PUBLICATIONS MATHEMATIQUES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

ANNEE 1968/1969

MATHEMATIQUE (425
(Service des Publications - Bibliothèque)
FACULTE DES SCIENCES
91 - ORSAY (France)

P U B L I C A T I O N S M A T H E M A T I Q U E S D ' O R S A Y

S E M I N A I R E
D' ALGEBRE NON COMMUTATIVE
O R S A Y

Année 1968/1969

Mathématique. (425)
(Service des Publications - Bibliothèque)
Faculté des Sciences
91 - ORSAY (France)

Table des matières

-:-:-:-:-:-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 1 du 16 octobre 1968

-:-:-:-:-:-

S.A. AMITSUR

Identités dans les algèbres de matrices,
rédigé par R. SMADJA.

-:-:-:-:-:-

I. Identités d'une algèbre associative A :

Soit K un corps commutatif ; soient $X_1, X_2, \ldots$ des indéterminées non commutatives sur K . Considérons l'anneau libre $K[X_1, X_2, \ldots] = K[X]$, qui est une algèbre sur K .

Soit A une algèbre associative sur K .

Les identités de A sont des polynômes $p[X_1, \ldots, X_n] \neq 0$ à coefficients dans K , qui prennent la valeur zéro lorsqu'on remplace $X_1, \ldots, X_n$ par n éléments quelconques de A .

Exemple :

$[[X,Y]^2, Z]$ est une identité de $\mathcal{M}_2(K)$, qui est de degré cinq.

. XY et YX ont même polynôme caractéristique donc même trace : la trace de (XY - YX) est nulle. Le théorème de CAYLEY-HAMILTON appliqué à $[X,Y] = XY - YX$ fournit alors $[X,Y]^2 + 0 \times [X,Y] + \delta = 0$.

Donc, quels que soient X et Y dans $\mathcal{M}_2(K)$, $[X,Y]^2$ est dans le centre de $\mathcal{M}_2(K)$.

D'où $\forall X,Y,Z \in \mathcal{M}_2(K) \qquad (XY-YX)^2 Z - Z(XY-YX)^2 = 0$.

Le polynôme $[[X,Y]^2, Z]$ n'est pas identiquement nul, donc c'est une identité de $\mathcal{M}_2(K)$.

Si $p[X_1, \ldots, X_n]$ est une identité de A et $q_1, \ldots, q_n$ des polynômes de $K[X]$, alors $p[q_1[X], \ldots, q_n[X]]$ est aussi une identité de A, si ce n'est pas le polynôme nul.

. Soit k_i le degré de $q_i[X]$.

Si $X^i = (A^i_1, \ldots, A^i_{k_i})$ est un k-uplet d'éléments de A, $q_i[X^i]$ est aussi un élément X_i de A car A est une algèbre.

Alors $p[q_1[X^1], \ldots, q_n[X^n]] = p[X_1, \ldots, X_n] = 0$.

Donc p s'annule sur tous les éléments de A.

II. Identités d'une algèbre de matrices sur un corps commutatif K :

1) Théorème de DEHN :

Théorème 1 : L'algèbre de matrices $\mathcal{M}_n(K)$ possède une identité de degré $2n$:

$S_{2n}[X_1, \ldots, X_{2n}] = \sum_i \varepsilon(i) X_{i_1} \ldots X_{i_{2n}}$ où i est une permutation de $[1, \ldots, 2n]$ et $\varepsilon(i)$ est la signature de i.

Lemme : Le polynôme $S_k[X_1, \ldots, X_k] = \sum_i \varepsilon(i) X_{i_1} X_{i_2} \ldots X_{i_k}$ possède les propriétés suivantes :

1) Multilinéarité : $S_k[X_1, \ldots, \alpha X_i + \beta Y_i, \ldots X_k] = \alpha S_k[X_1, \ldots, X_i, \ldots, X_k] + \beta S_k X_1, \ldots, Y_i, \ldots X_k]$.

2) Antisymétrie : $S_k[X_1, \ldots, X_i, \ldots, X_j, \ldots, X_k] = 0$ si $X_i = X_j = X$ si $i \neq j$.

3) $S_k[X_1, \ldots, X_h, \ldots X_i, \ldots, X_j, \ldots, X_k] = \pm S_{k-2} X_1, \ldots, \hat{X}_k, \ldots, \hat{X}_i, \ldots, X_h X_i X_j, \ldots, X_k]$

+ termes où ne figurent pas $X_h X_i X_j$ ainsi groupés.

.. Seule la troisième propriété n'est pas évidente :

Permutons X_j avec chacun de ses suivants successivement jusqu'à ce que X_j se trouve à la place de X_k ; faisons de même avec X_i et X_h, pour les amener à la place de X_{k-1} et X_{k-2} respectivement. En procédant par cette suite de transpositions, on n'a pu affecter que le signe de S_k :

$$S_k[X_1,\dots,X_h,\dots,X_i,\dots,X_j,\dots,X_k] = \pm S_k[X_1,\dots,X_h,X_i,X_j] .$$

Les permutations σ de $[1,\dots,k]$ conservant groupés $(k-2)(k-1)(k)$ correspondent bijectivement aux permutations σ' de $[1,\dots,k-2]$; la parité de σ et σ' est la même car si k introduit p inversions, le groupement $(k-2)(k-1)(k)$ en introduit $3p = p+2p$ donc la parité est inchangée.

$S_k[X_1,\dots,X_h,X_i,X_j] = S_{k-2}[X_1,\dots,X_h,X_i,X_j]$ + termes où ne figurent pas $X_h X_i X_j$ ainsi groupés.

Le lemme est démontré en réunissant les deux égalités ci-dessus.

. Montrons alors que $A_i \in \mathcal{M}_n(K)$ $1 \leqslant i \leqslant 2n \Longrightarrow S_{2n}[A_1,\dots,A_{2n}] = 0$.

<u>1ère réduction</u> : Il suffit de le montrer lorsque les A_i sont de la forme

$$A_i = C_{\ell m} = \left(\begin{array}{c|c|c} 0 & & 0 \\ \hline & 1 & \\ \hline 0 & & 0 \end{array}\right) \begin{matrix} \\ \ell \\ \\ \end{matrix} \quad \overset{m}{} .$$

.. Cela résulte immédiatement de la multilinéarité.

Remarquons que la règle de calcul $C_{ij}C_{k\ell} = \delta_{jk}C_{i\ell}$ prouve qu'un élément $C_{\ell m}$ est soit un idempotent C_{mm}, soit de carré nul.

<u>2ème réduction</u> : Il suffit de montrer le théorème dans le cas où deux C_{ij} sont idempotents.

.. Montrons que si $S_{2n}[C_{i_1 j_1},\dots,C_{i_{2n} j_{2n}}]$ est nul lorsque deux C_{ij} sont idempotents, il en est de même lorsque l'on suppose seulement un C_{ij} idempotent. La démonstration est ensuite analogue pour passer d'un idempotent à aucun.

Considérons donc un polynôme $S_{2n}[C_{i_1 j_1}, \ldots, C_{i_{2n} j_{2n}}]$ où l'un des C_{ij} intervenant est un idempotent C_{hh}. Quitte à changer le signe de S_{2n} on peut supposer que C_{hh} est en première position : $S_{2n}[C_{hh}, C_{i_2 j_2}, \ldots, C_{i_{2n} j_{2n}}]$.

Si deux C_{ij} sont égaux, S_{2n} est nul et la démonstration est achevée. Sinon, il existe parmi les $C_{i_k j_k}$ un terme C_{ij} tel que $i \neq h$ et $j \neq h$.

En effet, les C_{ij} figurant dans S_{2n} et autres que C_{hh} sont au nombre de $(2n-1)$ et il n'y a que $(2n-2)$ termes tels que $i = h$ ou $j = h$.

$\left.\begin{matrix} C_{1h}, \ldots, C_{nh} \\ C_{h_1}, \ldots, C_{h_n} \end{matrix}\right\}$ $2n$ termes desquels il faut ôter deux fois C_{hh}.

Choisissons un tel C_{ij} et calculons $S_{2n}[C_{hh}, C_{ij} + C_{ii}, \ldots]$:

$$S_{2n}[C_{hh}, C_{ij} + C_{ii}, \ldots] = S_{2n}[C_{hh}, C_{ij}, \ldots] + S_{2n}[C_{hh}, C_{ii}, \ldots]$$

($S_{2n}[C_{hh}, C_{ii}, \ldots]$: terme nul car il y figure deux idempotents.)

D'après l'antisymétrie, $S_{2n}[C_{hh}, C_{i_2 j_2}, \ldots, C_{ij}, \ldots] = 0$

$$\iff S_{2n}[C_{hh}, C_{ij}, \ldots, C_{i_2 j_2}, \ldots] = 0 .$$

Montrer que $S_{2n}[C_{hh}, C_{ij}, \ldots]$ est nul revient, d'après le calcul ci-dessus, à montrer que $S_{2n}[C_{hh}, C_{ij} + C_{ii}, \ldots]$ est nul ; il est équivalent de multiplier à gauche et à droite par des éléments inversibles et de montrer la nullité de l'expression ainsi obtenue. $(1+C_{ij})(1-C_{ij}) = (1-C_{ij})(1+C_{ij}) = 1$, puisque $i \neq j$ (S_{2n} est supposé n'avoir que C_{hh} comme idempotent). Donc $(1+C_{ij})$ et $(1-C_{ij})$ sont inversibles.

$$(1+C_{ij}) S_{2n}[C_{hh}, C_{ij}+C_{ii}, \ldots] (1-C_{ij}) = S_{2n}[(1+C_{ij}) C_{hh} (1-C_{ij}),$$
$$(1+C_{ij})(C_{ij}+C_{ii})(1-C_{ij}), \ldots,$$
$$(1+C_{ij}) C_{i_k j_k} (1-C_{ij}), \ldots] .$$

(Cette égalité vient du fait que $(1+C_{ij})X_1 \ldots X_{2n}(1-C_{ij}) =$

$(1+C_{ij})X_1\underbrace{(1-C_{ij})(1+C_{ij})}_{1}X_2 \ldots \underbrace{(1-C_{ij})(1+C_{ij})}_{1}X_{2n}(1+C_{ij}) =$

$S_{2n}[C_{hh}, C_{ii}, \ldots, (1+C_{ij})C_{i_kj_k}(1-C_{ij}), \ldots]$.

(Pour le premier terme, la simplification a lieu car i et j sont différents de h , pour le second :

$(1+C_{ij})(C_{ij}+C_{ii})(1-C_{ij}) = (C_{ij}+C_{ii})(1-C_{ij}) = C_{ii}+C_{ij}-C_{ij} = C_{ii}) = 0$ car il y a deux idempotents.

D'après les assertions précédentes, ceci achève la démonstration de la deuxième réduction.

$S_{2n}[C_{i_1j_1},\ldots,C_{i_{2n}j_{2n}}]$ est une somme de produits du type $C_{\alpha_1\beta_1}\ldots C_{\alpha_{2n}\beta_{2n}}$.

Considérons un tel produit $C_{\alpha_1\beta_1}\ldots C_{\alpha_{2n}\beta_{2n}}$ et cherchons à quelle condition il est non nul. Notons $f(i)$ le nombre de fois qu'apparait l'indice i dans ce produit $f(i) = \text{card}\left\{k \mid \alpha_k = i \text{ ou } \beta_k = i\right\}$.

Puisqu'il y a deux indices par terme et 2n termes dans le produit, on a $\sum_{i=1}^{n} f(i) = 4n$. Pour que le produit soit non nul, il faut et il suffit que, à chaque fois qu'apparait un produit $C_{\alpha_k\beta_k}C_{\alpha_{k+1}\beta_{k+1}}$ on ait $\beta_k = \alpha_{k+1}$. Ceci prouve que, excepté éventuellement les deux extrêmes (termes) α_1 et β_{2n} , tous les indices interviennent un nombre pair de fois dans le produit. Selon que α_1 et β_{2n} sont égaux ou différents, il y a respectivement zéro ou deux termes qui interviennent un nombre impair de fois : $f(i)$ est impair pour zéro ou deux valeurs, pair pour les autres valeurs de i .

<u>3ème réduction</u> : On peut supposer que les valeurs $f(i)$ sont toutes supérieures ou égales à 3 .

.. Pour $n = 1$, on a $S_2 = XY-YX = 0$, donc le théorème est démontré.

Supposons donc $n > 1$. S_{2n} est alors formé de produits d'au moins quatre termes. Montrons, par récurrence sur n , que s'il existe i tel que $f(i) \leqslant 2$, S_{2n} est alors nul. On a déjà vu que S_2 est nul (quel que soit $f(i)$ d'ailleurs). Soit donc $n \geqslant 2$ et $S_{2(n-1)} \equiv 0$. L'indice i peut intervenir 0, 1 ou 2 fois.

Si l'indice i n'intervient pas :

$$S_{2n}[C_{i_1 j_1},\ldots,C_{i_{2n} j_{2n}}] = \sum_{\substack{m=1..2n \\ p=1..2n \\ q=1..2n}} (\text{termes contenant } C_{i_m j_m} C_{i_p j_p} C_{i_q j_q} \text{ ainsi groupés})$$

$$= \sum_{\text{idem}} \pm S_{2n-2}[C_{i_1 j_1},\ldots,C_{i_m j_m} C_{i_p j_p} C_{i_q j_q},\ldots,C_{i_{2n} j_{2n}}] .$$

La bijection canonique de $\mathcal{M}_{n-1}(K)$ sur les matrices de $\mathcal{M}_n(K)$ dont la $i$ème ligne et la $i$ème colonne sont nulles est un isomorphisme d'espace vectoriel qui conserve la structure multiplicative, donc c'est un isomorphisme d'algèbre.

On peut donc considérer ici que S_{2n-2} opère sur $2n-2$ éléments de $\mathcal{M}_{n-1}(K)$: dans ce cas l'étude de S_{2n} se ramène à celle de $S_{2(n-1)}$ qui est nul.

Si l'indice i intervient une fois :

Le coefficient où intervient i est soit C_{ij} soit C_{ki} ; les produits où ce coefficient intervient ne sont non nuls que s'ils sont de la forme :

C_{ij} ..... ou ..... C_{ki}

car si C_{ij} est multiplié à gauche (ou C_{ki} à droite) par $C_{\ell m}$, où ℓ et m sont différents de i , le produit est nul.

On peut n'étudier que le cas C_{ij} par symétrie :

$$S_{2n} = C_{ij} \sum_{m=j_1 \ldots j_{2n}} \pm C_{jm} \varepsilon(p) C_{p_1} \ldots C_{p_{2n-2}} = C_{ij} \sum_{m=j_1 \ldots j_{2n}} \pm C_{jm} S_{2(n-1)}$$

p = permutation de $[1,\ldots,\hat{i},\ldots,\hat{m},\ldots 2n]$

$$[C_{i_1 j_1},\ldots,\hat{C}_{ij},\ldots,\hat{C}_{jm},\ldots,C_{i_{2n} j_{2n}}] .$$

Dans ce cas encore, l'étude de S_{2n} se ramène à l'étude de $S_{2(n-1)}$ qui est nul.

Si l'indice i intervient deux fois :

Ce peut être sous l'une des trois formes $\left|\begin{array}{ll} C_{ii} & (1) \\ (C_{ij} \text{ et } C_{ik}) \text{ ou } (C_{ji} \text{ et } C_{ki}) & (2) \\ C_{ij} \text{ et } C_{ki} & (3) \end{array}\right.$

Forme (1) : C_{ii} intervient dans un produit d'au moins deux termes, donc est multiplié soit à gauche soit à droite, par un terme où l'indice i ne figure pas ; donc le produit est nul. Ainsi, tous les produits, dont S_{2n} est la somme, sont nuls.

Forme (2) : Le raisonnement étant symétrique, supposons que l'on soit dans le cas $\{C_{ij} \text{ et } C_{ik}\}$. L'un de ces deux termes ne figure pas en première position dans le produit ; il est donc multiplié à gauche par un terme du type C_{ℓ_m} où $m \neq i$; donc le produit est nul.

Forme (3) : D'après les considérations précédentes, les seuls produits a-priori non nuls, contenant C_{ij} et C_{ki}, sont du type :

$$C_{ij} \cdots\cdots C_{ki} \quad \text{ou} \quad C_{ki}C_{ij} \cdots\cdots\cdots$$

∴ Les produits du type $C_{ij} \cdots C_{ki}$, intervenant dans S_{2n}, ont pour somme

$$s = \sum_p \varepsilon(p) C_{ij}C_{ip_2jp_2} \cdots C_{ip_{2n-1}jp_{2n-1}}C_{ki}$$

où p est une permutation de $[1, \ldots, 2n]$ telle que $i(1)$ et $i(2n)$ soient fixés.

Cela revient, au signe près, à considérer les permutations de $[1, \ldots, 2n-2]$:

$$s = \pm C_{ij} \left(\sum_p \varepsilon(p)\, C_{ip_1jp_1} \cdots C_{ip_{2n-2}j_{2n-2}}\right) C_{ki}$$

$$= \pm C_{ij} \left(S_{2n-2}[C_{i_2j_2} \cdots C_{i_{2n-2}j_{2n-2}}]\right) C_{ki} .$$

Les matrices intervenant dans S_{2n-2} n'ont ni ligne i ni colonne i, donc l'étude est ramenée à celle de $S_{2(n-1)}$: s est nulle car $S_{2(n-1)}$ l'est.

. . Les produits du type $\ldots C_{ki}C_{ij} \ldots$, intervenant dans S_{2n}, ont pour somme

$$s' = \sum_{m} \text{(termes où } C_{ki}C_{ij}C_{jm} \text{ interviennent ainsi groupés)}$$

$$= \sum_{m, C_{jm} = C_{i_\ell j_\ell}} \pm S_{2n-2}[C_{i_1 j_1}, \ldots, C_{k_m}, \ldots, C_{i_{2n-2} j_{2n-2}}] \text{ d'après le lemme.}$$

On est donc encore une fois ramené à l'étude de $S_{2(n-1)}$, puisque les matrices intervenant ne contiennent pas la colonne i ni la ligne i. Donc $s' = 0$.

∴ Alors $S_{2n} = s + s'$ est aussi nul dans ce cas.

<u>4ème réduction</u> : Si $C_{i_1 i_1}$ et $C_{i_2 i_2}$ sont les deux idempotents, on peut supposer $f(i_1) \geqslant 5$ et $f(i_2) \geqslant 5$.

.. Soit C_{ii} un idempotent, étudions les cas $f(i) = 3$ et $f(i) = 4$.

Si $f(i) = 3$: dans le produit figurent C_{ii} et C_{ij} (ou C_{ii} et C_{ki}, ce qui revient au même) donc les produits non nuls sont ceux où figure le groupement $C_{ii}C_{ij}$. On est ramené, par un calcul analogue à ceux faits ci-dessus à $S_{2(n-1)}[\ldots]$ qui est nul.

Si $f(i) = 4$: deux possibilités s'offrent pour la répartition des indices

C_{ii} , C_{ij}, C_{ki} (1)

C_{ii} , C_{ij}, C_{ik} (ou la possibilité symétrique C_{ii}, C_{ji}, C_{ki}) (2)

Remarquons qu'en effet $C_{ii}C_{ii}$ fournit un produit nul.

Les produits non nuls sont alors de l'un des types suivants :

$C_{ii}C_{ij}$ M C_{ki} (1a)

où $M = C_{i_3 j_3} \ldots C_{i_{2n-1} j_{2n-1}}$

où $C_{i_2 j_2} \ldots C_{i_{2n-2} j_{2n-2}}$

C_{ij} M C_{ki} C_{ii} (1b)

$\ldots C_{ki}C_{ii}C_{ij} \ldots\ldots$ (2) .

∴ Pour la répartition (1) , associons le produit (1a) et le produit (1b)

obtenus pour la même valeur de M ; ils interviennent tous les deux dans S_{2n}, et sont affectés de signes opposés puisque le passage de la substitution $(\ell_1, \ell_2, \ldots, \ell_n)$ à $(\ell_2, \ldots, \ell_n, \ell_1)$ s'effectue au moyen de $(2n-1)$ transpositions ; leur somme est donc nulle.

∴ Pour la répartition (2), on ne considère que les produits où figure le groupement $C_{ki}C_{ii}C_{ij}$, ce qui revient à calculer $S_{2(n-1)}[\ldots C_{kj}\ldots]$ qui est nul. Montrons alors que l'équation $\sum_{i=1}^{n} f(i) = 4n$ est impossible lorsque deux des valeurs $f(i)$ sont supérieures ou égales à 5, toutes les autres supérieures ou égales à 3, ces valeurs étant de plus assujetties à être toutes paires ou toutes paires sauf deux.

Valeurs toutes paires $\Longrightarrow \sum_{i=1}^{n} f(i) \geqslant 6 + 6 + 4 + 4 + \ldots + 4 = 4n + 4 > 4n$

Deux valeurs impaires $\Longrightarrow \sum_{i=1}^{n} f(i) \geqslant 5 + 5 + 4 + 4 + \ldots + 4 = 4n + 2$

ou $\geqslant 6 + 5 + 3 + 4 + \ldots + 4 = 4n + 2$

ou $\geqslant 6 + 6 + 3 + 3 + 4 + \ldots + 4 = 4n + 2$.

Ceci prouve que l'on se trouve nécessairement dans l'un des cas particuliers étudiés précédemment, donc que $S_{2n}[X_1, \ldots, X_{2n}]$ est nul pour tous les éléments X_i de $\mathcal{M}_n(K)$.

2) <u>Compléments</u> :

a) S_{2n} est une identité de degré minimal de : $\mathcal{M}_n(K)$:

<u>Lemme</u> : Soit A un anneau possédant une identité polynomiale de degré d, $\mathcal{R}$ son radical nilpotent. Alors, pour tout élément nilpotent a de A, $a^{[\frac{d}{2}]}$ est dans $\mathcal{R}$.

. Soit a un élément nilpotent de A, si a est dans $\mathcal{R}$, le lemme est démontré. Supposons donc que a ne soit pas dans $\mathcal{R}$ et notons n l'indice de a modulo $\mathcal{R}$, c'est-à-dire l'entier n tel que $a^n \notin \mathcal{R}$, $a^{n+1} \in \mathcal{R}$.

Le lemme équivaut à l'inégalité $n < [\frac{d}{2}]$.

Considérons les $(2n+1)$ sous-anneaux suivants de A :

$$(1)\begin{cases} A_{2j-1} = a^{n-j+1}Aa^{j-1} & \text{pour } j = 1, 2, \ldots, n+1 \\ A_{2j} = a^{n-j+1}Aa^{j} & \text{pour } j = 1, 2, \ldots, n \end{cases}$$

On a donc $A_1 = a^nA$, $A_2 = a^nAa$, $A_3 = a^{n-1}Aa$, ..., $A_{2n} = aAa^n$, $A_{2n+1} = Aa^n$.

Formons les produits $B_i = A_1.A_2, \ldots, A_i$, pour $i = 1, 2, \ldots, 2n+1$. De (1) , on déduit immédiatement :

$$(2)\begin{cases} B_{2j-1} = (a^nA)^{2j-1}\, a^{j-1} & \text{pour } j = 1, 2, \ldots, n+1 \\ B_{2j} = (a^nA)^{2j}\, a^{j} & \text{pour } j = 1, 2, \ldots, n \end{cases}$$

$s > t \Longrightarrow A_sA_t \subseteq Aa^{n+1}A$.

.. Désignons par $j_s = [\frac{s+1}{2}]$ et $j_t = [\frac{t+1}{2}]$ les indices permettant de construire A_s et A_t :

<u>1er cas</u> : $s = 2j$

$s = 2j \Longrightarrow t \leqslant 2j-1 \Longrightarrow j_t \leqslant j \Longrightarrow j-j_t \geqslant 0$ ⇓

$A_sA_t = (a^{n-j+1}Aa^j)(a^{n-j_t+1}Aa^{\ell}) \subseteq Aa^{n+j-j_t+1}A \subseteq Aa^{n+1}A$.

<u>2ème cas</u> : $s = 2j-1$

$s = 2j-1 \Longrightarrow t \leqslant 2j-2 \Longrightarrow j_t \leqslant j-1 \Longrightarrow j-t_t+1 \geqslant 0$ ⇓

$A_sA_t = (a^{n-j+1}Aa^{j-1})(a^{n-j_t+1}Aa^{\ell}) \subseteq Aa^{n+j-j_t-1+1}A \subseteq Aa^{n+1}A$

Ainsi, si r est un entier inférieur ou égal à $2n+1$ et $(i_1, \ldots, i_r)$ une substitution de $(1, \ldots, r)$ non égale à $(1, \ldots r)$, dans cette substitution figurent au moins deux indices consécutifs s et t tels que s soit supérieur à t , donc

$$r \leqslant 2n+1 \ , (i_1, \ldots, i_r) \neq (1, \ldots r) \Longrightarrow A_{i_1}.A_{i_2}, \ldots, A_{i_r} \subseteq Aa^{n+1}A \ .$$

Ecrivons l'identité donnée sous la forme

$$\alpha X_1 \ldots X_d = \sum_{\substack{i \in \sigma d \\ i \neq \text{identité}}} \alpha_i X_{i_1} \ldots X_{id} \qquad \begin{matrix} \alpha \in K \\ \alpha_i \in K \end{matrix} \qquad (3) \ .$$

.. Montrons que l'on peut ramener à cette forme toute identité polynomiale de degré d :

Si $P[X_1,\ldots,X_k]$ n'est pas linéaire en l'une des variables (X_1 par exemple, intervenant à un degré n strictement supérieur à un), la transformation

$$Q[X'_1,X''_1,X_2,\ldots,X_k] = P[X'_1 + X''_1, X_2, \ldots, X_k] - P[X'_1, X_2, \ldots, X_k] - P[X''_1, X_2, \ldots, X_k]$$

fournit une identité Q , dont le degré en X'_1 et X''_1 est au plus n-1 (car les termes en X'^n_1 et X''^n_1 ont disparu), et dont le degré total n'est pas plus élevé que celui de P .

Si une indéterminée (X_1 par exemple) n'apparaît dans aucun monôme dont le coefficient est non nul, la somme des autres monômes $R[X_2, \ldots, X_k]$ est évidemment une identité de A .

Si l'identité P n'est pas homogène , chacune de ses parties homogènes est aussi une identité car le polynôme en t obtenu en multipliant chaque indéterminée par t doit être identiquement nul.

Ces trois remarques, appliquées successivement à une identité $P[X_1,\ldots,X_k]$ de A , permettent de ramener cette dernière à la forme (3) indiquée plus haut, sous laquelle on peut donc supposer donnée l'identité considérée dans l'énoncé du lemme.

Raisonnons par l'absurde, en supposant n supérieur ou égal à $[\frac{\alpha}{2}]$:

$$n \geqslant [\tfrac{d}{2}] \Longrightarrow n \geqslant \frac{d-1}{2} \Longleftrightarrow d \leqslant 2n+1 \ .$$

On peut alors remplacer r par d dans les calculs de la page précédente :

$\forall (i_1,\ldots,i_d) \neq (1,\ldots d)$, on a $A_{i_1},\ldots,A_{i_d} \subseteq Aa^{n+1}A$.

Le membre de droite de (3) est alors somme d'éléments de $Aa^{n+1}A$ donc est élément de $Aa^{n+1}A$. Le membre de gauche l'est donc aussi :

$$\alpha A_1 A_2 \ldots A_d = \alpha B_d \subseteq Aa^{n+1}A \ .$$

Des formules (2) on déduit alors

$\alpha B_d = \alpha(a^nA)^{2q-1}a^{q-1} \subseteq Aa^{n+1}A$ si $d = 2q-1$

$\alpha B_d = \alpha(a^nA)^{2q}\ a^q \subseteq Aa^{n+1}A$ si $d = 2q$

Multiplions à droite la première de ces inclusions par $(a^{n-q+1}Aa^nA)$, la seconde par $(a^{n-q}A)$; compte tenu de ce que l'on a $\alpha a^nA = a^nA$, on obtient dans les deux cas de parité de d

$(a^nA)^{2q+1} \subseteq Aa^{n+1}A$.

n étant choisi comme il a été indiqué au début de la démonstration, c'est-à-dire tel que $a^n \notin \mathcal{R}$ $a^{n+1} \in \mathcal{R}$, on a :

$a^{n+1} \in \mathcal{R} \Longrightarrow Aa^{n+1}A$ idéal nilpotent $\Longrightarrow (Aa^{n+1}A)^t = 0$ pour un entier t

$\Longrightarrow \exists t \in \mathbb{N} \quad (a^nA)^{t(2q+1)} = 0$

$\Longrightarrow a^n \in \mathcal{R}$: absurde .

La contradiction vient de ce que l'on a supposé $n \geqslant [\frac{q}{2}]$.

Donc, nécessairement, n est inférieur strictement à $[\frac{d}{2}]$, ce qui démontre le lemme.

Théorème 2 : Les identités de $\mathcal{M}_n(K)$ sont de degré supérieur ou égal à $2n$.

. Dans $\mathcal{M}_n(K)$, il existe des éléments nilpotents d'ordre n dont la puissance $(n-1)$ème est non nulle (la matrice de JORDAN

$$\left(J = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix}\right) \quad \text{par exemple).}$$

Le radical de $\mathcal{M}_n(K)$ étant nul, on doit avoir :

$J^{[\frac{d}{2}]} = 0$ et $J^{n+1} \neq 0$.

Ceci prouve que l'on a nécessairement $n \leqslant [\frac{d}{2}]$ donc $d \geqslant 2n$.

Corollaire : S_{2n} est une identité de degré minimum de $\mathcal{M}_n(K)$.

. En effet, le degré de S_{2n} est exactement $2n$.

b) S_{2n} est l'identité minimale de $\mathcal{M}_n(K)$.

Théorème 3 : Toute identité de degré minimal de $\mathcal{M}_n(K)$ est, à un scalaire multiplicatif près, égale à S_{2n} .

. Comme on l'a vu précédemment, toute identité de degré minimal de $\mathcal{M}_n(K)$ est de degré $2n$ et peut se mettre sous la forme :

$$(1) \qquad \sum_{i \in \sigma_{2n}} \alpha_i X_{i_1} \dots X_{i_{2n}} = 0 \ .$$

Comparons deux monômes de cette identité qui, mis à part leur coefficient, ne diffèrent que par une transposition de deux indéterminées consécutives : on peut toujours se ramener au cas :

$$(2) \begin{cases} \alpha X_1 \dots X_{r-1} X_r X_{r+1} X_{r+2} \dots X_{2n} \\ \beta X_1 \dots X_{r-1} X_{r+1} X_r X_{r+2} \dots X_{2n} \end{cases} .$$

1er cas : $r = 2i-1$

Ecrivons que (1) est une identité, pour la spécialisation suivante des variables:

$$\left.\begin{array}{l} X_{2j-1} = C_{j,j} \\ X_{2j} = C_{j,j+1} \end{array}\right\} \text{ si } j < i \qquad X_{2i-1} = X_{2i} = C_{ii} \qquad \text{si } j > i \begin{cases} X_{2j-1} = C_{j-1,j} \\ X_{2j} = C_{j,j} \end{cases}$$

Pour ce choix, les seuls monômes non nuls de (1) sont les deux monômes (2).

Leur somme vaut $\alpha C_{1,n} + \beta C_{1,n}$. Donc $(\alpha+\beta)C_{1,n} = 0 \Longrightarrow \alpha + \beta = 0$.

