THÈSE

présentée à

l'UNIVERSITÉ des SCIENCES et TECHNIQUES de LILLE

pour obtenir

LE GRADE DE DOCTEUR DE 3ÈME CYCLE
Spécialité : MATHÉMATIQUES PURES

par

Louis YOUSSEF

LE GROUPE DES MODULES BILINÉAIRES.

SOUS-MODULES D'ALGÈBRES DE QUATERNIONS.

Membres du Jury : ZINN-JUSTIN N., Présidente
LEGRAND D., Rapporteur
FAKIR S., Examinateur

Soutenue le 18 Octobre 1983

Je dédicace cette thèse

à mes parents,

à mes biens aimés HASSIBA, HOUSSAM, MARWAN *et* ALISSAR,

à mes amis.

Je tiens à remercier ici Denise LEGRAND qui m'a beaucoup aidé dans ce travail et à qui je réserve toute ma gratitude et mon respect.

Je remercie également Nicole ZINN-JUSTIN qui a dirigé mes premiers pas dans la recherche mathématique et Sabah FAKIR d'avoir accepté de participer au jury.

Raymonde BÉRAT a dactylographié ce travail avec soin, rapidité et patience, je la remercie vivement, ainsi que les services de l'imprimerie de l'U.E.R. de Mathématiques de LILLE I.

1ère PARTIE

LE GROUPE DES MODULES BILINEAIRES

ET

LE GROUPE DES ALGEBRES BILINEAIRES

INTRODUCTION

Ce travail est inspiré de l'article de A. MICALI et A. PAQUES intitulé "Le groupe des algèbres quadratiques" [5]. Dans cet article, les deux auteurs reprennent la théorie des algèbres munies de formes quadratiques afin de constuire pour les algèbres projectives de rang constant $\geqslant 2$ sur un anneau dans lequel 2 est inversible, l'analogue du groupe $Q_{\text{sép}}(K)$ des extensions quadratiques séparables d'un anneau K, commutatif et associatif à élément unité, étudié par T. KANZAKI [4]. Pour ce faire, ils développent la théorie des algèbres quadratiques traitée de leur point de vue, puis ils construisent leur groupe.

Dans notre étude, nous reprenons la théorie des modules munis de formes bilinéaires dans le but de construire l'analogue du groupe des algèbres quadratiques étudié dans [5], sans condition d'inversibilité pour 2. On procède comme suit :

Dans la première partie, on définit les modules bilinéaires et les algèbres bilinéaires sur un anneau K, commutatif et associatif à élément unité dont l'élément 2 n'est pas nécessairement inversible. Un module bilinéaire est un triplet (A,φ,e) où A est un K-module, φ une forme bilinéaire symétrique sur A et e un élément dans A tel que $\varphi(e,e) = 1$.

On voit que e est libre et que A admet une décomposition de la forme $A = Ke \oplus X(A)$. On définit également les morphismes et les isomorphismes qu'on appelle bilinéaires, de modules bilinéaires.

Dans la deuxième partie, on définit une opération notée (*) sur l'ensemble des K-modules bilinéaires projectifs de type fini et de rang constant ≥ 2, munis de formes bilinéaires symétriques strictement non dégénérées : Pour deux tels modules bilinéaires (A,φ,e) et (A',φ',e'), on pose $A*A' = K\varepsilon \oplus (X(A) \otimes_K X(A'))$ où ε est libre. Le K-module $A*A'$ est projectif de type fini et de rang constant ≥ 2. On munit $A*A'$ d'une forme bilinéaire symétrique Φ telle que :

$$\Phi(\varepsilon,\varepsilon) = 1 \quad \text{et} \quad \forall (x,x') \text{ et } (y,y') \text{ dans } X(A) \times X(A') :$$

$$\Phi(\varepsilon,x\otimes x') = \varphi(x,e)\varphi'(x',e'),$$

$$\Phi(x\otimes x',y\otimes y') = \varphi(x,e)\varphi(y,e)\varphi'(x',y') + \varphi'(x',e')\varphi'(y',e')\varphi(x,y) - \varphi(x,y)\varphi'(x',y')$$

(Ces relations sont différentes des relations utilisées dans [5]).
Φ est alors strictement non dégénérée. $A*A'$ dépend du choix de $X(A)$ et $X(A')$, mais la classe d'isomorphisme bilinéaire de $(A*A,\Phi,\varepsilon)$ est indépendante de ce choix. La relation (*) induit sur l'ensemble des classes d'isomorphisme bilinéaire des K-modules bilinéaires de rang 2, une structure de groupe abélien qu'on note $\mathcal{B}_2$; et sur l'ensemble des toutes les classes d'isomorphisme bilinéaire des K-modules bilinéaires de rang constant ≥ 2, une structure de monoïde commutatif noté $\mathcal{B}$ contenant $\mathcal{B}_2$ qui y opère fidèlement.

Le groupe des K-modules bilinéaires est le groupe universel du monoïde commutatif $\mathcal{B}$. On l'appelle aussi groupe des algèbres bilinéaires sur K si on suppose de plus 2 régulier dans K.

P L A N

Pages

1. MODULES BILINEAIRES ET ALGEBRES BILINEAIRES.

Dans toute la suite, K est un anneau commutatif unitaire d'élément neutre noté 1 et dont l'élément 2 n'est pas nécessairement inversible. Les K-modules considérés sont des K-modules unitaires.

1.1. - *Modules et algèbres associés aux formes bilinéaires.*

Soient A un K-module et $\varphi : A \times A \to K$ une forme bilinéaire symétrique sur A.

Définition 1.1.1.- On dira que A est un module bilinéaire associé à φ, s'il existe un élément e dans A tel que $\varphi(e,e) = 1$.

A tout $e \in A$ tel que $\varphi(e,e) = 1$, on associe le module bilinéaire (A,φ) muni de e que l'on notera (A,φ,e) et qu'on appellera simplement module bilinéaire s'il n'y a pas de confusion possible quant à e.

On définit sur (A,φ,e) un produit par :

$$(1) \qquad \forall\, x, y \in A, \quad xy = -\varphi(x,y)e + \varphi(x,e)y + \varphi(y,e)x .$$

Il est immédiat que le module A muni de ce produit est une algèbre d'unité e.

Définition 1.1.2.- On dira que A est une algèbre bilinéaire associée à φ et e, si (A,φ,e) est un module bilinéaire muni du produit défini par (1). On la notera également (A,φ,e).

Proposition 1.1.3.- L'algèbre bilinéaire (A,φ,e) est une algèbre de Jordan commutative.

En effet, il est immédiat que $\forall\, x, y \in A$,
$(x^2y)x = x^2(yx)$ et $xy = yx$.

Proposition 1.1.4.- Soit (A,φ,e) un K-module bilinéaire, alors :

i) e est libre,

ii) Ke est facteur direct de A, et A admet une décomposition orthogonale $Ke \perp B$.

Preuve :

i) Si $ae = 0$ pour un élément a de K, alors $\varphi(a\,e,e) = a = 0$.

ii) Soit $\sigma : A \to A$, l'application définie par :

$\forall\, x \in A,\quad \sigma(x) = \varphi(x,e)e$

σ est K-linéaire car φ est K-bilinéaire et $\sigma \circ \sigma = \sigma$

σ est donc un projecteur.

Ainsi $A = \sigma(A) \oplus \sigma^{-1}(0) = \mathrm{Im}\,\sigma \oplus \mathrm{Ker}\,\sigma$.

Or, $\mathrm{Im}\,\sigma = Ke$ et $\mathrm{Ker}\,\sigma = \{y \in A \mid \varphi(y,e) = 0\} = (Ke)^{\perp}$ car e est libre.

Par conséquent $A = Ke \perp \mathrm{Ker}\,\sigma$.

On notera $X(A)$ un supplémentaire quelconque de Ke dans A et on écrira $A = Ke \oplus X(A)$. Dans le cas où $X(A) = (Ke)^{\perp}$, on écrira $A = Ke \perp X(A)$.

1.2. - *Morphismes de modules bilinéaires.*

Soient (A,φ,e) et (A',φ',e') deux K-modules bilinéaires.

Définition 1.2.1.- Un morphisme $h : (A,\varphi,e) \to (A',\varphi',e')$ de K-modules bilinéaires est une application K-linéaire $h : A \to A'$ telle que $h(e) = e'$ et $\forall\, x, y \in A$, $\varphi(x,y) = \varphi'(h(x),h(y))$.

On appelle un tel h, un morphisme bilinéaire.

Un isomorphisme bilinéaire est un morphisme bilinéaire bijectif.

Proposition 1.2.2.- i) Si $h : (A,\varphi,e) \to (A',\varphi',e')$ est un morphisme de modules bilinéaires, alors h est un morphisme d'algèbres bilinéaires.

ii) Si A et A' sont projectifs de rang constant et 2 régulier dans l'anneau K, on a :

$$\underset{(a)}{(h \text{ est un isomorphisme de modules bilinaires})} \iff \underset{(b)}{(h \text{ est un isomorphisme d'algèbres bilinéaires})}.$$

Preuve :

i) h est K-linéaire tel que $h(e) = e'$ et $\forall\, x, y \in A$, on a :

$$\begin{aligned} h(xy) &= h(-\varphi(x,y)e + \varphi(x,e)y + \varphi(y,e)x) \\ &= h(-\varphi'(h(x),h(y))e + \varphi'(h(x),e')y + \varphi'(h(y),e')x) \\ &= -\varphi'(h(x),h(y))e' + \varphi'(h(x),e')h(y) + \varphi'(h(y),e')h(x) \\ &= h(x)h(y). \end{aligned}$$

ii) (a) $\Longrightarrow$ (b) d'après i).

(b) $\Longrightarrow$ (a), en effet,

On a pour tout $(x,y) \in A^2$, $h(xy) = h(x)h(y)$

$h(xy) = -\varphi(x,y)h(e) + \varphi(x,e)h(y) + \varphi(y,e)h(x)$

$h(x)h(y) = -\varphi'(h(x),h(y))h(e) + \varphi'(h(x),h(e))h(y) + \varphi'(h(y),h(e))h(x)$

d'où, puisque h est injectif

$$(\varphi'(h(x),h(y)) - \varphi(x,y))e + (\varphi'(h(x),h(e)) - \varphi(x,e))y + (\varphi'(h(y),h(e)) - \varphi(y,e))\,x = 0.$$

Ce qui implique, compte tenu du fait que $A = Ke \oplus X(A)$ avec e libre :

$\forall\, x,y \in X(A)$, $\varphi'(h(x),h(y)) = \varphi(x,y)$

et $(\varphi'(h(x),h(e)) - \varphi(x,e))y + (\varphi'(h(y),h(e)) - \varphi(y,e))x = 0.$

En particulier, on a :

$\forall\, x \in X(A)$, $2(\varphi'(h(x),h(e)) - \varphi(x,e))x = 0.$

Mais $X(A)$ est projectif et l'application

$g : x \mapsto 2(\varphi'(h(x),h(e)) - \varphi(x,e))$ est une forme linéaire sur $X(A)$.

Donc, $\forall x \in X(A)$, $2(\varphi'(h(x),h(e)) - \varphi(x,e)) = 0$

(en effet, on peut trouver un prolongement nul de g à un module libre dont $X(A)$ est facteur direct).

Puisque 2 est régulier dans K, on a

$\forall x \in X(A)$, $\varphi'(h(x),h(e)) = \varphi(x,e)$.

C.Q.F.D.

