

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

JEAN-PIERRE LAFON

Anneau des endomorphismes d'un module de type fini sur un anneau local

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 2 (1958-1959), exp. n° 15, p. 1-18

http://www.numdam.org/item?id=SD_1958-1959__12_2_A2_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1958-1959, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

16 février 1959

Séminaire P. DUBREIL,
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)

Année 1958/59

ANNEAU DES ENDOMORPHISMES D'UN MODULE DE TYPE FINI SUR UN ANNEAU LOCAL

par Jean-Pierre LAFON

On peut, pour l'étude de l'anneau $L(E)$ des A -endomorphismes d'un module de type fini E sur un anneau local A , se placer à deux points de vue différents : l'étude globale de $L(E)$ et l'étude d'un endomorphisme particulier. C'est le premier point qui fera le but du présent exposé.

NOTATIONS et RAPPELS. - A désignera un anneau local (commutatif), c'est-à-dire un anneau à élément unité tel que l'ensemble des non-inversibles forme un idéal m qui est alors l'unique idéal maximal de A ; k sera le corps des restes A/m . Nous supposons A noethérien, pour simplifier, mais il apparaîtra que cette hypothèse est parfois inutile.

E est un A -module de type fini (unitaire); E/mE a une structure de k -espace vectoriel, nous le noterons \bar{E} . (e_1, \dots, e_n) est un système minimal de générateurs de E sur A ; il résulte du lemme de Nakayama que ceci est équivalent à : les classes $\bar{e}_1, \dots, \bar{e}_n$ forment une base sur k de \bar{E} .

Un sous-module de E sera dit caractéristique s'il est invariant par tous les A -endomorphismes de E : ce terme est souvent réservé aux sous-modules invariants par tous les automorphismes de E , mais, comme nous n'aurons pas dans cet exposé à considérer de tels sous-modules, cette définition sera sans inconvénient.

Un anneau non commutatif sera dit complètement primaire si l'ensemble des non-inversibles à gauche forme un idéal qui est alors nécessairement maximal à gauche et à droite : c'est donc un idéal bilatère et le quotient par cet idéal est un corps, non nécessairement commutatif.

1. Une filtration de $L(E)$.

Remarquons que les sous-modules $m^i E$ sont caractéristiques : en effet, soit u un élément de $L(E)$, si $x \in m^i E$, x peut s'écrire au moins d'une façon $x = a_1 e_1 + \dots + a_n e_n$ avec $a_j \in m^i$. Il en résulte

$u(x) = a_1 u(e_1) + \dots + a_n u(e_n) \in m^i E$. . Donc $u(m^i E) \subset m^i R$.

Nous voyons donc que si $x \equiv y \pmod{m^i E}$, $u(x) \equiv u(y) \pmod{m^i E}$. Si ξ est la classe de x modulo $m^i E$, nous poserons $u_i(\xi) =$ classe de $u(x)$ modulo $m^i E$.

On vérifie sans difficulté que u_i est une application de $E/m^i E$ dans $E/m^i E$ qui est A/m^i -linéaire, que l'application $u \rightarrow u_i$ est un homomorphisme de $L(E)$ dans $L(E/m^i E)$. Pour que u appartienne au noyau de cet homomorphisme, il faut et il suffit que pour tout $x \in E$, $u(x) \in m^i E$; ce noyau est, donc, $\text{Hom}_A(E, m^i E)$ et on peut donc écrire la suite exacte suivante.

PROPOSITION 1 :

$$0 \longrightarrow \text{Hom}_A(E, m^i E) \longrightarrow L(E) \longrightarrow L(E/m^i E) \longrightarrow \dots$$

où $E/m^i E$ sera considéré comme muni de sa structure de A/m^i -module.

REMARQUE. - Plus généralement, si C est un sous-module caractéristique, on aura de la même manière, la suite exacte

$$0 \longrightarrow \text{Hom}_A(E, C) \longrightarrow L(E) \longrightarrow L(E/C) \longrightarrow \dots$$

D'autre part, nous voyons que si u agit sur le système de générateurs comme la matrice (a_{ji}) , $(u(e_i) = \sum a_{ji} e_j)$, u_i agira sur les images modulo $m^i E$, qui forment un système minimal de générateurs de $E/m^i E$ sur A/m^i , comme la matrice obtenue en réduisant modulo m^i les coefficients de (a_{ji}) .

Il est possible de présenter autrement cette question, avec l'avantage de nous donner les termes suivants de la suite exacte écrite.

On peut associer à la suite exacte $0 \rightarrow m^i E \rightarrow E \rightarrow E/m^i E \rightarrow 0$, la suite exacte des ext :

$$0 \longrightarrow \text{Hom}_A(E, m^i E) \longrightarrow \text{Hom}_A(E, E) \longrightarrow \text{Hom}_A(E, E/m^i E) \longrightarrow \text{Ext}_A^1(E, m^i E) \longrightarrow \dots$$

Montrons que $\text{Hom}_A(E, E/m^i E)$ s'identifie canoniquement à $\text{Hom}_A(E/m^i E, E/m^i E)$, puis à $\text{Hom}_{A/m^i}(E/m^i E, E/m^i E)$.

Soit $u : E \rightarrow E/m^i E$ et soit $x = a_1 e_1 + \dots + a_n e_n$ avec $a_j \in m^i$ un élément de $m^i E$, il vient $u(x) = a_1 u(e_1) + \dots + a_n u(e_n) \in m^i E$. $E/m^i E = 0$;

donc, le noyau de u contient $m^i E$ et u induit un endomorphisme \tilde{u} de $E/m^i E$; d'où une application $i : u \rightarrow \tilde{u}$ de $\text{Hom}_A(E, E/m^i E)$ dans $L(E/m^i E)$. Réciproquement à $\tilde{u} \in L(E/m^i E)$, on fait correspondre $j(\tilde{u}) = u \circ \varphi$ il est immédiat que $j \circ i$ (resp. $i \circ j$) est l'application identique de $\text{Hom}_A(E, E/m^i E)$ (resp. $L(E/m^i E)$). Donc i est une bijection de $\text{Hom}_A(E, E/m^i E)$ sur $L(E/m^i E)$ et j sa bijection réciproque.