2ème cas : $r = 2i$

Considérons la spécialisation :

$$\left.\begin{array}{l} X_{2j-1} = C_{j,j+1} \\ X_{2j} = C_{j+1,j+1} \end{array}\right\} j < i \qquad \begin{array}{l} X_{2i-1} = C_{i,i+1} \\ X_{2i} = C_{i+1,i+1} \end{array}$$

$$\left.\begin{array}{l} X_{2j-1} = C_{j,j} \\ X_{2j} = C_{j,j+1} \end{array}\right\} i < j \leq n-1 \qquad \begin{array}{l} X_{2n-1} = C_{m,n} \\ X_{2n} = C_{n,1} \end{array}$$

Dans ce cas, la somme (1) ne se réduit pas aux deux monômes étudiés, car les permutations cycliques de $[1,\ldots,n]$ fournissent des monômes a-priori non nuls.

Toutefois, le terme $\alpha+\beta$ peut être caractérisé comme étant le coefficient de $C_{1,1}$ dans la somme, donc $\alpha+\beta = 0$.

Les deux cas précédents permettent d'affirmer que si (i) et (j) sont deux substitutions ne diffèrent que par une transposition de deux termes consécutifs, les monômes intéressant dans l'identité donnée, qui leur sont relatifs, sont affectés de coefficients opposés.

Considérons alors un terme quelconque $\alpha_i X_{i_1} \ldots X_{i_{2n}}$ de l'identité (1) : comme toute permutation (i) est déduite de la permutation identique par une suite de transpositions successives de termes adjacents (la parité étant celle de (i)) , on déduit du calcul précédent que $\alpha_i = \varepsilon(i)\alpha$.

Donc $\sum_{(i)} \alpha_i X_{i_1} \ldots X_{i_{2n}} = \alpha\, S_{2n}[X]$.

c) Relations entre les idéaux d'identités :

Notons Σ_n l'idéal de $K[X_1,X_2,\ldots]$ engendré par $S_{2n}[X_1,\ldots,X_{2n}]$

M_n l'idéal de $K[X_1,X_2,\ldots]$ constitué de toutes les identités de $\mathcal{M}_n(K)$.

Pour tout n , on a $\Sigma_n \subseteq M_n$.

Proposition 1 : $\Sigma_1 = M_1$ si le corps K est infini.

Nous verrons au paragraphe suivant que, pour n différent de un, l'inclusion $\Sigma_n \subset M_n$ est stricte.

. $\Sigma_1 = \{XY - YX\}$.

Soit $P[X_1,\ldots,X_m] = 0$ une identité de $\mathcal{M}_n(K)$. Transformons ce polynôme en utilisant le fait que pour tout i $X_1X_i = X_iX_1$.

X_1 commute avec toutes les variables (et avec les scalaires) donc on peut écrire :

$$P[X_1,\ldots,X_m] = f_0[X_2,\ldots,X_m]X_1^k + f_1[X_2,\ldots,X_m]X_1^{k-1} + \ldots + f_k[X_2,\ldots,X_m] .$$

Puisque $P[X_1,\ldots,X_m]$ est une identité de $\mathcal{M}_n(K)$, il s'annule en particulier lorsque l'on fixe $X_1 = 0$; donc $f_k[X_2,\ldots,X_m] = 0$.

Au lieu de prendre $X_1 = 0$, prenons maintenant X_1 inversible : $P[X_1,\ldots,X_n]X_1^{-1}$ est aussi une identité de $\mathcal{M}_n(K)$, etc... D'où $f_0[X_2,\ldots,X_m] = \ldots = f_k[X_2,\ldots,X_m] = 0$.

L'identité donnée P se décompose donc en identités où ne figure plus X_1 .

On peut recommencer l'opération avec $X_2, X_3, \ldots$ etc, donc on voit que P se ramène à un polynôme nul. Donc $XY-YX = 0$ est la seule identité de $\mathcal{M}_1(K)$.

Proposition 2 : Pour tout n supérieur ou égal à un, on a $M_{n+1} \subsetneq M_n$.

. L'inclusion au sens large est évidente car si un polynôme s'annule sur toutes les matrices de $\mathcal{M}_{n+1}(K)$, il s'annule en particulier sur celles de ces matrices qui ont leur première ligne et leur première colonne nulles (sous-algèbre isomorphe à $\mathcal{M}_n(K)$).

L'inclusion stricte vient de ce que S_{2n} est une identité de $\mathcal{M}_n(K)$ mais ne peut être une des identités de $\mathcal{M}_{n+1}(K)$ puisque ces dernières ont un degré supérieur ou égal à $(2n+2)$.

3) Quelques méthodes pour obtenir des identités d'un anneau de matrices :

a) Première méthode pour obtenir des identités de $\mathcal{M}_n(K)$:

Le théorème de CAYLEY-HAMILTON prouve que toute matrice $n \times n$ est solution d'un polynôme de degré n

$$X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n = 0 \qquad \alpha_i \in K .$$

C'est-à-dire que X^n est combinaison linéaire de $1, X, \ldots, X^{n-1}$:

$$X^n = -\sum_{i=1}^{n-1} \alpha_i X^{n-i} .$$

Considérons, pour X et Y éléments quelconques de $\mathcal{M}_n(K)$, le polynôme :

$$S_{n+1}[Y,YX,YX^2,\ldots,YX^n] = \sum_{i \in \sigma_{n+1}} \varepsilon(i) YX^{i_0} YX^{i_1} \ldots X^{i_n} .$$

Ce polynôme est identiquement nul sur $\mathcal{M}_n(K)$ puisque YX^n est combinaison linéaire de $Y,\ldots,YX^{n-1}$ $\left(YX^n = -\sum_{i=1}^{n-1} \alpha_i X^{n-i}\right)$ et que S_{n+1} est antisymétrique.

b) Application :

Proposition 3 : Pour n supérieur ou égal à deux, on a $\Sigma_n \not\subset M_n$.

. D'après le (a), il suffit de montrer que l'on a

$$S_{n+1}[Y,YX,\ldots,YX^n] \notin \left\{S_{2n}[X_1,\ldots,X_{2n}]\right\} .$$

Supposons que l'on ait : $S_{n+1}[Y,YX,\ldots,YX^n] = \Sigma\, u[X_1,\ldots,X_k] S_{2n}[X_1,\ldots,X_{2n}]$

$$v[X_1,\ldots,X_k] .$$

Ceci est une égalité dans l'anneau libre $K[X_1,X_2,\ldots]$ donc, si, dans le membre de droite, intervenaient des variables autres que X et Y, l'égalité aurait encore lieu en donnant à ces variables la valeur zéro (ce qui n'affecte pas le premier membre).

On peut donc se ramener, dans tous les cas, à une égalité du type :

$$S_{n+1}[Y,YX,\ldots,YX^n] = \sum_i u_i[X,Y] S_{2n}^{(i)}[X_1,\ldots,X_{2n}] v_i[X,Y]$$

où les éléments X_i sont des sommes de produits de puissances de X et de puissances de Y. D'après la linéarité de S_{2n}, on peut d'ailleurs supposer que $X_1,\ldots,X_{2n}$ sont des monômes (et non nécessairement des polynômes) en X et Y.

$S_{n+1}[Y,YX,\ldots,YX^n]$ est une somme de monômes de degré $\begin{cases} (n+1) \text{ en } Y \\ 1 + \ldots + n = \dfrac{n(n+1)}{2} \text{ en } X . \end{cases}$

Si l'on remplace Y par TY, on obtient au second membre un polynôme en t, dont seul le coefficient de t^{n+1} est égal à $S_{n+1}[Y,YX,\ldots,YX^n]$, (qui est le

coefficient de t^{n+1} dans le premier membre), et les autres nuls. On peut donc supposer le second membre homogène de degré $(n+1)$ en Y ; de même, on peut le supposer homogène de degré $\frac{n(n+1)}{2}$ en Y .

Le monôme $\pm\, YX^nYX^{n-1}\ldots YXY$ doit apparaître au second membre. Soit $u[X,Y]S_{2n}[X_1,\ldots,X_{2n}]v[X,Y]$ le terme dans lequel il apparaît. Ce terme est non nul, donc les $2n$ éléments $X_1,\ldots,X_{2n}$ doivent être tous différents.

1. Si Y n'intervient que dans n de ces éléments au plus, les autres éléments X_k sont alors des puissances de X , toutes différentes, au nombre de n au moins, et dont la somme des exposants est $\frac{n(n+1)}{2}$ au plus (au plus, car X peut intervenir dans u et v) .

La puissance zéro ne peut intervenir puisque S_{2n} est non nul.

.. Montrons en effet que $S_{2n}[X_1,\ldots,X_{2n}]$ est nul si $X_1 = 1$ (on peut se limiter à X_1 d'après l'antisymétrie).

On obtient toutes les permutations de $[1,\ldots 2n]$ en fixant d'abord la valeur de l'image de 1 , puis en faisant opérer sur $[2,\ldots,2n]$ l'ensemble des permutations de $(2n-1)$ éléments :

L'image de $\mathfrak{S}_{2n}$ est

$$\Big\{\big\{1,\sigma(2),\ldots,\sigma(2n)\big\}_{\sigma\in\mathfrak{S}_{2n-1}} \cup \big\{\sigma(2),1,\sigma(3),\ldots,\sigma(2n)\big\}_{\sigma\in\mathfrak{S}_{2n-1}} \cup \ldots \cup \big\{\sigma(2),\ldots,\sigma(2n),1\big\}_{\sigma\in\mathfrak{S}_{2n-1}}\Big\}$$

Lorsque l'on groupe les $2n$ termes correspondant à une même permutation $\sigma\in\mathfrak{S}_{2n-1}$, on obtient $2n$ fois le monôme $X_{\sigma(2)}\ldots X_{\sigma(2n)}$, affecté n fois du signe plus et n fois du signe moins (ci-dessus, le signe change car il y a une transposition, entre chaque symbole $\cup$). La somme est donc nulle pour chaque permutation σ . La somme

des monômes correspondant à toutes les permutations σ de $\mathfrak{S}_{2n-1}$, somme qui est égale à S_{2n}, est alors aussi nulle.

Donc il intervient au moins n puissances de X, toutes d'exposant supérieur ou égal à un. Comme la somme des exposants doit être au plus égale à $\frac{n(n+1)}{2}$, ces puissances de X sont $X, X^2, \ldots, X^n$ et sont exactement au nombre de n ; de plus X n'apparaît pas dans les autres termes X_k qui sont donc simplement des puissances de Y. Or ces termes sont au nombre de n, tous différents, et tels que la somme de leurs degrés (en Y) soit au plus (n+1), c'est impossible.

2. Donc Y doit apparaître dans (n+1) des termes $X_1, \ldots, X_{2n}$.

Dans ces (n+1) termes, Y apparait chaque fois à la puissance un (car le degré total en Y est au plus (n+1). Comme tous ces termes doivent être différents, ils sont nécessairement de la forme $X_k = X^i Y X^j$, avec (n+1) couples (i,j) différents.

Parmi ces couples (i,j), on ne peut obtenir qu'une fois au plus les couples (0,0), (0,1), (1,0), donc dans le produit des (n+1) termes X_k, X figure avec un degré au moins égal à $0 + 1 + 1 + 2(n-2) = 2n-2$.

Les (n-1) termes où ne figure pas Y sont (n-1) puissances différentes, non nulles, de X, donc la somme de leurs exposants est supérieure ou égale à $\frac{n(n-1)}{2}$.

Si $n > 2$: le degré en X est au moins $\frac{n(n-1)}{2} + 2n-2 > \frac{n(n-1)}{2} + n = \frac{n(n-1)}{2}$: absurde.

Si $n = 2$: dans le cas limite où les trois couples (0,0), (1,0) interviennent effectivement, on a à considérer $S_4[Y,YX,XY,X]$.

On ne peut rien déduire de l'étude globale des degrés, et a priori on pourrait fort bien avoir

$S_3[Y,YX,YX^2] = \lambda S_4[Y,YX,XY,X]$.

Mais, dans le premier membre, il n'existe pas de terme en Y^3

(Y × Y × Y consécutifs) alors que le second membre contient le monôme $\pm (XY)Y(YX)X$.

Le résultat est donc démontré pour tout n supérieur à un .

c) Deuxième méthode pour obtenir des identités de $\mathcal{M}_n(K)$:

$$S_n[Y,YX,\ldots,YX^{n-2},YX^n] = S_n[Y,YX,\ldots,YX^{n-2},-\sum_{i=0}^{n-1}\alpha_i YX^i$$

. en appliquant à X le théorème de CAYLEY-HAMILTON.

$$= S_n[Y,YX,\ldots,YX^{n-2}, -\alpha_{n-1} YX^{n-1}]$$

. d'après l'antisymétrie

$$S_n[Y,YX,\ldots,YX^{n-1},YX^n] = -\alpha_{n-1} \cdot S_n[Y,YX,\ldots,YX^{n-2},YX^{n-1}]$$

Terme dépendant de Y ; terme ne dépendant que de X ; terme dépendant de Y

Formons alors le polynôme :

$$S = S_n[Y,YX,\ldots,YX^{n-2},YX^n]Z\, S_n[Y,YX,\ldots,YX^{n-2},YX^{n-1}] - S_n[Y,\ldots,YX^{n-2},YX^{n-1}]Z\, S_n[Y,\ldots,YX^{n-1},YX^n] .$$

Ce polynôme est identiquement nul sur $\mathcal{M}_n(K)$ puisque α_{n-1} commute avec tous les termes. Ce n'est pas le polynôme nul car tous les termes situés avant le signe moins ne sont pas nuls, donc il existe au moins un terme de la forme PZQ où P contient X^n , qui soit non nul ; un tel terme n'a pas son pareil après le signe moins donc il figure dans S . On a donc bien une identité de $\mathcal{M}_n(K)$.

III. Remarques :

Si A est une algèbre de dimension finie sur le corps commutatif K , A satisfait à une identité de degré $d \leqslant ([A : K] + 1)$.

. Soit $k = [A : K]$. k+1 éléments $X_1,\ldots,X_{k+1}$ de A sont toujours linéairement dépendants, donc $S_{k+1}[X_1,\ldots,X_{k+1}] \equiv 0$, dans A .

Cette majoration est trop forte : pour un anneau de matrices par exemple, on obtient (n^2+1) au lieu de 2n .

- BIBLIOGRAPHIE -

DEHN M. Über die Grundlagen der Projektiven Geometrie und Allgemeine Zahlsysteme. (Math. Annalen 85 (1922), 184-194).

LEVITZKI J. and AMITSUR S.A. Minimal identities for Algebras (Proc. Am. Math. Soc. 1950, 449-463.

-:-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-

Conférence n° 2 du 6 novembre 1968 par

C. PROCESI

Anneau A_{mn} des polynômes à m matrices n × n génériques sur un corps commutatif F

-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-

Conférence n° 3 du 13 novembre 1968 par

C. PROCESI

Géométrie algébrique construite à partir de l'anneau A_{mn} des polynômes à m matrices n x n génériques sur F

-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

RESULTATS COMPLEMENTAIRES SUR LES J-ANNEAUX

par M. DJABALI

-:-:-:-:-:-:-

Conférence n° 4

Ce travail fait suite à [2] . Nous y donnons des résultats complémentaires sur les J-anneaux, en particulier sur ceux qui vérifient les conditions F.2 et F.3 de [2] . Ceci nous amènera à retrouver en utilisant une approche un peu différente les résultats de COLBY et RUTTER sur les J-anneaux artiniens qui sont somme directe d'idéaux à gauche co-irréductibles (cf. [1]) .

I. ETUDE D'UN J-ANNEAU ISOTYPIQUE -

1) Rappels :

Soient A un J-anneau isotypique de dimension n et E l'enveloppe injective de A considéré comme A-module à gauche. L. LESIEUR et R.CROISOT ont montré dans [4] que E était un anneau simple. R.E. JOHNSON est arrivé au même résultat dans [3] . Rappelons rapidement la construction de [4] . Soient X_i , $1 \leqslant i \leqslant n$, n idéaux à gauche co-irréductibles dont la somme est directe. On appellera E_i une enveloppe injective de X_i . On aura alors $E = \oplus E_i$. Soit p_i l'endomorphisme de E projection de E sur E_i parallèlement à $E_i' = \underset{j}{\oplus} E_j$, $j \neq i$. Les E_i sont des

A-modules à gauche indécomposables et tout A homomorphisme non nul de E_i dans E est injectif. En particulier nous appellerons g_i un isomorphisme de E_i sur E_1 ; il en existe au moins un puisque nous supposons que A est isotypique. Dans la suite si f et g sont deux homomorphismes nous écrirons par convention : $fg = g_0 f$.

Dans ces conditions on munit E d'une structure d'anneau en montrant qu'il est isomorphe à $\underset{A}{\mathrm{Hom}}(E,E)$. En effet si $x \in E$, il existe un A homomorphisme et un seul de E dans E qui prolonge l'homomorphisme : $\lambda \longrightarrow \lambda x$, $\forall\, \lambda \in A$. Il en existe un puisque E est injectif et il est unique puisque A est à idéal singulier nul. Ceci dit, x étant donné dans E , nous appellerons γ_{ij} l'homomorphisme de E_i dans E_j défini par :

$$\gamma_{ij}(\lambda) = p_j(\lambda x) \ , \ \forall\, \lambda \in E_i \ .$$

Appelons K le corps des A-homomorphismes de E_1 dans E_1. Nous faisons correspondre à γ_{ij} l'élément θ_{ij} de K défini par : $\theta_{ij} = g_i^{-1} \gamma_{ij} g_j$. Soit e_{ij} la matrice carrée d'ordre n dont tous les coefficients sont nuls, excepté celui de la i^e ligne et de la j^e colonne qui est égal à 1 . Alors l'application qui à x fait correspondre la matrice $\Sigma \theta_{ij} e_{ij}$ est un isomorphisme d'anneaux de E sur $M_n(K)$.

2) Etude des matrices associées aux éléments de A .

Soit R le radical du J-anneau A (cf [2]) . Nous supposerons que $R^p \neq 0$, $R^{p+1} = 0$. Si n_k est la dimension de R^k nous poserons : $m_k = \mathrm{codim}\, R^k = n - n_k$. R^p étant de dimension n_p il existe une somme directe de n_p idéaux co-irréductibles X_ℓ tels que : $X_\ell \cap R^p \neq 0$. Nous pouvons compléter les X_ℓ par $n - n_{p-1}$ idéaux co-irréducti-

bles X_ℓ, $n_p < \ell \leqslant n_{p-1}$, tels que $X_\ell \cap R^{p-1} \neq 0$ et tels que la somme $\sum_1^{n_{p-1}} X_\ell$ soit directe. En procédant ainsi de proche en proche nous pouvons construire une somme directe de n idéaux co-irréductibles tels que pour $1 \leqslant \ell \leqslant n_k$ on ait $X_\ell \cap R^k \neq 0$. Remarquons que puisque R^k est de dimension n_k, $(\sum_1^{n_k} X_\ell) \cap R^k$ est essentiel dans R^k et que l'on a donc : $(\sum_{n_k+1}^{n} X_\ell) \cap R^k = 0$.

Dans la suite nous poserons $i = n-\ell$ de sorte que l'on pourra écrire pour

$$m_k \leqslant i \leqslant n \quad , \quad X_i \cap R^k \neq 0 .$$

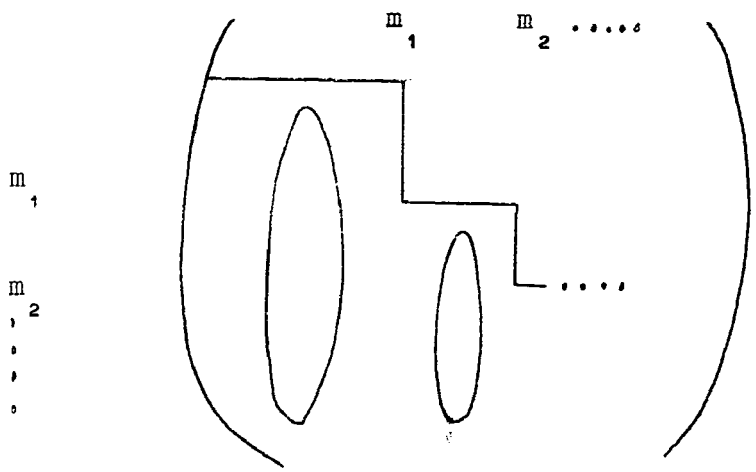
a) forme de la matrice associée à un élément de A. Soit $a \in A$. Construisons le représentant de a dans $M_n(K)$. Soit i avec $m_1 \leqslant i$. Supposons que $E_i a$ ne soit pas nul. L'homomorphisme $y \longrightarrow ya$ est un A-homomorphisme non nul de E_i dans $E_i a$. C'est donc un isomorphisme. Soit λ un élément non nul contenu dans $X_i \cap R$: alors $\lambda a \neq 0$. Mais R étant un idéal bilatère $\lambda a \in R$. On voit donc que $E_i a \cap R \neq 0$. Mais $E_i a$ étant un A-module co-irréductible (puisque isomorphe à E_i), $E_i a$ appartient à l'enveloppe injective de R. On peut donc écrire :

$$E_i a \subset \sum_{m_1}^{n} E_j .$$

Dans ces conditions γ_{ij} est nul pour : $1 \leqslant j < m_1$.

De même si nous calculons θ_{ij} pour $m_2 \leqslant i$, en utilisant maintenant le fait que R^2 est un idéal bilatère nous voyons que θ_{ij} est nul pour $1 \leqslant j < m_2$. Plus généralement on verra que pour $m_k \leqslant i$, $\theta_{ij} = 0$ pour $1 \leqslant j < m_k$.

Donc a peut être représenté par une matrice de la forme :



b) étude des matrices associées aux éléments de R . Soit a un élément de R . Considérons un indice i tel que $m_k \leqslant i$, c'est-à-dire tel que $X_i \cap R^k \neq 0$. Si x est un élément non nul appartenant à $X_i \cap R^k$, xa appartient à R^{k+1} . Pour les mêmes raisons que précédemment $E_i a$ est un idéal non nul co-irréductible qui appartient à l'enveloppe injective de R^{k+1} . On peut donc écrire

$$E_i a \subset \sum_{m_{k+1}}^{n} E_j \quad .$$

On en déduit que la matrice associée à a est telle que si $m_k \leqslant i$, $\gamma_{ij} = 0$ pour $j < m_k$.

Réciproquement un calcul direct montre que l'ensemble de toutes les matrices de la forme précédente forme un idéal nilpotent de A : cet idéal est donc le radical de A.

c) forme de la matrice associée à un élément de $0 : R^k$.

Si $a \in 0 : R^k$ on a : $R^k a = 0$ et donc $E_i a = 0$ pour tout i tel que $m_k \leqslant i$.

En effet on sait que $\overline{R^k}a = 0$ et à fortiori $(\sum_{m_k}^{n} E_j)a = 0$ puisque $\sum_{m_k}^{n} E_j$ est l'enveloppe injective de R^k .

La matrice associée à a sera donc telle que $\gamma_{ij} = 0$ si $m_k \leqslant i$. Réciproquement on voit facilement qu'une matrice de cette forme représente un élément de $0.\cdot R^k$.

2) Sur les J-anneaux qui vérifient les conditions F.2 et F.3 [2] .

Rappelons que dire que la condition F.2 est vérifiée revient à dire qu'il existe une somme directe d'idéaux à gauche co-irréductibles X_i qui contient un élément régulier. On peut donc écrire : $b_o = \Sigma u_i$, $u_i \in X_i$, b_o étant un élément régulier.

D'autre part nous poserons $A_k = A/0.\cdot R^k$ pour tout entier positif K . Lorsque tous les anneaux A_k qui ne sont pas nuls sont de dimension finie nous dirons que la condition F.3 est vérifiée.

Nous avons montré dans [2] que les X_i sont tels que la situation étudiée dans le paragraphe 1 est vérifiée, à savoir qu'on peut les numéroter de telle sorte que pour $m_k \leqslant i \leqslant n$, $X_i \cap R^k \neq 0$.

Dans la suite nous appellerons Ψ_k l'application canonique de A sur A_k . Nous supposerons toujours implicitement que A_k n'est pas nul.

Nous nous servirons des propositions suivantes qui sont démontrées dans [2] .

Proposition 2,1 : Soit X un idéal co-irréductible tel que $X \cap R^k \neq 0$, $X \cap R^{k+1} = 0$. Alors $X \cap R = X \cap (0 \cdot R^k)$.

Proposition 2,2 : Soit A un J-anneau que vérifie la condition F.2. Si Y est un idéal tel que : $Y \cap X_i \not\subset R$, $\forall i$, alors Y contient un élément régulier.

Démontrons maintenant d'autres résultats.

Lemme 2,1 : Soit b un élément régulier de A : alors $\Psi_k(b)$ est régulier dans A_k. Il est immédiat que $\Psi_k(b)$ est régulier à droite. Montrons qu'il l'est aussi à gauche. Si $b\lambda \in 0 \cdot R^k$, c'est-à-dire si $R^k b\lambda = 0$, une démonstration analogue à celle de la propriété 2,8 de [2] montre que $R^k \lambda = 0$.

Proposition 2,3 : Si A vérifie la condition F.2, A_k a un idéal singulier à gauche nul. Soit a un élément tel que $0 \cdot \Psi_k(a)$ soit essentiel dans A_k. Pour $m_k \leqslant i$, X_i n'appartient pas à $0 \cdot R^k$ (cf. [2])). Donc nous avons : $\Psi_k(X_i) \cap [0 \cdot \Psi_k(a)] \neq 0$. Cela veut dire qu'il existe un élément $v_i = \lambda_i u_i$, $v_i \in 0 \cdot R^k$ tel que $v_i a \in 0 \cdot R^k$, ou encore tel que $R^k v_i a = 0$. Puisque $R^k v_i \neq 0$, on a $0 \cdot a \cap X_i \neq 0$ et donc $X_i \subset 0 \cdot a$ (cf. [2]). Alors $u_i a = 0$. D'autre part pour $i < m_k$, $u_i a \subset 0 \cdot R^k$. Ceci nous permet d'affirmer que $b_o a \in 0 \cdot R^k$. D'après le lemme 2,1 nous en concluons que $a \in 0 \cdot R^k$. Donc $\Psi_k(a) = 0$.

Proposition 2,4 : Si A vérifie la condition F.2 A_k possède un idéal nilpotent maximum. Soit Y un idéal bilatère de A. Supposons qu'il existe un entier

s tel que $Y^s \subset 0.\cdot R^k$. On pourra écrire $Yb_0 = \oplus Yu_i$. On aura alors $(Yu_i)^s \subset 0.\cdot R^k$. Pour $m_k \leqslant i < m_{k+1}$ on aura donc $(Yu_i)^s \subset X_i \cap (0.\cdot R^k)$ et donc $(Yu_i)^s \subset R$. Ceci permet de conclure que $Yu_i \subset R$. Maintenant nous remarquons que si $K' \supset K$, $Y^s \subset 0.\cdot R^{k'}$ et donc que pour $m_{k'} \leqslant i < m_{k'+1}$, $Yu_i \subset R$. En définitive pour $m_k \leqslant i$ notre conclusion est que $Yu_i \subset R$. Si l'on remarque que pour $i < m_k$, $Yu_i \subset 0.\cdot R^k$, nous pouvons écrire :

$$(1) \qquad Yb_0 \subset R + 0.\cdot R^k \quad .$$

Réciproquement supposons qu'un idéal bilatère Y soit tel que $Yb_0 \subset R+0.\cdot R^k$. Nous supposerons que $R^p \neq 0$, $R^{p+1} = 0$. Nous voyons alors que : $(Yb_0)^{p+1-k} \subset R^{p+1-k} + 0.\cdot R^k$. Donc nous pouvons écrire que : $R^k(Yb_0)^{p+1-k} = 0$. Nous en déduirons aisèment que $R^k(Y)^{k+1-p} = 0$ (cf. la démonstration de la propriété 2,8 de [2]) .

La somme de tous les idéaux bilatères qui vérifient l'inclusion (1) est encore un idéal bilatère qui vérifie la même inclusion. Celui-ci a pour image canonique un idéal R_k de A_k qui est l'idéal nilpotent maximum de A_k .

Corollaire : $(R_k)^{p+1-k} = 0$.

Proposition 2,5 : Soit A un J-anneau qui vérifie les conditions F.2 et F.3 . Si b est un élément de A tel que $\Psi_k(b)$ soit régulier dans A_k , alors $Ab + 0.\cdot R^k$ contient un élément régulier de A .

Puisque A_k est de dimension finie, $A_k \Psi_k(b)$ est essentiel dans A_k . Donc

pour tout indice i tel que $m_k \leqslant i < m_{k+1}$ $A_k\, \Psi_k(b) \cap \Psi_k(X_i) \neq 0$. Si nous posons $Y_i = X_i \cap (Ab + 0.\cdot R^k)$ nous voyons que $Y_i \not\subset 0.\cdot R^k$. Alors $Y_i \not\subset R$ (prop. 2,1) et il en est de même Y_i^2 . Or un élément y appartenant à Y_i peut se mettre sous la forme $Y = \lambda b + \alpha$, $\alpha \in 0.\cdot R^k$. Mais α étant annulé par R^k est annulé par $\overline{R^k}$ et en particulier par Y_i qui appartient à $\overline{R^k}$ (cf. [2]) . On voit alors que $Y_i y \subset Ab$ et on en conclut que $Y_i^2 \subset Ab \cap X_i$. Maintenant si l'on considère un indice i tel que $m_{k'} \leqslant i < m_{k'+1}$, $k' \supset k$, on voit facilement que $\Psi_{k'}(b)$ est encore un élément régulier de $A_{k'}$ et le même raisonnement montrera qu'il existe un idéal non nilpotent contenu dans $Ab \cap X_i$. Enfin on remarque que pour $i < m_k$, $X_i \subset 0.\cdot R^k$. La proposition 2,2 appliquée à $Ab + 0.\cdot R^k$ donne le résultat.

Corollaire : A_k possède un anneau de fractions.

Nous savons déjà que A possède un anneau de fractions (cf. [2]) . Soit donc $\Psi_k(b)$ un élément régulier de A_k et soit $\Psi_k(a)$ un élément quelconque. Il existe un élément régulier de A_{b_1} contenu dans $Ab + 0.\cdot R^k$. Alors il existe un élément b' régulier dans A tel que $b'a = a_1 b_1$. Donc $b'a \in Ab + 0.\cdot R^k$. Il suffit de remarquer que $\Psi_k(b')$ est un élément régulier de A_k (lemme 2,1) et que l'on a :

$$\Psi_k(b')\, \Psi_k(a) \in A_k\, \Psi_k(b) \ .$$

Proposition 2,6 : Si A vérifie les conditions F.2 et F.3 , l'idéal $\Psi_k(X_i)$ est co-irréductible pour tout entier i tel que $m_k \leqslant i < m_{k+1}$.

Pour de tels indices on sait que $X_i \cap R = X_i \cap (0.\cdot R^k)$. La démonstration

découle du lemme 2,1 en utilisant un procédé analogue à celui utilisé dans la démonstration de la proportion 4,5 de [2] .

3) Etude de certains J-anneaux artiniens.

COLBY et RUTTER ont étudié dans [1] les J-anneaux artiniens qui sont somme directe d'idéaux co-irréductibles et ils ont donné un théorème de structure qui permet d'obtenir tous les anneaux de ce type. Remarquons qu'un tel anneau vérifie les conditions F.2 et F.3 . Justement nos résultats de [2] nous permettent d'énoncer le théorème suivant :

Théorème 3,1 : Pour qu'un anneau unitaire possède un anneau de fractions artinien, à idéal singulier nul il faut et il suffit que ce soit un J-anneau qui vérifie les conditions F.2 et F.3 .

