PUBLICATIONS MATHEMATIQUES D'ORSAY

SEMINAIRE

D'ALGEBRE NON COMMUTATIVE

1ère Partie

Année 1970/71

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

TABLE DES MATIERES

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

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' A L G E B R E   N O N   C O M M U T A T I V E

<u>1ère Partie</u>

Année 1970/71

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

FACULTE DES SCIENCES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE.

-:-:-:-:-:-

Conférence n° 1 du 4 Novembre 1970

- GENERALITES SUR LES ANNEAUX DE GROUPE -

par

G. RENAULT

rédigée par J. de SAINTIGNON

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

1. DEFINITION.

Dans tout ce qui suit, A sera un anneau unitaire, dont on notera 1 l'élément unité, et G un groupe multiplicatif d'élément neutre e.

Définition : On appelle anneau de groupe, associé à A et G, et noté $A[G]$, l'ensemble de toutes les applications r de G dans A, qui sont à support fini (supp. $r = \{g \in G \; ; \; r(g) \neq 0\}$). On peut munir cet ensemble $A[G]$ des deux opérations suivantes :

- une addition : $r, r' \in A[G]$, $g \in G$: $(r+r')(g) = r(g) + r'(g)$.

- une multiplication : $r, r' \in A[G]$, $g \in G$: $(rr')(g)$

$$= \sum_{hh'=g} r(h)r'(h')$$

qui confèrent à $A[G]$ une structure d'anneau unitaire. (L'élément unité de $A[G]$ est l'application caractéristique de $e \in G$).

Remarques :

a) On peut plonger A et G dans $A[G]$ de la façon suivante :

- à tout $a \in A$, on associe $a^* \in A[G]$: $\begin{cases} a^*(e) = a \\ \forall_{g \neq e} \; a^*(g) = 0 \end{cases}$

Cette application $a \to a^*$ est un monomorphisme d'anneaux de A dans $A[G]$, ce qui permet d'identifier les éléments $a \in A$ à leurs images $a^* \in A[G]$.

- à tout $g \in G$, on associe $g^+ \in A[G]$: $\begin{cases} g^+(g) = 1 \\ \forall_{h \neq g} \; g^+(h) = 0 \end{cases}$.

Cette application $g \to g^+$ est un monomorphisme de semi-groupes de G dans $A[G]$, ce qui nous permet d'identifier les éléments $g \in G$ à leurs images $g^+ \in A[G]$.

b) Les fonctions g^+ sont les applications caractéristiques des éléments de G d'où : $\forall_{r \in A[G]} \quad r = \sum_{g \in G} r(g) * g^+$, ce que l'on peut écrire, d'après a) :

$$r = \sum_{g \in G} r(g) g .$$

c) $A[G]$ est un A-module libre de base G, car il est clair, d'après b), que G engendre $A[G]$, et que :

$$r = \sum_{g \in G} r(g) g = 0 \iff \forall_{g \in G} \quad r(g) = 0 .$$

d) En se référant à la remarque a), on montre que :

$$\forall_{a \in A} \quad \forall_{g \in G} \qquad ag = ga .$$

e) Enfin, remarquons que, dans tout ce qui vient d'être fait, le groupe G peut être remplacé par un ensemble quelconque S. L'ensemble $A\{S\}$ ainsi obtenu n'aura qu'une structure de A-module libre de base S.

Ceci ne servira ici, que dans le cas où $S = G/H$, H étant un sous groupe quelconque de G . On pourra alors définir les applications :

$$f_H : A[G] \to A\{G/H\}$$

par :

$$f_H(\sum_{g\in G} r(g)g) = \sum_{g\in G} r(g)\, gH .$$

(gH classe à droite de g dans G/H). On vérifie que les f_H sont des épimorphismes de A-modules.

2. IDEAUX REMARQUABLES DE $A[G]$.

Nous allons établir une correspondance ω entre l'ensemble des sous-groupes de G et l'ensemble des idéaux à gauche de $A[G]$: à tout sous-groupe de G , associons l'idéal à gauche de $A[G]$, engendré par les éléments $(1-h)$, où $h \in H$. On notera cet idéal $\omega(H)$.

Proposition 1 : si H est un sous-groupe de G , on a :

$$\ker f_H = \omega(H) .$$

Démonstration :

- f_H étant un homomorphisme de A-modules, on a :

$$h \in H \Longrightarrow f_H(1-h) = f_H(1) - f_H(h) = 0$$

d'où :

$$f_H(\omega(H)) = \{0\} .$$

- si $r \in A[G]$ est tel que $f_H(r) = 0$, et si S est un système de représentants des classes $\{gH , g \in G\}$ de G/H :

$$f_H(r) = \sum_{g\in G} r(g)gH = \sum_{s\in S} [\sum_{h\in H} r(sh)]sH = 0$$

d'où :

$$\forall_{s\in S} \sum_{h\in H} r(sh) = 0$$

et on peut écrire :

$$r = \sum_{g\in G} r(g)g = \sum_{s\in S}\sum_{h\in H} r(sh)sh = \sum_{s\in S}\sum_{h\in H} r(sh)(sh-s)$$

d'où : $$r = \sum_{s\in S}\sum_{h\in H} r(sh)s(h-1) \in \omega(H) .$$

La proposition est ainsi démontrée.

Conséquence : ω est une application strictement croissante.

Démonstration : Tout d'abord il est clair que ω est croissante, et si H et H' sont deux sous-groupes de G :

$$H \underset{\neq}{\subset} H' \Rightarrow \exists_{h'\in H'} \quad h' \notin H \Rightarrow f_H(1-h') = f_H(1) - f_H(h') \neq 0$$

d'où : $$(1-h') \notin \omega(H) \quad \text{et donc} \quad \omega(H) \underset{\neq}{\subset} \omega(H') .$$

Remarques :

1) Si H est un sous-groupe normal de G, G/H est alors un groupe multiplicatif, et $A[G/H]$ un anneau de groupe. Alors f_H devient un épimorphisme d'anneaux, et, d'après la Proposition 1, $\omega(H)$ est un idéal bilatère.

2) En particulier $\ker f_G = \omega(G)$ et f_G permet de définir un isomorphisme d'anneaux : $A \simeq A[G]/\omega(G)$. Cela entraîne que $\omega(G)$ est un idéal propre de $A[G]$, ainsi d'ailleurs que tous les $\omega(H)$, d'après le corollaire.

On appelle $\omega(G)$ l'idéal fondamental de $A[G]$ et

$f_G \left(\sum_{g\in G} r(g)g \to \sum_{g\in G} r(g)\right)$ l'application d'augmentation de $A[G]$.

Proposition 2 : si H est un sous-groupe d'ordre infini, alors l'annulateur à gauche de $\omega(H)$ et l'annulateur à droite de $\omega(H)$ sont nuls.

Démonstration : Soit $\ell(\omega(H))$ l'annulateur à gauche de $\omega(H)$. Supposons qu'il existe dans $\ell(\omega(H))$ un élément x non nul :

$$x = a_1 g_1 + \dots + a_n g_n \quad \text{avec} \quad a_1 \neq 0 .$$

Alors $\forall_{h\in H}$ $x(1-h) = 0 \Rightarrow a_1g_1 + \dots + a_ng_n = a_1g_1h + \dots + a_ng_nh$ et comme l'ensemble des $g_1^{-1}g_i$ est fini

$$\exists_{h\in H}\ \forall_{i=1,\dots,n}\ h \neq g_1^{-1}g_i \text{ , c'est-à-dire } \exists_{h\in H}\ \forall_{i=1,\dots,n}\ g_1h \neq g_i$$

et $$a_1g_1 + \dots + a_ng_n = a_1g_1h + \dots + a_ng_nh$$

sont deux décompositions distinctes d'un même élément de $A[G]$, ce qui est impossible, puisque $A[G]$ est un A-module libre.

Donc $\ell(\omega(H)) = \{0\}$, et on montrerait de la même façon que $r(\omega(H)) = \{0\}$.

Proposition 3 : si H est un sous-groupe de G engendré par la famille d'éléments $(h_i)_{i\in I}$. Alors $\omega(H)$ est l'idéal à gauche de $A[G]$ engendré par $(1-h_i)_{i\in I}$.

Démonstration : Tout d'abord, il est clair que $\omega(H)$ contient l'idéal à gauche de $A[G]$ engendré par $(1-h_i)_{i\in I}$. D'autre part si $h \in H$, h est un produit fini de h_i et de h_i^{-1} , et on montre que $(1-h)$ est combinaison linéaire de $(1-h_i)$ par récurrence sur le nombre de h_i et de h_i^{-1} qui interviennent dans h .

Problème.

A quelles conditions l'anneau $A[G]$ est-il régulier au sens de Von Neuman ?

- Il faut que A soit régulier, car $A \simeq A[G]/\omega(G)$.

- Il faut que G soit localement fini car si H est un sous-groupe de type fini de G , $\omega(H)$ est un idéal à gauche de type fini, et comme $A[G]$ est régulier, $\omega(H)$ est principal et facteur direct dans $A[G]$, d'où $\ell(\omega(H)) \neq \{0\}$ et donc, d'après la Proposition 2, H est fini.

- Il faut que l'ordre de tout sous-groupe fini de G soit unité dans A .

Montrons que l'ordre de tout élément d'ordre fini de G est unité dans A . Soit donc $g \in G$, $O(g) = n$, par hypothèse :

$$\exists_{r \in A[G]} \quad (1-g)r(1-g) = 1 - g$$

d'où : $$(1-(1-g)r)(1-g) = 0$$

ce qui entraîne : $$(1-(1-g)r \in \ell(1-g) = A[G](1+g+..+g^{n-1})$$

(cf. RIBENBOIM [8]). D'où :

$$\exists_{r' \in A[G]} \quad 1-(1-g)r = r'(1+g+..+g^{n-1})$$

et en appliquant l'homomorphisme f_G , on obtient :

$$f_G(1-(1-g)r = 1 - f_G(r'(1+g+..+g^{n-1})) = f_G(1')n$$

d'où : $$f_G(1')n = 1$$

et n est bien inversible.

Il est possible (cf. LAMBEK [6]) de montrer que ces trois conditions nécessaires sont suffisantes pour que $A[G]$ soit régulier.

<u>Remarque</u> : si H est un sous-groupe fini de G , d'ordre inversible dans A , $\omega(H)$ est facteur direct dans $A[G]$.

Car si $n = O(H)$ est inversible dans A :

$$\omega(H) = A[G](1-n^{-1} \sum_{h \in H} h)$$

en effet $$r(1-n^{-1} \sum_{h \in H} h) = rn^{-1}(\sum_{h \in H} (1-h) \in \omega(H)$$

et si $g_i \in H$: $(1-g_i)n^{-1}(n+(1+g_2+\dots+g_n)) = (1-g_i)$

d'où : $$(1-g_i) \in A[G]\ (1-n^{-1} \sum_{h \in H} h) .$$

Donc, on a bien l'égalité annoncée, et comme il est facile de vérifier que $(1-n^{-1} \sum_{h \in H} h)$ est un idempotent de $A[G]$, $\omega(H)$ est facteur direct dans $A[G]$.

On peut d'ailleurs améliorer ce résultat dans le cas de G , et montrer que :

$\omega(G)$ est facteur direct dans $A[G]$ si et seulement si G est fini et d'ordre inversible dans A .

La condition suffisante a été montrée ci-dessus, et pour la condition nécessaire, si $\omega(G)$ est facteur direct, $\ell(\omega(G))$ est non nul et donc G est fini d'ordre n . Alors si $G = \{g_1, \ldots, g_n\}$, et comme on a :

$$\ell(\omega(G)) = r(\omega(G)) = A(g_1+\ldots+g_n)$$

et $$A[G] = \omega(G) \oplus \ell(\omega(G)) \qquad \text{(cf. CONNELL [4])}$$ on peut écrire :

$$\exists_{a_1,\ldots,a_n \in A} \quad 1 = \sum_{i=2}^{n} a_i(1-g_i) + a_1(g_1+\ldots+g_n)$$

d'où : $$1 = \sum_{i=1}^{n} a_i + \sum_{i=2}^{n} (a_1-a_i)g_i$$

et comme $A[G]$ est un A-module libre :

$$\forall_{i = 2,\ldots,n} \quad a_i = a_1$$

et donc : $$1 = na_1 .$$

3. RADICAL DE JACOBSON DE $A[G]$.

Dans ce paragraphe, nous noterons $\mathrm{rad}(R)$ le radical premier de l'anneau R et $\mathrm{Rad}(R)$ son radical de Jacobson.

Il est bien connu, cf. RIBENBOIM [8] , que l'on a toujours l'égalité :

$$\mathrm{rad}(A) = A \cap \mathrm{rad}(A[G])$$

alors que, pour les radicaux de Jacobson, on n'a, en général, que l'inclusion :

$$\mathrm{Rad}(A) \supset \mathrm{Rad}(A[G]) \cap A .$$

Toutefois, il est possible d'améliorer ce dernier résultat dans les deux cas suivants :

- quand A est artinien à gauche, car alors les deux radicaux de A

sont égaux et on a :

$$\mathrm{Rad}(A) = \mathrm{rad}(A) = A \cap \mathrm{rad}(A[G]) \subset A \cap \mathrm{Rad}(A[G]) .$$

- quand G est localement fini : on doit montrer que si $a \in \mathrm{Rad}(A)$, $a \in \mathrm{Rad}(A[G])$, c'est-à-dire que : $a \in \mathrm{Rad}(A) \Longrightarrow \forall_{r\in A[G]} \exists_{x\in A[G]} (1+ar)x = 1$.

Soient donc $a \in \mathrm{Rad}(A)$, $r \in A[G]$ et $H = \{1,g_2,\dots,g_n\}$ le sous-groupe de G engendré par le support de r.(H est fini car G est localement fini). Alors si $r = a_1+a_2g_2+\dots+a_ng_n$, l'élément x que nous cherchons, devra être de la forme :

$$x = x_1 + x_2g_2 + \dots + x_ng_n$$

et tel que $((1+aa_1) + aa_2g_2 + \dots + aa_ng_n)(x_1 + \dots x_ng_n) = 1$. Ce qui nous conduit à résoudre un système de la forme :

$$\begin{cases} (1+aa_1)x_1 + aa_{12}x_2 + \dots + aa_{1n}x_n = 1 \\ aa_{21}x_1 + (1+aa_1)x_2 + \dots + aa_{2n}x_n = 0 \\ \dots\dots\dots\dots\dots\dots \\ aa_{n1}x_1 + aa_{n2}x_2 + \dots + (1+aa_1)x_n = 0 \end{cases}$$

Or, d'après JACOBSON [11], si B est l'anneau des matrices $n \times n$ à coefficients dans A, le radical de Jacobson de B est l'anneau des matrices $n \times n$ à coefficients dans $\mathrm{Rad}(A)$.

Il ne reste plus alors qu'à écrire le système ci-dessus sous forme matricielle : $(1+b)u = v$, où u et v sont les vecteurs colonnes $(1,0,\dots,0)$ et $(x_1,\dots,x_n)$ et qu'à constater que la matrice b est à coefficients dans $\mathrm{Rad}(A)$.

D'où $(1+b)$ étant une matrice inversible : $v = (1+b)^{-1} u$. Ce qui finit de démontrer le résultat annoncé.

Problème ouvert :

Est-ce que le radical de Jacobson d'un anneau de groupe $K[G]$, où K est un corps de caractéristique 0 et G un groupe, est nul ?

C'est une question à laquelle on ne sait pas répondre dans le cas général, mais à laquelle on sait répondre affirmativement dans les cas particuliers suivants :

- si $K = \mathbb{R}$ ou $\mathbb{C}$, il a été montré par une méthode analytique, due à RICKART [10], que $\mathrm{Rad}(\mathbb{R}[G]) = \mathrm{Rad}(\mathbb{C}[G]) = 0$.

- AMITSUR [2] a étendu ce résultat en montrant que cette propriété est vraie pour tous les corps non dénombrables de caractéristique 0.

- Et VILLAMAYOR [9] a montré que si K est un corps de caractéristique 0 et G un groupe localement fini modulo son centre (c'est-à-dire $G/e(G)$ est un groupe localement fini), $\mathrm{Rad}(K[G]) = 0$.

Enfin, citons deux résultats importants sur les radicaux de Jacobson des K-algèbres.

- si A est une K-algèbre et si $\mathrm{card}(K) > \dim_K A$, alors le radical de Jacobson de A est un nilidéal (AMITSUR [1]).

- le radical de Jacobson d'un anneau de groupe $K[G]$, où K est un corps de caractéristique p et G un groupe d'ordre p^n, est :

$$\mathrm{Rad}(K[G]) = \omega(G) \qquad \text{(JENNINS [5])}.$$

4. QUELQUES THEOREMES DE TRANSFERT.

Dans ce paragraphe, nous ne ferons qu'énoncer une suite de résultats, dont la démonstration se trouve dans LAMBEK [6] et dans RIBENBOIM [8].

(1) $A[G]$ est semi-premier si et seulement si on a les deux conditions :

a) A est semi-premier,

b) l'ordre de tout sous groupe normal fini de G est non diviseur de zéro dans A.

(2) $A[G]$ est premier si et seulement si on a les deux conditions :

a) A est premier,

b) G n'a pas de sous-groupe normal fini différent de $\{e\}$.

(3) Si $A[G]$ est noethérien à gauche, A est noethérien à gauche et toutes les suites croissantes de sous-groupes de G sont stationnaires.

Mais on ne sait pas si ces deux dernières conditions sont suffisantes pour que $A[G]$ soit noethérien à gauche, et ce n'est que sous l'hypothèse G abélien que l'on obtient une C.N.S. :

Si G est abélien, $A[G]$ est noethérien à gauche si et seulement si A est noethérien à gauche et G de type fini.

(4) $A[G]$ est artinien à gauche si et seulement si A est artinien à gauche et G fini.

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

- BIBLIOGRAPHIE -

[1] AMITSUR : "Algebras over infinite fields". Proc. Amer. Math. Soc. 7(1956) p. 35-48 .

[2] AMITSUR : "The radical of field extensions" Bull. Res. Council Isreal Section F (1957-1958) p. 1-10.

[3] AMITSUR : "On the semi-simplicity of the group algebra". Mich. Math. J. 6(1959), p. 251-253.