Il faut remarquer que ceci ne s'applique pas à un sous-module caractéristique quelconque, mais aux sous-modules de la forme IE où I est un idéal de A .

Les sous-modules $\text{Hom}_A(E, m^i E)$ constituent une filtration décroissante de $L(E)$ et les quotients associés à chaque terme fournissent des approximations de $L(E)$; en particulier, $L(E)/\text{Hom}_A(E, mE)$ fournit une première approximation de $L(E)$ par une algèbre à élément unité de dimension finie sur le corps des restes k . Cette approximation très simple fournit déjà quelques résultats intéressants, (surtout, peut-être, pour l'étude d'un endomorphisme particulier).

2. Représentation matricielle de $L(E)$.

La représentation matricielle sera très utile pour la construction d'exemples et surtout de contre-exemples.

Soit $0 \rightarrow R \rightarrow L \rightarrow E \rightarrow 0$ le premier terme d'une résolution minimale de E : L est le A -module libre engendré par les e_j , R est le sous-module des relations. Nous admettrons (voir, par exemple, BOURBAKI, [3], paragraphe 2 exercice 2).

$L(E)$ est isomorphe au quotient $M(E)/O(E)$ où $M(E)$ est l'anneau des endomorphismes u^* de L tels que $u^*(R) \subset R$, i.e. laissant stable le sous-module des relations, et $O(E)$ l'ensemble des u^* tels que $u^*(L) \subset R$, qui forment de manière évidente un idéal bilatère de $M(E)$.

Comme L est noethérien, R est de type fini et est engendré par y_1, \dots, y_m . Si $L = Ax_1 \oplus Ax_2 \oplus \dots \oplus Ax_n$, on peut écrire $y_i = \sum b_{ji} x_j$ et nous désignerons par P la matrice (b_{ji}) qui a n lignes et m colonnes, et, nous dirons que c'est la matrice de passage de R . Si nous prenons pour u^* sa matrice par rapport à la base x_j , nous trouvons sans difficulté que $(a_{ji}) \in M(E)$ si et seulement s'il existe une matrice carrée de rang m à coefficients dans A , (a'_{ji}) telle que $(a_{ji})(b_{ji}) = (b_{ji})(a'_{ji})$, représentant, en fait, l'effet de l'endomorphisme induit par u^* sur les y_i . Pour

que $(a_{ji}) \in O(E)$, il faut et il suffit que $(a_{ji}) = (b_{ji})(b'_{ji})$ où (b'_{ji}) est une matrice à coefficients dans A à m lignes et n colonnes.

PROPOSITION 2. - $L(E)$ est le quotient $M(E)/O(E)$ où $M(E)$ est l'ensemble des matrices carrées d'ordre n satisfaisant à $MP = PM'$ où P est la matrice de passage du sous-module des relations, et, où $O(E)$ est l'ensemble des matrices carrées PB' d'ordre n de la forme PB' ,

Il est important de remarquer que les matrices de $M(E)$ fournissent les endomorphismes de E de la façon suivante : $u(e_i) = \sum a_{ji} e_j$, c'est-à-dire si u^* agit sur x_i comme (a_{ji}) , alors l'endomorphisme induit sur E agit sur e_i comme (a_{ji}) , les anneaux quotients $L(E)/\text{Hom}_A(E, m^i E)$ s'obtenant alors facilement.

En particulier $\text{Im}(L(E) \rightarrow L(\bar{E}))$ s'obtient en réduisant modulo m les coefficients des matrices de $M(E)$: en effet, les éléments de $O(E)$ sont des matrices à coefficients dans m comme (b_{ji}) (si, par exemple, $b_{11} \notin m$, on aurait $e_1 = (b_{11})^{-1} (b_{21} e_2 + \dots + b_{n1} e_n)$, contrairement à l'hypothèse faite sur les e_i).

Nous avons, en prenant $\text{Im}(L(E) \rightarrow L(\bar{E}))$ un procédé de construction d'algèbres à élément unité de dimension finie sur un corps k . Peut-on obtenir toute telle algèbre par ce procédé par choix convenable de A et E ?

THÉORÈME. - Soit S une algèbre à élément unité de dimension finie sur le corps k . Il existe un anneau local A (au moins un) de corps des restes k et un module de type fini E sur A avec $\text{rg}(E) = d$ tel que $S = \text{Im}(L(E) \rightarrow L(\bar{E}))$.

Nous considérerons S comme identifiée à sa représentation régulière. Soit S' le commutant de S . Il est classique que S est égale à son bicommutant, i.e. une matrice $M \in S$ si et seulement si elle commute avec tout élément de S' . Si $1, M_2, \dots, M_n$ est une base de S' sur k , il revient au même de dire que M commute avec cette base, soit, si X_1, \dots, X_n sont des indéterminées, avec $X_1 1 + X_2 M_2 + \dots + X_n M_n = P$, matrice à coefficients dans $k[[X_1, \dots, X_n]]$ et, d'ailleurs, formes linéaires en les X_i . Prenons alors $A = k[[X_1, \dots, X_n]]$ et E quotient du module libre A^n par le sous-module dont la matrice de passage est P . Montrons que $\text{Im}(L(E) \rightarrow L(\bar{E}))$ est S .

Il est d'abord clair, d'après la proposition 2, que S se plonge dans $L(E)$. Soit (a_{ji}) une matrice représentant un endomorphisme u ; elle satisfait à

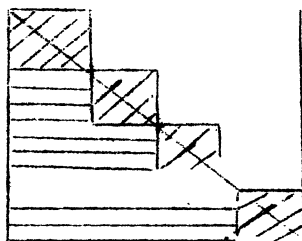
$(a_{ij})^P = P(a_{ji}^!)$. Désignons par (\bar{a}_{ji}) (resp. $(\bar{a}_{ji}^!)$) la matrice obtenue à partir de (a_{ji}) (resp. $(a_{ji}^!)$) en ne gardant que les termes constants. L'homogénéité de P en les X_i implique $(\bar{a}_{ji})^P = P(\bar{a}_{ji}^!)$. Si l'on fait $X_2 = \dots = X_n = 0$ et $X_1 = 1$ dans P , on obtient $(\bar{a}_{ji}) = (\bar{a}_{ji}^!)$; donc $(\bar{a}_{ji})^P = P(\bar{a}_{ji}^!)$ et $(\bar{a}_{ji}) \notin S$. Donc, $S = \text{Im}(L(E) \rightarrow L(\bar{E}))$.

