}\mathrm{N}, \end{array}$$

c.-à-d., tel que

$$(*) \qquad (\mathrm{S}^{-1}f)(m/s) = f(m)/s, \qquad \forall\, m \in \mathrm{M},\ s \in \mathrm{S}.$$

Si g : N → P *est un morphisme de* A*-modules, on a*

$$(1) \qquad \mathrm{S}^{-1}(g \circ f) = (\mathrm{S}^{-1}g) \circ (\mathrm{S}^{-1}f), \quad \text{et} \quad \mathrm{S}^{-1}\,\mathrm{id}_{\mathrm{M}} = \mathrm{id}_{\mathrm{S}^{-1}\mathrm{M}}\,.$$

Par conséquent, la localisation en S *est* **fonctorielle***, c.-à-d., respecte les morphismes. En particulier, si* f *est un isomorphisme, alors* $\mathrm{S}^{-1}f$ *aussi.*

2) *De plus, si* f' *est un second* A-*morphisme de* M *vers* N, *alors*

$$\mathrm{S}^{-1}(f+f') = (\mathrm{S}^{-1}f) + (\mathrm{S}^{-1}f');$$

par conséquent, la localisation en S *est un foncteur* **additif**.

Démonstration. — $\tau_{\mathrm{N}} \circ f$ est un A-morphisme de M vers le S^{-1}A-module S^{-1}N. Donc, d'après la propriété universelle de S^{-1}M (cf. théorème 4.9), il existe un unique morphisme de S^{-1}A-modules $\mathrm{S}^{-1}f : \mathrm{S}^{-1}\mathrm{M} \to \mathrm{S}^{-1}\mathrm{N}$ tel que $(\mathrm{S}^{-1}f) \circ \tau_{\mathrm{M}} = \tau_{\mathrm{N}} \circ f$, c.-à-d.,

$$(*) \qquad (\mathrm{S}^{-1}f)(m/s) = f(m)/s, \qquad \forall\, m \in \mathrm{M},\ s \in \mathrm{S}.$$

On déduit de cette formule que $\mathrm{S}^{-1}(g \circ f) = (\mathrm{S}^{-1}g) \circ (\mathrm{S}^{-1}f)$ et $\mathrm{S}^{-1}\,\mathrm{id}_{\mathrm{M}} = \mathrm{id}_{\mathrm{S}^{-1}\mathrm{M}}$. Ceci signifie que la transformation $\mathrm{M} \mapsto \mathrm{S}^{-1}\mathrm{M}$ est un **foncteur** (de la catégorie des A-modules vers celle des S^{-1}A-modules). Le point 1) en démontré.

D'autre part, si f' est un second A-morphisme de M vers N, alors l'application $f + f' : \mathrm{M} \to \mathrm{N}$, définie par $(f+f')(m) = f(m) + f'(m)$, est encore un morphisme de A-modules, et il résulte de la formule $(*)$ que l'on a

$$\mathrm{S}^{-1}(f+f') = (\mathrm{S}^{-1}f) + (\mathrm{S}^{-1}f').$$

Ceci signifie que le foncteur $\mathrm{M} \mapsto \mathrm{S}^{-1}\mathrm{M}$ est un foncteur **additif**. Le théorème est démontré. □

Définition 4.25. — 1) On dit qu'un diagramme

$$\mathrm{N} \xrightarrow{\ f\ } \mathrm{M} \xrightarrow{\ g\ } \mathrm{P}$$

de morphismes de A-modules est **exact en** M si $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

2) On dit qu'une suite de morphismes de A-modules

$$\cdots \xrightarrow{f_{n-1}} \mathrm{M}_{n-1} \xrightarrow{f_n} \mathrm{M}_n \xrightarrow{f_{n+1}} \mathrm{M}_{n+1} \xrightarrow{f_{n+2}} \cdots$$

est un **complexe** si pour tout n on a

$$f_{n+1} \circ f_n = 0, \quad \text{c.-à-d.,} \quad \mathrm{Im}(f_n) \subseteq \mathrm{Ker}(f_{n+1}).$$

On dit que ce complexe est une **suite exacte** si le diagramme ci-dessus est exact en chaque M_n, c.-à-d., si pour tout n on a $\mathrm{Im}(f_n) = \mathrm{Ker}(f_{n+1})$.

3) On appelle **suite exacte courte** une suite exacte de la forme suivante :

$$(*) \qquad 0 \longrightarrow \mathrm{N} \xrightarrow{\ f\ } \mathrm{M} \xrightarrow{\ g\ } \mathrm{P} \longrightarrow 0.$$

Donc, dire qu'un diagramme $(*)$ est une suite exacte courte équivaut à dire que : f est injectif et g induit un isomorphisme $\mathrm{M}/f(\mathrm{N}) \cong \mathrm{P}$.

Donc, se donner une suite exacte courte $(*)$ équivaut à se donner : un sous-module N' de M, et deux isomorphismes $f : N \xrightarrow{\sim} N'$ et $g : M/N' \xrightarrow{\sim} P$. Ceci est plus souple que d'exiger que N soit égal à N', comme le montrent les deux exemples suivants.

Exemple 4.26. — On a une suite exacte de $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\ 2\ } \mathbb{Z} \xrightarrow{\ \pi\ } \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

où le morphisme $\xrightarrow{2}$ est la multiplication par 2, et π est la projection canonique.

Exemple 4.27. — Soit $\lambda \in \mathbb{C}$ et soit $\phi_\lambda : \mathbb{C}[X] \to \mathbb{C}$ le morphisme de $\mathbb{C}$-algèbres défini par $\phi_\lambda(X) = \lambda$. Alors on a une suite exacte de $\mathbb{C}[X]$-modules

$$0 \longrightarrow \mathbb{C}[X] \xrightarrow{X-\lambda} \mathbb{C}[X] \xrightarrow{\phi_\lambda} \mathbb{C} \longrightarrow 0,$$

où la seconde flèche désigne la multiplication par $X - \lambda$.

Remarque 4.28. — Soit

$$\cdots \xrightarrow{f_{n-1}} M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \xrightarrow{f_{n+2}} \cdots$$

un complexe de A-modules. Pour tout n, posons $K_n = \operatorname{Ker}(f_n)$ et $I_n = \operatorname{Im}(f_n)$. Alors, on a des suites exactes

$$0 \longrightarrow K_n \longrightarrow M_n \longrightarrow I_n \longrightarrow 0$$

et des complexes

$$0 \longrightarrow I_{n-1} \longrightarrow M_n \longrightarrow I_n \longrightarrow 0, \tag{$*_n$}$$

et le complexe est exact si, et seulement si, chaque $(*_n)$ est une suite exacte courte.

Théorème 4.29. — 1) *Soient* N *un sous-module de* M*, et* $\pi : M \to M/N$*. Alors* $S^{-1}N$ *est un sous-module de* $S^{-1}M$*, et* $S^{-1}\pi$ *induit un isomorphisme*

$$S^{-1}M/S^{-1}N \xrightarrow{\sim} S^{-1}(M/N).$$

(*Slogan à retenir : « la localisation commute au quotient »*).

