Un quotient est-il une sommande ?

A∼Z / Justin Carel

December 15, 2022

Non. $\mathbb{Z}/2\mathbb{Z} \cong \dfrac{\mathbb{Z}/4\mathbb{Z}}{2\mathbb{Z}/4\mathbb{Z}}$, mais $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ en tant qu'anneau comme module. La question présente tout de même un intérêt: "Dans quel cas un quotient est-il une sommande[1]?".

Pour les espaces vectoriels, on sait que le quotient est toujours isomorphe à un supplémentaire. Autrement dit, si $F \subseteq E$ sont deux k-ev, alors $E \cong F \times E/F$, et il existe un sev $G \cong E/F$ tel que $E = F \oplus G$. Ces faits sont conséquences du théorème de la base incomplète; on étend une base de F en une base de E.

Pour les modules sur un anneau — non nécessairement commutatif — la situation est moins claire: l'existence d'une base n'est pas garantie et on ne peut pas toujours identifier un quotient avec un sous-module. Afin d'obtenir une réponse partielle, nous allons tout d'abord nous concentrer sur la notion de somme et produit directs de modules.

1 Propriétés universelles de la somme et du produit

Commençons avec un rappel.

Définition 1.1 (Somme directe)**.** *Soit M un R-module à gauche et $(A_i)_{i\in I}$ une famille de sous-modules. On dit que $(A_i)_{i\in I}$ est en somme directe, notée*

$$\bigoplus_{i\in I} A_i := \sum_{i\in I} A_i,$$

si tout élément x de $\sum_i A_i$ s'exprime de manière unique en une somme $x = \sum_i a_i$ où (a_i) est à support fini et chaque a_i appartient à A_i.

Cette définition exprime le fait que tous les A_i sont "indépendants", ie qu'on ne trouve pas de combinaison linéaire non triviale annulant des éléments de A_i. Cela nous mène à une première caractérisation élémentaire:

Proposition 1.1. *Une famille $(A_i)_{i\in I}$ est en somme directe si et seulement si on a pour tout i,*

$$A_i \cap \sum_{i\neq j\in I} A_j = 0.$$

Preuve.

⇒) Si a est dans l'intersection, alors en particulier

$$a = \sum_{i\neq j\in I} a_j$$

pour certains a_j (à support fini). En posant $a_i = -a \in A_i$, on a $0 = \sum_j a_j$ donc $a = 0$.

⇐) Il suffit de montrer l'unicité de l'écriture pour 0.
Si $\sum_j a_j = 0$, alors pour tout i on a

$$a_i = -\sum_{i\neq j\in I} a_j$$

dans l'intersection, donc nul. □

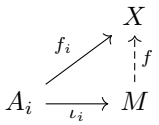
[1] J'ai complètement inventé ce terme — traduction douteuse de l'anglais "summand". Si quelqu'un connaît un mot réel utilisable ici, je suis toute ouïe.

En considérant les inclusions de chacun des A_i dans leur somme directe, cette caractérisation nous dit qu'elles ne se marchent pas sur les pieds. Autrement dit, $\bigoplus_i A_i$ est le plus petit R-module à gauche qui contient toute l'information des A_i. Précisons cette affirmation:

Théorème 1.1 (Propriété universelle du coproduit[2]). *Soit M un R-module à gauche. $M \cong \bigoplus_i A_i$ si et seulement si il est muni de R-morphismes $\iota_i : A_i \to M$ tels que pour tout X possédant des $f_i : A_i \to X$, il existe un unique f pour lequel*

$$\forall i \in I, f_i = f\iota_i.$$

Le diagramme suivant résume la situation:



On dit qu'un tel diagramme ***commute*** si tous les chemins sont les mêmes (ici, si $f_i = f\iota_i$).

Preuve.

⇒) Soit $M = \bigoplus_{i\in I} A_i$. On pose ι_i l'inclusion naturelle de A_i dans la somme directe. Si $a = \sum_i a_i \in \bigoplus_i A_i$, tout morphisme f respectant la condition $f_i = f\iota_i$ doit être de la forme

$$f(a) = f\left(\sum_{i\in I} a_i\right) = \sum_{i\in I} f(a_i) = \sum_{i\in I} f_i(a_i).$$

Réciproquement, cette somme définit bien un R-morphisme car (a_i) est à support fini.