Soit (A,φ,e) un K-module bilinéaire. L'élément $e \in A$ est choisi tel que $\varphi(e,e) = 1$. On a vu que e est libre et Ke facteur direct dans A. Il existe en particulier un supplémentaire de Ke dans A qui est l'orthogonal de Ke pour φ.

Soit $X(A)$ un supplémentaire quelconque de Ke dans A. On écrit $A = Ke \oplus X(A)$.

Proposition 1.2.3.- <u>Il existe une forme bilinéaire symétrique Ψ sur A pour laquelle $X(A)$ est l'orthogonal de Ke et telle que $(A,\varphi,e) \simeq (A,\Psi,e)$, autrement dit, telle que φ soit équivalente à Ψ.</u>

Preuve :

L'application $\sigma : A \to A$ définie pour tout $y = \alpha e + x \in A$ par $\sigma(\alpha e+x) = \alpha e + \varphi(x,e)e - x$ est un K-automorphisme de A. En effet, elle est K-linéaire et $\sigma \circ \sigma = 1_A$.

Soit Ψ la forme bilinéaire symétrique définie sur A par

$\forall x, y \in A, \Psi(x,y) = \varphi(\sigma(x),\sigma(y))$ (ou ce qui est équivalent par

$\forall x, y \in A, \varphi(x,y) = \Psi(\sigma(x),\sigma(y))$).

σ est un isomorphisme de modules bilinéaires de (A,Ψ,e) sur (A,φ,e).

$X(A)$ est l'orthogonal de Ke pour Ψ et $\sigma(X(A))$ est l'orthogonal de Ke pour φ.

Donc (A,Ψ,e) et (A,φ,e) appartiennent à la même classe d'isomorphisme. La forme φ sur $Ke \oplus X(A)$ est équivalente à une forme Ψ pour laquelle $X(A)$ est l'orthogonal de Ke.

Proposition 1.2.4.- Si (A,φ,e) et (A',φ',e') sont deux K-modules bilinéaires libres, isomorphes, alors les discriminants de φ et φ' sont égaux à un carré d'élément inversible près dans K. La réciproque est vraie si A et A' sont de dimension 2.

Preuve :

Soit $h : (A,\varphi,e) \to (A',\varphi',e')$ un isomorphisme bilinéaire où A et A' sont munis des bases respectives $(e_i)_{0\leqslant i\leqslant n-1}$ où $e = e_o$ et $(e'_j)_{0\leqslant j\leqslant n-1}$ où $e'_o = e'$.

Alors, $\text{disc}\ \varphi = \text{disc}\ \varphi'(\det N)^2$ où N est la matrice de passage de la base $(e'_j)_j$ à la base $(h(e_j))_j$ dont le déterminant est un élément inversible de K et $\text{disc}\ \varphi$ et $\text{disc}\ \varphi'$ les discriminants de φ et φ' par rapport à $(e_i)_i$ et $(e'_j)_j$ respectivement.

Réciproquement, si A et A' sont libres de dimension 2 et de bases respectives $\{e,x\}$ et $\{e',x'\}$ tels que :
$\text{dis}\ \varphi \equiv \text{disc}\ \varphi' \pmod{U^2(K)}$ où $U(K)$ est le groupe des éléments inversibles de K, alors, (A,φ,e) et (A',φ',e') sont isomorphes. En effet, d'après la proposition précédente, il existe une forme Ψ équivalente à φ et une forme Ψ' équivalente à φ' telles que :

$$\Psi(e,e) = 1,\quad \Psi(e,x) = 0,\quad \Psi(x,x) = \delta$$

et $\Psi'(e',e') = 1$, $\Psi'(e',x') = 0$, $\Psi'(x',x') = \delta' = u^2\delta$ où $u \in U(K)$, δ et δ' sont les discriminants de φ et φ' pour ces bases.
$\{e',u^{-1}x'\}$ est encore une base de A' et l'application linéaire $g : A \to A'$ définie sur la base $\{e,x\}$ de A par $g(e) = e'$ et $g(x) = u^{-1}x'$ est un isomorphisme bilinéaire de (A,Ψ,e) sur (A',Ψ',e').

C.Q.F.D.

2. LE GROUPE DES MODULES BILINEAIRES.

Dans cette partie, les modules bilinéaires considérés sont des modules projectifs de type fini et de rang constant $n \geq 2$.

2.1. - *L'opération* (*).

Soient (A,ψ,e) et (A',ψ',e') deux K-modules bilinéaires. On écrit $A = Ke \oplus X(A)$ et $A' = Ke' \oplus X(A')$ où $X(A)$ et $X(A')$ sont des supplémentaires quelconques de Ke et de Ke' respectivement. Ces supplémentaires étant fixés, on pose $A * A' = K\varepsilon \oplus (X(A) \otimes_K X(A'))$. $A * A'$ est ainsi un K-module projectif de type fini et de rang constant ≥ 2.

On va définir sur $A * A'$ une structure de module bilinéaire.

Proposition 2.1.1.- Il existe une application K-bilinéaire unique $\Phi : (A * A') \times (A * A') \to K$ telle que :

$$\begin{cases} \Phi(\varepsilon,\varepsilon) = 1, \\ \forall(x,x') \in X(A) \times X(A'), \Phi(\varepsilon, x \otimes x') = \psi(x,e)\psi'(x',e') \\ \forall(x,x'),\ (y,y') \in X(A) \times X(A'), \\ \Phi(x\otimes x', y\otimes y') = \psi(x,e)\psi(y,e)\psi'(x',y')+\psi'(x',e')\psi'(y',e')\psi(x,y)-\psi(x,y)\psi'(x',y'). \end{cases}$$

Preuve :

1) L'application $\psi_o : (x,x') \mapsto \psi(x,e)\psi'(x',e')$ de $X(A) \times X(A')$ dans K est K-bilinéaire, il existe donc une application K-linéaire unique $\psi_1 : X(A) \otimes X(A') \to K$ telle que

$$\forall(x,x') \in X(A) \times X(A'),\ \psi_1(x \otimes x') = \psi_o(x,x') = \psi(x,e)\psi'(x',e').$$

On pose pour tous $\alpha \in K$ et $z \in X(A) \otimes X(A'), \Phi(\alpha\varepsilon, z) = \alpha\psi_1(z)$.

2) L'application $\psi_2 : (x,x',y,y') \to \psi(x,e)\psi(y,e)\psi'(x',y') +$
$\psi'(x',e')\psi'(y',e')\psi(x,y) - \psi(x,y)\psi'(x',y')$

de $X(A) \times X(A') \times X(A) \times X(A')$ dans K est 4-linéaire, il lui correspond une forme K-bilinéaire unique Φ sur $X(A) \otimes X(A')$ telle que

$\forall (x,x'), (y,y') \in X(A) \times X(A')$,

$\Phi(x\otimes x',y\otimes y') = \psi(x,e)\psi(y,e)\psi'(x',y')+\psi'(x',e')\psi'(y',e')\psi(x,y)-\psi(x,y)\psi'(x',y')$

(cf. [1], ch. II p. 82).

On pose $\Phi(\varepsilon,\varepsilon) = 1$ et comme tout élément de $A * A'$ s'écrit de manière unique $\alpha\varepsilon + z$ avec $\alpha \in K$ et $z \in X(A) \otimes X(A')$, on en déduit le résultat.

La forme bilinéaire obtenueest symétrique, on la notera $\psi * \psi'$.

Remarques :

1) $(A * A',\Phi,\varepsilon)$ dépend des choix de $X(A)$ et $X(A')$.

2) Lorsque $X(A) = (Ke)^{\perp}$ et $X(A') = (Ke')^{\perp}$, $X(A * A') = X(A)\otimes X(A') = (K\varepsilon)^{\perp}$.

Proposition 2.1.2.- Soient (A,ψ,e) et (A',ψ',e') deux modules bilinéaires. S'il existe un isomorphisme bilinéaire $f : (A,\psi,e) \to (A_1,\psi_1,e_1)$ tel que $f(X(A)) = X(A_1)$ et un isomorphisme bilinéaire $f' : (A',\psi',e') \to (A'_1,\psi'_1,e'_1)$ tel que $f'(X(A')) = X(A'_1)$, alors les modules bilinéaires $(A * A',\psi * \psi',\varepsilon)$ et $(A_1 * A'_1,\psi_1 * \psi'_1,\varepsilon_1)$ sont isomorphes.

En effet, l'unique application K-linéaire $F : A * A' \to A_1 * A'_1$ telle que $F(\varepsilon) = \varepsilon_1$ et $F_{|X(A)\otimes X(A')} = f_{|X(A)} \otimes f_{|X(A')}$ est un isomorphisme bilinéaire comme on le vérifie immédiatement.

Proposition 2.1.3.- La classe d'isomorphisme bilinéaire du module bilinéaire $(A * A',\Phi,\varepsilon)$ est indépendante des choix de $X(A)$ et $X(A')$.

Preuve :

D'après les propositions précédentes 1.2.3. et 2.1.2., on peut se ramener au cas où $X(A)$ est l'orthogonal de Ke dans A et $X(A')$ est l'orthogonal de Ke' dans A' i.e. Φ est la forme pour laquelle

$X(A) \otimes X(A')$ est l'orthogonal de $K\varepsilon$ dans $A * A'$.

Soit $X_1(A)$ (resp. $X_1(A')$) un supplémentaire quelconque de Ke dans A (resp. de Ke' dans A') et soit $(A \underset{1}{*} A', \Phi_1, \varepsilon)$ le K-module bilinéaire associé où $A \underset{1}{*} A' = K\varepsilon \oplus (X_1(A) \otimes X_1(A'))$.

On a, $\begin{cases} \Phi(\varepsilon,\varepsilon) = 1 \text{ et } \forall (x,x') \text{ et } (y,y') \in X(A) \times X(A') \\ \Phi(x \otimes x',\varepsilon) = 0 \text{ et } \Phi(x \otimes x', y \otimes y') = -\psi(x,y)\psi'(x',y') \end{cases}$

$$\begin{cases} \Phi_1(\varepsilon,\varepsilon) = 1 \text{ et } \forall (x_1,x_1') \text{ et } (y_1,y_1') \in X_1(A) \times X_1(A') \\ \Phi_1(x_1 \otimes x_1',\varepsilon) = \psi(x_1,e)\psi'(x_1',e') \text{ et} \\ \Phi_1(x_1 \otimes x_1', y_1 \otimes y_1') = \psi(x_1,e)\psi(y_1,e)\psi'(x_1',y_1') + \\ \qquad + \psi'(x_1',e')\psi'(y_1',e')\psi(x_1,y_1) - \psi(x_1,y_1)\psi'(x_1',y_1'). \end{cases}$$

Tout $x_1 \in X_1(A)$ s'écrit de manière unique $x_1 = x + \psi(x_1,e)e$ avec $x \in X(A)$ et tout $x_1' \in X_1(A')$ s'écrit de manière unique $x_1' = x' + \psi'(x_1',e')e'$ avec $x' \in X(A')$.

L'application $\tau : x_1 \to x_1 - \psi(x_1,e)e$ est un K-isomorphisme de $X_1(A)$ sur $X(A)$ (c'est la restriction à $X_1(A)$ de la projection canonique de A sur $X(A)$).

De même, l'application $\tau' : x_1' \to x_1' - \psi'(x_1',e')e'$ est un K-isomorphisme de $X_1(A')$ sur $X(A')$.

