Formes quadratiques et isomorphisme : la simplification de modules projectifs et de formes hermitiennes

Laura Fainsilber

Dans un ensemble muni d'une loi de composition interne notée $+$, on dit que l'on peut simplifier par un élément b, ou que b est réguher, si pour toute paire d'éléments a, c tels que $a + b = c + b$, on a $a = c$. Dans un groupe, tous les éléments sont réguliers.

Nous allons voir ici des situations où l'on a une notion naturelle de somme, mais où l'on ne peut pas toujours simplifier. Autrement dit, on trouvera dans l'ensemble des modules ainsi que dans l'ensemble des formes quadratiques ou hermitiennes des objets X, Y, Z tels que $X \oplus \mathrm{Y} \simeq Z \oplus \mathrm{Y}$ mais $X \not\simeq Z$ On trouve également des problèmes de simplification dans la théorie des noeuds de dimension supérieure.

La question de la simplification (cancellation en anglais) est très importante pour voir quels éléments s'annulent lorsque l'on définit une structure de groupe sur l'ensemble.

1. Modules projectifs, K_0

Definitions : Soit A un anneau, pas nécessairement commutatif, et soit M, un module à gauche sur A. On dit que M est *de type fini* s'il existe une famille génératrice finie $(m_i)_{1<i<s}$ telle que tout élément du module s'ecrive comme combinaison $A-$ linéaire des m_i. On dit que M est *libre* s'il existe une famille génératrice pour laquelle cette écriture est unique. Dans ce cas, les m_i forment une base, et $M \simeq A^s$. Un module M est dit *projectif* s'il existe un A-module N tel que $M \oplus N$ soit un module libre.

On s'intéressera ici aux modules projectifs de type fini. Tous les modules considérés dams la suite seront de ce type.

Exemples
• si $A = k$ est un corps, les modules de type fini sont les espaces vectoriels $V = k^n$; ils sont tous libres, et *a fortiori* projectifs.
• Si $A = \mathrm{Z}$, les modules $\mathrm{Z}/n\mathrm{Z}$ ont de la torsion alors que Z n'en a pas, et ne sont donc pas projectifs. Les seuls modules projectifs sont les libres $\mathbb{Z}^s$.
• Soit $A = \mathrm{Mn(k)}$ l'anneau des matrices carrées de dimension n sur un corps k. Alors le k-espace vectoriel $V = k^n$ est un module projectif mais pas libre. On a un isomorphisme de A-modules $V \oplus V^{n-1} \simeq A$.

Le groupe K_0. Le premier (ou plutôt le 0-ième) niveau de construction de la K$-$ théorie est la construction d'un groupe additif à partir de l'ensemble des A-modules projectifs de type fini.

Soit M un A-module projectif de type fini. On note $[M]$ sa classe d'isomorphisme, et l'on considère toutes les sommes formelles $\sum_{i=1}^{n} a_i[M_i]$ de A-modules avec $a_i \in \mathbb{Z}$,

en posant l $[M]+(-l[M]) = [0] = 0$. On définit une relation d'équivalence engendrée par les relations

$$[M \oplus M'] \equiv [M] + [M']$$

et l'on pose

$$\mathrm{K_0(A)} = \left\{ \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{a_i}\,[\mathrm{M_i}] \right\} / \equiv .$$

On dit qu'un A-module projectif est *stablement libre* s'il existe des entiers naturels r, s tels que $M \oplus A^s \simeq A^r$, autrement dit, si l'on peut prendre un module libre comme complément de M dans la définition de projectif. En particulier, tout module libre est stablement libre. Dans les exemples ci-dessus, tous les modules stablement libres étaient en fait libres, mais ce n'est pas toujours le cas (voir la question Q'_1 ci-dessous).

De manière similaire, on peut affaiblir la notion d'isomorphisme en disant que deux modules M et N sont *stablement isomorphes* s'il existe un entier naturel r tel que $M \oplus A^r \simeq N \oplus A^r$, autrement dit s'ils sont isomorphes à l'addition d'un module libre près.

Proposition 1 *Soient M et M' deux A-modules projectifs de type fini. Alors $[M]$ et $[M'\mathrm{J}$ représentent la même classe dans $\mathrm{K_0}$ si et seulement si M et M' sont stablement isomorphes.*

La démonstration est la suivante : $[M \oplus A^r] = [M' \oplus A^r] \Leftrightarrow [M]+[A^r] \equiv [M']+[A^r] \Leftrightarrow [M]+[A^r]-[A^r] \equiv [M']+[A^r]-[A^r] \Leftrightarrow [M] \equiv [M']$.