Pour un M isomorphe à $\bigoplus_{i\in I} A_i$ par g, il suffit de poser $\iota'_i = g\iota_i$ et $f' = fg^{-1}$.

⇐) On prend $X = \bigoplus_{i\in I} A_i$ et f_i l'injection naturelle. La propriété universelle donne des uniques $f : M \to X$ et $g : X \to M$ tels que $f_i = f\iota_i$ et $\iota_i = gf_i$. Ainsi, on a $\iota_i = gf\iota_i$. En remplaçant X par M dans la propriété universelle, cela veut dire que $gf : M \to M$ convient. Mais l'identité 1_M convient aussi, et l'unicité donne $gf = 1_M$. Réciproquement, $fg = 1_X$; f est un isomorphisme de M vers $X = \bigoplus_{i\in I} A_i$. □

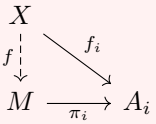
Remarque 1.1. Si $(A_i)_{i\in I}$ est une famille de R-modules à gauche, on peut définir le "produit à support fini" par le sous-ensemble du produit cartésien donné par les familles (a_i) où seul un nombre fini d'a_i est non nul. Ce sous-ensemble est stable par somme et multiplication par un scalaire, c'est donc un sous R-module à gauche; il s'avère qu'il vérifie la propriété universelle du coproduit.

On peut donc parler de somme directe externe: le théorème précédent nous permet de l'identifier à la somme directe interne dans le cas où les A_i sont des sous-modules en somme directe.

Exemple 1.1. Si R est un anneau commutatif, alors $R[X] \cong \bigoplus_{\mathbb{N}} R$.

De manière analogue, le produit direct peut être vu comme le module qui possède le plus d'informations sur les (A_i): si X peut se projeter sur tous les A_i, alors il peut se projeter de manière compatible sur leur produit.

Définition 1.2 (Propriété universelle du produit). *On appelle produit direct de $(A_i)_{i\in I}$ le R-module à gauche M muni de projections $\pi_i : M \to A_i$ telles que pour tout X muni de $f_i : X \to A_i$, il existe un unique f faisant commuter le diagramme suivant:*



De même que précédemment, cette propriété universelle définit un unique objet à isomorphisme près, que l'on notera

$$M = \prod_{i\in I} A_i.$$

Il n'y a pas de conflit de notations avec le produit cartésien, ce dernier vérifiant la propriété universelle.

[2]Somme et coproduit sont deux termes interchangeables.

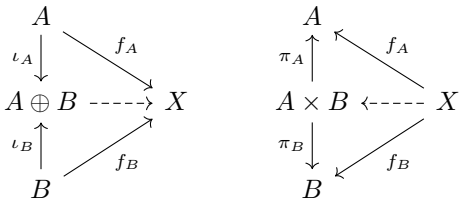
Exemple 1.2. Si R est un anneau commutatif, $R[[X]] \cong \prod_{\mathbb{N}} R$ en tant que modules.

Remarque 1.2. Dans le cas fini, le "produit à support fini" n'est autre que le produit tout court. Ainsi, pour les modules, les produits finis sont exactement les coproduits finis: on parle de biproduit. Les projections et les injections sont alors "compatibles" entre elles. En effet,

$$\pi_i \iota_i = 1_{A_i} \text{ et } \pi_i \iota_j = 0 \text{ si } i \neq j.$$

Remarque 1.3. Les propriétés universelles permettent de définir le produit et le coproduit pour d'autres objets que des modules. Cependant, on n'a pas toujours de biproduit dans le cas fini; par exemple, le coproduit d'anneaux est donné par le produit tensoriel (les injections étant $a \mapsto a \otimes 1$ et $b \mapsto 1 \otimes b$) tandis que le produit d'anneaux est simplement le produit cartésien.

Par la suite, on s'intéressera surtout au biproduit de deux modules. Il est donc important de garder les diagrammes correspondant en tête:



2 Quotients et Suites exactes

Définition 2.1. *On dit qu'une famille de morphismes $(f_i : X_i \to X_{i+1})_{i \in I}$ est une suite exacte si pour tout i,* $\operatorname{im} f_i = \ker f_{i+1}$.