On a $\forall (x_1,x_1')$ et $(y_1,y_1') \in X_1(A) \times X_1(A')$,

$$\Phi(\tau(x_1) \otimes \tau'(x_1'),\varepsilon) = 0 = \Phi_1(x_1 \otimes x_1' - \Phi_1(x_1 \otimes x_1',\varepsilon),\varepsilon)$$

$$\begin{aligned} \Phi(\tau(x_1) \otimes \tau'(x_1'),\tau(y_1) \otimes \tau'(y_1')) &= -\psi(\tau(x_1),\tau(y_1))\psi'(\tau'(x_1'),\tau'(y_1')) \\ &= -\psi(x_1-\psi(x_1,e)e, y_1-\psi(y_1,e)e)\psi'(x_1'-\psi'(x_1',e')e', y_1'-\psi'(y_1',e')e') \\ &= -\psi(x_1,y_1)\psi'(x_1',y_1') + \psi(x_1,e)\psi(y_1,e)\psi'(x_1',y_1') + \\ &\quad \psi'(x_1',e')\psi'(y_1',e')\psi(x_1,y_1) - \psi(x_1,e)\psi(y_1,e)\psi'(x_1',e')\psi'(y_1',e') \\ &= \Phi_1(x_1 \otimes x_1', y_1 \otimes y_1') - \Phi_1(x_1 \otimes x_1',\varepsilon)\Phi_1(y_1 \otimes y_1',\varepsilon) \\ &= \Phi_1(x_1 \otimes x_1' - \Phi_1(x_1 \otimes x_1',\varepsilon)\varepsilon, y_1 \otimes y_1' - \Phi_1(y_1 \otimes y_1',\varepsilon)\varepsilon). \end{aligned}$$

On associe à Φ_1 la forme équivalente Ψ_1 pour laquelle $X_1(A) \otimes X_1(A')$ est l'orthogonal de $K\varepsilon$.

On a $\Phi(\tau(x_1) \otimes \tau'(x_1'),\varepsilon) = 0 = \Psi_1(x_1 \otimes x_1',\varepsilon)$

et $\Phi(\tau(x_1) \otimes \tau'(x_1'),\tau(y_1) \otimes \tau'(y_1')) = \Psi_1(x_1 \otimes x_1',y_1 \otimes y_1')$.

Si T est l'application de $(K\varepsilon \oplus (X_1(A) \otimes X_1(A')),\Psi_1,\varepsilon)$ sur $(K\varepsilon \oplus (X(A) \otimes X(A')),\Phi,\varepsilon)$ définie par

$T(\alpha\varepsilon + z_1) = \alpha\varepsilon + (\tau \otimes \tau')(z_1)$ pour tous $\alpha \in K$ et $z_1 \in X_1(A) \otimes X_1(A')$, T est un isomorphisme bilinéaire.

Donc Φ et Ψ_1 et par suite Φ et Φ_1 sont équivalentes.

C.Q.F.D.

Corollaire.- Soient (A,φ,e) et (A',φ',e') deux modules bilinéaires et (A_1,φ_1,e_1) (resp. (A_1',φ_1',e_1')) un module bilinéaire isomorphe à (A,φ,e) (resp. (A',φ',e')) alors les modules bilinéaires $(A * A',\varphi * \varphi',\varepsilon)$ et $(A_1 * A_1',\varphi_1 * \varphi_1',\varepsilon_1)$ sont isomorphes.

Proposition 2.1.4.- Si (A,φ,e) et (A',φ',e') sont deux K-modules bilinéaires alors, φ et φ' sont strictement non-dégénérées si et seulement si $\Phi = \varphi * \varphi'$ est strictement non-dégénérée.

Preuve :

1) *Cas libre*.

On doit montrer que :

(disc $\varphi \in U(K)$ et disc $\varphi' \in U(K)$) $\Longleftrightarrow$ (disc $\Phi \in U(K)$).

Comme deux modules bilinéaires libres, isomorphes ont les mêmes discriminants à un carré d'élément inversible près dans K, on peut donc se ramener au cas où $X(A) = (Ke)^{\perp}$ et $X(A') = (Ke')^{\perp}$ avec $A = Ke \oplus X(A)$ et $A' = Ke' \oplus X(A')$.

Si A est de dimension n et de base $\{e,x_1,\dots,x_{n-1}\}$ et A'

de dimension m et de base $\{e', x'_1, \ldots, x'_{m-1}\}$, alors

$A * A' = K\varepsilon \oplus (X(A) \otimes X(A'))$ est de dimension $(n-1)(m-1) + 1$ et de base $\{\varepsilon, x_i \otimes x_j \ (i = 1,\ldots,n-1,\ \ j = 1,\ldots,m-1)\}$ muni de la forme $\Phi = \psi * \psi'$ définie antérieurement et pour laquelle $X(A) \otimes X(A') = (K\varepsilon)^{\perp}$.

Soient δ, δ' et Δ les discriminants correspondants de ψ, ψ' et Φ on a

$\delta = \det(\psi(x_i,x_j))_{i,j}$ où la matrice $(\psi(x_i,x_j))_{i,j}$ est de rang $n-1$

$\delta' = \det(\psi'(x'_i,x'_j))_{i,j}$ où la matrice $(\psi'(x'_i,x_j))_{i,j}$ est de rang $m-1$

$\Delta = \det(-\psi(x_i,x_j)\psi'(x'_k,x'_\ell))_{i,j,k,\ell} = (-1)^{(n-1)(m-1)}\det(\psi(x_i,x_j)\psi'(x'_k,x'_\ell))_{i,j,k,\ell}$

est le déterminant d'une matrice de rang $(n-1)(m-1)$.

$(\psi(x_i,x_j))_{i,j}, (\psi'(x'_k,x'_\ell))_{k,\ell}$ et $(\psi(x_i,x_j)\psi'(x'_k,x'_\ell))_{i,j,k,\ell}$ étant les matrices des endomorphismes $I : K^{n-1} \to K^{n-1}$, $J : K^{m-1} \to K^{m-1}$ et $I \otimes J : K^{(n-1)(m-1)} \to K^{(n-1)(m-1)}$ par rapport aux bases canoniques, donc $\Delta = (-1)^{(n-1)(m-1)}\det(I \otimes J)$.

Or, $\det(I \otimes J) = \det((I \otimes 1_{K^{m-1}}) \circ (1_{K^{n-1}} \otimes J)) = \det(I \otimes 1_{K^{m-1}})\det(1_{K^{n-1}} \otimes J)$

$$= \det \underbrace{\begin{pmatrix} I & & 0 \\ & \ddots & \\ 0 & & I \end{pmatrix}}_{(m-1) \text{ blocs}} \cdot \det \underbrace{\begin{pmatrix} J & & 0 \\ & \ddots & \\ 0 & & J \end{pmatrix}}_{(n-1) \text{ blocs}} = \delta^{m-1}\delta'^{\,n-1}$$

(cf. [1] chap. III, p. 101).

D'où $\left[\Delta = (-1)^{(m-1)(n-1)}\delta^{m-1}\delta'^{\,n-1} \in U(K)\right] \Longleftrightarrow \left[\delta, \delta' \in U(K)\right]$

2) *Cas projectif de rang constant* $\geqslant 2$.

Soit Ω l'ensemble des idéaux maximaux de K, alors

(ψ et ψ' sont strictement non-dégénérées) $\Longleftrightarrow$ $(\forall P \in \Omega)$ (ψ_p et ψ'_p sont strictement non-dégénérées).

([6], p. 17)

$\iff$ $(\forall\, p \in \Omega)(\psi_p * \psi'_p$ est strictement non dégénérée) ; d'après 1)

$\iff$ $(\forall\, p \in \Omega)((\psi * \psi')_p$ est strictement non dégénérée) ; "du fait qu'il existe un isomorphisme bilinéaire canonique entre $A_p * A'_p$ muni de la forme $\psi_p * \psi'_p$ et $(A * A')_p$ muni de $(\psi * \psi')_p$".

$\iff$ $(\psi * \psi' = \Phi$ est strictement non dégénérée).

C.Q.F.D.

Dans tout ce qui suit, les modules bilinéaires considérés seront des modules projectifs de type fini et de rang constant $\geqslant 2$, dont les formes bilinéaires symétriques associées sont strictement non-dégénérées.

Soient $\mathcal{B}_n$ l'ensemble des classes d'isomorphisme bilinéaire des tels modules bilinéaires de rang n et $\mathcal{B} = \bigcup_{n \geqslant 2} \mathcal{B}_n$. La classe d'un module bilinéaire (A,ψ,e) sera notée $\bar{A}$.

2.2. - *Etude de* $\mathcal{B}_2$.

Soient (A,ψ,e) et (A',ψ',e') deux K-modules bilinéaires tels que $\bar{A}$ et $\bar{A}'$ soient dans $\mathcal{B}_2$. Alors $A * A'$ est un module projectif de rang 2 sur K et sa forme $\psi * \psi'$ est strictement non dégénérée (proposition 2.1.4.). La classe d'équivalence $\overline{A * A'}$ de $A * A'$ ne dépend que des classes $\bar{A}$ et $\overline{A'}$ (corollaire de la proposition 2.1.3.), on la notera $\bar{A} * \overline{A'}$.

A tout couple $(\bar{A},\overline{A'})$ d'éléments de $\mathcal{B}_2$, on associe l'élément $\bar{A} * \overline{A'}$ de $\mathcal{B}_2$. On définit ainsi une loi de composition interne (*) sur $\mathcal{B}_2$.

Proposition 2.2.1.- $\mathcal{B}_2$ muni de la loi (*) est un groupe abélien.

Preuve :

i) Commutativité : Si (A,ψ,e) et (A',ψ',e') sont tels que $\bar{A} \in \mathcal{B}_2$ et $\bar{A}' \in \mathcal{B}_2$ alors l'application $\beta : (A*A',\psi*\psi',\varepsilon) \to (A'*A,\psi'*\psi,\varepsilon)$

définie sur les générateurs par $\beta(\varepsilon) = \varepsilon$ et pour tous $x \in X(A)$ et $x' \in X(A')$, $\beta(x \otimes x') = x' \otimes x$, est évidemment un isomorphisme bilinéaire. ([1], II p. 78).
(On se ramène dans toute la suite au cas orthogonal).

ii) Associativité : Si (A,φ,e), (A',φ',e') et (A'',φ'',e'') sont tels que $\bar{A}$, $\overline{A'}$ et $\overline{A''}$ soient dans $\mathcal{B}_2$ alors l'application K-linéaire

$\gamma : (A * (A'*A''),\varphi * (\varphi'*\varphi''),\varepsilon) \to ((A*A') * A'',(\varphi * \varphi') * \varphi'',\varepsilon_1)$ telle que $\gamma(\varepsilon) = \varepsilon_1$ et $\gamma(x \otimes (x' \otimes x'')) = (x \otimes x') \otimes x''$ pour tout (x,x',x'') dans $X(A) \times X(A') \times X(A'')$, est un isomorphisme ($\gamma_{|X(A)\otimes(X(A')\otimes X(A''))}$ est l'isomorphisme d'associativité). ([1], II, p. 94).