On peut remarquer que $\text{dh}(A)$ (dimension homologique de A) = $\dim(S') \dim(A)$. Il n'y a pas unicité de l'obtention de S : nous verrons, par exemple, que l'algèbre des matrices à coefficients dans k de la forme :

$$\begin{vmatrix} a & 0 \\ b & c \end{vmatrix}$$

peut être obtenue à partir d'un anneau de valuation discrète, alors que notre construction nous oblige à prendre $A = k[[X_1, X_2, X_3]]$. Il est intéressant de se demander, étant donnée une algèbre S , quels anneaux locaux et quels modules permettent de l'obtenir. Nous ne savons actuellement apporter que les précisions suivantes :

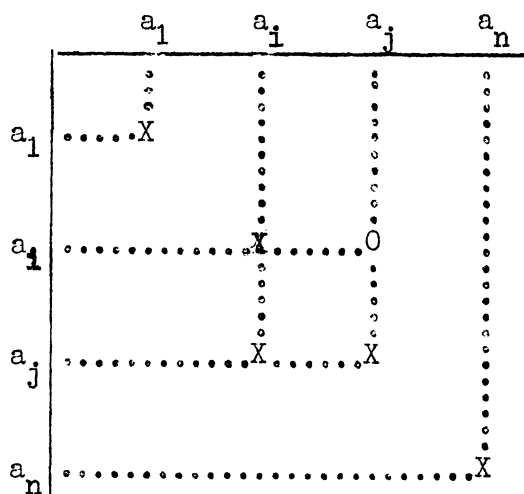
Pour que S puisse être obtenue à partir d'un anneau de valuation discrète il faut et il suffit qu'elle puisse avoir une représentation matricielle de la forme



où les éléments dans les zones hachurées sont arbitraires, les autres étant nuls (on reconnaîtra la partie semi-simple de S , à savoir les blocs diagonaux et le radical de Jacobson hachuré horizontalement).

Plus généralement, on peut étudier les algèbres obtenues avec des sommes directes de modules monogènes : $E = A/a_i$ où a_i sont des idéaux de A .

Considérons le tableau :



On aura un élément arbitraire noté X à l'intersection de la i -ième colonne et de la j -ième ligne si et seulement si $a_i \subset a_j$ sinon on obtiendra 0 .

On obtient ainsi les algèbres de ce type dont la représentation matricielle est le graphe d'une relation d'ordre. On peut montrer qu'en dimension 2, on peut réaliser toute relation d'ordre sur n éléments au moyen d'idéaux de A . Par le procédé considéré, avec des sommes directes de modules monogènes, on obtiendra, donc, en dimension 2 toutes les algèbres indiquées ci-dessus. Il faut remarquer que pour qu'une telle algèbre soit commutative ou semi-simple, il faut et il suffit qu'il n'y ait aucune relation d'inclusion entre les a_i .

3. Passage au complété, puis à un anneau régulier complet.

Il résulte des propriétés de platitude de la complétion que si \hat{A} est le complété de A , \hat{E} le complété de E :

$$\text{Hom}_{\hat{A}}(\hat{E}, \hat{m}^i \hat{E}) = \widehat{\text{Hom}_A(E, m^i E)} \quad \text{et} \quad L(\hat{E}) = \widehat{L(E)} .$$

Pour ces propriétés, voir [11].

On en déduit que

$$L(\hat{E})/\text{Hom}_{\hat{A}}(\hat{E}, \hat{m}^i \hat{E}) = \widehat{L(E)/\text{Hom}_A(E, m^i E)} .$$

Il sera ainsi possible, dans un certain nombre de questions de supposer A complet.

D'autre part, en vertu des théorèmes de structure de Cohen, tout anneau local complet est quotient d'un anneau local régulier complet B de même corps des

restes k . Si E est un A -module de type fini de système minimal de générateurs (e_i) , on peut le munir de façon évidente d'une structure de B -module. Notons E_B , E muni de cette structure. Par des arguments évidents et déjà utilisés, on voit que $L(E_B)$ s'identifie canoniquement à $L(E)$ et que $\text{Im}(L(E_B) \rightarrow L(\bar{E})) = \text{Im}(L(E) \rightarrow L(\bar{E}))$.

Ce qui précède justifie, dans une certaine mesure, l'importance des séries formelles pour la recherche de contre-exemples.

4. Etude des $\text{Hom}_A(E, m^i E)$

Montrons d'abord que $\text{Hom}_A(E, mE)$ est contenu dans le radical de Jacobson r de $L(E)$.

LEMME. - Si $R \subset L$ où L est un module libre de type fini sur l'anneau commutatif A à élément unité, si u est un automorphisme de L stable sur R , alors u^{-1} est stable sur R , et, par suite u induit un automorphisme sur R et sur L/R .

Soit en effet x_1, \dots, x_n une base de L sur R et supposons que : $u(x_i) = \sum a_{ji} x_j$. Si $\chi_u(X)$ est le polynôme caractéristique de (a_{ji}) , le théorème d'Hamilton Cayley montre que $\chi_u(u) = 0$, soit :

$$u^n + a_1 u^{n-1} + \dots + a_n = 0$$

avec $a_n = \det(a_{ji})$. Si u est un automorphisme de L , a_n est inversible dans A et

$$1 = (a_n)^{-1} (u^{n-1} + a_1 u^{n-2} + \dots + a_{n-1})u ;$$

l'inverse de u est donc un polynôme en u à coefficients dans A et il laisse stable R . u induit donc un automorphisme sur R et sur L/R .