2) *Plus généralement, si on a une suite exacte courte* $0 \to K \xrightarrow{f} M \xrightarrow{g} Q \to 0$*, alors la suite ci-dessous est exacte :*

$$0 \longrightarrow S^{-1}K \xrightarrow{S^{-1}f} M \xrightarrow{S^{-1}g} Q \longrightarrow 0.$$

(*« la localisation préserve les suites exactes ».*)

3) *Soit* I *un idéal de* A*, et soit* $\pi : A \to A/I$*. Alors* $S^{-1}I$ *est un idéal de* $S^{-1}A$*, et* $S^{-1}\pi$ *induit un isomorphisme d'anneaux*

$$\phi : (S^{-1}A)/(S^{-1}I) \cong S^{-1}(A/I), \qquad s^{-1}a + S^{-1}I \mapsto s^{-1}(a + I). \tag{$\dagger$}$$

Posons, de plus, $\overline{\mathrm{S}} = \pi(\mathrm{S})$. *C'est une partie multiplicative de* A/I *(sauf qu'on peut avoir* $0 \in \overline{\mathrm{S}}$*), et l'on a un isomorphisme d'anneaux*

$$(\ddagger) \qquad (\mathrm{S}^{-1}\mathrm{A})/(\mathrm{S}^{-1}\mathrm{I}) \cong \overline{\mathrm{S}}^{-1}(\mathrm{A}/\mathrm{I}).$$

(*à nouveau, le slogan est : « la localisation commute au quotient »*).

4) *Soient* $\mathrm{M}_1, \mathrm{M}_2$ *des* A*-modules. Alors*

$$\mathrm{S}^{-1}(\mathrm{M}_1 \bigoplus \mathrm{M}_2) \cong \mathrm{S}^{-1}\mathrm{M}_1 \bigoplus \mathrm{S}^{-1}\mathrm{M}_2$$

(*« la localisation commute à la somme directe »*).

Démonstration. — 1) et 2). On va montrer le point 2), le point 1) en étant un cas particulier.

D'abord, $\mathrm{S}^{-1}f$ est injectif, car si $0 = (\mathrm{S}^{-1}f)(x/s) = f(x)/s$, il existe $u \in \mathrm{S}$ tel que $0 = uf(x) = f(ux)$. Comme f est injectif, il vient $ux = 0$, et donc $x/s = 0$ dans $\mathrm{S}^{-1}\mathrm{K}$.

Soit $y = q/s$ un élément arbitraire de $\mathrm{S}^{-1}\mathrm{Q}$. Comme g est surjectif, il existe $m \in \mathrm{M}$ tel que $g(m) = q$, et donc $(\mathrm{S}^{-1}g)(m/s) = y$. Ceci montre que $\mathrm{S}^{-1}g$ est surjectif.

De plus, $(\mathrm{S}^{-1}g) \circ (\mathrm{S}^{-1}f) = \mathrm{S}^{-1}(g \circ f) = 0$, donc $\mathrm{Im}(\mathrm{S}^{-1}f) \subseteq \mathrm{Ker}(\mathrm{S}^{-1}g)$. Enfin, soit m/s un élément arbitraire de $\mathrm{Ker}(\mathrm{S}^{-1}g)$. Alors $g(m)/s = 0$, donc il existe $u \in \mathrm{S}$ tel que $0 = ug(m) = g(um)$, c.-à-d., $um \in \mathrm{Ker}(g)$. Par hypothèse, il existe $x \in \mathrm{K}$ tel que $f(x) = um$. Alors $(\mathrm{S}^{-1}f)(x/us) = m/s$. Ceci prouve l'exactitude en $\mathrm{S}^{-1}\mathrm{M}$. Le point 2) est démontré, et avec lui, le point 1).

3) D'après ce qui précède, $\mathrm{S}^{-1}\mathrm{I}$ est un idéal de $\mathrm{S}^{-1}\mathrm{A}$ et ϕ est un isomorphisme de A-modules. Et, d'après la formule (†), on voit facilement que c'est un morphisme d'anneaux. Ceci prouve la première assertion.

Il est clair que $\overline{\mathrm{S}}$ contient 1 et est stable par multiplication. Il peut arriver que $0 \in \overline{\mathrm{S}}$; c'est le cas si et seulement si $\mathrm{S} \cap \mathrm{I} \neq \varnothing$, dans ce cas $\mathrm{S}^{-1}\mathrm{I} = \mathrm{S}^{-1}\mathrm{A}$ et les deux anneaux de (‡) sont l'anneau nul $\{0\}$. On peut donc supposer que $0 \notin \overline{\mathrm{S}}$, donc que $\overline{\mathrm{S}}$ est une partie multiplicative.

L'image de tout $s \in \mathrm{S}$ par le morphisme d'anneaux

$$\mathrm{A} \longrightarrow \mathrm{A}/\mathrm{I} \longrightarrow \overline{\mathrm{S}}^{-1}(\mathrm{A}/\mathrm{I})$$

est inversible, donc ce morphisme induit un morphisme d'anneaux

$$\phi : \mathrm{S}^{-1}\mathrm{A} \longrightarrow \overline{\mathrm{S}}^{-1}(\mathrm{A}/\mathrm{I}) \quad \text{tel que} \quad \phi(a/s) = \pi(s)^{-1}\pi(a), \quad \forall\, a \in \mathrm{A},\ s \in \mathrm{S}.$$

Ce morphisme est surjectif, puisque tout élément de $\overline{\mathrm{S}}^{-1}(\mathrm{A}/\mathrm{I})$ est de la forme $\pi(s)^{-1}\pi(a)$ donc égal à $\phi(a/s)$. D'autre part, il est clair que $\mathrm{S}^{-1}\mathrm{I} \subseteq \mathrm{Ker}\,\phi$. Réciproquement, si $a/s \in \mathrm{Ker}\,\phi$, il existe $u \in \mathrm{S}$ tel que

$$0 = \pi(u)\pi(a) = \pi(ua), \quad \text{d'où} \quad ua \in \mathrm{I}$$

et donc $a/1 \in \mathrm{S}^{-1}\mathrm{I}$ et $a/s \in \mathrm{S}^{-1}\mathrm{I}$. Ceci montre que $\operatorname{Ker}\phi = \mathrm{S}^{-1}\mathrm{I}$, et donc ϕ induit un isomorphisme d'anneaux

$$\overline{\phi} : \frac{\mathrm{S}^{-1}\mathrm{A}}{\mathrm{S}^{-1}\mathrm{I}} \xrightarrow{\sim} \overline{\mathrm{S}}^{-1}(\mathrm{A}/\mathrm{I}), \qquad s^{-1}a + \mathrm{S}^{-1}\mathrm{I} \mapsto \pi(s)^{-1}\pi(a).$$

Ceci achève la preuve du point 3).