Autrement dit, $\mathrm{K_0(A)}$ est le groupe des classes d'isomorphisme stable de A-modules. On a pour ainsi dire forcé la simplification par les modules libres dans le groupe $\mathrm{K_0(A)}$. Lorsque pour un anneau A les libres ne se simplifient pas, on introduit par ce biais de nouvelles simplifications, si bien que $\mathrm{K_0(A)}$ ne reflète pas toujours bien la structure donnée par la somme directe sur l'ensemble des A-modules, et qu'il arrive que $\mathrm{K_0(A)}$ soit réduit à l'élément neutre (voir la question $\mathrm{Q_2}$).

Questions. Etant donné un anneau A, on peut se poser les questions suivantes :

$\mathrm{Q_1}$ Est-ce que tous les A-modules projectifs sont libres ?

La réponse est oui si A est un corps, si $A = \mathrm{Z}$, si A est un anneau principal, ou si A est un anneau de polynômes sur un corps. Pour ce dernier cas, la question a été posée par J.-P. Serre vers 1950, et résolue indépendemment par Quillen et Suslin. On a vu que la réponse était non dans le cas d'un anneau de matrices.

Q'_1 Est-ce que tous les A-modules projectifs sont stablement libres ?

C'est un affaiblissement de la première question. Il y a des exemples d'anneaux d'entiers de corps de nombres (des extensions de Q par le groupe quaternionien d'ordre 32 $\mathbb{H}_{32}$ données par Swan) possédant des modules stablement libres mais non libres. Si la réponse est oui pour un anneau A, alors on a pour tout M, des entiers r et s tels que $M \oplus A^s \simeq A^r$ d'où, dans $\mathrm{K_0(A)}$, $[M] \equiv [A^r] - [A^s] \equiv [A^{r-s}]$, et dans ce cas $\mathrm{K_0(A)}$ est le groupe cyclique engendré par $[A]$. La réponse est encore non pour l'anneau $\mathrm{M_n(k)}$ de matrices carrées de dimension n sur un corps k ; en fait $\mathrm{K_0(M_n(k))}$ est engendré par la classe de l'espace vectoriel k^n.

$\mathrm{Q_2}$ Est-ce que deux modules stablement isomorphes sont isomorphes ?
Autrement dit, peut-on simplifier par les modules libres ?

Si oui, alors en particulier les modules stablement libres sont libres. Si la réponse aux questions $\mathrm{Q_1'}$ et $\mathrm{Q_2}$ est oui, alors tous les modules projectifs sont libres, et $\mathrm{K_0(A)} = \langle [\mathrm{A}] \rangle \simeq \mathbb{Z}$ est cyclique infini. Un exemple d'anneau pour lequel la réponse à $\mathrm{Q_2}$ est négative est l'anneau d'endomorphismes d'un espace vectoriel de dimension infinie sur un corps. Pour un tel anmeau A, on a $A \oplus A \simeq A$. En fait, dans ce cas, $\mathrm{K_0(A)} = \{0\}$.

Simplification. Soient P, Q, et N des A-modules tels que $P \oplus N \simeq P \oplus Q$; a-t-on $P \simeq Q$?

n-simplification. Soient P et Q des A-modules tels que $P \oplus \ldots \oplus P \simeq Q \oplus \ldots \oplus Q$ (n copies de P et de Q) ; a-t-on $P \simeq Q$? Des contre-exemples sont donnés par des anneaux tels que $\mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\zeta_{23}], \mathbb{Z}[X]$.

M_n-simplification. Soient A et B des anneaux tels que les algèbres de matrices $M_n(A)$ et $M_n(B)$ soient isomorphes. A-t-on $A \simeq B$?

On a la simplification et la n-simplification sur tous les anneaux pour lesquels le théorème de Krull-Schmidt de décomposition unique des modules est valable. Il en va ainsi par exemple des anneaux principaux, des anneaux artiniens, des algèbres qui sont des modules de type fini sur un anneau local complet tel que $\mathbb{Z}_p$. On peut aussi avoir la simplification et la n-simplification sans le théorème de Krull-Schmidt, par exemple pour des algèbres finies sur un anneau commutatif local.