Une suite exacte est souvent représentée par un diagramme de la forme suivante:

$$\ldots \xrightarrow{f_{i-1}} X_i \xrightarrow{f_i} X_{i+1} \xrightarrow{f_{i+1}} \ldots$$

Un type spécifique de suite exacte nous intéresse particulièrement pour sa relation avec les quotients: les suites exactes courtes

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

Notons qu'il n'est nul besoin de représenter les flèches partant de et allant en 0, car il s'agit nécessairement du morphisme nul. Le caractère exact de la suite force f à être injective ($\ker f = \operatorname{im} 0 = 0$) et g à être surjective ($\operatorname{im} g = \ker 0 = C$). De plus $\ker g = \operatorname{im} f \cong A$, et le premier théorème d'isomorphisme donne $C \cong B/A$.

Cette identité motive une réécriture des théorèmes d'isomorphismes en termes de suites exactes courtes.

Théorème 2.1 (Premier théorème d'isomorphisme)**.** *Pour tout R-morphisme $f : X \to Y$, la suite*

$$0 \longrightarrow \ker f \xrightarrow{\iota} X \xrightarrow{f} \operatorname{im} f \longrightarrow 0$$

est exacte, où $\iota : \ker f \to X$ est l'inclusion.

Preuve. Par définition. □

Théorème 2.2 (Second théorème d'isomorphisme)**.** *Si A et B sont des sous-modules de M, alors il existe f tel que le diagramme*[3]

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A\cap B & \hookrightarrow & A & \xrightarrow{\pi_1} & \dfrac{A}{A\cap B} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow f & & \\ 0 & \longrightarrow & B & \hookrightarrow & A+B & \xrightarrow{\pi_2} & \dfrac{A+B}{B} & \longrightarrow & 0 \end{array}$$

commute, ses lignes sont exactes, et f est un isomorphisme.

Preuve. L'exactitude est donnée par le théorème précédent. La commutativité demande $f\pi_1 = \pi_2\iota$, où ι est l'inclusion. Ainsi, si f existe alors $f(a+A\cap B) = \pi_2(a) = a+B$ pour tout a de A. On définit exactement f de cette manière: comme $A\cap B \subseteq A$, il s'agit du morphisme d'élargissement de classes.

Un élément de $(A+B)/B$ s'écrit $a+b+B = a+B$, donc $f\pi_1 = \pi_2\iota$ est surjective, soit f l'est. f est aussi injective: si $a\in A$, alors $f(a+A\cap B) = a+B = 0+B \iff a\in B \iff a\in A\cap B$, soit $a+A\cap B = \pi_1(a) = 0+A$ par exactitude. □

Théorème 2.3 (Troisième théorème d'isomorphisme)**.** *Si $C\subseteq B\subseteq A$ sont des R-modules à gauche, alors la suite*

$$0 \longrightarrow B/C \xrightarrow{\iota} A/C \xrightarrow{\pi} A/B \longrightarrow 0$$

est exacte, où ι et π sont l'inclusion et l'élargissement de classes.

Preuve. $\ker\pi = \{a+C \mid a\in B\} = \operatorname{im}\iota$. □

La propriété universelle de la somme directe de A et B demande deux injections $\mathrm{in}_l : A\to A\oplus B$ et $\mathrm{in}_r : B\to A\oplus B$. Celle du produit demande des projections $\pi_A : A\oplus B\to A$ et $\pi_B : A\oplus B\to B$. Une suite exacte courte $0\to A\to C\to B\to 0$ présente déjà deux de ces morphismes: une inclusion de A dans C et une projection de C dans B. Il ne manque donc qu'une injection $B\to C$ ou une projection $C\to A$ compatibles pour que $C = A\oplus B$.