Pour démontrer le point 4), posons $\mathrm{M} = \mathrm{M}_1 \oplus \mathrm{M}_2$ et introduisons l'inclusion $\tau_1 : \mathrm{M}_1 \hookrightarrow \mathrm{M}$, $x \mapsto (x, 0)$, et la projection $\pi_1 : \mathrm{M} \to \mathrm{M}_1$, $(x, y) \mapsto x$, et définissons de même τ_2 et π_2. Alors on a

$$\pi_1 \circ \tau_1 = \mathrm{id}_{\mathrm{M}_1}, \qquad \pi_2 \circ \tau_2 = \mathrm{id}_{\mathrm{M}_2}\,; \tag{1}$$

$$\pi_2 \circ \tau_1 = 0 = \pi_1 \circ \tau_2\,; \tag{2}$$

$$\mathrm{id}_{\mathrm{M}} = \tau_1 \circ \pi_1 + \tau_2 \circ \pi_2\,. \tag{3}$$

Lemme 4.30. — *Ces égalités caractérisent la somme directe, c.-à-d., si* $\mathrm{M}_1, \mathrm{M}_2$, *et* M *sont des* A-*modules arbitraires et si l'on a des* A-*morphismes*

$$\mathrm{M}_1 \underset{\pi_1}{\overset{\tau_1}{\rightleftarrows}} \mathrm{M} \underset{\pi_2}{\overset{\tau_2}{\leftrightarrows}} \mathrm{M}_2$$

vérifiant ces égalités, alors $\mathrm{M}_i \cong \tau_i(\mathrm{M}_i)$ *pour* $i = 1, 2$ *et l'on a*

$$\mathrm{M} = \tau_1(\mathrm{M}_1) \bigoplus \tau_2(\mathrm{M}_2).$$

Démonstration. — Comme $\pi_i \circ \tau_i = \mathrm{id}_{\mathrm{M}_i}$ alors chaque τ_i est injective, donc un isomorphisme de M_i sur $\tau_i(\mathrm{M}_i)$. De plus, (3) entraîne que

$$\mathrm{M} = \tau_1(\mathrm{M}_1) + \tau_2(\mathrm{M}_2).$$

Enfin, d'après (2), la somme est directe car si $m \in \tau_1(\mathrm{M}_1) \cap \tau_2(\mathrm{M}_2)$, alors

$$m = \tau_1(x_1) = \tau_2(x_2), \quad \text{avec} \quad x_i \in \mathrm{M}_i,$$

et d'après (2) l'on a $x_1 = \pi_1(m) = \pi_1(\tau_2(x_2)) = 0$, d'où $m = 0$. Ceci prouve le lemme. □

On peut maintenant achever la preuve du point 4). Comme la localisation est un foncteur additif (cf. théorème 4.24), les morphismes $\mathrm{S}^{-1}\tau_i$ et $\mathrm{S}^{-1}\pi_i$, pour $i = 1, 2$, vérifient les égalités (1)–(3), avec M_i et M remplacés par $\mathrm{S}^{-1}\mathrm{M}_i$ et $\mathrm{S}^{-1}\mathrm{M}$. Par conséquent, il résulte du lemme que

$$\mathrm{S}^{-1}\mathrm{M} \cong \mathrm{S}^{-1}\mathrm{M}_1 \bigoplus \mathrm{S}^{-1}\mathrm{M}_2.$$

Le théorème est démontré. □

4.5. Idéaux premiers de $S^{-1}A$, anneaux locaux. — Réparons d'abord un oubli. La proposition suivante est extrêmement importante, et aurait dû être signalée juste après la définition des idéaux premiers, au début de la section 4. On rappelle qu'on désigne par Spec(B) l'ensemble des idéaux premiers d'un anneau B.

Proposition 4.31. — *Soit $\phi : A \to B$ un morphisme d'anneaux commutatifs, et soit $\mathfrak{p} \in \mathrm{Spec}(B)$. Alors $\phi^{-1}(\mathfrak{p})$ est un idéal premier de A.*

Démonstration. — Le noyau du morphisme $A \xrightarrow{\phi} B \to B/\mathfrak{p}$ est l'idéal

$$\phi^{-1}(\mathfrak{p}) = \{a \in A \mid \phi(a) \in \mathfrak{p}\}.$$

Donc ϕ induit un morphisme d'anneaux injectif

$$A/\phi^{-1}(\mathfrak{p}) \hookrightarrow B/\mathfrak{p},$$

et comme $B/\mathfrak{p}$ est intègre, $A/\phi^{-1}(\mathfrak{p})$ l'est aussi. Ceci montre que l'idéal $\phi^{-1}(\mathfrak{p})$ est premier. □

Remarque 4.32. — **Attention !** Si $\mathfrak{m}$ est un idéal maximal de B, alors $\phi^{-1}(\mathfrak{m})$ est premier mais pas nécessairement maximal ! Par exemple, soit ϕ l'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$; alors (0) est un (le seul) idéal maximal de $\mathbb{Q}$, et son image inverse est l'idéal (0) de $\mathbb{Z}$ qui est premier mais pas maximal.

Soient A un anneau commutatif, S une partie multiplicative de A, et M un A-module. Soit τ_M le morphisme de A-modules $M \to S^{-1}M$, $m \mapsto m/1$.

Pour tout sous-$S^{-1}A$-module $\mathscr{N}$ de $S^{-1}M$, son image inverse

$$\tau_M^{-1}(\mathscr{N}) = \{m \in M \mid m/1 \in \mathscr{N}\}$$

est un sous-A-module de M ; par abus de notation, on le note $\mathscr{N} \cap M$ et on l'appelle « l'intersection » de $\mathscr{N}$ avec M.

Proposition 4.33. — 1) *Pour tout sous-$S^{-1}A$-module $\mathscr{N}$ de $S^{-1}M$, on a*

$$\mathscr{N} = S^{-1}(\mathscr{N} \cap A).$$

(*on dit que « tout sous-module de $S^{-1}M$ est étendu »*).

2) *Si N est un sous-module de M, on a*

$$M \cap S^{-1}N = \{m \in M \mid \text{ il existe } s \in S \text{ tel que } sm \in N\}.$$

En particulier, si I est un idéal de A, on a $S^{-1}I = S^{-1}A \Leftrightarrow I \cap S \neq \varnothing$.

Démonstration. — 1) L'inclusion $\supseteq$ est claire. Réciproquement, soit $x \in \mathscr{N}$. Alors $x = m/s$, avec $m \in M$ et $s \in S$, et $\mathscr{N}$ contient $sx = m/1$. Donc $m \in \mathscr{N} \cap M$ et $x = m/s$ appartient à $S^{-1}(\mathscr{N} \cap M)$.

2) Soit $m \in M$. S'il existe $s \in S$ tel que $sm \in N$, alors $m/1 = sm/s \in S^{-1}N$ et donc $m \in M \cap S^{-1}N$.

