Théorème chinois *versus* lemme des noyaux

Soit A un anneau principal et $a \in A$ un élément. Comme tout anneau principal est factoriel, il existe une décomposition en irréductibles $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec u inversible, $p_1, \dots, p_r$ des irréductibles distincts, et $\alpha_i \geqslant 1$. Elle est unique à l'ordre près des facteurs et à des inversibles près. Si M est un A-module, on note $a : M \to M$, $x \mapsto ax$ la multiplication par a dans M et $M(a)$ son noyau.

1 Un énoncé général

Théorème 1. *Soient A un anneau principal, M un A-module, $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ un élément de A.*

(1) *Le module $M(a)$ est somme directe de ses sous-modules $M(p_i^{\alpha_i})$, i.e. le morphisme*

$$\begin{aligned} M(p_1^{\alpha_1}) \oplus \dots \oplus M(p_r^{\alpha_r}) &\longrightarrow M(a) \\ (x_1, \dots, x_r) &\longmapsto x_1 + \dots + x_r \end{aligned}$$

est un isomorphisme.

(2) *Le module M/aM est produit direct de ses quotients $M/p_i^{\alpha_i}M$, i.e. le morphisme*

$$\begin{aligned} M/aM &\longrightarrow M/p_1^{\alpha_1}M \times \dots \times M/p_r^{\alpha_r}M \\ x &\longmapsto (x, \dots, x) \end{aligned}$$

est un isomorphisme.

Remarque. On rappelle que la *somme directe* d'une famille de modules $\{M_i\}_{i \in I}$ est le sous-module du produit direct $\prod_{i \in I} M_i$ composé des familles (x_i) telles que seul un nombre fini des x_i sont non nuls. Lorsque l'ensemble d'indices I est fini, ce qui est le cas dans le théorème, la somme directe est donc égale au produit direct.

Démonstration : Pour chaque $i = 1, \dots, r$ soit $q_i = \prod_{j \neq i} p_j^{\alpha_j}$. On note que l'on a $p^{\alpha_i} q_i = u^{-1}a$ pour tout i. Les q_i n'ont aucun facteur irréductible commun (car p_i ne divise pas q_i), de sorte qu'ils sont premiers entre eux dans leur ensemble. D'après le théorème de Bézout, il existe $u_1, \dots, u_r$ dans A tels que $u_1 q_1 + \dots + u_r q_r = 1$.

(1) Considérons le morphisme $M(a) \to M(p_1^{\alpha_1}) \oplus \dots \oplus M(p_r^{\alpha_r})$, $y \mapsto (u_1 q_1 y, \dots, u_r q_r y)$. Celui-ci est bien défini car $y \in M(a)$ implique $q_i y \in M(p_i^{\alpha_i})$. On peut vérifier que c'est un isomorphisme inverse pour le morphisme donné ; nous laissons les détails en exercice au lecteur.

(2) Considérons le morphisme $M/p_1^{\alpha_1}M \times \dots \times M/p_r^{\alpha_r}M \to M/aM$, $(y_1, \dots, y_r) \mapsto u_1 q_1 y_1 + \dots + u_r q_r y_r$. Celui-ci est bien défini car pour si $y_i \in p_i^{\alpha_i}M$, l'image de $q_i y_i$ dans M/aM est nulle, de sorte que $q_i y_i \in M/aM$ est bien défini pour les y_i *modulo* $p_i^{\alpha_i}M$. (On a noté par la même lettre un élement de M et sa classe modulo $p_i^{\alpha_i}M$, pour simplifier.) On peut vérifier que c'est un isomorphisme inverse pour le morphisme donné ; nous laissons les détails en exercice à la lectrice. □

2 Cas des modules de a-torsion

Définition. Un A-module M est *de a-torsion* si $aM = 0$, c'est-à-dire si $ax = 0$ pour tout $x \in M$.

Tout A-module possède un plus grand sous-module qui est de a-torsion, c'est $M(a)$. De même, tout A-module possède un plus grand quotient qui est de a-torsion, c'est M/aM. Le théorème précédent est essentiellement un énoncé sur les modules de a-torsion : l'énoncé dans le cas général s'obtient en appliquant le point (1) au module de a-torsion $M(a)$ et le point (2) au module de a-torsion M/aM.