Revenons au cas A local, et E , A -module de type fini ; et considérons la suite exacte déjà utilisée : $0 \rightarrow R \rightarrow L \rightarrow E \rightarrow 0$. Le lemme montre que, si u est induit par un automorphisme de L , c'est un automorphisme de E . Réciproquement, si u est un automorphisme de E il existe $v \in L(E)$ tel que $uv = 1$; si u^* et v^* sont des endomorphismes de L induisant u et v , $u^* v^* \in 1 + \text{Hom}_A(L, mL)$, donc u^* est inversible dans $L(L)$, i.e. u^* est un automorphisme de L .

PROPOSITION 3. - Si $0 \rightarrow R \rightarrow A^n \rightarrow E \rightarrow 0$ est une suite exacte, où E est de rang n, tout automorphisme de E est induit par un automorphisme de A^n (stable sur R), et, réciproquement, si un endomorphisme de A^n (stable sur R) induit un automorphisme de E, c'est un automorphisme de A^n .

On en déduit :

COROLLAIRE. - On a les inclusions $m^i L(E) \subset \text{Hom}_A(E, m^i E) \subset r$, radical de Jacobson de $L(E)$.

Il est immédiat que $m^i L(E) \subset \text{Hom}_A(E, m^i E)$ car un endomorphisme de $m^i L(E)$ admet une matrice de représentation (et éventuellement une seule) à coefficients dans m^i .

Pour montrer que $\text{Hom}_A(E, m^i E) \subset r$, il suffit de montrer que tout $u \in 1 + \text{Hom}_A(E, mE)$ est inversible. Or, le lemme montre, en fait, que la condition nécessaire et suffisante pour que u soit inversible est que u possède une matrice de représentation inversible (et, alors toute matrice de représentation l'est). Si $u \in 1 + \text{Hom}_A(E, mE)$, le déterminant d'une matrice de représentation de u est congru à 1 modulo m , donc inversible.

On n'a pas forcément $\text{Hom}_A(E, m^i E) = m^i L(E)$. Prenons, en effet, $A = k[[X_1, X_2]]$ et E quotient du module libre $Ax_1 \oplus Ax_2$ par le sous-module $Ay_1 + Ay_2$ avec $y_1 = X_1 x_1$ et $y_2 = X_2^2 x_2$. On vérifie en utilisant la représentation matricielle que $L(E)/mL(E)$ est isomorphe à l'algèbre des matrices de la forme

$$\begin{vmatrix} a & 0 & 0 \\ 0 & b & 0 \\ c & 0 & b \end{vmatrix}$$

alors que $L(E)/\text{Hom}_A(E, mE)$ est isomorphe à l'algèbre des matrices de la forme

$$\begin{vmatrix} a & 0 \\ 0 & b \end{vmatrix} .$$

On n'a pas, non plus, forcément $\text{Hom}_A(E, mE) = r$. Prenons le même A que ci-dessus et pour E le quotient du même L par le sous-module $Ay_1 + Ay_2$ avec $y_1 = X_1 x_1$ et $y_2 = X_2 x_1 + X_1 x_2$. On vérifie que $L(E)/\text{Hom}_A(E, mE)$ est isomorphe à l'algèbre des matrices à coefficients dans k de la forme

$$\begin{vmatrix} a & b \\ 0 & a \end{vmatrix}$$

qui n'est autre que l'algèbre des nombres duaux sur k , anneau local d'idéal maximal l'ensemble des matrices de la forme

$$\begin{vmatrix} 0 & b \\ 0 & 0 \end{vmatrix}$$

Il faut remarquer que si E est libre ou monogène (plus généralement A/a libre si a est l'annulateur de E), $nL(E) = \text{Hom}_A(E, nE) = r$. Nous verrons ultérieurement des précisions sur le cas $r = nL(E)$.

5. Etude de la surjectivité de $\varphi : L(E) \rightarrow L(\bar{E})$.

Les exemples qui précèdent montrent que $\text{Im}(L(E) \rightarrow L(\bar{E}))$ n'est pas en général $L(\bar{E})$ tout entier. Il en est ainsi si E est libre ou monogène (ou ce qui recouvre ces deux cas, si E est A/a -libre, si a est l'annulateur de E). Nous voulons démontrer la réciproque :

THÉOREME. - La condition nécessaire et suffisante pour que $\varphi : L(E) \rightarrow L(\bar{E})$ soit une surjection est que E soit A/a -libre si a est l'annulateur de E .

Nous allons utiliser comme lemme un théorème d'Azumaya qui se révélera très utile pour l'étude d'un endomorphisme particulier. La démonstration en est trop longue pour figurer ici et nous renvoyons à [1]. Signalons toutefois que, dans le cas d'un anneau local complet, le lemme bilinéaire de Samuel permet d'abrégér sensiblement cette démonstration. Dans ce théorème, algèbre signifiera modulo de type fini sur l'anneau local A , avec, en plus, une structure d'anneau.

THÉOREME (AZUMAYA). - Si R est une algèbre sur l'anneau local hensélien A

1° pour tout idéal bilatère I de R , tout système d'idempotents orthogonaux de R/I , peut être relevé en un système d'idempotents orthogonaux de R .

2° Si I est contenu dans le radical de Jacobson de R , toute base canonique de sous-algèbres de matrices de R/I peut être relevée dans R .

Notons que ce théorème généralise des théorèmes classiques pour les algèbres de dimension finie sur un corps k [7].

Rappelons qu'un anneau local complet est hensélien, la réciproque étant fautive, exemple : séries convergentes en n variables à coefficients complexes.

Il résulte de 3 que $L(E) \rightarrow L(\bar{E})$ surjectif est équivalent à $L(\hat{E}) \rightarrow L(\bar{E})$ surjectif. Nous supposons donc A complet.