Réciproquement, supposons que $m/1 \in \mathrm{S}^{-1}\mathrm{N}$. Alors il existe $y \in \mathrm{N}$ et $s \in \mathrm{S}$ tels que $m/1 = y/s$, donc il existe $u \in \mathrm{S}$ tel que $u(sm-y) = 0$. Par conséquent, $usm = uy$ appartient à N. Ceci prouve l'égalité voulue.

En particulier, si I est un idéal de A, on a

$$\mathrm{S}^{-1}\mathrm{I} = \mathrm{S}^{-1}\mathrm{A} \Leftrightarrow 1 \in \mathrm{S}^{-1}\mathrm{I} \Leftrightarrow \mathrm{I} \cap \mathrm{S} \neq \varnothing.$$

La proposition est démontrée. □

Remarque 4.34. — Soit I un idéal de A ne rencontrant pas S. On n'a pas nécessairement l'égalité $\mathrm{I} = \mathrm{A} \cap \mathrm{S}^{-1}\mathrm{I}$; mais on va voir ci-dessous que c'est le cas si I est premier.

***Théorème 4.35* (Idéaux premiers de $\mathrm{S}^{-1}\mathrm{A}$)**. — *Les idéaux premiers de $\mathrm{S}^{-1}\mathrm{A}$ sont exactement les $\mathrm{S}^{-1}\mathfrak{p}$, pour $\mathfrak{p}$ idéal premier de A ne rencontrant pas S.*

De façon plus précise, l'application $\mathfrak{p} \mapsto \mathrm{S}^{-1}\mathfrak{p}$ est une bijection de $\{\mathfrak{p} \in \mathrm{Spec}(\mathrm{A}) \mid \mathfrak{p} \cap \mathrm{S} = \varnothing\}$ sur $\mathrm{Spec}(\mathrm{S}^{-1}\mathrm{A})$, dont la bijection réciproque est $\mathrm{P} \mapsto \mathrm{P} \cap \mathrm{A}$.

Démonstration. — Posons $\mathrm{X} = \{\mathfrak{p} \in \mathrm{Spec}(\mathrm{A}) \mid \mathfrak{p} \cap \mathrm{S} = \varnothing\}$, et soit $\mathfrak{p} \in \mathrm{X}$. Il résulte du point 2) de la proposition précédente que

$$\mathrm{A} \cap \mathrm{S}^{-1}\mathfrak{p} = \mathfrak{p}. \tag{1}$$

En effet, si $x \in \mathrm{A} \cap \mathrm{S}^{-1}\mathfrak{p}$, il existe $s \in \mathrm{S}$ tel que $sx \in \mathfrak{p}$. Comme $\mathfrak{p}$ est premier et $s \notin \mathfrak{p}$ (puisque $\mathrm{S} \cap \mathfrak{p} = \varnothing$), ceci entraîne $x \in \mathfrak{p}$.

En particulier, (1) montre que $\mathrm{S}^{-1}\mathfrak{p}$ est un idéal propre de $\mathrm{S}^{-1}\mathrm{A}$. De plus, d'après le point 3) du théorème 4.29, on a

$$\mathrm{S}^{-1}\mathrm{A}/\mathrm{S}^{-1}\mathfrak{p} \cong \overline{\mathrm{S}}^{-1}(\mathrm{A}/\mathfrak{p}),$$

et ceci est un anneau intègre puisque c'est un sous-anneau du corps des fractions de $\mathrm{A}/\mathfrak{p}$ (cf. 4.13). Ceci montre que $\mathrm{S}^{-1}\mathfrak{p}$ est un idéal premier de $\mathrm{S}^{-1}\mathrm{A}$. De plus, (1) montre que l'application

$$\theta : \mathrm{X} \longrightarrow \mathrm{Spec}(\mathrm{S}^{-1}\mathrm{A}), \qquad \mathfrak{p} \mapsto \mathrm{S}^{-1}\mathfrak{p}$$

est injective.

Elle est aussi surjective. En effet, soit $\mathrm{P} \in \mathrm{Spec}(\mathrm{S}^{-1}\mathrm{A})$. D'après la proposition 4.31, $\mathfrak{p} := \mathrm{P} \cap \mathrm{A}$ est un idéal premier et, d'après le point 1) de la proposition 4.33, l'on a $\mathrm{P} = \mathrm{S}^{-1}\mathfrak{p}$. Il en résulte que $\mathfrak{p} \cap \mathrm{S} = \varnothing$, et que θ est surjective. C'est donc une bijection, dont la réciproque est l'application $\mathrm{P} \mapsto \mathrm{P} \cap \mathrm{A}$. Le théorème est démontré. □

***Définition 4.36* (Anneaux locaux)**. — Un anneau A est dit **local** s'il ne possède qu'un seul idéal maximal $\mathfrak{m}$. Dans ce cas, on écrit parfois que $(\mathrm{A}, \mathfrak{m})$ est un anneau local, et l'on dit que le corps $k = \mathrm{A}/\mathfrak{m}$ est le **corps résiduel** de A.

Définition 4.37. — Soit $\mathfrak{p} \in \operatorname{Spec}(A)$ et soit M un A-module. On note $A_\mathfrak{p}$ et $M_\mathfrak{p}$ les localisés $S^{-1}A$ et $S^{-1}M$, où S est la partie multiplicative

$$A \setminus \mathfrak{p} = \{a \in A \mid a \notin \mathfrak{p}\}.$$

***Proposition 4.38* ($A_\mathfrak{p}$ est local)**. — *Soit* $\mathfrak{p} \in \operatorname{Spec}(A)$*. Alors* $A_\mathfrak{p}$ *est un anneau local : son unique idéal maximal est l'idéal* $\mathfrak{p}A_\mathfrak{p}$*.*

Le corps résiduel $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ *est noté* $\kappa(\mathfrak{p})$ *et est souvent appelé « corps résiduel de* $\mathfrak{p}$ *».*

Démonstration. — D'après le théorème 4.35, les idéaux premiers de $A_\mathfrak{p}$ sont les idéaux $\mathfrak{q}A_\mathfrak{p}$, pour $\mathfrak{q}$ idéal premier de A ne rencontrant pas $S = A \setminus \mathfrak{p}$, c.-à-d., contenu dans $\mathfrak{p}$. Donc, tout idéal premier de $A_\mathfrak{p}$ est contenu dans $\mathfrak{p}A_\mathfrak{p}$; celui-ci est donc l'unique idéal maximal de $A_\mathfrak{p}$ (car un idéal maximal est nécessairement premier). Ceci prouve la proposition. □

5. Modules de type fini, lemme de Zorn, existence d'idéaux maximaux

5.1. Modules de type fini. — Soient A un anneau, M un A-module.

Définition 5.1. — Soit $(x_i)_{i\in I}$ (où I est un ensemble fini ou infini) une famille d'éléments de M. On rappelle (cf. proposition 3.0) que le sous-module engendré par les x_i est l'ensemble des sommes **finies**

$$\sum_{\substack{J\subseteq I \\ J \text{ fini}}} a_j x_j, \qquad a_j \in A.$$

On le note $\sum_{i\in I} Ax_i$, étant entendu que ceci désigne l'ensemble des sommes finies de termes $a_i x_i$.