γ est bilinéaire en effet, pour tout $(x,x',x'') \in X(A) \times X(A') \times X(A'')$
$(\varphi * (\varphi'*\varphi''))(\varepsilon,x \otimes (x'\otimes x'')) = 0 = ((\varphi*\varphi') * \varphi'')(\varepsilon_1,(x\otimes x') \otimes x'')$ et pour tous (x,x',x''), $(y,y',y'') \in X(A) \times X(A') \times X(A'')$ on a

$$(\varphi * (\varphi'*\varphi''))(x \otimes (x'\otimes x''),y \otimes (y'\otimes y'')) = -\varphi(x,y)(\varphi'*\varphi'')(x'\otimes x'',y'\otimes y'')$$
$$= \varphi(x,y)\varphi'(x',y')\varphi''(x'',y'') = ((\varphi*\varphi') * \varphi'')((x \otimes x') \otimes x'',(y\otimes y') \otimes y'').$$

iii) Existence d'un élément neutre :

Soit $K \times K$ le K-module libre muni de la base canonique $\{(1,0),(0,1)\}$ et soit $\mu : (K \times K) \times (K \times K) \to K$ l'application définie par :
$\forall (a,b) \in K \times K$. $\forall (c,d) \in K \times K, \mu((a,b),(c,d)) = ac-bd$.
μ est une forme bilinéaire symétrique strictement non-dégénérée puisque, pour cette base, disc $\mu = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} = -1 \in U(K)$.

Ainsi $(K \times K,\mu,(1,0))$ est un module bilinéaire et $\overline{K \times K} \in \mathcal{B}_2$.
(Tout module libre est projectif).

Pour tout module bilinéaire (A,φ,e) tel que $\bar{A} \in \mathcal{B}_2$, on considère l'application K-linéaire $\rho : A * (K \times K) = K\varepsilon \oplus (X(A) \otimes K) \to A = Ke \oplus X(A)$ telle que $\rho(\varepsilon) = e$ et $\rho(x \otimes a) = ax$ pour tout $(x,a) \in X(A) \times K$.
ρ est clairement un K-isomorphisme ([1], II, p. 83), cet isomorphisme est bilinéaire, en effet

$\forall(a,x) \in K \times X(A)$, on a $\psi(\rho(x\otimes a),e) = (\psi*\mu)(x\otimes a,\varepsilon) = 0$

et $\forall\ x,y \in X(A)$, $(\psi*\mu)(x\otimes a,y\otimes b) = -\psi(x,y)\mu((0,a),(0,b)) = ab\ \psi(x,y)$

$$= \psi(ax,by) = \psi(\rho(x\otimes a),\rho(y\otimes b)).$$

Donc $\overline{K \times K}$ est l'élément neutre de $\mathcal{B}_2$.

iv) Eléments inversibles :

Tout élément de $\mathcal{B}_2$ a un inverse. En effet :

Soit (A,ψ,e) tel que $\bar{A} \in \mathcal{B}_2$ et $A = Ke \oplus X(A)$ avec $X(A) = (Ke)^{\perp}$

$\psi|_{X(A)}$ étant strictement non-dégénérée, l'application

$\theta : X(A) \to X(A)^* = \mathrm{Hom}_K(X(A),K)$ définie par $\theta(x) = (\psi_x : y \to \psi(x,y))$

pour tout $x \in X(A)$ est un isomorphisme.

On considère le K-module $Ke' \oplus X(A)^* = A'$ et la forme bilinéaire symétrique strictement non-dégénérée $\psi' : A' \times A' \to K$ définie par $\psi'(e',e') = \psi(e,e) = 1$ et $\psi'(\psi_x,\psi_y) = \psi(x,y)$.

Ainsi (A',ψ',e') est un K-module bilinéaire tel que $\overline{A'} \in \mathcal{B}_2$ et $X(A)^* = (Ke')^{\perp}$.

$X(A)$ étant projectif de rang 1, alors l'unique application K-linéaire

$\ell : (A*A' = K\varepsilon \oplus (X(A)\otimes X(A)^*),\psi*\psi',\varepsilon) \to (K \times K,\mu,(1,0))$ telle que

$\ell(\varepsilon) = (1,0)$ et $\ell(x\otimes\psi_y) = (0,\psi(x,y))$ pour tous $x \in X(A),\psi_y \in X(A)^*$

est un isomorphisme bilinéaire. En effet, il suffit de le montrer localement.

On suppose donc $X(A)$ libre de base $\{x\}$, $X(A)^*$ l'est aussi de base $\{\psi_x\}$.

$\psi(x,x)$ est alors le discriminant de ψ, soit $\delta \in U(K)$, pour cette base. ℓ est donc l'application qui à ε associe $(1,0)$ et à $x \otimes \psi_x$ associe $(0,\delta)$ avec $\delta \in U(K)$. Ainsi ℓ est un isomorphisme ([3], p. 143).

Cet isomorphisme est bilinéaire en effet :

$$(\varphi * \varphi')(\varepsilon, x \otimes \varphi_x) = 0 = \mu((1,0),(0,\varphi(x,x)))$$

$$\text{et} \quad (\varphi * \varphi')(x \otimes \varphi_x, x \otimes \varphi_x) = -\varphi(x,x)^2 = \mu((0,\varphi(x,x)),(0,\varphi(x,x))).$$

Donc $\bar{A}'$ est l'inverse de $\bar{A}$. Or $(A,\varphi,e) \simeq (A',\varphi',e')$ donc $\bar{A}' = \bar{A}$ et l'inverse de $\bar{A}$ n'est autre que $\bar{A}$ lui-même.

Remarque :

Si on désigne par $\mathcal{B}_{2\ell}$ l'ensemble des classes d'isomorphisme bilinéaire des modules bilinéaires libres de dimension 2, $\mathcal{B}_{2\ell}$ est clairement un sous-groupe de $\mathcal{B}_2$.

2.3. - *Etude de* $\mathcal{B} = \bigcup_{n \geq 2} \mathcal{B}_n$.

Comme pour $\mathcal{B}_2$, on définit sur $\mathcal{B}$ une loi de composition interne $(*)$ en posant pour tout $(\bar{A},\bar{A}')$ dans $\mathcal{B} \times \mathcal{B}$, $\bar{A} * \bar{A}' = \overline{A * A'}$

Proposition 2.3.1.- $\mathcal{B}$ muni de la loi $(*)$ est un monoïde commutatif.

En effet, la commutativité et l'associativité se démontrent comme pour $\mathcal{B}_2$. L'élément neutre $\overline{K \times K}$ de $\mathcal{B}_2$ est aussi l'élément neutre de $\mathcal{B}$ du fait que pour tout (A,φ,e) représentant de $\bar{A}$ dans $\mathcal{B}_2$, $A * (K \times K) \simeq A$ (isomorphisme analogue à l'isomorphisme utilisé pour $\mathcal{B}_2$).

Notre groupe des modules bilinéaires est le groupe universel $K_o(\mathcal{B})$ du monoïde commutatif $\mathcal{B}$.

L'opération $(*)$ induit une action de $\mathcal{B}_2$ sur chaque $\mathcal{B}_n$ $(n \geq 2)$ et par suite une action de $\mathcal{B}_2$ sur $\mathcal{B}$ et sur le sous-monoïde $\mathcal{B}^p = \bigcup_{k \geq 1} \mathcal{B}_{2k}$ de $\mathcal{B}$.

Proposition 2.3.2.- i) $\mathcal{B}_2$ opère fidèlement sur $\mathcal{B}$ et sur $\mathcal{B}^p$.

ii) Lorsque K est un anneau semi-local, $\mathcal{B}_2$ opère fidèlement sur chaque $\mathcal{B}_{2k}$ $(k \geqslant 1)$.

Preuve :

i) Immédiat : $\mathcal{B}_2$ est un sous-monoïde de $\mathcal{B}$ et de $\mathcal{B}^p$.

ii) Soit $k \geqslant 1$ fixé, $\mathcal{B}_2$ opère fidèlement sur $\mathcal{B}_{2k}$ si et seulement si

$$\forall\ \bar{D}, \bar{D}' \in \mathcal{B}_2, \quad (\forall\ \bar{A} \in \mathcal{B}_{2k}, \ \bar{D} * \bar{A} = \bar{D}' * \bar{A}) \Rightarrow \bar{D} = \bar{D}'.$$

Soient $\bar{A} \in \mathcal{B}_{2k}$, $\bar{D} \in \mathcal{B}_2$, $\bar{D}' \in \mathcal{B}_2$, A, D, D' des représentants de $\bar{A}$, $\bar{D}$, $\bar{D}'$ respectivement. Puisque K est semi-local, A est libre de dimension 2k, D et D' libres de dimension 2 ([3], p. 143). (Pour simplifier, on a écrit A au lieu de (A,φ,e) etc...).

Soient δ_A, δ_D et $\delta_{D'}$ les discriminants de A, D, D' (définis à un facteur près dans $U^2(K)$).

$\bar{D} * \bar{A} = \bar{D}' * \bar{A} \Rightarrow \mathrm{dis}(D * A) \equiv \mathrm{disc}(D' * A) \pmod{U^2(K)}$

$\bar{D} * \bar{A} = \bar{D}' * \bar{A} \Rightarrow (-1)^{2k-1}\delta_D{}^{2k-1}\delta_A \equiv (-1)^{2k-1}\delta_{D'}{}^{2k-1}\delta_A \pmod{U^2(K)}$

$\bar{D} * \bar{A} = D' * \bar{A} \Rightarrow \delta_D \equiv \delta_{D'} \pmod{U^2(K)}$.

Il résulte de la proposition 1.2.4. que

$$\bar{D} * \bar{A} = \bar{D}' * \bar{A} \Rightarrow \bar{D} = \bar{D}'.$$

Remarque :

L'action de $\mathcal{B}_2$ sur les $\mathcal{B}_n$ $(n > 2)$ n'est pas en général transitive (exemple $K = \mathbb{R}$).

2.4. - *Le groupe des algèbres bilinéaires.*

On suppose de plus dans ce paragraphe que 2 est régulier dans l'anneau K. Ainsi, un isomorphisme bilinéaire de modules bilinéaires est un isomorphisme d'algèbres bilinéaires associées. Donc, le groupe des modules bilinéaires $K_o(\mathcal{B})$ pourra être appelé le groupe des algèbres bilinéaires.

Proposition 2.4.1.- L'anneau K s'injecte canoniquement comme K-algèbre dans toute K-algèbre bilinéaire.

En effet, si (A,φ,e) est une algèbre bilinéaire, l'application $i : K \to A$ définie par $i(\alpha) = \alpha e$ pour tout $\alpha \in K$ est un morphisme d'algèbres injectif car e libre.

Proposition 2.4.2.- Soient (A,φ,e) une K-algèbre bilinéaire et $f : A \to K$ la forme quadratique sur A définie par $f(x) = \varphi(x,x)$ pour tout $x \in A$, alors (A,f,e) est une algèbre quadratique au sens de [5].

En effet, la forme bilinéaire symétrique associée à f est 2φ. D'après le produit défini sur (A,φ,e), on a

$$\forall\, x \in A, \quad x^2 = -\varphi(x,x)e + 2\varphi(x,e)x.$$

Soient (A,φ,e) et (A',φ',e') deux algèbres bilinéaires, $f : A \to K$ et $f' : A' \to K$ les formes quadratiques sur A et A' définies pour tous $x \in A$ et $x' \in A'$ par $f(x) = \varphi(x,x)$ et $f'(x') = \varphi'(x',x')$.

Proposition 2.4.3.- $h : (A,\varphi,e) \to (A',\varphi',e')$ est un isomorphisme d'algèbres bilinéaires si et seulement si $h : (A,f,e) \to (A',f',e')$ est un isomorphisme d'algèbres quadratiques au sens de [5].