Nous nous proposons de retrouver certains des résultats de COLBY et RUTTER en utilisant les résultats des paragraphes précédents. Il est facile de voir (cf. [1]) qu'on peut se limiter au cas où A est isotypique.

Nous étudions donc un J-anneau artinien isotypique somme directe d'idéaux co-irréductibles X_i . Nous savons que tout élément de A peut se représenter par une matrice du type défini dans le paragraphe 1 . Remarquons qu'alors A contient les matrices e_{ii} que nous pouvons identifier aux idempotents qui engendrent les idéaux X_i . En définitive nous pourrons écrire $A = \Sigma\, G_{ij} e_{ij}$, le groupe additif G_{ij} étant isomorphe au groupe additif $e_{ii} A e_{jj}$.

Proposition 3.1 : $0.^{\cdot}R$ est somme directe d'idéaux à gauche tous isomorphes. $0.^{\cdot}R$ est un $A_{/R}$ module et donc un A-module semi-simple. C'est pourquoi $0.^{\cdot}R$ est somme directe d'idéaux maximaux. Or si nous posons $X_{1i} = X_i \cap (0.^{\cdot}R)$, nous voyons tout de suite da $0.^{\cdot}R = \oplus X_{1i}$. Chacun des idéaux X_{1i} étant co-irréductible on en déduit qu'il est minimal. Nous voyons même que c'est l'unique idéal minimal contenu dans X_i . Remarquons maintenant que $X_{1i} = X_i$ pour $i \leqslant m_1$. Nous avons déjà appelé φ_i un A-isomorphisme de E_i sur E_1 . Dans ces conditions $\varphi_i^{-1}(X_1)$ est un A-module isomorphe à X_1 et donc un A-module minimal. On á alors $\varphi_i^{-1}(X_1) = X_{1i}$ puisque X_{1i} est l'unique idéal minimal contenu dans X_i . Nous voyons bien qu'il existe un A-isomorphisme de X_1 sur X_{1i} pour tout i .

Proposition 3.2 : Le corps des A-homomorphismes de X_1 dans X_1 est isomorphe à K . E_1 étant l'enveloppe injective de X_1 , tout A-homomorphisme de X_1 dans X_1 se prolonge d'une manière et d'une seule à un A-homomorphisme de E_1 dans E_1 (cf. [4]) .

Réciproquement X_1 étant un idéal minimal, une démonstration analogue à celle que nous venons de faire pour démontrer la proposition précédente montre que tout A-homomorphisme de E_1 dans E_1 induit un A-homomorphisme de X_1 dans X_1 .

Avant de continuer rappelons que $0.^{\cdot}R^k$ est constitué par les matrices telles que $\theta_{ij} = 0$ pour $i \geqslant m_k$. Dans ces conditions on peut identifier $\Psi_k(a)$ à la matrice obtenue en supprimant de celle qui représente a les m_k premières lignes et les m_k premières colonnes. Nous poserons $e^1_{ij} = \Psi_k(e_{ij})$. Nous pourrons identifier l'anneau A_k à l'anneau $\Sigma G_{ij} e^1_{ij}$ avec $i \geqslant m_k$, $j \geqslant m_k$. Appelons R_k le radical de A_k & la donnée

des G_{ij} pour $m_k \leqslant i < m_{k+}$ permettra de définir tous les éléments de $0.^{\cdot}R_k$. Posons alors : $X_i^1 = \Psi_k(X_i) \cap (0.^{\cdot}R_k)$. Nous remarquons déjà que $X_i^1 = \Psi_k(X_i)$ pour $m_k \leqslant i < m_{k+1}$. D'autre part nous pouvons écrire : $0.^{\cdot}R_k = \oplus X_i^1$.

Proposition 3,3 : les idéaux X_i^1 sont des idéaux minimaux pour $m_k \leqslant i < m_{k+1}$. On sait déjà que X_i^1 est co-irréductible (prop. 2,6) . Il est donc en plus minimal puisque $0.^{\cdot}R_k$ est semi-simple.

Proposition 3,4 : le groupe additif $\underset{A}{\mathrm{Hom}}\,(X_i,X_j)$ (resp. l'anneau $\underset{A}{\mathrm{Hom}}\,(X_i,X_i)$) est isomorphe au groupe additif $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_j^1)$ (resp. l'anneau $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_i^1)$) pour $i \geqslant m_k$ et $j \geqslant m_k$.

D'après ce que nous avons dit si $a = \Sigma\, G_{ij} e_{ij}$ nous pouvons identifier $\Psi_k(a)$ à la matrice $\Sigma\, G_{ij} e_{ij}^1$, $i \geqslant m_k$, $j \geqslant m_k$. Dans ces conditions ces deux groupes sont isomorphes au groupe G_{ij} .

Proposition 3,5 : si $m_k \leqslant i < m_{k+1}$, $\underset{A}{\mathrm{Hom}}\,(X_i,X_i)$ est un corps.

En effet puisque X_i^1 est un A_k module minimal, la propriété est vraie pour $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_i^1)$.

Corollaire : Pour $m_k \leqslant i < m_{k+1}$, G_{ii} est un sous-corps de K .

Lemme 3,1 : Soit Y^1 un idéal minimal de A_k . Alors si $m_k \leqslant i < m_{k+1}$, le groupe additif $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,Y^1)$ est ou bien nul, ou bien isomorphe à $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,Y_i^1)$.

Propriété 3,6 : si $m_k \leq i < m_{k+1}$ et $m_k \leq j$, le groupe $\underset{A}{\mathrm{Hom}}\,(X_i,X_j)$ est un espace vectoriel de dimension finie sur $\underset{A}{\mathrm{Hom}}\,(X_i,X_i)$.

En effet l'idéal X_j^1 est somme directe de modules minimaux. Ecrivons donc :

$$X_j^1 = \oplus\, X_{jk}^1 \ .$$

Dans ces conditions il est immédiat que $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_j^1)$ est somme directe des groupes $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_{jk}^1)$. D'après le lemme précédent les groupes $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_{jk}^1)$ sont ou nuls ou isomorphes à $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_i^1)$. Enfin il est immédiat que $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_i^1)$ est un espace vectoriel à droite sur $\underset{A_k}{\mathrm{Hom}}\,(X_i^1,X_j^1)$.

Corollaire : le groupe G_{ij} est un espace vectoriel à gauche sur G_{ii} de dimension finie. Le fait que G_{ij} soit maintenant un espace vectoriel à gauche résulte de la convention que nous avons adoptée pour la multiplication des homomorphismes.

Pour en arriver au théorème de structure tel qu'il est exposé dans [1] il suffit de grouper les idéaux X_i de manière convenable. Pour ceci on définit une relation d'équivalence : $X_i \sim X_j \iff$ il existe un isomorphisme de X_i sur X_j . On voit que si $X_i \cap R^k \neq 0$, $X_i \cap R^{k+1} = 0$ alors $X_j \cap R^k \neq 0$, $X_j \cap R^{k+1} = 0$. Il suffit de remarquer que K est le plus grand entier tel que $R^k X_i \neq 0$. Donc si nous considérons l'ensemble des X_i tels que $m_k \leq i < m_{k+1}$, nous pouvons en réaliser une partition en classes d'équivalence. Donc nous pouvons définir des entiers $m_{k,\ell}$ tels que :

$$m_k = m_{k,1} < m_{k,2} < \ldots < m_{k,\ell} < \ldots < m_{k+1} \ .$$

Alors pour $m_{k,\ell} \leqslant i < m_{k,\ell+1}$ les X_i seront tous isomorphes.

- BIBLIOGRAPHIE -

[1] R.R. COLKY et E.A. RUTTER : The structure of certain artinian rings with zero singular ideal (J. of Algebra 8, 1968, p. 156-164).

[2] M. DJABALI : Anneau de fractions d'un J-anneau (Can. J. Math., Vol. 20, 1968, p. 182-202).

[3] R.E. JOHNSON : Quotient rings of rings with zero singular ideal (Pacific J. Math., 11, 1961).

[4] L. LESIEUR et R. CROISOT : Coeur d'un module (J. Math. Pures et Appl., 9e série, 42, 1963, p. 367-407).

-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-

Conférence n° 5 du 27 novembre 1969 par

J. MENARD

- Anneaux réversifs -

-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Sur les Anneaux tels que tout A-module simple est injectif

Exposé de Guy RENAULT

rédigé par Marie-Christine GERMA

-:-:-:-:-

Conférence n° 6

Dans tout ce qui suit les anneaux seront des anneaux unitaires non nécessairement commutatifs et les modules seront des modules unitaires sur des anneaux unitaires.

Problème n° 1 (Faith).

(1) Caractériser les anneaux A tels que tout A-module simple est injectif.

Dans le cas où A est commutatif la réponse est donnée par le théorème de Kaplansky : les anneaux qui vérifient la propriété (1) sont les anneaux réguliers (au sens de Von Neumann).

Proposition 1 : (Rappel)

Un anneau A est régulier (V.N.) s'il vérifie l'une des conditions équivalentes suivantes :

(i) $\forall x \in A$, $\exists a \in A$ tel que $x = xax$

(ii) tout idéal à gauche monogène est facteur direct

(iii) tout idéal à gauche de type fini est facteur direct.

On trouvera d'autres caractérisations des anneaux réguliers dans [1]. Dans le cas non commutatif la réponse au problème 1 est donnée par le théorème de Villa mayor :

Proposition 2 :

A étant un anneau unitaire non nécessairement commutatif, les conditions suivantes sont équivalentes.

(1) Tout A-module à gauche simple est injectif

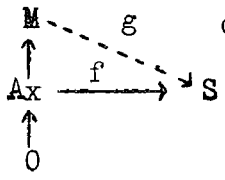
(2) Pour tout A-module à gauche M et tout sous-module N de M avec $N \neq M$, N est égal à l'intersection des sous-modules maximaux de M qui le contiennent.

(3) Tout idéal à gauche propre de A est égal à l'intersection des idéaux à gauche maximaux qui le contiennent.

On démontre les implications suivantes (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1) .

(1) $\Rightarrow$ (2). Par passage au quotient on se ramène au cas où $N=(o)$; avec l'hypothèse (1) on va montrer que si x est un élément non nul de M , il existe un sous-module maximal P de M qui ne contient pas x .

On considère le A-module simple $S = A/\mathfrak{P}$ [où $\mathfrak{P}$ est un idéal à gauche maximal de A contenant l'annulateur de x] et f un homomorphisme non nul de Ax dans S . S étant injectif, f se prolonge en un homomorphisme non nul g de M



dans S ; P=ker g est le sous-module maximal de M cherché - [en effet S est isomorphe à $M/\ker g$ et $x \notin \ker g$ car $g(x) = f(x) \neq 0$].

(2) $\Rightarrow$ (3) . évident .

(3) $\Rightarrow$ (1) . soit S un A-module à gauche simple ; on montre qu'il est injectif en montrant que tout homomorphisme f d'un idéal à gauche I (de A) dans S se prolonge en un homomorphisme g de A dans S .

si $f = 0$ le prolongement est l'application nulle

si $f \neq 0$ alors f est surjective et ker f est un sous-module propre maximal de I .

Il existe un idéal à gauche maximal P de A qui de plus contient ker f et ne contient pas I [ceci se déduit de la propriété (3) appliquée à l'idéal à gauche $\ker f \neq I$] ; ker f étant maximal dans I, on en déduit $\ker f = I \cap P$. - on a alors :

$$S \simeq I/I \cap P \simeq I + P/P = A/P$$

et il existe $i \in I$ tel que $f(i) = x_0 \in S$ et $\operatorname{Ann} x_0 = P$.

(On applique à S et A/P la propriété suivante : Bourbaki Alg. ch. VIII, § 4, ex. 2). En particulier $i \notin \ker f$ et $i \notin P$, donc $A = Ai + P$, $I = Ii + P \cap I$ et $1 = \lambda i + p$ où $\lambda \in A$ et $p \in P$; d'où $i = i\lambda i + ip$ et $f(i) = f(i\lambda i)$; on pose alors $g(1) = f(\lambda i) = \lambda x_0$. Pour montrer que g prolonge f il suffit de vérifier que g et f coïncident sur i et $P \cap I$; or $g(i) = f(i\lambda i) = f(i)$ et $g(P \cap I) = 0 = f(P \cap I)$

c.q.f.d.

Remarque sur le cas commutatif : proposition 3 :

Si A est un anneau commutatif unitaire, les 4 propriétés suivantes sont équivalentes,

(i) Tout idéal propre de A est égal à l'intersection des idéaux maximaux qui le contiennent.

(ii) A est régulier.

(iii) dans A tout idéal est égal à sa racine.

(iV) A est réduit et tout idéal premier est maximal.

Démonstration :

(i) $\Longleftrightarrow$ (ii) : voir [2] p. 85 .

(i) $\Longrightarrow$ (iii) : par définition $r(I)$ = Σ idéaux nilpotents modulo I , donc dans tout anneau unitaire on a :

$$I \subseteq r(I) \subseteq \cap(\text{idéaux premiers contenant } I) \subseteq \cap(\text{idéaux maximaux} \supseteq I)$$

d'où $I = r(I)$ dès que A vérifie (i) .

(iii) $\Longrightarrow$ (ii) : soit $x \in A$, de l'inclusion $(Ax)^2 \subseteq Ax^2$ on déduit

$$Ax^2 \subseteq Ax \subseteq r(Ax^2) = Ax^2$$

d'où

$$Ax^2 = Ax = r(Ax^2)$$

donc il existe $a \in A$ tel que $x = ax^2$ et A est régulier.

(ii) $\Longleftrightarrow$ (iV) : voir [1] .

Cas non commutatif.

Proposition 4 :

Si A est un anneau régulier réduit tout A-module simple est injectif.

Démonstration : [3] p. 211.

Remarque : on donnera à la fin de cet exposé un exemple d'anneau régulier qui ne vérifie pas la propriété que tout A-module simple est injectif.

Conjecture de Renault. Si A est un anneau unitaire réduit tel que tout A-module simple est injectif alors A est régulier.

Définition : R étant le radical de Jacobson d'un anneau A, on dit que R est T-nilpotent à gauche, si, et seulement si, pour toute suite $(a_i)_{i \in \mathbb{N}}$ d'éléments de R il existe un entier n tel que $a_1 a_2 \ldots a_n = 0$.

Proposition 5 :

Si R est le radical de Jacobson d'un anneau A, les conditions suivantes sont équivalentes.

(i) Pour tout A-module à gauche M non nul on a $M \neq RM$.

(ii) R est T-nilpotent à gauche.

Démonstration : cf. [4] .

(i) ==> (ii) : Soit $(a_i)_{i \in \mathbb{N}}$ une suite de R - on considère les A-modules suivants : F est le A-module libre de base dénombrable $(x_i)_{i \in \mathbb{N}}$ et G le

sous-module de F engendré par les éléments de F de la forme $x_i - a_i x_{i+1}$ où i parcourt $\mathbb{N}$. Soit $M = F/G$; dans M on a l'égalité $\bar{x}_i = a_i \bar{x}_{i+1}$ donc $M = RM$, $M = 0$ et $F = G$. On peut donc écrire $x_1 \in F$ sous la forme suivante :

$x_1 = \lambda_1(x_1 - a_1 x_2) + \lambda_2(x_2 - a_2 x_3) + \ldots + \lambda_K(x_K - a_K x_{K+1})$ et en identifiant les coefficients des deux membres on obtient :

$$\lambda_1 = 1 , \quad \lambda_2 = \lambda_1 a_1 = a_1 , \ldots, \lambda_K = \lambda_{K-1} a_{K-1} = a_1 a_2 \ldots a_{K-1} , \quad \lambda_K a_K = 0 .$$

Soit $a_1 a_2 \ldots a_K = 0$. c.q.f.d.

(ii) $\Longrightarrow$ (i) : Soit M un A-module non nul. Si $M = RM$, soit x un élément non nul de M, $x = \sum_i r_i X_i$ avec $r_i X_i \neq 0$, $r_i \in R$ et $X_i \in M$; de même $X_i = \sum_j r_{ij} X_{ij}$, avec $r_{ij} X_{ij} \neq 0$ et $r_{ij} \in R$; il existe un indice j tel que $r_i r_{ij} \neq 0$; on continue ce procédé en écrivant que $X_{ij} \in RM$, et ainsi de suite. On met ainsi en évidence une suite infinie d'éléments de R dont les produits successifs sont tous non nuls, ce qui contredit le fait que R est T-nilpotent à gauche.

Propriété (P) : Un anneau A vérifie la propriété (P) si et seulement si tout A-module à gauche non nul M contient un sous-module maximal.

Remarque : Si A vérifie la propriété (2) de la proposition 2 alors A vérifie (P).

Proposition 6 :

Les propriétés suivantes sont équivalentes :

(i) A vérifie (P) ,

(ii) A/R vérifie (P) et R est T-nilpotent à gauche.

Démonstration :

(i) $\Longrightarrow$ (ii) : si A vérifie (P), il est immédiat que A/R vérifie aussi (P) ; le fait que R est T-nilpotent à gauche se déduit de la proposition 5 et du lemme de Nakayama (proposition 7) ; en effet soient M un A-module à gauche non nul et M_0 un sous-module maximal de M ; M/M_0 est un A-module non nul, de type fini (car il est simple) donc $M/M_0 \neq R.M/M_0 = RM/M_0$, d'où $M \neq RM$.

(ii) $\Longrightarrow$ (i) : soit M un A-module non nul, il vérifie (prop. 5) $M \neq RM$. M/RM est un A-module annulé par R , donc un A/R-module. M/RM admet donc un sous A/R-module maximal, qui est en même temps un sous A-module maximal de M/RM , donc qui est de la forme M_0/RM où M_0 est un sous A-module maximal de M .

c.q.f.d.

On rappelle pour mémoire :

proposition 7 : Lemme de Nakayama .

Si M est un A-module non nul de type fini sur un anneau A , et si R est le radical de Jacobson de A alors :

(i) M contient un sous-module propre maximal,

(ii) $M \neq RM$.

Remarques sur le cas commutatif : on a les propositions suivantes 8 et 9.

Proposition 8 :

Un anneau commutatif A tel que R = 0 est un anneau réduit.

En effet soit a un élément de A tel que $a^n = 0$; alors, pour tout $\lambda \in A$, on a $(\lambda a)^n = 0$ donc $(1 - \lambda a)$ est inversible et $a \in R$, d'où $a = 0$.

Proposition 9 :

Si A est un anneau commutatif réduit vérifiant la propriété (P) alors A est régulier.

D'après la proposition 3 il suffit de montrer que dans A tout idéal premier est maximal. Ceci résulte du lemme suivant.

Lemme : Si B est un anneau commutatif intègre vérifiant la propriété (P) alors B est un corps.

Démonstration : Soit K le corps des fractions de B ; K est un B-module à gauche divisible et K contient un sous B-module maximal L . K/L est encore un B-module divisible, de plus il est simple ; il est donc isomorphe à B/P où P est un idéal maximal de B ; mais B/P étant divisible alors $P = 0$ ce qui entraîne que B est un corps. ($P = 0$, en effet supposons $P \neq 0$, soit s un élément non nul de P et y un élément non nul de B/P alors $sx = y$ n'a pas de solution dans B/P car $sx = 0$ pour tout $x \in B/P$) .

Conjecture de Bass.

Pour un anneau A les propriétés (a) et (b) suivantes sont équivalentes :

(a) $\begin{cases} (1) & \text{il n'existe pas dans A une infinité d'idempotents orthogonaux} \\ (2) & \text{tout A-module à droite non nul contient un sous-module simple.} \end{cases}$

(b) $\begin{cases} (1) & \text{il n'existe pas dans } A \text{ une infinité d'idempotents orthogonaux} \\ (2') & \text{tout } A\text{-module à gauche contient un sous-module maximal.} \end{cases}$

Anneau de Björk :

On dit que l'anneau A est un anneau de Björk (on vérifie la propriété (B)) si et seulement si : pour tout $x \in A$ il existe $a \in A$ et $n \in \mathbb{N}$ tels que $ax^{n+1} = x^n$.

Conséquence : si A est un anneau de Björk alors $R(A)$ est un nil idéal.

Remarque : si A est artinien à gauche alors A est un anneau de Björk.

Proposition 10 : [5]

Si l'anneau A vérifie la propriété (B) alors :

(1) $xy = 1 \Longrightarrow yx = 1$.

(2) tout élément non diviseur de 0 à droite est inversible.

(3) $J(A) \subseteq R(A)$ où $J(A)$ désigne l'idéal singulier de A .

Démonstration :

(1) soient x et y deux éléments de A tels que $xy = 1$; la propriété (B) donne un a et un n tels que $ax^{n+1} = x^n$; comme $x^n y^n = 1$, on en déduit $ax = 1$ d'où $a = y$ et $yx = 1$.

(2) si x est un élément non diviseur de zéro à droite on écrit :

$ax^{n+1} = x^n$ soit $(ax - 1)x^n = 0$ d'où $ax = 1 = xa$,

ce qui montre que x est inversible.

(3) on rappelle la définition suivante : $j(A) = \{ x \in A$, Annx est essentiel dans $A\}$. Pour montrer $J(A) \subseteq R(A)$ il suffit de montrer que pour tout $x \in J(A)$ $(1 - x)$ est inversible et d'après (2) il suffit de montrer que $(1 - x)$ est non diviseur de 0 à droite. Supposons que a soit un élément non nul de A tel que $a(1 - x) = 0$, Annx est essentiel dans A donc il existe un élément b de A tel que $ba \neq 0$ et $ba \in$ Annx; or $ba(1 - x) = 0$ donc $ba = 0$ ce qui est impossible donc $(1 - x)$ est bien non diviseur de zéro à droite.

c.q.f.d.

Proposition 11 :

Pour un anneau A unitaire les propriétés suivantes sont équivalentes :

(i) A est noethérien à gauche et A vérifie (B) ,

(ii) A est artinien à gauche.

(ii) $\Longrightarrow$ (i) évident ,

(i) $\Longrightarrow$ (ii) A/R vérifie les hypothèses du théorème de Goldie et d'après (10)-2 il est égal à son anneau de quotients à gauche, il est donc semi-simple. A/R est donc isomorphe à un produit fini d'anneaux de matrices sur un corps et il est artinien à gauche. On en déduit que A est lui-même artinien à gauche car R est nilpotent.

Cas commutatif.

Proposition 12 :

Si A est un anneau commutatif vérifiant la propriété (P) alors A est un anneau de Björk.

Démonstration : Ceci résulte des propositions 6, 8, 9. En effet A/R est un anneau commutatif réduit vérifiant la propriété (P) donc il est régulier ; pour tout $\bar{x} \in A/R$ il existe $\bar{a} \in A/R$ tel que $\bar{x} = \bar{x}^2\bar{a}$ soit $(\overline{x - x^2a}) = 0$. R étant T-nilpotent à gauche est un nil idéal et il existe un entier n tel que $(x - x^2a)^n = 0$ d'où l'existence d'un élément b tel que $x^n = bx^{n+1}$.

La démonstration de J.E. Björk, concernant la proposition 12 dans le cas d'un anneau non nécessairement commutatif, et transmise personnellement à G. Renault s'est révélée inexacte, et les résultats établis dans [5] sont vrais modulo la démonstration de la conjecture suivante :

Conjecture : Si A est un anneau non nécessairement commutatif, tel que tout A-module non nul contient un sous-module maximal, alors A est un anneau de Björk.

Corollaire de la proposition 12 :

Si A est un anneau commutatif régulier alors A est un anneau de Björk. Dans le cas non commutatif ceci n'est pas vrai.

Exemple d'anneau régulier qui ne vérifie pas la propriété de Björk.

On va donner un anneau dans lequel on a deux éléments f et g qui vérifient $g \circ f = 1$ et $f \circ g \neq 1$. Il ne vérifiera pas la propriété (B) d'après la proposition 10. On considère un espace vectoriel V de dimension infinie dénombrable sur un corps K : $V = \bigoplus_{i=0}^{\infty} Ke_i$, et on considère l'anneau $A = \underset{K}{\mathrm{End}}(V)$. On prend pour f l'endomorphisme de V défini par $f(e_i) = e_{i+1}$ pour tout $i \in N$ et pour g l'endomorphisme de V défini par $g(e_i) = e_{i-1}$ pour tout entier $i \geq 1$ et $g(e_0) = 0$.

Problème : un anneau (non nécessairement commutatif) régulier qui vérifie la propriété [(10)-(1)] est-il un anneau de Björk ?

Exemple d'anneau régulier tel que tout A-module simple ne soit pas injectif :

On reprend l'exemple précédent $V = \bigoplus_{i=o}^{\infty} Ke_i$ et $A = \underset{K}{End}(V)$. On considère $p_i \in A$, $p_i : V \longrightarrow Ke_i : x = \sum_{j=1}^{n} k_j e_j \longrightarrow k_i e_i$ $\ker p_i = \bigoplus_{j \neq i} Ke_j$. V est un A-module à gauche simple isomorphe à Ap_i car on a :

$$\underset{A}{Ann}(e_i) = \underset{A}{Ann}(p_i) = \left\{ f,\ f \in A,\ f(e_i) = 0 \right\} .$$

V n'est pas injectif : on considère l'idéal à gauche S de A :

$$S = \sum_{i \in o}^{+\infty} Ap_i$$

et on définit un homomorphisme φ de S dans V en posant $\varphi(p_i) = e_i$, quel que soit $i \geqslant 0$. Si V était injectif, il existerait un élément x de V tel que $x = \Sigma \lambda_i e_i$ avec $e_i = \varphi(P_i) = P_i \circ x = P_i(x) = \lambda_i e_i$, soit $\lambda_i = 1$ quel que soit $i \geqslant 0$ ce qui est absurde car I est infini.

- BIBLIOGRAPHIE -

[1] J. FORT et G. RENAULT - Séminaire d'Algèbre de Poitiers, 1966-67.

[2] L. LESIEUR - Divers aspects de la théorie des idéaux d'un anneau commutatif. Enseignement mathématique; T. XIII, Fasc. 2 - 1967.

[3] G. RENAULT - Anneaux réduits non commutatifs. Journal de mathématiques pures et appliquées, 1967, p. 203-214.

[4] G. RENAULT - Sur les anneaux A, tels que tout A-module à gauche non nul contient un sous-module maximal. C.R.A.S., t. 264, p. 622-624. (1967) -

[5] G. RENAULT - Sur les anneaux A, tels que tout A-module à gauche non nul contient un sous-module maximal. C.R.A.S., T. 267, p. 792-794. (1968) -

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-

Conférence n° 7 du 11 décembre 1968

par G. RENAULT

- II anneaux A tels que tout A-module non nul contient un sous-module maximal. -

-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 8 du 16 décembre 1968

par J.Y. CHAMARD

-:-:-:-:-:-:-

1. Introduction.

Un module M est dit complément décomposable s'il est somme directe d'injectifs indécomposables ; il est dit bien complémenté si l'intersection de deux sous-modules compléments dans M est un complément dans M ; On dira que M vérifie la condition (C) s'il est complètement décomposable, et ne possède pas de sous-module essentiel propre complètement décomposable.

En 1958, MATLIS pose dans [8] la question suivante : tout facteur direct d'un module complètement décomposable est-il également complètement décomposable ; cette question est restée sans réponse pendant près de dix ans ; en 1967, FAITH et WALKER ont apporté dans [4] une réponse positive dans le cas où M est un module injectif. Nous avons démontré dans [3] qu'il en était de même lorsque M est bien complémenté.

Nous nous proposons de démontrer ici que :

(i) Dans tout module complètement décomposable vérifiant la condition (C), les facteurs directs sont des sous-modules complètement décomposables (théorème 1).

(ii) Tout module quasi-injectif complètement décomposable vérifie la condition (C) (théorème 2).

(iii) Tout module complètement décomposable et bien complémenté est quasi-injectif (Théorème 3).

2. Résultats préliminaires.

Nous rappelons qu'un sous-module N d'un module M est dit essentiel dans M (ou encore M est dit extension essentielle de N) si, pour tout sous-module non nul X de M, on a $X \cap N \neq 0$.

Un module M est dit quasi-injectif si tout homomorphisme d'un sous-module N de M dans M se prolonge en un endomorphisme de M (pour une étude détaillée de ces modules, on pourra se rapporter à JOHNSON et WONG [7], et FAITH et UTUMI [4]).

On appelle indécomposable un module qui ne peut se décomposer en somme directe de deux sous-modules propres.

N étant un sous-module d'un module M, un sous-module K de M est dit complément relatif de N dans M si l'on a $N \cap K = 0$, et si K est maximal pour cette propriété ; $N \oplus K$ est alors un sous-module essentiel de M.

Un sous-module K de M est appelé sous-module complément dans M s'il existe un sous-module de M dont K soit un complément relatif ; on démontre qu'il en est ainsi si et seulement si K ne possède pas d'extension essentielle propre contenue dans M.

On dit qu'un module non nul M est co-irréductible si l'intersection de deux sous-modules non nuls de M n'est jamais nulle. Il est équivalent de dire ([8] proposition 2.2) que M admet une enveloppe injective indécomposable, ou que M est extension essentielle de tous ses sous-modules non nuls.

Théorème A :

Soient $(E_i)_{i \in I}$ et $(F_j)_{j \in J}$ deux familles indépendantes maximales de

sous-modules injectifs indécomposables d'un module injectif Q .

Il existe un automorphisme φ de Q et une bijection σ de I sur J tels que

$$i \in I \qquad \varphi(E_i) = F_{\sigma(i)} \ .$$

- Ce théorème, généralisant celui d'AZUMAYA [1] , a été démontré par FORT [6] et MIYASHITA [9] .

Corollaire :

Si N_1 et N_2 sont deux sous-modules essentiels d'un module M , et sont somme directe d'injectifs indécomposables, ils sont isomorphes.

Théorème B :

Soit M un A-module, et E une enveloppe injective de M ; les assertions suivantes sont équivalentes :

1) M est quasi-injectif ,

2) M est stable pour $\mathrm{End}_A(E)$.

- Ce théorème classique a été démontré par JOHNSON et WONG dans [7] , théorème 1.1. .

Lemme 1 :

Soit N un sous-module non nul d'une somme directe $\bigoplus_{i \in I} N_i$ de sous-modules

de M ; il existe alors un indice i de I et un sous-module non nul N'_i de N_i isomorphe à un sous-module non nul N' de N .

Démonstration :

On peut toujours supposer que N est monogène, et se ramener ainsi au cas où card I est fini.

- card I = 1 est trivial.
- card I = 2 : $N \subset N_1 \oplus N_2$

  si $N \cap N_1 = (0)$, N est isomorphe à un sous-module de $N_1 \oplus N_2/N_1 = N_2$,

  si $N \cap N_1 \neq (0)$, ce sous-module répond à la question.
- card I = n : $N \subset N_1 \oplus (N_2 \oplus \ldots \oplus N_n)$; on se ramène au cas n = 2 .

Proposition 1 :

Soit M un module, extension essentielle d'une somme directe de sous-modules co-irréductibles ; tout sous-module non nul de M possède la même propriété.

Démonstration : (FORT [6])

Remarquons tout d'abord qu'en vertu du lemme 5 , tout sous-module non nul N de M contient au moins un sous-module co-irréductible. Soit alors $(C_i)_{i \in I}$ une famille indépendante maximale de sous-modules co-irréductibles de N (dont l'existence est assurée par le théorème de Zorn) , et soit T un complément de $\bigoplus_{i \in I} C_i$ dans N ; T ne contenant aucun sous-module co-irréductible, il est nul, et donc $\bigoplus_{i \in I} C_i$ est essentiel dans N .

