MÉMOIRES DE LA S. M. F.

A. MICALI
PH. REVOY

Modules quadratiques

Mémoires de la S. M. F., tome 63 (1979)
<http://www.numdam.org/item?id=MSMF_1979__63__1_0>

Bull. Soc. Math. France
Mémoire 63 , 1979 , 144p.

MODULES QUADRATIQUES

par

A. MICALI - Ph. REVOY

TABLE DES MATIERES

Table des matières.

Introduction. 7

1. Le groupe de Witt 9

1.1. Applications quadratiques 9
1.2. Applications quadratiques et puissances divisées 12
1.3. Extension des scalaires 14
1.4. Formes et applications quadratiques non dégénérées 17
1.5. Produit tensoriel d'applications quadratiques 18
1.6. Puissances extérieures et déterminant 21
1.7. Espaces hyperboliques et réflexivité 26
1.8. Groupes de Witt-Grothendieck et groupe de Witt 28
1.9. Retour aux espaces hyperboliques 32
1.10. L'homomorphisme de dimension 35
1.11. Décompositions orthogonales 38
1.12. Groupes et transformations orthogonales 43
1.13. Théorème de simplification de Witt 45
1.14. Autour du Satz 7 de Witt 48
1.15. Groupes de Witt d'un corps de caractéristique 2 52
1.16. Anneau de Witt d'un anneau de Prüfer 54
1.17. Exemples 56

2. Algèbres de Clifford 59

2.1. Définitions 59
2.2. Produit tensoriel gradué et algèbre de Clifford d'une somme 61
2.3. Structure de module de l'algèbre de Clifford 63
2.4. Extensions quadratiques 69
2.5. Extensions quadratiques graduées 77
2.6. Algèbres d'Azumaya et algèbres de Clifford 80
2.7. Algèbres de quaternions 88
2.8. Le groupe des classes d'algèbres de Clifford 93

3. Produits vectoriels et variétés de Stiefel 105

3.1. Produits vectoriels réels 105
3.2. Produit vectoriel algébrique 106
3.3. Algèbres cayleyennes et produit vectoriel 110
3.4. Variétés de Stiefel algébriques 117
3.5. Anneaux factoriels et sphères 123

4. Classes de Stiefel-Whitney 130

4.1. Introduction 130
4.2. Modules quadratiques sur les anneaux semi-locaux 131
4.3. Invariants de Stiefel-Whitney d'un plan 134
4.4. L'invariant de Stiefel-Whitney pour un espace quelconque 138

Bibliographie 141

INTRODUCTION

Après les travaux de Hasse sur l'arithmétique des formes quadratiques sur les corps de nombres algébriques, c'est H. Witt qui a fondé la théorie algébriques des formes quadratiques sur un corps quelconque, le cas particulier de la caractéristique 2 étant étudié par C. Arf quelques années plus tard. Le discriminant et l'algèbre de Clifford sont des invariants des formes quadratiques ; C.T.C. Wall combine ces deux invariants en un seul en introduisant, pour un corps, le groupe de Brauer gradué. Pour suivre le développement de la théorie algébrique des formes quadratiques sur un corps, le lecteur peut consulter les livres de T.Y. Lam et F. Lorenz cités dans la bibliographie.

En ce qui concerne la théorie des formes quadratiques sur un anneau quelconque, elle a été développée d'une part par H. Bass, d'autre part par A. Micali et O.E. Villamayor. Le premier, dans des notes du Tata Institute de 1967, a généralisé les constructions de C.T.C. Wall au cas des anneaux à l'aide des suites exactes de la K-théorie algébrique. Utilisant la notion de foncteur cofinal pour les espaces hyperboliques et les algèbres d'endomorphismes de modules projectifs $\mathbb{Z}/(2)$-gradués il construit ainsi un homomorphisme du groupe de Witt d'un anneau A dans le groupe de Brauer-Wall (ou groupe de Brauer gradué) de A.

Dans le même temps, A. Micali et O.E. Villamayor étudient les algèbres de Clifford des modules quadratiques sur un anneau et construisent l'image du groupe de Witt de A dans le groupe de Brauer-Wall. Dans un article ultérieur, H. Bass étudie les liens entre algèbres de Clifford et norme spinorielle (K-théorie du groupe orthogonal développée aussi par A. Bak).

Dans ce fascicule, les deux premiers chapitres sont consacrés à la construction explicite des deux invariants d'une forme quadratique : discriminant et algèbre de Clifford. Les chapitres 3 et 4 concernent des problèmes algébriques liés à des questions classiques de géométrie sur les espaces euclidiens et les sphères.

Plus précisément le but du premier chapitre est d'étudier la catégorie des modules quadratiques sur un anneau commutatif arbitraire, d'introduire le groupe de Witt-Grothendieck et le groupe de Witt et de donner quelques illustrations à l'aide de cas simples pris parmi les corps ou certains anneaux, par exemple aux paragraphes 11, 13, 14 et 15.

Dans le chapitre 2, nous définissons l'algèbre de Clifford et montrons que l'algèbre de Clifford d'une somme orthogonale est le produit tensoriel gradué

des algèbres de Clifford de chaque facteur. Ensuite nous étudions en détail la structure de module de cette algèbre. Les paragraphes 2.4 et 2.5 décrivent le groupe des extensions quadratiques de A dans les cas gradué et non gradué, groupe qui sert à définir le discriminant. La présentation s'inspire directement des travaux de O.E. Villamayor et A. Micali et de l'article de C. Small cité dans la bibliographie. Les paragraphes suivant commencent par des rappels, réduits au minimum, sur les algèbres d'Azumaya (ou centrales séparables). Ensuite, nous étudions le centre et la séparabilité de l'algèbre de Clifford et de sa composante homogène de degré 0, suivant le rang modulo 2 du module quadratique. Ensuite on étudie particulièrement les algèbres de quaternions qui permettent au dernier paragraphe de décrire, de façon très précise, la loi de groupe dans le groupe de Brauer-Wall, c'est à dire la relation entre l'algèbre de Clifford d'une somme orthogonale et celle de chaque facteur. Le groupe $\mathcal{H}(A)$ est l'image du groupe de Witt de A dans le groupe de Brauer-Wall de A.

Dans le chapitre 3, nous rappelons les résultats de Eckmann et Whitehead sur les r-produits vectoriels dans l'espace euclidien $\mathbb{R}^n$ et cherchons les modules quadratiques sur un anneau dans lequel 2 est inversible qui possèdent un r-produit vectoriel, la réponse étant pratiquement complète. Ensuite nous construisons les variétés de Stiefel algébriques et étudions la factorialité de l'anneau de la sphère sur un corps. Nous donnons ainsi une solution simple à un problème de R. Fossum (résolu de façon indépendante et compliqué par Ogama). Ensuite nous faisons des remarques sur un analogue algébrique de la parallélisabilité des sphères topologiques.

Le quatrième chapitre est consacré aux invariants de Steifel-Whitney des modules quadratiques sur un anneau semi-local (cf. [44]). Le cas des corps est dû à A. Delzant et Scharlau et celui des anneaux locaux à E. Hornix. Nous en donnons ici une construction plus simple à plusieurs égards.

Tout au long de ce travail, nous nous sommes efforcés d'utiliser des méthodes élémentaires dans la résolution des problèmes abordés. De plus, nous avons utilisé, de façon systématique, les méthodes d'algèbre commutative.

Qu'il nous soit ici permis de remercier tous ceux qui ont collaborés à la bonne mise en forme de ce travail. Nous remercions également Madame J. CELLIER et Monsieur J. MEYRAN, du secrétariat Mathématique de l'Université de Montpellier II, pour tout le travail matériel fourni en vue de la préparation de ce fascicule.

A. MICALI - Ph. REVOY

Montpellier, le 23 Novembre 1979.

1. LE GROUPE DE WITT

Tout anneau est commutatif à élément unité, tout morphisme d'anneaux est unitaire et tout module est unitaire. Désignons par Ann la catégorie des anneaux, par Mod celle des modules et par Mod(A) celle des A-modules, où A est un anneau fixé.

1.1. APPLICATIONS QUADRATIQUES.

Soient A un anneau et M et N deux A-modules. On dira que $q : M \to N$ est une application A-quadratique si les conditions suivantes sont vérifiées : A Q 1) pour tout $(a,x) \in A \times M$, $q(a\,x) = a^2\, q(x)$; A Q 2) l'application $\varphi : M \times M \to N$ définie par $(x,y) \mapsto q(x+y) - q(x) - q(y)$ est A-bilinéaire, nécessairement symétrique. On dira que φ est l'application A-bilinéaire symétrique associée à q.

Si $q : M \to A$ est une application A-quadratique, on dira aussi que q est une forme A-quadratique et que $\varphi : M \times M \to A$ est la forme A-bilinéaire symétrique associée à q.

Considérons la catégorie $\mathbf{C}$ dont les objets sont les quadruplets (A,M,q,N), où (A,M) et (A,N) sont des objets de Mod et $q : M \to N$ est une application A-quadratique ; les morphismes sont les triplets $(f,g,h) : (A,M,q,N) \to (A',M',q',N')$, où $(f,g) : (A,M) \to (A',M')$ et $(f,h) : (A,N) \to (A',N')$ sont des morphismes de Mod rendant commutatif le diagramme :

$$\begin{array}{ccc} M & \xrightarrow{\;q\;} & N \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ M' & \xrightarrow{\;q'\;} & N' \end{array}$$

Il est clair que si $(f,g,h) : (A,M,q,N) \to (A',M',q',N')$ est un morphisme de $\mathbf{C}$ le diagramme

$$\begin{array}{ccc} M\times M & \xrightarrow{\;\varphi\;} & N \\ {\scriptstyle g\times g}\downarrow & & \downarrow{\scriptstyle h} \\ M'\times M' & \xrightarrow{\;\varphi'\;} & N' \end{array}$$

est commutatif, où φ (resp. φ') est l'application A-bilinéaire (resp. A'-bilinéaire) symétrique associée à q (resp. q').

Réciproquement, la commutativité de ce dernier diagramme n'entraîne pas, en général, que $(f,g,h) : (A,M,q,N) \to (A',M',q',N')$ soit un morphisme de $\mathbf{C}$. Par contre, il en est bien ainsi si l'homothétie définie par 2 dans N' est injective. Ceci nous dit que, engénéral, on a

$$\mathrm{Hom}_{\mathbf{C}}\,((A,M,q,N),\,(A',M',q',N')) \subset_{\neq} \mathrm{Hom}_{\underline{\mathrm{Ann}}}\,(A,A') \times \mathrm{Hom}_{A}(M,M') \times \mathrm{Hom}_{A}(N,N').$$

Si l'on fixe l'anneau A, on notera $\mathbf{C}(A)$ la sous-catégorie de $\mathbf{C}$ dont les morphismes sont de la forme $(\mathrm{id}_A,g,h) : (A,M,q,N) \to (A,M',q,N')$, où g et h sont des applications A-linéaires rendant commutatif le diagramme :

$$\begin{array}{ccc} M & \xrightarrow{\;q\;} & N \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ M' & \xrightarrow{\;q'\;} & N' \end{array}$$

Si de plus, on fixe aussi le A-module N, on notera $\mathbf{C}(A,N)$ la sous-catégorie de $\mathbf{C}(A)$ dont les morphismes sont de la forme $(\mathrm{id}_A,\ g,\ \mathrm{id}_N) : (A,M,q,N) \to (A,M',q,N)$, i.e., g est une application A-linéaire rendant commutatif le diagramme:

$$\begin{array}{ccc} M & \xrightarrow{\;g\;} & M' \\ & {\scriptstyle q}\searrow \quad \swarrow{\scriptstyle q'} & \\ & N & \end{array}$$

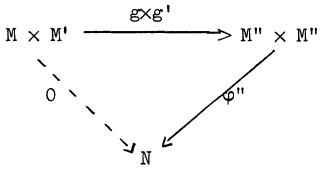
En vue de simplifier l'écriture, on notera $(f,g) = (f,g,\mathrm{id}_N)$, $g = (\mathrm{id}_A,\ g,\ \mathrm{id}_N)$ et $(M,q) = (A,M,q,N) \in \mathrm{Ob}\ \mathbf{C}(A,N)$ si aucune confusion n'est à craindre.