[4] CONNELL : "On the group ring". Can. J. Math. 15(1963) p. 650-685.

[5] JENNINS : "Structure of the group ring of a p-group over a modular field". Trans. Amer. Math. Soc. 50(1941) p. 175-185.

[6] LAMBEK : "Lectures on rings and modules".

[7] LOSEY : "On group algebra of p-group". Mich. Math. J. 7(1960) pages 237-240.

[8] RIBENBOIM: "Rings and modules". (Princeton).

[9] VILLAMAYOR:"On the semi-simplicity of group algebras". Proc. Amer. Math. Soc. 10(1959), pages 27-31.

[10] RICKART : "The uniquenen of norm problem in banach algebras". Annals of Math. (2) 51 (1950) pages 615-

[11] JACOBSON : "Structure of rings". (Providence 1956).

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

FACULTE DES SCIENCES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

-:-:-:-:-:-

Conférence n° 2 du 18 Novembre 1970

SUR LES ANNEAUX DE GROUPES

par

G. RENAULT

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

On étudie les anneaux A et les groupes G tels que les anneaux de groupes $A[G]$ soient locaux, semi-locaux, parfaits à gauche et auto-injectifs à gauche.

A désignera un anneau unitaire non nécessairement commutatif, G un groupe, les corps qui interviennent ne sont pas nécessairement commutatifs. Pour un exposé sur les anneaux de groupes on pourra consulter J. Lambek [11] et P. Ribenboim [13] .

I. ANNEAUX DE GROUPES LOCAUX.

On généralise un résultat de T. Gulliksen - P. Ribenboim - T.M. Viswanathan [7] p. 153 obtenu dans le cadre des anneaux de groupes commutatifs.

Théorème 1 : Soient A un anneau, G un groupe $\neq \{e\}$ tels que l'anneau de groupe $A[G]$ soit local. On a alors les propriétés suivantes :

a) A est un anneau local dont l'idéal à gauche maximal sera noté M.

b) le corps $K = A/M$ est de caractéristique $p \neq 0$.

c) G est un p-groupe.

Si on suppose de plus G localement fini, ces conditions sont suffisantes pour que $A[G]$ soit local.

L'anneau A isomorphe à un anneau quotient de $A[G]$ est local d'où a). Pour la même raison $K[G]$ est un anneau local. Soit H un sous-groupe de G ; alors $K[H]$ est local. En effet, soit R (resp. R') le radical de $K[G]$ (resp. $K[H]$); d'après un résultat de Connell ([3] p. 665) $K[H] \cap R \subset R'$; comme R est l'idéal fondamental de $K[G]$, $K[H] \cap R$ est l'idéal fondamental de $K[H]$: c'est un idéal à gauche maximal qui est donc égal à R' et $K[H]$ est local. Soient $x \neq e$ un élément de G , H_o le sous-groupe engendré par x . $K[H_o]$ est un anneau local et par suite l'élément $e+x-x^2$ est inversible. Il est facile de voir que cette dernière condition implique la finitude de H_o . Soit q l'ordre de x ; si q était inversible dans K , l'élément $e-q^{-1} \sum_{i=o}^{q-1} x^i$ serait un idempotent non trivial de $K[G]$ ce qui est exclu. On en déduit immédiatement les propriétés b) et c) .

Soient A un anneau, G un groupe localement fini vérifiant les conditions du théorème. G étant localement fini, $M\,A[G]$ est contenu dans le radical de $A[G]$ ([3] p. 665) et il suffit de démontrer que l'anneau $K[G]$ est local ce qui résulte facilement du lemme suivant qui est bien connu lorsque le corps est commutatif.

Lemme 2 : Soient K un corps (non nécessairement commutatif) de caractéristique $p \neq o$, G un p-groupe fini. Alors $K[G]$ est un anneau local dont le radical est un nilidéal.

Soient $H \neq \{e\}$ le centre de G , $\omega(H)$ l'idéal engendré par les éléments e-h , $h \in H$. H est produit de groupes cycliques engendrés par des éléments b_i, $1 \leqslant i \leqslant s$, et $\omega(H)$ est engendré par les $e-b_i$. Soit $x = \sum_i a_i(e-b_i)$, $a_i \in K[G]$, un élément de $\omega(H)$. Quel que soit l'entier n

$$x^n = \sum_{i_1,\ldots,i_n} a_{i_1} \times \ldots \times a_{i_n} (e-b_{i_1}) \times \ldots \times (e-b_{i_n}) .$$

Pour tout i, il existe un entier $n(i)$ tel que $(e-b_i)^{p^{n(i)}} = 0$, et $x^n = 0$ pour n suffisamment grand : $\omega(H)$ est un nilidéal contenu dans le radical de $K[G]$. $K[G]/\omega(H)$ est isomorphe à $K[G/H]$, une récurrence facile sur l'ordre de G permet de terminer la démonstration.

Remarque : Soient G le p-groupe infini engendré par trois éléments qui est décrit dans [8], k le corps à p éléments. $K[G]$ est un anneau local bien que G ne soit pas localement fini.

II. ANNEAUX DE GROUPES SEMI-LOCAUX.

Dans ce paragraphe A et G sont commutatifs.

Théorème 3 : Les conditions suivantes sont équivalentes :

1) $A[G]$ est un anneau semi-local.

2) a - A est un anneau semi-local de radical R.

b - G est fini ou G est infini et dans ce cas A/R est un anneau de caractéristique $p \neq 0$, $G = G_p \times G_0$, où G_p est un p-groupe infini, et où G_0 est un groupe fini dont l'ordre n'est pas divisible par p.

La démonstration de ce théorème n'est pas difficile, et constitue un excellent entraînement aux techniques des anneaux de groupes ; elle est donc laissée en exercice....

III. ANNEAUX DE GROUPES PARFAITS A GAUCHE [1].

Rappelons que si A est parfait à gauche, les sous-modules de type fini de tout A-module à droite vérifient la condition de chaîne descendante [2].

Théorème 4 : Soient A un anneau, G un groupe. Les conditions suivantes sont équivalentes :

(i) $A[G]$ est parfait à gauche.

(ii) a - A est parfait à gauche.

b - G est fini.

(ii) $\Longrightarrow$ (i) Car les idéaux à droite de type fini de $A[G]$ qui sont des A-modules à droite de type fini vérifient la condition de chaîne descendante [2]

(i) $\Longrightarrow$ (ii) Soit R le radical de A. Les anneaux A, $A/R[G]$ qui sont des anneaux quotients de $A[G]$ sont parfaits à gauche et il suffit d'étudier le cas où A est un anneau simple de centre k. $A[G]$ est un $k[G]$-module libre, le lemme 12 de [13] p. 150 et les résultats de [2] montrent que $k[G]$ est parfait à gauche. Supposons G infini ; alors $k[G]$ n'est pas semi-premier et il en résulte les conséquences suivantes : la caractéristique de k est $p > o$ et il existe un sous-groupe normal H_1 de G dont l'ordre soit divisible par p ([11] p. 162) G/H_1 est infini et $k[G/H_1]$ est parfait à gauche, il existe donc un sous-groupe normal H_2 de G contenant H_1 tel que p divise l'ordre de H_{2/H_1}. On met ainsi en évidence une suite croissante de sous-groupes normaux (H_n) de G d'ordre $p^{s(n)} q_n$, p ne divisant pas q_n, tels que $s(n) > s(n-1)$. Les théorèmes de Sylow permettent de construire une suite infinie strictement croissante de p-groupes finis dont la réunion est un p-groupe infini G_o. $k[G]$ est un $k[G_o]$-module libre, le lemme 12 de [13] p. 150 et les résultats de [2] prouvent que $k[G_o]$ est parfait à gauche. $k[G_o]$ est un anneau local dont le radical est l'idéal fondamental $\omega(G_o)$; le socle droit de $k[G_o]$ est non nul car $k[G_o]$ est parfait à gauche et G_o est fini ([13] p. 137) ce qui contredit l'hypothèse faite sur G.

Comme cas particulier, on obtient la caractérisation des anneaux de groupes artiniens (I.G. Connell [3]).

IV. AUTO-INJECTIVITE DES ANNEAUX DE GROUPES.

Le résultat suivant a été établi par I.G. Connell ([3] p. 663).

Proposition 5 :

(i) Soient A un anneau auto-injectif à gauche, G un groupe fini. Alors $A[G]$ est auto-injectif à gauche.

(ii) Soit $A[G]$ un anneau de groupe auto-injectif à gauche. Alors A est auto-injectif à gauche et G est un groupe de torsion.

L'assertion (ii) se complète ainsi.

Lemme 6 : Si $A[G]$ est auto-injectif à gauche, alors G est un groupe localement fini.

Soit H un sous-groupe de type fini de G, l'idéal à droite $\omega(H)$ engendré par les éléments $1-h$, $h \in H$, est un idéal à droite de type fini de $A[G]$ et d'après un résultat d'Ikeda et de Nakayama (Proc. Amer. Math. Soc. 5 (1964) pp. 15-19) l'annulateur à gauche de $\omega(H)$ est non nul et H est fini [11].

Proposition 7 : Soit A un sous-anneau d'un anneau B tel que B soit un A-module à droite libre. Alors tout B-module à gauche injectif est A-injectif.

Ce résultat est une conséquence de (H. Cartan - S. Eilenberg, p.123, exercice 10). Nous allons donner la démonstration de ce cas particulier. Soit $(g_i)_{i \in I}$ une base de B sur A.

$$B = \bigoplus_{i \in I} g_i A \ .$$

Si J est un idéal à gauche de A , l'idéal à gauche de B engendré par J est l'idéal :

$$J' = \bigoplus_{i \in I} g_i J .$$

Soient M un B-module à gauche injectif et f un homomorphisme de J dans M . On définit un B-homomorphisme f de J' dans M en posant :

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

M étant B-injectif, il existe $m \in M$ tel que :

$$f'(a') = a'm \quad \text{quel que soit} \quad a' \in J'$$

en particulier on a :

$$g_i A[f(a)-am] = 0 \qquad \forall i \in I , \qquad \forall a \in J ,$$

ce qui entraîne :

$$f(a) = am \qquad \forall a \in J$$

et M est A-injectif.

<u>Lemme 8</u> : <u>Soit H un sous-groupe de G . Alors $A[G]$ est un $A[H]$ module libre à droite et à gauche.</u>

Soit $(g_i)_{i \in I}$ un système de représentants des classes à gauche de H dans G . $(g_i)_{i \in I}$ est une base du $A[H]$-module à droite $A[G]$.

<u>Lemme 9</u> : <u>Soit A une k-algèbre. Alors $A[G]$ est un $k[G]$-module libre à gauche et à droite.</u>

Soit $(e_i)_{i \in I}$ une base de A sur k . Tout élément x de $A[G]$ s'écrit :

$$x = \sum_g r(g)g \qquad r(g) \in A \qquad \forall g \in G .$$

Posons $r(g) = \sum_i r(g)_i \, e_i$. $r(g)_i \in k$, $\forall i \in I$ on obtient :

$$x = \sum_i \left(\sum_g r(g)_i \, g \right) e_i$$

et $(e_i)_{i \in I}$ est une base du $k[G]$-module $A[G]$.

<u>Proposition 10</u> : <u>Soient A un anneau, G un groupe infini tels que $A[G]$ soit auto-injectif à gauche. Alors :</u>

(i) <u>Pour tout sous-groupe H de G . $A[H]$ est auto-injectif à gauche.</u>

(ii) <u>L'intersection des sous-groupes infinis de G est un sous-groupe normal G_o d'indice fini et G_o est un groupe abélien de type p^∞</u> .

(i) Soit H un sous-groupe de G ; le lemme 8 et la proposition 7 impliquent que $A[H]$ est auto-injectif à gauche.

(ii)

<u>Lemme 11</u> : <u>Soient A un anneau, G un groupe infini tels que $A[G]$ soit auto-injectif à gauche. Alors A est un anneau quasi-frobenusien.</u>

D'après la proposition 7, $A[G]$ est un A-module à gauche libre, donc A est Σ-injectif ; il en résulte d'après C. Faith [4] que A est quasi-frobenusien. Soit H un sous-groupe infini de G ; d'après le lemme 8 et la proposition 7, $A[G]$ est un $A[H]$-module injectif. H étant infini, $A[H]$ n'est pas un anneau quasi-frobenusien et d'après C. Faith [4] H est d'indice fini. Les sous-groupes d'indice fini de G vérifient donc la condition de chaîne descendante et le lemme de Poincaré [11] montre l'existence d'un sous-groupe d'indice fini minimum G_o qui est un sous-groupe normal de G et tout sous-groupe propre de G_o est fini.

D'après les résultats de Kegel-Wehrfrits-Sunkov [10] [14] , G_o est un groupe abelien de type p^∞ .

Proposition 12 : Soient A un anneau de radical R , G un groupe tels que $A[G]$ soit auto-injectif à gauche et tel que l'ordre $O(g)$ de tout élément g de G , $g \neq 1$ soit non diviseur de zéro dans A . Alors G est un groupe fini et $R(A[G]) = \{ \sum_g r(g)g : r(g) \in R \}$.

D'après le lemme 11 on peut supposer A quasi-frobenusien et par suite $O(g)$ est inversible dans A donc dans A/R ; G étant localement fini (lemme 8) $A/R[G]$ est un anneau régulier de Von Neumann [11] et par suite :

$$R(A[G]) \subset R(G) = \{ \sum_g r(g)g \ ; \ r(g) \in R\} .$$

Comme d'autre part on a $R(A[G]) \cap A = R$ ([3]) p. 665) il en résulte que $R(A[G]) = R[G]$. D'après un théorème de Y. Utumi [15] ; $A[G]/R(A[G])$ est un anneau régulier auto-injectif à gauche et $A/R[G]$ isomorphe à $A[G]/R(A[G])$ est auto-injectif à gauche. On se ramène de façon standard à examiner le problème lorsque A est un anneau simple de sous-corps premier k ; le lemme 9 et la proposition 7 montrent qu'il suffit d'étudier le cas $k[G]$ régulier auto-injectif à gauche où $k = \mathbb{Z}/(p)$ (resp. $\mathbb{Q}$) . Nous allons utiliser une méthode due à E. Gentile [6] . D'après la proposition 10 , G est dénombrable et la semi-simplicité de $k[G]$ donc la finitude de G résultera de la propriété suivante :

Lemme 13 : Soient A un anneau de radical R , tel que A/R soit dénombrable, G un groupe tel que $A[G]$ soit auto-injectif à gauche. Si R' désigne le radical de $A[G]$, alors $A[G]/R'$ est un anneau semi-simple.

$B = A[G]/R'$ est un anneau régulier auto-injectif à gauche [9] et dénombrable et tout idéal à gauche de B est projectif (J. Kaplansky[9]) donc B est un anneau héréditaire. Tout B-module cyclique est injectif, donc B est semi-simple (B. Osofsky [12]).

Théorème 14 : Soient A un anneau, G un groupe infini tels que $A[G]$ soit auto-injectif à gauche. Alors on a les propriétés suivantes :

(i) A est un anneau quasi-frobenusien de caractéristique p^n (p premier).

(ii) L'intersection des sous-groupes infinis de G est un sous-groupe normal G_0 d'indice fini et G_0 est isomorphe au groupe abelien de type p^∞.

Cela résulte des résultats précédents et du théorème 73. 1, p. 283 de [5].

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

BIBLIOGRAPHIE

[1] H. BASS : Finistic homological Algebra and a Homological generalization of semi-primary rings. Trans. Amer. Math. Soc., 95 (1960), pp. 466-488.

[2] J.E. BJORK : Journal Für die Reine und angewandte Mathemati. Band 236 (1969).

[3] I.G. CONNELL : On the groups rings. Can. J. Math. 15 (1963) pp. 650-685.

[4] C. FAITH : Rings with ascending condition on annihilators. Nagoya Math. J. 27 (1966) pp. 179-191.

[5] L. FUCHS : Abelian groups. Budapest Hungarian Academy of Sciences (1968).

[6] E. GENTILE : A note on injective groups rings. Proc. Amer. Math. Soc. vol. 23 N° 2 (1969).

[7] T. GULLIKSEN - P. RIBENBOIM - T.M. VISWANATHAN : J. Für die Reine und angew. Math., band 242 (1970) pp. 148-162.

[8] I.N. HERSTEIN : Non commutative rings (the carus Mathematical Monographs).

[9] I. KAPLANSKY : On dimension of modules and algebras. Nagoya. Math. J. 13 (1969) pp. 85-88.

[10] O.H. KEGEL and B.A.F. WEHRFRITZ : Strong Finiteness Conditions in locally Finite groups. Math. Z. 117. pp. 309-324 (1970).

[11] J. LAMBECK : Lectures on rings and modules - Blaisde 11 Waltham (1966).

[12] B. OSOFSKY : Rings all whose finitely generated modules are injective, Pacific J. Math., 14 (1964) pp. 645-650).

[13] P. RIBENBOIM : Rings and modules. Tracts in Mathematics 24 Interscience.

[14] V.P. SUNKOV : On the minimality problem for locally finite groups : Algebra i Logika 9 (1970) pp. 220-248.

[15] Y. UTUMI : On continuous rings and self injective rings. Trans. Amer. Math. Soc. 118 (1965) pp. 158-173.

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

FACULTE DES SCIENCES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence n° 3 du 2 Décembre 1970

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

MODULES SUR LES ANNEAUX DE POLYNOMES DIFFERENTIELS

par Richard E. BLOCK

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

Une dérivation δ d'un anneau A est une application additive de A dans A telle que :

$$\delta(ab) = \delta(a)b + a(\delta b) \qquad \forall a,b \in A \ .$$

Soient A un anneau (associatif) unitaire, et $\Delta = \{\delta_\omega\}_{\omega \in \Omega}$ une famille de dérivations de A. Nous construisons alors un anneau $A[X ; \Delta]$ appelé anneau de polynômes différentiels, de la façon suivante :

soit $X = \{X_\omega\}_{\omega \in \Omega}$ une famille d'indéterminées ; $A[X ; \Delta]$ est le A-module à gauche libre engendré par l'ensemble des monômes (non commutatifs) de la forme : $X_{\omega_1} \ldots X_{\omega_n}$ $(n = 0,1,\ldots)$; la multiplication est déterminée par la formule :

$$X_\omega a = a X_\omega + \delta_\omega a \ ,$$

c'est-à-dire inductivement par :

$$(aX_{\omega_1} \ldots X_{\omega_n})(bX_{\omega_{n+1}}, X_{\omega_{n+k}}) = (aX_{\omega_1} \ldots X_{\omega_{n-1}})(bX_{\omega_n} \ldots X_{\omega_{n+k}})$$
$$+ (aX_{\omega_1} \ldots, X_{\omega_{n-1}})((\delta_{\omega_n} b)X_{\omega_{n+1}} \ldots X_{\omega_{n+k}}) \ .$$

Montrons que cette multiplication est associative : nous considérons A comme un sous-anneau de $A[X\ ;\ \Delta]$; on remarque que dans tout anneau B (non nécessairement associatif), l'ensemble :

$$N = \{u \in B \mid (uv)w = u(vw) \qquad \forall v,w \in B\}$$

est un sous-anneau.