Le point (1) du théorème s'écrit parfois $\ker(p_1^{\alpha_1}) \oplus \cdots \oplus \ker(p_r^{\alpha_r}) \simeq \ker(a)$, avec la notation $\ker(a)$ pour $M(a)$, qui est naturelle compte tenu de sa définition. L'énoncé fait penser au lemme des noyaux en algèbre linéaire. En effet, le lemme des noyaux est le cas particulier où $A = k[X]$ est l'anneau des polynômes sur un corps k, et M est un k-espace vectoriel muni d'un endomorphisme f. Cet endomorphisme définit une structure de $k[X]$-module via $P.v = (P(f))(v)$ pour tous $P \in k[X]$ et $v \in M$. Si l'on prend pour a le polynôme minimal de f, ou son polynôme caractéristique, le $k[X]$-module E est de a-torsion.

Le point (2) du théorème, quant à lui, rappelle le théorème chinois : ce dernier est en effet le cas particulier obtenu en prenant $A = \mathbb{Z}$ et $M = \mathbb{Z}/n\mathbb{Z}$ pour un entier $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

Lorsque M est de a-torsion, on a $M(a) = M = M/aM$ de sorte que les énoncés (1) et (2) du théorème donnent tous deux une description de M. Une différence fondamentale est que (1) décrit M en termes de sous-modules alors que (2) décrit M en termes de modules quotients. Néanmoins, nous allons voir que ces énoncés sont en fait essentiellement les mêmes, et le lien entre sous-modules et modules quotients sera fait par l'observation suivante.

Lemme. *Soit M un module de a-torsion. Alors, le morphisme composé $\phi_i : M(p_i^{\alpha_i}) \hookrightarrow M \to M/p_i^{\alpha_i}M$ est un isomorphisme.*

Démonstration : Pour simplifier notons $p = p_i$, $\alpha = \alpha_i$, $q = q_i$, $\phi = \phi_i$. Fixons une relation de Bézout $vp^\alpha + wq = 1$ dans A. Montrons l'injectivité. On a $\ker(\phi) = M(p^\alpha) \cap p^\alpha M$. Si x est dans ce noyau, il existe $y \in M$ tel que $x = p^\alpha y$. De la relation de Bézout et du fait que $ay = 0$, on tire $x = p^\alpha y = vp^{2\alpha}y + wqp^\alpha y = vp^{2\alpha}y = vp^\alpha x = 0$. Montrons la surjectivité. Soit $z \in M/p^\alpha M$ et $\widetilde{z} \in M$ un élément qui le relève. On peut écrire $\widetilde{z} = vp^\alpha\widetilde{z} + wq\widetilde{z}$, ce qui montre que $\widetilde{z}$ est congru modulo $p^\alpha M$ à l'élément $wq\widetilde{z}$ qui appartient à $M(p^\alpha)$. Ainsi $\phi(wq\widetilde{z}) = z$ et ceci conclut. $\square$

Pour un module de a-torsion, on peut identifier $M(p_1^{\alpha_1}) \oplus \cdots \oplus M(p_r^{\alpha_r})$ et $M/p_1^{\alpha_1}M \times \cdots \times M/p_r^{\alpha_r}M$ à l'aide du morphisme $\phi := (\phi_1, \dots, \phi_r)$ défini par $\phi(x_1, \dots, x_r) = (\phi_1(x_1), \dots, \phi_r(x_r))$. On voit alors que les isomorphismes type « lemme des noyaux » et type « théorème chinois » se correspondent :

Théorème 2. *Soit M un module de a-torsion. Alors l'isomorphisme ϕ ci-dessus permet d'identifier les isomorphismes (1) et (2) du théorème 1, au sens où l'on a un diagramme commutatif :*

$$\begin{tikzcd}
M(p_1^{\alpha_1}) \oplus \cdots \oplus M(p_r^{\alpha_r}) \arrow[dd, "\phi"', "\wr"] \arrow[dr, bend left, "\text{lemme des noyaux}"] & \\
& M \arrow[dl, bend left, "\text{théorème chinois}"] \\
M/p_1^{\alpha_1}M \times \cdots \times M/p_r^{\alpha_r}M &
\end{tikzcd}$$

Démonstration : Il s'agit de vérifier ceci avec les formules explicites pour les trois isomorphismes en jeu. Il n'y a pas de véritable difficulté et ceci est laissé à la lectrice. $\square$