Soient (M,q) et (M',q') deux objets de $\mathbf{C}(A,N)$. On définit $(M,q) \perp (M',q') = (M \oplus M',\ q \oplus q')$, où $q \oplus q' : M \oplus M' \to N$ est l'application A-quadratique définie par $(x,x') \mapsto q(x) + q'(x')$. Les injections canoniques $j : M \hookrightarrow M \oplus M'$ et $j' : M' \hookrightarrow M \oplus M'$ nous fournissent des morphismes de $\mathbf{C}(A,N)$ rendant commutatif le diagramme .

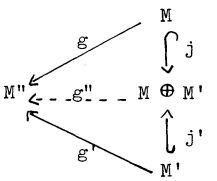
$$\begin{array}{ccc} M \times M' & \xrightarrow{\;j\times j'\;} & (M \oplus M') \times (M \oplus M') \\ & {\scriptstyle 0}\searrow \quad \swarrow{\scriptstyle \varphi''} & \\ & N & \end{array}$$

où φ'' est l'application A-bilinéaire symétrique associée à l'application A-quadratique $q \oplus q'$, i.e., $\varphi''((x,x'),\,(y,y')) = \varphi(x,y) + \varphi'(x',y')$, quels que soient

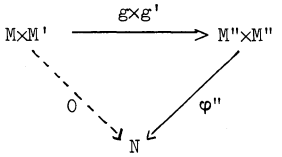
$x,y, \in M$ et $x',y' \in M'$ où φ (resp. φ') est l'application A-bilinéaire symétrique associée à q (resp. q'). De plus, quels que soient $g : (M,q) \to (M'',q'')$ et $g' : (M',q') \to (M'',q'')$, morphisme de $\mathbf{C}(A,N)$ rendant commutatif le diagramme



où φ'' est l'application A-bilinéaire symétrique associée à q'', il existe un <u>unique</u> morphisme $g'' : (M,q) \perp (M',q') \to (M'',q'')$ de $\mathbf{C}(A,N)$ rendant commutatifs les diagrammes :



On dira que $(M,q) \perp (M',q') = (M \oplus M', q \oplus q')$ est la <u>somme orthogonale</u> des objets (M,q) et (M',q'). Nous venons de démontrer que la somme orthogonale $(M,q) \perp (M',q')$ est un <u>objet initial</u>, donc l'objet initial (à isomorphisme près) de la catégorie suivante : les objets sont les couples de morphismes de $\mathbf{C}(A,N)$, $((M,q) \xrightarrow{g} (M'',q''), (M',q') \xrightarrow{g'} (M'',q''))$, rendant commutatif le diagramme



où φ'' est l'application A-bilinéaire symétrique associée à q'' et où les morphismes $h : (g,g') \to (g_1,g_1')$ sont les morphismes $h : (M'',q'') \to (M_1'',q_1'')$ de $\mathbf{C}(A,N)$ tels que $h \circ g = g_1$ et $h \circ g' = g_1'$.

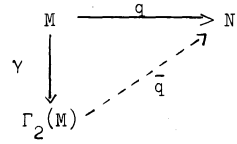
<u>Proposition</u> 1.1.1. <u>La somme orthogonale munit</u> $\mathbf{C}(A,N)$ <u>d'une structure naturelle de catérogie monoïdale à objet nul</u>.

En effet, définissons les foncteurs $\perp : \mathbf{C}(A,N) \times \mathbf{C}(A,N) \to \mathbf{C}(A,N)$, $((M,Q),(M',q')) \mapsto (M,q) \perp (M',q')$ et $T : \mathbf{C}(A,N) \times \mathbf{C}(A,N) \to \mathbf{C}(A,N) \times \mathbf{C}(A,N)$,

$((M,q),(M',q')) \mapsto ((M',q'),(M,q))$ (foncteur transposition). Il est trivial de vérifier qu'il existe des isomorphismes naturels $\perp \circ (\perp \times Id_{\mathcal{C}}) \approx \perp \circ (Id_{\mathcal{C}} \times \perp)$ et $\perp \circ T \approx \perp$. De plus, si l'on considère le foncteur $F : \mathcal{C}(A,N) \to \mathcal{C}(A,N) \times \mathcal{C}(A,N)$, $(M,q) \mapsto ((M,q),0)$, où 0 est l'objet nul de $\mathcal{C}(A,N)$, alors il existe un isomorphisme naturel $\perp \circ F \approx Id_{\mathcal{C}}$. La proposition est donc démontrée.

1.2. APPLICATIONS QUADRATIQUES ET PUISSANCES DIVISEES

Pour tout A-module M, désignons par $\Gamma_2(M)$ le sous-A-module des éléments homogènes de degré 2 de l'algèbre $\Gamma(M)$ des puissances divisées . Cet A-module est solution du problème universel suivant : il existe une application A-quadratique $\gamma : M \to \Gamma_2(M)$ telle que pour toute application A-quadratique $q : M \to N$, il existe une application A-linéaire et une seule $\bar{q} : \Gamma_2(M) \to N$ rendant commutatif le diagramme :

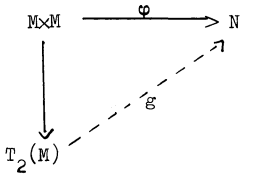


Pour le construire, on procède comme suit. Soient M un A-module, $T_2(M) = M \otimes_A M$, $(e_x)_{x \in M}$ la base canonique du A-module libre $A^{(M)}$ et R le sous-A-module de $A^{(M)} \times T_2(M)$ engendré par les éléments de la forme

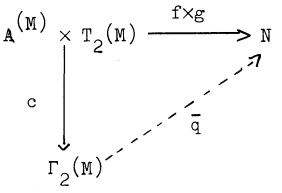
$$(e_{x+y} - e_x - e_y, - x \otimes y)$$
$$(e_{ax} - a^2 e_x, 0) ,$$

où $x,y \in M$ et $a \in A$. Notons $\Gamma_2(M) = A^{(M)} \times T_2(M)/R$ le A-module quotient et $\gamma : M \to A^{(M)} \times T_2(M) \xrightarrow{c} \Gamma_2(M)$ l'application (évidente) composée. Montrons que $\gamma : M \to \Gamma_2(M)$ est une application A-quadratique. En effet, $\gamma(ax) = c(e_{a\,x},0) = c((e_{a\,x} - a^2 e_x, 0) + (a^2 e_x, 0)) = a^2\,\gamma(x)$, quels que soient $a \in A$ et $x \in M$. De plus, $\gamma(x+y) - \gamma(x) - \gamma(y) = c(e_{x+y} - e_x - e_y, 0) = c((e_{x+y} - e_x - e_y, - x \otimes y) + (0, x \otimes y)) = c(0, x \otimes y)$, quels que soient $x,y \in M$. Ceci nous dit que l'application $M \times M \to \Gamma_2(M)$ définie par $(x,y) \mapsto \gamma(x+y) - \gamma(x) - \gamma(y)$ est A-bilinéaire.

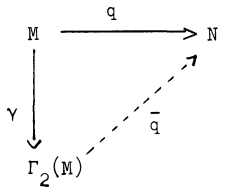
Soient maintenant $q : M \to N$ une application A-quadratique et $\varphi : M \times M \to N$ l'application A-bilinéaire symétrique associée à q. Il existe une unique application A-linéaire $g : T_2(M) \to N$ qui rend commutatif le diagramme



où la flèche verticale est canonique. D'autre part, il existe une application A-linéaire $f : A^{(M)} \to N$ donnée par $\sum_{x \in M} a_x e_x \mapsto \sum_{x \in M} a_x q(x)$, donc une unique application A-linéaire $f \times g : A^{(M)} \times T_2(M) \to N$ vérifiant $(f \times g)(e_x, y \otimes z) = q(x) + \varphi(y,z)$, quels que soient $x,y,z \in M$. Comme $(f \times g)(R) = 0$, il existe une unique application A-linéaire $\bar{q} : \Gamma_2(M) \to N$ telle que le diagramme



soit commutatif. Donc, le diagramme



est commutatif. Pour montrer l'unicité de $\bar{q}$ vérifiant $\bar{q} \circ \gamma = q$, il suffira de démontrer que l'ensemble $\{\gamma(x)\}_{x \in M}$ engendre $\Gamma_2(M)$ en tant que A-module et pour ce faire, il suffit de voir que quels que soient $x,y,z \in M$, on a $c(e_x, y \otimes z) = \gamma(x) + \gamma(y+z) - \gamma(y) - \gamma(z)$.

Une autre construction de $\Gamma_2(M)$ consiste à passer par les puissances symétriques. En effet, désignons par R le sous-A-module de $A^{(M)} \times S_2(M)$ engendré par les éléments de la forme

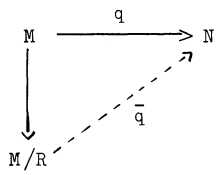
$$(e_{x+y} - e_x - e_y, - x \vee y)$$
$$(e_{a\,x} - a^2 e_x, 0),$$

où $x,y \in M$ et $a \in A$, par $\Gamma_2(M) = A^{(M)} \times S_2(M)/R$ le A-module quotient et $\gamma : M \to A^{(M)} \times S_2(M) \to \Gamma_2(M)$ l'application (évidente) composée où $S_2(M)$ désigne la deuxième puissance symétrique du A-module M et $\vee$ le produit symétrique. Il est clair que $\gamma : M \to \Gamma_2(M)$ est une application A-quadratique et que $\Gamma_2(M)$ est encore solution du problème universel posé au début.

1.3. EXTENSION DES SCALAIRES

Soient A un anneau, $q : M \to N$ une application A-quadratique, $\varphi : M \times N \to N$ l'application A-bilinéaire symétrique associée à q et R un sous-A-module de M. On dira que q est <u>constante modulo</u> R si la relation $x \equiv y \pmod{R}$, avec $x,y \in M$, entraîne $q(x) = q(y)$. Les assertions suivantes sont de vérification immédiate : (i) q est constante modulo R si et seulement si quels que soient $x \in M$ et $y \in R$ on a $q(x+y) = q(x)$; (ii) si q est constante modulo R, alors $q(y) = 0$ pour tout $y \in R$; (iii) si q est constante modulo R on a $\varphi(x,y) = 0$, quels que soient $x \in M$ et $y \in R$; (iv) si $\varphi(x,y) = 0$ quels que soient $x \in M$ et $y \in R$ et si l'homothétie définie par 2 dans N est injective, alors q est constante modulo R.