3. Facteurs directs des modules complètement décomposables.

Condition (P) :

Un module complètement décomposable vérifie la condition (C) , s'il ne possède pas de sous-module essentiel propre qui soit complètement décomposable.

Exemple :

Tout module injectif complètement décomposable vérifie la condition (C) en vertu du théorème A (tout sous-module essentiel complètement décomposable de E devant être injectif, puisque isomorphe à E , donc facteur direct de E , et finalement égal à E) .

Lemme 2 :

Soient $M = \bigoplus_{i \in I} E_i$ un module, somme directe d'injectifs indécomposables, K un facteur direct de M , et N un sous-module de type fini de K ; il existe une enveloppe injective de N contenue dans K .

Démonstration (FAITH et WALKER [5]) :

N étant de type fini, il existe un sous-ensemble fini J de I tel que N soit contenu dans le module injectif $M' = \bigoplus_{i \in J} E_i$; soit N_0 une enveloppe injective de N contenue dans M' , donc dans M .

Soit p la projection de M sur K , dont le noyau est un supplémentaire de K dans M .

Ker p $\cap$ N étant nul, il en est de même pour Ker p $\cap N_o$; $p(N_o)$ est ainsi isomorphe à N_o, donc est injectif. En outre, Ker p étant facteur direct de M, $p(N) = N$ est essentiel dans $p(N_o)$. Il en résulte que $p(N_o)$ est une enveloppe injective de N contenue dans K.

Proposition 2 :

Soit M un module, somme directe d'injectifs indécomposables ; tout facteur direct de M est extension essentielle d'une somme directe d'injectifs indécomposables.

Démonstration :

Soit K un facteur direct de M ; en vertu de la proposition 2, K est extension essentielle d'une somme directe de sous-modules co-irréductibles $(C_j)_{j \in J}$, que l'on peut supposer monogènes. Le lemme 1 nous permet de remplacer chacun des C_j pour une enveloppe injective E_j contenue dans K, et K est alors extension essentielle de la somme directe des E_j.

Théorème 1 :

Soit M un module complètement décomposable vérifiant la condition (C) ; tout facteur direct de M est complètement décomposable.

Démonstration :

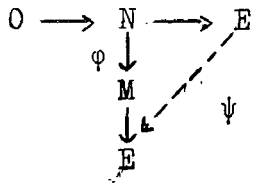
Soit L un supplément de K dans M ; d'après la proposition 3, L et K sont extensions essentielles de modules complètement décomposables L' et K' ; $L' \oplus K'$ est alors un sous-module essentiel complètement décomposable de M. Il résulte de la condition (C) que $M = L' \oplus K'$, donc que $K = K'$ est un sous-module complètement décomposable.

Théorème 2 :

Tout module quasi-injectif complètement décomposable M vérifie la condition (C).

Démonstration :

Soit N un sous-module essentiel complètement décomposable de M, théorème A. Appelant F une enveloppe injective de M (et donc de N), on note ψ l'endomorphisme de E prolongeant φ



N, isomorphe à M, étant quais-injectif, il est stable par φ (théorème 2) ; on a donc $\psi(N) \subset N$.

Or $\psi(N) = \varphi(N) = M$; il en résulte que $M = N$.

Proposition 3 :

Si M est un module complètement décomposable quasi-injectif, il y a identité entre facteurs directs de M et sous-modules complètement décomposables de M.

Démonstration :

Nous venons de voir que tout facteur direct est complètement décomposable ; considérons réciproquement un sous-module complètement décomposable K de M, et soit L un complément de K dans M. M étant quasi-injectif, L est facteur direct de M, donc est, d'après la proposition 3, extension essentielle d'un module complètement décomposable L' ; M est alors égal à $L' \oplus K$ (condition (C)), ce qui prouve que K est facteur direct de M.

4. Quasi-injectivité des modules complètement décomposables bien complémentés.

Théorème 3 :

Tout module complétement décomposable bien complémenté est quasi-injectif.

Démonstration :

On sait ([10] , théorème 4.3.) qu'un module M est bien complémenté si et suelement si, pour tout complément K de M et tout endomorphisme φ de $E(M)$ dont le noyau est essentiel dans $E(M)$, on a

$$\varphi(K) \subseteq E(K) .$$

Ici, $$M = \bigoplus_{i \in I} E_i \ ;$$

chaque E_i étant un complément dans M , on a

$$\varphi(E_i) \subseteq E_i \ ,$$

d'où $$\varphi(M) \subseteq M$$

dès que $\operatorname{Ker} \varphi$ est essentiel dans $E(M)$.

La proposition résulte alors du lemme suivant :

Lemme 3 : (CAILLEAU [2])

Soit M un module somme directe d'injectifs indécomposables ; M est quasi-injectif si et seulement si, pour tout endomorphisme φ de $E(M)$ dont le noyau est essentiel dans $E(M)$, on a :

$$\varphi(M) \subseteq M \ .$$

- BIBLIOGRAPHIE -

[1] AZUMAYA G. - Conections and supplementaries to my paper concerning Krull-Remak-Schmidt's theorem (Nagoya Math. J. Vol. I, 1950, p. 117-124).

[2] CAILLEAU A. -Anneau associé à un module injectif riche en co-irréductibles (C.R. Acad. Sc. Paris, t. 264, p. 1040-1042, 12 juin 1967).

[3] CHAMARD J.Y.-Modules riches en co-irréductibles et sous-modules compléments (C.R. Acad. Sc. Paris, t. 264, p. 987-990, 1967).

[4] FAITH C. et UTUMI Y.- Quasi injective modules and their endomorphism rings (Arch. Math. Vol. 15, 1964, p. 166-174).

[5] FAITH C. et WALKER E.- Direct-sum representations of injective modules (J. of algebra 5, 1967, p. 203-221).

[6] FORT J. - Sommes directes de sous-modules co-irréductibles d'un module (Math. Zeitahr, vol. 103; 1968, p. 363-388).

[7] JOHNSON R.E. et WONG E.T.- Quasi-injective modules and irreductible rings (J. London, Math. Soc. 72, 1952, p. 327è340).

[8] MATLIS E. - Injective modules over noetherian rings (Pacific J. Math. 8, 1958, p. 511-528).

[9] MIYASHITA Y. -On quasi-injective modules, a generalisation of the theory of completely reducible modules (J. Fac. Sc. Hokkaïdo Univ. 18, 1965, p. 158-187).

[10] RENAULT G. - Etude des sous-modules compléments dans un module (Bull. Soc. Math. de France, série "Mémoires", no 9, thèse, Paris 1966).

-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-:-

Conférence n^{os} 9. 11. 12 des 6, 20 et 27 janvier 1969

Exposés élémentaires sur la représentation linéaire des groupes finis par Melle M. VIEL, Mme G. VORS, et M. L. LESIEUR.

-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence 10 du 13 janvier 1969

Théorèmes de stabilité pour des dérivations dans une algèbre associative

par EARL J. TAFT

-:-:-:-:-:-:-

1. Introduction et explication du problème.

Soit A une algèbre associative, de dimension finie sur un corps commutatif F. Soit R le radical de A ; on suppose dans cet article que l'algèbre A/R est séparable. Alors, grâce au théorème bien connu de Wedderburn, on peut écrire $A = S + R$, où S est une sous-algèbre séparable, $S \cap R = 0$ et $S \cong A/R$. Une telle sous-algèbre S s'appelle un facteur de Wedderburn dans A. S n'est pas unique, en général, mais on a le théorème d'unicité de Malcev, qui dit que si S est une sous-algèbre de A et si T est un facteur de Wedderburn dans A, alors il existe x dans R tel que l'automorphisme intérieur C_{1-x} dans A déterminé par $1 - x$ envoie S dans T. (On ne suppose pas que A contient une unité 1, la notation ayant un sens, de toute façon). En particulier, si S et T sont des facteurs de Wedderburn dans A, S et T sont isomorphes via un automorphisme dans A, de la manière indiquée. On peut trouver une bonne exposition des théorèmes de Wedderburn et Malcev dans [4].

Maintenant on introduit une algèbre de Lie L sur F, dont les membres sont des dérivations dans A, c'est-à-dire, si $D \in L$, D est une application F-linéaire de A et $D(ab) = (Da)b + a(Db)$ pour tous $a, b \in A$. On va supposer que L est complètement réductible en tant qu'ensemble d'applications linéaires dans A, c'est-à-dire, tout sous-espace de A qui est stable pour L a un sous-espace complémentaire dans A qui est aussi stable pour L. Maintenant, on va poser deux questions :

Question 1 : Est-ce qu'il existe un facteur de Wedderburn dans A qui est stable pour L ?

Question 2 : Si S et T sont deux facteurs de Wedderburn qui sont stables pour L, qu'elle est la relation entre S et T ?

Pour expliquer davantage la seconde question, on remarque que si $x \in R$ est un L-constant, c'est-à-dire, $Dx = 0$ pour tout $D \in L$, alors l'automorphisme C_{1-x} dans A donné par $C_{1-x}(a) = (1-x)a(1-x)^{-1}$ commute avec tous les éléments de D, et donc, si S est une sous-algèbre de A stable pour L, $C_{1-x}S$ l'est aussi. Alors la relation indiquée à la question 2 est que S et T seraient isomorphes par un automorphisme intérieur C_{1-x} dans A, où x est un L-constant dans R.

On remarque que des questions analogues à ces deux questions sont déjà traitées dans la littérature, où, au lieu de L, on a un groupe G d'automorphismes dans A (voir [7], [9]). On va voir qu'on peut utiliser ces résultats pour G pour donner des réponses affirmatives aux questions 1 et 2, dans le cas où le caractéristique p de F est égal à 0, mais pour obtenir cela, il faudra employer les notions

de groupe algébrique et d'algèbre de Lie associée. D'autre part, on va aussi donner une réponse définitive à la question 2 qui est valable pour n'importe quel $p \geq 0$, et dont la démonstration est purement algébrique.

Nous remarquons enfin que les résultats décrits dans cet exposé sont contenus dans la thèse de M. Charles Hallakan, Rutgers University, 1968 et qu'ils seront contenus dans l'article [5].

2. Le cas de caractéristique zéro.

Théorème 1 : Soit A une algèbre associative de dimension finie sur un corps F de caractéristique 0. Soit R le radical de A. Soit L une algèbre de Lie complètement réductible de dérivations dans A. Alors :

1) A contient un facteur de Wedderburn qui est stable pour L,

2) Si S est une sous-algèbre semi-simple de A qui est stable pour L, et si T est un facteur de Wedderburn dans A qui est stable pour L, alors il existe un L-constant x dans R tel que $C_{1-x}S \subset T$.

Pour démontrer ce théorème, nous utilisons les notions de groupe algébrique et algèbre de Lie algébrique, comme expliquées, par exemple, dans [2], [3], [8]. Soit $\bar{L}$ la plus petite algèbre de Lie algébrique qui contient L, et soit G le groupe algébrique (connexe) dont $\bar{L}$ est l'algèbre de Lie algébrique. Les membres de $\bar{L}$ sont des dérivations dans A, ceux de G sont des automorphismes dans A, et puisque L, $\bar{L}$ et G stabilisent les mêmes sous-espaces de A, $\bar{L}$ et G sont aussi complètement réductibles. Maintenant on fait appel au théorème de [7] qui dit que A

a un facteur de Wedderburn S qui est stable pour G . Le groupe G_S des applications F-linéaires non singulières dans A qui laissent stable S est un groupe algébrique, et on a $G \subset G_S$. L'algèbre de Lie algébrique qui corresponde à G_S est L_S , toutes les applications F-linéaires dans A qui stabilisent S . Enfin, on a $L \subset \bar{L} \subset L_S$, ce qui montre que S est un facteur de Wedderburn dans A qui est stable pour L . La première partie du théorème est donc démontrée.

Pour la deuxième partie, on utilise le résultat dans [9] qui dit qu'il existe x dans R tel que $C_{1-x}S \subset T$ et tel que x soit point fixe pour G , c'est-à-dire, $gx = x$ pour tout $g \in G$. Alors $G \subset G_x$, le groupe algébrique de toutes les applications F-linéaires non-singulières dans A qui ont x comme point fixe. L'algèbre de Lie algébrique qui correspond à G_x est $\overbrace{L_x}^{\text{ensemble de}}$, toutes les applications F-linéaires dans A qui s'annulent en x . Enfin, on a $L \subset \bar{L} \subset L_x$, ce qui montre que x est un L-constant, et on a démontré le théorème 1 .

On remarque que, si A et L sont comme indiqués dans le théorème, et si S et T sont deux facteurs de Wedderburn stables pour L , alors il existe x dans R qui est constant pour L tel que $C_{1-x}S = T$.

La première partie du théorème 1 a été remarquée dans [1] dans le cas om A est une algèbre de Lie de dimension finie sur un corps commutatif F de caractéristique zéro.

3. Le théorème d'unicité dans le cas général.

On ignore si la conclusion de la première partie du théorème 1 reste valable lorsque la caractéristique de F est positive et aussi pour la question analogue pour un groupe G d'automorphismes dans A (ici on suppose A/R séparable). Cependant, on peut généraliser la deuxième partie du théorème 1 au cas d'une caractéristique quelconque.

Théorème 2 : Soit A une algèbre associative de dimension finie sur un corps commutatif F. Soit R le radical de A, et on suppose que A/R est séparable. Soit L une algèbre de Lie complètement réductible de dérivations dans A telle que $LR \subset R$. Soit S une sous-algèbre séparable de A qui est stable pour L, et soit T un facteur de Wedderburn dans A qui est stable pour L. Alors, il existe un L-constant $\underset{\sim}{x}$ dans R tel que $C_{1-\underset{\sim}{x}}S \subset T$.

Pour démontrer ce théorème, on considère deux cas :

Cas 1 : $R^2 = 0$.

Grâce au théorème de Malcev, il existe $\underset{\sim}{x}$ dans R tel que $C_{1-\underset{\sim}{x}}S \subset T$. Si $s \in S$, on a $(1-\underset{\sim}{x})s(1+\underset{\sim}{x}) \in T$, c'est-à-dire, $s - \underset{\sim}{x}s + s\underset{\sim}{x} \in T$. Soit $D \in L$. Si on applique D à cette relation, on a $Ds - x(Ds) - (Dx)s + (Ds)x + s(Dx) \in T$. Mais $Ds \in S$ et on a aussi : $Ds - \underset{\sim}{x}(Ds) + (Ds)\underset{\sim}{x} \in T$. On soustrait pour trouver : $s(D\underset{\sim}{x}) - (Dx)s \in T$. Mais on suppose que $Dx \in R$ et donc $s(Dx) - (Dx)s \in T \cap R = 0$.

$Dx \in C(S) \cap R$, où $C(S) = \left\{ a \in A \mid as = sa \text{ , tout } s \in S \right\}$.

Maintenant R est stable pour L par hypothèse, et $C(S) \cap R$ est un sous-

espace de R qui est stable pour L . L'action de L sur un sous-espace de R qui est stable pour L (où sur le quotient de deux tels sous-espaces) étant complètement réductible, on peut décomposer $R = (C(S) \cap R) \oplus U$, où $LU \subset U$. Ecrivons $x = y + u$, $y \in C(S) \cap R$, $u \in U$. Alors, si $D \in L$, on a $Du = Dx - Dy \in (C(S) \cap R) \cap U = 0$ et u est un L-constant. Enfin, $T \supset C_{1-x}S = C_{1-u}\, C_{1-y}S = C_{1-u}S$ parce que $y \in C(S)$.

Cas 2 : $R^2 \neq 0$.

Appelons $\bar{A} = A/R^2$, où $a \longrightarrow \bar{a}$ est l'homomorphisme canonique de A sur $\bar{A}$. On va raisonner par récurrence sur la dimension de A sur F . L agit sur $\bar{A}$ comme algèbre de Lie complètement réductible de dérivations, $\bar{S}$ est une sous-algèbre séparable de $\bar{A}$ qui est stable pour L et $\bar{T}$ est un facteur de Wedderburn dans $\bar{A}$ qui est stable pour L . Alors il existe x dans R tel que $\bar{x}$ est un L-constant et $C_{1-\bar{x}}\bar{S} \subset \bar{T}$. Si $D \in L$, on a donc : $Dx \in R^2$. R^2 est un sous-espace de R qui est stable pour L , et on décompose $R = R^2 \oplus U$ ou U est stable pour L . Ecrivons $x = y + u$, $y \in R^2$ et $u \in U$. Alors, pour $D \in L$, on a : $Du = Dx - Dy \in R^2 \cap U = 0$. u est donc un L-constant, et aussi $\bar{u} = \bar{x}$. Donc, $C_{1-\bar{u}}\bar{S} \subset \bar{T}$, qui entraîne que $C_{1-u}S + R^2 \subset T + R^2$. L'algèbre $T + R^2$ est strictement contenue dans A et est stable pour L . $C_{1-u}S$ est une sous-algèbre séparable de $T + R^2$ qui est stable pour L (parce que u est un L-constant) et T est un facteur de Wedderburn dans $T + R^2$ qui est stable pour L . Donc, par récurrence, il existe $v \in R^2$ qui est un L-constant, tel que $C_{1-v}C_{1-u}S \subset T$. Enfin, l'élément $w = u + v - uv$ est un L-constant dans R tel que $C_{1-w}S \subset T$, ce qui démontre le théorème 2 .

Nous remarquons, d'abord, que si $p = 0$, la condition $LR \subset R$ est toujours valable pour n'importe quel ensemble L de dérivations dans A (voir [6]). Alors,

le théorème 2 généralise la deuxième partie du théorème 1 quand $p = 0$.

Nous remarquons aussi que si p est positif, l'hypothèse $LR \subset R$ ne peut être omise. Il existe un exemple (voir [5]) qui montre que le théorème 2 ne reste plus valable si on ne suppose pas que $LR \subset R$.

Enfin, si A et L sont comme indiqués dans le théorème 2, et si S et T sont deux facteurs de Wedderburn dans A qui sont stables pour L , alors il existe un L-constant x dans R tel que $C_{1-x}S = T$. Ce corollaire n'est plus valable si on ne suppose pas que $LR \subset R$.

BIBLIOGRAPHIE

[1] L. Auslander et J. Brezin, Almost algebraic Lie algebras and Lie groups, Journal of Algebra 8 (1968), p. 295-313.

[2] C. Chevalley, théorie des groupes de Lie : II. Groupes algébriques, Hermann, Paris, 1951.

[3] C. Chevalley, Théorie des groupes de Lie : III. Théorèmes généraux sur les algèbres de Lie. Hermann, Paris, 1955.

[4] C. Curtis et I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New-York, 1962.

[5] C. Hallakan, Stability theorems for Lie algebras of derivations (à paraître).

[6] C. Hochschild, Semi-simple algebras and generalized derivations, American J. Math. 64 (1942), p. 677-694.

[7] G. Mostow, Fully reducible subgroups of algebraic groups, American J. Math. 78 (1956), p. 200-221.

[8] G. Seligman, Algebraic groups, Yale University, 1964.

[9] E. Taft, Orthogonal conjugacies in associative and Lie algebras, Transactions Amer. Math. Soc. 113 (1964), p. 18-29.

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-:-:-

Conférence n° 13 du 3 février 1969

par J. CALAIS

- Problèmes de Burnside et Kurosh dans les groupes et les algèbres -

-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-

Conférence n° 14 du 10 février 1969

par J. CALAIS

- Théorème de Golod-Shavarevitch et applications -

-:-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-

Conférence n° 15 du 24 février 1969 par

J. RIGUET

Notion de radical dans les catégories .

-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-

Conférences n^{os} 16-17 des 3 et 10 mars 1969 par

J. FORT

Algèbres de Frobenius et représentation des groupes.

-:-:-:-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-

Conférence n° 18 du 17 mars 1969 par

Y. QUENTEL

- Sur la compacité du spectre minimal d'un anneau -

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 19 du 14 avril 1969

-:-:-:-:-:-:-:-

LA FACTORISATION DANS LES ANNEAUX NON-COMMUTATIFS -I-

par P.M. COHN

-:-:-:-:-:-:-:-:-

0. La notion d'anneau factoriel est assez bien connue dans le cas commutatif. Le premier exemple sans doute est $\mathbf{Z}$, l'anneau d'entiers, dont la factorialité a été démontrée par Euclide, en utilisant l'algorithme qui porte son nom (pour être précis, Euclide s'occupe du demi-anneau d'entiers positifs, mais nous nous passons de ce raffinement).

Dans le cas non-commutatif, la théorie est de date beaucoup plus récente. Elle commence dans l'analyse où on considère les équations différentielles linéaires ; par exemple, prenons :

$$a_0 y^{(n)} + a_1 y^{(n-1)} + \dots + a_n y = 0 \quad ,$$

qui s'écrit en forme d'opérateurs,

$$(a_0 D^n + a_1 D^{n-1} + \dots + a_n)y = 0 \quad .$$

On s'aperçoit que ces opérateurs forment un anneau analogue à l'anneau de polynômes en D, à coefficients dans un corps K, mais avec la règle de commutation

$$Da = aD + a' \qquad \left(a' \equiv \frac{da}{dX}\right) .$$

Cet anneau apparaît déjà en Schlesinger [97], qui montre que c'est un anneau intègre. Un peu plus tard, Landau [02] et Loewy [03] montrent que chaque opérateur admet une factorisation complète, deux telles factorisations ont même nombre de facteurs, et on peut établir une correspondance entre eux tels que des facteurs qui se correspondent sont du même type, dans un sens qui a déjà été défini par Poincaré.

Loewy reprit la question dans plusieurs articles, mais ce fut Ore [32] qui donna une théorie algébrique qui s'applique à un anneau euclidien quelconque (non-commutatif). Peu après, Asano [38] étendait la théorie aux anneaux principaux, comme dans la présentation donnée dans le livre de Jacobson [43] . Mais tout se passe sans que la définition d' "anneaux factoriels" intervienne. Cette définition (qui était "dans l'air") fut donnée dans Cohn [63] , où se trouve aussi la description d'une classe d'anneaux factoriels beaucoup plus vaste que les anneaux principaux. Ce sont les "anneaux de Bezout faibles à factorisation complète", ou dans un langage plus à jour : les "2-firs atomiques". Ils comprennent les algèbres associatives libres sur un corps, le produit libre de corps gauches, etc....

Mon programme dans ces conférences sera la suivant :

I. Définition et propriétés principales d'un anneau factoriel.

II. Relations avec l'algorithme faible.

III. Factorisation de matrices.

IV. Localisation.

1. Tous les anneaux ont un élément-unité 1 , qui sera respecté par homomorphismes, sous-anneaux, modules, etc... Un anneau R est dit <u>intègre</u> si $R^* = R \setminus \{0\}$ est non-vide et admet une multiplication. Le groupe d'unités sera noté $U(R)$.

Soit donnée une factorisation d'un élément c de R^* :

$$c = a_1 a_2 \dots a_k \quad . \tag{1}$$

On y associe la chaîne de modules (idéaux à droite) :

$$R \supseteq a_1 R \supseteq \dots \supseteq a_1 \dots a_k R = cR$$

avec quotients :

$$R/a_1 R \ , \quad a_1 R/a_1 a_2 R \tilde{=} R/a_2 R \ , \ \dots \ , \ R/a_k R \ .$$

Une seconde factorisation de c :

$$c = b_1 b_2 \dots b_\ell \tag{2}$$

est dite <u>isomorphe</u> à (1) si $\ell = k$ et s'il existe une permutation $i \longmapsto i'$ tel que

$$R/a_i R \tilde{=} R/b_{i'} R \ .$$

Par <u>atome</u> on entend un élément qui n'est ni unité, ni produit de deux éléments non-unités. Une factorisation (1) est dite <u>complète</u> si chaque a_i est un atome. Maintenant il est clair qu'on va définir un anneau factoriel comme suit :

<u>Définition</u> : Un anneau R est <u>factoriel</u> s'il est intègre et si chaque élément qui n'est ni 0, ni unité, admet une factorisation complète, deux telles factorisations d'un même élément étant isomorphes.

D'abord notons que cela redonne la définition habituelle au cas commutatif. Il suffit de remarquer que $R/aR = R/bR \Longrightarrow aR = bR$ (parce que aR peut être caractérisé comme annulateur de R/aR). Définissons généralement : a est <u>semblable</u> à b : $a \sim b$, si $R/aR \tilde{=} R/bR$. Dans le cas commutatif les éléments semblables sont associés, comme nous venons de le voir, donc il est équivalent de regarder des factorisations ou des chaînes de modules. Mais dans le cas général il est plus commode de considérer ces dernières, ce qui remplace la condition compliquée de similitude par la condition simple d'isomorphisme de modules.

Par quel moyen peut-on prouver la factorialité d'un anneau ? Soit R un

anneau (intègre et) principal. Alors tout élément admet une factorisation complète ; en plus le théorème de Jordan-Hölder pour les treillis modulaires affirme que deux factorisations complètes d'un même élément sont isomorphes. Donc on a :

Théorème 1 : Tout anneau intègre principal est factoriel.

Pour étendre ce résultat, il est utile de séparer les questions d'existence et d'unicité.

Existence. Convenons d'appeler atomique un anneau intègre dans lequel tout élément est soit zéro, soit unité, soit produit d'atomes. Par exemple, il est facile de montrer (et nous le verrons plus tard) qu'un anneau intègre qui satisfait à la condition maximum pour les idéaux principaux à droite et à gauche est atomique.

Soit maintenant R un anneau intègre atomique. Pour pouvoir affirmer que R est factoriel, il suffit que les idéaux principaux à droite forment un treillis modulaire. La façon la plus évidente de remplir cette condition est que les idéaux principaux à droite forment un sous-treillis du treillis de tous les idéaux à droite (qui est sûrement modulaire). Cela veut dire que la somme et l'intersection de deux idéaux principaux à droite sont encore principaux. Pour que cela arrive il faut se placer dans un anneau de Bezout à droite (par définition), ce qui sort très peu du cadre des anneaux principaux. Mais on peut étendre la classe d'anneaux par une petite observation qui constitue la clef pour la suite : pour comparer deux factorisations d'un élément $C \neq 0$ nous n'avons pas affaire aux idéaux principaux quelconques, mais seulement aux idéaux qui contiennent cR. Donc, il suffit d'exiger que $aR + bR$ et $aR \cap bR$ soient principaux seulement dans le cas $aR \cap bR \neq 0$. Les anneaux intègres satisfaisant à cette condition s'appellent parfois anneaux de Bezout faibles. On peut montrer que - malgré les apparences - la notion est symétrique à droite et à gauche. Mais à présent on utilise un terme plus court et plus systématique qui sera expliqué

bientôt : le 2-fir. D'abord notons qu'on peut simplifier la définition d'un anneau de Bezout faible :

Lemme : Soit R un anneau intègre, tel que $aR \cap bR \neq 0 \Longrightarrow aR + bR$ principal. Alors $aR \cap bR$ est principal, pour tous $a, b \in R$.

Démonstration : Il faut montrer que $aR \cap bR$ est principal, et on peut évidemment supposer que $aR \cap bR \neq 0$. On a une suite exacte

$$0 \longrightarrow aR \cap bR \xrightarrow{\lambda} aR \oplus bR \xrightarrow{\mu} aR + bR \longrightarrow 0 .$$

où $\mu(x,y) = x-y$, et $\lambda(x) = (x,y)$. Par hypothèse, $aR + bR$ est principal, donc libre et alors la suite est scindée. Cela veut dire que $aR \cap bR$ est image de $aR \oplus bR$, donc c'est un idéal engendré par deux éléments, qui ne forment pas une famille libre (parce que le noyau de l'application est $aR + bR \neq 0$) et par la propriété de R cela montre que $aR \cap bR$ est principal.

On peut exprimer la définition d'un anneau de Bezout faible comme suit : si deux éléments de R sont linéairement dépendants à droite (sur R), alors l'idéal à droite qu'ils engendrent est principal. Car $aR \cap bR \neq 0$ veut dire justement qu'il existe a', b' non tous les deux nuls, tels que $ab' - ba' = 0$.

De plus on peut exprimer la condition d'être anneau intègre de la même façon: si un élément de R est linéairement dépendant, alors l'idéal à droite qu'il engendre est nul. Cela nous mène à la définition suivante :

Définition : un anneau R s'appelle n-fir si tout idéal à droite engendré par une famille linéairement dépendante de m ($\leq n$) éléments a aussi une famille génératrice comportant $< m$ éléments.

Selon cette définition, 1-fir n'est autre chose qu'un anneau intègre, et 2-fir est justement un anneau de Bezout faible. Le nom n-fir s'explique par la

propriété suivante qui peut aussi servir comme définition :

Dans un n-fir, tout idéal à droite qui peut être engendré par n éléments au plus, est libre, de rang bien déterminé.

Remarquons que tout n-fir est aussi n'-fir, pour $n' < n$. Un anneau qui est n-fir pour tout n , est caractérisé par le fait que tous ses idéaux à droite de type finis sont libres, de rangs bien déterminés. Cela s'appelle semi-fir. Enfin un fir (= free ideal ring) à droite est un anneau dans lequel tout idéal à droite est libre, de rang bien déterminé.

Remarquons encore (sans preuve) que la notion de n-fir est symétrique à droite et à gauche, donc aussi celle de semi-fir. Par contre, il existe des firs à droite qui ne le sont pas à gauche.

Pour revenir à la factorisation, nous avons vu que, pour la factorialité, il suffit que l'anneau soit atomique et ses idéaux principaux à droite contenant un $cR \neq 0$ donné forment un sous-treillis du treillis de tous les idéaux à droite, donc on obtient :

Théorème 2 : Tout 2-fir atomique est un anneau factoriel.

2. Avant de donner des exemples il faut éclaircir un peu la notion d'anneau factoriel. Ce que j'ai dit jusqu'à présent ne suffit même pas pour décider si cette notion est symétrique à droite et à gauche (la définition ne l'est pas, à cause du caractère unilatère de la similitude). Donc on va étudier de plus près la notion de similitude.

Commençons par un anneau R quelconque. Soit A un idéal à droite dans R . On définit l'idéalisateur de A comme

$$I(A) = \{x \in R \mid xA \subseteq A\} .$$

Evidemment c'est un sous-anneau de R , en effet c'est le plus grand

sous-anneau dans lequel A est idéal bilatère. On peut donc former l'anneau quotient

$$E(A) = I(A)/A ,$$

qui s'appelle anneau propre (eigenring) de l'idéal A. Quand A est bilatère dans R (par ex. si R est commutatif), $E(A)$ est réduit à R/A. En général on a le

Théorème 3 : (Fitting [35]) Soit A un idéal à droite dans un anneau R quelconque. Alors

(1) $$E(A) \tilde{=} \mathrm{End}_R(R/A) .$$

On le démontre en observant que tout $r \in I(A)$ définit un endomorphisme α_r du module à droite R/A :

(2) $$\alpha_r : \bar{x} \longmapsto \overline{rx} \qquad (\bar{x} \text{ désigne la classe de } x \in R) ,$$

et que l'application $r \longmapsto \alpha_r$ est un homomorphisme d'anneaux :

(3) $$I(A) \longrightarrow \mathrm{End}_R(R/A) .$$

Etant donné $\theta \in \mathrm{End}_R(R/A)$, si $\theta(\bar{1}) = \bar{r}$, alors $\theta(\bar{x}) = \overline{rx} = \alpha_r(\bar{x})$, ce qui montre la surjectivité de (3). Le noyau est visiblement A, donc on obtient (1).