Preuve :

Si h est un isomorphisme d'algèbres bilinéaires ; alors h est un isomorphisme de modules bilinéaires i.e. h est K-linéaire bijectif tel que $h(e) = e'$ et pour tout $x \in A$,

$f(x) = \varphi(x,x) = \varphi'(h(x),h(x)) = f'(h(x)) = (f' \circ h)(x)$.

Réciproquement, si h est un isomorphisme d'algèbres quadratiques, alors h est K-linéaire bijectif tel que $h(e) = e'$ et $\forall\, x \in A$, $\forall\, y \in A$ on a

$$2\varphi(x,y) = f(x+y) - f(x) - f(y)$$

$$2\varphi(x,y) = f'(h(x) + h(y)) - f'(h(x)) - f'(h(y))$$

$$2\varphi(x,y) = 2\varphi'(h(x),h(y)).$$

Donc $\varphi(x,y) = \varphi'(h(x),h(y))$ puisque 2 est régulier.

Donc h est un isomorphisme de modules bilinéaires et par conséquent d'algèbres bilinéaires.

Conclusion.

D'après ce qui précède, on en conclut que :

1) La classe d'isomorphisme d'une algèbre bilinéaire (A,φ,e) n'est autre que la classe d'isomorphisme de l'algèbre quadratique (A,f,e) où f est la forme quadratique associée à φ.

2) Dans une algèbre bilinéaire (A,φ,e), φ est strictement non-dégénérée, mais dans l'algèbre quadratique (A,f,e), f ne l'est nécessairement que lorsque 2 est inversible.

3) Le groupe $\mathcal{B}_2$ peut être donc considéré comme groupe des extensions quadratiques de K non nécessairement séparables.

B I B L I O G R A P H I E

[1] BOURBAKI N. - Algèbre, chap. I, II, III.

[2] BOURBAKI N. - Algèbre, chap. IX.

[3] BOURBAKI N. - Algèbre commutative, chap. 1 et 2.

[4] KANZAKI T. - On the quadratic extensions and the extended Witt ring of a commutative ring (Nagoya Math. J. 49, 1973, p. 127-141).

[5] MICALI A. - PAQUES A. - Le groupe des algèbres quadratiques. (comm. in algebra, 1982).

[6] MICALI A - REVOY P. - Modules quadratiques. (Bull. Soc. Math. de France, Mémoire n° 63).

2ème PARTIE

SOUS-MODULES D'ALGEBRES DE QUATERNIONS

INTRODUCTION

Dans son article "Submodules of quaternion algebras" [4], KAPLANSKY reprend le travail de Brandt sur la composition des formes quadratiques quaternaires, le généralise convenablement et ajoute plusieurs points nouveaux. On essaie de voir d'une autre façon ou bien de généraliser quelques théorèmes apparus dans cet article. Pour cela, on expose tout ce qui est lié à cette étude en précisant les preuves des résultats cités par KAPLANSKY qui ne semblent pas immédiates.

Les paragraphes § 1, § 2, § 3 et § 4 reprennent les résultats de KAPLANSKY. Dans § 1, on introduit les notions de base sur les modules admissibles sur un anneau de Prüfer R. Dans § 2, on prouve quelques propriétés des $*$ - algèbres (algèbres avec une involution ($*$) convenable) : on montre qu'un module inversible est localement principal et que pour tout module admissible A, la norme est multiplicative sur A^*A. Dans § 3, on se restreint aux algèbres de quaternions et on prouve le résultat suivant : "pour tout module admissible A, AA^* est le produit d'un ordre par la norme de A". Dans § 4, on présente les principaux résultats de Brandt, généralisés par KAPLANSKY qui considère des sous R-modules admissibles d'une algèbre de quaternions sur le corps des fractions d'un anneau de Bezout R, et établit le lien entre ces modules et la classification et la composition des formes quadratiques.

Dans § 5, on essaie d'établir des résultats analogues aux résultats apparus dans § 4 dans le cas plus général où l'anneau de base est un anneau de Prüfer.

P L A N

§ 1 - *MODULES ADMISSIBLES.*

Soit R un anneau de Prüfer c'est-à-dire un anneau commutatif intègre dans lequel chaque idéal de type fini est inversible. On montre qu'un anneau commutatif intègre R est de Prüfer si et seulement si pour tout idéal maximal M de R, R_M est un anneau de valuation (cf. [8], p. 127).

Soient K le corps des fractions de R et L une algèbre associative unitaire de dimension finie sur K.

Définition 1.1.- Un sous R-module A de L est dit admissible s'il est de type fini sur R et engendre L comme un espace vectoriel sur K.

Il est immédiat que si A, B, A_i, $(i = 1,\dots,n)$ sont des modules admissibles et $x \in L$ inversible, les modules AB, xA, $\bigcap_{i=1}^{n} A_i$ et $E = \{x \in | L\ xA \subseteq B\}$ sont admissibles.

Remarque :

On entend par module admissible un sous R-module admissible de L.

Définitions 1.2.- i) Un ordre est un module admissible qui est un anneau contenant 1.

ii) Si A est un module admissible, $P = \{x \in L | xA \subseteq A\}$ est l'ordre à gauche de A et $Q = \{x \in L | Ax \subseteq A\}$ est l'ordre à droite de A.

$A^{-1} = \{x \in L | AxA \subseteq A\}$ est l'inverse de A.

Il est clair que P et Q sont des ordres et que $AA^{-1} \subseteq P$ et $A^{-1}A \subseteq Q$.

Définition 1.3.- Si $AA^{-1} = P$ on dit que A est inversible à droite. Si $A^{-1}A = Q$, on dit que A est inversible à gauche. Si A est inversible à gauche et à droite, on dit que A est inversible.

Remarque :

Dans la suite, on laisse tomber l'adjectif admissible puisque tous les modules considérés sont admissibles.

On en déduit que si x est un élément inversible de L et A un module inversible d'ordre à gauche P et d'ordre à droite Q alors

1) A^{-1} est inversible, d'inverse A, d'ordre à gauche Q et d'ordre à droite P.

2) xA est inversible d'inverse $A^{-1}x^{-1}$, l'ordre à droite de xA est Q et l'ordre à gauche est le conjugué xPx^{-1}.

L'observation fondamentale de Brandt est qu'on ne peut travailler convenablement avec le produit AB que lorsque l'ordre à droite de A coïncide avec l'ordre à gauche de B. On est amené à poser la définition :

Définition 1.4.- Soient A et B deux modules, le couple ordonné (A,B) est dit concordant si l'ordre à droite de A est égal à l'ordre à gauche de B.

Ainsi, si A et B sont deux modules inversibles et si (A,B) est concordant, le produit AB est inversible d'inverse $B^{-1}A^{-1}$, l'ordre à gauche de AB est l'ordre à gauche de A et l'ordre à droite de AB est l'ordre à droite de B.

Définition 1.5.- Un module est dit principal s'il est de la forme xP où P est un ordre et x un élément inversible de L.

Cette définition est symétrique puisque $xP = (xPx^{-1})x$ (donc $xP = Qx$ où Q est un ordre).

Il en découle qu'un module principal est inversible.

Il est classique qu'un module A est inversible si et seulement si pour tout idéal maximal M de R, A_M est inversible comme R_M-module. Pour utiliser cette méthode locale, on va montrer que lorsque R est un anneau de valuation, les modules inversibles sont principaux. C'est vrai si l'algèbre L est commutative. Dans le paragraphe 2, on étendra ce résultat aux $*$ - algèbres. Pourtant ce n'est pas toujours vrai ([4], 2, p. 221).

On utilisera le lemme suivant :

Lemme 1.6.- Soit A un module inversible dont les ordres à gauche et à droite sont égaux disons à P. On suppose que pour un certain entier $n > 0$, $A^{n+1} = A^n$, alors $A = P$.

En effet, d'après ce qui précède, A^n est inversible d'ordres à gauche et à droite égaux à P. On multiplie sur la droite de $A^{n+1} = A^n$, par l'inverse de A^n, ce qui donne $AP = P$, d'où $A = P$.

§ 2 - * - ALGEBRES.

Soient R un anneau de Prüfer, K son corps des fractions et L une algèbre associative unitaire sur K.

Définition 2.1.- L est une $*$ - algèbre si L possède une involution $(*)$ telle que

$$\forall x \in L, \quad x + x^* \in K \quad \text{et} \quad xx^* \in K.$$

$x + x^*$ est la trace de x, on la note Tx ou $T(x)$.

xx^* est la norme de x, on la note Nx ou $N(x)$.

Il est clair que si L est une K- $*$ - algèbre, l'involution $(*)$ est unique, pour tout $x \in L$, x^* commute avec x et $x^2 - (Tx)x + Nx = 0$ i.e. L est une algèbre quadratique dans le sens que chaque élément vérifie une équation quadratique et que si K a plus de deux éléments et L est une algèbre quadratique, L est une $*$-algèbre.

Sur une $*$-algèbre L, N est une forme quadratique, la forme bilinéaire symétrique associée est l'application qui à tout couple (x,y) d'éléments de L associe l'élément $xy^* + yx^*$ de K que l'on note (x,y), et pour tout $x \in L$ on a $(x,x) = 2Nx$.

Définition 2.2.- Soit A un sous-R-module de la $*$-algèbre L. La norme de A qu'on note $N(A)$ est le R-idéal (éventuellement fractionnaire) engendré sur R par l'ensemble des Nx tels que $x \in A$.

Proposition 2.3.- i) L'idéal $N(A)$ est de type fini ;

ii) $\forall x \in L$, $N(xA) = Nx\, N(A)$;

iii) Si A et B sont des sous-modules de L, $N(AB) \supseteq N(A)N(B)$;

Si de plus le couple (A,B) est concordant et A ou B principal, $N(AB) = N(A)N(B)$.

En effet, $N(A)$ est de type fini car si les éléments x_i en nombre fini engendrent A sur R, les éléments Nx_i et (x_i,x_j) qui sont en nombre fini engendrent $N(A)$, d'où i).

ii) et iii) sont faciles à vérifier.

Définition 2.4.- Un semi-ordre est un sous R-module admissible A de L tel que $1 \in A$ et $N(A) = R$.

Cette définition est justifiée par le fait qu'un ordre est un semi-ordre.

On étudie d'abord le cas particulier où R est un anneau de valuation, on utilisera ensuite des méthodes de localisation.

Proposition 2.5.- Soient R un anneau de valuation, K son corps des fractions et L une $*$-algèbre, alors

i) si A est un sous-R-module de L, $N(A)$ est un idéal principal et la plus petite norme est atteinte. Soit $x \in A$ tel que $(Nx) = N(A)$ et soit $B = x^{-1}A$.

ii) B ainsi défini est un semi-ordre tel que $B = B^*$ et les ordres à gauche et à droite de B coïncident, il est libre de même dimension que L sur K, soit n.

iii) R est un facteur direct de B, $B^{n-1} = B^n$ et si de plus B est inversible, B est un ordre.

Preuve :

i) C'est vérifié d'après la définition d'un anneau de valuation, (étant donné un nombre fini d'éléments dans R, l'un divise tous les autres). ([3], p. 89-91).

ii) B est un semi-ordre car $1 = x^{-1}x \in x^{-1}A = B$ et de plus $N(B) = (N(1)) = (1) = R$.