Pour $B = A[X\ ;\ \Delta]$, on a évidemment :

$$A \subseteq N$$

et il suffit de montrer que : $X_\omega \in N$, c'est-à-dire :

$$(X_\omega u)v = X_\omega(uv) \qquad \forall u,v \in A[X\ ;\ \Delta]$$

et il suffit d'étudier le cas où u est de la forme $aX_{\omega_1},\ldots,X_{\omega_n}$ et v est un élément de A, ce qui se fait par induction :

si $n = 0$, on a :

$$\begin{aligned} X_\omega(av) &= avX_\omega + \delta_\omega(av) = avX_\omega + a(\delta_\omega v) + (\delta_\omega a)v \\ &= aX_\omega v + (\delta_\omega a)v = (X_\omega a)v \end{aligned}$$

car δ_ω est une dérivation.

Le passage de $(n-1)$ à n est laissé au lecteur.

Dans le cas où l'ensemble d'indices Ω ne contient qu'un seul élément la structure de $A[X\ ;\ \Delta]$ a été étudiée sous différents aspects (en particulier lorsque A est un corps), par plusieurs auteurs : cette étude commence en fait avec les travaux de Noether et Schmeidler, de Ore et de Jacobson et est à l'origine de la théorie des anneaux non commutatifs.

Nous voulons, dans cet exposé, étudier la structure des A-modules qui sont aussi des $A[X\ ;\ \Delta]$-modules.

Nous constatons que $A[X\ ;\ \Delta]$ a une propriété universelle pour certaines applications.

En fait, pour tout anneau B, toute famille $\{d_\omega\}_{\omega \in \Omega}$ d'éléments de B, et tout homomorphisme : $\tau : A \to B$, tel que :

$$[d_\omega\ ,\ \tau a] = \tau(d_\omega a) \qquad \forall \omega \in \Omega \quad a \in A$$

il existe un unique homomorphisme f de $A[X\ ;\ \Delta]$ dans B, tel que :

$$f(a) = \tau(a) \qquad \forall a \in A$$

$$f(X_\omega) = d_\omega \qquad \forall \omega \in \Omega \quad .$$

Cette propriété universelle peut aussi se traduire par la représentabilité d'un certain foncteur.

Soit ${}_AM$ un module, qui sera toujours supposé unitaire, τ la représentation correspondante, de A dans M, et

$D = \{d_\omega\}_{\omega \in \Omega}$ une famille d'éléments de $\mathrm{Hom}_{\mathbb{Z}}(M,M)$, avec :

$[d_\omega, \tau a] = \tau(\delta_\omega a) \qquad (\forall \omega \in \Omega\ ,\ a \in A)$ où

$[\alpha,\beta] = \alpha \circ \beta - \beta \circ \alpha$ dans $\mathrm{Hom}_{\mathbb{Z}}(M,M)$

D est alors appelée une famille de transformations différentielles de M par rapport à Δ.

D'après la propriété universelle ci-dessus, il existe une unique représentation σ de $A[X\ ;\ \Delta]$ dans M prolongeant la représentation τ et telle que :

$$\sigma X_\omega = d_\omega \qquad (\forall \omega \in \Omega)$$

Réciproquement, si M est un $A[X\ ;\ \Delta]$-module (avec la représentation σ), alors $\{\sigma X_\omega\}_{\omega \in \Omega}$ est une famille de transformations différentielles de ${}_AM$ par rapport à Δ.

<u>Définitions</u> : Le A-module M (ou la représentation τ correspondante) est <u>A-admissible</u> s'il existe une famille de transformations différentielles (c'est-à-dire si on peut prolonger τ en une représentation σ de $A[X ; \Delta]$ dans M).

M est <u>Δ-irréductiblement admissible</u> si on peut prolonger τ en une représentation irréductible de $A[X ; \Delta]$ dans M (ce qui est équivalent à l'existence d'une famille D de transformations différentielles de ${}_A M$ par rapport à Δ telle qu'il n'existe aucun sous-module propre N de ${}_A M$ pour lequel : $\delta_\omega N \subset N \qquad (\forall \omega \in \Omega)$)

M est aussi appelé <u>différentiablement irréductible</u> s'il existe une famille Δ telle qu'il soit Δ-irréductiblement admissible.

Un des résultats principaux de cet exposé est la détermination explicite de tous les A-modules différentiablement irréductibles, lorsque A est artinien (à gauche ou à droite).

Pour pouvoir énoncer ce résultat nous avons encore besoin de certaines difinitions.

Un idéal I de A est appelé <u>Δ-idéal</u> si :

$$\delta_\omega I \subseteq I \qquad (\forall \omega \in \Omega) .$$

On remarque que les Δ-idéaux bilatères sont justement les noyaux de ces homomorphismes de A dans un anneau arbitraire, qu'on peut prolonger en un homomorphisme de $A[X ; \Delta]$ dans le même anneau.

Pour tout idéal bilatère I de A , il existe un unique plus grand Δ-idéal I_Δ de A contenu dans I (obtenu comme la somme de tous les Δ-idéaux bilatères de A contenus dans I). On appelle R_Δ le Δ-radical de A , où R est le radical de Jacobson de A .

On a aussi : $R_\Delta = \bigcap_P P_\Delta$ où P parcourt l'ensemble des idéaux primitifs de A.

A est Δ semi-simple si $R_\Delta = 0$, Δ-simple s'il ne contient aucun Δ-idéal propre, et différentiablement simple s'il existe une famille Δ telle qu'il soit Δ-simple.

Donnons des exemples :

si A est simple, alors A est Δ-simple pour toute famille Δ,

si ${}_AM$ est la somme directe d'une famille de A-modules irréductibles isomorphes, alors M est différentiablement irréductible.

En effet, on peut choisir $\delta_\omega = 0$ $(\forall \omega \in \Omega)$, et les éléments d_ω appartenant au commutant de ${}_AM$.

Soit F un anneau commutatif de caractéristique p premier, et n un entier : on note $B_n(F)$ l'anneau commutatif :

$$F[X_1,\ldots, X_n]/(X_1^P,\ldots, X_n^P)$$

où $X_1, \ldots, X_n$ sont des indéterminées ; il est appelé aussi l'anneau des polynômes tronqués,

si S est un anneau simple de caractéristique p, $S \otimes_{\mathbb{Z}_p} Bn(\mathbb{Z}_p)$ est un anneau différentiablement simple, car on peut prendre :

$$\Delta = \{\delta_1,\ldots,\delta_n\} \quad \text{où} \quad \delta_i = id_S \otimes (\partial/\partial X_i)$$

ou

$$\Delta = id_S \otimes \sum_{i=1}^{n} (X_1,\ldots,X_{i-1})^{p-1}(\partial/\partial X_i) .$$

Cet anneau s'identifie à l'anneau de groupe SG, où G est le produit direct de n groupes cycliques d'ordre p (les générateurs étant de la forme $1+X_i$) et ne dépend que de S et de n.

Soit W un S-module, somme directe de sous-modules irréductibles isomorphes et soit : $M = W \otimes_{\mathbb{Z}_p} B_n(\mathbb{Z}_p)$ un $S \otimes B_n(\mathbb{Z}_p)$-module, produit tensoriel de W et du module régulier $B_n(\mathbb{Z}_p)$; on peut voir alors immédiatement que ${}_A M$ est différentiablement irréductible.

Par abus de notation, on écrira :

$$A = S \otimes B_n(\mathbb{Z}_p) \quad , \quad \text{ou aussi} \quad A = B_n(S) \ ,$$

si A possède un sous-anneau simple S tel que :

$$A \simeq S \otimes B_n(\mathbb{Z}_p)$$

Et, dans le même cas, on écrira aussi :

$$M = W \otimes B_n(\mathbb{Z}_p) \quad \text{ou même} \quad M = B_n(W) \ .$$

Dans les constructions précédentes, on peut remplacer $\mathbb{Z}_p$ par un sous-anneau quelconque du centre de S sans changer A et M .

On pose également :

$$B_o(S) = S$$

$$B_o(W) = W$$

(où S est simple, de caractéristique arbitraire).

J'ai démontré les deux théorèmes suivants dans [1] (en fait dans un cadre plus général) ; la démonstration du premier en particulier est très longue.

<u>Théorème 1</u> : <u>Soit A un anneau différentiablement simple, contenant un idéal bilatère minimal.</u>

<u>Alors A est de la forme :</u> $B_n(S)$, <u>où S est simple et de caractéristique non nulle, si n est positif non nul.</u>

Théorème 2 : Soit A un anneau et Δ une famille de dérivations de A. Si A est Δ-semi-simple, si les idéaux bilatères satisfont la condition minimale, et si A/p est artinien pour tout idéal primitif P, alors A est une somme directe finie d'anneaux différentiablement simples.

Ces deux théorèmes déterminent alors les anneaux différentiablement semi-simples artiniens à gauche ou à droite.

Dans ce qui suit, A est un anneau artinien à gauche ou à droite, Δ une famille de dérivations de A, et les modules sont unitaires.

Les deux théorèmes suivants sont les résultats principaux de cet exposé.

Théorème 3 : Soit ${}_AM$ un module fidèle, différentiablement irréductible ; alors

$$A = B_n(S)$$
$${}_AM = B_n(W)$$

avec $n \geqslant 0$, S simple artinien, et ${}_SW$ somme directe de copies de l'unique S-module irréductible.

Théorème 4 : Soit A un anneau Δ-semi-simple tel que :

$$A = \bigoplus_{i=1}^{r} B_{n_i}(S_i)$$

et soit ${}_AM$ un module Δ-admissible ; alors ${}_AM = \bigoplus_{\lambda} M_\lambda$, où chaque M_λ est annulé par tous les $B_{n_i}(S_i)$ sauf un, correspondant à l'indice i ; on a alors : $M_\lambda = B_{n_i}(W_i)$ en tant que $B_{n_i}(S_i)$-module, où W_i est l'unique S_i-module irréductible.

Démonstration des théorèmes 3 et 4 : Supposons, pour commencer, que M est un $A[X,\Delta]$-module irréductible, que ${}_AM$ est fidèle, et que I est un Δ-idéal bilatère non nul de A ; alors : $IM = M$; en effet : IM est un sous-module de ${}_AM$ invariant par toutes les applications δ_ω, car :

$$\delta_\omega a\, m = a\, \delta_\omega m + (\delta_\omega a)m$$

appartient à IM si a est dans I et m dans M. L'anneau A étant artinien à gauche ou à droite, R_Δ est nilpotent, et : $R_\Delta M \neq M$ car M est non nul; donc : $R_\Delta = 0$, et A est Δ-semi-simple. Si $A = A_1 \oplus A_2$, A_1 étant un Δ-idéal non nul de A, alors :

$$A_1 M = M \quad , \quad A_2 M = A_2 A_1 M = 0$$

et $A_2 = 0$, donc A est Δ-simple et la démonstration du théorème 3 se ramène à celle du théorème 4.

Maintenant, supposons seulement que A est Δ-semi-simple et que M est Δ-admissible.

Si S est simple, artinien, on a :

$${}_S S = \bigoplus_{i \in I} V_i$$

où les V_i sont irréductibles et isomorphes :

$$B_n(S)^{B_n(S)} = B_n\Big(\bigoplus_{i \in I} V_i\Big) = \bigoplus_{i \in I} B_n(V_i)$$

et les composantes indécomposables principales sont toutes isomorphes à $B_n(V_i)$ qui est ainsi le module régulier réduit de $B_n(S)$.

On sait que $B_n(S)$, étant un anneau de groupe fini sur un anneau simple artinien, est un anneau quasi-frobénusien, c'est-à-dire artinien et auto-injectif ; donc $A = \bigoplus_{i \in I} B_{n_i}(S_i)$ est quasi-frobénusien. Les anneaux $B_n(S)$ étant auto-injectifs, chaque module $B_n(W)$ (où W est irréductible), est injectif.

Donc, tout A-module satisfaisant la conclusion du théorème 4 est injective, car une somme directe de modules injectifs, sur un anneau noethérien, est injectif.

Soit S l'ensemble des sous-modules de ${}_A M$ qui vérifient la conclusion du théorème 4, ordonné par la relation suivante :

$S_1 \leqslant S_2$ si et seulement si il existe un sous-module S_3 dans

S tel que : $\qquad S_2 = S_1 \oplus S_3$, alors $(S , \leqslant)$ est inductif.

Soit N un élément maximal de S ; le module N étant injectif, on a :

$$M = N \oplus P \ .$$

Soient Π_N et Π_P les projections canoniques de M sur N et sur P, et soit D une famille de transformations différentielles de M par rapport à Δ ; alors $\{\Pi_P d_\omega/P\}$ est une famille de transformations différentielles de P par rapport à Δ , car :

$$0 = d_\omega am - ad_\omega m - (\delta_\omega a)m = \Pi_N d_\omega am + (\Pi_P d_\omega)am - a\Pi_N d_\omega m - a(\Pi_P d_\omega)m - (\delta_\omega a)m \ .$$

Soit I l'annulateur de P .

Alors I est un Δ-idéal bilatère de A .

$A = I \oplus J$, où J est un Δ-idéal bilatère de A , et on obtient une Δ-représentation (ou plutôt Δ/P-représentation) fidèle, de J dans P .

On utilise le théorème suivant : (voir [2] p. 404) un module fidèle sur un anneau quasi-frobénusien contient toujours comme sous-module, une copie du module régulier réduit de l'anneau. On obtient ainsi un A-sous-module Q de P qui est, en tant que J-module, le module régulier réduit de J .

Donc : $\qquad Q \in S$, $N \oplus Q \in S$ d'où $Q = 0$, $J = 0$ et $P = 0$,

donc : $\qquad N = M \in S$ $\qquad\qquad$ c.q.f.d.

En conclusion, signalons que les résultats ci-dessus permettent d'étendre aux anneaux artiniens Δ-semi-simples, les caractérisations des anneaux artiniens semi-simples, à l'aide des modules projectifs, injectifs, ou complètement irréductibles.

- BIBLIOGRAPHIE -

[1] R.E. BLOCK, Determination of the differentiably simple rings with a minimal ideal, Annals of Math. 90 (1969), pp. 433-459.

[2] C.W. CURTIS and J. REINER, Representation theory of finite groups and associative algebras, New York, Interscience, (1962).

FACULTE DES SCIENCES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE.

Conférence n° 4 du 9.12.1970

ETUDE DES IDEAUX DES ANNEAUX NOETHERIENS PREMIERS HEREDITAIRES D'APRES UN ARTICLE DE ROBSON ET EISENBUD [J. of Algebra-1970]

par Mme A. GERMA

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

I. RAPPELS - DEFINITIONS - NOTATIONS.

Définition : Un anneau R est dit ordre (à droite) dans un anneau Q si et seulement si Q est un anneau de fraction (à droite) de R.

Notation : soit R un ordre dans Q, A et B deux sous-ensembles de Q

$$A .\cdot B = \{q \in Q \quad qB \subseteq A\} \qquad A \cdot. B = \{q \in Q \quad Aq \subseteq B\} .$$

Définition : Soit R un ordre dans Q, I une partie de Q. I est dit R-idéal fractionnaire à droite si et seulement si

$$IR \subseteq I \quad , \quad \exists a \text{ régulier } a \in I \; , \; \exists b \text{ régulier } \quad bI \subseteq R \quad [III]$$

Si R est un ordre dans un anneau simple artinien les R-idéaux fractionnaires à droite I admettent la définition suivante $IR \subseteq I$ $\exists a$ régulier dans Q tel que aI soit essentiel dans R.

Notations : soit I un R-idéal, R ordre dans Q, $I^* = R .\cdot I$, $O_\ell(I) = \{q \in Q \quad qI \subseteq I\}$.

Proposition : Soit R un ordre dans un anneau simple artinien Q et soit I un R-idéal à droite fractionnaire. Alors I est projectif si et seulement si $II^* = O_\ell(I)$ et alors I et I^* sont des R-modules de type fini [I].

Définition : Soit R un ordre dans Q , soit X un idéal bilatère de R . X est dit inversible si et seulement si $X(X^{\cdot}.R) = (R.^{\cdot}X)X = R$ et alors on note $X^{-1} = X^{\cdot}.R = R.^{\cdot}X$.

Définition : On appelle anneau de Dedekind premier à droite un anneau noethérien à droite, héréditaire à droite, premier, qui est un ordre maximal dans son anneau de quotients [III] .

Proposition : Pour un anneau qui est un ordre à droite dans un anneau simple artinien, il y a équivalence entre :

a) R est un anneau de Dedekind premier.

b) R a une arithmétique d'idéaux [IV] .

Définition : Un anneau est dit avoir assez d'inversibles si et seulement si tout idéal bilatère contient un idéal inversible.

Définition : R est dit "essentiellement borné" à droite si et seulement si tout idéal à droite essentiel dans R contient un idéal bilatère non nul.

Définition : R est dit primitif à droite si R admet un idéal maximal à droite qui ne contient pas de bilatère non nul ou encore si il existe un R-module simple d'annulateur nul.

Proposition : Soit R un anneau noethérien, héréditaire, premier. Alors il y a équivalence entre a R admet un idéal à droite minimal et b R est simple artinien [I] .

Proposition : Soit R un anneau premier noethérien héréditaire et I un idéal à droite essentiel de R , alors R/I est un R-module à droite de longueur finie [I] .