Plus généralement, étant donné des idéaux à droite A, A' de R, tout homomorphisme $R/A' \longrightarrow R/A$ peut être réalisé par un élément $b \in R$ tel que $bA' \subseteq A$. C'est l'application qui envoie

$$x(\mathrm{mod}\ A') \longmapsto bx(\mathrm{mod}\ A).$$

Comme au théorème 3, c'est surjectif si et seulement si $A + bR = R$, et injectif si et seulement si $A' = \{x \in R / bx \in A\}$. Cela nous donne un critère pour l'isomorphisme de R/A et R/A'. Pour les idéaux principaux cela nous donne un critère de similitude. Nous en ajoutons un autre, en omettant la démonstration (voir Cohn [67]) :

Lemme : Soient a, a' des éléments d'un anneau R, tels que ni a, ni a' ne soient diviseurs de zéro à gauche (c'est-à-dire $x \mapsto ax$, $x \mapsto a'x$ sont injectifs).

Alors les trois conditions qui suivent sont équivalentes :

1) a est semblable à a' $(R/aR \tilde{=} R/a'R)$.

2) $aR + bR = R$ et $aR \cap bR = ba'R$ pour un $b \in R$ convenable.

3) Il existe une matrice de la forme $\begin{pmatrix} a & * \\ * & * \end{pmatrix}$ avec inverse de la forme $\begin{pmatrix} * & * \\ * & a' \end{pmatrix}$

Indiquons seulement la démonstration 1) $\Longleftrightarrow$ 2). On a vu que la condition de similitude est $aR + bR = R$ et $a'R = \{x \in R / bx \in aR\}$. Mais cette dernière condition se traduit par $ba'R = bR \cap aR$. Pour passer en sens inverse, il semble qu'on doit exiger que b ne soit pas diviseur de zéro à gauche ; mais la même chose peut être démontrée avec l'hypothèse du lemme.

Cela montre en tout cas que dans un anneau intègre $R/aR \tilde{=} R/a'R$ $\Longleftrightarrow R/Ra \tilde{=} R/Ra'$. Donc la notion d'anneau factoriel est bien symétrique. Cela se voit de façon plus claire encore du point de vue catégorique que nous adopterons plus tard.

Regardons encore le cas spécial d'un 2-fir. La deuxième partie de 2) montre qu'on a une relation

$$ab' = ba' \quad , \tag{4}$$

où a', b' sont sans facteur commun à droite. A cause de la première partie de 2), a, b sont sans facteur commun à gauche. Disons qu'une telle relation est étrangère (coprime). Maintenant, soit (4) une relation étrangère (et $ab' \neq 0$). Alors $aR + bR = dR$ (parce que R est 2-fir, et d est unité, donc $aR + bR = R$. De plus $aR \cap bR = mR$, et ici $m = ba'$ parce que a', b' sont étrangers à droite. Donc on a le

Lemme : Dans un 2-fir R, deux éléments a, a' $(\neq 0)$ sont semblables si et seulement si il existe une relation étrangère de la forme (4).

Bibliographie à la fin de la Conférence III.

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 20 du 21 avril 1969

(suite) par P.M. COHN

-:-:-:-:-:-:-

3. Nous avons vu que la définition d'anneau factoriel se réduit à la notion usuelle dans le cas commutatif. Regardons comment elle s'en distingue dans le cas général.

Quand on a deux factorisations complètes d'un élément c :

(1) $$c = a_1 \dots a_r = b_1 \dots b_r \ ,$$

on sait qu'il y a une permutation $i \longmapsto i'$ tel que $a_i \sim b_{i'}$. Mais en général on n'a pas les propriétés suivantes qui sont valables dans le cas commutatif :

α) a_i est associé à $b_{i'}$ et

β) on peut obtenir c en rangeant les b_i dans l'ordre $b_{1'}, b_{2'}, \dots b_{r'}$.

Pour le cas des 2-fir on a quand même quelques précisions sur α et β. Car on sait que deux facteurs consécutifs dans (1), disons $a_{i-1}a_i$, peuvent être transposés précisément quand on a une relation étrangère :

(2) $$a_{i-1}a_i = a'_i a'_{i-1} \ .$$

Donc la permutation dont il est question dans β est produit de transpositions comme (2), que nous convenons d'appeler "transpositions maximales".

D'ailleurs les transpositions maximales entrent aussi dans α, car deux éléments a, a' dans un 2-fir sont semblables si et seulement si il y a une relation étrangère

$$ab' = ba' \ .$$

On peut étudier sous quelles conditions α ou β seraient encore valables dans le cas non-commutatif. Nous allons plutôt regarder le cas où l'ordre est complétement fixe. On dit qu'un élément c d'un anneau factoriel est à factorisation rigide (ou tout court : c est rigide) si étant donné deux factorisations de c comme dans (1), on a forcément :

$$b_i = u_{i-1}^{-1} a_i u_i \qquad (u_i \in U(R) , \quad u_o = u_n = 1) .$$

On a le lemme suivant, dont une forme plus faible a été remarquée par Košević [66]:

Lemme : Soit R un 2-fir atomique, et $x \in R$. Alors si les atomes d'une factorisation complète de R engendrent un idéal bilatère propre de R, x est rigide.

Pour le démontrer, il suffit de montrer qu'aucune transposition ne peut se produire. Soit donc $ab' = ba'$ une transposition maximale, où a, b' appartiennent à la factorisation complète de x donnée, et donc a, $b' \in \mathcal{U}$ où $\mathcal{U}$ est un idéal bilatère propre. On sait qu'alors a, b' figurent dans deux matrices mutuellement inverses (Cohn [67]) :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad A^{-1} = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} .$$

Donc $1 = d'a - b'c \in \mathcal{U}$, ce qui est une contradiction.

Un anneau R s'appelle anneau factoriel rigide, si R est factoriel et tout élément est rigide. On peut décrire tous les anneaux factoriels rigides comme suit. Rappelons qu'un anneau local est un anneau dont le complément de $U(R)$ (c'est-à-dire les non-unités) forment un idéal. Un tel anneau peut aussi être caractérisé par la propriété : $a \notin U(R) \Longrightarrow 1 + a \in U(R)$. Maintenant on a :

Théorème 4 : Pour un anneau R quelconque les deux assertions suivantes sont équivalentes :

i) R est 2-fir atomique, et local,

ii) R est anneau factoriel rigide.

Démonstration :

i ⟹ ii : Quand R est local tous ses atomes appartiennent à l'idéal maximal, donc aucune transposition ne peut se produire, c'est-à-dire R est rigide.

ii ⟹ i : Soit R un anneau factoriel rigide, alors il est atomique

Pour montrer que R est local, prenons $a \notin U(R)$, et posons $a = pa_1$ où p est un atome. On a la relation évidente :

$$(1 + a)p = (1 + pa_1)p = p(1 + a_1 p) .$$

Si $1 + a \notin U(R)$ alors par rigidité $1 + a = pb$, donc $p(b - a_1) = 1$, et p serait inversible, ce qui est absurde. Donc $1 + a \in U(R)$. Il reste à montrer que R est 2-fir. On sait déjà qu'il est intègre. Supposons $aR \cap bR \neq 0$, $ab' = ba' \neq 0$; alors par rigidité on a $a = p_1 \dots p_r$, $b = p_1 \dots p_s$ (quitte à multiplier par des unités à droite). Si $r \leq s$, alors $b \in aR$, donc $aR + bR = aR$. De même, si $r \geq s$, on obtient $aR + bR = bR$. Donc $aR + bR$ est principal, ce qu'il fallait montrer.

L'observation que l'hypothèse "R 2-fir" n'intervient pas dans la démonstration ii) ⟹ i) , est due à Bowtell [67] . Exemples d'anneaux factoriels rigides.

1) Tout anneau à valuation discrète (même non-commutatif). Car évidemment c'est un anneau principal local, donc 2-fir atomique local . D'ailleurs, tout anneau factoriel rigide commutatif est à valuation discrète.

2) L'anneau de séries formelles à plusieurs indéterminées non-permutables, sur un corps. Cet anneau s'obtient en complétant une algèbre associative libre. Notons l'algèbre libre R , sa complétée $\hat{R}$, alors on peut trouver dans $\hat{R}$ un mode de calcul qui s'appelle l'algorithme inverse faible (cf. Cohn [62] grâce auquel nous pouvons montrer que $\hat{R}$ est un semi-fir atomique, donc un 2-fir atomique, et comme R est aussi un

anneau local, on obtient donc un anneau factoriel rigide. D'autre part, $\hat{R}$ n'est pas un fir (cela se montre à partir d'un théorème de S. Chase, voir Cohn [66] pour la méthode). Donc on est amené au

Problème : Trouver un anneau factoriel rigide qui est un fir, sans être principal.

4. Comment vérifie-t-on qu'un anneau donné est un 2-fir ? Ici, comme dans le cas commutatif, l'outil le plus pratique est l'algorithme d'Euclide. Pour simplifier un peu, nous nous bornons au cas d'anneaux valués, ce qui suffira pour la discussion de la factorisation.

On considère un anneau R avec une fonction v, à valeurs dans $\mathbb{Z}^+ \cup \{-\infty\}$, qui satisfait à :

V.1. $v(0) = -\infty \qquad v(x) \geqslant 0 \quad$ pour $\quad x \neq 0$,

V.2. $v(x+y) \leqslant \max\{v(x), v(y)\}$,

V.3. $v(xy) = v(x) + v(y)$.

On dit que R admet un stathme élémentaire si, étant donné $a, b \in R$ tels que $v(a) \geqslant v(b)$, on peut trouver $c \in R$ tel que

(1) $\qquad v(a - bc) < v(a)$.

Visiblement c'est vrai quand R est euclidien. Inversement, si on a (1), prenons $q \in R$ tel que $r = a - bq$ soit de valeur minimale. Si $v(r) \geqslant v(b)$, il existerait $c \in R$ tel que $v(r - bc) < v(r)$, donc $v(a - b(q+c)) < v(r)$ en contradiction avec l'hypothèse faite sur r. Donc on a :

(2) $\qquad a = bq + r \qquad v(r) < v(b)$.

qui est le stathme sous sa forme habituelle.

Pour le traduire au cas non-commutatif, on doit postuler (1), moyennant une

hypothèse sur a et b (comme le 2-fir était défini par la principalité de l'idéal $aR + bR$, moyennant une hypothèse sur a, b, à savoir que $aR \cap bR \neq 0$). Ainsi on est conduit à la

Définition. Un anneau R valué (comme ci-dessus), satisfait à l'algorithme faible à 2 termes (brèvement : AF_2) si les conditions $v(a) \geqslant v(b)$ et $v(ab' - ba') < v(ab')$ $(a,b, a', b' \in R)$, impliquent l'existence de $c \in R$ tel que $v(a - bc) < v(a)$.

Remarquons (sans entrer dans les détails) que ce n'est qu'un premier cas d'une chaîne de conditions AF_n $(n = 1, 2, \ldots)$ dont la conjonction est l'algorithme faible proprement dit (Cohn [63']).

Nous nous intéressons ici à AF_2 parce qu'on peut l'utiliser pour prouver la propriété de 2-fir. Donc soit R un anneau valué qui satisfait à AF_2. Etant valué, R est intègre. Considérons $a, b \in R$; nous choisissons $a_1, b_1 \in R$ tels que $a_1R + b_1R = aR + bR$ et $v(a_1) + v(b_1)$ atteint sa valeur minimum. Si c'est $-\infty$, alors l'un des deux éléments, a_1, b_1 est nul et l'idéal est principal. Dans le cas contraire, on affirme que a_1, b_1 sont linéairement indépendants à droite. Car sinon, on aurait $a_1b' - b_1a' = 0$, donc par AF_2, il existe $c \in R$ tel que $v(a_1 - b_1c) < v(a_1)$ (si par exemple $v(a_1) \geqslant v(b_1)$). Donc on a $a_1R + b_1R = (a_1 - b_1c)R + b_1R$ ce qui contredit le choix de a_1, b_1 parce que $v(a_1 - b_1c) + v(b_1) < v(a_1) + v(b_1)$. Cette contradiction montre que a_1, b_1 sont linéairement indépendants, donc R est un 2-fir. De plus, R est atomique. Pour le voir, montrons d'abord que $v(x) = 0$ implique $x \in U(R)$. Car on a $x.1 - 1.x = 0$ et $v(x) = v(1)$, donc il existe $y \in R$ tel que $v(1 - xy) < 0$; cela veut dire $1 - xy = 0$, donc comme R est intègre, $x \in U(R)$. Tout élément non-unité est donc de valeur au moins 1. Etant donné $c \in R^*$ et une factorisation de c en non-unités $c = a_1 \ldots a_r$, on voit donc que $r \leqslant \Sigma v(a_i) = v(c)$, ce qui nous donne une borne

pour r . En somme, on a démontré :

Théorème 5 : Tout anneau valué R à algorithme faible à 2 termes est 2-fir atomique.

Corollaire : Tout anneau valué R à algorithme faible à 2 termes est factoriel.

Par exemple l'algèbre associative libre sur un corps satisfait à l'algorithme faible, donc aussi à AF_2 (cf. Cohn [61]) , et cela montre que c'est un anneau factoriel. Pour donner un exemple d'un élément à deux factorisations essentiellement différentes, prenons dans l'algèbre libre sur x , y , l'élément

$$xyx + x = (xy + 1)x = x(yx + 1) \quad . \tag{1}$$

Cela nous montre le type de factorisation qui apparaît. Pour étudier les relations comme (1) en détail , il faut regarder l'algorithme de plus près.

Soit R un anneau valué à AF_2 et soit donné une relation quelconque

$$ab' = ba' \neq 0 \quad , \tag{2}$$

(pas forcément étrangère). Pour commencer on choisit $q_1 \in R$ tel que $r_1 = a - bq_1$ est de valeur minimum. Alors

$$a = bq_1 + r_1 \qquad v(r_1) < v(b) \quad . \tag{3}$$

Quand on substitue dans (2) , on obtient $r_1 b' = (a - bq_1)b' = b(a' - q_1 b')$. Donc si on met $r_1' = a' - q_1 b'$, on a

$$r_1 b' = br_1' \quad . \tag{4}$$

De plus, $v(b) + v(r_1') = v(r_1) + v(b') < v(b) + v(b')$, donc $v(r_1') < v(b')$. Cela montre qu'on a une symétrie parfaite des deux côtés. Maintenant on recommence avec (4). En somme on obtient les chaînes suivantes :

$$(5)\quad \begin{cases} a = bq_1 + r_1 & a' = q_1 b' + r'_1 & r_1 b' = b r'_1 \\ b = r_1 q_2 + r_2 & b' = q_2 r'_1 + r'_2 & r_2 r'_1 = r_1 r'_2 \\ r_1 = r_2 q_3 + r_3 & r'_1 = q_3 r'_2 + r'_3 & r_3 r'_2 = r_2 r'_3 \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ r_{n-2} = r_{n-1} q_n + r_n & r'_{n-2} = q_n r'_{n-1} + r'_n & r_n r'_{n-1} = r_{n-1} r'_n \\ r_{n-1} = r_n q_{n+1} & r'_{n-1} = q_{n+1} r'_n & r_{n+1} = r'_{n+1} = 0 \,. \end{cases}$$

La chaîne doit se terminer parce que $v(r_1) > v(r_2) > \ldots$ est une série d'entiers positifs strictement décroissants. On a noté r_{n+1} le premier reste nul à droite (il est facile à vérifier que r'_{n+1} est aussi le premier reste nul à gauche). Remarquons que les restes de deux côtés sont en général différents, tandis que les quotients q_i sont les mêmes des deux côtés.

La première équation du système (5) s'écrit en forme de matrices comme suit :

$$(a\ b) = (b\ r_1) \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} .$$

Cela nous suggère de poser, pour $x \in R$ quelconque,

$$P(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \quad \text{avec inverse} \quad P(x)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -x \end{pmatrix} .$$

Alors la première colonne (5) peut s'écrire :

$$(6)\qquad (a\ b) = (r_n\ 0)\, P(q_{n+1})\, P(q_n) \cdots P(q_1) ,$$

donc on a $a = r_n a_0$, $b = r_n b_0$. Ces équations montrent que r_n est facteur commun à gauche de a et b. Pour voir que c'est le plus grand tel facteur, multiplions (6) par $[P(q_{n+1}) \cdots P(q_1)]^{-1}$. Alors on obtient $(a\ b)Q = (r_n\ 0)$ pour une certaine matrice Q, donc $r_n = ax - by$, ce qui démontre l'assertion. De plus on voit sur ces équations que $aR + bR = r_n R$. On a de la même manière $Ra' + Rb' = Rr'_n$.

BIBLIOGRAPHIE à la fin de la conférence III.

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

- Conférence n° 21 du 28 avril 1969 -

FACTORISATIONS (III) par P.M. COHN

-:-:-:-:-:-:-:-

Quand on a un produit de matrices $P(t_i)$, les éléments du produit s'expriment ainsi : on prend des indéterminées non-commutatives $t_1, t_2, \ldots$ à coefficients entiers et on définit des polynômes $p_{-1}, p_0, p_1 \ldots$ par des équations de récurrence :

(7) $\qquad p_{-1} = 0 , \qquad p_0 = 1$

et

(8) $\quad p_n(t_1,\ldots,t_n) = p_{n-1}(t_1,\ldots,t_{n-1})t_n + p_{n-2}(t_1,\ldots,t_{n-2}) .$

Parfois, on omet l'indice dans les p_i. Il est facile de voir que

$$P(t_1)\ldots P(t_n) = \begin{pmatrix} p(t_1,\ldots,t_n) & p(t_1,\ldots,t_{n-1}) \\ p(t_2,\ldots,t_n) & p(t_2,\ldots,t_{n-1}) \end{pmatrix}$$

Donc p_n peut aussi être défini par (7) et

(9) $\quad p_n(t_1,\ldots,t_n) = t_1 p_{n-1}(t_2,\ldots,t_n) + p_{n-2}(t_3,\ldots,t_n) .$

Les premiers sont : $p_1 = t_1$, $p_2 = t_1t_2 + 1$, $p_3 = t_1t_2t_3 + t_1 + t_3$,

$p_4 = t_1t_2t_3t_4 + t_1t_2 + t_3t_4 + t_1t_4 + 1$. Ils sont liés par les relations suivantes, bien connues (dans le cas commutatif) dans la théorie des fractions continues :

$$p(t_1,\ldots,t_n)\,p(t_{n-1},\ldots,t_1) - p(t_1,\ldots,t_{n-1})\,p(t_n,\ldots,t_1) = 0 ,$$

$$p(t_1,\ldots,t_n)\,p(t_{n-1},\ldots,t_2) - p(t_1,\ldots,t_{n-1})\,p(t_n,\ldots,t_2) = (-1)^n .$$

En appliquant l'algorithme faible à deux factorisations d'un élément donné, on obtient le

Théorème 6 : Soit R un anneau filtré avec AF_2 (par exemple l'algèbre associative libre). Alors le monoïde R^* est engendré par $U(R)$ et des atomes de R, et un ensemble de relations définissantes est donné par les équations :

$$p(a_1,\dots,a_n)\, p(a_{n-1},\dots,a_1) = p(a_1,\dots,a_{n-1})\, p(a_n,\dots,a_1) ,$$

où $n = 2, 3, \dots$ et les $a_1,\dots,a_n$ parcourent R.

Notons aussi que deux éléments a, a' dans un anneau à AF_2 sont semblables si et seulement si ils ont la forme

$$\alpha p(a_1,\dots,a_n) \quad , \quad p(a_n,\dots,a_1)\beta \quad , \quad \alpha,\beta \in U(R) ,$$

où $a_1, \dots, a_n$ sont non-inversibles.

5. Revenons maintenant à un anneau R quelconque. On a vu des raisons pour étudier la factorisation d'un élément c par le module R/cR. Si on veut que les résultats s'appliquent aux anneaux non-intègres on doit supposer non seulement que c soit non-diviseur de zéro, mais que ses facteurs ne le sont pas non plus. Convenons d'appeler un tel élément régulier.

Un module M sur R est dit strictement cyclique ou $\mathcal{C}$-module, s'il est de la forme R/cR où c est régulier. La sous-catégorie pleine de la catégorie mod-R dont les objets sont des modules strictement cycliques est notée $\mathcal{C}$ ou $\mathcal{C}_R$, et ${}_R\mathcal{C}$ est définie d'une façon analogue à partir de R-mod.

Un homomorphisme de $\mathcal{C}_R$,

(1) $$f : R/aR \longrightarrow R/bR ,$$

est donné par un élément $c \in R$ tel que

(2) $\qquad ca = bc'$

pour un c' convenable de R. Par symétrie, c' définit un homomorphisme

$$f_* : {}_R/_{Rb} \longrightarrow {}_R/_{Ra} .$$

L'élément c n'est pas univoquement déterminé par f, mais si on a $c_1 = c + bu$, alors $c_1 a = ca + bua = bc' + bua = b(c' + ua)$ et il est clair que $c' + ua$ donne le même homomorphisme f_*. De plus la correspondance $f \longrightarrow f_*$ est un foncteur contre-variant de $\mathcal{C}_R$ à ${}_R\mathcal{C}$. Si on répète la construction, on obtient un foncteur ${}_R\mathcal{C} \longrightarrow \mathcal{C}_R$ et il est facile de voir que $f_{**} = f$. Donc on a le

Théorème 7 : Dans un anneau R quelconque, la catégorie ${}_R\mathcal{C}$ est duale de la catégorie $\mathcal{C}_R$.

De cette affirmation, apparemment triviale, on peut tirer des conséquences intéressantes :

Corollaire 1. (Fitting [36]) : Si a, a' sont des éléments réguliers alors ${}_R/_{aR} \tilde{=} {}_R/_{a'R} \iff {}_R/_{Ra} \tilde{=} {}_R/_{Ra'}$.

Cela montre que la relation de similitude est symétrique à droite et à gauche. C'est même vrai pour des a, a' non-diviseurs de zéro (comme le montre d'ailleurs Fitting) ; évidemment on peut le prouver en remplaçant la catégorie $\mathcal{C}_R$ par la catégorie de tous les ${}_R/_{aR}$ avec a non-diviseur de zéro. Par contre, le Corollaire 1 n'est plus vrai si a, a' sont des éléments quelconques, comme le montrent des exemples dus à Fitting.

Corollaire 2 : L'anneau propre de Ra est opposé à celui de aR :

$$E(Ra) \tilde{=} E(aR)^0 .$$

Car ce sont des anneaux d'endomorphismes d'objets correspondants dans des catégories anti-isomorphes.

La catégorie $\mathcal{C}_R$ a l'inconvénient pour une étude plus détaillée de la factorisation, de ne pas admettre des sommes directes. Ce dont nous avons besoin est une catégorie additive (peut-être même abélienne) qui comprend $\mathcal{C}_R$. Pour cela nous devons nous limiter au cas d'un semi-fir. Sur un semi-fir R, tout module M de présentation finie forme partie d'une suite exacte

$$0 \longrightarrow R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0 \ .$$

Par le lemme de Schamuel (Mac Lane [63], le nombre $n-m$ ne dépend que de M. On pose $\chi(M) = n-m$ et on l'appelle caractéristique de M. Si M est de type fini, mais pas de présentation finie, on pose $\chi(M) = -\infty$, autrement (quand M n'est pas de type fini), $\chi(M) = \infty$.

D'abord, notons le

Lemme : Pour toute suite exacte courte de modules sur un semi-fir :

$$0 \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

on a

$$\chi(M) = \chi(M') + \chi(M'')$$

avec les conventions habituelles sur ∞, et les règles :

(i) si $\chi(M'') = \infty$, alors $\chi(M) = \infty$,

(ii) si $\chi(M'') = -\infty$, et $\chi(M') = \infty$, il n'y a pas de conclusion.

Démonstration : Supposons pour commencer que M est de type fini, à n générateurs

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & R^{\alpha} & \longrightarrow & R^{\alpha} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & R^{\beta} & \longrightarrow & R^{n} & \longrightarrow & M'' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
\end{array}$$

Par le lemme de 3×3 on peut compléter le diagramme par les flèches pointées de la première colonne, de façon qu'il soit commutatif et exact. Maintenant l'équation

$$n - \alpha = n - \beta + (\beta - \alpha)$$

nous donne la conclusion voulue quand β est fini. Sinon, on a $\chi(M'') = -\infty$, et si on n'est pas dans le cas (ii), alors M' est aussi de type fini et on peut faire la démonstration en prenant des résolutions simultanées de M' et M''.

Il reste le cas où M n'est pas de type fini, donc $\chi(M) = \infty$. Par (i), nous pouvons supposer que $\chi(M'') < \infty$ et il faut montrer que $\chi(M') = \infty$. Mais c'est clair: si M' et M'' sont de type fini M l'est aussi.

Définition : Un module M sur un semi-fir est dit de torsion si

(i) $\chi(M) = 0$ et

(ii) pour tout sous-module M' de M, $\chi(M') \geq 0$.

On aurait pu également définir les modules de torsion par (i) et

(iii) pour tout quotient M'' de M, $\chi(M'') \leq 0$.

Cela donne la définition habituelle des modules de type fini sur un anneau principal, car alors (ii) est automatique. Par contre, pour les semi-firs (et même les firs) (ii) n'est pas superflu, comme le montre l'exemple d'une algèbre associative libre : $k\langle x_1, x_2, \ldots\rangle$. Soit M engendré par e_1, e_2, e_3 avec les relations $e_1 x_1 + e_2 x_2 + e_3 x_3 = 0$, $e_3 x_4 = e_3 x_5 = 0$. Alors $\chi(M) = 0$, $\chi(e_3 R) = -1$.

On note T_R la sous-catégorie pleine de Mod-R dont les objets sont les modules de torsion (R étant un semi-fir). Par exemple, tout $\mathcal{C}$-module est dans T_R. Inversement, soit $M \in T_R$ monogène, alors on a une présentation

$$0 \longrightarrow R \xrightarrow{\lambda a} R \longrightarrow M \longrightarrow 0$$

donc $M = R/aR$ et $M \in \mathcal{C}_R$. Donc $\mathcal{C}_R$ n'est autre que la partie monogène de T_R.

En général, un sous-module d'un module de torsion n'est pas nécessairement de torsion. Toutefois, on a le

Lemme : Etant donné une suite exacte courte

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \ ,$$

si deux quelconques de M, M', M'' sont de torsion, alors le troisième l'est aussi.

Démonstration : Deux de $\chi(M')$, $\chi(M'')$ sont 0, donc aussi le troisième. Il reste à vérifier la deuxième condition :

a) M', $M'' \in T_R$. Si $N \subseteq M$, on a $(N+M')/M' \cong N/N \cap M'$.

Le premier membre est dans M'', donc de caractéristique ≥ 0, et

$$\chi(N) = \chi(N)/N \cap M') + \chi(N \cap M') \geq 0 \quad \text{parce que} \quad N \cap M' \subseteq M' \ .$$

b) $M \in T_R$. Alors tout sous-module de M' est sous-module de M, donc satisfait à (ii), tandis que tout quotient de M'' est quotient de M, donc satisfait à (iii).

Cela nous met en état de démontrer le :

Théorème 8 : T_R est une catégorie abélienne.

Démonstration : Nous savons que T_R est une sous-catégorie pleine de la catégorie abélienne mod-R. La somme de deux modules de T_R l'est encore, et pour voir que T_R est abélienne il suffit de vérifier que ker f, coker f, sont de torsion, pour tout morphisme f. Soit donné $f : M \longrightarrow N$ dans T_R, alors $\chi(\text{im } f) \geq 0$, $\chi(\text{coim } f) \leq 0$ parce que $\text{coim } f = M/\ker f$ est quotient de M. Mais $\text{im } f \cong \text{coim } f$, donc $\chi(\text{im } f) = 0$, et tout sous-module de im f, étant dans N, est de caractéristique ≥ 0 ; donc im f est de torsion et par le lemme précédent, ker f, coker $f \in T_R$.

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n°22 du 12 mai 1969

FACTORISATIONS (IV) par P.M. COHN

-:-:-:-:-:-:-:-

Corollaire : Soit M un objet simple de la catégorie T_R (nous disons : M est un module T-simple). Alors $End_R(M)$ est un corps (gauche) .

Ce n'est que le lemme de Schur.

Par exemple, l'anneau propre d'un atome dans un semi-fir (même dans un 2-fir) est un corps gauche.

Regardons de plus près la relation entre factorisationset extensions. Soit $M \in T_R$ à n générateurs, donc on a une suite exacte

$$0 \longrightarrow R^n \xrightarrow{\lambda} R^n \longrightarrow M \longrightarrow 0 \ ,$$

où λ est une multiplication à gauche par une matrice $n \times n$, disons $c : x \longrightarrow cx$, où x est une colonne. Si $c = ab$ est une factorisation de c , on a la suite exacte

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \ ,$$

où $M' \cong aR^n/abR^n \cong R^n/bR^n$ est un sous-module, avec quotient $M'' \cong R^n/aR^n$. Cela montre que $\chi(M')$, $\chi(M'')$ sont finis et comme M est de torsion

(1) $$\chi(M'') = -\chi(M') \leqslant 0 \ .$$

Pour montrer que a est régulier à droite, nous utilisons le

Lemme : Si A est une matrice $m \times n$ sur un semi-fir R, alors l'annulateur à droite de A (dans R^n) est de la forme ER_n, où $E = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Démonstration : Soit N l'annulateur $R^n/N \tilde{=} AR^n$; le 2ème membre est libre donc

(2) $\qquad R^n = N \oplus N'$

où $N \tilde{=} R^r$, avec $r \leqslant n$. Prenons une base de R^n adaptée à la décomposition (2) : cela donne $N = ER^n$, où E est comme indiquée.

Revenons à la factorisation $c = ab$. Si $ax = 0$, alors l'annulateur de a est $(1 - e)R^n$, donc $a = ae = (c_1, \ldots, c_r, 0 \ldots 0)$. Mais cela veut dire que $\chi(M') = n-r \geqslant 0$ ce qui n'est possible (tenant compte de (1)) que quand $r = n$. Cela montre que a est régulier à droite. De la même façon, b est régulier à droite, parce que $c = c.1$ l'est. Si b n'est pas régulier à gauche, alors $b = fb$ pour un idempotent f et $c = ab = afb$ où af n'est pas régulier à droite, ce qui est une contradiction. Donc c est régulier.

Inversement, si M n'est pas de torsion, ou bien $m \neq n$, ou bien, $m = n$, mais on a un sous-module N tel que $\chi(N) = -r < 0$. Soit M donné par la suite exacte

$$0 \longrightarrow R^n \xrightarrow{\lambda} R^n \xrightarrow{\mu} M \longrightarrow 0 .$$

On voit que $\mu^{-1}(N)$ est un sous-module de R^n, donc il est libre, et $\mu^{-1}(N)/\operatorname{im}\lambda \tilde{=} N$. Donc on a

$$\chi(\mu^{-1}(N)) = \chi(N) + n = n - r ,$$

ce qui montre $\mu^{-1}(N) = R^{n-r}$. Comme $\operatorname{im}\lambda \subseteq \mu^{-1}(N)$, on a une factorisation de λ

$$\begin{array}{ccc} R^n & \xrightarrow{\lambda} & R^n \\ & \searrow \quad \nearrow & \\ & R^{n-r} & \end{array}$$

Cela nous donne $c = ab$ où a est $n \times (n-r)$, et b est $(n-r) \times n$. Si on complète a et b par des colonnes (resp. lignes) de zéros pour avoir des matrices ,

$n \times n$, soit $a_1 = (a\ 0)$, $b_1 = \binom{b}{0}$ alors $c = a_1 b_1$ où a_1 est diviseur de zéro (aussi bien que b). Donc c n'est pas régulier et on a démontré le

Théorème 9 : Les modules de torsion sur un semi-fir sont précisément les modules $M = R^n / cR^n$ définis par une matrice régulière c .