Si $\bar{x}_1, \dots, \bar{x}_n$ est une base de \bar{E} , soit $(\bar{\varepsilon}_{ij})$ la base canonique de $L(\bar{E})$ associée. Puisque $\text{Hom}_A(E, mE) \subset r$, on peut appliquer le théorème d'Azunaya et relever cette base canonique en une base canonique (ε_{ij}) d'une sous-algèbre de matrices de $L(E)$. Remarquons que $\varepsilon_{11} + \dots + \varepsilon_{nn} = s$ est inversible, car $s \in 1 + \text{Hom}_A(E, mE)$. D'autre part, les ε_{ii} sont des idempotents deux à deux orthogonaux. Si s^{-1} est l'inverse de s , $s^{-1} \varepsilon_{11} + \dots + s^{-1} \varepsilon_{nn} = 1$ et par multiplication à droite par ε_{ii} , il vient $s^{-1} \varepsilon_{ii} = \varepsilon_{ii}$, d'où $\varepsilon_{11} + \dots + \varepsilon_{nn} = 1$.

Posons $E_i = \varepsilon_{ii}(E)$; on voit que E est somme directe des E_i et que les E_i sont monogènes car $E_i/mE_i = E_i + mE/mE = k\bar{x}_i$. Soit, donc, $E_i = Ax_i$ ($i = 1, \dots, n$) où x_i est un représentant de \bar{x}_i dans E_i . On a le formulaire :

$$\varepsilon_{ii}(x_i) = \ell_i x_i$$

avec ℓ_i inversible comme on le voit en passant à \bar{E}

$$\varepsilon_{ji}(x_j) = \varepsilon_{jj} \varepsilon_{ji}(x_i) \in \varepsilon_{jj}(E) = Ax_j \quad ;$$

d'où $\varepsilon_{ji}(x_i) = \ell_{ij} x_j$ avec ℓ_{ij} inversible.

$$\varepsilon_{jk}(x_i) = \varepsilon_{jk} \varepsilon_{ii}(\ell_i x_i) = 0 \quad \text{si } k \neq i$$

Supposons d'abord E fidèle et supposons qu'il existe une relation :

$a_1 x_1 + \dots + a_n x_n = 0$ à coefficients dans A . On en déduit, par application de ε_{ji} , $a_i x_j = 0$ ($j = 1, \dots, n$), soit $a_i E = 0$, donc $a_i = 0$ et E est A -libre.

Si A n'était pas complet, il est clair que E fidèle sur A implique \hat{E} fidèle sur \hat{A} . Si on prend pour \hat{E} un système minimal de générateurs qui soit aussi un système minimal de générateurs de E , ce système est une base de \hat{E} , d'après NAKAYAMA, c'est donc une base de E qui est A -libre.

Si E n'était pas fidèle, on considérerait E comme un A/a -module où a est l'annulateur de E . Le théorème est donc démontré.

On peut déduire de ce qui précède un critère de liberté d'un module de type fini fidèle sur un anneau local. Ecrivons la suite exacte

$$0 \rightarrow \text{Hom}_A(E, mE) \rightarrow \text{Hom}_A(E, E) \rightarrow \text{Hom}_A(E, E/mE) \rightarrow \text{Ext}_A^1(E, mE) \rightarrow \text{Ext}_A^1(E, E) \rightarrow \text{Ext}_A^1(E, mE) = 0$$

implique que $L(E) \rightarrow L(\bar{E})$ est surjectif, donc que E est A -libre. Réciproquement, si E est A -libre $\text{Ext}_A^1(E, mE) = 0$. D'où

COROLLAIRE. - Si E est un module de type fini sur l'anneau local A , fidèle, il y a équivalence entre :

- i. E est A -libre ;
- ii. $\text{Ext}_A^1(E, mE) = 0$
- iii. $L(E) \rightarrow L(\bar{E})$ est surjectif.

Il faut remarquer que les conclusions du corollaire et du théorème restent valables si A n'est pas noethérien, à condition de le supposer hensélien. On peut se demander ce que signifie la nullité de certains des termes suivants de la suite des Ext . Il n'est pas difficile de voir que :

$\text{Ext}_A^1(E, E/mE)$ est équivalent à E est A -libre.

Si A est un anneau de valuation discrète, ou plus généralement, si E est de dimension homologique 1, $\text{Ext}_A^1(E, E) = 0$ implique que E est A -libre (immédiat à partir des deux conditions obtenues).

6. Structure des $L(E)$.

Les $L(E)$ sont évidemment des algèbres au sens d'AZUMAYA. Ils rentrent dans la famille plus vaste des anneaux semi-locaux généralisés définis par BATHO comme des anneaux non nécessairement commutatifs R de radical de Jacobson J tels que :

- i. $\bigcap J^n = (0)$
- ii. R est noethérien à gauche
- iii. R/J est artinien à gauche.

Si l'on munit un tel anneau de sa topologie J -adique, on en fait un espace métrique, d'où par des arguments standard la possibilité de définir la complétion \hat{R} de R comme un sur-anneau complet de R dans lequel R soit partout dense. Dans le cas commutatif, on retrouve évidemment les anneaux semi-locaux usuels.

Il est immédiat qu'une algèbre au sens d'AZUMAYA est un tel anneau : en effet, $mR \subset J$, donc R/J est une algèbre à élément unité de dimension finie sur le corps des restes k . Les idéaux à gauche de R/J sont des sous-espaces vectoriels et satisfont donc à la condition de chaîne ascendante. D'autre part, J/mR est le radical de R/mR qui est artinien en tant qu'algèbre de dimension finie sur k . J/mR est donc nilpotent et il existe un entier p tel que $J^p \subset mR$. Il s'ensuit que les topologies J -adique et mR -adique coïncident ; ceci implique (i) Nous voyons de plus que si A est complet, il en est de même de R dans la topologie J -adique.

THÉORÈME (AZUMAYA). - Si A est hensélien et si R est une algèbre sur A .

$$R = M_{n_1}(C_1) \oplus \dots \oplus M_{n_p}(C_p) \oplus N$$

où chaque C_i est complètement primaire et où N est un sous-groupe de J .

Le principe de la démonstration est : R/J est semi-simple ; on relève les idempotents centraux qui donnent les composantes simples en des idempotents qui ne sont plus forcément centraux : ceci fournit une décomposition en somme directe d'idéaux à gauche ; si on veut des idéaux bilatères on utilise la décomposition de Peirce qui donne un sous-groupe N de J . Chaque idéal bilatère apparaissant dans la somme directe donne en passant au quotient une composante simple de R/J , on relève alors les bases canoniques d'algèbres de matrices [1].