Soit donc $q : M \to N$ constante modulo R et définissons $\bar{q} : M/R \to N$ par $\bar{x} \mapsto q(x)$, où $\bar{x} \in M/R$ désigne la classe de $x \in M$ modulo R. Il est clair que $\bar{q}$ est bien définie et est une application A-quadratique ; $\bar{q}$ est l'<u>unique</u> application A-quadratique rendant commutatif le diagramme



où la flèche verticale est l'application A-linéaire canonique. Si $\bar{\varphi} : (M/R) \times (M/R) \to N$ est l'application A-bilinéaire symétrique associée à $\bar{q}$, alors $\bar{\varphi}(\bar{x},\bar{y}) = \varphi(x,y)$, quels que soient $\bar{x},\bar{y} \in M/R$.

Pour toute application A-quadratique $q : M \to N$, on définit le <u>noyau</u> de q comme étant le sous-A-module de M défini par $\mathrm{Ker}(q) = \{x \mid x \in M,\ q(x) = 0$ et $\varphi(x,y) = 0,\ \forall\, y \in M\}$, où φ est l'application A-bilinéaire symétrique associée à q. Pour chaque $y \in M$, considérons l'application A-linéaire $\varphi_y : M \to N$ définie par $x \mapsto \varphi(x,y)$. Il est clair que $\mathrm{Ker}(q) = \{x \mid x \in M,\ q(x) = 0\} \cap \bigcap_{y \in M} \mathrm{Ker}(\varphi_y)$.

Si l'homothétie définie par 2 dans N est injective, l'équation $2q(x) = \varphi_x(x) = 0$ entraîne $q(x) = 0$, i.e., $\mathrm{Ker}(q) = \bigcap_{y \in M} \mathrm{Ker}(\varphi_y)$.

Les assertions suivantes sont encore faciles à établir : (v) $q : M \to N$ est constante modulo R si et seulement si $R \subset \mathrm{Ker}(q)$; (vi) si $q : M \to N$ est constante modulo R et si $\bar{q} : M/R \to N$ est l'application A-quadratique obtenue par passage au quotient, alors $\mathrm{Ker}(\bar{q}) = \mathrm{Ker}(q)/R$.

Lemme 1.3.1. *Soient $q : M \to N$ une application A-quadratique et $\varphi : M \times N \to N$ l'application A-bilinéaire symétrique associée à q. Pour toute famille $(x_i)_{i \in I}$ d'éléments de M et pour toute famille $(a_i)_{i \in I}$ à support fini d'éléments de A, on a $q(\sum_{i \in I} a_i x_i) = \sum_{i \in I} a_i^2 q(x_i) + \sum_{\{i,j\}} a_i a_j \varphi(x_i, x_j)$, où $\sum_{\{i,j\}}$ désigne la somme étendue aux sous-ensembles $\{i,j\}$ de I à deux éléments.*

On peut supposer, dans la démonstration, que I est un ensemble fini et, par récurrence sur le nombre d'éléments de I, que I a deux éléments. Mais dans ce cas, on a trivialement $q(a_1 x_1 + a_2 x_2) = a_1^2 q(x_1) + a_2^2 q(x_2) + a_1 a_2 \varphi(x_1, x_2)$.

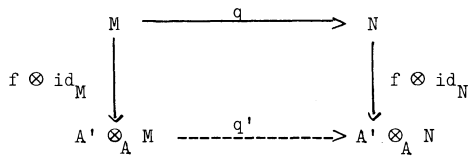
Lemme 1.3.2. *Soient L un A-module libre, $(e_i)_{i \in I}$ une base de L sur A et N un A-module. Pour toute famille $(y_{ij})_{(i,j) \in I \times I}$ d'éléments de N telle que $y_{ij} = y_{ji}$ quels que soient $i, j \in I$, il existe une unique application A-quadratique $q : L \to N$ vérifiant les conditions $q(e_i) = y_{ii}$ pour tout $i \in I$ et $\varphi(e_i, e_j) = y_{ij}$ pour tout $(i,j) \in I \times I$, où $\varphi : L \times L \to N$ est l'application A-bilinéaire symétrique associée à q.*

En effet, pour tout $x = \sum_{i \in I} a_i e_i \in L$ on a $q(x) = \sum_{i \in I} a_i^2 q(e_i) + \sum_{\{i,j\}} a_i a_j \varphi(e_i, e_j) = \sum_{(i,j) \in I \times I} a_i a_j y_{ij}$, d'où l'unicité de q.

Ence qui concerne l'existence de q, on commence par munir I d'une structure d'ensemble totalement ordonné. Pour toute famille (y_{ij}) d'éléments de N telle que $y_{ij} = y_{ji}$ pour tout $(i,j) \in I \times I$, il existe une famille (y'_{ij}) d'éléments de N vérifiant les conditions $y'_{ii} = y_{ii}$ pour tout $i \in I$ et $y'_{ij} + y'_{ji} = y_{ij}$ pour tout $(i,j) \in I \times I$, $i \neq j$. En effet, il suffit de choisir $y'_{ij} = y_{ij}$ si $i < j$, $y'_{ij} = 0$ si $i > j$ et $y'_{ii} = y_{ii}$.

Considérons maintenant l'application A-bilinéaire $\psi : L \times L \to N$ définie par $(e_i, e_j) \mapsto y'_{ij}$ et soit $q : L \to N$ l'application A-quadratique définie par $x \mapsto \psi(x,x)$. Il est évident que $q(e_i) = \psi(e_i, e_i) = y'_{ii} = y_{ii}$ pour tout $i \in I$ et que $\varphi(e_i, e_j) = q(e_i + e_j) - q(e_i) - q(e_j) = \psi(e_i, e_j) + \psi(e_j, e_i) = y'_{ij} + y'_{ji} = y_{ij}$, pour tout $(i,j) \in I \times I$, $i \neq j$.

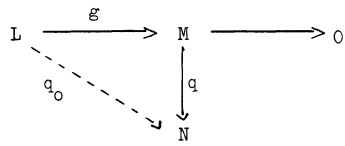
Théorème 1.3.3. *Soient $f : A \to A'$ un morphisme de Ann et $q : M \to N$ une application A-quadratique. Il existe une unique application A'-quadratique $q' : A' \otimes_A M \to A' \otimes_A N$ rendant commutatif le diagramme :*



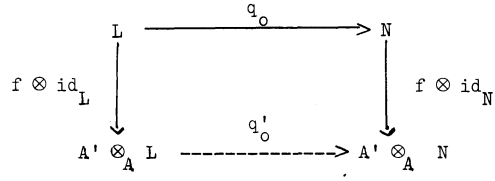
L'unicité de q' est triviale. En ce qui concerne l'existence, la démonstration sera faite en deux étapes, où l'on examinera d'abord le cas libre.

Supposons donc que M soit un A-module libre de base $(e_i)_{i\in I}$ et posons $y_{ii} = q(e_i)$ pour tout $i \in I$ et $y_{ij} = \varphi(e_i,e_j)$ pour tout $(i,j) \in I\times I$, $i \neq j$, où φ est l'application A-bilinéaire symétrique associée à q. D'après le lemme 1.3.2., il existe une unique application A'-quadratique $q' : A' \otimes_A M \to A' \otimes_A N$ vérifiant les conditions $q'(1' \otimes e_i) = 1' \otimes y_{ii}$ pour tout $i \in I$ et $\varphi'(1' \otimes e_i, 1' \otimes e_j) = 1' \otimes y_{ij}$ pour tout $(i,j) \in I\times I$, $i \neq j$, où φ' est l'application A'-bilinéaire symétrique associée à q'. Si $x = \sum_{i\in I} a_i e_i \in M$, on a $1' \otimes x = \sum_{i\in I} f(a_i)\,(1' \otimes e_i)$, donc $q'(1' \otimes x) = \sum_{(i,j)\in I\times I} f(a_i) f(a_j)(1' \otimes y_{ij}) = 1' \otimes \sum_{(i,j)\in I\times I} a_i a_j y_{ij} = 1' \otimes q(x)$, i.e., $q'(1' \otimes x) = 1' \otimes q(x)$ pour tout $x \in M$.

Le A-module M est maintenant quelconque et écrivons-le comme quotient d'un A-module libre L :

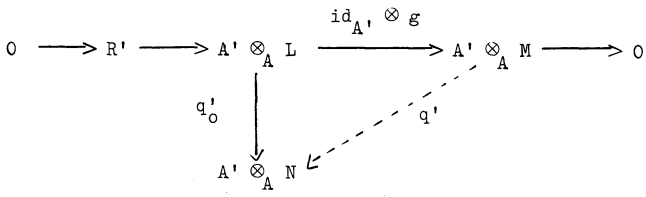


D'après le <u>cas libre</u>, il existe une unique application A'-quadratique $q'_o : A' \otimes_A L \to A' \otimes_A N$ rendant commutatif le diagramme :



Si maintenant on note $R' = \mathrm{Ker}\,(A' \otimes_A L \xrightarrow{1'\otimes g} A' \otimes_A M)$, il est clair que q'_o est constante modulo R', ou encore, $R' \subset \mathrm{Ker}\,(q'_o)$. Par passage au quotient, il existe

une unique application A'-quadratique $q' : A' \otimes_A M \to A' \otimes_A N$ rendant commutatif le diagramme :



Il s'ensuit que pour tout $x \in M$, $q'(1' \otimes x) = 1' \otimes q(x)$.

1.4. FORMES ET APPLICATIONS QUADRATIQUES NON DEGENEREES

Soient $q : M \to N$ une application A-quadratique, $\varphi : M \times N \to N$ l'application A-bilinéaire symétrique associée à q et $d_\varphi : M \to \mathrm{Hom}_A(M,N)$ l'application A-linéaire définie par $x \mapsto (y \mapsto \varphi(x,y))$. On dira que l'application A-quadratique $q : M \to N$ est <u>non dégénérée</u> si l'application A-linéaire $d_\varphi : M \to \mathrm{Hom}_A(M,N)$ est injective et que q est <u>strictement non dégénérée</u> si $d_\varphi : M \xrightarrow{\sim} \mathrm{Hom}_A(M,N)$ est un isomorphisme de A-modules.

Il est clair que toute application quadratique strictement non dégénérée est non dégénérée, mais la réciproque est, en général, fausse. En effet, il suffit de considérer le cas où A est un corps, M un A-espace vectoriel de dimension infinie et $q : M \to A$ une forme quadratique non dégénérée. L'application $d_\varphi : M \to M^*$ est injective mais, toujours, non surjective car M^* est beaucoup "plus gros" que M.

Une autre remarque est la suivante : si M est un A-module projectif de type fini et fidèle et $q : M \to N$ une application A-quadratique strictement non dégénérée, en tout point $\mathfrak{p} \in \mathrm{Spec}(A)$, on a $r_N(\mathfrak{p}) = 1$, i.e., N est nécessairement de rang 1. Si l'on impose tout simplement que M est projectif de type fini (non nécessairement fidèle), alors on a $r_N(\mathfrak{p}) \leq 1$ pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$.

<u>Proposition</u> 1.4.1. <u>Soit</u> $q : M \to N$ <u>une application A-quadratique, où</u> M <u>est un A-module de présentation finie. Les conditions suivantes sont équivalentes</u> : (i) <u>l'application A-quadratique</u> $q : M \to N$ <u>est non dégénérée (resp. strictement non dégénérée)</u> ; (ii) <u>pour tout idéal premier</u> $\mathfrak{p}$ <u>de</u> A, <u>l'application</u> $A_\mathfrak{p}$<u>-quadratique</u> $q_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ <u>est non dégénérée (resp. strictement non dégénérée)</u> ; (iii) <u>pour tout idéal maximal</u> $\mathfrak{m}$ <u>de</u> A, <u>l'application</u> $A_\mathfrak{m}$<u>-quadratique</u> $q_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ <u>est non dégénérée (resp. strictement non dégénérée)</u>.