Exemple : $R = k\langle x_1, x_2, \ldots \rangle$, $M = e_1 R + e_2 R + e_3 R$ avec les relations définissantes $e_1 x_1 + e_2 x_2 + e_3 x_3 = 0$, $e_3 x_4 = e_3 x_5 = 0$. $\chi(M) = 0$, mais $\chi(e_3 R) = -1$, donc M n'est pas de torsion. La factorisation correspondante est

$$\begin{pmatrix} x_1 & 0 & 0 \\ x_2 & 0 & 0 \\ x_3 & x_4 & x_5 \end{pmatrix} = \begin{pmatrix} x_1 & 0 & 0 \\ x_2 & 0 & 0 \\ x_3 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x_4 & x_5 \\ 0 & 0 & 0 \end{pmatrix} ,$$

On ne peut pas espérer une vraie théorie de la factorisation sur un semi-fir, parce que cela n'existe même pas dans le cas commutatif (où semi-fir = anneau de Bezout). Donc il faut ajouter des hypothèses de finitudes : en effet, il suffit de prendre un fir pour R . Il est intéressant de constater que cela va nous donner des conditions de chaînes, vu que les firs comprennent des anneaux comme les algèbres libres associatives (même à une infinité d'indéterminées), l'algèbre de groupe d'un groupe libre quelconque etc....

Théorème 10 : Soit R un fir à droite. Alors R satisfait à la condition maximum pour les idéaux à droite à n générateurs.

Démonstration : Au lieu de regarder les idéaux à n générateurs dans R nous regardons les idéaux principaux dans R_n . Comme il y a une correspondance biunivoque entre ces deux classes d'idéaux :

$$(a_1,\dots,a_n)R \longleftrightarrow \begin{pmatrix} a_1 & \dots & a_n \\ 0 & \dots & 0 \\ 0 & \dots & 0 \end{pmatrix} R_n$$

il suffit de démontrer le théorème pour le cas des idéaux principaux à droite dans R_n. Il est vrai que R_n n'est plus un fir, mais il existe un module projectif P tel que $P^n \cong R_n$ (comme R_n-modules, prendre $P = R^n$), et tout idéal à droite dans R_n est somme directe d'exemplaires de P (voir Cohn [67]).

On pose $T = R_n$ et on considère une chaîne

$$a_1T \subseteq a_2T \subseteq \dots \tag{1}$$

Si la chaîne se termine, la réunion est principale. Sinon, elle est somme d'une infinité d'exemplaires du projectif minimal P, donc aussi somme infinie d'exemplaires de T, c'est-à-dire libre sur T.

Soit (c_λ) une base pour la réunion de (1), alors $c_1 \in a_kT$, disons

$$c_1 = a_ku .$$

En remplaçant k par un entier plus grand au besoin, on peut supposer que u n'est pas inversible. On a aussi $a_k = \Sigma\, c_\lambda v_\lambda$, donc en multipliant par u,

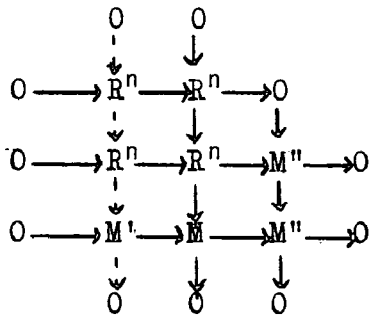
$$c_1 = a_ku = \Sigma\, c_\lambda v_\lambda u .$$

Mais les c_λ forment une base, donc $v_1u = 1$. Maintenant 1 est régulier, donc u n'est pas diviseur de zéro, et comme $(uv_1-1)u = 0$, il s'ensuit que u est inversible, ce qui est une contradiction. Cela démontre le théorème.

Corollaire : La catégorie T_R des modules de torsion sur un fir à droite est noethérienne (c'est-à-dire tous ses objets satisfont à la condition maximale.

D'après le théorème, le corollaire sera démontré si on établit que tout sous-module de torsion d'un module de torsion à n générateurs est encore à n générateurs.

Soit $M \in T_R$ à n générateurs, et M' un sous-module de torsion. Alors $M'' = M/M'$ est de torsion et on a le diagramme suivant, qu'on a utilisé déjà :



On peut le compléter par les flèches pointées, ce qui montre bien que M' est à n générateurs, donc la conclusion.

Pour une théorie complète de la factorisation, il nous faut encore la condition minimale. Cela s'obtient à partir d'une dualité qui étend ce qu'on a vu pour les modules strictement cycliques. Pour faire la même chose ici, nous nous servons du foncteur Ext , qui permet de le faire d'une manière agréable.

Commençons par le cas un peu plus général d'un module lié, c'est-à-dire d'un module M qui n'admet pas de fonctionnelle linéaire non zéro, ou encore $M^* = 0$ où $M^* = \mathrm{Hom}(M, R)$. Prenons un module M lié, de présentation finie :

$$0 \longrightarrow R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0 \ ,$$

et appliquons le foncteur $\mathrm{Hom}(-,R)$:

$$0 \longrightarrow M^* \longrightarrow (R^n)^* \longrightarrow (R^m)^* \longrightarrow \mathrm{Ext}(M,R) \longrightarrow \mathrm{Ext}(R^n,R) \longrightarrow \ldots .$$

cela est la définition même de Ext (une définition au moins). On sait que $\mathrm{Ext}(R^n,R) = 0$, tandis que $(R^n)^* \tilde{=} R$ et $M^* = 0$ par hypothèse. Donc on obtient (en écrivant $\hat{M} = \mathrm{Ext}(M,R)$) la suite exacte

$$0 \longrightarrow R^n \longrightarrow R^m \longrightarrow \hat{M} \longrightarrow 0 \ .$$

Quand on applique $\mathrm{Hom}(-, R)$ encore une fois, et quand on considère l'application

canonique $M \longrightarrow M^{**}$ pour un module quelconque, on a la diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^m & \longrightarrow & R^n & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ (\hat{M})^* & \longrightarrow & R^m & \longrightarrow & R^n & \longrightarrow & \hat{M} & \longrightarrow & 0 \end{array}$$

Mais les flèches $R^k \longrightarrow R^k$ sont des isomorphismes. Donc par le lemme de cinq, les autres flèches verticales le sont aussi, et on a $(\hat{M})^* = 0$, donc $\hat{M}$ est lié, et $\hat{\hat{M}} \cong M$, ce qui nous donne la dualité voulue. Nous nous passons des détails nécessaires pour l'établir et nous énonçons le

Théorème 11 : Le foncteur $\mathrm{Ext}(-, R)$ établit une dualité entre T_R et ${}_RT$, pour un semi-fir R.

Ce théorème est immédiat une fois qu'on est persuadé que tout module de torsion est lié. Donc soit $f : M \longrightarrow R$ un homomorphisme non-nul. Alors $M/\ker f \cong \mathrm{im}\, f$ est libre, donc on a $M = \ker f \oplus F$ où $F \cong \mathrm{im}\, f$ est libre. Mais F est de rang $\chi(M) - \chi(\ker f) \leqslant 0$ parce que M est de torsion, donc $F = 0$ et $f = 0$. Cela nous montre que M est lié.

Soit R un fir (bilatère). Alors ${}_RT$ est noethérienne, donc par dualité T_R est artinienne (i.e. condition minimum pour les sous-objets). Avec le corollaire du théorème 10, cela démontre le

Corollaire : La catégorie T_R des modules de torsion sur un fir(bilatère) est noethérienne et artinienne, donc tout objet a une longueur de composition finie.

Rappelons-nous que toute chaîne maximale

$$M \supset M_1 \supset \ldots \supset M_k \supset 0$$

correspond à une factorisation complète de l'élément régulier qui définit M. On peut généraliser la définition d'anneau factoriel comme suit :

Si R est un anneau quelconque et S un ensemble multiplicativement fermé,

d'éléments réguliers, tel que tout facteur d'un élément de S est encore dans S (i.e. S est saturé), on dit que S est factoriel dans R si tout élément de S est inversible ou admet une factorisation complète, et deux telles factorisations sont isomorphes. Avec cette définition on a le

Théorème 12 : Soit R un fir, et $n \geq 1$. Alors l'ensemble des éléments réguliers de R_n est factoriel.

Pour $n = 1$ cela nous redonne le fait que R est un anneau factoriel (qui correspond aux propriétés de la catégorie $\mathcal{C}_R$). Pour le cas d'un anneau principal, on retrouve la factorisation des matrices non-singulières. Mais dans ce cas-là on sait, de plus, que toute matrice, est associée à une matrice diagonale. Ce n'est pas forcément vrai pour un fir quelconque. Par exemple sur l'algèbre libre la matrice

$$\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$$

n'est pas associée à une matrice diagonale. On peut même se demander si les anneaux principaux peuvent être caractérisés parmi les firs par cette propriété, c'est-à-dire, si la propriété suivante est vraie :

Si toute matrice régulière sur un fir R est associée à une matrice diagonale, alors R est principal.

J'ignore la réponse.

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 23 du 12 mai 1969

-:-:-:-:-:-

FACTORISATION DANS LES ANNEAUX NON-COMMUTATIFS

par P.M. COHN

-:-:-:-:-:-

5. Dans le cas commutatif, il y a un principe général qui permet de passer de la factorialité de R à celle de $R[X]$, du à NAGATA. Nous convenons d'appeler un élément p d'un anneau R commutatif premier si R/pR est intègre. Il est facile de voir que dans un anneau intègre tout élément premier est un atome, mais non pas inversement. En effet, la réciproque, en présence de la condition maximale pour les idéaux principaux, caractérise les anneaux factoriels. Le théorème de NAGATA peut être énoncé comme suit : (cf. SAMUEL [63])

Soit R un anneau commutatif, intègre et atomique, et S un sous-monoïde de R^*, engendré par des éléments premiers de R. Si le localisé R_S est factoriel, alors R l'est aussi.

La démonstration consiste à vérifier que tout atome de R est premier, soit parce qu'il reste un atome dans R_S (en utilisant la factorialité de R_S) soit parce qu'il divise un élément de S.

La façon dont on se sert de ce théorème pour prouver la factorialité de $\mathbb{Z}[x]$ ou $k[x,y]$ (k un corps) est bien connue. Notre but est d'obtenir un analogue qui nous permettra de traiter les anneaux de la forme $\mathbb{Z}\langle x,y\rangle$. Malheureusement celui-ci n'est pas factoriel. Par exemple, on a :

$$xyx + 2x = x(yx + 2) = (xy + 2)x ,$$

et il est facile de vérifier que $xy + 2$ n'est semblable ni à x ni à $yx + 2$. Si on examine de plus près ce qu'il nous faut pour une généralisation, on trouve que la relation de similitude doit être conservée par le passage de R_S à R. Ici on s'imagine qu'on a localisé par rapport à un monoïde S tel que (R,S) satisfait aux conditions de Ore, par exemple si S est dans le centre de R, ou plus généralement, si S est formé des éléments <u>invariants</u>, i.e. des éléments $c \in R^*$ tels que $cR = Rc$. Le problème est donc d'élargir la notion de similitude, avec un affaiblissement correspondant de la notion de factorialité, de telle sorte qu'elle soit conservée par le passage de R_S à R. Ce problème a été résolu par BRUNGS [69], avec quelques hypothèses supplémentaires, qui permettent néanmoins de traiter le cas $\mathbb{Z}\langle x,y\rangle$. Nous suivons une route légèrement différente, qui donne des résultats un peu plus symétriques (cf. COHN [69]).

Soit R un anneau intègre. Nous considérons la catégorie $\mathcal{C}_R$ des modules strictement cycliques, et nous disons que $a, a' \in R$ sont <u>monosemblables à droite</u>, s'il existe des monomorphismes dans $\mathcal{C}_R$:

(1) $\qquad f : R/aR \longrightarrow R/a'R \qquad\qquad g : R/a'R \longrightarrow R/aR .$

De la même façon on définit des éléments <u>monosemblables à gauche</u> et <u>épisemblables (à droite et à gauche)</u>, à l'aide des épimorphismes (1). Il est

clair qu'il s'agit de relations d'équivalence ; de plus, par la dualité entre $\mathcal{C}_R$ et ${}_R\mathcal{C}$, on voit que 'mono à droite' équivaut à 'épi à gauche' . Evidemment deux éléments semblables sont mono et épisemblables (à droite et à gauche). Dans un 2-fir, la réciproque est vraie : soient a, a' des éléments monosemblables à droite dans un 2-fir. Alors il existe des monomorphismes f, g comme dans (1), et ker f $\in \mathcal{C}_R$, donc ker f = 0 . Cela montre que f, g sont des injections. Alors on a une injection gf : $R/_{aR} \longrightarrow R/_{aR}$ et comme $R/_{aR}$ est de longueur finie dans $\mathcal{C}_R$, f et g sont des isomorphismes.

Définition : Un anneau R est dit monofactoriel à droite si R est intègre et atomique et deux factorisations complètes d'un élément quelconque :

$$c = a_1 \dots a_r = b_1 \dots b_s$$

sont telles que s = r et pour une permutation $i \longmapsto i'$, a_i est monosemblable à droite de $b_{i'}$.

Les notions monofactorielles à gauche et épifactorielles (à droite et à gauche) se définissent d'une manière analogue. D'après ce qui a été dit, tout anneau factoriel est aussi mono (et épi) factoriel à droite (et à gauche) ; et un monofactoriel à droite est la même chose qu'un épifactoriel à gauche.

Ces définitions se justifient par le fait qu'une forme du théorème de NAGATA est vraie. D'abord il nous faut une description des monomorphismes dans $\mathcal{C}_R$. Au niveau formel les mono et épimorphismes jouent les mêmes rôles, mais en termes pratiques il se trouve que les monomorphismes sont plus maniables.

Lemme : Soit R un anneau intègre. Un homomorphisme f : M —> N entre $\mathcal{C}$-modules est un monomorphisme (dans la catégorie $\mathcal{C}_R$) si et seulement

si ker f est sans torsion (i.e. $xr = 0$, où $x \in \ker f$, $r \in R$ implique $x = 0$ ou $r = 0$).

Démonstration : Par définition, f est un monomorphisme si et seulement si $f\gamma = 0 \Longrightarrow \gamma = 0$, i.e. $\ker f \supseteq \operatorname{im} \gamma \Longrightarrow \gamma = 0$. Ici $\operatorname{im} \gamma$ peut être n'importe quelle image propre de R . Donc si $\ker f$ est sans torsion, il ne contient aucune image propre de R , sauf 0 , et inversement.

Nous allons utiliser ce lemme pour trouver des conditions sous lesquelles deux éléments monosemblables dans R_S le sont encore dans R . On va prendre pour S un monoïde d'éléments invariants. Pour être plus précis, définissons :

(i) un élément p d'un anneau intègre R est premier si $pR = Rp \neq 0$ et R/pR est intègre.

(ii) Un élément $a \in R$ est étranger à $X \subseteq R$ s'il n'y a aucun élément invariant qui divise à la fois a et un élément de X .

Quand on dit 'a divise b' il y a de l'ambiguité dans le cas non-commutatif, mais cela est résolu si a ou b est invariant ; donc (ii) a un sens. Notons aussi que tout élément premier est invariant.

Lemme : Soit R un anneau intègre atomique, et S un sous-monoïde de R^* engendré par des éléments premiers de R , qui sont facteurs d'éléments centraux, contenus dans S . Etant donné $a, a' \in R$, étrangers à S , si a et a' sont monosemblables à droite dans R_S , ils le sont aussi dans R .

Démonstration : On pose $T = R_S$. L'homomorphisme $f : T/a'T \longrightarrow T/aT$ est donné par $b \in T$ tel que $ba' \in aT$ et

$$\ker f = (aT \cap bT)/ba'T \quad .$$

Nous supposons que f est mono, et montrons qu'il est induit par un mono : $R/a'R \longrightarrow R/aR$.

Posons $b = b_1 s_1^{-1}$, $b_1 \in R$, $s_1 \in S$. Par hypothèse il existe un élément central $c_1 = s_1 d_1 \in S$, donc $b = b_1 q_1 (s_1 d_1)^{-1} = b_2 c_1^{-1}$, et on a

(2) $\quad (aT \cap bT)/ba'T = (aT \cap b_2 T)/b_2 a'T \qquad$ où $\quad b_2 \in R$.

Ensuite nous montrons comment on peut remplacer b_2 par un élément étranger à S . S'il existe un facteur premier p qui divise b_2 et un élément de S , on peut écrire $b_2 = b_3 p$. L'invariance de p donne une équation

(3) $\quad pa' = a_1' p$.

Si on avait $p \mid a_1'$, on pourrait simplifier p à gauche dans (3) , donc $p \mid a'$, ce qui contredit le fait que a' est étranger à S . Donc $p \nmid a_1'$ et tout élément de $a_1'R \cap pR$ est multiple à droite de $a_1'p = pa'$, i.e.

$$a_1'R \cap pR = pa'R \ .$$

Cela nous donne un monomorphisme (même une injection) $R/a'R \longrightarrow R/a_1' R$ et il suffit de trouver un monomorphisme $R/a_1'R \longrightarrow R/aR$ pour compléter la démonstration. Comme $b_2 a' = b_3 pa' = b_3 a_1' p$, on a

$$(aT \cap bT)/ba'T = (aT \cap b_2 T)/b_2 a'T = (aT \cap b_3 T)/b_3 a_1'T \ .$$

Donc on est ramené au même problème avec b_2 remplacé par b_3 . Par récurrence sur le nombre de facteurs de b_2 , on peut donc supposer b_2 étranger à S . Le problème maintenant est le suivant : étant donné que $(aT \cap bT)/ba'T$ est sans torsion, où a, a', $b \in R$ sont étrangers à S , montrer que $(aR \cap bR)/ba'R$ est sans torsion.

Sinon, il existe u, v, x, $y \in R$ tels que $au = bv$ $\quad v \notin a'R$, et

aux = bvx = ba'y , $x \neq 0$. Par hypothèse, $bv = ba'r^{-1}$ où $r \in R$, $s \in S$, donc

(4) $\qquad vs = a'r$.

Ici s est produit d'éléments premiers. Fixons un tel élément p . Il divise a'r , mais non pas a' , donc $p|r$ et on peut simplifier p dans (4) . Par récurrence s peut être simplifié avec r , et on obtient $v = a'r_1$. Mais cela contredit l'hypothèse $v \notin a'R$. Donc $(aR \cap bR)/ba'R$ est sans torsion et nous avons construit un monomorphisme $R/a'R \longrightarrow R/aR$. Par symétrie le monomorphisme $T/aT \longrightarrow T/a'T$ vient d'un monomorphisme $R/aR \longrightarrow R/a'R$, donc a est monosemblable à droite à a' .

Théorème 14 : Soit R un anneau intègre atomique et S un sous-monoïde de R^* engendré par des éléments premiers, chacun facteur d'un élément central, appartenant à S . Si R_S est monofactoriel à droite, alors R l'est aussi.

Démonstration : Par hypothèse, tout élément $\neq 0$ dans R admet une factorisation complète. Si p est premier et se trouve dans une factorisation de c il se trouve dans toute autre (comme dans le cas commutatif) et peut être simplifié. Il ne reste que des facteurs atomiques de c qui ne sont pas dans S ; pour établir une correspondance entre eux nous passons à R_S , qui est monofactoriel à droite, et nous appliquons le dernier lemme pour relever les monosimilitudes de R_S à R .

Il est évident qu'on a des résultats analogues pour les épifactoriels. Dans le cas d'un anneau commutatif les quatre notions de factorialité se réduisent à la factorialité habituelle. Evidemment il suffit de regarder la monofactorialité à droite. Soit donc R un anneau commutatif intègre atomique. L'atomicité montre

que les objets de la catégorie $\mathcal{C}_R$ ont une longueur finie. Soit $f : R/a'R \longrightarrow R/aR$ un monomorphisme ; alors $\ker f$ est sans torsion, mais $(\ker f)a' = 0$, donc $\ker f = 0$, i.e. f est une injection. Un argument déjà vu nous montre que la monosimilitude entraîne la similitude, donc un monofactoriel est factoriel.

Par contre, dans le cas général les nouvelles notions sont plus larges, par exemple, l'anneau $\mathbb{Z}\langle x,y\rangle$ qui est l'algèbre libre sur x, y à coefficients entiers, est factoriel. On applique le théorème 14 avec $S = \mathbb{Z}^*$. De la même façon on montre que l'algèbre de groupe d'un groupe libre sur $\mathbb{Z}$ est mono (et épi) factoriel à droite (et à gauche).

Il serait souhaitable de trouver une formulation du théorème 14 sans les conditions un peu gênantes sur S. Toutefois quelques restrictions seront nécessaires comme le montre l'exemple suivant :

Soit R l'algèbre sur un corps k engendrée par x,y avec la seule relation $xy - yx = 1$. Considérons le monoïde $S = k[y]^*$; ses éléments ne sont pas tous invariants, mais le couple (R, S) satisfait aux conditions de Ore, donc on peut former l'anneau R_S, qui est un anneau de polynômes gauches sur le corps $k(y)$, donc factoriel. R est même intègre et atomique, mais il ne reste rien de la factorialité : il existe des éléments avec factorisations complètes à nombres de facteurs différents. Par exemple, on a :

$$yxy + y = y(1 + xy) = xy^2$$

et on voit aisément que x, y, $1 + xy$ sont des atomes (au moins si la car. de k est $\neq 2$).

- BIBLIOGRAPHIE -

ASANO K. [38] - Nichtkommutative Hauptidealringe ASI n° 696 (Paris 1938)

COHN P.M.[63] - Noncommutative unique factorization domains, Trans. Amer. Math. Soc. 109 (1963) 332 - 356.

COHN P.M.[67] - Torsion modules over free ideal rings, Proc. London Math. Soc. (3) 17 (1967) 577 - 599.

FITTING H.[35]- Primarkomponentenzerlegung in nichtkommutativen Ringen, Math. Ann. 111 (1935) 19 - 41.

JACOBSON N.[43]-Theory of rings (Providence 1943).

LANDAU E. [02]- Ein Satz über die Zerlegung homogener linearer differentialansdrücke in irreduzible Faktoren, J. reine angew. Math. 124 (1902) 115 - 120.

LOEWY A. [03] - Über reduzible homogene differentialansdrücke, Math. Ann. 56 (1903) 549 - 584.

ORE O. [32] - Formale theorie der linearen differentialgleichungen, J. reine angew. Math. 167 (1932) 221 - 234, 168 (1932) 233 - 252.

SCHLESINGER L.[97] - Handbuch der linearen differentialgleichungen Bd. 1 (Leipzig 1897).

BOWTELL A.J. [67] - The multiplicative semigroup of a ring and the embedding of rings in skew fields (thèse Londres 1967).

COHN P.M. [62] - Factorization in non commutative power series rings, Proc. Camb. Phil. Soc. 58 (1962) - 452 - 464.

COHN P.M. [66] - Some remarks on the invariant basis property, Topology 5. (1966) 215 - 228.

KOŠEVOI E.G. [66] - Sur le demi-groupe multiplicatif d'une classe d'anneaux sans diviseurs de zéro (en russe) Algebra i Logika 5, n° 5 (1966) 49 - 54.

COHN P.M. [63'] - Rings with a weak algorithm, Frans. Amer. Math. Soc. 109 (1963) 332 - 356.

COHN P.M. [61] - On a generalization of the Euclidean algorithm. Proc. Camb. Phil. Soc. 57 (1961) 18 - 30.

SAMUEL P. [63] - Anneaux factoriels (São Paulo 1963).

BRUNGS H.H. [69]-Ringe mit eindeutiger Faktorzerlegung, J. reine angew. Math. (à paraître).

COHN P.M. [69] - Factorization in general rings and strictly cyclic modules; J. reine angew. Math. (à paraître).

-:-:-:-:-:-:-:-:-

UNIVERSITE DE PARIS
FACULTE DES SCIENCES
D' ORSAY

1968-1969

-:-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 24

-:-:-:-:-:-:-:-

Remarques sur la structure d'un anneau local artinien à gauche

par Michel HACQUE .

-:-:-:-:-:-:-:-

1. Remarques préliminaires.

L'étude de la structure d'un anneau local artinien à gauche A , exposée dans [1] a été réalisée en raisonnant par récurrence sur l'exposant n du radical D et en considérant des involutions τ assujetties à certaines conditions.

Dans le das $n = 1$, le théorème 1 de [1] caractérise les groupes G qui sont les groupes multiplicatifs K^* d'un corps K , par l'existence d'une bijection involutive τ de $H = G - \{1\}$ sur lui-même, vérifiant les conditions (1), (2), (3) de la propriété 1.

Ce résultat intéressant montre néanmoins qu'étant donné un groupe G arbitraire, il n'existe pas nécessairement d'involution τ vérifiant ces conditions et il semble difficile de pouvoir trouver un critère simple permettant d'assurer qu'il en existe au moins une.

De même, dans le cas $n = 2$, en se fixant les données du théorème 2, à l'exception de τ , il n'est pas évident qu'il est possible de trouver au moins une bijection involutive τ vérifiant les conditions (1), (2), (2'), (3), (3') du théorème 2.

En d'autres termes, dans les théorèmes de structure énoncés dans [1], dont les conditions ne sont pas nécessairement incompatibles d'après les exemples 1^0 et 2^0, une partie des données étant fixée, il n'est pas évident qu'il est possible de la compléter de façon à obtenir un ensemble d'éléments caractérisant un anneau local artinien à gauche.

Pour remédier à cet inconvénient, on sera amené à décomposer les données en deux parties : les données initiales fixées arbitrairement et les données complémentaires pouvant bénéficier d'un ou de plusieurs degrés de liberté, de telle sorte qu'il soit toujours possible de les choisir de façon à caractériser un anneau local artinien à gauche.

Dans ce but, on modifiera d'abord la forme des données et on transformera les conditions auxquelles elles sont assujetties pour en donner une interprétation plus maniable.

2. Examen des données dans le cas $n = 2$.

Les données du théorème 2 de [1] comportent en particulier le corps résiduel K, un espace vectoriel à gauche non nul D de dimension finie sur K et une injection i du corps K dans l'anneau des endomorphismes $\mathcal{L}_K(D)$ de telle sorte que $i(1') = e$. Ces données signifient que D est un bi-module unitaire sur K [espace vectoriel à gauche et à droite sur K tel que $(\lambda d)\mu = \lambda(d\mu)$] non nul, de dimension finie comme espace vectoriel à gauche sur K.

Il en résulte que les données du théorème 2 de [1] peuvent être classées de la façon suivante :

2-1 - Données initiales :

Un corps K.

Un bi-module unitaire non nul D sur K qui est un espace vectoriel à gauche de dimension finie sur K,

2-2 - Données complémentaires :

(α) Un groupe multiplicatif G.

Un homomorphisme φ de G sur K^*.

Un isomorphisme σ du groupe multiplicatif H noyau de φ, sur le groupe additif D.

(α') Un élément involutif -1 du centre de G tel que $\varphi(-1) = 1'$.

(β) Une bijection involutive τ de G-H sur lui-même, vérifiant les conditions (1), (2), (2'), (3), (3'), de [1] .

3. Transformation des données complémentaires, dans le cas $n = 2$.

3-1 - Transformation des données (α) :

Les données initiales étant fixées, les données (α) caractérisent G comme une extension de K^* de noyau isomorphe à D .

D'après la théorie de la cohomologie des groupes [2] , en faisant opérer K^* sur D par : $\lambda * d = \lambda d \lambda^{-1}$, il existe une bijection entre l'ensemble des "classes d'extensions isomorphes" de K^* de noyau isomorphe à D et le second groupe de cohomologie $H^2(K^*, D)$.

Ainsi, les données (α) , définies à un isomorphisme près respectant les données initiales, correspondent exactement aux éléments du groupe $H^2(K^* , D)$.

De façon précise, $\eta \in H^2(K^* , D)$ peut être caractérisé par un 2-cocycle normalisé, c'est-à-dire une application $f : K^* \times K^* \longrightarrow D$, vérifiant

$$(I_o) \qquad \lambda * f(\lambda', \lambda'') - f(\lambda\lambda', \lambda'') + f(\lambda, \lambda'\lambda'') - f(\lambda, \lambda') = 0$$

avec la condition de normalisation $f(1, 1) = 0$ qui entraîne $f(\lambda, 1) = f(1, \lambda') = 0$.

Deux 2-cocycles normalisés caractérisent le même élément $\eta \in H^2(K^*, D)$ si et seulement si ils diffèrent d'un 2-cobord normalisé, c'est-à-dire d'une application $\delta^1 h : K^* \times K^* \longrightarrow D$ définie par :

$$(II_o) \qquad (\delta^1 h)(\lambda, \lambda') = \lambda * h(\lambda') - h(\lambda\lambda') + h(\lambda')$$

relation dans laquelle h est une 1-cochaine normalisée, c'est-à-dire une application $h : K^* \longrightarrow D$, vérifiant $h(1) = 0$.

Pour $\eta \in H^2(K^*, D)$, un représentant de la "classe d'extensions isomorphes" associée, est constitué par l'ensemble $D \times K^*$, muni de la multiplication définie par :

$$(M_o) \qquad (d, \lambda)(d', \lambda') = (d + \lambda d' \lambda^{-1} + f(\lambda, \lambda') , \lambda\lambda') .$$

Alors, on a :

$\varphi[(d, \lambda)] = \lambda$; $H = \{(d, 1)\}$ et $\sigma : H \xrightarrow{\sim} D$ est défini par $\sigma[(d, 1)] = - d$.

Soit u la bijection de $D \times K^*$ sur lui-même définie par $u[(d, \lambda)] = (d\lambda, \lambda)$. Il est facile de vérifier que u est un isomorphisme de l'ensemble $D \times K^*$, muni de la multiplication définie par (M_0), sur l'ensemble $D \times K^*$ muni de la multiplication définie par :

$$(M') \qquad (d, \lambda)(d', \lambda') = (d\lambda' + \lambda d' - \gamma(\lambda, \lambda') , \lambda\lambda')$$

relation dans laquelle l'application $\gamma : K^* \times K^* \longrightarrow D$, associée à f est définie par

$$\gamma(\lambda, \lambda') = - f(\lambda, \lambda')\lambda\lambda' .$$

La condition (I_0) se traduit alors par la condition :

$$(I') \qquad \lambda\gamma(\lambda', \lambda'') - \gamma(\lambda\lambda', \lambda'') + \gamma(\lambda, \lambda'\lambda'') - \gamma(\lambda, \lambda')\lambda'' = 0$$

et la condition $f(1, 1) = 0$ donne $\gamma(1, 1) = 0$ qui entraîne $\gamma(\lambda, 1) = \gamma(1, \lambda') = 0$.

De même, pour toute 1-cochaine normalisée h, en posant $\nu(\lambda) = - h(\lambda)\lambda$, on voit que l'application associée au 2-cobord normalisé $\delta^1 h$ est l'application $\delta\nu$ caractérisée par :

$$(II') \qquad (\delta\nu)(\lambda, \lambda') = \lambda\nu(\lambda') - \nu(\lambda\lambda') + \nu(\lambda)\lambda'$$

la condition $h(1) = 0$ se traduisant par $\nu(1) = 0$.

Il existe une bijection évidente entre l'ensemble des applications $\gamma : K^* \times K^* \longrightarrow D$ et l'ensemble des applications $\gamma_1 : K \times K \longrightarrow D$ qui prolongent γ par les conditions : $\gamma_1(k, 0) = \gamma_1(0, k') = 0$. La condition (I') se traduit alors par la condition (I) formellement analogue, obtenue en remplaçant $\lambda, \lambda', \lambda''$ par des éléments quelconques de K et $\gamma(1,1)$ se traduit par $\gamma_1(1,1) = 0$.