THÉORÈME (AZUMAYA, BATHO) il y a équivalence entre :

i. R est somme directe d'algèbres de matrices sur les anneaux complètement primaires.

ii. R est non ramifiée, i.e. $J = mR$.

iii. les idempotents qui apparaissent dans la décomposition du théorème précédent sont centraux.

(i) \Leftrightarrow (iii) si $R = e_1 R e_1 \oplus \dots \oplus e_n R e_n$ tout $r \in R$ s'écrit $r = e_1 r e_1 + \dots + e_n r e_n$, d'où $r e_i - e_i r = e_i r e_i - e_i r e_i = 0$.

Réciproquement, si les e_i sont centraux

$$r = r e_1 + \dots + r e_n = e_1 r e_1 + \dots + e_n r e_n$$

(i) \Leftrightarrow (ii) en effet, si $J = mR$, on a $R = (e_1 R e_1) \oplus \dots \oplus (e_n R e_n) \in mR$ et il suffit d'appliquer le lemme de Nakayama.

Réciproquement, il est clair que si $R = e_1 R e_1 \oplus \dots \oplus e_n R e_n$, on a $J = mR$.

COROLLAIRE. - Soit E un A -module de type fini A local hensélien, la condition nécessaire et suffisante pour que $r = nL(E)$ est que E soit somme directe de sous-modules caractéristiques E_i tels que $L(E_i)$ soit une algèbre complète de matrices sur un anneau complètement primaire.

Supposons, en effet, les e_i du théorème dans le centre de $L(E)$, i.e. quel que soit $u \in L(E)$, $ue_i = e_i u$. Alors $u(e_i(E)) = e_i(u(E)) \subset e_i(E)$; le sous-module $E_i = e_i(E)$ est donc caractéristique et E est somme directe des E_i . On a de plus $L(E_i) = M_{n_i}(C_i)$.

Réciproquement, soit $E = \bigoplus E_i$ où les E_i sont caractéristiques et tels que $L(E_i) = M_{n_i}(C_i)$. Soit p_i le projecteur associé à E_i . E_i caractéristique implique $up_i(E) \subset p_i(E)$ pour tout $u \in L(E)$, soit $(1 - p_i)up_i = 0$ d'où $up_i = p_i up_i$. Mais on a de même $u \sum_{j \neq i} e_j = \sum_{j \neq i} p_j up_j$, soit $p_i u(1 - p_i) = 0$ d'où $up_i = p_i u = p_i up_i$.

EXEMPLE. - $A = k[[X_1, X_2]]$ $E = k[[X_1]] \oplus k[[X_2]]$.

Le corollaire est en particulier valable si $L(E)$ est commutatif (ce qui est possible; exemple précédent).

Si, en particulier, $L(E) = C_1 \oplus \dots \oplus C_p$ où les C_i sont complètement primaires, $E = E_1 \oplus \dots \oplus E_p$ où les E_i sont caractéristiques et indécomposables. On vérifie alors, sans difficulté (voir BOURBAKI, [5] chap. 7 paragraphe 4 exercice 16) qu'il y a unicité de la décomposition de E en somme directe de modules indécomposables: ceci donne une interprétation dans un cas particulier d'un théorème d'Azumaya ("On generalized semi primary rings and Krull-Remark-Schmid's theorem").

Il est évident qu'au stade où nous en sommes certains problèmes restent en suspens.

Le plus intéressant sans doute est de savoir si E et F sont deux modules sur le même anneau local A , ce qu'implique $L(E) = L(F)$ pour E et F .

Dans le cas d'anneaux locaux primaires principaux, SCHIFFMANN, BAER et JABOBSON ont montré que tout isomorphisme de $L(E)$ et $L(F)$ est induit par un isomorphisme de E et F . Les deux premiers se sont servi, à cet effet, de la théorie des idéaux de $L(E)$. Mais, dans le cas plus général que nous envisageons, quelques

difficultés se présentent et pratiquement, nous limiterons aux idéaux bilatères maximaux. Signalons, toutefois, que certains résultats de Schiffman non mentionnés ici passent sans difficulté grâce à un formulaire partiel analogue.

7. Idéaux de $L(E)$.

Certains résultats se transposeront immédiatement aux idéaux à droite ; il suffira pour les sous-modules de supprimer "caractéristique".

A tout sous-module caractéristique C de E correspondent deux idéaux bilatères :

$$l(C) = \text{Hom}_A(E, C)$$

$$r(C) = \text{ensemble des } u \in L(E) \text{ tels que } u(C) = 0$$

A un idéal bilatère I correspondent deux sous-modules caractéristiques

$$l(I) = \sum_{u \in I} u(E)$$

$\mathfrak{N}(I)$ noyau de I , i.e. ensemble des $x \in E$ tels que $u(x) = 0$ pour tout $u \in I$

On a le formulaire (SCHIFFMAN)

$$\mathfrak{N}(r(C)) \subset C \quad r(\mathfrak{N}(I)) \supset I$$

$$l(l(C)) \subset C \quad l(l(I)) \supset I$$

si

$$C_1 \subset C_2, \quad r(C_1) \supset r(C_2), \quad l(C_1) \subset l(C_2)$$

si

$$I \subset J, \quad \mathfrak{N}(I) \supset \mathfrak{N}(J), \quad l(I) \subset l(J)$$

$$r(\mathfrak{N}(r(C))) = r(C), \quad \mathfrak{N}(r(\mathfrak{N}(I))) = \mathfrak{N}(I)$$

$$l(l(l(C))) = l(C), \quad l(l(l(I))) = l(I)$$

$$r(C) l(C) = 0$$

mais on n'a pas

$$l(l(C)) = C \quad \text{et} \quad \mathfrak{N}(r(C)) = C$$

comme l'avait SCHIFFMAN.