Lemme 2.1 (Lemme de Séparation)**.** *Soit $0\to A\xrightarrow{f} C\xrightarrow{g} B\to 0$ une suite exacte courte. Les conditions suivantes sont équivalentes:*

1. *Il existe un isomorphisme $\varphi : C\cong A\oplus B$ tel que φf est l'injection naturelle de A et $g\varphi^{-1}$ est la projection naturelle sur B.*
2. *Il existe une flèche $\iota : B\to C$ telle que $g\iota = 1_B$.*
3. *Il existe une flèche $\pi : C\to A$ telle que $\pi f = 1_A$.*

La suite est alors dite ***séparée****.*

Preuve. Les propriétés universelles de la somme et du produit montrent $1\Rightarrow 2$ et $1\Rightarrow 3$.

$2\Rightarrow 1)$ Si une telle application existe, alors $(\iota g)^2 = \iota g\iota g = \iota g$, donc ιg est un projecteur sur $\iota(B)$ et $C\cong \ker\iota g\oplus\iota(B)\cong A\oplus B$ de manière compatible.

$3\Rightarrow 1)$ De même. □

Remarque 2.1. Au premier abord, il pourrait sembler que le lemme de séparation répond intégralement à la question originelle. Cependant, il ne s'agit en fait que d'une reformulation de la propriété universelle de la somme (2.) ou du produit (3.) dans le cadre des suites exactes. On a en quelque sorte déplacé le problème; ce nouveau langage se révèle néanmoins utile pour parler efficacement du problème en jeu.

[3] Les flèches en crochet représentent des inclusions.

3 Modules libres et projectifs

La séparation de toute suite exacte courte d'espaces vectoriels est due au théorème de la base incomplète: on peut toujours choisir une base et obtenir un projecteur sur une partie de la base. Définissons l'analogue dans le cas des modules:

Définition 3.1. *Soit M un R-module à gauche, soit X un ensemble. M est dit* ***libre*** *de base X si*

$$M \cong \bigoplus_{x \in X} \langle x \rangle,$$

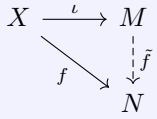
et $\langle x \rangle \cong R$ pour tout x de X.

Exemple 3.1. Pour tout n de $\mathbb{N}$, R^n est libre de base $\{(1,0,0,\dots,0,0),(0,1,0,\dots,0,0),\dots,(0,0,0,\dots,0,1)\}$. Plus généralement, $X^* := \bigoplus_X R$ est libre de base $(f_x)_{x \in X}$ où $f_x(y) = \delta_{x,y}$. On peut identifier f_x à x et dire que X^* est libre de base X.

Exemple 3.2. Soit R un domaine, et $a \in R$ un élément non nul. L'idéal principal aR est isomorphe à R en tant que R-modules (à droite) par $ar \mapsto r$. Ainsi, aR est libre de base a.

La notion de base capture l'idée que les éléments de X génèrent M de manière indépendante. Pour les espaces vectoriels, étudier une fonction sur une base est suffisant pour en déduire la fonction sur tout l'espace: nous montrons ci-après que cette propriété est non seulement nécessaire mais aussi suffisante pour caractériser une base.

Théorème 3.1 (Propriété universelle de l'objet libre)**.** *M est libre de base X si et seulement si pour tout module N muni d'une fonction $f : X \to N$, il existe un unique R-morphisme $\tilde{f} : M \to N$ faisant commuter le diagramme suivant:*



*On appelle $\tilde{f}$ l'****extension par linéarité*** *de f.*

Preuve.

$\Rightarrow$) Soit $f : X \to N$. Si $a \in M$ alors a se décompose en une somme finie $a = \sum_x r_x x$ où $r_x \in R$. On veut $\tilde{f}$ telle que

$$\tilde{f}(a) = \tilde{f}\left(\sum_{x \in X} r_x x\right) = \sum_{x \in X} r_x \tilde{f}(x) = \sum_{x \in X} r_x f(x).$$

Utiliser cette identité comme définition de $\tilde{f}$ donne un R-morphisme, bien défini par unicité de la décomposition.