On note $\varphi : M \times M \to N$ l'application A-bilinéaire symétrique associée à q et $d_\varphi : M \to \mathrm{Hom}_A(M,N)$ l'application A-linéaire définie par $x \mapsto (y \mapsto \varphi(x,y))$.

La suite exacte de A-modules $0 \to \mathrm{Ker}\,(d_\varphi) \to M \xrightarrow{d_\varphi} \mathrm{Hom}_A(M,N) \to \mathrm{Coker}\,(d_\varphi) \to$ $\to 0$ et le fait que M soit de présentation finie, nous donnent la suite exacte de $A_{\mathfrak{m}}$-modules $0 \to \mathrm{Ker}(d_\varphi)_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{d_{\varphi_{\mathfrak{m}}}} \mathrm{Hom}_{A_{\mathfrak{m}}}(M_{\mathfrak{m}},N_{\mathfrak{m}}) \to \mathrm{Coker}(d_\varphi)_{\mathfrak{m}} \to 0$, i.e., $\mathrm{Ker}(d_\varphi)_{\mathfrak{m}} = \mathrm{Ker}(d_{\varphi_{\mathfrak{m}}})$ et $\mathrm{Coker}(d_\varphi)_{\mathfrak{m}} = \mathrm{Coker}(d_{\varphi_{\mathfrak{m}}})$. Ceci étant vrai, quel que soit $\mathfrak{m}$ idéal maximal de A, on en déduit que (iii) $\Rightarrow$ (i). L'implication (ii) $\Rightarrow$ (iii) est triviale et (i) $\Rightarrow$ (ii) est facile à établir.

Proposition 1.4.2. Soit $q : P \to N$ une application A-quadratique, où P est un A-module projectif de type fini et $\mathrm{Hom}_A(P,N)$ est plat. Les conditions suivantes sont équivalentes : (i) l'application A-quadratique $q : P \to N$ est strictement non dégénérée ; (ii) pour tout idéal premier $\mathfrak{p}$ de A, l'application $(A/\mathfrak{p})$-quadratique $q_{/\mathfrak{p}} : P/\mathfrak{p}P \to N/\mathfrak{p}N$ est strictement non dégénérée ; (iii) pour tout idéal maximal $\mathfrak{m}$ de A, l'application $(A/\mathfrak{m})$-quadratique $q_{/\mathfrak{m}} : P/\mathfrak{m}P \to N/\mathfrak{m}N$ est strictement non dégénérée.

Il suffit de remarquer que, comme P est projectif de type fini, pour tout idéal premier $\mathfrak{p}$ de A, il existe un isomorphisme de $(A/\mathfrak{p})$-modules $(A/\mathfrak{p}) \otimes_A \mathrm{Hom}_A(P,N) \approx \mathrm{Hom}_{A/\mathfrak{p}}(P/\mathfrak{p}P,\ N/\mathfrak{p}N)$.

On remarque que si P est projectif de type fini et fidèle et si $\mathrm{Hom}_A(P,N)$ est plat, alors N est lui-même plat. En effet, comme P est projectif de type fini et fidèle, il existe un A-module projectif de type fini Q tel que $P \otimes_A Q = L$ soit libre (cf. [57]). Comme $\mathrm{Hom}_A(P,N) \approx P^* \otimes_A N$ est plat, il en est de même de $Q^* \otimes_A P^* \otimes_A N$, donc si $L = A^{(I)}$, alors $N^{(I)}$ est un A-module plat et, par suite, N est lui-même plat. Ainsi, dans la proposition 1.4.2., si l'on suppose P fidèle, il suffira de supposer que N soit plat.

1.5. PRODUIT TENSORIEL D'APPLICATIONS QUADRATIQUES

Théorème 1.5.1. Soient $q_i : M_i \to N_i$ $(i = 1,2)$ deux application A-quadratiques et φ_1 (resp. φ_2) l'application A-bilinéaire symétrique associée à q_1 (resp. q_2). Il existe une unique application A-quadratique $q : M_1 \otimes_A M_2 \to N_1 \otimes_A N_2$ vérifiant les conditions $q(x_1 \otimes x_2) = 2\, q_1(x_1) \otimes q_2(x_2)$ et $\varphi(x_1 \otimes x_2,\ y_1 \otimes y_2) = \varphi_1(x_1,y_1) \otimes \varphi_2(x_2,y_2)$, quels que soient $x_1,y_1 \in M_1$ et $x_2,y_2 \in M_2$, où φ est l'application A-bilinéaire symétrique associée à q.

L'unicité d'une telle application quadratique vérifiant les conditions

imposées, est triviale. En ce qui concerne l'existence, on commence par étudier le cas où M_1 et M_2 sont libres et après, on passe au cas général.

Supposons donc que M_1 et M_2 soient des A-modules libres et soient $(e_i)_{i\in I}$ une base de M_1 et $(f_j)_{j\in J}$ une base de M_2. On définit une famille $(y_{(i,j),(k,\ell)})$ d'éléments de $N_1 \otimes_A N_2$ de la façon suivante : $y_{(i,j),(k,\ell)} = \varphi_1(e_i,e_k) \otimes \varphi_2(f_j,f_\ell)$ si $(i,j) \neq (k,\ell)$ et $y_{(i,j),(k,\ell)} = 2\, q_1(e_i) \otimes q_2(f_j)$ si $(i,j) = (k,\ell)$, où $(i,j) \in I\times J$ et $(k,\ell) \in I\times J$. D'après le lemme 1.3.2., il existe une unique application A-quadratique $q : M_1 \otimes_A M_2 \to N_1 \otimes_A N_2$ vérifiant les conditions $q(e_i \otimes f_j) = y_{(i,j),(i,j)}$ pour tout $(i,j) \in I\times J$ et $\varphi(e_i \otimes f_j , e_k \otimes f_\ell) = y_{(i,j),(k,\ell)}$ quels que soient $(i,j),(k,\ell) \in I\times J$, $(i,j) \neq (k,\ell)$, où φ est l'application A-bilinéaire symétrique associée à q. Il est facile de vérifier que l'application A-quadratique q satisfait les conditions du théorème.

Supposons maintenant que M_1 et M_2 soient quelconques et écrivons les comme quotients de modules libres L_1 et L_2 respectivement :

$$0 \to R_1 \to L_1 \xrightarrow{g_1} M_1 \to 0 \quad , \quad 0 \to R_2 \to L_2 \xrightarrow{g_2} M_2 \to 0$$

avec $q_1' : L_1 \to N_1$, $q_1 : M_1 \to N_1$ et $q_2' : L_2 \to N_2$, $q_2 : M_2 \to N_2$.

D'après le cas libre, il existe une unique application A-quadratique $q' : L_1 \otimes_A L_2 \to N_1 \otimes_A N_2$ vérifiant les conditions du théorème. Or, si l'on désigne par $R = \mathrm{Im}(R_1 \otimes_A L_2 + L_1 \otimes_A R_2 \to L_1 \otimes_A L_2)$, il est clair que $R \subset \mathrm{Ker}(q')$, donc par passage au quotient, il existe une unique application A-quadratique $q : M_1 \otimes_A M_2 \to N_1 \otimes_A N_2$ rendant commutatif le diagramme :

$$\begin{array}{ccccccccc} 0 & \to & R & \to & L_1 \otimes_A L_2 & \xrightarrow{g_1 \otimes g_2} & M_1 \otimes M_2 & \to & 0 \\ & & & & \downarrow{\scriptstyle q'} & \swarrow{\scriptstyle q} & & & \\ & & & & N_1 \otimes_A N_2 & & & & \end{array}$$

Ceci achève la démonstration du théorème.

On notera $q = q_1 \otimes q_2$ et on dira que q est le produit tensoriel

des applications A-quadratiques q_1 et q_2. De plus, on posera $(A,M_1,q_1,N_1) \otimes_A (A, M_2,q_2,N_2) = (A,M_1 \otimes_A M_2, q_1 \otimes q_2, N_1 \otimes N_2)$.

Les démonstrations des propositions 1.5.2. et 1.5.3. sont triviales :

Proposition 1.5.2. Quels que soient (A,M,q,N), (A,M',q',N') et (A,M'',q'',N'') objets de $C(A)$ on a des isomorphismes $(A,M,q,N) \otimes_A (A,M',q',N') \approx (A,M',q',N') \otimes_A (A,M,q,N)$ et $((A,M,q,N) \otimes_A (A,M',q',N')) \otimes_A (A,M'',q'',N'') \approx (A,M,q,N) \otimes_A ((A,M',q',N') \otimes_A (A,M'',q'',N''))$.

Supposons que 2 soit inversible dans l'anneau A et considérons l'application A-quadratique $i : A \to A$ définie par $a \mapsto \frac{1}{2} a^2$.

Proposition 1.5.3. Pour tout objet (A,M,q,N) de C tel que 2 soit inversible dans A, il existe des isomorphismes $(A,M,q,N) \perp_A (A,A,i,A) \approx (A,M,q,N)$ et $(A,A,i,A) \otimes_A (A,M,q,N) \approx (A,M,q,N)$.

Proposition 1.5.4. Soient $q_i : P_i \to N_i$ $(i = 1,2)$ deux applications A-quadratiques où P_1 et P_2 sont des A-modules projectifs de type fini. Si q_1 et q_2 sont non dégénérées (resp. strictement non dégénérées), alors $q_1 \otimes q_2$ est non dégénérée (resp. strictement non dégénérée).

En effet, désignons par $q = q_1 \otimes q_2$ et par φ (resp. φ_1, φ_2) l'application A-bilinéaire symétrique associée à q (resp. q_1, q_2). A isomorphisme près, on a $d_\varphi = d_{\varphi_1} \otimes d_{\varphi_2}$, d'où le résultat.

Proposition 1.5.5. Quels que soient (A,M,q,N), (A,M_1,q_1,N') et (A,M_2,q_2,N') objets de $C(A)$, on a un isomorphisme $(A,M,q,N) \otimes_A ((A,M_1,q_1,N') \perp (A,M_2,q_2,N')) \approx (A,M,q,N) \otimes_A (A,M_1,q_1,N') \perp (A,M,q,N) \otimes_A (A,M_2,q_2,N')$.

La démonstration (facile) est laissée au lecteur.

On appelle A-module bilinéaire et on note (M,φ) un couple formé d'un A-module M et d'une forme A-bilinéaire symétrique $\varphi : M \times M \to A$. Les morphismes de A-modules bilinéaires se définissent aisément et on peut, comme pour les formes quadratiques définir la somme orthogonale de deux modules bilinéaires. On peut aussi supposer, plus généralement qu'on a des modules M munis d'une application A-bilinéaire symétrique $\varphi : M \times M \to N$ où N est un A-module (qui n'est pas nécessairement l'anneau A) ; de tels objets sont notés (M,φ,N).

Définissons le produit tensoriel de deux objets (M,φ,N) et (M',φ',N'). Soit, en effet, $u : M \times M' \times M \times M' \to N \otimes_A N'$ l'application qui à (x,x',y,y') associe l'élément $\varphi(x,y) \otimes \varphi'(x',y')$. Cette application est A-linéaire par rapport à chaque variable x,x',y et y' et induit donc une application

$(M \otimes_A M') \times (M \otimes_A M') \to N \otimes_A N'$, qu'on notera $\varphi \otimes \varphi'$ et qui vérifie $(\varphi \otimes \varphi')(x \otimes x', y \otimes y') = \varphi(x,y) \otimes \varphi(x',y')$; c'est une application A-bilinéaire symétrique. Si $N = N' = A$, $N \otimes_A N' \approx A$ et $\varphi \otimes \varphi'$ est une forme A-bilinéaire symétrique sur le A-module $M \otimes_A M'$.