Un contre-exemple en est fourni par $\Lambda = k[[X_1, X_2, X_3]]$ quotient du module libre $\Lambda x_1 \oplus \Lambda x_2 \oplus \Lambda x_3$ par le sous-module engendré par $y_1 = X_1 x_1$; $y_2 = X_2 x_1 + X_1 x_2$; $y_3 = X_3 x_1 + X_1 x_3$ et $C = \Lambda e_1 + \Lambda e_2 + \Lambda e_3$ avec des notations évidentes

$$\text{In}(L(E) \longrightarrow L(\bar{E}))$$

est alors

$$\begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$$

THEOREME. - Si I est un idéal bilatère maximal, ou bien $L(I) = E$, ou $I = \text{Hom}_{\Lambda}(E, C)$ où C peut être choisi caractéristique maximal. Réciproquement si C est un sous-module caractéristique maximal $\text{Hom}_{\Lambda}(E, C) = I(C)$ est un idéal bilatère maximal.

Soit I un idéal bilatère maximal de $L(E)$. Il contient le radical de Jacobson de $L(E)$ sinon on aurait $I + r = L(E)$, il existerait donc $u \in r$ tel que $1 + u \in I$. Or, $1 + u$ est inversible. A fortiori I contient $\text{Hom}_{\Lambda}(E, mE)$.

Remarquons que I est engendré par un nombre fini d'éléments u_1, \dots, u_p sur Λ . On en déduit que $\mathcal{L}(I) = u_1(E) + \dots + u_p(E)$. Soit

$$\bar{I} = I / \text{Hom}_{\Lambda}(E, mE)$$

et posons pour simplifier

$$\mathcal{L}(I) = C, \quad \bar{u}_1(\bar{E}) + \dots + \bar{u}_p(\bar{E}) = \bar{C}.$$

Soit I^* l'idéal à droite engendré par \bar{I} dans $L(\bar{E})$, $I^* = \bar{I}L(\bar{E})$. En tant qu'idéal I^* admet la base $\bar{u}_1, \dots, \bar{u}_p$. Il en résulte que, si $u^* \in I^*$, $u^*(\bar{E}) \subset \bar{C}$. Il est bien connu, dans ces conditions, que $I^* = \text{Hom}_k(\bar{E}, \bar{C})$. Soit $R = \text{In}(L(E) \longrightarrow L(\bar{E}))$.

$I^* \cap R$ est donc l'ensemble des $\bar{u} \in R$ tels que $\bar{u}(\bar{E}) \subset \bar{C}$. C'est un idéal à droite de R mais c'est aussi un idéal à gauche d'après la définition de I^* .

$R/\bar{I} = L(E)/I$ est simple, donc deux possibilités :

$I^* \cap R = R$, ce qui implique $I^* = L(\bar{E})$, donc $\bar{C} = \bar{E}$ soit $E = C$,
ou, sinon, $I^* \cap R = \bar{I}$. Remarquons que $\mathcal{L}(\text{Hom}_{\Lambda}(E, mE)) = mE$ et que, par

suite, $mE \subset C$. Il y a équivalence entre $\bar{u} \in \bar{I}$ et $u \in I$; $\bar{u} \in \bar{I}$ implique $\bar{u}(E) \subset \bar{C}$, donc $u(E) \subset C$. Réciproquement $u(E) \subset C$ implique $\bar{u}(E) \subset \bar{C}$ donc $\bar{u} \in R \cap \text{Hom}_k(\bar{E}, \bar{C}) = R \cap I^* = \bar{I}$, donc $u \in I$. Nous verrons ultérieurement que l'on peut avoir $L(I) = C = E$. Remarquons que si C' est un sous-module caractéristique maximal contenant C , dans le cas $C \neq E$, $\text{Hom}_A(E, C) \subset \text{Hom}_A(E, C')$ d'où $I = \text{Hom}_A(E, C')$.

Réciproquement, soit C un sous-module caractéristique maximal et utilisons la suite exacte :

$$0 \longrightarrow \text{Hom}_A(E, C) \longrightarrow L(E) \longrightarrow L(\tilde{E}) \quad \text{où } \tilde{E} = E/C.$$

La somme de deux sous-modules caractéristiques est caractéristique. Il en résulte que tout sous-module caractéristique maximal C contient mE : sinon, on aurait $C + mE = E$, d'où $C = E$.

Si $u \notin I(C)$, considérons l'idéal bilatère engendré par u dans $L(E)$, i.e. l'ensemble des sommes finies $x_1 uy_1 + \dots + x_n uy_n$ où $x_i, y_i \in L(E)$. Le sous-module $\sum_{x_i \in L(E)} x_i u(E)$ associé à cet idéal est caractéristique et il ne contient pas C , car il contient $u(E)$; donc, $C + \sum_{x_i \in L(E)} x_i u(E) = E$. Nous noterons \tilde{a} ce que l'on obtient à partir de a par passage au quotient par C ou $\text{Hom}_A(E, C)$. Soit R l'image de $L(E)$ dans $L(\tilde{E})$. Il vient

$$\sum_{x_i \in \tilde{R}} \tilde{x}_i \tilde{u}(\tilde{E}) = \tilde{E}.$$

\tilde{R} est semi simple : \tilde{R} est artinien, il suffit de montrer qu'il n'y a pas de radical. Or celui-ci, \tilde{r} est nilpotent. Soit p un entier tel que $\tilde{r}^p = 0$ et $\tilde{r}^{p-1} \neq 0$. Prenons $\tilde{v} \in \tilde{r}^{p-1}$ et $\neq 0$. Si $\tilde{u} \in \tilde{r}$ est différent de zéro :

$$\tilde{v}(\tilde{E}) = \sum_{x_i} \tilde{v}x_i \tilde{u}(\tilde{E}) = 0, \text{ car } \tilde{v}x_i \tilde{u} \in \tilde{r}^p = 0 \text{ quel que soit } \tilde{x}_i \in \tilde{R}.$$

Ceci est contraire à l'hypothèse faite aux \tilde{v} . Donc, \tilde{R} est bien semi-simple. Soit alors \tilde{u} un idempotent dans le centre de \tilde{R} , on a $\tilde{u}(\tilde{E}) = \tilde{E}$ car la somme considérée ci-dessus se réduit au premier membre. On a alors

$$(1 - \tilde{u})(\tilde{E}) = (1 - \tilde{u})\tilde{u}(\tilde{E}) = 0, \text{ donc, } \tilde{u} = 1. \text{ Il s'ensuit que } \tilde{R} \text{ est simple.}$$

On peut aussi montrer que le centre de \tilde{R} est un corps : si $\tilde{u} \in$ centre $\tilde{u} \neq 0$, $\tilde{u}(\tilde{E}) = \tilde{E}$, donc \tilde{u} est inversible dans $L(\tilde{E})$, donc dans \tilde{R} (car l'inverse est un polynôme en \tilde{u} à coefficients dans k). Donc $\text{Hom}_A(E, C)$ est maximal.