<u>Définition</u> : R et S étant ordres dans Q ils sont dits équivalents si et seulement si il existe a, b, c, d réguliers de Q tels que $aRb \subseteq S$ et $cSd \subseteq R$.

<u>Définition</u> : Un ordre R est dit maximal s'il est maximal parmi les ordres de Q qui lui sont équivalents.

Dans tout le développement les anneaux considérés seront supposés unitaires, et lorsqu'on ne précisera pas si l'on considère qu'une propriété est vérifiée à gauche ou à droite, c'est qu'elle l'est des deux côtés. Nous utiliserons ainsi le terme idéal pour désigner un idéal bilatère et un anneau noethérien représentera un anneau noethérien à gauche et à droite.

II. <u>IDEAUX IDEMPOTENTS.</u>

<u>Lemme</u> : Soit R un ordre dans un anneau Q simple artinien et soit I un R-idéal projectif. Alors I^*I est idempotent, $I = I^{*\cdot}.R$.

<u>Preuve</u> :

$$(I^*I)(I^*I) = I^*(II^*)I = I^*O_\ell(I)I = I^*I \ .$$

$$I \subseteq I^{*\cdot}.R \subseteq O_\ell(I)(I^{*\cdot}.R) = II^*(I^{*\cdot}.R) \subseteq IR \subseteq I \ , \ I = I^{*\cdot}.R \ .$$

<u>Théorème</u> : Soit R un anneau noethérien, premier, héréditaire ; R est un anneau de Dedekind premier si et seulement si il ne contient pas d'idéaux idempotents.

<u>Preuve</u> : si R est un anneau de Dedekind premier alors les idéaux bilatères non nuls forment un groupe, donc R ne contient pas d'idéaux idempotents.

D'autre part, soit X un idéal bilatère. $(R.^{\cdot} X)X$ et $X(X^{\cdot}.R)$ sont des idéaux idempotents donc ne peuvent être des idéaux propres si R ne contient pas d'idempotents . Donc $(R.^{\cdot} X)X = X(X^{\cdot}.R) = R$.

R représente maintenant un ordre dans un anneau simple artinien tel que tout idéal bilatère soit projectif, donc de type fini à gauche et à droite.

<u>Proposition</u> : Soit X un idéal inversible. Tout sous-module bilatère V de X^{-1} qui contient R est un R-idéal fractionnaire et est projectif et de type fini à gauche et à droite.

<u>Preuve</u> : Il suffit de prouver les propriétés à droite, à cause de la symétrie de la définition. Soit x un élément régulier de X. On a $xR \subseteq xV \subseteq R$ mais xR étant essentiel dans R, xV est essentiel dans R, donc V est un R-idéal fractionnaire à droite. VX est un idéal bilatère de R et donc est projectif par hypothèse. Donc $(VX)(VX)^* = O_\ell(VX)$. Nous voulons montrer que $VV^* = O_\ell(V)$. Or $VV^* \subseteq O_\ell(V) = O_\ell(VX)$. Il suffit de prouver $X(VX)^* \subseteq V^*$ c'est-à-dire $[X(VX)^*]V \subseteq R$, mais $X^{-1}[X(VX)^*]VX \subseteq R$ donc $X(VX)^*V \subseteq XRX^{-1}=R$.

<u>Proposition</u> : Si X est un idéal bilatère inversible de X, toute chaîne décroissante d'idéaux entre R et X est stationnaire à partir d'un certain rang.

<u>Preuve</u> : Soit $R \supseteq I_1 \supseteq I_2 \supseteq \dots \supseteq X$ une telle suite. On a $R \subseteq I_1^* \subseteq \dots \subseteq X^{-1}$. Soit $V = \bigcup_{k=1}^{\infty} I_k^*$. Alors $R \subseteq V \subseteq X^{-1}$, donc V est de type fini. La suite croissante I_k^* est donc stationnaire à partir d'un certain rang. Il en est de même de la suite décroissante I_k puisque $I_k=I_k^{*\cdot}.R$.

<u>Lemme</u> : Soit A un idéal idempotent de R, $A^*A = A$ et $A^* = O_\ell(A)$.

<u>Preuve</u> : $A^*A^2 = A^*A \subseteq RA = A \subseteq A^*A$. On a donc $A^* \subseteq O_\ell(A)$ mais $O_\ell(A) \subseteq A^*$ est toujours vrai pour un idéal A d'un ordre R.

<u>Théorème</u> : Soit X un idéal inversible de R. Il existe une correspondance biunivoque entre les idéaux idempotents A tels que $X \subseteq A \subseteq R$ et les anneaux S tels que $R \subseteq S \subseteq X^{-1}$, définie par :

$$A \mapsto O_\ell(A) = A^* \qquad S \mapsto S^{\cdot}.R .$$

Il existe une autre correspondance biunivoque définie par :

$$A \mapsto O_r(A) \qquad S \mapsto S\cdot R$$

<u>Preuve</u> : Si $X \subseteq A \subseteq R$ alors $R \subseteq A^* = O_\ell(A) \subseteq X^{-1}$. D'autre part $A = A^*\cdot R$. Par ailleurs soit S tel que $R \subseteq S \subseteq X^{-1}$. S est un R-idéal projectif de type fini, donc $S(S\cdot R)$ est un idéal idempotent de R. Il est clair que $S\cdot R = S(S\cdot R)$ et $X \subseteq S\cdot R \subseteq R$ donc $(S\cdot R)^* = S$.

<u>Proposition</u> : Soit A et B deux idéaux idempotents contenant X. Alors $A+B$ est idempotent et $O_\ell(A+B) = O_\ell(A) \cap O_\ell(B)$. Si $A \subseteq B$, $O_\ell(A) \supseteq O_\ell(B)$.

<u>Preuve</u> :

$(A+B)^2 = A^2+B^2+AB+BA = A+B+AB+BA \supseteq A+B$, $\quad A+B \subseteq (A+B)^2$

$O_\ell(A+B) \supseteq O_\ell(A) \cap O_\ell(B)$; $\quad (A+B)^* \subseteq A^* \cap B^*$

$A \subseteq B \quad A^* \supseteq B^*$ donc $O_\ell(A) \supseteq O_\ell(B)$.

<u>Proposition</u> : Soit A un idéal idempotent de R tel que $X \subseteq A \subseteq R$. Il existe une correspondance biunivoque entre les idéaux idempotents B de R tels que $B \subseteq A$ et les idéaux idempotents C de $S = O_\ell(A)$ définie par

$$B \mapsto BS \qquad C \mapsto CA$$

<u>Preuve</u> : C idéal de $S = O_\ell(A) = A^*$; $CA \subseteq A^*A = A \subseteq R$; $AC = AA^*C = SC = C$

$$(CA)^2 = (CA)(CA) = C(AC)A = C^2A = CA$$

donc CA est idempotent $CAS = CAA^* = CS = C$.

Par ailleurs soit B un idéal idempotent de R avec $B \subseteq A$

$BS = BA^* \subseteq AA^* = S \qquad BA = AB = B$

$(BA^*)^2 = BA^*BA^* = (BA)A^*(AB)A^* = B(AA^*A)BA^* = BABA^* = BA^*$

$BA^*A = (BA)A^*A = BA = B$.

<u>Proposition</u> : Soit S un sur-anneau de R contenu dans X^{-1}, S

est un ordre et les idéaux de S sont projectifs. Si R est un anneau noethérien premier héréditaire, il en est de même pour S.

Preuve : S est évidemment un ordre puisque R en est un. Soit I un idéal de S : I est un R-idéal donc est projectif en tant que R-module. Donc $I(R.\cdot I) = O_\ell(I)$. Or $(R.\cdot I) \subseteq (S.\cdot I)$, donc $I(S.\cdot I) = O_\ell(I)$. Supposons R noethérien, héréditaire, premier. On démontre que tout idéal à droite essentiel de S est projectif donc de type fini. Or tout idéal à droite de S est facteur direct d'un idéal à droite essentiel de S.

III. IDEAUX INVERSIBLES.

Dans ce paragraphe R désigne un ordre dans un anneau simple artinien, et les idéaux bilatères de R sont projectifs. Les idéaux bilatères sont donc de type fini à gauche et à droite et par suite R est noethérien bilatère.

Proposition : Tout idéal inversible X de R est un produit d'idéaux inversibles maximaux (parmi les inversibles).

Preuve : Soit X un idéal inversible et P_1 maximal inversible contenant X, $X \subset P_1 \subset R$; $P_1^{-1}X$ est un idéal inversible de R avec $R \supseteq P_1^{-1}X \supseteq X$. Soit P_2 maximal inversible contenant $P_1^{-1}X$ donc $R \supseteq P_2^{-1}P_1^{-1}X \supseteq P_1^{-1}X$. La condition noethérienne bilatère permet de conclure le résultat désiré.

Proposition : Tout idéal maximal M de R est inversible ou idempotent.

Preuve : Les idéaux $M(M.\cdot R)$ et $(R\cdot.M)M$ qui contiennent M ne peuvent être égaux qu'à R ou à M. S'ils sont tous deux égaux à R M est inversible par définition. Si M est égal à l'un d'eux M est idempotent.

Corollaire : Si N est un idéal maximal inversible alors ou bien N est maximal, ou bien les idéaux maximaux qui contiennent N sont idempotents.

En fait, nous allons montrer que les idéaux maximaux inversibles sont l'intersection des maximaux qui les contiennent.

<u>Lemme</u> : Soit X un idéal inversible et soit M un idéal maximal idempotent contenant X. Il existe un idéal maximal idempotent M' contenant X avec $O_r(M)=O_\ell(M')$.

<u>Preuve</u> : Soit $S = O_r(M)$ et $M' = S^{*}.R$. Les propositions du paragraphe II permettent de démontrer que M' répond aux conditions du théorème. Montrons que M' est un idéal maximal. Si M' n'était pas maximal il existerait P maximal inversible contenant M'. On aurait donc $X \subseteq M' \subsetneq P$ et par suite $X \subseteq M' \subset P^n$ pour tout n. La suite décroissante P^n au-dessus d'un inversible est stationnaire à partir d'un rang N $P^N = P^{N+k}$ pour tout entier k positif. Or ceci est impossible si P est un idéal propre inversible.

<u>Proposition</u> : Soit X un idéal inversible de R, soit $M_1 \supset X$ un idéal maximal idempotent. Alors $X \subseteq M_1 \cap M_2 \cap \dots \cap M_n$ où M_i est un idéal maximal idempotent et $O_r(M_1) = O_\ell(M_2)$, $O_r(M_2) = O_\ell(M_3)$ ..., $O_r(M_n) = O_\ell(M_1)$.

<u>Preuve</u> : On construit les M_i par un procédé récurrent à l'aide du lemme précédent. On obtient ainsi $M_1 \supseteq M_1 \cap M_2 \supseteq M_1 \cap M_2 \cap M_3 \supseteq \dots \supseteq X$ Cette chaîne est stationnaire à partir d'un certain rang. Ceci n'est possible que si deux des M_i coïncident. Or si $M_i = M_{i+N}$, $O_r(M_{n+i-1}) = O_\ell(M_{n+i}) = O_\ell(M_i) = O_r(M_{i-1})$ et par suite $M_{n+i-1} = M_{i-1}$. On a donc $M_1 = M_{n+1}$.

<u>Définition</u> : On appelle cycle un ensemble fini d'idéaux maximaux idempotents liés pour $O_r(M_i) = O_\ell(M_{i+1})$, ou un idéal maximal inversible.

<u>Proposition</u> : Soit $M_1, M_2, \dots, M_n$ une union de cycles de R. $X = \bigcap_{k=1}^{n} M_k$ est un idéal inversible.

Preuve : Supposons que nous considérons l'intersection sans éléments superflus. Si M_k est idempotent soit $S_k = O_\ell(M_k)$ et $M_{k'}$ l'idéal maximal idempotent tel que $O_\ell(M_k) = O_r(M_{k'})$. $M_k{}^* = S_k$ donc $M_k S_k = S_k$ $M_{k'} S_k = M_{k'}$. Soit A le produit des M_i différents de M_k et $M_{k'}$. On a

$$R \supseteq M_{k'} S_k \supseteq XS_k \supseteq AM_{k'} M_k S_k = AM_{k'} \quad , \text{ par suite}$$

$$S_k \subseteq X^{\bullet}. R \quad \text{et} \quad X(X^{\bullet}.R) \not\subseteq M_k$$

Si M_k est inversible, soit B le produit des M_i différents de M_k

$$R = M_k M_k{}^{-1} \supseteq XM_k{}^{-1} \supseteq BM_k M_k{}^{-1} = B \quad , \text{ par suite}$$

$$M_k{}^{-1} \subseteq X^{\bullet}. R \quad \text{et} \quad X(X^{\bullet}.R) \not\subseteq M_k \text{ .}$$

Donc $X(X^{\bullet}.R)$ contient X et n'est contenu dans aucun des maximaux qui contiennent X. Donc $X(X^{\bullet}.R) = R$ et de même $(R.^{\bullet}X)X = X$. X est donc inversible.

Théorème : Tout idéal maximal inversible de R est l'intersection d'un cycle.

Preuve : C'est là une conséquence immédiate des deux résultats précédents.

Proposition : Deux cycles sur R coïncident ou sont disjoints.

Preuve : Considérons l'union des deux cycles et l'intersection X des idéaux de cette union. La construction d'un cycle à partir d'un idéal maximal idempotent contenant X est canonique, d'où le résultat.

Proposition : Soit $I = M_1 \cap M_2 \cap \ldots \cap M_n$ une intersection d'idéaux maximaux de R et soit X un idéal inversible qui n'est contenu dans aucun des M_i. Alors $XI = X \cap I = IX$.

Preuve : Soit $J = X \cap I \subseteq X$; $J = XX^{-1}J$; $X^{-1}J$ est un idéal de R. Pour tout i $XX^{-1}J \subseteq M_i$, $X \not\subseteq M_i$, donc $X^{-1}J \subseteq M_i$ ou

$X^{-1}J \subseteq I$ $\quad J = X \cap I \subseteq XI$ donc $X \cap I = XI$ et de même $X \cap I = IX$.

Théorème : Les idéaux inversibles de R engendrent un groupe abélien.

Preuve : Nous avons vu que tout idéal inversible est produit d'idéaux maximaux inversibles. Or un idéal maximal inversible est l'intersection d'un cycle. On voit alors à l'aide de la proposition précédente que le produit de deux idéaux maximaux inversibles est commutatif, donc le produit de deux inversibles est commutatif.

Corollaire : Si R a assez d'idéaux inversibles, les R-idéaux fractionnaires inversibles forment un groupe commutatif.

Preuve : Soit X un R-idéal fractionnaire inversible. Alors il existe un idéal Y de R tel que XY soit un idéal de R . Nous pouvons supposer Y inversible. Alors XY est inversible et donc X appartient au groupe abélien engendré par les idéaux inversibles.

IV. IDEAUX FINALEMENT IDEMPOTENTS.

Définition : On appelle idéal finalement idempotent un idéal I dont une puissance n est idempotente. On note :

$$ev(I) = \operatorname*{Inf}_{I^n = I^{2n}} n = \operatorname*{Inf}_{I^n = I^{n+1}} n .$$

On appelle alors idéal finalement idempotent un idéal I pour lequel on a $ev(I) < +\infty$.

Dans ce paragraphe nous considérons un anneau R héréditaire, noethérien et premier, ce qui implique que R est un ordre dans un anneau simple artinien, que les idéaux bilatères sont projectifs, que R satisfait la condition de chaîne décroissante pour les idéaux au-dessus d'un bilatère non nul, et que les idéaux premiers sont maximaux.

<u>Lemme</u> : Soit $X \subset R$ un idéal inversible. Alors $Y = \bigcap_{n \in N} X^n = 0$ et X ne contient pas d'idéaux idempotents non nuls.

<u>Preuve</u> : Soit $Y = \cap X^n$, supposons $Y \neq 0$. Alors R satisfait la condition artinienne au-dessus de Y et donc pour un certain n $X^n = X^{n+1}$, avec X inversible propre, ce qui est impossible.

Soit A un idéal idempotent $A \subset X$. Pour tout n on a $A \subseteq X^n$ donc $A \subseteq \cap X^n = 0$.

<u>Proposition</u> : Tout idéal maximal idempotent de R est maximal.

<u>Preuve</u> : En effet, s'il n'était pas maximal il serait contenu dans un maximal inversible.

<u>Théorème</u> : Soit R un anneau noethérien héréditaire premier et I un idéal de R . Alors $I = XA$ où X est un idéal inversible et A un idéal finalement idempotent.

<u>Preuve</u> : Nous supposons I non inversible. Soit X un idéal minimal parmi les inversibles contenant I . Si $Y \neq R$ est un idéal inversible contenant $X^{-1}I$ alors $X \supset XY \supseteq I$ et puisque XY est inversible ceci contredit le choix de X . Donc $I = XA$ où $A = X^{-1}I$ n'est contenu dans aucun idéal propre inversible. Nous allons montrer qu'un tel idéal est finalement idempotent.

<u>Proposition</u> : Soit $M_1, M_2, \dots, M_k$ des idéaux maximaux de R tels que $A = M_1 \cap M_2 \cap \dots \cap M_k$ n'est contenu dans aucun idéal inversible. Alors A est finalement idempotent et $ev(A) \leq k$.

<u>Preuve</u> : Si $k = 1$ $A = M_1$, M_1 maximal et A non inversible. Alors M_1 est maximal idempotent, alors $ev(A) = 1$.

A étant non inversible, un au moins des idéaux $A(A.{}^{\cdot}R)$ et $(R{}^{\cdot}.A)A$ est différent de R . Supposons $A*A \neq R$, $A*A$ est idempotent. Si $A = A*A$, c'est fini. Nous pouvons supposer $A \subset A*A \subset R$.

Or $\frac{R}{A} = \frac{R}{\bigcap_{i=1}^{n} M_i} \simeq \prod_{i=1}^{n} \frac{R}{M_i}$ car chaque M_i est maximal. Or R/M_i est simple donc R/A est semi-simple. Donc $\frac{R}{A*A}$ est isomorphe au produit d'un certain nombre des R/M_i , soit $A*A = M_1 \cap M_2 \cap \dots \cap M_j = B$. Soit alors $C = M_{j+1} \cap \dots \cap M_k$ $BC \subseteq B \cap C = A = AA*A = AB = (B \cap C)B \subseteq CB \subseteq B \cap C$. Donc $CB = A \supseteq BC$. Nous pouvons supposer (hypothèse de récurrence) $ev(B) \leqslant j$, $ev(C) \leqslant k-j$.