Le produit tensoriel de modules bilinéaires possède les propriétés d'associativité et de commutativité à isomorphisme près, ainsi que de double distributivité par rapport à la somme orthogonale.

Nous allons maintenant voir les relations entre produit tensoriel d'applications bilinéaires et d'applications quadratiques. Un corollaire immédiat de 1.5.1. est le suivant :

Corollaire 1.5.6. Soient (M,q,N) et (M',q',N') deux objets de $\mathcal{C}(A)$. L'application A-bilinéaire symétrique associée à leur produit tensoriel est le produit tensoriel des applications A-bilinéaires associées à (M,q,N) et à (M',q',N').

Soient maintenant (M,q,N) un objet de $\mathcal{C}(A)$ et (M',φ',N') un module A-bilinéaire ; nous allons montrer qu'ils possèdent un produit tensoriel qui est un objet de $\mathcal{C}(A)$. On a, en effet, le théorème suivant :

Théorème 1.5.7. Il existe une application quadratique unique $\bar{q} : M \otimes_A M' \to N \otimes_A N'$ dont l'application A-bilinéaire symétrique associée $\bar{\varphi}$ vérifie les conditions suivantes : $\bar{q}(x \otimes x') = q(x) \otimes \varphi'(x',x')$ et $\bar{\varphi}(x \otimes x', y \otimes y') = \varphi(x,y) \otimes \varphi'(x',y')$, quels que soient x,y dans M et x',y' dans M'.

La démonstration se fait comme pour 1.5.1. ; l'unicité est claire et l'existence se démontre en supposant d'abord les modules libres puis en passant au cas général.

Corollaire 1.5.8. Soient (M,q,N) et (M',q',N') deux objets de $\mathcal{C}(A)$ et notons φ et φ' les modules A-bilinéaires associés. Le produit tensoriel de (M,q,N) et de (M',q',N') est aussi le produit tensoriel de (M,q,N) et de φ' (resp. de φ et de (M',q',N')).

Il suffit de comparer le théorème précédent et le théorème 1.5.1. pour obtenir le corollaire.

1.6. PUISSANCES EXTERIEURES ET DETERMINANT

Soit f une forme A-bilinéaire sur le A-module M. Les puissances extérieures de f se définissent classiquement ainsi : si n est un entier naturel et $x_1,\dots,x_n, y_1,\dots,y_n$ sont $2n$ éléments de M, nous posons $\Delta_f(x_1,\dots,x_n ; y_1,\dots,y_n) = \det(f(x_i,y_j))_{1\le i,\, j\le n}$. C'est une fonction multilinéaire et alternée par rapport aux x_i d'une part, aux y_j d'autre part ; Δ_f induit donc une forme A-bilinéaire sur $\Lambda^n M$, notée $\Lambda^n f$, telle que

$\Lambda^n f(x_1 \wedge \ldots \wedge x_n, y_1 \wedge \ldots \wedge y_n) = \Delta_f(x_1,\ldots,x_n ; y_1,\ldots,y_n)$. Si f est symétrique, $\Lambda^n f$ l'est aussi ; si f est alternée (i.e., $f(x,x) = 0$ pour tout x dans M), $\Lambda^n f$ n'est pas toujours alternée : si n est pair, $\Lambda^n f$ est symétrique et si n est impair, $\Lambda^n f$ est alternée car $\Lambda^n f(x_1 \wedge \ldots \wedge x_n, x_1 \wedge \ldots \wedge x_n)$, déterminant d'une matrice alternée d'ordre impair, est nul.

Supposons f symétrique ; l'application A-linéaire $d_{\Lambda^n f}$ associée à $\Lambda^n f$, qui va de $\Lambda^n M$ dans $\mathrm{Hom}_A(\Lambda^n M, A)$ est l'application composée

$\Lambda^n M \xrightarrow{d_{\Lambda^n f}} \Lambda^n(\mathrm{Hom}_A(M,A)) \xrightarrow{t_n} \mathrm{Hom}_A(\Lambda^n M, A)$, où t_n est l'application naturelle $f_1 \wedge \ldots \wedge f_n \mapsto (x_1 \wedge \ldots \wedge x_n \mapsto \det (f_i(x_j))_{1 \le i,\, j \le n})$. Si M est projectif de type fini, t_n est un isomorphisme de sorte que, quand $d_f : M \to \mathrm{Hom}_A(M,A)$ est un isomorphisme de A-modules, il en est de même de $d_{\Lambda^n f}$.

Supposons maintenant que 2 est inversible dans A : il y a bijection entre formes A-bilinéaires symétriques et formes quadratiques donné par $f \mapsto (q_f : x \mapsto f(x,x))$ et $q \mapsto \varphi_q$ comme il a été déjà vu plus haut. On peut donc définir de façon naturelle les puissances extérieures d'une forme quadratique : $\Lambda^n q$ est la forme quadratique définie sur le A-module $\Lambda^n M$ qui est associée à la forme A-bilinéaire symétrique $\Lambda^n(\varphi_q)$ et par construction $d_{\Lambda^n q} \approx \Lambda^n(d_q)$. Si q est strictement non dégénérée, les puissances extérieures de q sont strictement non dégénérées.

Si 2 n'est pas inversible, il n'est pas toujours possible de définir raisonnablement les puissances extérieures d'une forme quadratique. Ainsi, si l'anneau A est de caractéristique 2, une A-forme bilinéaire symétrique ne provient d'une forme quadratique que si elle est alternée. C'est donc impossible en général pour $\Lambda^n(\varphi_q)$, si n est pair. Cela suggère cependant de chercher quelque chose si n est impair. Pour cela nous utilisons une remarque due à A. GROTHENDIECK, à savoir:

Lemme 1.6.1. Soient $A_n = \mathbb{Z}[X_{ij}]$, $1 \le i \le j \le n$ et Δ_n le déterminant

$$\Delta_n = \begin{vmatrix} 2X_{11} & X_{12} & \cdots & X_{1n} \\ X_{12} & 2X_{22} & \cdots & X_{2n} \\ X_{13} & X_{23} & \cdots & X_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ X_{1n-1} & X_{2n-1} & \cdots & X_{n-1n} \\ X_{1n} & X_{2n} & \cdots & 2X_{nn} \end{vmatrix}$$

. Si n est impair, il existe un élément P_n de A_n tel que $\Delta_n = 2P_n$.

En réduisant modulo 2, on trouve que Δ_n est le déterminant d'une matrice alternée d'ordre impair, donc 0.

Supposant n impair, nous allons construire la puissance extérieure $n^{\text{ième}}$ d'une forme quadratique sur un A-module quelconque.

Théorème 1.6.2. *Soient* (M,q) *un objet de* $\mathcal{C}(A,A)$ *et* n *un entier impair. Il existe sur* $\Lambda^n M$ *une forme quadratique et une seule, qu'on notera* $\Lambda^n q$, *telle que :* (i) $\Lambda^n q(x_1 \wedge \ldots \wedge x_n) = P_n(x_{ij})$, $1 \leq i \leq j \leq n$, *où* $x_{ii} = q(x_i)$ *et* $x_{ij} = \varphi(x_i,x_j)$, *si* $i \neq j$; (ii) $\varphi_{\Lambda^n q} = t_n \circ \Lambda^n \varphi_q$.

L'unicité de $\Lambda^n q$ est claire, puisque les conditions (i) et (ii) permettent de calculer la valeur de $\Lambda^n q$ sur tout élément de $\Lambda^n M$.

Pour démontrer l'existence de $\Lambda^n q$, considérons la suite exacte de A-modules, $0 \to R \to A^{(M)} \to M \to 0$ où l'on note $(e_x)_{x \in M}$, la base canonique de $A^{(M)}$, supposée totalement ordonnée. Définissons sur $\Lambda^n A^{(M)}$ une forme quadratique $\bar{q}$ par $\bar{q}(e_{x_1} \wedge \ldots \wedge e_{x_n}) = P_n(q(x_i), \varphi(x_i,x_j))_{i<j}$ et $\bar{\varphi}(e_{x_1} \wedge \ldots \wedge e_{x_n}, e_{y_1} \wedge \ldots \wedge e_{y_n}) = \det(\varphi(x_i,y_j))_{1 \leq i,j \leq n}$, où $x_1 < \ldots < x_n$, $y_1 < \ldots < y_n$. Dans la suite exacte $0 \to R' \to \Lambda^n(A^{(M)}) \to \Lambda^n M \to 0$, le sous-module R' est engendré par les éléments de la forme $(e_{ax} - ae_x) \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}$ et $(e_{x+y} - e_x - e_y) \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}$, où $x,y,x_2,\ldots,x_n$ sont dans M et a dans A. Il est facile de vérifier que R' est contenu dans le noyau de $\bar{q}$ car, par exemple, $\bar{q}((e_{ax} - ae_x) \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) = \bar{q}(e_{ax} \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) + a^2\, \bar{q}(e_x \wedge \ldots \wedge e_{x_n}) - a\, \bar{\varphi}(e_{ax} \wedge \ldots \wedge e_{x_n}, e_x \wedge \ldots \wedge e_{x_n}) = 0$. D'autre part, les éléments de R' sont orthogonaux à tous les éléments de $A^{(M)}$ et il ne reste plus qu'à calculer $\bar{q}((e_{x+y} - e_x - e_y) \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) = \bar{q}(e_{x+y} \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) + \bar{q}(e_x \wedge \ldots \wedge e_{x_n}) + \bar{q}(e_y \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) - \bar{\varphi}(e_{x+y} \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}, e_x \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) - \bar{\varphi}(e_{x+y} \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}, e_y \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) + \bar{\varphi}(e_x \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}, e_y \wedge e_{x_2} \wedge \ldots \wedge e_{x_n})$, si bien qu'il s'agit de montrer que $\bar{q}(e_{x+y} \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) = \bar{q}(e_x \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) + \bar{q}(e_y \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}) + \bar{\varphi}(e_x \wedge e_{x_2} \wedge \ldots \wedge e_{x_n}, e_y \wedge e_{x_2} \wedge \ldots \wedge e_{x_n})$, résultat qui exprime le caractère quadratique de l'application $x \mapsto \bar{q}(e_x \wedge e_{x_2} \wedge \ldots \wedge e_{x_n})$. Comme $\operatorname{Ker} \bar{q} \supset R'$, la forme quadratique $\bar{q}$ passe

au quotient en une forme quadratique $q' : \Lambda^n M \to A$ qui vérifie, par construction, les conditions (i) et (ii).

Supposons maintenant donnés deux modules M_1 et M_2 munis de formes A-bilinéaires symétriques, notées respectivement f_1 et f_2. Alors leur somme orthogonale $f = f_1 \perp f_2$ sur $M_1 \oplus M_2$ a, pour $n^{\text{ième}}$ puissance extérieure, $\Lambda^n f \approx \bigperp_{p_1+p_2=n} \Lambda^{p_1} f_1 \otimes \Lambda^{p_2} f_2$. C'est une conséquence immédiate de la décomposition $\Lambda^n (M_1 \oplus M_2) \approx \bigoplus_{p_1+p_2=n} \Lambda^{p_1} M_1 \otimes \Lambda^{p_2} M_2$, où $\otimes = \otimes_A$.