Soit $y \in B$ alors $N(y) \in R$ et $N(1+y) \in R$ c'est-à-dire $(1+y)(1+y^*) = 1+y+y^*+yy^* \in R$. Donc $Ty = y+y^* \in R$, d'où $y \in B^*$. Inversement, si $y^* \in B^*$, $N(y^*) = N(y) \in R$ et $N(1+y^*) = N(1+y) \in R$. Donc $Ty^* = Ty = y+y^* \in R$ et $y^* \in B$.

Puisque de façon générale, l'ordre à gauche d'un module C est égal à l'ordre à droite de C^*, les ordres à gauche et à droite de B coïncident. Soit P cet ordre. Alors P est l'ordre à droite de A et xPx^{-1} son ordre à gauche.

B étant un module de type fini et sans torsion sur un anneau de valuation est libre ([3], p. 110) ; il engendre L comme K-espace vectoriel. La dimension du R-module libre B est donc la dimension du K-espace vectoriel L. Soit n cette dimension.

iii) On a $B \cap K = R$ et l'anneau de valuation R est intégralement clos, donc R est un facteur direct de B ([3], p. 92). Ainsi, on peut choisir une base de B de la forme $\{1,u_2,\ldots,u_n\}$. Pour montrer que $B^n = B^{n-1}$, il suffit de montrer qu'un produit de n éléments de la base de B appartient à B^{n-1}. Si 1 est parmi ces n éléments, c'est fini ; sinon il y a une répétition des u_i. Grâce à l'identité :

$$ab + ba = (Tb)a + (Ta)b - (a,b),$$

les u_i répétés peuvent être repoussés à la gauche des termes de B^{n-1}, jusqu'à ce qu'ils rencontrent leur homologue, en ce moment, on applique le fait que $u_i^2 - (Tu_i)u_i + Nu_i = 0$, les termes obtenus sont dans B^{n-1}.

Si, de plus, B est inversible, d'après le lemme 1.6., B est un ordre.

Théorème 2.6.- <u>Soient</u> R <u>un anneau de Prüfer</u>, K <u>son corps des fractions et</u> L <u>une *-algèbre, alors l'inversibilité d'un côté d'un sous-module de</u> L <u>implique l'inversibilité</u>.

Preuve :

Il suffit de montrer le théorème localement. Donc, soient R un anneau de valuation et A un sous-module de L. D'après la proposition précédente A se normalise en un semi-ordre $B = x^{-1}A$. On suppose que A est inversible à gauche ou à droite, alors il en est de même pour B. Puisque $B = B^*$, en appliquant l'involution on voit que B est inversible de l'autre côté, donc inversible. Il en résulte que A est inversible.

Théorème 2.7.- Soient R un anneau de valuation, K son corps des fractions et L une $*$-algèbre sur K, alors tout sous-module inversible de L est principal.

Preuve :

Si A est un sous-R-module inversible de L, avec les notations précédentes il en est de même pour $B = x^{-1}A$. Ainsi, d'après la proposition précédente B est un ordre. Donc $A = xB$ est principal.

Théorème 2.8.- Soient R un anneau de Prüfer, K son corps des fractions, L une $*$-algèbre sur K, A et B deux sous-modules de L tels que le couple (A,B) soit concordant et A ou B inversible, alors $N(AB) = N(A)N(B)$.

Preuve :

Il suffit de le montrer localement. Lorsque R est un anneau de valuation, d'après le théorème précédent, A ou B est principal et d'après la proposition 2.3. $N(AB) = N(A)N(B)$.

Théorème 2.9.- Soient R un anneau de Prüfer, K son corps des fractions, L une $*$-algèbre sur K et A un sous-module de L, alors $N(A^*A) = N(A^*)N(A)$.

Preuve :

Dans le cas où R est un anneau de valuation, on passe comme plus haut de A à $B = x^{-1}A$.

On a $B^{n-1} = B^n = B^{n+1} = \dots = B^{2n-2}$

donc B^{n-1} est un ordre. Les éléments d'un ordre sont entiers et ainsi la norme des puissances de B est R.

En particulier $N(B^2) = R$. On revient à $A = xB$ et on a

$A^*A = Bx^*xB = (Nx)B^2$.

Or, $(N(x)) = N(A) = N(A^*)$. D'où $N(A^*A) = N(A^*)N(A)$.

Ce résultat se globalise immédiatement. ([2], p. 112-113).

Théorème 2.10.- Soient R un anneau de Prüfer, K son corps des fractions, L une $*$-algèbre sur K de dimension n et $m = [n/2]$, alors pour tout sous-module A de L on a $(A^*A)^m \doteq N(A)^m P$ où P est un ordre.

Preuve :

Il suffit de le montrer lorsque R est un anneau de valuation.

$$m = [n/2] \iff 2m = \begin{cases} n-1 & \text{si } n \text{ est impair.} \\ n & \text{si } n \text{ est pair.} \end{cases}$$

On a $B^{n-1} = B^n = P$ où P est un ordre. Donc, $B^{2m} = P$ et $(A^*A)^m = (Nx)^m B^{2m} = N(A)^m P$ où $A = xB$. Pour $n = 4$, on a $m = 2$ et $(A^*A)^2 = N(A)^2\ P$.

Dans le paragraphe suivant, on va montrer que $A^*A = N(A)P$ dans le cas où L est une algèbre de quaternions.

§ 3 - *ALGEBRES DE QUATERNIONS*.

Définition 3.1.- Une algèbre de quaternions L sur un corps K est une algèbre centrale simple de dimension 4, elle est ou bien une algèbre de division, ou bien l'algèbre de toutes les matrices 2×2 sur K.

Il est connu qu'une algèbre de quaternions L est une $*$-algèbre et que la forme bilinéaire symétrique associée à la norme est non-dégénérée, même en caractéristique 2 quand cette forme est alternée.

Les deux lemmes suivants sont bien connus :

Lemme 3.2.- Si a et b sont deux éléments inversibles de L, l'application $x \to axb$ est un automorphisme de L qui multiplie toute norme par $N(ab)$. Mais, l'involution $x \to x^*$ laisse les normes stables. (L étant une algèbre de quaternions sur K).

Inversement,

Lemme 3.3.- Soit F une transformation linéaire bijective de L qui multiplie toute norme par un facteur fixe non nul. Alors F à la forme $x \to axb$ ou $x \to ax^*b$ pour des éléments inversibles convenables a et b de L.

Soient R un anneau de Prüfer, K son corps des fractions et L une algèbre de quaternions sur K.

Théorème 3.4.- Si A est un sous-module de L, $A^*A = N(A)P$ où P est un ordre.

Preuve :

Il suffit de le montrer lorsque R est un anneau de valuation. On a vu qu'on peut normaliser A en un semi-ordre $B = x^{-1}A$ avec $x \in A$, élément de norme minimale. On a prouvé que $B^3 = B^4$. On pose $P = B^3$. Alors P est un ordre (preuve du th. 2.9).

Soient M l'unique idéal maximal de R et $P_o = P/MP$. Alors P_o est une algèbre de dimension 4 sur le corps résiduel R/M et chaque élément de P_o vérifie une équation quadratique, B s'applique sur un sous-espace B_o de P_o qui contient 1 et engendre l'algèbre P_o. Si la dimension de B_o est 1 ou 2, B_o est une sous-algèbre propre et ne peut pas engendrer P_o, donc B_o est au moins de dimension 3 et par suite $B_o^2 = P_o$.

Ainsi $B^2 = P$ d'après le lemme de Nakayama ([5], p. 242).

Donc $A^*A = (Nx)B^2 = N(A)P$.

On en déduit le résultat suivant (bien connu dans le cas où R est un anneau de Dedekind) :

Théorème 3.5.- Soient Q un ordre maximal contenu dans L et A un sous-module de L dont l'ordre à droite est Q. Alors A est inversible.

Preuve :

D'après le théorème précédent $A^*A = N(A)P$ pour un ordre convenable P. P contient l'ordre à droite Q de A. Puisque Q est maximal, $P = Q$. Mais $N(A)^{-1}A^*A = P$ ce qui implique $N(A)^{-1}A^* \subseteq A^{-1}$, ainsi $A^{-1}A = P$ et A est inversible (théorème 2.6).

C.Q.F.D.

§ 4 - GENERALISATION DES RESULTATS DE BRANDT.

Avant d'aborder l'étude des théorèmes d'inversibilité de Kaplansky nous donnons rapidement le lien entre la théorie des modules et la théorie de composition des formes quadratiques quaternaires selon Brandt, théorie qui a conduit Kaplansky à donner ces théorèmes. Kaplansky utilise la technique des couples.

Couples - Equivalence de couples.

Si on utilise la définition naturelle d'équivalence des modules ($B \sim A$ s'il existe deux éléments inversibles x et y de L tels que $B = xAy$) des difficultés apparaissent. Par exemple, les ordres à droite et à gauche d'une classe d'équivalence ne sont définis qu'aux automorphismes intérieurs près, la concordance a un sens mais le produit des classes d'équivalence n'est pas bien défini.

Soit $\mathcal{C}$ l'ensemble des couples (A,a) tels que A soit un sous-module (admissible) de L et a un élément non nul de K.

Définition 4.1.- <u>On dit que les couples</u> (B,b) <u>et</u> (A,a) <u>sont équivalents et on écrit</u> $(B,b) \sim (A,a)$, <u>s'il existe deux éléments inversibles</u> x <u>et</u> y <u>de</u> L <u>tels que</u> $B = xAy$ <u>et</u> $b = N(xy)a$.

Il est immédiat que la relation $(\sim)$ est une relation d'équivalence sur $\mathcal{C}$.

Par définition

. La norme d'un couple (A,a) est $N(A,a) = N(A)/a$.

. Le conjugué de (A,a) est (A^*,a).

. L'inverse de (A,a) est (A^{-1},a^{-1}).

. Le produit de deux couples (A,a) et (B,b) est (AB,ab).

. Un couple (A,a) est dit primitif si $N(A,a) = R$.

. Si A est libre de base $\{\alpha_1,\dots,\alpha_4\}$, le discriminant $\Delta_\alpha(A)$ relatif à cette base est le déterminant de la matrice $((\alpha_i,\alpha_j))$. Le déterminant $\Delta(A)$ de A est en fait la classe de $\Delta_\alpha(A)$ modulo $U^2(R)$ (où $U(R)$ est le groupe des éléments inversibles de R). Il est connu que $\Delta_\alpha(A)$ est un carré dans K donc un carré dans R s'il est dans R car R est intégralement clos.

Le discriminant du couple (A,a) relatif à la base $(\alpha_1,\dots,\alpha_4)$ est $\Delta_\alpha(A)/a^4$. Le discriminant de (A,a) que l'on note $\Delta(A,a)$ est la classe de $\Delta_\alpha(A)/a^4$ modulo $U^2(R)$.

Tout scalaire appartenant à cette classe est aussi appelé un discriminant du couple.

Il est à noter que la norme de la classe d'équivalence d'un couple est bien définie et que le discriminant d'un couple est bien défini sur la classe d'équivalence de ce couple.

Correspondance.

Dans la suite de ce paragraphe § 4, on se place dans le cas particulier où R est un anneau de Bezout c'est-à-dire un anneau commutatif intègre dans lequel tout idéal de type fini est principal. Dans ce cas, les sous-modules (admissibles) de L sont libres.

Etant donné un couple (A,a), on munit A de la forme quadratique donnée par la norme divisée par a. Lorsqu'on choisit une base de A, il correspond à cette base une forme quadratique quaternaire concrète.