$\Leftarrow$) On pose $N = X^*$ et $f : x \mapsto f_x$. On obtient $\tilde{f} : M \to X^*$ telle que $\tilde{f}\iota = f$ et $\tilde{\iota} : X^* \to M$ telle que $\tilde{\iota} f = \iota$. On a $\tilde{\iota}\tilde{f}\iota = \iota$, et en prenant $N = M$ l'unicité donne $\tilde{\iota}\tilde{f} = 1_M$. On montre de même que $\tilde{f}\tilde{\iota} = 1_{X^*}$, soit $\tilde{f} : M \to X^*$ est un R-isomorphisme. □

Proposition 3.1 (Unicité du rang)**.** *Si R est un anneau commutatif, alors $R^n \cong R^m$ si et seulement si $n = m$. Si M est libre de base finie X, on appelle* $\operatorname{rg} M = |X|$ *le* ***rang*** *de M.*

Preuve. Considérons $\mathfrak{m}$ un idéal maximal de R: $R/\mathfrak{m}$ est un corps. Montrons que $R^n \cong R^m$ en tant que R-modules implique $(R/\mathfrak{m})^n \cong (R/\mathfrak{m})^m$ en tant que $R/\mathfrak{m}$-espace vectoriels: l'unicité de la dimension permettra alors de conclure. Remarquons tout d'abord que si $M = A \oplus B$ est un R-module, alors $\mathfrak{m}M = \mathfrak{m}A \oplus \mathfrak{m}B$. D'où les égalités

$$(R/\mathfrak{m})^n \cong R^n/\mathfrak{m}^n = R^n/\mathfrak{m}R^n \cong R^m/\mathfrak{m}R^m = R^m/\mathfrak{m}^m \cong (R/\mathfrak{m})^m$$

en tant que R-modules. Comme $\mathfrak{m} \subseteq \operatorname{Ann}_R(R/\mathfrak{m})^n = \operatorname{Ann}_R(R/\mathfrak{m})^m$, une structure de $R/\mathfrak{m}$-espace vectoriel est induite. □

Exemple 3.3. La commutativité de R est nécessaire: autrement, le quotient par un idéal bilatère maximal peut ne pas résulter en un anneau à division.

Considérons $R = \operatorname{End} V$, où V est un espace vectoriel de dimension infinie. Prenons en une base X, et f une bijection entre X et $X \sqcup X$. On étend f par linéarité en $\tilde{f} : V \to V \times V$. L'application $\varphi = (- \circ \pi_1 \tilde{f}, - \circ \pi_2 \tilde{f})$, définie par

$$\varphi : \begin{array}{c} R \longrightarrow R \times R \\ g \longmapsto (g\pi_1\tilde{f}, g\pi_2\tilde{f}) \end{array}$$

est un R-isomorphisme entre R et R^2, considérés comme des R-modules à gauche.

Si M est un R-module et X est génératrice, on peut considérer M comme le module libre sur X dans lequel on force certaines équations à être vraies. Autrement dit, on se donne une nouvelle égalité plus faible qui est vérifiée si deux éléments s'écrivent comme les deux côtés d'une des équations susmentionnées. Il s'agit là exactement de la construction d'un quotient.

Lemme 3.1. *Tout module (finiment généré) est quotient d'un module libre (finiment généré).*

Preuve. Considérons X un ensemble de générateurs de M, et posons $L = X^*$ le module libre de base X. L'injection de X dans M s'étend par linéarité en un R-morphisme surjectif $f : L \to M$, soit $M \cong L/\ker f$. □

Nous avons désormais en mains les outils pour répondre partiellement à la question originale, en nous inspirant du cas des espaces vectoriels.

Théorème 3.2. *Soit M un R-module à gauche. Si M est libre, alors toute suite exacte de la forme*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} M \longrightarrow 0$$

est séparée.

Preuve. Considérons une telle suite, et posons X une base de M. Comme g est surjective, on peut choisir un antécédent $a(x)$ pour chaque x dans X. Soit $\tilde{a} : M \to B$ l'extension par linéarité de a:

$$\text{Si } m = \sum_{x \in X} m_x x, \text{ alors } ga(m) = \sum_{x \in X} m_x ga(x) = \sum_{x \in X} m_x x = m.$$

Ainsi $ga = 1_M$ et la suite exacte est séparée. □

Définition 3.2. *Un R-module à gauche M est dit **projectif** si toute suite exacte $0 \to A \to B \to M \to 0$ est séparée.*

Dans ce nouveau langage, le théorème précédent nous dit que tout module libre est projectif. Cette notion va nous permettre d'étudier dans quels cas la réciproque est vraie; établissons tout d'abord un lien plus précis entre modules libres et projectifs.