Il existe une formule analogue pour les formes quadratiques, à savoir : $\Lambda^{2h+1}(q \perp q') \approx (\bigperp_{r=0}^{h} \Lambda^{2r} \varphi_q \otimes \Lambda^{2(h-r)+1} q') \perp (\bigperp_{s=0}^{h} \Lambda^{2(h-s)+1} q \otimes \Lambda^{2s} \varphi_{q'})$. La démonstration se fait de la façon suivante : il faut tout d'abord vérifier l'orthogonalité vis-à-vis de la forme quadratique $\Lambda^{2h+1}(q \perp q')$ des couples de sous-modules $\Lambda^{p_1} M_1 \otimes \Lambda^{p_2} M_2$ et $\Lambda^{q_1} M_1 \otimes \Lambda^{q_2} M_2$ où $p_1 + p_2 = q_1 + q_2 = 2h+1$ et $p_1 \neq q_1$ ce qui est clair car ceci est dû aux formes A-bilinéaires symétriques. Ensuite on calcule la restriction de $\Lambda^{2h+1}(q \perp q')$ à $\Lambda^{2r} M_1 \otimes \Lambda^{2(h-r)+1} M_2$, par exemple, et cela se fait sans difficultés à l'aide des formules (i) et (ii) du théorème précédent. Notons que si 2 est inversible dans A, la formule signalée s'écrit tout simplement $\Lambda^n(q \perp q') \approx \bigperp_{r=0}^{n} (\Lambda^r q \otimes \Lambda^{n-r} q')$, du fait de la formule correspondante pour les formes A-bilinéaires symétriques.

On peut faire des constructions analogues pour les applications quadratiques (ou A-bilinéaires symétriques), quand le A-module des valeurs N est projectif de type fini et de rang 1 ; la puissance extérieure $n^{\text{ième}}$ est alors à valeurs dans $\overset{n}{\otimes} N$. Notons aussi que si q est strictement non dégénérée, il en est de même pour $\Lambda^n q$ telle qu'elle a été définie par le théorème 1.6.2.

En théorie des formes bilinéaires symétriques entières définies, on distingue les formes de type I et les formes de type II, ces dernières provenant de formes quadratiques strictement non dégénérées. Le théorème précédent dit que si f est une forme bilinéaire symétrique entière de type II, alors $\Lambda^n f$ est de type II, si n est impair.

On va maintenant définir le déterminant d'un A-module quadratique (objet de $C(A,A)$). Supposons d'abord que P soit le A-module libre A^n et soit $q : A^n \to A$ la forme quadratique définie sur A^n. Si $(e_i)_{1 \leq i \leq n}$, est une base de A^n et $(e'_i)_{1 \leq i \leq n}$ la base duale, la matrice de l'application d_q est la matrice $(\varphi(e_i, e_j)_{1 \leq i, j \leq n}$ dont le déterminant Δ est inversible dans A car d_q est

un isomorphisme. Si $(f_i)_{1\leq i\leq n}$ est une autre base de A^n, le déterminant $\Delta' = \det(\varphi(f_i,f_j))_{1\leq i,\ j\leq n}$ est égal à Δ au carré d'un élément inversible de A près et on appelle <u>déterminant</u> de q la classe de Δ dans $U(A)/U^2(A)$.

Si q et q' sont deux formes quadratiques strictement non dégénérées sur des modules libres A^n et $A^{n'}$, le déterminant de $q \perp q'$ n'est autre que le produit dans le groupe $U(A)/U^2(A)$ des déterminants de q et de q' précédemment définies, car la matrice associée à $q \perp q'$ dans une base réunion d'une base de A^n et d'une base de $A^{n'}$ est de la forme $\begin{pmatrix} D_n & 0 \\ 0 & D_{n'} \end{pmatrix}$, où D_n et $D_{n'}$ sont deux matrices d'ordre n et n' respectivement.

La généralisation au cas non libre se fait de la façon suivante : soit (P,q) un objet de $\mathbf{C}(\mathbf{A},\mathbf{A})$ et supposons P projectif de type fini et de rang constant n. On considère alors l'objet $(\Lambda^n P, \Lambda^n \varphi_q)$ et on appelle <u>déterminant</u> de (P,q) la classe d'isomorphisme de $(\Lambda^n P, \Lambda^n \varphi_q)$. Si $P = A^n$, $\Lambda^n P \approx A$ et si $\{e_1,\ldots,e_n\}$ est une base de P, $e_1 \wedge \ldots \wedge e_n$ est un générateur de $\Lambda^n P$ et $\Lambda^n \varphi_q(e_1 \wedge \ldots \wedge e_n, e_1 \wedge \ldots \wedge e_n)$ est le scalaire Δ vu plus haut. La forme bilinéaire symétrique $\Lambda^n \varphi_q$ est déterminée, à isomorphisme près, par la donnée du scalaire Δ à un carré près. Si maintenant (P,q) et (P',q') sont deux objets de $\mathbf{C}(A,A)$ projectifs de type fini et de rangs constants respectifs n et n', la formule qui donne la puissance extérieure d'une somme orthogonale montre que $\det((P,q) \perp (P',q'))$ est le produit tensoriel $\det(P,q) \otimes \det(P',q')$.

Si P n'est pas de rang constant, on s'y ramène aisément en décomposant l'anneau A en un produit fini d'anneaux $A = \prod_{i=1}^{m} A_i$ tel que $P \otimes_A A_i$ soit de rang constant n_i sur A_i (cf. 1.10.). On a alors $(P,q) \approx \perp_{i=1}^{m} (P \otimes_A A_i, q_i)$, où q_i est la restriction de q à $P \otimes A_i$. Le déterminant de (P,q) n'est autre que la somme orthogonale des $\det(P \otimes_A A_i, q_i)$. Ceci est un cas particulier du fait que, étant donnée une fonction continue r de $\mathrm{Spec}(A)$ dans $\mathbf{N}$ et un module bilinéaire (P,f), où P est projectif de type fini et f symétrique, on sait définir le module bilinéaire $(\Lambda^r P, \Lambda^r f)$ de la façon suivante. Comme les valeurs prises par la fonction rang de P et par la fonction r sont en nombre fini, il existe un nombre fini d'idempotents $e_1,\ldots,e_p$ deux à deux orthogonaux de somme 1 tels que sur Ae_i, P est de rang constant n_i et r prend la valeur m_i. Alors $(\Lambda^r P, \Lambda^r f) = \perp_{i=1}^{p} (\Lambda^{m_i} Pe_i, \Lambda^{m_i} fe_i)$. Il suffit d'appliquer ce résultat à la fonction $r = r_P$ et au module bilinéaire déduit de (P,q) (si $n_i = 0$ et $m_i = 0$, $(\Lambda^0 0, \Lambda^0 0)$ n'est pas autre chose que Ae_i muni de la forme bilinéaire symétrique naturelle $g(ae_i, be_i) = abe_i$).

Le déterminant d'un espace hyperbolique $h(P)$ (cf. 1.7.) est une forme bilinéaire symétrique sur le A-module $\Lambda^{r_P} P \otimes_A \Lambda^{r_P} P^*$, canoniquement isomorphe à A, car $\Lambda^{r_P} P^* \approx (\Lambda^{r_P} P)^*$. Il est donc donné par un élément de $U(A)/U^2(A)$ est un calcul utilisant la multiplicativité du déterminant montre que ce déterminant n'est autre que $(-1)^{r_P} = 1 - 2e$, où e est l'idempotent tel que $P \otimes_A Ae$ est de rang impair et $P \otimes_A A(1-e)$ est de rang pair.

1.7. ESPACES HYPERBOLIQUES ET REFLEXIVITE

Soient A un anneau, M et N deux A-modules et $q : M \oplus \mathrm{Hom}_A(M,N) \to N$ l'application A-quadratique définie par $(x,f) \mapsto f(x)$. Si φ est l'application A-bilinéaire symétrique associée à q, on a $\varphi((x,f),(y,g)) = (f+g)(x+y) - f(x) - g(y) = f(y) + g(x)$, quels que soient $x,y \in M$ et $f,g \in \mathrm{Hom}_A(M,N)$. On dira que $(A, M \oplus \mathrm{Hom}_A(M,N), q, N)$, en tant qu'objet de $\mathbf{C}$, est l'<u>espace hyperbolique</u> défini par M et N et on le note $h(A,M,N)$ ou simplement $h(M,N)$ et $h(M,A) = h(M)$, si aucune confusion n'est à craindre.

Considérons l'application A-linéaire $d_\varphi : M \oplus \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M \oplus \mathrm{Hom}_A(M,N), N) \approx \mathrm{Hom}_A(M,N) \oplus \mathrm{Hom}_A(\mathrm{Hom}_A(M,N),N)$ canoniquement associée à φ. Etudier l'injectivité ou la bijectivité de d_φ revient à étudier ces même propriétés pour l'application A-linéaire $c_{M,N} : M \to \mathrm{Hom}_A(\mathrm{Hom}_A(M,N),N)$ définie $x \mapsto (g \mapsto g(x))$ et il est clair que $\mathrm{Ker}(c_{M,N}) = \bigcap_{g \in \mathrm{Hom}_A(M,N)} \mathrm{Ker}(g)$.

Dans l'étude de la non dégénérescence d'un espace hyperbolique, on voit apparaître une notion de réflexivité relative. On dira qu'un A-module M est N-<u>réflexif</u>, où N est un A-module, si l'application A-linéaire $c_{M,N} : M \to \mathrm{Hom}_A(\mathrm{Hom}_A(M,N),N)$ est un isomorphisme de A-modules. Ainsi, une condition nécessaire et suffisante pour que l'application A-quadratique $q : M \oplus \mathrm{Hom}_A(M,N) \to N$ soit non dégénérée est que $\mathrm{Ker}(c_{M,N}) = 0$ et une condition nécessaire et suffisante pour que l'application A-quadratique $q : M \oplus \mathrm{Hom}_A(M,N) \to N$ soit strictement non dégénérée est que M soit N-réflexif.

Soit $u : M \xrightarrow{\sim} \mathrm{Hom}_A(M,N)$ un isomorphisme A-linéaire et ${}^t u : \mathrm{Hom}_A(\mathrm{Hom}_A(M,N),N) \xrightarrow{\sim} \mathrm{Hom}_A(M,N)$ l'isomorphisme transposé défini par $f \mapsto f \circ u$. Si l'on considère l'isomorphisme composé $\alpha = ({}^t u)^{-1} \circ u : M \xrightarrow{\sim} \mathrm{Hom}_A(\mathrm{Hom}_A(M,N),N)$, on a le lemme suivant :

Lemme 1.7.1. Pour que α coïncide avec le morphisme canonique $c_{M,N}$, il faut et il suffit que l'application A-bilinéaire $\varphi_u : M \times M \to N$ définie par $(x,y) \mapsto u(x)(y)$ soit symétrique.

En effet, comme u est un isomorphisme, pour chaque $g \in \mathrm{Hom}_A(M,N)$, il existe un élément unique $y \in M$ tel que $g = u(y)$, donc $c_{M,N}(x) : \mathrm{Hom}_A(M,N) \to N$ est l'application A-linéaire donnée par $u(y) \mapsto u(y)(x) = \varphi_u(y,x)$. Calculons maintenant $\alpha(x)$. Or, l'application $({}^t u)^{-1} : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(\mathrm{Hom}_A(M,N),N)$ est définie par $f \mapsto f \circ u^{-1}$, où $(f \circ u^{-1})(g) = f(u^{-1}(g))$ pour tout $g \in \mathrm{Hom}_A(M,N)$. Donc, si $g = u(y)$, $(f \circ u^{-1})(g) = f(u^{-1}(u(y))) = f(y)$. Comme $\alpha(x) = ({}^t u)^{-1}(u(x)) = u(x) \circ u^{-1}$, alors $\alpha(x)(u(y)) = u(x)(u^{-1}(u(y))) = u(x)(y) = \varphi_u(x,y)$. Le lemme est ainsi démontré.