De même, il existe une bijection évidente entre l'ensemble des applications $\nu : K^* \longrightarrow D$ et l'ensemble des applications $\nu_1 : K \longrightarrow D$ qui prolongent ν par la condition $\nu_1(0)$ et $\nu(1) = 0$ se traduit par $\nu_1(1) = 0$.

En résumant ces résultats, on obtient donc :

<u>Proposition 3-1-1-</u> Les données initiales étant fixées, les données (α) peuvent être caractérisées par une application $\gamma_1 : K \times K \longrightarrow D$ vérifiant la condition.

$$(I) \qquad k\gamma_1(k',k'') - \gamma_1(kk',k'') + \gamma_1(k,k'k'') - \gamma_1(k,k')k'' = 0 ,$$

et les conditions de normalisation :

(I_n) $\begin{cases} \gamma_1(k,0) = \gamma_1(0,k') = 0 \\ \gamma_1(1,1) = 0 \quad \text{(qui entraîne} \quad \gamma_1(k,1) = \gamma_1(1,k') = 0) \end{cases}$.

Le groupe G est isomorphe au produit $D \times K^*$ muni de la multiplication définie par :

$$(M) \quad (d,k)(d',k') = (dk' + kd' - \gamma_1(k,k'),\ kk')$$

on a $\varphi[(d,k)] = k$, $H = \left\{(d,1)\right\}$ et $\sigma : H \xrightarrow{\sim} D$ est défini par $\sigma[(d,1)] = -d$.

De plus, on obtient des données (α) qui se déduisent l'une de l'autre par un isomorphisme respectant les données initiales si et seulement si les applications γ_1 associées diffèrent d'une application $\delta\nu_1$ caractérisée par :

$$(II) \quad (\delta\nu_1)(k,k') = k\,\nu_1(k') - \nu_1(kk') + \nu_1(k)k'$$

relation dans laquelle ν_1 est une application de K dans D vérifiant les conditions de normalisation

$$(II_n) \quad \nu_1(0) = \nu_1(1) = 0 \ .$$

Remarque 3-1-2- Lorsqu'on a fixé les données initiales et les données (α) déterminées par une application γ_1 vérifiant (I) et (I_n), la structure multiplicative de l'anneau A que l'on désire construire est isomorphe à la structure multiplicative déterminée sur $D \times K$ par la condition (M) dans laquelle k et k' sont maintenant des éléments quelconques de K [et non plus seulement des éléments de K^*].

3-2- Transformation de la donnée (α') :

Proposition 3-2-1- Dans l'énoncé de la proposition 3-1-1 , il est possible d'imposer à γ_1 et à ν_1 les conditions de normalisation supplémentaires

$$(I_{ns}) \quad \gamma_1(-1,1) = 0 \qquad (II_{ns}) \quad \nu_1(-1) = 0 \ .$$

En outre, elles entrainent les relations :

$$\gamma_1(-1,k) = \gamma_1(-1,-k) \ , \quad \gamma_1(k,-1) = \gamma_1(-k,-1) \quad \text{et} \quad \gamma_1(k,-1) = \gamma_1(-1,k) \ .$$

Si K est de caractéristique 2, dans K on a $-1 = 1$ et les conditions (I_n) et (II_n) montrent que les relations précédentes sont automatiquement vérifiées.

Dans le cas contraire, il suffit de remplacer γ_1 par $\gamma_1' = \gamma_1 + \delta\nu_1$ l'application ν_1 étant choisie de sorte que $\nu_1(-1) = \frac{1}{2}\gamma_1(-1,-1)$ et alors deux applications γ_1' déterminent des données isomorphes si et seulement si elles diffèrent d'une application $\delta\nu_1'$ pour laquelle $\nu_1'(-1) = 0$.

La condition (I) entraîne les relations :

$$(-1)\gamma_1(-1,k) - \gamma_1(1,k) + \gamma_1(-1,-k) - \gamma_1(-1,-1)k = 0$$

$$k\,\gamma_1(-1,-1) - \gamma_1(-k,-1) + \gamma_1(k,1) - \gamma_1(k,-1)(-1) = 0$$

et compte tenu des relations (I_n) et (I_{ns}) , il en résulte

$$\gamma_1(-1,k) = \gamma_1(-1,-k) \quad \text{et} \quad \gamma_1(k,-1) = \gamma_1(-k,-1) .$$

La condition (I) entraîne aussi :

$$(-1)\gamma_1(-k,-1) - \gamma_1(k,-1) + \gamma_1(-1,k) - \gamma_1(-1,-k)(-1) = 0$$

qui, compte tenu des deux relations précédentes, s'écrit aussi :

$$2\,\gamma_1(k,-1) = 2\,\gamma_1(-1,k)$$

et comme K n'est pas de caractéristique 2, il en résulte bien $\gamma_1(k,-1) = \gamma_1(-1,k)$.

Corollaire 3-2-2- Les données initiales étant fixées, les données (α) déterminent la donnée (α') .

La condition $\varphi(-1) = -1'$, montre que dans G , l'élément -1 doit être de la forme $(\varepsilon, -1)$. La définition de la multiplication dans G entraîne les relations :

$$(\varepsilon,-1)(d,k) = (\varepsilon k - d - \gamma_1(-1,k), -k)$$

$$(d,k)(\varepsilon,-1) = (-d + k\varepsilon - \gamma_1(k,-1), -k)$$

$$(\varepsilon,-1)(\varepsilon,-1) = (-\varepsilon - \varepsilon - \gamma_1(-1,-1); 1) .$$

Comme l'élément neutre de G est naturellement $(0,1)$, il en résulte que pour que $(\varepsilon, -1)$ soit un élément involutif appartenant au centre de G, il faut et il suffit que l'on ait :

$$\begin{cases} \varepsilon + \varepsilon + \gamma_1(-1, -1) = 0 \\ \varepsilon k - \gamma_1(-1, k) = k\varepsilon - \gamma_1(k, -1) . \end{cases}$$

En choisissant γ_1 vérifiant $\gamma_1(-1, -1) = 0$, la proposition 3-2-1 montre que ce système admet toujours pour solution $\varepsilon = 0$ et il en résulte que l'élément $-1 = (0, -1)$ satisfait aux conditions de la donnée (α').

Remarque 3-2-3 - Dans la suite, on pourra toujours supposer que l'application γ_1 caractérisant G, vérifie les conditions de normalisation :

$$(N) \qquad \gamma_1(k,0) = \gamma_1(0,k') = 0 \quad \text{et} \quad \gamma_1(1,1) = \gamma_1(-1,-1) = 0$$

qui entraînent en particulier les relations

$$\gamma_1(k,1) = \gamma_1(1,k') = 0 \quad \text{et} \quad \gamma_1(k,-1) = \gamma_1(-1,k) = 0$$

et l'existence de l'élément $-1 = (0,-1)$ qui caractérise la donnée (α').

3-3- Transformation de la donnée (β).

Les données initiales étant fixées et les données (α) et (α') étant déterminées de la manière indiquée ci-dessus, on a $G = D \times K^*$, $A = D \times K$ et $G-H$ est l'ensemble des couples (d,λ) avec $d \in D$, $\lambda \in K$ et $\lambda \neq 0$, $\lambda \neq 1$.

Toute bijection involutive τ de $G-H$ sur lui-même se prolonge de façon unique en une bijection involutive τ' de A sur lui-même de façon à ce que les restrictions de τ' à H et D se déduisent respectivement de σ et de σ^{-1}.

Lorsque τ vérifie la doncition (1), il en résulte que l'application τ' est caractérisée par une application $T : A = D \times K \longrightarrow D$ de sorte que pour $a = (d,k) \in A$, on ait :

$$\tau'[a] = \tau'[(d,k)] = (-d + T[(d,k)],\ 1 - k) ,$$

avec naturellement $\qquad T[(d,0)] = T[(d,1)] = 0 .$

Pour deux éléments $a = (d,\lambda)$ et $a' = (d',\lambda')$ de G-H [λ et λ' différents de 0 et de 1], on posera $\mu = 1 - \lambda$, $\mu' = 1 - \lambda'$ et

$$U(\lambda,\lambda') = \gamma_1(\lambda,\lambda') + \gamma_1(\lambda,\mu') + \gamma_1(\mu,1 + \mu^{-1}\lambda\mu') - \gamma_1(\mu,\mu^{-1}\lambda\mu') - \mu\gamma_1(-1,\mu^{-1}\lambda\mu') .$$

Lorsque $aa' \in H$, on a $\lambda\lambda' = 1$ et on peut vérifier que la condition (2') s'écrit:

$$\lambda\, T[(d',\lambda')] + T[(d,\lambda)] = U(\lambda,\lambda') .$$

Comme le second membre de cette relation ne dépend que de λ, il en résulte que la condition (2') implique que $T[(d,\lambda)]$ est indépendant de d.

La caractérisation d'une bijection τ vérifiant (2') se ramène donc à celle d'une application τ' qui est donc caractérisée par une application $t : K \longrightarrow D$, vérifiant $t(0) = t(1) = 0$, de sorte que τ' soit définie par :

$$\tau'[(d,k)] = (-d + t(k),\ 1 - k) .$$

Compte tenu de ces remarques, il est facile de vérifier que les conditions (2) et (2') se traduisent alors par la seule relation :

$$\lambda t(\lambda') - t(\lambda\lambda') + t(\lambda) + \mu^{-1}t(-\mu^{-1}\lambda\mu') = U(\lambda,\lambda') .$$

Pour un élément $a = (d,k)$ de A et un élément $\mathcal{C} = (d',\omega)$ de $G[\omega \neq o]$, on posera :

$$V(k,\omega) = \omega[\gamma_1(\omega^{-1},\omega) - \gamma_1(\omega^{-1},(1-k)\omega) - \gamma_1(\omega^{-1},k\omega)] - [\gamma_1(1-k,\omega) + \gamma_1(k,\omega) - \gamma_1(1,\omega)].$$

Il est facile de vérifier que les conditions (3) et (3') se traduisent alors par la relation

$$\omega t(\omega^{-1}k\,\omega) - t(k)\omega = V(k,\omega)$$

pour $k \neq 0$.

On peut remarquer que la condition (3') qui correspond à la valeur $k = 1$ est trivialement vérifiée et que la relation précédente est également vérifiée par $k = 0$. Enfin, pour que τ soit involutive, il faut et il suffit que t vérifie $t(k) = t(1-k)$.

Il en résulte donc la propriété suivante :

Proposition 3-3-1 - L'existence d'une bijection involutive τ de G-H sur lui-même vérifiant les conditions (1), (2), (2'), (3), (3') de [1] est équivalente à l'existence d'une application $t : K \longrightarrow D$, vérifiant les conditions suivantes :

(n_0) $t(0) = t(1) = 0$

(s_0) $t(k) = t(1-k)$

(a_0) $\lambda t(\lambda') - t(\lambda\lambda') + t(\lambda) + \mu^{-1}t(-\mu^{-1}\lambda\mu') = U(\lambda,\lambda')$

pour deux éléments λ et λ' de K différents de 0 et de 1, avec $\mu = 1 - \lambda$ et $\mu' = 1 - \lambda'$.

(d_0) $\omega t(\omega^{-1}k\omega) - t(k)\omega = V(k,\omega)$

pour deux éléments k et ω de K, avec $\omega \neq 0$.

4. Structure d'un anneau local artinien à gauche d'exposant deux.

4-1- Formules pour l'addition.

Les données initiales étant fixées et les données (α) et (α') étant déterminées de la manière indiquée ci-dessus, on peut supposer que la donnée (β) est caractérisée par une application $t : K \longrightarrow D$ vérifiant les conditions de la proposition 3-3-1 .

On peut alors vérifier que pour deux éléments $a = (d,k)$ et $a' = (d',k')$ de A, les formules d'addition données dans [1] se traduisent par la formule unique :

$$(d,k) + (d',k') = (d + d' + v(k,k') \ , \ k + k')$$

dans laquelle l'application $v = K \times K \longrightarrow D$ est caractérisée par les conditions suivantes :

$$(v)\quad v(k,k') = \begin{cases} \gamma_1(k,k^{-1}k') - \gamma_1(k,1 + k^{-1}k') + k\gamma_1(-1,k^{-1}k') + kt(-k^{-1}k') & \text{pour } k \neq 0 . \\ 0 \quad \text{pour } k = 0 . \end{cases}$$

Il en résulte facilement les relations :

$$v(k,0) = v(0,k') = 0 \ ,$$

On peut également remarquer que réciproquement, v détermine t par la condition :

$$(t)\qquad t(k) = v(1, -k) - \gamma_1(-1, -k) \ .$$

La proposition 3-2-1 entraîne aussi :

$$t(k) = v(1, -k) - \gamma_1(-1, k) \ .$$

4-2- Compatibilité des données dans le cas $n = 2$.

Les données initiales étant fixées, on supposera que les données (α) et (α') sont déterminées de la manière indiquée ci-dessus.

Un calcul direct donne le résultat suivant :

Lemme 4-2-1 - Pour toute application $t : K \longrightarrow D$, l'application $v : K \times K \longrightarrow D$ associée à t par les conditions (v) vérifie la condition :

(d_1) $v(kk_1,kk_2) - kv(k_1,k_2) = \gamma_1(k,k_1) + \gamma_1(k,k_2) - \gamma_1(k,k_1 + k_2)$.

De même, en tenant compte de la proposition 3-2-1, des calculs directs entraînent les résultats suivants :

Proposition 4-2-2 - Pour toute application $t : K \longrightarrow D$, soit $v : K \times K \longrightarrow D$ l'application associée à t par les conditions (v) . Alors :

(1) - La condition (d_0) est équivalente à la condition :

(d_2) $v(k_1k,k_2k) - v(k_1,k_2)k = \gamma_1(k_1,k) + \gamma_1(k_2,k) - \gamma_1(k_1 + k_2, k)$

(2) - La condition (a_0) est équivalente à la condition :

(a) $v(k',k'') - v(k + k',k'') + v(k,k' + k'') - v(k,k') = 0$.

Théorème 4-2-3 - Les données initiales étant fixées et les données (α) et (α') étant déterminées par une application $\gamma_1 : K \times K \longrightarrow D$ vérifiant la condition (I) de la proposition 3-1-1 et les conditions de normalisation (N) , l'existence d'une bijection involutive τ de G-H sur lui-même, vérifiant les conditions (1), (2), (2'), (3), (3') de [1] est équivalente à l'existence d'une application $\gamma_2 : K \times K \longrightarrow D$ vérifiant les conditions suivantes :

(n) $\gamma_2(k,0) = \gamma_2(0,k') = 0$ et $\gamma_2(1, -1) = 0$

(s) $\gamma_2(k,k') = \gamma_2(k',k)$

(a) $\gamma_2(k',k'') - \gamma_2(k+k',k'') + \gamma_2(k,k'+k'') - \gamma_2(k,k') = 0$

(d_1) $\gamma_2(kk_1,kk_2) - k\gamma_2(k_1,k_2) = \gamma_1(k,k_1) + \gamma_1(k,k_2) - \gamma_1(k,k_1 + k_2)$

(d_2) $\gamma_2(k_1k,k_2k) - \gamma_2(k_1,k_2)k = \gamma_1(k_1,k) + \gamma_1(k_2,k) - \gamma_1(k_1 + k_2,k)$.

De plus, lorsque ces conditions sont satisfaites, la structure de l'anneau local artinien à gauche d'exposant deux, est déterminée sur l'ensemble $A = D \times K$ par l'addition et la multiplication définies par les formules :

$$(A) \quad (d,k) + (d',k') = (d + d' + \gamma_2(k,k'),\ k + k')$$

$$(M) \quad (d,k)(d',k') = (dk' + kd' - \gamma_1(k,k'),\ kk') \ .$$

Soit t une application de K dans D vérifiant (n_0), (a_0) et (d_0). Les conditions (v) déterminent une application γ_2 de $K \times K$ dans D. Il est immédiat que γ_2 vérifie (n) et d'après le lemme 4-2-1 et la proposition 4-2-2, il en résulte que γ_2 vérifie aussi (a), (d_1) et (d_2).

Réciproquement, soit γ_2 une application de $K \times K$ dans D vérifiant (n), (a), (d_1) et (d_2). Soit t l'application de K dans D associée à γ_2 par la condition (t), c'est-à-dire par :

$$t(k) = \gamma_2(1,-k) - \gamma_1(-1,-k) \ .$$

La condition (d_2) implique :

$$\gamma_2(-k,k) - \gamma_2(1,-1)(-k) = \gamma_1(1,-k) + \gamma_1(-1,-k) - \gamma_1(0,-k)$$

et compte tenu de (n) et de la proposition 3-2-1, il en résulte

$$\gamma_1(-1,-k) = \gamma_2(-k,k) = \gamma_2(k,-k)$$

qui entraîne :

$$t(k) = \gamma_2(1,-k) - \gamma_2(-k,k) \ .$$

La condition (a) implique :

$$\gamma_2(-k,k) - \gamma_2(1-k,k) + \gamma_2(1,0) - \gamma_2(1,-k) = 0$$

et compte tenu de (n), il en résulte :

$$t(k) = \gamma_2(1,-k) - \gamma_2(-k,k) = -\gamma_2(1-k,k) \ .$$

Cette relation montre que (n) implique que t vérifie (n_0).

Soit v l'application de $K \times K$ dans D, associée à t par la condition (v). D'après (n), pour $k = 0$, on a $v(k,k') = \gamma_2(k,k') = 0$ et pour $k \neq 0$, on a :

$$v(k,k') = \gamma_1(k,1) + \gamma_1(k,k^{-1}k') - \gamma_1(k,1+k^{-1}1') + k\gamma_2(1,k^{-1}k') \ ,$$

et la condition (d_1) implique

$$\gamma_2(k,k') - k\gamma_2(1,k^{-1}k') = \gamma_1(k,1) + \gamma_1(k,k^{-1}k') - \gamma_1(k,1+k^{-1}k')$$

qui entraîne donc

$$v(k,k') = \gamma_2(k,k') \ .$$

Ainsi, γ_2 coïncide avec v et la proposition 4-2-2 montre que t vérifie (a_0) et (d_0) .

Il en résulte que les conditions (v) et (t) établissent des bijections réciproques entre les applications $t : K \longrightarrow D$ vérifiant (n_0) , (a_0) et (d_0) et les applications $\gamma_2 : K \times K \longrightarrow D$ vérifiant (n) , (a) , (d_1) et (d_2) .

Lorsque t et γ_2 sont associées par cette correspondance, la relation

$$t(k) = - \gamma_2(1-k,k)$$

montre que la condition (s) implique la condition (s_0) .

Réciproquement, on a toujours $\gamma_2(-k,k) = \gamma_2(k,-k)$ et lorsque $k + k' = \alpha \neq 0$, en posant $k = \alpha k_1$ et $k' = \alpha k_2$, la condition (d_1) implique

$$\gamma_2(k,k') = \alpha\gamma_2(k_1,k_2) = \gamma_1(\alpha,k_1) + \gamma_1(\alpha,k_2) - \gamma_1(\alpha, k_1 + k_2)$$

et

$$\gamma_2(k',k) - \alpha\gamma_2(k_2,k_1) = \gamma_1(\alpha,k_2) + \gamma_1(\alpha,k_1) - \gamma_1(\alpha, k_2 + k_1)$$

qui entraînent

$$\gamma_2(k,k') - \gamma_2(k',k) = \alpha[\gamma_2(k_1,k_2) - \gamma_2(k_2,k_1)] \ .$$

Comme $k_1 + k_2 = 1$, on a

$$\gamma_2(k_1,k_2) = \gamma_2(k_1,1-k_1) = - t(1-k_1) \quad \text{et} \quad \gamma_2(k_2,k_1) = \gamma_2(1-k_2,k_1) = -t(k_1)$$

qui entraînent

$$\gamma_2(k,k') - \gamma_2(k',k) = \alpha[t(k_1) - t(1-k_1)]$$

et il en résulte que la condition (s_0) implique la condition (s) .

D'après la proposition 3-3-1, l'existence d'une bijection involutive τ de G-H sur lui-même vérifiant les conditions (1), (2), (2'), (3), (3') de [1] est donc bien

équivalente à l'existence d'une application $\gamma_2 : K \times K \longrightarrow D$ vérifiant (n), (s), (a), (d_1) et (d_2) et les formules caractérisant l'addition et la multiplication résultent de ce qui précède.

Remarque 4-2-4 - Si l'application γ_1 a été choisie de façon à ce qu'elle soit bi-additive, les seconds membres de (d_1) et de (d_2) sont nuls et il en résulte que l'application γ_2 identiquement nulle satisfait aux conditions du théorème 4-2-3. Dans ce cas il en résulte qu'il n'y a pas d'obstruction à la détermination d'une donnée (β) compatible avec les données initiales et les données (α) et (α'). De plus, la structure additive de l'anneau A ainsi obtenue, est alors triviale.

On verra dans la suite ce que signifie cette possibilité.

5 - Structure des anneaux locaux artiniens à gauche.

5-1 - Rappels sur les extensions spéciales d'algèbres.

Soit β un anneau commutatif unitaire.

Soit $\beta : E \longrightarrow \Lambda$ un homomorphisme surjectif de β-algèbre. Si M est le noyau de β et si $M^2 = \{0\}$, il est facile de vérifier que la multiplication dans E induit sur M une structure de Λ-bimodule. On dit alors que (E,β) constitue une extension spéciale de la β-algèbre Λ de noyau M.

Lorsque la β-algèbre Λ et le Λ-bimodule M sont fixés, deux extensions spéciales (E,β) et (E',β') sont dites équivalentes s'il existe un isomorphisme $\theta : E \longrightarrow E'$ qui induit l'identité sur M et tel que $\beta = \beta' \circ \theta$.

D'après la théorie de la cohomologie des algèbres associatives [3], étant donnés une β-algèbre Λ et un Λ-bimodule M, il existe une correspondance bijective entre l'ensemble des classes d'équivalence d'extensions spéciales de la β-algèbre Λ de noyau M et le β-module $H^2(\Lambda,M)$ défini par U. Skukla [3], qui est le second module de cohomologie de Λ pour M.

Lemme 5-1-1 - Etant donnés un anneau commutatif unitaire β, une β-algèbre Λ et un Λ-bimodule M, lorsque Λ est β-projective, toute extension spéciale (E,β) de la β-algèbre Λ de noyau M est caractérisée par une application β-bilinéaire γ de $\Lambda \times \Lambda$ dans M vérifiant

(I) $\lambda_1 \gamma(\lambda_2,\lambda_3) - \gamma(\lambda_1\lambda_2,\lambda_3) + \gamma(\lambda_1,\lambda_2\lambda_3) - \gamma(\lambda_1,\lambda_2)\lambda_3 = 0$

et

(n_1) $\gamma(1,1) = 0$.

L'anneau sous-jacent à la β-algèbre E est isomorphe à l'anneau défini sur l'ensemble $M \times \Lambda$ par l'addition et la multiplication caractérisées par les formules

$$(m_1,\lambda_1) + (m_2,\lambda_2) = (m_1 + m_2,\ \lambda_1 + \lambda_2)$$

$$(m_1,\lambda_1)\,(m_2,\lambda_2) = (m_1\lambda_2 + \lambda_1 m_2 - \gamma(\lambda_1,\lambda_2)\ ,\ \lambda_1\lambda_2)$$

et β est défini par

$$\beta[m,\lambda)] = \lambda \ .$$

De plus, deux telles extensions spéciales (E,β) et (E',β') caractérisée par des applications γ et γ' sont équivalentes si et seulement si il existe une application β-linéaire h de Λ dans M telle que $h(1) = 0$ et vérifiant

(II) $\gamma(\lambda_1,\lambda_2) - \gamma'(\lambda_1,\lambda_2) = \lambda_1 h(\lambda_2) - h(\lambda_1\lambda_2) + h(\lambda_1)\lambda_2$.

En posant $\Lambda^e = \Lambda \otimes_\beta \Lambda^*$, lorsque Λ est β-projective, on sait [3] que $H^2(\Lambda,M)$ est isomorphe à $E \times t^2_{\Lambda^e}(\Lambda,M)$ et aussi au β-module $\mathrm{Hoch}^2(\Lambda,M)$ déterminé par la méthode de Hochschild [4]. Le lemme 5-1-1 résulte alors de [3] et de la caractérisation des éléments de $\mathrm{Hoch}^2(\Lambda,M)$.

5-2 - Extensions spéciales d'anneaux.

Définition 5-2-1 - Soit Λ un anneau unitaire et soit M un Λ- bimodule.

Un 2-cocycle de Λ dans M est un couple $g = (\gamma_1,\gamma_2)$ constitué par deux applications γ_1 et γ_2 de $\Lambda \times \Lambda$ dans M vérifiant :

(n_0) $\gamma_2(\lambda,0) = \gamma_2(0,\lambda') = 0$

(s) $\gamma_2(\lambda,\lambda') = \gamma_2(\lambda',\lambda)$

(a_0) $\lambda\,\gamma_1(\lambda',\lambda'') - \gamma_1(\lambda\lambda',\lambda'') + \gamma_1(\lambda,\lambda'\lambda'') - \gamma_1(\lambda,\lambda')\lambda'' = 0$

(a) $\gamma_2(\lambda',\lambda'') - \gamma_2(\lambda+\lambda',\lambda'') + \gamma_2(\lambda,\lambda'+\lambda'') - \gamma_2(\lambda,\lambda') = 0$

(d_1) $\gamma_2(\lambda\lambda_1,\lambda\lambda_2) - \lambda\gamma_2(\lambda_1,\lambda_2) = \gamma_1(\lambda,\lambda_1) + \gamma_1(\lambda,\lambda_2) - \gamma_1(\lambda,\lambda_1+\lambda_2)$

(d_2) $\gamma_2(\lambda_1\lambda,\lambda_2\lambda) - \gamma_2(\lambda_1,\lambda_2)\lambda = \gamma_1(\lambda_1,\lambda) + \gamma_1(\lambda_2,\lambda) - \gamma_1(\lambda_1+\lambda_2,\lambda)$.

Un 2-cocycle g est normalisé s'il vérifie la condition

(n_1) $\gamma_1(1,1) = 0$.

Un 2-cobord de Λ dans M est un couple $\delta f = (\nu_1,\nu_2)$ dans lequel les applications ν_1 et ν_2 de $\Lambda\times\Lambda$ dans M, sont associées à une application f de Λ dans M vérifiant $f(0) = 0$, par les conditions :

(δ_1) $\nu_1(\lambda_1,\lambda_2) = \lambda_1 f(\lambda_2) - f(\lambda_1\lambda_2) + f(\lambda_1)\lambda_2$

(δ_2) $\nu_2(\lambda_1,\lambda_2) = f(\lambda_1+\lambda_2) - f(\lambda_1) - f(\lambda_2)$.

Un 2-cobord δf est normalisé si f vérifie la condition

(n'_1) $f(1) = 0$.

Lemme 5-2-2 - Soit Λ un anneau unitaire (considéré comme $\mathbb{Z}$-algèbre) et soit M un Λ-bimodule.

Tout élément $\zeta \in H^2(\Lambda,M)$ peut être caractérisé par un 2-cocycle normalisé $g = (\gamma_1,\gamma_2)$ de Λ dans M.

De plus, deux 2-cocycles normalisés g et g' caractérisent un même élément de $H^2(\Lambda,M)$ si et seulement si $g-g'$ est égal à un 2-cobord normalisé δf de Λ dans M.

La caractérisation générale des éléments de $H^2(\Lambda,M)$ donnée dans [3], montre que lorsque $\beta = \mathbb{Z}$, tout élément $\zeta \in H^2(\Lambda,M)$ est caractérisé par un 2-cocycle de Λ dans M et que deux 2-cocycles caractérisent un même élément de $H^2(\Lambda,M)$ si et seulement si, ils sont cohomologues, c'est-à-dire s'ils diffèrent d'un 2-cobord de Λ dans M.

Tout revient à montrer que tout 2-cocycle est cohomologue à un 2-cocycle normalisé et que deux 2-cocycles normalisés cohomologues diffèrent d'un 2-cobord normalisé, ce qui est facile à vérifier.

Lemme 5-2-3- Soit Λ un anneau unitaire (considéré comme $\mathbb{Z}$-algèbre) et soit M un Λ-bimodule.

Il existe une correspondance bijective entre les éléments $\zeta \in H^2(\Lambda,M)$ et les classes d'équivalence d'extensions spéciales (A,β) de l'anneau Λ de noyau M.

A un élément $\zeta \in H^2(\Lambda,M)$ qui peut être caractérisé par un 2-cocycle normalisé $g = (\gamma_1,\gamma_2)$ de Λ dans M, cette correspondance associe une extension spéciale (A,β) de l'anneau Λ de noyau M, dans laquelle l'anneau A est isomorphe à l'anneau défini sur l'ensemble $M \times \Lambda$ par l'addition et la multiplication caractérisées par les formules

$$(A)\quad (m_1,\lambda_1) + (m_2,\lambda_2) = (m_1 + m_2 + \gamma_2(\lambda_1,\lambda_2)\ ,\ \lambda_1 + \lambda_2)$$

$$(M)\quad (m_1,\lambda_1)\,(m_2,\lambda_2) = (m_1\lambda_2 + \lambda_1 m_2 - \gamma_1(\lambda_1,\lambda_2)\ ,\ \lambda_1\lambda_2)$$

et β est défini par $\beta[(m,\lambda)] = \lambda$.

En outre, l'unité est l'élément $\bar{1} = (0,1)$ et le zéro est l'élément $\bar{0} = (0,0)$.

La première et la seconde partie résultent du lemme 5-2-2 et des résultats de [3].

La condition (n_1) et la condition (a_0) entraînent les relations :

(c_1) $\gamma_1(\lambda,1) = \gamma_1(1,\lambda') = 0$.

Il en résulte que $\bar{1} = (0,1)$ est l'unité.

La condition (n_0) et les conditions (d_1) et (d_2) entraînent les relations :

(c_2) $\gamma_1(\lambda,0) = \gamma_1(\lambda',0) = 0$.

La condition (n_0) montre que $\bar{0} = (0,0)$ est le zéro.

5-3- Anneau local artinien à gauche d'exposant deux.

Théorème 5-3-1 - Tout anneau local artinien à gauche A d'exposant deux est caractérisé par les données suivantes :

(1) Données initiales - Un corps K

- Un bimodule unitaire non nul D sur K qui est un espace vectoriel à gauche de dimension finie sur K .

(2) Donnée complémentaire - Un élément $\zeta \in H^2(K,D)$ qui peut être caractérisé par un 2 cocycle normalisé $g = (\gamma_1, \gamma_2)$ de K dans D .

L'anneau local artinien à gauche A d'exposant deux caractérisé par ces données est isomorphe à l'anneau défini sur l'ensemble $D \times K$ par l'addition et la multiplication caractérisées par les formules

$$(A) \quad (d_1,k_1) + (d_2,k_2) = (d_1 + d_2 + \gamma_2(k_1,k_2) , k_1 + k_2)$$

$$(M) \quad (d_1,k_1)(d_2,k_2) = (d_1 k_2 + k_1 d_2 - \gamma_1(k_1,k_2) , k_1 k_2) .$$

Le radical de A est isomorphe à D et le corps résiduel de A est isomorphe à K .

Tout anneau local artinien à gauche A d'exposant deux détermine des données initiales dans lesquelles K est le corps résiduel et D est le radical muni de la structure de K-bimodule induite par la multiplication de A . De plus, en désignant par β l'homomorphisme surjectif canonique de A sur K , le couple (A,β) constitue une extension spéciale de l'anneau K de noyau D . Le lemme 5-2-3 montre alors que A détermine un élément $\zeta \in H^2(K,D)$ pouvant être caractérisé par un 2-cocycle normalisé $g = (\gamma_1,\gamma_2)$ de K dans D , et que A possède bien la structure décrite dans le théorème 5-3-1 .