Proposition 3.2. *Un module est projectif si et seulement si il est une sommande d'un module libre. Autrement dit, M est projectif si et seulement si il existe L libre et $N \subseteq L$ tels que $L = M \oplus N$.*

Preuve.

⇒) Si M est projectif, alors la suite exacte $0 \to \ker \pi \to M^* \xrightarrow{\pi} M \to 0$ est séparée, donc $M \oplus \ker \pi \cong M^*$ est libre.

⇐) Si $0 \to A \xrightarrow{f} B \xrightarrow{g} M \to 0$ est exacte, alors

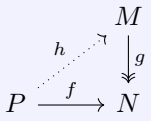
$$0 \longrightarrow A \xrightarrow{\iota_B f} B \oplus N \xrightarrow{\langle g, 1_N \rangle} M \oplus N \longrightarrow 0$$

est exacte, où $\iota_B : B \to B \oplus N$ est l'injection naturelle et $\langle g, 1_N \rangle (b, n) = (g(b), n)$. Mais $M \oplus N$ est libre, donc la suite est séparée: on trouve $\pi_A : B \oplus N \to A$ telle que $\pi_A \iota_B f = 1$. En considérant $\pi_A \iota_B$, la suite originelle est séparée. □

Exemple 3.4. Un sous-module d'un module libre M peut ne pas lui-même être libre — autrement tous les modules projectifs seraient libres. En prenant $R = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, R est libre mais pas le sous-module $\mathbb{Z}/2\mathbb{Z}$. Plus généralement, si $R = S \times T$ en tant qu'anneaux avec $S \ncong R \ncong T$ en tant que R-modules, alors S et T sont projectifs mais pas libres.

Un module projectif M, considéré comme un quotient $M \cong N/K$ au sein d'une suite exacte courte, "relève" tous les morphismes vers N/K en morphismes vers N — il suffit de composer avec l'injection $M \to M \oplus K \cong N$. En fait, il relève même les morphismes vers d'autres quotients quand il en est l'origine.

Théorème 3.3 (Propriété de relèvement)**.** *Un R-module à gauche P est projectif si et seulement si pour tous R-morphismes $f : P \to N$ et $g : M \twoheadrightarrow N$[4], il existe h faisant commuter le diagramme suivant:*



Preuve.

⇒) Il suffit de montrer l'implication pour un module libre. Il existe en effet P' tel que $P \oplus P'$ est libre, et on peut ajouter $1_P : P \to P \oplus P' \to P$ à gauche du diagramme.

Considérons donc une base X de P. g étant une surjection, on peut trouver une section $g' : N \to M$. Alors $g'f$ est une fonction de X dans M, que l'on étend par linéarité en un morphisme $h : P \to M$. De plus $gh(x) = gg'f(x) = f(x)$ pour tout x de X, donc $gh = f$.

⇐) Considérons une suite exacte courte $0 \to \bullet \to M \xrightarrow{g} P \to 0$. Comme g est surjective, prendre $N = P$ et $f = 1_P$ donne un relèvement de g. La suite est donc séparée. □

Remarque 3.1. On n'est pas en présence d'une propriété universelle: le relèvement h n'est presque jamais unique. En effet, h' est un autre relèvement si et seulement si $g(h - h') = 0$, soit si $h(x) - h'(x) \in \ker g$ pour tout x de X. On trouve donc $|\ker g|^{|X|}$ relèvements distincts.

Une raison pour laquelle il existe des modules projectifs non libres est que R peut posséder des sous-modules non isomorphes à lui-même. Si tous les sous-modules de R sont isomorphes à R, ils sont en particulier cycliques: R est principal. De plus, l'isomorphisme assure que le générateur de l'idéal n'est pas un diviseur de 0: R est intègre.

Théorème 3.4. *Soit R un anneau principal à gauche, c'est à dire intègre et tel que tout idéal gauche est principal. Alors tout sous-module d'un R-module à gauche libre est libre. En particulier, tout R-module à gauche projectif est libre.*

Est donnée ci-dessous une preuve tirée de nlab. Voir aussi [Rot15, p.332].