En particulier, lorsque I est un ensemble fini, $I = \{1, \dots, n\}$, le sous-module engendré par $x_1, \dots, x_n \in M$ est

$$Ax_1 + \cdots + Ax_n = \{a_1x_1 + \cdots + a_nx_n \mid a_i \in A\};$$

on le note aussi $(x_1, \dots, x_n)$.

Exemple 5.2. — Soient $A = \mathbb{C}[X, Y]$ et $M = A$. Alors l'idéal engendré par X et Y est

$$(X, Y) = \{PX + QY \mid P, Q \in A\} = AX + AY.$$

Définition 5.3. — On dit qu'un A-module M est **de type fini** s'il peut être engendré par un nombre fini d'éléments, c.-à-d., s'il existe $x_1, \dots, x_n \in M$ tels que

$$M = Ax_1 + \cdots + Ax_n,$$

c.-à-d., si tout $m \in M$ s'écrit $m = a_1x_1 + \cdots + a_nx_n$, avec $a_i \in A$.

Exemples 5.4. — 1) Le A-module A est de type fini : il est engendré par l'élément 1 puisque $a = a1$ pour tout $a \in \mathrm{A}$.

2) Plus généralement, pour tout $n \geqslant 1$, la somme directe

$$\mathrm{A}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathrm{A}\}$$

est un A-module de type fini. En effet, introduisons les éléments

$$e_1 = (1, 0, \dots, 0), \quad \cdots \quad , e_n = (0, \dots, 0, 1).$$

(Si $\mathrm{A} = k$ est un corps, alors les e_i sont simplement les vecteurs de la base canonique de k^n.) Alors, tout élément $\underline{a} = (a_1, \dots, a_n)$ de A^n s'écrit (de façon unique)

$$\underline{a} = a_1 e_1 + \cdots + a_n e_n.$$

3) Le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ est de type fini, puisqu'il est engendré par l'élément $\overline{1}$. Par contre, ici, l'écriture n'est pas unique puisque $a\overline{1} = b\overline{1}$ si $a - b \in n\mathbb{Z}$.

Exercice 5.5. — Soit V un $\mathbb{R}$-espace vectoriel. Montrer que V est de type fini comme $\mathbb{R}$-module si et seulement si $\dim_{\mathbb{R}} \mathrm{V} < \infty$. Donc, pour un espace vectoriel, type fini = dimension finie.

Proposition 5.6. — *Soient* M *un* A*-module et* N *un sous-module.*

1) *Si* M *est de type fini,* M/N *l'est aussi.*

2) *Si* N *et* M/N *sont de type fini, alors* M *l'est aussi.*

Démonstration. — 1) Soit $\pi : \mathrm{M} \to \mathrm{M/N}$. Supposons M engendré par des éléments $x_1, \dots, x_n$. Alors tout $m \in \mathrm{M}$ s'écrit

$$m = a_1 x_1 + \cdots + a_n x_n,$$

et donc $\pi(m) = a_1\pi(x_1) + \cdots + a_n\pi(x_n)$. Ceci montre que M/N est engendré par $\pi(x_1), \dots, \pi(x_n)$, donc de type fini.

2) On suppose N et M/N de type fini. Soient $y_1, \dots, y_s \in \mathrm{N}$ des générateurs de N et soient $x_1, \dots, x_r \in \mathrm{M}$ dont les images engendrent M/N. Soit $m \in \mathrm{M}$ arbitraire. Alors, il existe $a_1, \dots, a_r \in \mathrm{A}$ tels que

$$\pi(m) = a_1\pi(x_1) + \cdots + a_r\pi(x_r),$$

d'où $m - \sum_{i=1}^r a_i x_i \in \mathrm{N}$.

Donc, il existe $b_1, \dots, b_s \in \mathrm{A}$ tels que

$$m - \sum_{i=1}^r a_i x_i = b_1 y_1 + \cdots + b_s y_s.$$

Par conséquent, $m = \sum_{i=1}^r a_i x_i + \sum_{j=1}^s b_j y_j$. Comme m était arbitrairement choisi dans M, ceci montre que M est engendré par $x_1, \dots, x_r, y_1, \dots, y_s$. La proposition est démontrée. $\square$

Remarque 5.7. — **Attention**, un sous-module d'un module de type fini n'est pas nécessairement de type fini. Voici un exemple. Soit A l'anneau des polynômes sur $\mathbb{C}$ en une infinité de variables :

$$\mathbb{C}[X_1, X_2, \dots] = \bigcup_{n \geqslant 1} \mathbb{C}[X_1, \dots, X_n],$$

et soit $\mathfrak{m}$ l'idéal de A engendré par les X_i. Bien sûr, A est un A-module de type fini, engendré par 1, mais on va montrer que le sous-module (l'idéal) $\mathfrak{m}$ n'est pas de type fini. On a la suite croissante d'idéaux

$$(X_1) \subseteq (X_1, X_2) \subseteq (X_1, X_2, X_3) \subseteq \cdots$$

et $\mathfrak{m}$ en est la réunion. Supposons que $\mathfrak{m}$ soit engendré par un nombre fini d'éléments $Q_1, \dots, Q_r$; alors, ils sont tous dans un certain $(X_1, \dots, X_n)$ et donc

$$\mathfrak{m} = (X_1, \dots, X_n).$$

Par conséquent, il existe $P_1, \dots, P_n \in A$ tels que

$$(*) \qquad X_{n+1} = \sum_{i=1}^{n} P_i X_i.$$

Tous les P_i appartiennent à $\mathbb{C}[X_1, \dots, X_N]$, pour un certain $N \geqslant n+1$, et donc l'égalité $(*)$ ci-dessus a lieu dans l'anneau $\mathbb{C}[X_1, \dots, X_N]$. Alors, on peut évaluer X_{n+1} en 1, et les autres X_i, pour $i \leqslant N$, $i \neq n+1$, en 0, et $(*)$ donne $1 = 0$, une contradiction ! Ceci montre que l'idéal $\mathfrak{m}$ n'est pas de type fini.

Toutefois, cette « pathologie » ne se produit pas pour les anneaux et modules noethériens, qu'on va étudier plus tard.

5.2. Union filtrante de sous-modules. — Soit M un A-module.

Définition 5.8. — Une famille de sous-modules $(M_i)_{i \in I}$ de M est dite **filtrante** si elle vérifie la propriété suivante :

$$\text{(filt)} \qquad \forall\, i, j, \quad \exists\, \ell \ \text{ tel que } \ M_i + M_j \subseteq M_\ell.$$

Remarque 5.9. — En particulier, toute suite croissante de sous-modules $M_0 \subseteq M_1 \subseteq \cdots$ est une famille filtrante : il suffit de prendre $\ell = \max\{i, j\}$. Mais on peut rencontrer des familles filtrantes de sous-modules plus générales.