Envisageons maintenant le cas où $\mathfrak{L}(I) = E$. Nous allons voir la complication apportée par la non-commutativité dans une question très classique.

Prenons pour A l'anneau de valuation discrète $k[[X]]$, pour E la somme directe des nombres triaux sur k , des nombres duaux sur k et de k . Il est immédiat que $R = \text{Im}(L(E) \rightarrow L(\bar{E}))$ est l'ensemble des matrices à coefficients dans k de la forme :

$$\begin{vmatrix} a_1 & 0 & 0 \\ a_2 & a_3 & 0 \\ a_4 & a_5 & a_6 \end{vmatrix}$$

Prenons pour I , dont l'image est \bar{I} obtenu en considérant les matrices telles que $a_3 = 0$. On vérifie, sans difficulté, que \bar{I} est un idéal bilatère maximal de R , que $\bar{I}L(\bar{E}) = L(\bar{E})\bar{I} = L(\bar{E})$; il s'ensuit que $L(I) = E$.

Le théorème d'Hamilton Cayley montre que $L(\bar{E})$ est entier sur R , ou si l'on préfère est un R -module de type fini (à droite ou à gauche). Il est clair que, dans le cas commutatif, une telle circonstance ne peut se produire. D'ailleurs la méthode du déterminant de Krull montre que si R est commutatif, ce phénomène ne peut se produire. Le lemme de Nakayama montre l'impossibilité également, si R est un anneau complètement primaire.

Remarquons que, dans l'exemple ci-dessus, on aurait pu prendre pour \bar{I} l'ensemble des matrices telles que $a_3 = a_5 = a_6 = 0$ sans changer le fait que $L(I) = E$. Ceci ne caractérise donc pas les idéaux bilatères maximaux. En compliquant légèrement l'exemple on pourrait montrer que plusieurs idéaux maximaux peuvent donner lieu au même phénomène.

8. Une remarque sur les termes suivants de la filtration.

On aurait pu espérer que pour i suffisamment grand, $L(E) \rightarrow L(E/m^i E)$ deviendrait surjectif. Il est probable que ceci est vrai si A est anneau de valuation discrète. Voici un contre-exemple simple dans le cas général.

Exemple déjà donné : $A = k[[X_1, X_2]]$ quotient du module libre $Ax_1 \oplus Ax_2$ par le sous-module $Ay_1 + Ay_2$ avec $y_1 = X_1 x_1$ et $y_2 = X_2^2 x_2$.

On vérifie que la matrice

$$g_1(\xi_1, \xi_2) = \xi_2^2 g_2(\xi_1, \xi_2) + \xi_1^{n-1} \\ \xi_1 g_3(\xi_1, \xi_2) + \xi_2^{n-1} g_4(\xi_1, \xi_2)$$

où g_1, g_2, g_3, g_4 sont des polynômes de degré convenable et où $\xi_1^{\alpha_1} \xi_2^{\alpha_2} = 0$, si $\alpha_1 + \alpha_2 = i$ définit effectivement un endomorphisme de $E/m^i E$, alors qu'un représentant dans $M_n(L)$ ne peut définir un endomorphisme de E .

BIBLIOGRAPHIE

- [1] AZUMAYA (Gorô). - On maximally central algebras, Nagoya math. J., t. 2, 1951, p. 119-150.
- [2] BATHO (Edward H.). - Non commutative semi-local and local rings, Duke math. J., t. 24, 1957, p. 163-172.
- [3] BOURBAKI (Nicolas). - Algèbre, Chap. 2 : algèbre linéaire, 2e éd. - Paris, Hermann, 1955 (Act. scient. et ind., 1032 = 1236 ; Eléments de Mathématique, 6).
- [4] BOURBAKI (Nicolas). - Algèbre, Chap. 3. - Paris, Hermann, 1948 (Act. scient. et ind., 1044 ; Eléments de Mathématique, 7).
- [5] BOURBAKI (Nicolas). - Algèbre, Chap. 6 et 7. - Paris, Hermann, 1952 (Act. scient. et ind., 1179 ; Eléments de Mathématique, 14).
- [6] BOURBAKI (Nicolas). - Algèbre, Chap. 8. - Paris, Hermann, 1958 (Act. scient. et ind., 1261 ; Eléments de Mathématique, 23).
- [7] JACOBSON (Nathan). - Structure of rings. - Providence, American mathematical Society, 1956 (Amer. math. Soc. Coll. Publ., 37).
- [8] KAPLANSKY (Irving). - Infinite abelian groups. - Ann Arbor, University of Michigan Press, 1954 (Univ. of Mich. Publ. Math., 2).
- [9] SAMUEL (Pierre). - Algèbre locale. - Paris, Gauthier-Villars, 1953. (Mém. Sc. math., fasc. 123).
- [10] SCHIFFMAN (Max). - The ring of automorphisms of an abelian group, Duke math. J., t. 6, 1940, p. 579-597.
- [11] SERRE (Jean-Pierre). - Géométrie algébrique et géométrie analytique, Ann. Inst. Fourier Grenoble, t. 6, 1955-56, p. 1-42.
- [12] WEYL (Hermann). - The classical groups, their invariants and representations. - Princeton, Princeton University Press, 1946 (Princeton math. Series, 1).