Preuve. Soit $M \subseteq L$ des R-modules tels que L soit libre de base J. On a $L \cong \bigoplus_J R$, et l'axiome du choix permet de supposer l'existence d'un bon-ordre[5] sur J. Définissons les sous-modules de L suivants:

$$L_{\leq j} = \bigoplus_{x \leq j} R_x \text{ et } L_{<j} = \bigoplus_{x<j} R_x, \text{ où les } R_x \text{ sont des copies de } R.$$

Tout élément de $M \cap L_{\leq j}$ s'écrivant de manière unique comme (x, r) où $x \in L_{<j}$ et $r \in R_j$, on peut définir le morphisme

$$p_j : \begin{array}{ccc} M \cap L_{\leq j} & \longrightarrow & R \\ (x, r) & \longmapsto & r \end{array}$$

de noyau $M \cap L_{<j}$ induisant une suite exacte

$$0 \longrightarrow M \cap L_{<j} \longrightarrow M \cap L_{\leq j} \xrightarrow{p_j} \operatorname{im} p_j \longrightarrow 0.$$

[4] Le harpon signifie que g est une surjection.
[5] Ordre pour lequel tout sous-ensemble admet un minimum.

Or $\operatorname{im} p_j$ est un sous-module de R qui est principal, donc $\operatorname{im} p_j = Rr_j$ pour un certain $r_j \in R$. Il est isomorphe ou à 0 ou à R par $xr_j \mapsto x$, donc libre, donc la suite exacte est séparée: $M \cap L_{\leq j} = M \cap L_{<j} \oplus \langle m_j \rangle$, où $p_j(m_j) = r_j$. Posons

$$K = \{m_j \mid j \in J, r_j \neq 0\},$$

et montrons que K est une base de M. Pour l'indépendance linéaire: si des $(a_i) \in R^n$ sont tels que

$$\sum_{i=1}^{n} a_i m_{k_i} = 0 \text{ où } k_1 < k_2 < \ldots < k_n,$$

alors $0 = a_n p_{k_n}(m_{k_n}) = a_n r_{k_n}$. R étant un domaine et r_{k_i} étant non nul, on en déduit $a_n = 0$. Par récurrence, les (a_i) sont nuls.

Pour le caractère générateur, considérons le plus petit j de J tel qu'on trouve $m \in M \cap L_{\leq j}$ ne pouvant s'exprimer comme combinaison linéaire des $(m_k)_{k \in K}$. Comme $\operatorname{im} p_j = Rr_j$, on trouve r tel que $p_j(m) = rr_j$. Ainsi $p_j(m - rm_j) = 0$ soit $m - rm_j \in M \cap L_{<j}$. Mais $m - rm_j$ ne peut s'exprimer en tant que combinaison linéaire des $(m_k)_{k \in K}$, ce qui contredit la minimalité de j.

On a bien $M = \bigoplus_{m \in K} \langle m \rangle$. □

Remarque 3.2. Ce théorème admet des analogues: Kaplansky a montré que tout module projectif sur un anneau local est libre [Kap58]; Quillen et Suslin ont fait de même pour des anneaux polynomiaux [Qui76; Sus76].

References

[Kap58] Irving Kaplansky. "Projective modules". English. In: *Ann. Math. (2)* 68 (1958), pp. 372–377. ISSN: 0003-486X. DOI: 10.2307/1970252.

[Qui76] Daniel Quillen. "Projective modules over polynomial rings". English. In: *Invent. Math.* 36 (1976), pp. 167–171. ISSN: 0020-9910. DOI: 10.1007/BF01390008.

[Rot15] Joseph J. Rotman. "Advanced modern algebra. Part 1". English. In: 3rd edition. Vol. 165. Grad. Stud. Math. Providence, RI: American Mathematical Society (AMS), 2015, p. 332. ISBN: 978-1-4704-1554-9.

[Sus76] A. A. Suslin. "Projective modules over a polynomial ring are free". English. In: *Sov. Math., Dokl.* 17 (1976), pp. 1160–1164. ISSN: 0197-6788.