Dans une situation où les modules se simplifient, on peut se demander si l'on a des simplifications similaires lorsque l'on ajoute une structure hermitienne.

2. Formes hermitiennes sur les anneaux

Soit A un anneau muni d'une anti-involution : $A \to A$ (i.e. une application bijective telle que, pour tous $a, b \in A, \overline{\overline{a}} = a$ et $\overline{ab} = \overline{b}\,\overline{a}$). Soit M un A-module à gauche, projectif de type fini.

Definitions. Une *forme hermitienne* sur M est une application $h : M \times M \to A$ qui est bi-additive, sesquilinéaire (i.e. pour tous $a, b \in A, m, n \in M$, on a $h(am,\ bn) = ah(m,\ n)\overline{b}$) et telle que pour tous $m, n \in M, h(n,\ m) = \overline{h(m, n)}$.

Lorsque par exemple A est un anneau commutatif ou un corps et que l'anti- involution est l'identité, les formes hermitiennes sont les formes bilinéaires symétriques. Si de plus 2 est inversible dans A, elles correspondent bijectivement aux formes quadratiques : on pose $q(m) = h(m,\ m)$ et $h(m,\ n) = \frac{1}{2}(q(m+n) - q(m) - q(n))$.

On note $M^{\perp} = \{m \in M\ ; \forall n \in M,\ h(m,\ n) = 0\}$. Une forme hermitienne est dite *régulière* si $M^{\perp} = \{0\}$.

On appelle *module hermitien* une paire $(M,\ h)$ formée d'un module et d'une forme sur ce module.

Un *morphisme* (resp. *isomorphisme*) de modules hermitiens de $(M,\ h)$ dans $(M^l,\ h')$ est un morphisme (resp. isomorphisme) de A-modules $f : M \to M'$ tel que $h^t(fm,\ fn) = h(m, n)$ pour tous les $m, n \in M$. On étudie l'ensemble des modules hermitiens à isomorphisme près.

La *somme directe* de deux modules hermitiens $(M, h) \oplus (M',\ h')$ est un module hermitien $(M \oplus M', h \oplus h$ où l'on pose $(h \oplus h')(m + m', n + n^l) = h(m, n) + h'(m', n$ pour tous $m, n \in M, m', n^l \in M'$.

Si le module M est libre, de base $(e_1, \ldots, e_r)$, on peut représenter h par une matrice $B = (b_{ij})_{i,j}$ où $b_{ij} = h(e_i,\ e_j)$. On a alors $h(m, n) = (m^t)B(\overline{n})$. Deux formes sont isomorphes si et seulement si elles sont représentées par des matrices congruentes : $B^l = P^t BP$, pour une matrice inversible P.

Simplification de modules hermitiens. Si A est un anneau local (i.e. ayant un seul idéal maximal) dans lequel 2 est inversible, ou si A est un corps, tous les modules projectifs sont libres, et toute matrice symétrique est congruente à une matrice diagonale. Dans une telle situation, où l'on a la simplification des modules, on se demande si les modules hermitiens se simplifient.

Le premier résultat important de la théorie des formes quadratiques qui concerne toutes les formes sur un corps, et non plus des formes ou des familles de formes particulières, comme par exemple les sommes de n carrés ou les formes binaires, a été démontré par Witt en 1937 :

Théorème de simplification de Witt : *Soit k un corps, alors on a la simptification pour les modules bilineaires symétriques réguliers. Autrement dit, soient* $(V,\ q)$, $(V_1,\ q_1)$, $(V_2,\ q_2)$ *trois modules bilinéaires symétriques sur k tels que*

$$(V_1, q_1) \oplus (V, q) \simeq (V_2, q_2) \oplus (V, q)$$

alors

$$(V_1, q_1) \simeq (V_2, q_2)$$

La démonstration est géométrique, on y étend des isométries en utilisant le lemme de Cartan-Dieudonné ([3])

On a pu généraliser ce résultat à une grande classe d'anneaux, commutatifs ou non (mais pour lesquels on a la simplification des modules), qui contient par exemple des algèbres de matrices $M_n(\mathbb{Z}_p)$, où $\mathbb{Z}_p$ est l'anneau des entiers p-adiques ($p \neq 2$) , et les anneaux de groupes $\mathbb{Z}_p[G]$ pour les groupes finis G.