__Lemme:__ Soit B et C des idéaux finalement idempotents avec $ev(B) = b$ et $ev(C) = c$. On suppose $BC \subseteq CB$. Alors CB est finalement idempotent et $ev(CB) \leqslant ev(C) + ev(B)$.

__Preuve__ : $(CB)^{c+b} \supseteq (CB)^{c+b+1} \supseteq B^{c+b+1} C^{c+b+1} = B^b C^c$

$B^b C^c \supseteq (CB)^{c+b}$ donc $(CB)^{c+b} = (CB)^{c+b+1}$

__Proposition__ : Soit A un idéal qui n'est contenu dans aucun inversible. Alors A est finalement idempotent. Plus précisément, il n'y a qu'un nombre fini d'idéaux maximaux $M_1, M_2, \dots, M_k$ qui contiennent A et $A^k = (M_1 \cap M_2 \cap \dots \cap M_k)^k$ est idempotent.

__Preuve__ : Comme R satisfait la condition artinienne au-dessus de A , l'intersection des idéaux maximaux qui contiennent A est de la forme $B = M_1 \cap M_2 \cap \dots \cap M_k$ et les M_i sont des idéaux maximaux idempotents. On a $B^k = B^{k+1}$. Par ailleurs, comme les idéaux premiers de R sont maximaux $\frac{B}{A}$ apparaît comme radical nilpotent de R/A qui est noethérien. Donc pour un certain ℓ on a $A^\ell \subseteq B$. Donc $B^k \supseteq A^k \supseteq B^{k\ell} = B^k$. Soit $A^k = B^k$.

__Corollaire__ : Un idéal idempotent de R n'étant contenu dans aucun inversible il existe $M_1, \dots, M_k$, maximaux idempotents tels que $A = A^k = (M_1 \cap M_2 \cap \dots \cap M_k)^k$.

<u>Corollaire</u> : L'anneau R a assez d'inversibles si et seulement si tout idéal maximal idempotent appartient à un cycle.

<u>Preuve</u> : Supposons que R a assez d'inversibles. Soit M un idéal maximal idempotent : M contient un inversible et donc M appartient à un cycle.

Soit I un idéal de R. Alors $I = XA$ avec X inversible et A finalement idempotent. Pour un certain n $B = A^n$ est idempotent, $I \supseteq XB$. Il suffit de prouver que B contient un inversible. $B = (M_1 \cap M_2 \cap \ldots \cap M_k)^k$ où les M_i sont des idéaux maximaux idempotents donc appartiennent à un cycle, donc contiennent l'intersection du cycle, Y_i, qui est un idéal inversible. Donc $B \supseteq (Y_1 Y_2 \ldots Y_k)^k$ qui est inversible. Donc I contient l'inversible $X(Y_1 Y_2 \ldots Y_k)^k$.

<u>Théorème</u> : Soit R un anneau noethérien héréditaire premier. Il y a équivalence entre :

a) R a un nombre fini d'idéaux idempotents.

b) R a un nombre fini d'idéaux maximaux idempotents.

c) R a un idéal idempotent minimal.

<u>Preuve</u> : Il est clair, à ce moment, que $a \Longleftrightarrow b$, par ailleurs, $a \Longrightarrow c$. Il reste donc à prouver que $c \Longrightarrow b$.

Soit $A = (M_1 \cap M_2 \cap \ldots \cap M_k)^k$ l'idéal idempotent minimal en question, M_i idéal maximal idempotent. Soit M un autre idéal maximal idempotent et $I = M \cap M_1 \cap M_2 \cap \ldots \cap M_k$. Alors $I^k \subseteq A \cap M \subseteq A$, donc I n'est pas finalement idempotent puisque A est idempotent minimal. Donc I est contenu dans un idéal maximal inversible X. $X = P_1 \cap P_2 \cap \ldots \cap P_\ell$ où $(P_1 \ldots P_\ell) \subseteq (MM_1 \ldots M_k)$ et les P_i forment un cycle.

Puisque A est idempotent on a $A \nsubseteq X$, donc M figure parmi les P_i. Si M est un idéal maximal idempotent, M et une partie de l'ensemble

$(M_1 \ldots M_k)$ forment un cycle. Or étant donné des idéaux maximaux idempotents en nombre fini il existe au plus un idéal maximal idempotent qui forme cycle avec ces idéaux; comme le nombre de parties de l'ensemble $(M_1 \ldots M_k)$ est fini, le nombre d'idéaux maximaux idempotents de R est fini.

Théorème : Soit R un anneau noethérien, héréditaire, premier avec un nombre fini d'idéaux maximaux idempotents, R ayant assez d'inversibles. Alors R est une intersection finie d'anneaux de Dedekind premiers.

Preuve : On considère l'ensemble des idéaux idempotents minimaux $A_1, A_2, \ldots, A_n$. R ayant assez d'inversibles, A_i contient un inversible. Soit X le produit de ces idéaux inversibles. Alors X est inversible contenu dans chaque A_i. Soit $B = A_1+A_2+\ldots+A_n$. Alors B est idempotent et $O_\ell(B) = \bigcap_{i=1}^{n} O_\ell(A_i)$, $O_r(B) = \bigcap_{i=1}^{n} O_r(A_i)$ et les $O_\ell(A_i)$ sont les sous-anneaux maximaux de X^{-1}, de même pour les $O_r(A_i)$. Donc $O_\ell(B)=O_r(B)$.

$B = B\,O_r(B) = B\,O_\ell(B) = BB^* = O_\ell(B)$ donc $B = R = \cap O_\ell(A_i)$. Comme R est noethérien héréditaire premier il en est de même de $O_\ell(A_i)$, qui, par ailleurs, ne contient pas d'idéaux idempotents sinon A_i en contiendrait. Donc $O_\ell(A_i)$ est un anneau de Dedekind premier.

Théorème : Soit R un anneau premier noethérien héréditaire. Alors R est, soit primitif à droite, soit "essentiellement borné" à droite, R possède ces deux propriétés simultanément si et seulement si il est simple artinien.

Preuve : Si R est primitif à droite et "essentiellement borné" alors il admet un idéal à droite maximal qui n'est pas essentiel, R admet donc un idéal minimal à droite, à savoir un complément du précédent, et donc R est simple donc artinien.

Supposons maintenant que R est non primitif à droite, c'est-à-dire que tout R-module simple est d'annulateur non nul. Nous pouvons supposer (hypothèse de récurrence) que tout module de longueur finie p est d'annulateur non nul. Soit U un module de longueur finie $p+1$ et V un sous-module de longueur 1 de U. V est d'annulateur non nul K, U/V est d'annulateur non nul J, R étant premier $0 \neq KJ \subseteq \text{Ann } U$. Donc tout module de longueur finie est d'annulateur non nul. Or nous savons que si I est un idéal à droite essentiel de R, R/I est un R-module de longueur finie, donc $\text{Ann } R/I = B \neq 0$, par suite I contient l'idéal bilatère B.

<u>Corollaire</u> : Si R a assez d'inversibles alors R est, soit primitif soit essentiellement borné.

Il suffit de montrer que si R est essentiellement borné à droite il l'est aussi à gauche. Soit I un idéal à gauche essentiel et soit $a \in I$, a régulier. Par suite aR est un idéal à droite essentiel qui contient un idéal bilatère et par suite, un inversible X $aR \supseteq X$ donc $Ra^{-1}aR \supseteq Ra^{-1}X$ $R \supseteq Ra^{-1}X$ $X^{-1} \supseteq Ra^{-1}$ $XX^{-1}a \supseteq XRa^{-1}a$ ou $I \supseteq Ra \supseteq X$. Donc R est essentiellement borné à gauche.

<u>Théorème</u> : Soit R un anneau noethérien, premier, héréditaire, essentiellement borné avec un nombre fini d'idéaux idempotents. Alors R a assez d'inversibles et c'est une intersection finie d'anneaux de Dedekind premiers essentiellement bornés.

<u>Preuve</u> : R étant essentiellement borné on peut démontrer que les ordres maximaux équivalents à R sont des R-idéaux fractionnaires, et l'on peut établir une correspondance biunivoque entre les idéaux idempotents de R et les ordres équivalents à R et contenant R. Soit M_1 un idéal idempotent maximal $M_2 = O_r(M_1)^{\cdot}.R$ est aussi idéal idempotent maximal et $O_r(M_1) = O_\ell(M_2)$. Puisqu'il n'y a qu'un nombre fini d'idéaux idempotents ce

procédé permet de fabriquer un cycle comprenant M_1 , donc, R a assez d'inversibles puisque tout idéal maximal idempotent appartient à un cycle. Par suite R est intersection fini d'anneaux de Dedekind premiers qui sont ordres équivalents à R et donc essentiellement bornés.

<u>Théorème</u> : Soit R un anneau noethérien premier héréditaire avec radical de Jacobson non nul. Alors R est essentiellement borné, R a un nombre fini d'idéaux maximaux et le radical de Jacobson J est inversible.

<u>Preuve</u> : R n'étant primitif ni à gauche ni à droite puisque tout idéal maximal à gauche ou à droite contient J , R est essentiellement borné. Nous allons montrer que tout idéal maximal à droite I contient un maximal bilatère. I contient un idéal bilatère non nul, lequel contient un produit de maximaux $I \supseteq M_1 M_2 \ldots \times M_n$ où les M_i sont bilatères maximaux.
Supposons $M_1 \not\subseteq I$ $\quad I+M_1 = R \quad I \supseteq (I+M_1)M_2 \ldots M_n = M_2 \ldots M_n$.

En reprenant ce raisonnement on voit que I contient l'un des M_i .

J est l'intersection des idéaux maximaux à droite, c'est donc une intersection finie de tels idéaux, or ils contiennent tous un idéal bilatère maximal. Donc J est aussi intersection des bilatères maximaux qui sont donc en nombre fini. Donc R a assez d'inversibles, par suite tout idéal maximal appartient à un cycle et donc J est inversible.

<u>BIBLIOGRAPHIE</u>

I. EISENBUD et ROBSON : Modules over Dedekind Prime Rings. J.Algebra 1970.
II. EISENBUD et ROBSON : Hereditary Noetherian Prime Rings. J.Algebra 1970.
III.JACOBSON : Theory of Rings. Math. Surveys II,Amer.Math.Soc.Providence 43.
IV. ROBSON : Non-commutative Dedekind Rings. J. Algebra 1968.

-:-:-:-:-:-

FACULTE DES SCIENCES

d' ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE.

Conférence n° 5 du 16 décembre 1970

-:-:-:-:-:-

PLONGEMENT D'UN FIR DANS UN CORPS,

d'après P.M. COHN

par Melle BESSON

-:-:-:-:-:-

Nous allons montrer, d'après [1]*, qu'on peut plonger dans un corps certains anneaux intègres non commutatifs, par une méthode qui n'est pas celle de la construction du corps des fractions à droite RR^{*-1}, ou à gauche $R^{*-1}R$, de l'anneau R considéré.

Nous utiliserons la "clôture honnête" de l'anneau R, qui si elle existe et si R satisfait certaines conditions, est un corps.

Cette méthode s'appliquera au cas d'un FIR, dont nous rappelons la définition :

Un anneau R est appelé <u>FIR</u> (Free Ideal Ring) <u>à droite</u> s'il a la propriété de rang invariant (c'est-à-dire si deux bases d'un R-module libre ont même cardinal) et si tout idéal à droite de R est libre.

Un <u>FIR à gauche</u> est défini de façon analogue. Un anneau R est un <u>FIR</u> si R est un FIR à droite et à gauche.

* On pourra aussi voir [8] .

Notons qu'un FIR à droite et à gauche est un anneau intègre (voir [4], ou le déduire de [2], propriété III). Mais, un FIR à droite ne satisfait pas, sauf dans le cas où il est principal à droite, la condition nécessaire et suffisante pour qu'un anneau R intègre ait un corps de fractions à droite : $aR \cap bR \neq 0$, pour tout $a, b \in R^*$. Pour un FIR à gauche, nous avons les conclusions analogues. Par conséquent, un FIR n'a en général pas de corps des fractions à gauche ou à droite.

§ 1. CLOTURE HONNETE DE R.

A) MATRICES PLEINES - DEFINITION ET PROPRIETES :

Soit $M_n(R)$ l'anneau des matrices carrées d'ordre n à coefficients dans R .

Définition : Une matrice A de $M_n(R)$ est dite pleine si A ne peut pas être écrite comme produit d'une matrice $n \times p$ et d'une matrice $p \times n$ à coefficients dans R , avec $p < n$.

Une matrice A est pleine si et seulement si l'endomorphisme α de R^n qu'elle définit ne peut pas s'écrire : $\alpha = \beta\gamma$, avec β homomorphisme de R^p dans R^n , γ homomorphisme de R^n dans R^p , et $p < n$.

Remarquons que dans le cas où R est sous-anneau d'un anneau S , une matrice A de $M_n(R)$ peut être pleine sans être pleine en tant que matrice de $M_n(S)$. On précisera alors : pleine sur R .

Proposition 1 : Si R est un corps les propriétés suivantes sont équivalentes :

(1) A est pleine.

(2) A est inversible dans $M_n(R)$.

(3) A est non diviseur de zéro dans $M_n(R)$.

On connait l'équivalence de (2), (3) et de la condition suivante : l'endomorphisme α de R^n défini par A est injectif. Or, si A est pleine, α est injectif, à cause de la factorisation suivante de $\alpha : R^n \to R^n/_{\ker \alpha} \to R^n$.

Inversement, si α est injectif, pour toute factorisation de α : $R^n \xrightarrow{\gamma} R^p \xrightarrow{\beta} R^n$ on a nécessairement la propriété : γ est injectif et par suite $p \geqslant n$.

Dans le cas général, il n'y a aucune implication entre les propriétés : A est pleine, et A est non diviseur de zéro [1] . Mais nous avons la propriété suivante :

<u>Proposition 2</u> : <u>Si A est un élément régulier de $M_n(R)$ (élément n'ayant aucun facteur diviseur de zéro à droite ou à gauche), A est une matrice pleine.</u>

Soit A un élément régulier de $M_n(R)$. Supposons : $A = BC$ avec B matrice $n \times r$, C matrice $r \times n$, et $r < n$. En complétant les matrices B et C avec des zéros nous obtenons des matrices B' et C' de $M_n(R)$, qui sont diviseurs de zéros dans $M_n(R)$ et qui vérifient : $A = B'C'$

On obtient aussi les propriétés suivantes :

<u>Proposition 3</u> : <u>Toute matrice de $M_n(R)$, facteur d'une matrice pleine de $M_n(R)$ est pleine.</u>

<u>Proposition 4</u> : <u>Soient $A \in M_n(R)$, $B \in M_p(R)$, C une matrice $n \times p$. Si la matrice $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$ est une matrice pleine de $M_{n+p}(R)$, A et B sont des matrices pleines.</u>

Indiquons, pour la proposition 4, qu'on utilise, afin de démontrer que A est pleine, la relation : $\begin{pmatrix} PQ & C \\ 0 & B \end{pmatrix} = \begin{pmatrix} P & C \\ 0 & B \end{pmatrix}\begin{pmatrix} Q & 0 \\ 0 & I \end{pmatrix}$.

Nous verrons, au § 3, que tout FIR satisfait les réciproques des propositions 2 et 4. Introduisons la définition suivante :

Un anneau R satisfait la propriété (P), si la réciproque de la proposition 4 est vérifiée.

On vérifie la propriété :

Proposition 5 : Si R satisfait (P), la matrice unité de $M_n(R)$ est pleine.

Corollaire : Si R satisfait (P), R a la propriété de rang invariant.
Pour que R ait la propriété de rang invariant, il suffit, d'après [2], que R vérifie la condition : la matrice unité I_n de $M_n(R)$ est pleine (c'est exactement la propriété II de [2]).

B) CLOTURE HONNETE :

Avant d'introduire cette définition, on démontrera le théorème :

Théorème 1 : Soit R un anneau satisfaisant (P), sous-anneau d'un anneau S et tel que toute matrice pleine sur R soit inversible sur S. Alors :

(a) le sous-anneau K de S engendré par R et les éléments des matrices inverses des matrices pleines sur R est égal à l'ensemble K_1 des premières composantes u_1 des solutions u dans S^n d'équations de la forme :

(1) $Au+a = 0$ avec $a \in R^n$ et A matrice pleine de $M_n(R)$.

(b) K est un corps.

- Montrons l'inclusion : $K_1 \subset K$. Soit $u_1 \in K_1$, correspondant à l'équation (1). Nous avons alors : $u = -A^{-1}a$. D'où : $u_1 \in K$.

- Pour obtenir l'inclusion $K_1 \supset K$, montrons que K_1 est un sous-anneau de S contenant R et les éléments des matrices inverses des matrices pleines sur R .

1) K_1 contient R , car l'élément $r \in R$ est solution de l'équation (1) , avec $n = 1$, $a = -r$ et $A = (1)$ (qui est une matrice pleine).

2) Soit $A^{-1} = \alpha_{ij})$ la matrice inverse d'une matrice pleine $A \in M_n(R)$. En égalant les $j^{\text{èmes}}$ colonnes des matrices AA^{-1} et I_n , puis en utilisant une matrice P de permutation convenablement choisie, on obtient :

$$(2) \qquad A\begin{pmatrix}\alpha_{ij}\\ \vdots \\ \alpha_{ij} \\ \vdots \\ \alpha_{1n}\end{pmatrix} = \begin{pmatrix}0\\ \vdots \\ 1 \\ \vdots \\ 0\end{pmatrix} \qquad AP\begin{pmatrix}\alpha_{ij}\\ \vdots \\ \alpha_{1j} \\ \vdots \\ \alpha_{1n}\end{pmatrix} = \begin{pmatrix}0\\ \vdots \\ 1 \\ \vdots \\ 0\end{pmatrix}$$

La matrice AP , facteur de la matrice $A = APP$, est pleine. L'équation (2) est donc de la forme (1) et, par suite, $\alpha_{ij} \in K_1$.