On veut établir une correspondance entre les classes d'équivalence de couples et les classes d'équivalence propre de formes quadratiques quaternaires concrètes (une équivalence propre correspond à un changement de base de déterminant 1, on supposera que K est de caractéristique $\neq 2$).

La correspondance est effective seulement pour les classes de couples et classes de formes admettant un discriminant donné.

On fixe un couple (A,a) admettant le discriminant Δ et on fixe arbitrairement une base $\{\alpha_1,\ldots,\alpha_4\}$ de A tel que le discriminant relatif à cette base soit exactement Δ.

Soit maintenant (B,b) un autre couple admettant le discriminant Δ.

Soit $(\beta_1,\ldots,\beta_4)$ une base de B et soit d le déterminant de la matrice exprimant les β_i en fonction des α_j. Il résulte des définitions que d^2a^4/b^2 est le carré d'une unité dans R. On dira que la base $(\beta_1,\ldots,\beta_4)$ est admissible si $da^2 = b^2$ (de telles bases existent). La forme quadratique concrète obtenue à partir d'une base admissible est l'image cherchée du couple (B,b).

Si (C,c) est un couple équivalent à (B,b), la classe d'équivalence de la forme quadratique concrète correspondante n'est pas changée.

On construit ainsi une application de l'ensemble des classes d'équivalence de couples de discriminant Δ dans l'ensemble des classes d'équivalence propre de formes quadratiques quaternaires concrètes de discriminant Δ. Cette application est injective. L'image est formée des classes des formes équivalentes sur K à un multiple scalaire de la forme fondamentale de L.

Composition.

Pour composer les classes d'équivalence propre de deux formes quadratiques quaternaires (lorsque cela est possible) on passe aux classes d'équivalence de couples et on multiplie. Le discriminant étant fixé, le produit doit avoir le même discriminant.

L'énoncé classique de Brandt peut être exprimé comme suit :

Si (A,a) et (B,b) sont primitifs avec (A,B) concordant, tous deux de discriminant Δ et si l'un des deux couples est inversible, alors (AB,ab) a pour discriminant Δ (ce qui est facile à montrer) et est primitif (ce qui résulte du théorème 2.8.).

Parmi les conditions données par Brandt pour que trois formes apparaissent dans une composition figurent des conditions qui correspondent à des conditions d'inversibilité. Kaplansky a généralisé comme suit les résultats de Brandt.

Théorèmes d'inversibilité de Kaplansky.

R désigne toujours un anneau de Bezout, K son corps des fractions et L une algèbre de quaternions sur K.

Les sous-modules (admissibles) de L sont donc libres de dimension 4.

Théorème 4.2.- Si A, B, C sont trois sous-modules de L, b et c deux éléments non nuls de K tels que $BC \subsetneq A$, que (B,b) et (C,c) soient primitifs et que (B,b), (C,c) et (A,bc) aient le même discriminant alors, $BC = A$, (A,bc) est primitif , A, B et C sont inversibles et (B,C) est concordant.

Preuve :

Il suffit d'établir le résultat localement. On peut ainsi supposer que R est un anneau de valuation. Soient x un élément de B de norme minimale et y un élément de C de norme minimale, c'est-à-dire tels que $(Nx) = N(B)$ et $(Ny) = N(C)$.

On pose $B_o = x^{-1}B$, $C_o = Cy^{-1}$ et $A_o = x^{-1}Ay^{-1}$.

Puisque (B,b) et (C,c) sont primitifs, $N(x)/b$ et $N(y)/c$ sont des unités dans R, il en résulte que A_o, B_o et C_o ont le même discriminant.

$B_oC_o = x^{-1}BCy^{-1} \subsetneq x^{-1}Ay^{-1} = A_o$ et puisque $1 \in C_o$, on a $B_o \subsetneq B_oC_o \subsetneq A_o$.

Or, deux modules comparables de même discriminant doivent être égaux.

Ainsi $A_o = B_o = C_o$ et $B_oC_o = A_o$.

D'après le théorème 3.4., $B_o^*B_o = N(B_o)P$ où P est un ordre

Or $B_o^* = B_o$ et $N(B_o) = R$.

Donc $B_oC_o = B_o^2 = A_o = P = B_o = C_o$.

Il s'ensuit que A, B et C sont principaux, d'où inversibles.

D'autre part, l'ordre à droite de B est P où $B = xB_o = xP$ et l'ordre à gauche de C est P où $C = C_oy = Py$, ainsi le couple (B,C) est concordant. Par conséquent, $N(BC)_{/bc} = N(B)N(C)_{/bc} = N(B)_{/b}N(C)_{/c} = R$ et $N(A,bc) = R$ i.e. (A,bc) est primitif.

C.Q.F.D.

Soit $A^{\#} = \{x \in L \,/\, (x,A) \subseteq R\}$ où A est un R-module et $(x,A) = \{(x,y) \,/\, y \in A\}$, (où (x,y) désigne le scalaire $xy^* + yx^*$).

La proposition suivante est facile à établir :

Proposition 4.3.- <u>Si</u> A <u>est un module admissible,</u> $A^{\#}$ <u>l'est aussi. Pour toute base</u> $\{u_1,\ldots,u_4\}$ <u>de</u> A, <u>il existe une base de</u> A <u>duale de la base</u> $\{u_1,\ldots,u_4\}$ <u>c'est-à-dire une base</u> $\{v_1,\ldots,v_4\}$ <u>de</u> $A^{\#}$ <u>telle que</u>

$$\forall\, i,j \in \{1,2,3,4\},\quad (u_i,v_j) = \delta_{ij}.$$

<u>La matrice</u> $((v_i,v_j))_{i,j}$ <u>est l'inverse de la matrice</u> $((u_i,u_j))_{i,j}$ <u>et par suite</u>

$$(1)\qquad \Delta_v(A^{\#}) = \Delta_u(A)^{-1}\ .$$

On note $\Delta(A)$ un discriminant quelconque de A. On sait que $\Delta(A)$ est un carré dans K. Soit $\delta(A)$ une racine carrée de $\Delta(A)$.

Théorème 4.4.- <u>Si</u> A, B <u>et</u> C <u>sont des sous-modules de</u> L <u>et</u> b <u>et</u> c <u>deux éléments non nuls de</u> K <u>tels que</u> $BC \subseteq A$, <u>que</u> (A,bc) <u>soit primitif et que</u> (B,b), (C,c) <u>et</u> (A,bc) <u>aient le même discriminant, on a</u> $N(A^{\#})\delta(A) \subseteq N(A)$.

Preuve :

$BC \subseteq A$, donc $(BC,A^{\#}) \subseteq R$ et puisque, pour tout $(x,y,z) \in B \times C \times A^{\#}, (xy,z) = (x,zy^*)$ on a aussi $(B,A^{\#}C^*) \subseteq R$ c'est-à-dire $A^{\#}C^* \subseteq B^{\#}$.

Donc $\forall\, t \in A^{\#},\ tC^* \subseteq B^{\#}$.

Puisque $\Delta(tC^*) = (Nt)^4\Delta(C^*)$, on a

$$(2)\qquad N(A^{\#})^4\Delta(C^*) \subseteq (\Delta(B^{\#})).$$

D'après (1), $\Delta(B^{\#}) = \Delta(B)^{-1}$. Il est clair que $\Delta(C^{*}) = \Delta(C)$ et l'égalité des discriminants de (B,b), (C,c) et (A,bc) implique que $\Delta(B) = \Delta(A)/c^4$ et $\Delta(C) = \Delta(A)/b^4$.

En substituant dans (2), on obtient :

$$(N(A^{\#}))^4 \Delta(A)^2 \subseteq (b^4c^4).$$

Puisque (A,bc) est primitif $(b^4c^4) = N(A)^4$. On en déduit l'inclusion $N(A^{\#})\delta(A) \subseteq N(A)$.

<u>*Théorème*</u> *4.5.-* $N(A^{\#})\delta(A) \subseteq N(A) \iff A$ <u>est inversible.</u>

<u>*Preuve*</u> :

Il suffit de prouver le théorème lorsque R est un anneau de valuation.

Si A est inversible, on applique le théorème 4.4. en prenant $C = A$, B = l'ordre à gauche de A, $b = 1$, $c = N(x)$ où x est de norme minimale.

Inversement, après normalisation de A, l'hypothèse devient $N(A^{\#})\delta(A) \subseteq R$. Puis on décompose A en somme directe orthogonale afin de prouver que $A^2 = A$ c'est-à-dire que A est un ordre et que le module de départ A est inversible. (La démonstration dans ([4],8) est détaillée et claire).

<u>*Théorème*</u> *4.6.-* <u>Si</u> A <u>est un anneau de valuation</u>, <u>alors pour tout sous-module</u> A <u>de</u> L, <u>ou</u> A <u>ou</u> $A^{\#}$ <u>est principal</u>.

<u>*Preuve*</u> :

R étant un anneau de valuation, les idéaux sont comparables. Si A n'est pas principal alors A n'est pas inversible et $N(A^{\#})\delta(A) \not\subseteq N(A)$; ainsi $N(A) \subseteq N(A^{\#})\delta(A)$.

Or $\delta(A) = \delta(A^{\#})^{-1}$, donc $N(A)\delta(A^{\#}) \subseteq N(A^{\#})$.

Par suite $A^{\#}$ est inversible, donc principal.

C.Q.F.D.

§ 5 - GENERALISATION DES RESULTATS DE KAPLANSKY.

Dans ce paragraphe, R désigne un anneau de Prüfer, K son corps des fractions et L une algèbre de quaternions sur K. Les sous-R-modules admissibles de L sont projectifs de rang 4. En effet, ils sont de type fini et localement libres de dimension 4.

On désigne par φ_N la forme bilinéaire symétrique associée à la norme N sur L. (On rappelle que $\forall\, x,y \in L$, $\varphi_N(x,y) = (x,y) = xy^* + yx^*$).

Soient A un sous-module de L et $a \in K - \{0\}$.

On utilise une notion élargie de discriminant (cf. [6], p. 24 ou [7], p. 12).

Définitions 5.1.- i) On appelle discriminant de A et on note $\Delta_o(A)$, la classe d'isomorphisme de $(\Lambda^4 A, \Lambda^4 \varphi_N)$.

ii) Le discriminant du couple (A,a) noté $\Delta_o(A,a)$ est la classe d'isomorphisme de $(\Lambda^4 A, \Lambda^4 \varphi_N / a^4)$.

On rappelle que $\Lambda^4 \varphi_N$ est l'unique forme bilinéaire symétrique définie sur $\Lambda^4 A$ telle que

$$\forall (x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4) \in A^4,$$

$$\Lambda^4\varphi_N(x_1 \wedge x_2 \wedge x_3 \wedge x_4, y_1 \wedge y_2 \wedge y_3 \wedge y_4) = \text{dét}((\varphi_N(x_i,y_j))_{i,j})$$

(cf. [1], p. 30).

Remarque :

Lorsque A est libre de dimension 4, $\Lambda^4 A$ est libre de dimension 1. Si $\{u_1,\dots,u_4\}$ est une base de A, $\{u_1 \wedge \dots \wedge u_4\}$

est une base de $\Lambda^4 A$ et la forme $\Lambda^4\psi_N : \Lambda^4 A \times \Lambda^4 A \to R$ est déterminée par la donnée de $\Lambda^4\psi_N(u_1 \wedge u_2 \wedge u_3 \wedge u_4, u_1 \wedge u_2 \wedge u_3 \wedge u_4)$ c'est-à-dire de $\det(((u_i,u_j))_{i,j})$.