Réciproquement, les données du théorème 5-3-1 étant fixées, d'après le lemme 5-2-3, elles déterminent une extension spéciale (A,β) de l'anneau K de noyau D , dans laquelle l'anneau A est défini sur l'ensemble $D \times K$ par l'addition et la multiplication caractérisées par les formules (A) et (M) . Tout revient à montrer que l'anneau A est local, artinien à gauche, d'exposant deux, de radical isomorphe à D et de corps résiduel isomorphe à K .

Comme $\bar{1} = (0,1)$ est l'unité de A , la formule (M) montre que tout élément (d,k) de A avec $k \neq 0$, est inversible et admet pour inverse l'élément :

$$(k^{-1}\gamma_1(k,k^{-1}) - k^{-1}dk^{-1}, k^{-1}) = (\gamma_1(k^{-1},k)k^{-1} - k^{-1}dk^{-1}, k^{-1}) .$$

Les conditions (n_0) et (c_2) montrent alors que A est un anneau local dont le radical est l'ensemble $D \times \{0\}$ isomorphe à D et dont le corps résiduel est isomorphe à K. De plus, la structure de K-bimodule sur $D \times \{0\}$ induite par la multiplication de A est bien isomorphe à celle de D.

La condition (c_2) entraîne la relation :

$$(d,k)\,(d',0) = (kd',0)$$

qui montre que les idéaux à gauche de A sont associés aux sous K-espaces vectoriel à gauche de D. Il en résulte que A est artinien à gauche. Enfin, A est d'exposant deux puisque D est non nul et vérifie $D^2 = \{0\}$, ce qui achève la démonstration.

Définition 5-3-2 - Un anneau local A est dit d'égale caractéristique s'il a la même caractéristique que son corps résiduel.

Corollaire 5-3-3 - Tout anneau local artinien à gauche A, d'exposant deux et d'égale caractéristique, est caractérisé par les données suivantes :

(1) Données initiales - Un corps K

- Un bimodule unitaire non nul D sur K qui est un espace vectoriel à gauche de dimension finie sur K.

(2) Donnée complémentaire - Un élément $\zeta \in H^2(K,D)$ qui peut être caractérisé par un 2-cocycle normalisé de K dans D de la forme $g = (\gamma,0)$, c'est-à-dire par une application bi-additive γ de $K \times K$ dans D, vérifiant :

$$(I)\quad \lambda_1\gamma(\lambda_2,\lambda_3) - \gamma(\lambda_1\lambda_2,\lambda_3) + \gamma(\lambda_1,\lambda_2\lambda_3) - \gamma(\lambda_1,\lambda_2)\lambda_3 = 0$$

et

$$(n_1)\quad \gamma(1,1) = 0\ ,$$

L'anneau local artinien à gauche A, d'exposant deux et d'égale caractéristique, caractérisé par ces données est isomorphe à l'anneau défini sur l'ensemble $D \times K$ par l'addition et la multiplication caractérisées par les formules:

$$(A')\quad (d_1,k_1) + (d_2,k_2) = (d_1 + d_2\ ,\ k_1 + k_2)$$

$$(M')\quad (d_1,k_1)\,(d_2,k_2) = (d_1k_2 + k_1d_2 - \gamma(k_1,k_2)\ ,\ k_1k_2)$$

Le radical A est isomorphe à D et le corps résiduel de A est isomorphe à K .

Si A est un anneau local de radical D et d'égale caractéristique, et si K_0 est le corps premier du corps résiduel K , il est immédiat qu'il existe un sous-corps L de A isomorphe à K_0 par la restriction à L de l'homomorphisme surjectif canonique $\beta : A \to K$. De plus, comme L est dans le centre de A , il en résulte que A et K sont des K_0-espaces vectoriels et aussi de K_0-algèbre.

Si A est d'exposant deux, il en résulte que (A,β) constitue une extension spéciale de K_0-algèbre de K de noyau D . Puisque K est K_0-libre, le lemme 5-1-1 montre qu'il existe une application k_0-bilinéaire donc bi-additive γ de $K \times K$ dans D vérifiant (I) et (n_1) , de telle qorte que A soit isomorphe à l'anneau décrit dans le corollaire 5-3-3 .

Cette application γ détermine un élément $\zeta \in H^2(K,D)$ qui peut être caractérisé par un 2-cocycle normalisé de K dans D de la forme : $g = (\gamma,0)$.

Réciproquement la donnée complémentaire étant déterminée par un 2-cocycle normalisé de K dans D de la forme $g = (\gamma,0)$, d'après le théorème 5-3-1 l'anneau décrit dans le corollaire 5-3-3 est un anneau local artinien à gauche d'exposant deux et la formule (A') montre que A est d'égale caractéristique, ce qui achève la démonstration.

Remarque 5-3-4 - Si dans les données initiales le corps K est supposé de caractéristique nulle, alors le corollaire 5-3-3 caractérise tous les anneaux locaux artiniens à gauche, de radical D , d'exposant deux et de corps résiduel K .

En effet, tout anneau local de corps résiduel K est alors d'égale caractéristique.

5-4 - Anneau local artinien à gauche.

Théorème 5-4-1 - Tout anneau local artinien à gauche A d'exposant p , avec $p \leqslant n$, est caractérisé par les données suivantes :

(1) Données initiales - Un corps K

- Un bimodule unitaire non nul Δ sur K qui est un espace vectoriel à gauche de dimension finie sur K ,

- Un anneau local artinien à gauche A' , d'exposant q , avec $q \leqslant n-1$ et $q \leqslant p$, de corps résiduel K .

[Si β' est l'homomorphisme surjectif canonique de A' sur K, soit $\Delta^{(\beta')}$ le A'-bimodule déduit de Δ par l'extension des scalaires déterminée par $\beta' : A' \longrightarrow K$] .

(2) Donnée complémentaire - Un élément $\zeta \in H^2(A', \Delta^{(\beta')})$ qui peut être caractérisée par un 2-cocycle normalisé $g = (\gamma_1, \gamma_2)$ de A' dans $\Delta^{(\beta')}$.

L'anneau local artinien à gauche A, d'exposant p, caractérisé par ces données est isomorphe à l'anneau défini sur l'ensemble $\Delta \times A'$ par l'addition et la multiplication caractérisées par les formules :

$$(A)\quad (\delta_1, a'_1) + (\delta_2, a'_2) = (\delta_1 + \delta_2 + \gamma_2(a'_1, a'_2),\ a'_1 + a'_2)$$

$$(M)\quad (\delta_1, a'_1)(\delta_2, a'_2) = (\delta_1 . \beta'(a'_2) + \beta'(a'_1).\delta_2 - \gamma_1(a'_1, a'_2),\ a'_1 a'_2) .$$

Le corps résiduel de A est isomorphe à K .

Soit A un anneau local artinien à gauche, d'exposant p, avec $p \leqslant n$.

Si K est le corps résiduel de A et si D est le radical de A, la multiplication dans A détermine, par passage au quotient, une structure de K-bimodule unitaire sur le groupe abélien non nul $\Delta = D^{p-1}$ et Δ est aussi un espace vectoriel à gauche de dimension finie sur K .

L'anneau quotient $A' = A/\Delta$ est local artinien à gauche d'exposant $q = p-1 \leqslant n-1$, de radical $D' = D/\Delta$ et de corps résiduel K .

Puisque $\Delta^2 = \{0\}$, le groupe abélien Δ est également muni d'une structure de A'-bimodule unitaire déduite de la multiplication dans A, mais cette structure n'est pas quelconque car il est immédiat qu'elle coïncide avec celle du A'-bimodule $\Delta^{(\beta')}$ déduit du K-bimodule Δ par l'extension des scalaires déterminée par $\beta' : A' \longrightarrow K$.

Ainsi, A détermine un ensemble de données initiales et en désignant par α l'homomorphisme surjectif canonique de A sur A', le couple (A, α) constitue une extension spéciale de l'anneau A' de noyau $\Delta^{(\beta')}$. Le lemme 5-2-3 montre que A détermine un élément $\zeta \in H^2(A', \Delta^{(\beta')})$ qui peut être caractérisé par un 2-cocycle normalisé $g = (\gamma_1, \gamma_2)$ de A' dans $\Delta^{(\beta')}$ et que A est isomorphe à l'anneau décrit dans le théorème 5-4-1 .

Réciproquement, les données du théorème 5-4-1 étant fixées, d'après le lemme 5-2-3 , elles déterminent une extension spéciale (A, α) de l'anneau A' de noyau

$\Delta^{(\beta')}$, dans laquelle l'anneau A est défini sur l'ensemble $\Delta \times A'$ par l'addition et la multiplication caractérisées par les formules (A) et (M) ,

Si D' est le radical de A' , comme dans la démonstration du théorème 5-3-1 , on vérifie facilement que tout élément (δ,a') de A avec $a' \notin D'$ (ce qui est équivalent à $\beta'(a') \neq 0$) est inversible et que l'ensemble $D = \Delta \times D'$ est l'unique idéal maximal de A , qui est donc un anneau local,

Il est immédiat que l'ensemble $\Delta_0 = \Delta \times \{0\}$ est un idéal bilatère de A et que les idéaux à gauche de A contenus dans Δ_0 sont caractérisés par les sous K-espaces vectoriels à gauche de Δ .

Tout idéal à gauche I de A (qui est donc contenu dans $D = \Delta \times D'$) détermine un idéal à gauche $\alpha(I)$ de A' (qui est donc contenu dans D') et un sous K-espace vectoriel à gauche $\alpha_0(I)$ de Δ caractérisé par :

$$\alpha_0(I) \times \{0\} = I \cap \Delta_0 = I \cap \alpha^{-1}(0) .$$

Plus généralement, pour tout $d' \in \alpha(I)$ soit $\alpha_{d'}(I)$ la partie de Δ caractérisée par :

$$\alpha_{d'}(I) \times \{d'\} = I \cap \alpha^{-1}(d') .$$

Soit Ψ une application de $\alpha(I)$ dans Δ vérifiant :

$$\Psi(d') \in \alpha_{d'}(I) \quad \text{pour tout} \quad d' \in \alpha(I) .$$

Pour $d' \in \alpha(I)$, la formule (A) et la condition (n_0) entraînent la relation :

$$(\delta,0) + (\Psi(d'), d') = (\delta + \Psi(d'), d')$$

qui montre l'équivalence des conditions :

$$(\delta,0) \in I \quad \text{et} \quad (\delta + \Psi(d'), d') \in I$$

c'est-à-dire des conditions :

$$\delta \in \alpha_0(I) \quad \text{et} \quad (\delta + \Psi(d') \in \alpha_{d'}(I) .$$

Puisque $\Psi(d') \in \alpha_{d'}(I)$, pour tout $d' \in \alpha(I)$, il en résulte les relations :

$$\alpha_{d'}(I) = \alpha_0(I) + \Psi(d') .$$

Soient I et J deux idéaux à gauche de A vérifiant :

$$I \subset J .$$

On a alors $\alpha(I) \subset \alpha(J)$, $\alpha_0(I) \subset \alpha_0(J)$ et aussi

$$\alpha_{d'1}(I) \subset \alpha_{d'1}(J) \quad \text{pour tout} \quad d' \in \alpha(I) .$$

D'après ce qui précède, pour tout $d' \in \alpha(I)$, on a :

$$\alpha_{d'1}(I) = \alpha_0(I) + \Psi(d')$$

et

$$\alpha_{d'1}(J) = \alpha_0(J) + \Psi(d')$$

puisque $\Psi(d') \in \alpha_{d'1}(I) \subset \alpha_{d'1}(J)$.

En particulier, si $\alpha_0(I) = \alpha_0(J)$, il en résulte $\alpha_{d'1}(I) = \alpha_{d'1}(J)$ pour tout $d' \in \alpha(I)$, et si de plus $\alpha(I) = \alpha(J)$, il en résulte $I = J$.

Ainsi, pour deux idéaux à gauche I et J de A vérifiant $I \subset J$, la relation $I = J$ est équivalente aux conditions :

$$\alpha(I) = \alpha(J) \quad \text{et} \quad \alpha_0(I) = \alpha_0(J) .$$

Ce résultat va permettre de montrer que A est artinien à gauche. En effet, si $\{I_m\}$ est une suite décroissante d'idéaux à gauche de A , les $\alpha(I_m)$ constituent une suite décroissante d'idéaux à gauche de A' qui est stationnaire puisque A' est artinien à gauche, et les $\alpha_0(I_m)$ constituent une suite décroissante de sous K-espaces vectoriels à gauche de Δ qui est stationnaire ; il en résulte que pour m assez grand on a $\alpha(I_m) = \alpha(I_{m+1})$ et $\alpha_0(I_m) = \alpha_0(I_{m+1})$, ce qui entraîne $I_m = I_{m+1}$, et montre que A est artinien à gauche.

Ainsi, A est un anneau local artinien à gauche, de radical $D = \Delta \times D'$ et de corps résiduel K .

La structure multiplicative du radical $D = \Delta \times D'$ de A est caractérisée par la formule :

$$(\delta_1, d'_1)(\delta_2, d'_2) = (-\gamma_{d'1}(d'_1, d'_2) , d'_1, d'_2) .$$

Il en résulte que le produit de m éléments (δ_2, d'_2) de D , se met sous la forme :

$$\prod_{i=1}^{i=m} (\delta_2, d'_2) = (-\gamma_1(\prod_{i=1}^{i=m-1} d'_2, d'_m), \prod_{i=1}^{i=m} d'_2) .$$

Puisque $D'^q = \{0\}$, cette formule et la relation (c_2) montrent que si $q \leqslant m-1$, le produit de m éléments de D est nul. Il en résulte que le produit de $q+1$ éléments de D est nul, ce qui entraîne $p \leqslant q+1 \leqslant n$ et comme il existe $q-1$ éléments de D' dont le produit n'est pas nul, il en est de même dans D, ce qui entraîne $q \leqslant p$ et achève la démonstration.

Remarque 5-4-2 - L'égalité $p = q+1$, équivaut à l'existence d'un élément $\delta' \in \Delta' = D'^{q-1}$ et d'un élément $d' \in D'$ tels que $\gamma_1(\delta', d') \neq 0$.

Corollaire 5-4-3 - Tout anneau local artinien à gauche A, d'exposant p avec $p \leqslant n$ et d'égale caractéristique, est caractérisé par les données suivantes :

(1) Données initiales - Un corps K

- Un bimodule unitaire non nul Δ sur K qui est un espace vectoriel à gauche de dimension finie sur K,

- Un anneau local artinien à gauche A', d'exposant q avec $q \leqslant n-1$ et $q \leqslant p$, de corps résiduel K et d'égale caractéristique.

(2) Donnée complémentaire - Un élément $\zeta \in H^2(A', \Delta^{(\beta')})$ qui peut être caractérisé par un 2-cocycle normalisé de A' dans $\Delta^{(\beta')}$ de la forme $g = (\gamma, 0)$, c'est-à-dire par une application bi-additive γ de $A' \times A'$ dans $\Delta^{(\beta')}$ vérifiant :

$$(I)\quad \beta'(a'_1).\gamma(a'_2, a'_3) - \gamma(a'_1 a'_2, a'_3) + \gamma(a'_1, a'_2 a'_3) - \gamma(a'_1, a'_2).\beta'(a'_3) = 0$$

et

$$(n_1)\quad \gamma(1', 1') = 0 \quad (1' \text{ unité de } A').$$

L'anneau local artinien à gauche A d'exposant p et d'égale caractéristique, caractérisé par ces données est isomorphe à l'anneau défini sur l'ensemble $\Delta \times A'$ par l'addition et la multiplication caractérisées par les formules :

$$(A')\quad (\delta_1, a'_1) + (\delta_2, a'_2) = (\delta_1 + \delta_2, a'_1 + a'_2)$$

$$(M')\quad (\delta_1, a'_1)(\delta_2, a'_2) = (\delta_1.\beta'(a'_2) + \beta'(a'_1)\delta_2 - \gamma(a'_1, a'_2), a'_1 a'_2).$$

Le corps résiduel de A est isomorphe à K.

Soit A un anneau local artinien à gauche, d'exposant p avec $p \leqslant n$, et d'égale caractéristique, de radical D et de corps résiduel K. Avec les notations précédentes, il est immédiat que $A' = A/\Delta$ est aussi d'égale caractéristique et si K_0 est le corps premier de K, comme dans le début de la démonstration du corollaire 6-3-3, il est facile de voir que les homomorphismes surjectifs canoniques $\alpha : A \longrightarrow A' = A/\Delta$ et $\beta' : A' \longrightarrow A'/D' = A/D = K$, sont des homomorphismes de K_0-espace vectoriel et aussi de K_0-algèbre.

Il en résulte que (A,α) constitue une extension spéciale de la K_0-algèbre A' de noyau $\Delta^{(\beta')}$. Puisque A' est K_0-libre, le lemme 5-1-1 montre qu'il existe une application K_0-bilénaire, donc bi-additive, γ de $A' \times A'$ dans $\Delta^{(\beta')}$ vérifiant (I) et (n_1), de telle sorte que A soit isomorphe à l'anneau décrit dans le corollaire 5-4-3.

Cette application γ détermine un élément $\zeta \in H^2(A', \Delta^{(\beta')})$ qui peut être caractérisé par un 2-cocycle normalisé de A' dans $\Delta^{(\beta')}$ de la forme $g = (\gamma, 0)$.

Réciproquement, la donnée complémentaire du corollaire 5-4-3 étant déterminée par un 2-cocycle normalisé de A' dans $\Delta^{(\beta')}$ de la forme $g = (\gamma, 0)$, d'après le théorème 5-4-1, l'anneau décrit dans le corollaire 5-4-3 est un anneau local artinien à gauche, d'exposant p avec $p \leqslant n$ et la formule (A') montre que A est d'égale caractéristique, ce qui achève la démonstration.

Remarque 5-4-4 - Si dans les données initiales le corps K est supposé de caractéristique nulle, alors le corollaire 5-4-3 caractérise tous les anneaux locaux artiniens à gauche, d'exposant p avec $p \leqslant n$ et de corps résiduel K.

En effet, tout anneau local de corps résiduel K est alors d'égale caractéristique.

5-5 - Remarques diverses.

5-5-1 - Sur le cas commutatif.

Pour obtenir les caractéristiques des anneaux locaux artiniens à gauche commutatifs, il suffit, dans les énoncés précédents, d'imposer les conditions supplémentaires suivantes : K est un corps commutatif, D ou Δ sont des K-espaces vectoriels, A' est commutatif et γ_1 ou γ sont symétriques.

5-5-2 - Sur les exemples de [1].

Le premier exemple de [1] est obtenu à partir du théorème 5-3-1 en utilisant un corps commutatif K, un espace vectoriel D de dimension une sur K et les applications γ_1 et γ_2 identiquement nulles.

Le second exemple de [1] est obtenu à partir du théorème 5-3-1 en utilisant le corps $K = \mathbb{C}$, le K-bimodule unitaire D constitué par $\mathbb{C}$ sur lequel $\mathbb{C}$ opère à gauche par multiplication et à droite par l'intermédiaire de l'automorphisme de conjugaison et les applications γ_1 et γ_2 identiquement nulles.

5-5-3 - Sur les problèmes de [1].

1) La première partie du premier problème n'a pas été examinée. Par contre, dans le cas $n = 2$, l'indépendance des axiomes (1), (2), (2'), (3), (3') de [1], a été mise en évidence par l'étude qui en a été donnée dans les propositions 3-3-1 et 4-2-2 et le théorème 4-2-3 dans lequel (a) traduit l'associativité de l'addition et (d_1) et (d_2) la distributivité à gauche et à droite de la multiplication par rapport à l'addition.

2) Le second problème demande des exemples d'anneaux locaux artiniens à gauche, non commutatifs. Les théorèmes 5-3-1 et 5-4-1 donnent des méthodes de construction. On va se limiter à montrer que pour tout entier $n \geqslant 2$, il existe au moins un anneau local artinien à gauche A, non commutatif et d'exposant n.

En effet, pour tout corps K possèdant un automorphisme σ différent de l'identité (par exemple $K = \mathbb{C}$), en posant $I = [0, n-1]$, on peut vérifier qu'on obtient un tel anneau A en définissant sur K^I, une addition et une multiplication caractérisées par les conditions suivantes :

- l'addition est celle de l'espace vectoriel K^I
- la multiplication associe à deux éléments $\alpha = (\alpha_i)$ et $\beta = (\beta_\gamma)$ un élément $\gamma = (\gamma_\kappa)$ dont les composants sont données par :

$$\gamma_\kappa = \sum_{k = i+j} \alpha_i \sigma^i(\beta_\gamma) \quad .$$

3) Le troisième problème n'a pas été traité sous sa forme initiale, mais le théorème 5-4-1 montre que dans la caractérisation des anneaux locaux artiniens à gauche, les A'-modules à gauche de type fini qui interviennent, se déduisent en fait, par extension des scalaires, à partir de bi-modules unitaires sur un corps K. Quant à l'étude des homomorphismes i de A dans $\mathcal{L}_A(D)$, leur interprétation à l'aide de

la notion de bi-module, montre également que pour la construction d'anneaux locaux artiniens à gauche, il convient surtout d'étudier les K-modules unitaires. Dans le cas général, lorsque D ou Δ sont de dimension m à gauche sur K , on est amené à étudier des systèmes de m^i applications additives de K dans K , assujetties à certaines conditions. Lorsque $m = 1$, on voit que D ou Δ est constitué par K sur lequel K opère à gauche par multiplication et à droite par l'intermédiaire d'un automorphisme de K .

- BIBLIOGRAPHIE -

[1] L. LESIEUR - Structure d'un anneau local artinien à gauche.
Séminaire Dubreil-Pisot : Algèbre et Théorie des nombres 21e année, 1967/68 - n° 3 , 10 p. -

[2] S. EILENBERG and S. MAC'LANE - Cohomology theory in abstract groups I.
Annals of Mathematics Vol. 48, 1947, p. 51-78. -

[3] U. SHUKLA - Cohomologie des algèbres associatives.
Ann. Scient. Ec. Norm. Sup. 3e série, t. 78, 1961, p. 163-209 -

[4] G. HOCHSCHILD - On the cohomology groups of an associative algebra -
Annals of Mathematics Vol. 46, 1945, p. 58-67 -

-:-:-:-:-:-:-

FACULTE DES SCIENCES

D'ORSAY

-:-:-:-

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 25 du 2 juin 1969

-:-:-:-:-:-:-:-:-:-

par M. Paul VAN PRAAG

(chargé de recherches du Fonds National belge de la Recherche scientifique) .

-:-:-:-:-

- LE PROBLEME DES DIMENSIONS POUR LES CORPS NON COMMUTATIFS -

1. Le problème est le suivant : K et k sont des corps et k est contenu dans K qui est dès lors un vectoriel à gauche et à droite sur k ; les dimensions à gauche et à droite $[K : k]_g$ et $[K : k]_d$ sont-elles toujours égales ?

La réponse est due à P.M. COHN [2] et est non.

Le seul but de ce texte est de décrire, suivant COHN, la "construction" d'un couple $k \subset K$ tel que :

$$[K : k]_g \neq [K : k]_d \quad .$$

Nous ne démontrons rien du tout. Une bibliographie complète du sujet (y compris des conditions suffisantes sous lesquelles les dimensions sont égales) se trouve dans [3] .

2. Préliminaires.

2.1. Z est l'anneau des entiers rationnels. Une valuation d'un anneau A est une application $v : A \to Z \cup \{\infty\}$ telle que :

(1) $v(x) = \infty$ si $x = 0$

(2) $v(xy) = v(x) + v(y)$

(3) $v(x-y) \geq \min \{v(x), v(y)\}$.

Soit A un anneau et v une valuation de A, pour tout $n \in Z$ on pose :

$$A_n = \{x \in A \mid v(x) \geq n\} .$$

Les A_n sont des sous-groupes de A, qui filtrent A, c'est-à-dire :

$$A_n \supseteq A_{n+1}$$

$$\bigcup_{n \in Z} A_n = A$$

$$\bigcap_{n \in Z} A_n = \{0\}$$

$$A_n A_m \subseteq A_{n+m}$$

Si $a_n \in A_n$ et $a_m \in A_m$, alors

$$a_n a_m + A_{n+m+1}$$

ne dépend que de $a_n + A_{n+1}$ et de $a_m + A_{m+1}$. Nous pouvons donc poser :

$$(a_n + A_{n+1}) \cdot (a_m + A_{m+1}) = a_n a_m + A_{n+m+1} .$$

En étendant cette loi par distributivité à la somme directe $G(v)$

des groupes quotients A_n/A_{n+1} , on érige $G(v)$ en un anneau.

Cet anneau est appelé anneau gradué de v , il ne contient pas de diviseurs de zéro (A non plus).

2.2. On sait (Ore) qu'un anneau A admet un corps de fractions à droite si il satisfait aux deux conditions :

O_1 : A $\not\ni$ de diviseurs de zéro,

O_2 : deux éléments non nuls de A ont toujours un multiple commun à droite dans A .

2.3. P.M. COHN a démontré [1] le

Théorème : Si A est un anneau et v une valuation de A telle que $G(v)$ satisfasse à la condition O_2 , alors il existe un corps D qui contient A .

Remarque : D n'est en général pas un corps de fractions de A (à moins que A ne satisfasse lui-même à O_2) mais on peut prolonger v à D et tout élément de D est la limite (pour v) d'une suite d'éléments $a_n b_n^{-1}$ avec a_n et $b_n \in A$: pour tout $x \in D$, il existe des a_n et des b_n dans A tels que si $n \to \infty$, alors $v(x - a_n b_n^{-1}) \to \infty$.

3. Les corps de COHN.

F est un corps commutatif et

$$B = \{a, b_0, b_1, \ldots\} .$$

A est l'algèbre libre associative engendrée par B sur F .

S est l'endomorphisme de A tel que :

$$a^S = -a \quad \text{et} \quad b_i^S = b_{i+1} ,$$

pour tout i .

W(B) est l'ensemble des mots associatifs en les éléments de B .

On pose : $a < b_0 < b_1 < \ldots$, et on ordonne W(B) lexicographiquement. Donc deux mots sont comparables, sauf si l'un est l'origine de l'autre.

Définition : Le mot $u \in W(B)$ est dit régulier si il est dans B, ou, pour toute décomposition propre $u = u_1 u_2$, on a :

$$u_2 u_1 < u .$$

Exemples :

1) le mot $u = b_0 b_0 a$ est régulier, car les décompositions propres sont $b_0 . b_0 a$ et $b_0 b_0 . a$ et l'on a :

$$b_0 a b_0 < b_0 b_0 a$$

et $$a b_0 b_0 < b_0 b_0 a .$$

2) le mot aa n'est pas régulier.

Remarque : $u_2 u_1 < u$ n'implique pas $u_2 < u_1$:

$$b_0 a b_0 < b_0 b_0 a ,$$

mais $$b_0 a \not< b_0 .$$

Maintenant on ordonne totalement les mots réguliers en posant : si u et v sont régulieres et $u = v v_1$, alors :

$$u < v .$$

CHIRCHOV a démontré [4] que pour tout mot régulier u, il existe une et une seule manière de mettre des parenthèses pour en faire un mot non associatif (u) tel que :

(*) si $u \in B$, alors $(u) = u$

(**) si $(u) = ((v)(w))$, alors v et w sont réguliers

(***) si $(u) = (((v_1)(v_2))w)$, alors $w \geq v_2$.

Exemple : si

$$u = b_0 b_0 a \text{ , alors}$$

$$(u) = (b_0)((b_0)(a))$$

$$= b_0(b_0 a) \text{ .}$$

Pour tout mot régulier u, on va définir $[u] \in A$ par induction comme suit :

1) si $u \in B$, alors $[u] = u$

2) si $u \notin B$ et si les $[v]$ sont définis par les mots de longueur $< \ell(u)$, alors soit

$$(u) = ((v)(w)) \text{ .}$$

Si $w \neq a$, on définit :

$$[u] = [v][w] - [w][v]$$

et si $w = a$,

$$[u] = [v]a - a[v^S] \text{ .}$$

Les $[u]$ sont appelés produits basiques, l'ensemble des produits basiques est noté U .

Exercice : calculez $[b_0 b_0 a]$.

Solution : on sait que :

$$(b_o b_o a) = b_o\,(b_o a) \ .$$

Il découle de la définition des crochets que :

$$[b_o a] = [b_o]a - a[b_o^S]$$

$$= b_o a - a b_1 \ ,$$

par définition de S .

Donc : $[b_o b_o a] = b_o(b_o a - a b_1) - (b_o a - a b_1)b_o$

$$= b_o b_o a - b_o a b_1 - b_o a b_o - a b_1 b_o \ .$$

On ordonne U par l'ordre sur les mots réguliers, et on démontre que les produits

$$[u_1]\,[u_2]\,\ldots\,[u_r]$$

où $\quad [u_i] \in U \quad$ et $\quad [u_1] \leq \ldots \leq [u_r]$

forment une base de A .

Remarque : si dans cette construction on remplace S par la transformation identique, les produits basiques forment une base de l'algèbre de LIE de A . Nous allons munir A d'une valuation v :

si $[u] \in U$, on pose :

$$v([u]) = \ell(u) - 1 \ ;$$

si $p = [u_1] \ldots [u_s]$, on pose :

$$v(p) = \sum_{i=1}^{s} v[u_i] \ ;$$

et si

$$f = \Sigma\, p a_p \ , \text{ où } \quad a_p \in F \ ,$$

alors

$$v(f) = \inf\{v(p) \mid a_p \neq 0\} \ .$$

On démontre que v ainsi défini est effectivement une valuation de A et que l'anneau gradué $G(v)$ satisfait à O_2 (on peut décrire $G(v)$ comme suit : soit $U_1 = U \setminus \{a\}$ et $R = F[U_1]$, l'anneau des polynômes commutatifs en U_1 sur F. Dès lors $G(v)$ est à un isomorphisme près l'anneau $R[a, S]$ des polynômes en a à coefficients dans R, la multiplication satisfaisant à :

$$ra = ar^S \quad \text{pour tout} \quad r \in R \quad) .$$

D'après le théorème de plongement de P.M. COHN (2.3.), A est contenu dans un corps V (S joue un rôle : V est complet pour une valuation qui prolonge v, laquelle est construite à partir des produits basiques qui font intervenir S dans leur définition).

K est le sous-corps de V engendré par B (le théorème de prolongement n'affirme pas que A engendre algébriquement V).

k est le sous-corps de K engendré par a^2 et $U_1 (= U \setminus \{a\})$.

On a :

$$[K : k]_d = 2$$

mais

$$[K : k]_g > 2 .$$

Si l'on peut démontrer l'existence d'un surcorps de K qui soit galoisien [4, chap. VII] sur k, alors on aura démontré [même référence] que :

$$[K : k]_g = \infty .$$

- BIBLIOGRAPHIE -

[1] P.M. COHN, On the embedding of rings in skew fields, Proc. London, Math. Soc. (3) 11 (1961) 511-30.

[2] P.M. COHN, Quadratic extensions of skew fields, Proc. London, Math. Soc. (3) 11 (1961) 531-56.

[3] N. JACOBSON, Structure of rings, Am. Math. Soc. Coll. Pub., vol. XXX VII, 1964, Revised ed.

[4] A.I. ŠIRŠOV, On free Lie rings, Math. Sbornik, 45 (87) (1958) 113-22.

-:-:-:-:-:-:-:-:-:-:-