On remarque que si S est une partie multiplicative de A et si M et N sont deux $S^{-1}A$-modules (resp. des (A/I)-modules, I étant un idéal de A), alors $\mathrm{Hom}_A(M,N) = \mathrm{Hom}_{S^{-1}A}(M,N)$ (resp. $\mathrm{Hom}_A(M,N) = \mathrm{Hom}_{A/I}(M,N)$). Ainsi, la N-réflexivité de M en tant que A-module équivaut à la N-réflexivité de M en tant que $S^{-1}A$-module (resp. (A/I)-module), ce qui fournit de nombreux exemples de couples (M,N), où M est N-réflexif.

Il nous sera plus utile de remarquer les faits suivants : si M, M_1 et M_2 sont des A-modules N-réflexifs, alors $M_1 \oplus M_2$, $\mathrm{Hom}_A(M,N)$ et tout facteur direct de M sont des A-modules N-réflexifs. Cela nous montre, en particulier, que pour que tout A-module projectif de type fini soit N-réflexif, il faut et il suffit que A lui-même soit N-réflexif, condition équivalente à $\mathrm{Hom}_A(N,N) \approx A$, i.e., N est un A-module fidèle dont tout endomorphisme est une homothétie. Cette condition est vérifiée, en particulier, si N est un A-module projectif de type fini et de rang 1 ; dans ce cas, réflexivité (ou A-réflexivité) et N-réflexivité coïncident.

Proposition 1.7.2. Soit (M,q,N) un objet de $\mathbf{C}(A)$, où $q : M \to N$ est strictement non dégénérée. Alors M est un A-module N-réflexif.

Pour démontrer la proposition, il suffira maintenant d'utiliser le lemme 1.7.1, en prenant pour application A-linéaire $u : M \to \mathrm{Hom}_A(M,N)$ l'application $x \mapsto (y \mapsto \varphi(x,y))$, où $\varphi : M \times M \to N$ est l'application A-bilinéaire symétrique associée à q. En effet, comme q est strictement non dégénérée, u est un isomorphisme, donc $c_{M,N} = ({}^t u)^{-1} \circ u$ est un isomorphisme et M est bien un A-module N-réflexif.

Les démonstrations des propositions suivantes sont laissées à la charge du lecteur.

Proposition 1.7.3. Si M_1, M_2, N sont des A-modules, il existe un isomorphisme de $\mathbf{C}(A)$, $h(M_1 \oplus M_2, N) \approx h(M_1,N) \perp h(M_2,N)$.

Proposition 1.7.4. Soient $A \to A'$ un morphisme d'anneaux et M et N deux A-modules. Si l'homomorphisme naturel $A' \otimes_A \mathrm{Hom}_A(M,N) \xrightarrow{\sim} \mathrm{Hom}_{A'}(A' \otimes_A M, A' \otimes_A N)$ est un isomorphisme de A'-modules, alors il existe un isomorphisme de $\mathbf{C}(A')$. $A' \otimes_A h(M,N) \approx h(A' \otimes_A M, A' \otimes_A N)$.

On remarque que l'hypothèse de 1.7.4. est vraie si M est un A-module projectif de type fini et pour tout changement d'anneau de base $A \to A'$ ou alors si M est un A-module de présentation finie et $A \to A'$ est plat.

1.8. GROUPE DE WITT-GROTHENDIECK ET GROUPE DE WITT.

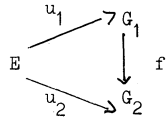
La définition générale des groupes de Witt et de Witt-Grothendieck que nous souhaitons donner, nous oblige à nous limiter à certains objets de $\mathbf{C}(A,N)$. Nous sommes amenés, à cause de 1.7., à supposer que N vérifie la condition $\mathrm{Hom}_A(N,N) \approx A$ de sorte que les A-modules projectifs de type fini soient N-réflexifs. Pour que l'espace hyperbolique d'un tel module soit dans la catégorie que nous considérons, nous appellerons $\mathbf{C}'(N)$ la sous-catégorie pleine de $\mathbf{C}(A,N)$ dont les objets (M,q) sont tels que q est strictement non dégénérée et le module sous-jacent M est de la forme $P_1 \oplus \mathrm{Hom}_A(P_2,N)$, où P_1 et P_2 sont deux A-modules projectifs de type fini. La somme orthogonale de deux objets de $\mathbf{C}'(N)$ est encore un objet de $\mathbf{C}'(N)$ et comme les classes d'isomorphismes d'objets de $\mathbf{C}'(N)$ forment un ensemble $E(N)$, on peut donner la proposition et définition suivantes :

Proposition et Définition 1.8.1. L'ensemble $E(N)$ muni de l'opération induite par la somme orthogonale est un monoïde abélien avec élément neutre dont le groupe universel est appelé groupe de Witt-Grothendieck de N et noté $WG(N)$.

C'est une conséquence immédiate des considérations précédentes et des isomorphismes d'associativité et de commutativité de 1.1.1.

Remarquons que si N est un A-module projectif de type fini et de rang 1, les objets de $\mathbf{C}'(N)$ sont de la forme (M,q), où M est projectif de type fini car $\mathrm{Hom}_A(P,N) \approx P^* \otimes_A N$ est alors projectif.

Rappelons que le groupe universel d'un monoïde abélien E est l'objet initial de la catégorie dont les objets sont les couples (G,u) où G est un groupe abélien et $u : E \to G$ un homomorphisme de monoïdes de E dans G et les morphismes $f : (G_1,u_1) \to (G_2,u_2)$, les homomorphismes de groupes abéliens $f : G_1 \to G_2$ qui font commuter le triangle :



La construction du groupe universel de E, $K(E)$, se fait en considérant dans $E\times E$ la relation d'équivalence $(x_1,x_2) \sim (y_1,y_2)$ s'il existe $z \in E$ tel que, dans E, $x_1 + y_2 + z = x_2 + y_1 + z$; si E est régulier, on peut simplifier z dans cette équation. L'ensemble quotient $E \times E / \sim$ muni de la loi de composition induite par celle de E est un groupe abélien et l'homomorphisme naturel $t : E \to K(E)$ est l'application t qui à x dans E associe à la classe de $(x,0)$. Tout élément de $K(E)$ s'écrit $t(x) - t(y)$ avec $x,y \in E$, c'est à dire comme différence de deux éléments de E.

La définition du groupe de Witt fait intervenir les espaces hyperboliques. Dans $WG(N)$, les images des classes d'isomorphismes des espaces $h(M,N)$, où $M = P_1 \oplus \mathrm{Hom}_A(P_2,N)$ avec P_1,P_2 projectifs de type fini, engendrent un sous-groupe $H(N)$ de $WG(N)$ et le groupe de Witt $W(N)$ est, par définition, le quotient $WG(N) / H(N)$. Si $N = A$, on obtient respectivement le groupe de Witt-Grothendieck et le groupe de Witt de l'anneau A. Ces groupes possèdent alors une structure supplémentaire. En effet, le produit tensoriel de deux objets de $\mathbf{C}'(A)$ est un objet de $\mathbf{C}'(A)$, ce qui donne la proposition suivante :

Proposition 1.8.2. Le produit tensoriel induit sur le groupe $WG(A)$ une structure d'anneau commutatif qui possède un élément unité si 2 est inversible dans A. Le groupe $H(A)$ est un idéal de $WG(A)$ et $W(A)$ est un anneau commutatif.

La première partie de la proposition provient de 1.5. ; l'élément unité est la classe de (A,q), où $q(a) = \frac{1}{2}a^2$ pour tout $a \in A$.

Pour la seconde, il suffira de démontrer que, si (P,q) est un objet de $\mathbf{C}'(A)$ et $h(M)$ est un espace hyperbolique, alors $(P,q) \otimes_A h(M)$ est encore un espace hyperbolique. En effet, soient $\alpha : P \xrightarrow{\sim} P^*$ l'isomorphisme de A-modules induit par la forme quadratique q et $\beta : P \otimes_A (M \oplus M^*) \to (P \otimes_A M) \oplus (P^* \otimes_A M^*)$ l'isomorphisme de A-modules défini par $x \otimes (y+f) \mapsto x \otimes y + \alpha(x) \otimes f$, où $x \in P$, $y \in M$ et $f \in M^*$. Il est clair que $\beta : (P,q) \otimes_A h(M) \xrightarrow{\sim} h(P \otimes_A M)$ est un isomorphisme dans la catégorie $\mathbf{C}'(A)$.

Les anneaux ci-dessus construits possèdent des propriétés fonctorielles simples. En effet, on a :

Proposition 1.8.3. L'anneau de Witt-Grothendieck (resp. L'anneau de Witt) est un foncteur covariant défini dans la catégorie des anneaux commutatifs à valeurs dans la catégorie des anneaux.

Soit, pour cela, $f : A \to A'$ un morphisme d'anneaux et (M,q) un objet de $\mathbf{C}'(A)$. Alors $(A' \otimes_A M,q')$, où $q' : A' \otimes_A M \to A'$ est la forme quadratique obtenue de q par extension de l'anneau des scalaires (cf. théorème 1.3.3.), est un objet de $\mathbf{C}'(A')$. Donc, f induit un morphisme naturel $WG(f) : WG(A) \to WG(A')$.

Etant donné que si P est un A-module projectif de type fini, il existe un isomorphisme, dans $\mathbf{C}'(A')$, $A' \otimes_A h(P) \approx h(A' \otimes_A P)$, $WG(f)$ passe au quotient et induit donc un morphisme d'anneaux $W(f) : W(A) \to W(A')$. Ceci démontre la proposition.

Le problème de l'extension des scalaires pour $WG(N)$ et $W(N)$ est moins simple, dans le cas général. Si N est un A-module pour lequel $WG(N)$ et $W(N)$ sont définis et si $f : A \to A'$ est un morphisme d'anneaux, il n'est pas sûr que $WG(A' \otimes_A N)$ et $W(A' \otimes_A N)$ soient définis, car la condition $\mathrm{Hom}_{A'}(A' \otimes_A N, , A' \otimes_A N) \approx A'$ n'est pas entraînée par $\mathrm{Hom}_A(N,N) \approx A$, comme on le voit dans l'exemple suivant : $A = k[X,Y]$ est l'anneau des polynômes en les indéterminées X et Y et à coefficients dans un corps k, $A' = k$ et $N = AX + AY$.

Cependant si N est projectif de type fini et de rang 1, alors $A' \otimes_A N$ l'est en tant que A'-module. On obtient, comme ci-dessus, deux homomorphismes naturels de groupes abéliens de $WG(N)$ dans $WG(A' \otimes_A N)$ et de $W(N)$ dans $W(A' \otimes_A N)$.

Soient maintenant (M,q) un objet de $\mathbf{C}'(N)$ et (P,q') un objet de $\mathbf{C}'(A)$. Leur produit tensoriel est un objet de $\mathbf{C}(A,N)$. De plus, les isomorphismes $\alpha : M \to \mathrm{Hom}_A(M,N)$ et $\alpha' : P \to \mathrm{Hom}_A(P,A)$ induits par q et q' respectivement donnent un isomorphisme $\alpha \otimes \alpha' : M \otimes_A P \to \mathrm{Hom}_A(M,N) \otimes_A \mathrm{Hom}_A(P,A)$ qui s'identifie canoniquement à $\mathrm{Hom}_A(M \otimes_A P,N)$. Comme cet isomorphisme n'est autre que l'application linéaire de $M \otimes_A P$ dans $\mathrm{Hom}_A(M \otimes_A P,N)$ induite par $q \otimes q'$, cela montre que le produit tensoriel de (M,q) et de (P,q') est un objet de $\mathbf{C}'(N)$.