A $\Delta_o(A)$ correspond la classe $\Delta(A)$ de $\Delta_u(A)$ mod $U^2(R)$ (discriminant usuel) et inversement.

On peut identifier $\Delta_o(A)$ et $\Delta(A)$ par cette bijection.

On a un résultat analogue pour $\Delta_o(A,a)$ et $\Delta(A,a)$.

Théorème 5.2.- Soient A, B, C trois sous-modules de L, a,b deux éléments non nuls de K. On suppose que $BC \subsetneq A$, que (B,b) et (C,c) sont primitifs et que (B,b), (C,c) et (A,bc) ont le même discriminant. Alors BC = A, (A,bc) est primitif ; A, B et C sont inversibles et le couple (B,C) est concordant.

Preuve :

Soit E un sous-module (admissible) quelconque de L et soit Ω l'ensemble des idéaux maximaux de R.

On sait que $\forall\, P \in \Omega$, il existe un isomorphisme canonique $\sigma_P : (\Lambda^4 E)_P \to \Lambda^4 E_P$ tel que

$\forall (x_1,x_2,x_3,x_4) \in E^4, \sigma_P((x_1 \wedge x_2 \wedge x_3 \wedge x_4) \otimes 1) = (x_1 \otimes 1) \wedge \ldots \wedge (x_4 \otimes 1)$.

$\forall (x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4) \in E^4$,

$(\Lambda^4\psi_N)_P((x_1 \wedge x_2 \wedge x_3 \wedge x_4) \otimes 1, (y_1 \wedge y_2 \wedge y_3 \wedge y_4) \otimes 1) =$

$= \Lambda^4(\psi_N)_P((x_1 \otimes 1) \wedge \ldots \wedge (x_4 \otimes 1), (y_1 \otimes 1) \wedge \ldots \wedge (y_4 \otimes 1))$.

Ainsi, la classe d'isomorphisme de $((\Lambda^4 E)_P, (\Lambda^4\psi_N)_P) = (\Delta_o(E))_P$ est égale à celle de $(\Lambda^4 E_P, \Lambda^4(\psi_N)_P) = \Delta_o(E_P)$.

On a, $\forall\, P \in \Omega$, R_P est un anneau de valuation, A_P, B_P et C_P sont libres de dimention 4, $B_P C_P \subsetneq A_P$, (B_P,b) et (C_P,c) sont primitifs.

Comme $\Delta_o(B,b) = \Delta_o(C,c) = \Delta_o(A,bc)$ alors $\forall$ $P \in \Omega$, $(\Lambda^4 B_P, \Lambda^4(\mathcal{O}_N)_P/b^4)$, $(\Lambda^4 C_P, \Lambda^4(\mathcal{O}_N)_P/c^4)$ et $(\Lambda^4 A_P, \Lambda^4(\mathcal{O}_N)_P/b^4c^4)$ sont isomorphes, ce qui revient à dire que $\Delta(B_P,b) = \Delta(C_P,c) = \Delta(A_P,bc)$.

Donc les conditions du théorème 4.2. sont remplies et on a : $B_PC_P = A_P$, (A_P,bc) est primitif, A_P, B_P et C_P sont inversibles et (B_P,C_P) est concordant, ceci pour tout $P \in \Omega$.

- Soit f l'injection canonique $f : BC \to A$ $\forall$ $P \in \Omega$, l'injection canonique correspondante $f_P : B_PC_P \to A_P$ ([2], p. 111-112), n'est autre que l'identité sur A_P, donc f est l'identité sur A et ainsi $BC = A$.

- On sait que A, B et C sont inversibles si et seulement si, $\forall$ $P \in \Omega$, A_P, B_P et C_P le sont.

- Montrer que (B,C) est concordant, c'est montrer que l'ordre à droite de B, soit D, est égal à l'ordre à gauche de C, soit G.

Soient pour tout $P \in \Omega$, D_P l'ordre à droite de B_P et G_P l'ordre à gauche de C_P. On va montrer que $D = \bigcap_{P\in\Omega} D_P$ et $G = \bigcap_{P\in\Omega} G_P$.

Il est immédiat que $\forall$ $P \in \Omega$, $(D)_P \subseteq D_P$ où $(D)_P$ est le localisé de D en P (en effet $D \subseteq D_P$ d'où $(D)_P \subseteq D_P$).

Comme $D = \bigcap_{P\in\Omega} (D)_P$, ([2], p. 112-113), il en résulte que $D \subseteq \bigcap_{P\in\Omega} D_P$.

Inversement, $\forall$ $x \in \bigcap_{P\in\Omega} D_P$, on a

$$\forall\ z_p \in B_P\ ,\quad z_p x \in B_p\ .$$

En particulier, on a, pour tout $y \in B$, $yx \in B_P$.

Comme $B = \bigcap_{P\in\Omega} B_P$, il en résulte que $yx \in B$. Donc $x \in D$.

On montre de même que $G = \bigcap_{P\in\Omega} G_P$. Il en résulte que $D = G$.

(On pouvait montrer que $\forall\, P \in \Omega$, $D_P = (D)_P$ et $G_P = (G)_P$).

Enfin, $N(A,bc) = N(A)/bc = N(BC)/bc = N(B)N(C)/bc$.

$N(A,bc) = R$.

Théorème 5.3.- Si A, B et C sont trois sous-modules de L et a,b deux éléments non nuls de K tels que $BC \subsetneq A$, que (A,bc) soit primitif et que (B,b), (C,c) et (A,bc) aient le même discriminant, alors

$$N(A^{\#})^2(\Lambda^4\psi_N\,(\Lambda^4 A \times \Lambda^4 A)) \subseteq N(A)^2 .$$

Preuve :

D'après la définition de $A^{\#}$, on remarque que $\forall\, P \in \Omega$, $(A^{\#})_P = (A_P)^{\#}$; R_P étant un anneau de valuation, A_P est libre, $(A^{\#})_P$ l'est aussi et de même dimension 4. Donc $A^{\#}$ est projectif de rang 4.

$\forall\, P \in \Omega$, A_P, B_P et C_P sont libres, $B_PC_P \subsetneq A_P$, (A_P,bc) est primitif et $\Delta(B_P,b) = \Delta(C_P,c) = \Delta(A_P,bc)$.

Donc, d'après la preuve du théorème 4.4., on a

$$[N_P((A_P)^{\#})]^2\Delta_{A_P} \subseteq [N_P(A_P)]^2 \tag{3}$$

où Δ_{A_P} est un discriminant quelconque de A_P.

Or $[N_P((A_P)^{\#})]^2 = [N_P(A^{\#})_P]^2 = (N(A^{\#}))^2_P$

$(N_P(A_P))^2 = (N(A))^2_P$ et $(\Delta_{A_P}) = \Lambda^4(\psi_N)_P(\Lambda^4 A_P \times \Lambda^4 A_P)$.

D'autre part, puisque $(N(A^{\#}))^2$, $(N(A))^2$ et $(\Lambda^4\psi_N(\Lambda^4 A \times \Lambda^4 A))$ sont des sous-R-modules de K, on a ([2], p. 112-113)) :

$$(N(A^{\#}))^2 = \bigcap_{P\in\Omega}(N(A^{\#}))^2_P , \qquad (N(A))^2 = \bigcap_{p\in\Omega}(N(A))^2_P ,$$

$$(\Lambda^4\psi_N(\Lambda^4 A \times \Lambda^4 A)) = \bigcap_{P\in\Omega} \Lambda^4(\psi_N)_P(\Lambda^4 A_P \times \Lambda^4 A_P)$$

et $\quad (N(A^{\#}))\,(\Lambda^4\psi_N(\Lambda^4 A \times \Lambda^4 A)) = \bigcap_{P\in\Omega} (N(A^{\#})_P)^2\,\Delta_{A_P}.$

On obtient, compte tenu de (3)

$$(N(A^{\#}))^2(\Lambda^4\psi_N(\Lambda^4 A \times \Lambda^4 A)) \subseteq (N(A))^2$$

Théorème 5.4.- Si A est un sous-module de L, alors :

$((N(A^{\#}))^2(\Lambda^4\psi_N(\Lambda^4 A \times \Lambda^4 A)) \subseteq (N(A))^2) \iff A$ est inversible.

Preuve :

Si A est inversible, alors $\forall P \in \Omega$, A_P est inversible R_P est un anneau de valuation, donc A_P est principal.

Soient B_P l'ordre à gauche de A_P et c un générateur de $N(A)_P$.

Alors les modules A_P, B_P et C_P où $C_P = A_P$ et les scalaires b et c où $b = 1$ vérifient les hypothèses du théorème précédent (pour l'anneau de base R_P). On a donc

$(N(A^{\#}))_P^2\Lambda^4(\psi_N)_P(\Lambda^4 A_P \times \Lambda^4 A_P) \subseteq (N(A))_P^2$ pour tout $P \in \Omega$,

d'où $(N(A^{\#}))^2(\Lambda^4\psi_N(\Lambda^4 A \times \Lambda^4 A)) \subseteq (N(A))^2$.

Inversement si l'on a cette inclusion on a, avec les notations du § 4 :

$$\forall P \in \Omega,\quad N(A_P^{\#})\,\delta(A_P) \subseteq N(A_P)$$

ce qui implique d'après le théorème 4.5. que A_P est inversible.

Donc A est inversible.

B I B L I O G R A P H I E

[1] BOURBAKI N. - Algèbre, Chap. IX.

[2] BOURBAKI N. - Algèbre commutative, Chap. 1 et 2.

[3] BOURBAKI N. - Algèbre commutative, Chap. 5 et 6.

[4] KAPLANSKY I. - Submodules of quaternion algebras, (Proc. London Math. Soc. (3) 19, 1969, p. 219-232).

[5] LANG S. - Algebra, (Addison - Wesley Publishing Company Inc. 1965).

[6] MICALI A. - REVOY P. - Modules quadratiques, (Bull. Soc. Math. de France, Mémoire n° 63).

[7] MILNOR J. - HUSEMOLLER D. - Symetric bilinear forms, (Springer-Verlag, Berlin Heidelberg, New York, 1973).

[8] RENAULT G. - Algèbre non commutative, (Gauthier-Villars).

RÉSUMÉ

Dans la première partie, on construit le monoïde des classes d'isomorphisme de modules bilinéaires pointés. Ces modules bilinéaires sont projectifs de type fini et de rang constant $\geqslant 2$, munis de formes bilinéaires symétriques strictement non dégénérées. On associe à ce monoïde "le groupe des modules bilinéaires" et lorsque 2 est régulier dans l'anneau de base, "le groupe des algèbres bilinéaires".

Afin de pouvoir donner une nouvelle présentation de la théorie de la composition des formes quadratiques quaternaires, Kaplansky a étudié les sous-modules admissibles des algèbres de quaternions. Il a donné en particulier des conditions d'inversibilité dans le cas où l'anneau de base est un anneau de Bezout. Dans la deuxième partie de ce travail, on reprend l'étude de Kaplansky et on établit des résultats analogues dans le cas plus général où l'anneau de base est un anneau de Prüfer.

<u>MOTS CLÉS</u> : . *PROJECTIF MODULE.*

. *SYMETRIQUE FORME BILINEAIRE.*

. *QUATERNION ALGEBRE.*

. *PRÜFER ANNEAU.*

. *INVERSIBLE MODULE.*