Théorème 1 ([*11*, [*21*) : *Soit A un anneau muni d'une anti-involution-, qui est une algèbre libre de type fini comme module sur un anneau de valuation discrète complet, et dont le centre contient un élement a tel que $a + \overline{a} = 1$ (par exemple $\frac{1}{2}$ si 2 est inversible dans A). Alors on a la simplification pour tous les modules hermitiens sur A.*

La démonstration fait intervenir des arguments de la théorie des catégories pour représenter les modules hermitiens sur A par des formes hermitiennes dans une autre catégorie. On représente ensuite ces formes par des formes plus simples sur des anneaux plus compliqués. On réduit alors la question à celle de la simplification sur les corps et on utilise le théorème de Witt.

Cependant, il ne faut pas avoir l'impression que la simplification des modules hermitiens suit en général la simplification des modules : voyons simplement comme contre-exemple le cas de l'anneau Z et des formes unimodulaires (i.e. représentées par des matrices inversibles). Il y a bien sûr moins de matrices inversibles sur $\mathbb{Z}$ que sur $\mathbb{Q}$, mais cela signifie surtout qu'il y a beaucoup moins d'isomorphismes de formes, en particulier les formes symétriques me soot pas toutes diagonalisables, et l'ensemble des formes unimodulaires sur $\mathbb{Z}$ est bien plus difficile à décrire.

Prenons par exemple ([3] 1.6), sur $V = \mathbb{Z}^2$, les formes quadratiques $q_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ et $q_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Ces formes me sont pas isomorphes, en effet, $q_1((x,\ y)) = 2xy + y^2$ peut prendre toutes les valeurs dans $\mathbb{Z}$ alors que $q_2((x,\ y))$ ne prend que des valeurs paires.

Or, $q_1 \oplus \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix} \simeq q_2 \oplus \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}$, comme le montre la congruence de matrices suivante :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & -1 \end{pmatrix}$$

Si l'on rend 2 inversible en se plaçant sur l'anneau $\mathbb{Z}[\frac{1}{2}]$, alors $q_1 \simeq q_2$ et ces formes ne fournissent plus un contre-exemple.

Cependant, on trouve aussi des contre-exemples plus fondamentaux, qui reposent sur le fait que $\mathbb{Z}$ n'est pas complet (voir [4]) ; les formes unimodulaires impaires indéfinies sont toutes isomorphes à des formes diagonales n'ayant que des 1 et des -1 sur la diagonale. Elles sont donc classifiées par le rang et la signature (nombre de 1 moins le nombre de -1 dans la forme diagonale) Or, les formes paires définies positives sont Γ_8 en rang 8, $\Gamma_8 \oplus \Gamma_8$ et Γ_{16} en rang 16. Les formes $\Gamma_8 \oplus \Gamma_8$ et Γ_{16} isomorphes après addition d'un plan hyperbolique $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. En rang 32, il y a plus de 80 millions de classes d'isomorphismes. En ajoutant à de telles formes un plan hyperbolique, on obtient des formes indéfinies impaires de rang 34 et de signature 30, donc toutes isomorphes. On voit ici que l'on est loin de pouvoir simplifier !

Ceci illustre la difficulté que l'on a sur $\mathbb{Z}$ à utiliser une structure de groupe sur l'ensemble des formes unimodulaires. En effet, deux formes qui sont stablement isomorphes correspondent forcément au même élément du groupe, or comme on a vu que de telles formes pouvaient ne pas être isomorphes, le groupe de Witt, qui est l'outil principal de représentation des formes sur un corps, ne peut pas refléter la richesse de l'ensemble des formes sur un anneau où la simplification de Witt me fonctionne pas.

Références

[1] *E. Bayer-Fluckigerl L. Fainsilber*, Non-unimodular Hermitian forms, Inventiones Mathematicae, à paraître.

[2] *L. Fainsilber*, Formes hermitiennes sur les algèbres p-adiques, thèse, Université de Franche-Comté (1994).

[3] *W. Scharlau*, Quadratic and Hermitian Forms, Grundlehren der Math : Wiss. **270**, Springer Verlag (1985).

[4] *J.-P. Serre*, Cours d'arithmétique, P.U.F., Paris (1970).

Laboratoire de Mathématiques
Université de Franche-Comté
16 route de Gray
25030 Besançon
email : laura@vega.univ-fcomte.fr