3) K_1 est un sous-anneau de S . Soient, en effet, $u_1 \in K_1$, $v_1 \in K_1$ correspondant respectivement aux équations : $Au+a = 0$, $Bv+b = 0$. On peut en déduire les équations suivantes :

$$\begin{pmatrix}1 & -1\ 0 & 1\ 0\\ 0 & A & 0\\ 0 & 0 & B\end{pmatrix}\begin{pmatrix}u_1-v_1\\ u\\ v\end{pmatrix} + \begin{pmatrix}0\\ a\\ b\end{pmatrix} = 0 \qquad \begin{pmatrix}A & a\ 0\\ & \\ 0 & B\end{pmatrix}\begin{pmatrix}uv_1\\ \\ v\end{pmatrix} + \begin{pmatrix}0\\ \\ b\end{pmatrix} = 0$$

Comme R satisfait (P) , les matrices figurant dans ces équations sont pleines. On obtient donc : $u_1-v_1 \in K_1$, $u_1v_1 \in K_1$.

- Il reste à démontrer que K est un corps, ou encore que tout élément u_1 non nul de K est inversible dans K . Nous avons $u_1 \in K_1$. Soit $Au+a = 0$ l'équation correspondante. Soit a_i la $i^{\text{ème}}$ colonne de A . Posons :

$$A_1 = (aa_2a_3 \dots a_n) \quad \text{et} \quad v = \begin{pmatrix}1\\ \vdots \\ u_2 \\ \vdots \\ u_n\end{pmatrix}$$

On vérifie l'égalité : $Au+a = A_1v+a_1u_1 = 0$.

On démontre (voir [1]) que A_1 est une matrice pleine. Par suite, elle est inversible sur S , et nous avons :

$$v + A_1^{-1}a_1u_1 = 0 .$$

La 1ère composante x de $-A_1^{-1}a_1$ est un élément de K et satisfait : $1 - xu_1 = 0$.

Introduisons les définitions suivantes :

Un anneau S est appelé <u>extension honnête</u> de R si R est un sous-anneau de S et si toute matrice pleine sur R est pleine sur S .

Un anneau S est appelé <u>clôture honnête</u> de S s'il satisfait les conditions :
- S est une extension honnête de R .
- Toute matrice pleine sur R est inversible sur S .
- S est engendré par R et les éléments des matrices inverses des matrices pleines sur R .

On notera $\Sigma(R)$ l'anneau obtenu en ajoutant "librement" à R les éléments de matrices inverses de matrices pleines sur R . Plus précisément, soient X un système de générateurs de R et Φ un système de relations définissant R . E étant l'ensemble des éléments des matrices pleines sur R , soient $\sigma : E \to X'$ une bijection et Φ' l'ensemble des relations :

$$\Sigma\alpha_{ik}\,\sigma(\alpha_{ki}) = 1 \quad \text{pour toute matrice } A = (\alpha_{ij}) \text{ pleine sur } R .$$

$\Sigma(R)$ est l'anneau défini par le système générateur $X \cup X'$ et les relations $\Phi \cup \Phi'$.

Notons f l'homomorphisme canonique $R \to \Sigma(R)$. L'anneau $\Sigma(R)$ satisfait (d'après [3] p. 151) la propriété suivante :

Pour tout homomorphisme $\varphi : R \to R'$ tel que toute matrice pleine sur R ait une image inversible sur R' , il existe un homomorphisme unique $\bar{\varphi} : \Sigma(R) \to R'$ tel que $\varphi = \bar{\varphi}f$.

Nous obtenons le théorème suivant :

Théorème 2 : Un anneau R satisfaisant (P) a une clôture honnête K si et seulement si l'homomorphisme $f : R \to \Sigma(R)$ est injectif ; si K existe, K est isomorphe à $\Sigma(R)$.

Si f est injectif, $\Sigma(R)$ satisfait les propriétés d'une clôture honnête. Inversement, si R a une clôture honnête K , K est un corps, d'après le théorème 1 . Soit i l'injection de R dans K . Il existe $\bar{i} : \Sigma(R) \to K$ tel que $i = \bar{i}f$. Par suite f est injectif ; $\Sigma(R)$ est une clôture honnête de R , donc un corps. On en déduit que l'homomorphisme $\bar{i} : \Sigma(R) \to K$ est injectif. De plus, l'image de $\bar{i}$ engendre K (d'après la 3ème propriété de la définition d'une clôture honnête). D'où : $K \simeq \Sigma(R)$.

§ 2. CONDITIONS SUFFISANTES D'EXISTENCE DE LA CLOTURE HONNETE D'UN ANNEAU SATISFAISANT (P) .

Théorème 3 : Un anneau R satisfaisant (P) a une clôture honnête si et seulement si on peut plonger, par un homomorphisme d'anneaux unitaires, l'anneau $M_n(R)$ dans un anneau F_n satisfaisant :

(1) Toute matrice pleine de $M_n(R)$ a une image inversible dans F_n .

La condition est évidemment nécessaire. Pour montrer qu'elle est suffisante, nous utiliserons les lemmes suivants :

Lemme 1 : Un anneau F unitaire possédant des éléments e_{ij} $(i,j = 1 \dots n)$ tels que $\sum_{i=1}^{n} e_{ii} = 1$, $e_{ij} = e_{h\ell} = \delta_{jh} e_{i\ell}$, est isomorphe à l'anneau $M_n(A)$, avec $A = e_{11}Fe_{11}$.

On vérifie que l'application $\sigma : F \to M_n(A)$ définie par $\sigma(x) = (\alpha_{ij})$

avec $\alpha_{ij} = e_{1i}xe_{j1}$, est un isomorphisme d'anneaux unitaires.

<u>Lemme 2</u> : <u>Si $M_n(R)$ est plongé, par un homomorphisme d'anneaux unitaires, dans un anneau F_n satisfaisant (1) , on peut plonger R dans un anneau R_n satisfaisant :</u>

(2) <u>Toute matrice pleine sur R d'ordre $\leqslant n$ a une image inversible sur</u> R_n .

Nous avons un homomorphisme injectif $\varphi_n : M_n(R) \to F_n$ et, d'après le lemme 1, l'isomorphisme $\sigma : F_n \to M_n(R_n)$, avec $R_n = \varphi_n(e_{11})F_n\varphi_n(e_{11})$. Soit $g_n : R \to R_n$ l'homomorphisme défini par $g_n(r) = r\varphi_n(e_{11})$. On en déduit $\overline{g_n} : M_n(R) \to M_n(R_n)$. On vérifie que l'on a : $\varphi_n = \sigma\overline{g_n}$. Par suite, $\overline{g_n}$ et g_n sont injectifs. Montrons de plus que R_n satisfait (2).

Soit $A \in M_n(R)$. Pour que $\varphi_n(A)$ soit inversible dans F_n , il faut et il suffit que $\overline{g_n}(A)$ le soit dans $M_n(R_n)$, c'est-à-dire que la matrice $\overline{g_n}(A)$ soit inversible sur R_n . Toute matrice pleine $A \in M_n(R)$ a une image $\overline{g_n}(A)$ inversible sur R_n .

Soit $A \in M_p(R)$ (avec $p \leqslant n$) une matrice pleine. Comme R satisfait (P) , la matrice $A' = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$ d'ordre n est pleine. Son image est inversible sur R_n . Il en est de même pour la matrice A .

<u>Démonstration du théorème 3</u> : Soit $\Sigma_n(R)$ l'anneau obtenu en ajoutant "librement" à R les éléments de matrices inverses des matrices pleines d'ordre $\leqslant n$. Nous obtenons un système inductif $\{\Sigma_n(R) , f_n^p\}$ où les homomorphismes f_n^p sont injectifs. La limite inductive de ce système est $\Sigma(R)$.

Soit f_n l'homomorphisme $R \to \Sigma_n(R)$. Il existe $h_n : \Sigma_n(R) \to R_n$ tel que $g_n = h_n f_n$. Comme g_n est injectif, f_n l'est aussi, ainsi que l'homomorphisme $R \to \Sigma(R)$, ce qui montre l'existence de la clôture honnête de R .

On est ramené à résoudre pour l'anneau des matrices carrées d'ordre n, l'ensemble $\mathcal{P}$ des matrices pleines d'ordre n, le problème suivant : plonger un anneau R dans un anneau R' où l'image de tout élément d'une partie S finie de R soit inversible. Ce problème a une solution si et seulement si l'homomorphisme de R dans R_S, anneau obtenu en ajoutant "librement" les inverses des éléments de S, est injectif.

Pour le cas d'un FIR, on appliquera à une partie de $\mathcal{P}$ le théorème suivant :

<u>Théorème 4</u> : <u>Soit R un anneau. S une partie finie de R telle que :</u>

(1) <u>tout élément $p \in S$ est non diviseur de zéro.</u>

(2) <u>pour tout $p \in S$</u> $\mathrm{End}_R(R/_{pR})$ <u>est un corps.</u>

(3) <u>pour tout $p, q \in S$, si $p \neq q$,</u> $\mathrm{Hom}_R(R/_{pR}, R/_{qR}) = 0$

<u>alors l'homomorphisme canonique $R \to R_S$ est injectif.</u>

La démonstration (voir [1]) utilise une construction de R_S au moyen d'anneaux tensoriels. Précisons cette construction, dans le cas $S = \{p\}$.

Si V est l'idéalisateur de pR, c'est-à-dire $V = \{v \in R \mid vp \in pR\}$, on construit le V-bimodule noté Rp^{-1} dont la structure de V-module à droite est celle de R, celle de V-module à gauche étant donnée par :

$$(rp^{-1})v = (rv')p^{-1} \quad \text{avec } vp = pv' \quad (v' \text{ est unique comme } p \text{ est non diviseur de zéro}).$$

On définit $(Rp^{-1})^n$ en posant $(Rp^{-1})^n = (Rp^{-1}) \otimes_V (Rp^{-1})^{n-1}$.

De l'homomorphisme injectif $f : V \to Rp^{-1}$ défini par $f(v) = vpp^{-1}$, on déduit un homomorphisme $(Rp^{-1})^{n-1} \to (Rp^{-1})^n$; on peut ainsi construire :

$$\varinjlim (Rp^{-1})^n = R_S .$$

§ 3. CAS D'UN FIR.

Proposition 6 : Soient R un fir, A une matrice de $M_n(R)$, α l'endomorphisme de R^n défini par A. Les propriétés suivantes sont équivalentes :

(1) A est pleine.

(2) A est un élément régulier de $M_n(R)$.

(3) Il existe un R-module de torsion M et une suite exacte

$$(s) : 0 \to R^n \xrightarrow{\alpha} R^n \to M \to 0 .$$

Rappelons que pour tout anneau R, nous avons (2) $\Longrightarrow$ (1).

On trouvera dans [4] (conférences 21-22), ou [5](§ 3), la définition des modules de torsion ainsi que la démonstration de : (3) $\Longrightarrow$ (2).

Il reste à démontrer : (1) $\Longrightarrow$ (3). Pour cela, montrons d'abord que α est injectif. $\mathrm{Ker}\,\alpha$, sous module d'un R-module libre, est libre (d'après [6] prop. 2.6.) ; de la factorisation de $\alpha : R^n \to R^n/_{\mathrm{Ker}\,\alpha} \to R^n$, on déduit donc : $\mathrm{Ker}\,\alpha = 0$. On peut alors construire la suite exacte (s). Pour montrer que M est un module de torsion, il suffit de montrer que tout sous module N de M satisfait : $x(N) \geqslant 0$ (voir [4] ou [5]).

Proposition 7 : Tout FIR satisfait (P).

Considérons les matrices pleines $A \in M_n(R)$, $B \in M_p(R)$, et la matrice $D = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$. Les matrices A et B définissent respectivement les endomorphismes injectifs α de R^n et β de R^p. On vérifie que l'endomorphisme γ de R^{n+p} défini par D est aussi injectif. Ceci permet d'obtenir le diagramme commutatif suivant, dont des 3 lignes et les 2 premières colonnes sont exactes :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & | & & | & & & & \\
0 & \to & R^n & \to & R^n & \to & M' & \to & 0 \\
 & & | & & | & & & & \\
0 & \to & R^{n+p} & \to & R^{n+p} & \to & M' & \to & 0 \\
 & & | & & | & & & & \\
0 & \to & R^p & \to & R^p & \to & M'' & \to & 0 \\
 & & | & & | & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

On peut compléter ce diagramme en un diagramme commutatif. D'après le lemme des 3×3, la 3ème colonne obtenue ainsi est exacte.

Les modules M' et M'' étant, d'après la proposition 6, des modules de torsion, M est un module de torsion (voir [4] ou [5]). Il en résulte que D est une matrice pleine.

<u>Proposition 8</u> : <u>Soit R un FIR. Alors</u> :

(1) <u>L'ensemble E des matrices pleines de $M_n(R)$ est factoriel).</u>

(2) <u>Si A est une matrice pleine atomique de $M_n(R) = R_n$, $\mathrm{End}_{R_n}(R_n/AR_n)$ est un corps.</u>

Si A et B sont deux matrices pleines atomiques non semblables de $M_n(R)$, on a :

$$\mathrm{Hom}_{R_n}(R_n/AR_n \ , \ R_n/BR_n) = 0 \ .$$

On trouvera dans [4], [5] ou [6] les définitions des notions utilisées ici, la démonstration de (1), ainsi que l'étude des propriétés de la catégorie T_R des R-modules de torsion, catégorie abélienne dont les objets simples (modules n'ayant pas de sous-modules propres et non nul de torsion) sont de la forme R^n/AR_n, avec A matrice pleine atomique. On peut en déduire (2) en passant à la catégorie T_{R_n} des R_n-modules de torsion (voir [5] ou [6]).

<u>Théorème 5</u> : <u>Si R est un FIR, l'anneau $M_n(R)$ peut être plongé dans un anneau tel que toute matrice pleine de $M_n(R)$ ait une image inversible.</u>

D'après la proposition précédente, (1), toute matrice pleine admet une factorisation en matrices atomiques pleines. D'autre part, si deux matrices A et B de $M_n(R)$ sont semblables et si A est inversible dans un anneau contenant $M_n(R)$, il en est de même de B (voir [1]).

Soit S un ensemble de matrices pleines atomiques deux à deux non semblables de $M_n(R)$, tel que toute matrice pleine atomique de $M_n(R)$ soit semblable à un élément de S. D'après la proposition 8, S satisfait les conditions du théorème 4 et l'homomorphisme $M_n(R) \to (M_n(R))_S$ est injectif. D'après le choix de S, toute matrice pleine de $M_n(R)$ est inversible dans $(M_n(R))_S$. Nous obtenons ainsi, d'après les théorèmes 2 et 3 :

<u>Théorème 6</u> : <u>Tout FIR peut être plongé dans un corps.</u>

<u>Remarque</u> : D'après [1], on peut affaiblir les hypothèses des propositions 6, 7, 8 et donc du théorème 5, et supposer seulement que R est un 2n-FIR (anneau avec rang invariant, où tout idéal engendré par moins de $2n$ générateurs est libre), satisfaisant la condition de chaîne croissante pour les idéaux à droite à n générateurs, ainsi que la condition de chaîne croissante pour les idéaux à gauche à n générateurs.

Pour $n = 1$, on obtient un 2-FIR atomique. Comme tout élément non nul correspond à une matrice 1×1 pleine, le théorème 5 se traduit par le résultat suivant :

Le semi-groupe des éléments non nuls d'un 2-FIR atomique peut être plongé dans un corps.

[1] signale aussi notamment, comme application du théorème 6, le théorème suivant :

<u>Théorème 7 : Deux corps K_1 et K_2 peuvent être plongés dans un même corps si et seulement si ils ont même caractéristique.</u>

Il est clair que la condition est nécessaire. Pour démontrer qu'elle est suffisante, on utilise la propriété suivante :

Le produit libre d'une famille K_i de corps sur un même sous-corps K existe (voir [7]) et est un FIR [1] .

Si K_1 et K_2 ont même caractéristique, ils ont même sous-corps premier K et peuvent donc être plongé dans un FIR : leur produit libre sur K, qui est lui-même plongé dans un corps.

- REFERENCES -

[1] COHN. The embedding of firs in skew fields (à paraître).

[2] COHN. Some remarks on the Invariant Basis Property (Topology 5 (1966) pp. 215-228).

[3] COHN. Universal Algebra - New York - Harper and Row (1965).

[4] COHN. Séminaire d'algèbre non commutative (1968-69) Orsay.

[5] COHN. Torsion Modules over Free Ideal Rings. Proc. London Math. Soc. 3, 17 (1967) pp. 577-599.

[6] COHN. Free Associative Algebra. Bull. London Math Soc. 1 (1969) pp. 1-39.

[7] COHN. On the free product of associative rings. Math. Zeits 71 (1959) pp. 380-398.

[8] Convegno Sulle algebre associative. Rome Nov. 1970.

FACULTE DES SCIENCES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE.

Conférence n° 6 du 11 Janvier 1971

-:-:-:-:-:-

ANNEAUX DE FRACTIONS DES ANNEAUX NOETHERIENS A GAUCHE D'EXPOSANT DEUX.

par L. LESIEUR

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

Le point de départ de cette étude est un exemple que j'ai donné dans [5][(1)] d'anneau noethérien à gauche co-irréductible d'exposant deux. Il se trouve que l'anneau considéré dans cet exemple possède un anneau de fractions à gauche. J'étudie ici cette question de l'anneau de fractions à gauche (classique) d'un anneau noethérien à gauche en la plaçant dans le cadre du théorème général de structure des anneaux noethériens à gauche d'exposant 2 , [6] . Je peux alors donner une condition nécessaire et suffisante pour l'existence de l'anneau de fractions (§ 5), et même définir la structure de celui-ci (§ 6). Auparavant je donne quelques rappels sur le théorème de structure (§ 1) et sur les éléments réguliers de l'anneau (§ 2) , puis je traite en détail l'anneau de fractions de l'exemple mentionné (§ 3).

(1) Voir la bibliographie placée à la fin de la conférence suivante.

RAPPELS sur la structure d'un anneau noethérien à gauche.