Le lemme suivant est important et sera utilisé de façon répétée.

Lemme 5.10. — *Soit* $(M_i)_{i \in I}$ *une famille filtrante de sous-*A*-modules de* M. *Alors, la réunion*

$$U := \bigcup_{i \in I} M_i$$

*est un sous-*A*-module de* M.

Démonstration. — Soient $a \in \mathrm{A}$ et $x, y \in \mathrm{U}$. Alors, il existe $i, j \in \mathrm{I}$ tels que $x \in \mathrm{M}_i$ et $y \in \mathrm{M}_j$ et donc, comme la famille est filtrante, il existe $\ell \in \mathrm{I}$ tel que $x, y \in \mathrm{M}_\ell$. Comme M_ℓ est un sous-module, on a $x + ay \in \mathrm{M}_\ell$, et donc $x + ay \in \mathrm{U}$. Ceci prouve le lemme. □

Définition 5.11. — Un sous-module **propre** de M est un sous-module $\mathrm{N} \neq \mathrm{M}$. De même, un **idéal propre** de A est un idéal $\neq \mathrm{A}$.

Définition 5.12. — Soit N un sous-module de M. On dit que N est un sous-module **maximal** s'il n'existe pas de sous-module propre N' contenant N strictement, c.-à-d., si N est un élément maximal (pour la relation d'inclusion) de l'ensemble des sous-modules propres.

Lemme 5.13. — *Soit* M *un* A-*module* **de type fini** *et soit* $(\mathrm{M}_i)_{i\in\mathrm{I}}$ *une famille filtrante de sous-modules* **propres** *de* M. *Alors* $\bigcup_{i\in\mathrm{I}} \mathrm{M}_i$ *est un sous-module* **propre** *de* M.

Démonstration. — Posons $\mathrm{U} := \bigcup_{i\in\mathrm{I}} \mathrm{M}_i$; on a déjà vu que c'est un sous-module de M (lemme 5.10). Montrons que c'est un sous-module propre. Soient $x_1, \dots, x_r$ un système fini de générateurs de M.

Alors, il existe des indices $i_1, \dots, i_r \in \mathrm{I}$ tels que $x_1 \in \mathrm{M}_{i_1}$, …, $x_r \in \mathrm{M}_{i_r}$. Comme la famille $(\mathrm{M}_i)_{i\in\mathrm{I}}$ est filtante, il existe ℓ tel que M_ℓ contienne $x_1, \dots, x_r$, et comme ces derniers sont des générateurs de M, ceci entraîne $\mathrm{M}_\ell = \mathrm{M}$, en contradiction avec l'hypothèse que chaque M_i, $i \in \mathrm{I}$, est un sous-module propre. Cette contradiction montre que $\mathrm{U} \neq \mathrm{M}$. Le lemme est démontré. □

On veut montrer que tout anneau commutatif non nul A possède au moins un idéal maximal. Plus généralement, on va montrer, dans le paragraphe suivant, que tout A-module non nul M **de type fini** possède au moins un sous-module maximal. L'hypothèse que M soit de type fini est nécessaire, comme le montre l'exercice suivant.

Exercice 5.14. — Soit A le sous-anneau du corps $\mathbf{C}(\mathrm{X})$ formé des fractions rationnelles définies en 0, c.-à-d.,

$$\mathrm{A} = \left\{ \frac{\mathrm{P}}{\mathrm{Q}} \;\middle|\; \mathrm{P}, \mathrm{Q} \in \mathbf{C}[\mathrm{X}],\ \mathrm{Q}(0) \neq 0 \right\}.$$

Soit N un sous-A-module de $\mathbf{C}(\mathrm{X})$. Montrez que N est engendré par X^n, pour un certain $n \in \mathbf{Z}$. En déduire que le A-module $\mathbf{C}(\mathrm{X})$ ne possède pas de sous-module maximal.

5.3. Théorème de Zorn et conséquences. — Rappelons d'abord qu'un **ensemble ordonné** est un ensemble E muni d'une relation $x \leqslant y$ qui soit une relation *d'ordre partiel*, c.-à-d., qui est

1) réflexive : $\forall\, x \in \mathrm{E}, \quad x \leqslant x$;

2) antisymétrique : $\forall\, x, y \in \mathrm{E}, \quad x \leqslant y$ et $y \leqslant x \Rightarrow x = y$;

3) transitive : $\forall\, x, y, z \in \mathrm{E}, \quad x \leqslant y$ et $y \leqslant z \Rightarrow x = z$.

Soient A un anneau commutatif et M un A-module de type fini. L'ensemble des sous-modules propres de M est ordonné par inclusion et, si $(\mathrm{M}_i)_{i\in\mathrm{I}}$ est une famille **filtrante** de sous-modules propres, alors $\mathrm{U} = \bigcup_{i\in\mathrm{I}} \mathrm{M}_i$ est un sous-module propre (d'après le lemme 5.13), qui est un **majorant** de chacun des M_i, c.-à-d., tel que $\mathrm{M}_i \subseteq \mathrm{U}$ pour tout $i \in \mathrm{I}$.

On peut maintenant énoncer la définition et le théorème suivants.

Définition 5.15. — Soit $(\mathrm{E}, \leqslant)$ un ensemble ordonné.

1) On dit qu'un sous-ensemble F de E est **filtrant** s'il vérifie la propriété suivante : pour tout $f, f' \in \mathrm{F}$, il existe $f'' \in \mathrm{F}$ tel que $f \leqslant f''$ et $f' \leqslant f''$.

2) On dit qu'un élément $x \in \mathrm{E}$ est un élément **maximal** s'il n'existe pas d'élément $y \in \mathrm{E}$ tel que $y > x$.

3) Soit S un sous-ensemble de E et soit $x \in \mathrm{E}$. On dit que x est un **majorant** de S si l'on a $s \leqslant x$ pour tout $s \in \mathrm{S}$ (on ne demande pas que x appartienne à S).

***Théorème 5.16* (Lemme de Zorn)**. — *Soit* E *un ensemble ordonné non-vide vérifiant la propriété suivante :*

($*$) *Tout sous-ensemble filtrant de* E *admet un majorant dans* E.

Alors E *possède au moins un élément maximal.*

Nous ne démontrerons pas ce théorème, qui appartient au domaine de la théorie des ensembles, et l'on renvoie le lecteur intéressé à [**Dou**, Chap.1] ou [**La**, Appendix 2].

Dans ces références, il est montré comment le lemme de Zorn se déduit de l'axiome du choix. Il est aussi montré que le lemme de Zorn entraîne le théorème de Zermelo, qui lui-même entraîne l'axiome du choix. Donc, en fait, axiome du choix, lemme de Zorn et théorème de Zermelo sont équivalents. □

Théorème 5.17. — *Soit* M *un* A*-module non nul de type fini et soit* N *un sous-module propre. Alors* M *possède au moins un sous-module maximal contenant* N.