J'utilise le théorème de structure d'un anneau noethérien à gauche d'exposant deux obtenu antérieurement [6] , et rappelé brièvement ici : l'anneau $A = (M, K, \xi)$ est défini à partir de :

K : anneau noethérien à gauche semi-premier,

M : K-bimodule de type fini à gauche,

$\xi = (\gamma_1, \gamma_2)$ cocycle défini par deux fonctions $\gamma_1 : K \times K \to M$ et $\gamma_2 : K \times K \to M$ vérifiant les identités suivantes :

$$(\mathrm{I}) \quad \begin{cases} k\gamma_1(k',k'') - \gamma_1(kk',k'') + \gamma_1(k,k'k'') - \gamma_1(k,k')k'' = 0 \\ \gamma_1(k,k') + \gamma_1(k,k'') - \gamma_1(k,k'+k'') = \gamma_2(kk',kk'') - k\gamma_2(k',k'') \\ \gamma_1(k',k) + \gamma_1(k'',k) - \gamma_1(k'+k'',k) = \gamma_2(k'k,k''k) - \gamma_2(k',k'')k \\ \gamma_2(k',k'') - \gamma_2(k+k',k'') + \gamma_2(k,k'+k'') - \gamma_2(k,k') = 0 \\ \gamma_2(k,k') = \gamma_2(k',k) \\ \gamma_1(1,1) = 0 \ , \qquad \gamma_2(k,0) = \gamma_2(0,k') = 0 \\ \text{d'où résulte :} \qquad \gamma_1(k,1) = \gamma_1(1,k') = 0 \\ \qquad\qquad\qquad\qquad \gamma_1(k,0) = \gamma_1(0,k') = 0 \ . \end{cases}$$

L'addition et la multiplication sont alors définies dans $A = M \times K$ par

$$(m,k) + (m',k') = (m+m'+\gamma_2(k,k') \ , \ k+k')$$

$$(m,k)(m',k') = (mk'+km'-\gamma_1(k,k') \ , \ kk') \ .$$

2. ELEMENTS REGULIERS.

Théorème 1 : Pour que (m,k) soit régulier à droite dans A , il faut et il suffit que l'on ait les deux conditions suivantes :

R_1 : k est régulier à droite dans K (donc régulier à gauche)

R_2 : k est régulier à droite dans M ($m'k = 0 \Longrightarrow m' = 0$)

Pour que (m,k) soit régulier (à droite et à gauche dans A) il faut et il suffit que l'on ait : R_1 , R_2 et

R_3 : k est régulier à gauche dans M ($km' = 0 \Longrightarrow m' = 0$) .

La condition R_1 est la traduction du théorème de Djabali-Goldie ([1] et [2]) qui exprime que si $a \in A$ est régulier à droite dans A , il est régulier modulo le radical premier $\mathcal{R}$ de A . Nous allons donner ici une démonstration nouvelle de ce théorème inspirée par le théorème de structure.

<u>Démonstration</u> :

1) Les conditions R_1 et R_2 sont suffisantes. En effet, soit :

$$(m',k')(m,k) = (m'k+k'm-\gamma_1(k',k)\ ,\ k'k) = 0 .$$

On a donc : $k'k = 0$, $m'k+k'm-\gamma_1(k',k) = 0$. Il en résulte : $k' = 0$ d'après R_1 , puis $m'k = 0$ d'après I , et $m' = 0$ d'après R_2 . En conclusion $(m',k') = 0$ et (m,k) est bien régulier à droite.

2) Les conditions R_1 et R_2 sont nécessaires. Démontrons le d'abord pour R_2 . La condition $m'k = 0$ implique d'après I : $(m',0)(m,k) = 0$. Si (m,k) est régulier à droite on a $(m',0) = 0$, donc $m' = 0$.

Pour établir R_1 , établissons un lemme qui lie la régularité dans M à la régularité dans K .

<u>Lemme 1</u> : <u>Si k est régulier à droite dans M , il existe c_o , λ , k_1 dans K tels que :</u>

(1) $c_o = \lambda k + k_1$, c_o <u>régulier dans K , et</u> $Mk_1 = 0$.

En effet, soit $B = 0 : M = \{\alpha \in K | M\alpha = 0\}$. C'est un idéal bilatère dans K . L'élément k est régulier à droite modulo B ($tk \in B \Longrightarrow Mtk = 0 \Longrightarrow Mt = 0 \Longrightarrow t \in B$). Soit E l'idéal à gauche $Kk+B$. Démontrons que E est essentiel dans K . Soit $i \neq 0$, $i \in K$; si $Mi = 0$, on a $i \in B \subset E$ et $E \cap Ki \neq 0$; si $Mi \neq 0$ on a $i \notin B$, et comme k est régulier à droite modulo B, il existe $ti = \ell k+\alpha$, $\alpha \in B$, $ti \notin B$. On a donc $0 \neq ti \in E \cap Ki$. L'idéal à gauche E, étant essentiel dans l'anneau noethérien à gauche semi-premier K, contient un élément régulier c_0, ce qui démontre le lemme.

Pour établir le théorème, démontrons maintenant la propriété suivante :

<u>Lemme 2 : Si (m,k) est régulier à droite dans A, et si</u> $Mk_1 = 0$, <u>il existe c_1 régulier dans K tel que :</u>

(2) $c_1k_1 = \mu k$, $\mu \in K$.

Soit F l'idéal à gauche $Kk\ k_1 = \{\alpha \in K | \alpha k_1 \in Kk\}$. Montrons que F est essentiel. Soit $i \neq 0$, $i \in K$. Si $ik_1 = 0$ on a $0 \neq i \in Ki \cap F$. Si $ik_1 \neq 0$, on a dans A : $(0,i)(0,k) \neq 0$. Comme (m,k) est régulier à droite dans A, il existe une relation :

$$\begin{aligned}(m',k')(m,k) &= (m_2,k_2)(0,i)(0,k_1) \neq 0\\ &= (m_3,k_2i)(0,k_1) \neq 0\\ &= (-\gamma_1(k_2i,k_1)\ ,\ k_2ik_1) \neq 0\ .\end{aligned}$$

Cela implique $k_2i \neq 0$ et $k'k = k_2ik_1$, donc $0 \neq k_2i \in F$ et F est bien essentiel, d'où le lemme 2.

Le théorème résulte alors des égalités (1) et (2), par :

$$c_1c_0 = \nu k\ ,\quad c_0 \text{ et } c_1 \text{ réguliers dans } K$$

car $C = c_1c_0$ est régulier dans K et cela implique k régulier dans K. On sait, en effet que, dans un anneau noethérien à gauche semi-premier, si k était diviseur de zéro à droite il en serait de même de νk.

La condition de régularité, à droite et à gauche, se démontre immédiatement par l'adjonction de la condition R_3. Celle-ci est nécessaire :

$km' = 0 \Longrightarrow (m,k)(m',0) = 0 \Longrightarrow (m',0) = 0 \Longrightarrow m' = 0$.

Elle est suffisante, avec R_1 et R_2, car :

$$(m,k)(m',k') = 0 \Longrightarrow mk'+km'-\gamma_1(k,k') = 0 \quad \text{et} \quad kk' = 0$$

d'où : $k' = 0$, $km' = 0$ et $m' = 0$, soit $(m',k') = 0$.

Corollaire : la régularité d'un élément (m,k) ne dépend que de k , et pas de m .

3. EXEMPLE, AVEC ANNEAU DE FRACTIONS A GAUCHE NON ARTINIEN.

J'ai donné dans [5] un exemple d'anneau noethérien à gauche qui se révèle comme ayant un anneau de fractions à gauche non artinien.

Soit $K = A'$ un anneau commutatif intègre et noethérien ; soit P un idéal premier non nul de A' . On pose $M = A'/_P$ et on appelle φ l'homomorphisme canonique d'anneau : $A' \to A'/_P$, tandis que i est un homomorphisme injectif de A' dans $A'/_P$. (Son existence est assurée dans le cas où $A' = \mathbb{R}[X]$ et $P = (X^2+1)$, $A'/_P \simeq \mathbb{C}$). Alors $M = A'/_P$ est un K bimodule par les opérations :

$$k.m = \varphi(k)m \quad , \quad m.k = mi(k)$$

et c'est un K-module de type fini à gauche, engendré par $\varphi(1)$. On prend de plus $\xi = (0,0)$ comme cocycle du théorème de structure. C'est évidemment le cas le plus simple dans la génération d'un anneau noethérien, mais il donne déjà comme nous allons voir des propriétés fort intéressantes. L'addition et la multiplication sont définies dans $A = M \times K$ par :

$$(m,k) + (m',k') = (m+m', k+k')$$

$$(m,k)(m',k') = (mi(k') + \varphi(k)m' \ , \ kk') \ .$$

Les éléments (m,k) réguliers à droite sont ceux qui vérifient $k \neq 0$. (Dans cet exemple, les conditions R_1 et R_2 du théorème 1 sont identiques). Les éléments (m,k) réguliers, à droite et à gauche, sont ceux qui vérifient $k \notin P$; la condition R_3 entraîne alors R_1 et R_2 .

Théorème 2 : L'anneau A construit dans l'exemple 1 de [ ] admet un anneau total de fractions à gauche, non artinien.

Il suffit de vérifier la condition C des multiples communs à gauche pour l'ensemble S des éléments réguliers. Etant donné $(m,k) \in S$ et $(m_1,k_1) \in A$, trouver $(m'',k'') \in S$ et $(m',k') \in A$ tels que :

$$(m',k')(m,k) = (m'',k'')(m_1,k_1) .$$

Prenons $m'' = \sigma$; cette condition s'écrit :

$$k'k = k''k_1 \ , \quad m'i(k) + \varphi(k')m = \varphi(k'')m_1 \ .$$

On aura une solution en prenant :

$$k'' = \sigma k \ , \quad k' = \sigma k_1 \ , \quad \sigma \notin P \ ,$$

puis : $$m'i(k) = - \varphi(\sigma)\ \varphi(k_1)m + \varphi(\sigma)\ \varphi(k)m_1 \ ,$$

ce qui est possible avec :

$\varphi(\sigma) = i(k) \neq 0$ (car $k \neq 0$), qui admet une solution $\sigma \notin P$,

et $$m' = - \varphi(k_1)m + \varphi(k)m_1 \ .$$

L'anneau de fractions ainsi obtenu n'est pas artinien, car autrement la condition de régularité de SMALL [7] serait vérifiée, ce qui n'est pas puisque R_1 n'implique pas R_3.

Par contre il est noethérien à gauche d'exposant 2 , et on peut déterminer sa structure conformément au théorème général (voir le § 6).

Dans le cas particulier où $A' = \mathbb{R}[X]$ et $P = (X^2+1)$ et, plus généralement, si A'/P est un corps on montre aisément que l'anneau A possède un anneau total de fractions à gauche et à droite (1) .

(1) Cette remarque m'a été communiquée par L. SMALL.

4. PLAN D'ETUDE.

Afin d'étudier le problème de l'existence de l'anneau de fractions à gauche d'un anneau noethérien à gauche d'exposant 2 , on peut séparer a priori les cas suivants :

I - Cas $A = (M,K,\xi = 0)$, comme dans l'exemple.

II - Cas $A = (M,K,\xi = (\gamma,0))$ où le cocycle ξ admet une forme particulière, analogue à celle qu'on rencontre dans l'étude des anneaux artiniens à gauche d'égale caractéristique.

III - Cas général $A = (M,K,\xi)$.

Enfin, le problème plus symétrique où l'on suppose l'anneau noethérien à gauche et à droite donne lieu à des distinctions analogues et risque de conduire à des résultats plus positifs.

Il se trouve, comme nous allons voir, que la forme de ξ n'intervient pas pour l'existence de l'anneau de fractions, et que les conditions ne portent que sur M et K . Malgré tout, les types I et II sont intéressants, en particulier parce que leurs anneaux de fractions, quand ils existent, sont du même type que l'anneau de départ.

5. EXISTENCE DE L'ANNEAU DE FRACTIONS.

Soit S l'ensemble des éléments $k \in K$, tels que k vérifie R_1 , R_2 , R_3 .

<u>Théorème 2</u> : <u>Pour que l'anneau $A = (M,K)$ possède un anneau total de fractions il faut et il suffit que l'on ait les 2 conditions suivantes</u> :

1) <u>K possède un anneau de fractions par rapport à S .</u>

2) <u>La condition des multiples communs est vérifiée pour M</u> et S

$$\forall m \in M\ ,\quad k \in S\ ,\quad \exists \sigma \in S\ ,\quad m' \in M \text{ avec } \sigma m = m'k\ .$$

Les conditions sont nécessaires car 1) résulte de la condition des multiples communs dans A appliquée à $(0,k)$ et $(0,k_1)$, $k \in S$. Elle donne :

$$(m,k')(0,k) = (m'',k'')(0,k_1)$$

avec $k'' \in S$ d'où (1) $\boxed{k'k = k''k_1}$, $k'' \in S$.

La condition 2 résulte de la condition des multiples communs appliquée dans A à $(m,0)$ et $(0,k)$

$$(m'',\sigma)(m,0) = (m',k')(0,k)\ ,\quad \sigma \in S$$

$0 = k'k$ d'où $k' = 0$ puisque $k \in S$, et

$$(2)\quad \boxed{\sigma m = m'k}\quad \sigma \in S\ .$$

Les conditions sont suffisantes.

Donnons nous (m,k) et (m_1,k_1) avec $k \in S$.

Il faut résoudre : $(m',k')(m,k) = (m'',k'')(m_1,k_1)$ avec $k'' \in S$

ce qui s'écrit :

$$\begin{cases} (3)\quad k'k = k''k_1 \\ (4)\quad m'k+k'm-\gamma_1(k',k) = m''k_1+k''m_1-\gamma_1(k'',k_1)\ . \end{cases}$$

Or l'équation (3) admet une solution k',k'' avec $k'' \in S$ d'après (1) et elle admet aussi les solutions $\sigma k'$, $\sigma k''$ avec σ quelconque $\in S$. En portant dans l'équation (4) celle-ci s'écrit donc :

$$m'k+\sigma k'm-\gamma_1(\sigma k',k) = m''k_1+\sigma k''m_1-\gamma_1(\sigma k'',k_1)$$

ou :

$$m'k = m''k_1+\sigma k''m_1-\sigma k'm+\gamma_1(\sigma k',k)-\gamma_1(\sigma k'',k_1)\ .$$

Or on a d'après les relations I :

$$\sigma\gamma_1(k',k)-\gamma_1(\sigma k',k)+\gamma_1(\sigma,k'k)-\gamma_1(\sigma,k')k = 0$$

$$\sigma\gamma_1(k'',k_1)-\gamma_1(\sigma k'',k_1)+\gamma_1(\sigma,k''k_1)-\gamma_1(\sigma,k'')k_1 = 0\ .$$

Comme $\boxed{k'k = k''k_1}$, on en déduit :

$$\gamma_1(\sigma k',k)-\gamma_1(\sigma k'',k_1) = \sigma[\gamma_1(k',k)-\gamma_1(k'',k_1)] + \gamma_1(\sigma,k'')k_1-\gamma_1(\sigma,k')k ,$$

et il faut résoudre :

$$m'k = m''k_1 + \sigma\overbrace{(k''m_1-k'm+\gamma_1(k',k)-\gamma_1(k'',k_1))}^{a} + \gamma_1(\sigma,k'')k_1-\gamma_1(\sigma,k')k$$

soit encore : $\quad$ (5) $[m'+\gamma_1(\sigma,k')]k = (m''+\gamma_1(\sigma,k'')k_1+\sigma a$.

Or je peux résoudre d'après (2) $m_2k = \sigma a$ en m_2 et σ une fois k et a connus ce qui est le cas, puis je calcule m' par $m'+\gamma_1(\sigma,k')=m_2$ et m'' par $m''+\gamma_1(\sigma,k'') = 0$, d'où (5) .

6. STRUCTURE DE L'ANNEAU DE FRACTIONS.

a) dans l'exemple 1

$$M = A'/_P \quad , \quad K = A' \quad , \quad A = M \times K$$

K possède un anneau de fractions par rapport à $S = A - P$, qui est l'ensemble des fractions $\frac{a}{b}$, $b \notin 0$, ou localisé A'_P de A' par rapport à P .

On considère le module M' formé par les couples $\frac{m}{b}$, $b \notin P$, avec la relation d'équivalence :

$$\frac{m}{b} = \frac{m'}{b'} \Longleftrightarrow \varphi(b')m = \varphi(b)m'$$

i.e. les fractions du domaine d'intégrité $A'/_P$ (dans le cas particulier $A' = \mathbb{R}[X]$, $A'/_P = \mathbb{C}$, et $M' = M$). On munit M' d'une structure de A'_P bi-module par :

$$\frac{a}{b}\,\frac{\alpha}{\beta} = \frac{\varphi(a)\alpha}{\varphi(b)\beta} \quad \text{et} \quad \frac{\alpha}{\beta}\circ\frac{a}{b} = \frac{\alpha i(a)}{\beta i(b)}$$

et la multiplication par :

$$\left(\frac{\alpha}{\beta} , \frac{a}{b}\right)\left(\frac{\alpha'}{\beta'} , \frac{a'}{b'}\right) = \left(\frac{\alpha}{\beta}\,\frac{i(a')}{i(b')} + \frac{\varphi(a)\alpha'}{\varphi(b)\beta'} , \frac{a}{b}\circ\frac{a'}{b'}\right)$$

tandis que l'addition est évidemment :

$$(\frac{\alpha}{\beta}, \frac{a}{b}) + (\frac{\alpha'}{\beta'}, \frac{a'}{b'}) = (\frac{\alpha}{\beta}+\frac{\alpha'}{\beta'}, \frac{a}{b}+\frac{a'}{b'}) .$$

Petite simplification dans le cas où $M = \mathbb{C}$.

b) dans le cas général

$$A = M \times K .$$

Soit K' l'anneau de fractions de K par rapport à S , constitué par les éléments $s^{-1}k$.

Soit M' l'ensemble des couples $\frac{m}{b}$, $b \in S$, avec la relation d'équivalence :

$$\frac{m}{b} \equiv \frac{m'}{b'} \iff \exists_{\substack{s_1 \\ s'_1}} \in S , \quad \text{avec} \quad \begin{cases} s_1 b = s'_1 b' \\ s_1 m = s'_1 m' \end{cases}$$

On munit M' d'une structure de bi-K' module par :

$$\frac{k}{s} \circ \frac{m}{b} = \frac{tm}{\sigma s} \quad \text{avec} \quad \sigma k = tb , \quad \sigma \in S \qquad \text{et}$$

$$\frac{m}{b} \frac{k}{s} = \frac{m'k}{\sigma b} , \quad \text{avec} \quad \sigma m = m's , \quad \sigma \in S .$$

(On laisse au lecteur le soin de faire les vérifications nécessaires, y compris le fait que M' soit un K'-module à gauche de type fini).

Puis on définit un co-cycle γ'_1 , γ'_2 par :

$$\gamma'_2(s^{-1}k , s^{-1}k') = s^{-1}\gamma_2(k,k')$$

$\gamma'_1(s^{-1}k , s^{-1}k')$ est plus compliqué,

$$\gamma'_1(s^{-1}k , s'^{-1}k') = - n'k' + \gamma_1(k_1,k')$$

où k_1, n' est une solution de :

$$\begin{cases} \sigma k = k_1 s' , \quad \sigma \in S \\ nk - \gamma_1(\sigma,k) = n's' - \gamma_1(k_1,s') . \end{cases}$$

Cette solution existe toujours (raisonnement analogue à celui du théorème d'existence). Les expressions proviennent du calcul dans l'anneau de fractions de :

$$\frac{(0,k)}{(0,s)} + \frac{0,k'}{(0,s)} = \frac{(\gamma_2(k,k') \ , \ k+k')}{(0,s)}$$

et $$\frac{(0,k)}{(0,s)} \times \frac{(0,k')}{(0,s')} = \frac{(n',k_1)(0,k')}{(n,\sigma)\ (0,s)} \quad \text{avec} \quad (n,\sigma)(0,) = (n',k_1)(0,s') \ .$$

Cas particulier : si $\gamma_1 = \gamma_2 = 0$, on peut prendre $n = n' = 0$ et $\gamma_1' = 0$, avec $\gamma_2' = 0$. Si $\gamma_2 = 0$ on a aussi $\gamma_2' = 0$.

Donc ces deux types d'anneaux se conservent par passage à l'anneau de fractions.

FACULTE DES SCIENCES D'ORSAY

SEMINAIRE D'ALGEBRE NON COMMUTATIVE

Conférence nº 7 du 18.1.1971

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

SUR LES ELEMENTS REGULIERS DES ANNEAUX NOETHERIENS A GAUCHE D'EXPOSANT 2.

par L. LESIEUR

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

Je rappelle d'abord l'énoncé du théorème qui caractérise les éléments réguliers, et les deux conditions nécessaires et suffisantes pour l'existence de l'anneau de fractions à gauche (§ 1). Je donne ensuite quelques propriétés des éléments réguliers qui montrent que ces conditions sont partiellement remplies dans le cas général (§ 2). Ensuite j'analyse les sous-ensembles $R_1(K)$, $R_2(K)$, $R_3(K)$ qui interviennent dans l'étude des éléments réguliers du point de vue des cas d'inclusion ; on rencontre ainsi au passage la condition de régularité de Small, et les anneaux noethériens complètement primaires à gauche (§ 3). Enfin, je considère pour terminer une application (§ 4).

1. LES ENSEMBLES $R_1(K)$, $R_2(K)$, $R_3(K)$.

Rappelons le théorème qui caractérise les éléments réguliers d'un anneau noethérien à gauche A d'exposant 2, défini par sa structure (M,K,ξ) (voir la conférence précédente)* .

Théorème 1 : Pour que (m,k) soit régulier à droite dans A, il faut et il suffit que l'on ait les deux conditions suivantes :

R_1 : k est régulier à droite dans K (donc régulier à gauche),

R_2 : k est régulier à droite dans M ($mk = 0 \Longrightarrow m = 0$).

Pour que (m,k) soit régulier (à droite et à gauche) dans A, il faut et il suffit que l'on ait R_1, R_2 et R_3 : k est régulier à gauche dans M ($km = 0 \Longrightarrow m = 0$) .

Désignons par $R_i(K)$ le sous-ensemble de K vérifiant la condition R_i ($i = 1,2,3$). $R_i(K)$ est un ensemble multiplicativement fermé. L'ensemble des éléments réguliers est alors :

$$S = R_1(K) \cap R_2(K) \cap R_3(K) .$$

Il est également stable pour la multiplication.

Rappelons aussi le théorème d'existence d'un anneau de fractions :

Théorème 2 : Pour que l'anneau (M,K,ξ) possède un anneau de fractions à gauche, il faut et il suffit :

i) K possède un anneau de fractions par rapport à S,

ii) La condition des multiples communs est vérifiée pour M et S :

$$\forall m \in M\ ,\ k \in S\ ,\ \exists \sigma \in S\ ,\ m' \in M \text{ tel que } \sigma m = m'k .$$

* K est un anneau noethérien à gauche semi-premier, M un K-bimodule de type fini à gauche, $\xi = (\gamma_1,\gamma_2)$ un co-cycle qui n'interviendra pas ici.

2. PROPRIETES VALABLES DANS LE CAS GENERAL.

Dans le cas général, voici quelques résultats prouvant que ces conditions sont partiellement vérifiées.

Rappelons d'abord que la condition des multiples communs de Ore est vérifiée pour l'ensemble $R_1(K)$ des éléments réguliers dans K :

$$\forall k \in R_1(K)\ ,\quad a \in K\ ,\quad \exists k' \in R_1(K)\ ,\quad a' \in K \quad \text{avec} \quad k'a = a'k\ .$$

C'est le théorème de Goldie d'existence d'un anneau total de fractions à gauche de K, et c'est déjà une approche de la condition (i).

Pour établir une propriété approchant la condition (ii), démontrons d'abord le lemme suivant :

<u>Lemme</u> : <u>Si $k \in R_2(K)$</u>, <u>(c'est-à-dire si k est régulier à droite dans (M), Mk est un sous-K-module à gauche essentiel dans M</u>.

En effet, soit $0 \neq m \in M$. On considère la somme :

$$Kmk + Kmk^2 + \ldots + Kmk^n + \ldots$$

qui est finie (condition noethérienne) et on choisit n minimum pour que :

$$mk^n = k_1mk + k_2mk^2 + \ldots + k_{n-1}mk^{n-1}\ .$$

Si $n = 2$ on a $mk^2 = k_1mk$ d'où, puisque k vérifie R_2, $mk = k_1m \neq 0$.

Si $n > 2$, on a :

$$mk^{n-1} = k_1m + k_2mk + \ldots + k_{n-1}mk^{n-2}$$

avec $k_1m \neq 0$ conformément au choix de n, d'où :

$$k_1m = m'k \neq 0\ .$$

<u>Propriété 1</u> : <u>Si</u> $k \in R_2(K)$ <u>(k régulier à droite dans M), pour tout $m \in M$, il existe</u> $c \in R_1(K)$ <u>(régulier dans K), et $m' \in M$, tels que</u> :

$$\underline{cm = m'k}\ .$$

En effet, considérons $I = Mk^{\bullet}. m = \{x \in K / xm \in Mk\}$. Comme M est un bi-module, I est un idéal à gauche de K. Montrons que I est essentiel. Soit $u \neq 0$, $u \in K$. Si $um = 0$ on a : $0 \neq u \in I \cap Ku$. Si $um \neq 0$, on prend d'après la propriété 1 :

$$k'um = m'k \neq 0 \quad \text{d'où} \quad 0 \neq k'u \in I \cap Ku .$$

D'après le théorème de Goldie, I contient un élément régulier c de K, et la propriété 1 est démontrée. Elle constitue une approche de la condition (ii).

<u>Propriété 2</u> : <u>Les éléments $m \in M$ tels qu'il existe $k \in R_1(K)$ (régulier dans K) avec $km = 0$, forment un sous-bimodule I de M.</u>

Soit $m \in I$, donc il existe $k \in R_1(K)$ tel que $km = 0$. On a pour tout $\mu \in K$, $km\mu = 0$. De plus, si $\lambda \in K$, la condition de Ore dans K donne : $c\lambda = uk$, avec $c \in R_1(K)$, d'où $c\lambda m = 0$ et $\lambda m \in I$. Enfin, si $km = k'm' = 0$, $k \in R_1(K)$, $k' \in R_1(K)$, il existe $\sigma = k_1 k = k_1' k' \in R_1(K)$ et $\sigma(m-m') = 0$.

3. <u>COMPARAISON DES CONDITIONS</u> R_1, R_2, R_3.

a) <u>Cas $R_2 \Longrightarrow R_1$</u> (ou $R_2(K) \subset R_1(K)$).

La régularité à droite dans M entraîne alors la régularité dans K.

Nous allons voir que cette implication est de règle en général.

<u>Propriété 3</u> : <u>On a</u> $R_2(K) \subset R_1(K)$, <u>s'il n'existe pas dans l'anneau $A = M \times K$ une décomposition de l'idéal nul</u>

(1) $$0 = \mathcal{P}_1 \cap Q_2 \cap \dots \cap Q_n$$

<u>réduite en idéaux tertiaires, dont l'une des composantes est un idéal premier</u> $\mathcal{P}_1$.

En effet, soit $k \in R_2(K)$, $k \notin R_1(K)$. L'élément $a = (0,k) \in A$ ne peut être régulier à droite dans A (théorème 1). Donc on a :

$$0^{\bullet}. a = \{x \in A | xa = 0\} \neq 0 .$$

D'autre part, le radical $\mathcal{R}$ de A est l'ensemble $(m,0)$ et la condition $k \in R_2(K)$ implique :

$$(0 \cdot\cdot a) \cap \mathcal{R} = 0 .$$

En effet : $(m,0)(0,k) = 0 \Longrightarrow mk = 0 \Longrightarrow m = 0$. Considérons une décomposition réduite de $0 \cdot\cdot a$ en idéaux à gauche tertiaires, et la décomposition de $\mathcal{R}$ comme intersection des idéaux premiers minimaux :

$$0 \cdot\cdot a = Q_1 \cap \dots \cap Q_h \ , \quad \mathcal{R} = \mathcal{P}_1 \cap \dots \cap \mathcal{P}_k .$$

On a donc :

$$0 = \mathcal{P}_1 \cap \dots \cap \mathcal{P}_k \cap Q_1 \cap \dots \cap Q_h$$

et, quand on réduit les éléments superflus, il reste au moins un idéal premier, soit $\mathcal{P}_1$; sinon on aurait $Q_1 \cap \dots \cap Q_h = 0 \cdot\cdot a = 0$. La propriété 3 est démontrée.

La réciproque de la propriété 3 n'est pas vraie en général, c'est-à-dire que la condition (1) n'assure pas toujours $R_2(K) \not\subseteq R_1(K)$, même dans le cas commutatif. Dans ce dernier cas, on peut préciser :

<u>Propriété 3'</u> : <u>Si A est commutatif, on a</u> $R_2(K) \subseteq R_1(K)$ <u>sauf si et seulement si il existe dans l'anneau $A = M \times K$ une décomposition de l'idéal nul en idéaux primaires, dont l'une des composantes est un idéal premier qui soit, en même temps, maximal parmi les idéaux premiers associés à 0</u>.

(Démonstration laissée aux soins du lecteur).

On peut donc dire que la situation $R_2(K) \not\subseteq R_1(K)$ est accidentelle, ou encore que $R_2(K) \subseteq R_1(K)$ est vérifiée en général.

b) <u>Cas $R_1 \Longrightarrow R_2$</u> (ou $R_1(K) \subseteq R_2(K)$).

(Condition de Small généralisée). On sait que, dans le cas commutatif, cette condition est vérifiée si et seulement si tous les idéaux premiers associés à 0 dans sa décomposition en idéaux primaires sont deux à deux incomparables (tous les composants primaires de 0 sont isolés).

Dans le cas non commutatif, la condition de Small s'écrit $R_1(K) \subset R_2(K) \cap R_3(K)$ et elle est vérifiée si et seulement si A possède un anneau de fractions à gauche artinien.

On retrouve immédiatement cette propriété comme conséquence des conditions (i) et (ii) du théorème 2. La condition (i) est la condition de Ore dans K ; la condition (ii) est exprimée par la propriété 1 que nous avons établie dans le cas général. Et l'anneau de fractions est artinien à gauche car d'après le théorème de structure vu dans la conférence précédente, l'anneau d'opérateurs de cet anneau de fractions est l'anneau de fractions de K, qui est semi-simple. La réciproque s'établit aisément :

c) <u>Cas d'un anneau complètement primaire à gauche</u> :

(voir la définition et les propriétés dans [5]).

<u>Propriété 4</u> : <u>Pour qu'un anneau soit complètement primaire à gauche il faut et il suffit qu'on ait</u> :

$$R_1(K) = R_2(K) = K - \{0\}$$

c'est-à-dire : K est intègre et $mk = 0 \Longrightarrow m = 0$ ou $k = 0$.

C'est une propriété qu'on a constatée dans l'exemple donné dans la conférence précédente.

La condition est nécessaire car on sait que $K \simeq A/\mathcal{R}$ est intègre, d'où $R_1(K)=K-\{0\}$. De plus, si k est diviseur de zéro à droite dans M, on a : $mk = 0$, $m \neq 0$. Mais cela entraîne : $(m,0)(0,k) = 0$ avec $(m,0) \neq 0$, d'où $(0,k)$ est nilpotent et k aussi, donc nul.

Démontrons que la condition est suffisante. Soit $(m',k')(m,k) = 0$, avec $(m',k') \neq 0$. On a donc $k'k = 0$ et $k' = 0$ ou $k = 0$. Si $k = 0$, $(m,0)$ est de carré nul donc nilpotent. Si $k' = 0$ on a $(m',0)(m,k) = (m'k,0) = 0$ d'où $m'k = 0$ avec $m' \neq 0$, donc $k = 0$ également.

<u>Conséquence</u> : <u>Dans un anneau complètement primaire à gauche on a</u> :

(1) $$R_3 \Longrightarrow R_1 \Longleftrightarrow R_2 \ , \quad R_3(K) \subseteq R_1(K) = R_2(K) \ .$$

En effet $R_3(K)$ est évidemment contenu dans $K - \{0\}$.

4. APPLICATION.

Dans l'exemple considéré à la conférence précédente on a en plus de (1) la propriété suivante :

(2) $$km = 0 \ , \quad m \neq 0 \Longrightarrow kM = 0 \ .$$

(En effet $\varphi(k)m = 0$ dans $A'/_P$ intègre, avec $m \neq 0$, entraîne $\varphi(k) = 0$ donc $kM = 0$).

Propriété 5 : Si un anneau vérifie la propriété (2) , l'ensemble $K-R_3(K)$ est un idéal de K complètement premier P ; le module M est P-isotypique et son coeur est égal à M .

Démontrons que P est un idéal bilatère. C'est en effet l'idéal $0 \cdot. M = \{p \in K | pM = 0\}$. Il est évidemment complètement premier : $abm = 0$, $m \neq 0 \Longrightarrow (bm \neq 0$ et $a \in P$, ou $bm = 0$ et $b \in P)$. Démontrons l'isotypie. Soit $0 = Km \cap Km'$, $m \neq 0$, $m' \neq 0$. On a $P = 0 \cdot. m = 0 \cdot. m'$ et les modules Km et Km' sont isomorphes. C'est une condition suffisante (cf. [3]). De plus, l'enveloppe injective $E(Km)$ est isomorphe à $E(K/_P)$ ce qui prouve que M est P-isotypique.

Le coeur (1) de M est non nul; si $0 \neq m \in C(M)$, on a $0 \cdot. m = P$ qui est donc maximal dans l'ensemble des idéaux annulateurs des éléments non nuls de l'enveloppe injective $E(M)$. Mais alors cette propriété reste vraie pour tout élément non nul de M , ce qui prouve que $M = C(M)$.

Supposons que l'anneau vérifie, en outre la propriété

(3) $$R_3(K) \subset R_1(K) \cap R_2(K) \ .$$

Cette propriété entraîne :

(3)' Tout élément régulier à gauche est régulier à droite.

En effet, si (m,k) est régulier à gauche, on a nécessairement $k \in R_3(K)$,

(1) Pour la définition et les propriétés du coeur, se reporter à [4] .

d'où (m,k) régulier à droite d'après (3).

<u>Propriété 6</u> : <u>Si un anneau vérifie les propriétés (2) et (3), la condition (ii) du théorème 2 d'existence d'un anneau de fractions est vérifiée.</u>

En effet, soit $k \in S = R_3(K)$ et $m \in M$. On peut supposer $m \neq 0$; comme Mk est essentiel dans M (lemme), il existe $k_1 m = m'k \neq 0$. Il en résulte $k_1 \in R_3(K)$; sinon on aurait $k_1 M = 0$ d'après la propriété (2), ce qui n'est pas. Alors on a : $k_1 \in S$ d'après la propriété (3).

Pour que l'anneau de fractions existe, il faut et il suffit donc que la condition (i) soit vérifiée, c'est-à-dire que K possède un anneau de fractions par rapport à $R_3(K) = K-P$. C'est ce qui a toujours lieu si K est commutatif comme dans l'exemple. Pour le cas général nous renvoyons à une autre étude [8].

-:-:-:-:-:-

- BIBLIOGRAPHIE -

[1] M. DJABALI, Sur les éléments réguliers d'un anneau noethérien à gauche (C.R. Acad. Sc. Paris, t. 264, 1967, pp. 493-495).

[2] A.W. GOLDIE, The transfer ideal (Séminaire Algèbre non commutative, Orsay, (1967-1968), conférence n° 19).

[3] L. LESIEUR, Algèbre noethérienne non commutative (Mémorial des Sc. Math., CLIV, PARIS, Gauthier-Villars - 1963).

[4] L. LESIEUR, Coeur d'un module (Journal de Math. Pures et Appliquées, 1963 - t. XLII, fascicule 4).

[5] L. LESIEUR, Anneaux noethériens à gauche complètement primaires et anneaux co-irréductibles (Journal f. die reine und angew Mathematik, Band 239/240, 1970, Seite 106-117).

[6] L. LESIEUR, Structure des anneaux noethériens à gauche d'exposant deux (Convegno sulle algebre associative, Istituto di Alta Matematica, ROMA, Nov. 1970).

[7] L. SMALL, Orders in artinian rings, J. of algebra, 4 (1966), pp. 13-41.

[8] L. LESIEUR, Idéal complètement premier d'un anneau noethérien intègre non commutatif (Séminaire Dubreil - Pisot, Février 1971).