Démonstration. — L'ensemble E des sous-modules propres de M contenant N est non-vide (il contient N) et vérifie la propriété ($*$), d'après le lemme 5.13. Il possède donc un élément maximal M', et M' est un sous-module maximal de M contenant N. □

Corollaire 5.18. — *Soient* A *un anneau commutatif non nul et* I *un idéal propre de* A. *Alors* I *est contenu dans un idéal maximal* $\mathfrak{m}$.

Démonstration. — Ceci résulte du théorème 5.17, puisque $\mathrm{A} = \mathrm{A} \cdot 1$ est un A-module de type fini. □

5.4. Un exemple d'application. — À titre d'illustration des techniques introduites jusqu'ici, démontrons la proposition suivante (qui était une question dans l'examen de septembre 2006).

Proposition 5.19. — *Soient* A *un anneau commutatif,* $\mathfrak{m}$ *un idéal maximal de* A, *et* $\mathrm{S} = \{a \in \mathrm{A} \mid a \notin \mathfrak{m}\}$. *Alors, pour tout* $n \geqslant 1$, *on a*

$$\mathrm{A}/\mathfrak{m}^n = \mathrm{S}^{-1}(\mathrm{A}/\mathfrak{m}^n).$$

Démonstration. — Soit $s \in \mathrm{S}$. Alors l'idéal $\mathrm{J} := \mathrm{A}s + \mathfrak{m}^n$ égale A.

En effet, supposons que ce ne soit pas le cas. Alors, d'après le corollaire 5.18, il existe un idéal maximal $\mathfrak{n}$ contenant J. Alors $\mathfrak{n}$ contient $\mathfrak{m}^n$ et, comme $\mathfrak{n}$ est premier, il contient $\mathfrak{m}$. Or $\mathfrak{m}$ est maximal, donc nécessairement $\mathfrak{n} = \mathfrak{m}$. Mais alors $\mathfrak{m} = \mathfrak{n}$ contient s, une contradiction. Ceci montre que $\mathrm{A}s + \mathfrak{m}^n = \mathrm{A}$.

Donc il existe $t \in \mathrm{A}$ et $x \in \mathfrak{m}^n$ tel que $ts + x = 1$, d'où $\overline{t}\,\overline{s} = 1$ dans $\mathrm{A}/\mathfrak{m}^n$. Ceci montre que tout $s \in \mathrm{S}$ est inversible dans $\mathrm{A}/\mathfrak{m}^n$. Le résultat découle alors de la proposition 4.15. □

6. Modules libres

6.1. Définitions et exemples. —

Définition 6.1. — Soit M un A-module et soit $(x_i)_{i\in \mathrm{I}}$ une famille d'éléments de M.

1) On dit que $(x_i)_{i\in \mathrm{I}}$ est une **famille libre** si les x_i sont **linéairement indépendants** sur A, c.-à-d., si la propriété suivante est vérifiée :

Pour tout sous-ensemble fini $\mathrm{J} = \{i_1, \dots, i_n\}$ de I, si $a_1, \dots, a_n \in \mathrm{A}$ et $a_1x_{i_1} + \cdots + a_nx_{i_n} = 0$, alors $a_i = 0$ pour tout $i = 1, \dots, n$.

(Noter que, même si I est infini, la condition ci-dessus ne fait intervenir qu'un nombre fini de x_i.)

2) On dit que $(x_i)_{i\in \mathrm{I}}$ est une **base** de M si les x_i sont linéairement indépendants sur A et engendrent M ; ceci équivaut à dire que tout $m \in \mathrm{M}$ s'écrit de façon **unique** comme une somme finie

$$m = \sum_{i\in \mathrm{I}} a_ix_i,$$

où les a_i sont dans A et sont nuls sauf pour un nombre fini d'entre eux.

3) On dit que M est un A-module **libre** s'il possède une base.

Remarque 6.2. — Si l'anneau A n'est pas un corps, il existe des A-modules qui ne sont pas libres. En effet, soit I un idéal propre non nul de A. Alors le A-module non nul A/I n'est pas libre. En effet, soit $\alpha \in \mathrm{I}$ non nul. Pour tout $x \in \mathrm{A/I}$, on a $\alpha x = 0$; par conséquent aucune famille non vide d'éléments de A/I n'est libre.

Une autre obstruction au fait d'être libre est donnée par la remarque suivante.

Remarque 6.3. — Toute partie libre de A est nécessairement réduite à un seul élément. En effet, entre deux éléments distincts $a, b \in \mathrm{A}$ on a toujours la relation de dépendance linéaire non triviale :

$$b \cdot a - a \cdot b = 0.$$

Comme conséquence de cette remarque, on a l'exemple suivant.

Exemple 6.4. — Soient $\mathrm{A} = \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ et soit $\mathfrak{m} = (\mathrm{X}, \mathrm{Y})$, l'idéal engendré par X et Y. Alors, $\mathfrak{m}$ n'est pas un A-module libre.

En effet, s'il l'était, il aurait, d'après la remarque précédente, une base formée d'un seul polynôme $\mathrm{P} \neq 0$. Mais alors P, divisant X et Y, devrait être une constante $\lambda \in \mathbb{C}^*$, absurde puisque $\mathfrak{m} \neq \mathrm{A}$.

Par contre, voici des exemples de A-modules libres.

Exemples 6.5. — 1) Le A-module A possède la base $\{1\}$. Donc A est un A-module libre.

2) Plus généralement, pour tout $n \geqslant 1$, le A-module

$$\mathrm{A}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathrm{A}\}$$

est un A-module libre. En effet, il possède la base $\mathrm{B} = (e_1, \dots, e_n)$, où :

$$e_1 = (1, 0, \dots, 0), \quad \cdots \quad , e_n = (0, \dots, 0, 1).$$

3) Soit A[X] l'anneau des polynômes sur A. Alors, comme A-module, A[X] possède la base $\{\mathrm{X}^n\}_{n \geqslant 0}$. Donc A[X] est un A-module libre.

Plus généralement, on va voir dans le paragraphe suivant que pour tout ensemble I, il existe un A-module libre $\mathrm{A}^{(\mathrm{I})}$ ayant une base paramétrée par I.

Remarque 6.6. — Si k est un corps et V un k-espace vectoriel, on sait que les bases de V sont aussi caractérisées comme étant les parties libres maximales, ou les parties génératrices minimales. Dans le cas d'un anneau, ces deux propriétés sont strictement plus faibles que le fait d'être une base, comme le montrent les deux exemples suivants. Prenons $\mathrm{A} = \mathbb{Z}$.

1) La partie $\{2\}$ est libre, car si $0 = n \cdot 2 = 2n$ alors $n = 0$. (Plus généralement, dans un anneau intègre A, tout singleton $\{a\}$ avec $a \neq 0$ est une partie libre). La partie $\{2\}$ est libre maximale, d'après la remarque 6.3. Pourtant $\{2\}$ n'engendre pas $\mathbb{Z}$: le sous-module engendré est $2\mathbb{Z}$, l'idéal des entiers pairs.

2) La partie $\{2, 3\}$ est génératrice, car l'idéal engendré contient $1 = 3 - 2$ donc est égal à $\mathbb{Z}$. Comme aucune des sous-parties $\{2\}$ ou $\{3\}$ n'engendre $\mathbb{Z}$, alors $\mathrm{X} = \{2, 3\}$ est une partie génératrice minimale. Mais ce n'est pas une base, car elle n'est pas libre, d'après la remarque 6.3 : on a $3 \cdot 2 - 2 \cdot 3 = 0$.

6.2. Les modules libres $\mathrm{A}^{(\mathrm{I})}$. — Soit A un anneau et soit I un ensemble arbitraire.

Définition 6.7. — Soit A^{I} l'ensemble **produit**, c.-à-d.,

$$\mathrm{A}^{\mathrm{I}} = \{(a_i)_{i\in\mathrm{I}} \mid a_i \in \mathrm{A}\}$$

est l'ensemble des familles paramétrées par I d'éléments de A. C'est un groupe abélien, l'addition étant définie composante par composante. C'est aussi un A-module, pour la loi

$$a \cdot (b_i)_{i\in\mathrm{I}} = (ab_i)_{i\in\mathrm{I}}.$$

Pour tout $i \in \mathrm{I}$, notons e_i la famille $(\delta_{ij})_{j\in\mathrm{I}}$, où δ_{ij} est le *symbole de Kronecker*, c.-à-d.,

$$\delta_{ij} = \begin{cases} 1 & \text{si } j = i; \\ 0 & \text{sinon.} \end{cases}$$

Lemme 6.8. — *Les e_i, pour $i \in \mathrm{I}$, sont linéairement indépendants sur* A.

Démonstration. — C'est clair. □

Définition 6.9. — On note $\mathrm{A}^{(\mathrm{I})}$ le sous-A-module de A^{I} engendré par les éléments e_i, pour $i \in \mathrm{I}$. Alors, d'après le lemme précédent, $(e_i)_{i\in\mathrm{I}}$ est une base de $\mathrm{A}^{(\mathrm{I})}$ et, d'après la définition du sous-A-module engendré, $\mathrm{A}^{(\mathrm{I})}$ est l'ensemble de toutes les sommes finies

$$\sum_{j\in\mathrm{J}} a_j e_j,$$

où J est un sous-ensemble **fini** de I, et $a_j \in \mathrm{A}$.

Exemple 6.10. — Soit $\mathrm{I} = \mathbb{N}$. Alors $\mathrm{A}^{\mathbb{N}}$ est l'ensembles des **suites** $(a_0, a_1, \dots)$ d'éléments de A, et $\mathrm{A}^{(\mathbb{N})}$ est l'ensemble des suites **nulles à partir d'un certain rang**. Pour tout $i \in \mathbb{N}$, l'élément e_i est la suite

$$e_i = (0, \dots, 0, 1, 0, \dots), \quad \text{où 1 est à la } i\text{-ème place,}$$

et si $\underline{\mathbf{a}} = (a_0, a_1, \dots)$ est une suite nulle à partir d'un certain rang, c.-à-d., telle que $a_n = 0$ pour tout $n \geqslant n_0$, on a bien

$$\underline{\mathbf{a}} = \sum_{i\in\mathbb{N}} a_i e_i = \sum_{i=0}^{n_0} a_i e_i.$$

Remarque 6.11. — 1) Si $\mathrm{I} = \{1, \dots, n\}$ alors $\mathrm{A}^{(\mathrm{I})}$ égale A^{I} et s'identifie au A-module A^n déjà considéré, de base $(e_1, \dots, e_n)$.

2) Si $\mathrm{I} = \mathbb{N}$, on peut identifier le A-module libre $\mathrm{A}^{(\mathbb{N})}$, avec sa base $(e_i)_{i\in\mathbb{N}}$, au A-module libre A[X], avec sa base $(\mathrm{X}^i)_{i\in\mathbb{N}}$.

Remarque 6.12. — On peut montrer (ce n'est pas facile) que le $\mathbb{Z}$-module produit $\mathbb{Z}^{\mathbb{N}}$ n'est pas un $\mathbb{Z}$-module libre, cf. [**BAlg**], Chap. VII, § 3, Exercice 8.

Afin d'énoncer la propriété universelle du A-module libre $\mathrm{A}^{(\mathrm{I})}$, introduisons la notation suivante. Pour tout ensemble Y, notons Applic(I, Y) l'ensemble des applications $\mathrm{I} \to \mathrm{Y}$.

Théorème 6.13 **(Propriété universelle du A-module $\mathrm{A}^{(\mathrm{I})}$)**

Soit P *un* A*-module arbitraire. Pour avoir un morphisme de* A*-modules* $\phi : \mathrm{A}^{(\mathrm{I})} \to \mathrm{P}$*, il suffit d'avoir une application d'ensembles* $\psi : \mathrm{I} \to \mathrm{P}$*. De façon plus précise, l'application*

$$\mathrm{Hom}_{\mathrm{A}}(\mathrm{A}^{(\mathrm{I})}, \mathrm{P}) \longrightarrow \mathrm{Applic}(\mathrm{I}, \mathrm{P}), \qquad \phi \mapsto \phi|_{\mathrm{I}},$$

où $\phi|_{\mathrm{I}}$ *désigne l'application* $i \mapsto \phi(e_i)$*, est une bijection. Son inverse est l'application* $\psi \mapsto \widetilde{\psi}$*, où* $\widetilde{\psi}$ *est définie, pour tout* $\underline{a} = \sum_{i\in\mathrm{I}} a_i e_i$*, par*

$$(*) \qquad \widetilde{\psi}\left(\sum_{i\in\mathrm{I}} a_i e_i\right) = \sum_{i\in\mathrm{I}} a_i \psi(e_i).$$

(*Le slogan à retenir est : « un morphisme de source un module libre est uniquement déterminé par l'image d'une base ».*)

Démonstration. — Observons d'abord que la formule $(*)$ qui définit $\widetilde{\psi}$ fait sens. En effet, pour chaque $\underline{a} = \sum_{i\in\mathrm{I}} a_i e_i$, il n'y a qu'un nombre fini de coefficients a_i qui sont $\neq 0$ et donc la somme de droite dans $(*)$ est une honnête somme finie d'éléments de P. Ceci étant vu, il est clair que $\widetilde{\phi|_{\mathrm{I}}} = \phi$ et $\widetilde{\psi}\Big|_{\mathrm{I}} = \psi$, c.-à-d., les applications $\phi \mapsto \phi|_{\mathrm{I}}$ et $\psi \mapsto \widetilde{\psi}$ sont inverses l'une de l'autre. Le théorème est démontré. $\square$

TABLE DES MATIÈRES

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

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

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

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

[ChL] A. Chambert-Loir, Algèbre corporelle, Presses de l'École polytechnique, 2005.

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

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[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.

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovàř, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[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.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.