On vérifie sans difficultés que cela induit une application de $WG(N) \times WG(A)$ dans $WG(N)$ qui est biadditive, car le produit tensoriel commute à la somme orthogonale. De plus, l'associativité du produit tensoriel montre que cela donne sur $WG(N)$ une structure de $WG(A)$-module, unitaire si $WG(A)$ est unitaire. Tout ceci passe au quotient par le sous-groupe des espaces hyperboliques. Ainsi, $W(N)$ se trouve muni d'une structure naturelle de $W(A)$-module : si h est un espace hyperbolique de $\mathbf{C}'(N)$ (resp. $\mathbf{C}'(A)$) et (M,q) un objet de $\mathbf{C}'(A)$ (resp. $\mathbf{C}'(N)$), $h \otimes_A (M,q)$ est un espace hyperbolique de $\mathbf{C}'(N)$, comme le montre une démonstration analogue à celle de la proposition 1.8.2.

Soient maintenant N et N' deux modules pour lesquels les groupes de Witt-Grothendieck et de Witt sont définis et supposons que N soit projectif de type fini et de rang 1. Alors $WG(N \otimes_A N')$ et $W(N \otimes_A N')$ sont définis. En effet $\mathrm{Hom}_A(N \otimes_A N', N \otimes_A N') \simeq \mathrm{Hom}_A(N,N) \otimes_A \mathrm{Hom}_A(N',N') \approx A$. Si maintenant (M,q) et (M',q') sont des objets de $\mathbf{C}'(N)$ et $\mathbf{C}'(N')$ respectivement, leur produit tensoriel est un objet de $\mathbf{C}'(N \otimes_A N')$ car l'application linéaire associée à cet objet

$\beta : M \otimes_A M' \to \mathrm{Hom}_A(M \otimes_A M', N \otimes_A N')$ est le produit tensoriel de $\alpha : M \to \mathrm{Hom}_A(M,N)$ et de $\alpha' : M' \to \mathrm{Hom}_A(M',N')$ en identifiant $\mathrm{Hom}_A(M \otimes_A M', N \otimes_A N')$ et $\mathrm{Hom}_A(M,N) \otimes_A \mathrm{Hom}_A(M',N')$. On obtient ainsi une application biadditive de $WG(N) \times WG(N')$ dans $WG(N \otimes_A N')$ qui se trouve, à cause de l'associativité du produit tensoriel dans $\mathbf{C}(A)$, être $WG(A)$-bilinéaire et induit donc un homomorphisme de $WG(A)$-modules de $WG(N) \otimes_{WG(A)} WG(N')$ dans $WG(N \otimes_A N')$.

Les même propriétés sont vraies avec les groupes de Witt : il existe une application $W(A)$-bilinéaire de $W(N) \times W(N')$ dans $W(N \otimes_A N')$ induite par le produit tensoriel, si N ou N' est projectif de type fini et de rang 1, donc une application $W(A)$-linéaire $W(N) \otimes_{W(A)} W(N') \to W(N \otimes_A N')$.

Cependant, l'application naturelle ainsi obtenue, $W(N) \otimes_{W(A)} W(N^*) \to W(N \otimes_A N^*) = W(A)$, où N est projectif de type fini et de rang 1, n'est pas nécessairement un isomorphisme.

Supposons que 2 soit inversible dans A et qu'il existe un A-module projectif P de type fini et de rang 1 tel que $N = P \otimes_A P$. Alors, l'application $q_o : P \to N$, $x \mapsto \frac{1}{2} x \otimes x$ est une application quadratique strictement non dégénérée et on a un isomorphisme de $W(A)$-modules $W(A) \to W(N)$ donné par $(M,q) \mapsto (M \otimes_A P, , q \otimes q_o)$. Ceci nous montre que $W(N)$ est un $W(A)$- module libre de rang 1.

La plus grande partie des notions introduites dans ce paragraphe peut être répétée pour certaines catégories de modules munis d'une application bilinéaire. Nous nous restreindrons ici au cas le plus simple et considérons la catégorie $\underline{\mathrm{Bil}}(A)$ dont les objets sont les couples (M,φ), où M est projectif de type fini et $\varphi : M \times M \to A$ une forme A-bilinéaire symétrique strictement non dégénérée et dont les morphismes $u : (M,\varphi) \to (M',\varphi')$ sont les applications linéaires $u : M \to M'$ telle que $\varphi'(u(x),u(y)) = \varphi(x,y)$, x et y parcourant M. La somme orthogonale et le produit tensoriel de deux objets de $\underline{\mathrm{Bil}}(A)$ sont encore dans $\underline{\mathrm{Bil}}(A)$; de plus, $\underline{\mathrm{Bil}}(A)$ possède un <u>élément unité</u>, à savoir, le module bilinéaire (A,μ) où μ est la multiplication de l'anneau A. On peut donc associer à $\underline{\mathrm{Bil}}(A)$ un anneau unitaire en considérant le monoïde abélien des classes d'isomorphismes d'objets de $\underline{\mathrm{Bil}}(A)$ muni de l'opération induite par la somme orthogonale . Ce monoïde a un groupe universel dans lequel le produit tensoriel induit une structure d'anneau commutatif dont l'élément unité est la classe de (A,μ). On notera $\mathrm{Bil}(A)$ cet anneau et on a alors le théorème suivant, compte tenu des notations et conditions exposées dans ce paragraphe :

<u>Théorème</u> 1.8.4. <u>Le produit tensoriel d'une application quadratique et d'une forme bilinéaire symétrique induit sur</u> $WG(N)$ <u>une structure de</u> $\mathrm{Bil}(A)$<u>-module unitaire</u>.

Le résultat est clair dès qu'on a vérifié que le produit tensoriel de (M,q,N) et de (P,φ) où q et φ sont strictement non dégénérées, est une application quadratique strictement non dégénérée, résultat qui provient du résultat analogue sur les formes bilinéaires symétriques. Naturellement, si 2 est inversible dans A, il y a identité entre applications bilinéaires symétriques et applications quadratiques ; $\mathrm{Bil}(A)$ n'est autre que l'anneau de Witt-Grothendieck de A et on retrouve sur $WG(N)$ la structure de $WG(A)$-module déjà vue. C'est un cas particulier du résultat suivant :

Proposition 1.8.5. *Le foncteur qui a un objet (M,q,N) de $\mathbf{C}(A)$ associe le module bilinéaire (M,φ_q,N) restreint à $\mathbf{C}'(A)$, induit un homomorphisme d'anneaux de $WG(A)$ dans $\mathrm{Bil}(A)$.*

C'est une conséquence de 1.5.6. ; ce morphisme n'est pas nécessairement unitaire car $WG(A)$ n'a pas nécessairement d'élément unité.

La structure de $WG(A)$-modules sur les groupes abéliens $WG(N)$ s'obtient alors à l'aide des deux résultats précédents par restriction des scalaires.

On pourrait aussi développer un formalisme analogue pour les groupes et anneaux de Witt mais nous nous abstiendrons de le faire.

1.9. RETOUR AUX ESPACES HYPERBOLIQUES

Soit (M,q,N) un objet de $\mathbf{C}(A)$; notant $-q : M \to N$ l'application quadratique définie par $x \mapsto -q(x)$, on cherche à quelles conditions on a un isomorphismes dans $\mathbf{C}(A)$, $(M,q,N) \perp (M,-q,N) \simeq h(M,N)$.

Si M est N-réflexif, ce que nous supposerons désormais, l'application quadratique de $h(M,N)$ est strictement non dégénérée. Il est donc nécessaire que q soit elle-même strictement non dégénérée. Nous montrons ici que la réciproque est vraie dans les cas suivants : 2 est inversible dans $\mathrm{Hom}_A(N,N)$ ou M est projectif.

Lemme 1.9.1. *Soit (M,q,N) un objet de $\mathbf{C}(A)$. Il existe une application A-bilinéaire $B : M \times M \to N$ telle que $q(x) = B(x,x)$ pour tout $x \in M$ dans les cas suivants : 1) l'homothétie de rapport 2 est inversible dans N ; 2) M est projectif ; 3) M est somme directe d'un module projectif et d'un module $\mathrm{Hom}_A(M',N)$, où M' est projectif et pour toute application quadratique $q_o : N \to N$, il existe une application bilinéaire $\varphi_o : N \times N \to N$ telle que $q_o(y) = \varphi_o(y,y)$ pour tout $y \in N$.*

Dans le premier cas on prend $B(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$, x et y parcourant M.

Pour le second cas, soit M_1 un supplémentaire de M tel que $L = M \oplus M_1$ soit libre. On prolonge alors q sur L par 0 sur M_1 et il suffit de montrer le résultat pour M libre. Soit $(e_i)_{i\in I}$ une base de M et supposons l'ensemble d'indices I totalement ordonné. On pose $B(e_i,e_i) = q(e_i)$ pour tout $i \in I$, $B(e_i,e_j) = \varphi(e_i,e_j)$ si $i < j$ et $B(e_i,e_j) = 0$ si $i > j$, où $\varphi : M \times M \to N$ est l'application A-bilinéaire associée à q. Alors B satisfait aux conditions demandées.

Dans le troisième cas, $M = M_1 \oplus \mathrm{Hom}(M_2,N)$ et on peut, comme dans le second cas, supposer M_1 et M_2 libres, donc $M_1 \simeq A^{(I)}$, $M_2 \simeq A^{(J)}$ et $M = A^{(I)} \oplus N^{(J)}$. On suppose les ensembles d'indices I et J totalement ordonnés. Si $(e_i)_{i\in I}$ est une base de M_1, on pose $B(e_i,e_i) = q(e_i)$ pour tout $i \in I$, $B(e_i,e_j) = \varphi(e_i,e_j)$ si $i < j$ et $B(e_i,e_j) = 0$ si $i > j$, $B(e_i,y_j) = \varphi(e_i,e_j)$ pour tout $i \in I$ et y_j dans le $j^{\text{ième}}$ facteur de $N^{(J)}$, $B(y_j,e_i) = 0$ pour y_j dans le $j^{\text{ième}}$ facteur de $N^{(J)}$ et $i \in I$, $B(y_i,y_j) = \varphi(y_i,y_j)$ si $i < j$ et $B(y_i,y_j) = 0$ si $i > j$ où y_i (resp. y_j) est dans le $i^{\text{ème}}$ (resp. $j^{\text{ième}}$) facteur de $N^{(J)}$. Il reste finalement à définir B sur les paires (x_j,y_j) où x_j et y_j sont dans le $j^{\text{ième}}$ facteur de $N^{(J)}$. Dans ce cas, considérons la restriction de q à ce facteur : c'est une forme quadratique $q_j : N \to N$ pour laquelle il existe, par hypothèse, une forme A-bilinéaire $\varphi_j : N \times N \to N$ telle que $q_j(y) = \varphi_j(y,y)$ pour tout $y \in N$. On définit alors $B(x_j,y_j) = \varphi_j(x_j,y_j)$. Il est facile maintenant de vérifier que $B(x,x) = q(x)$ pour tout $x \in M$.

Lemme 1.9.2. Soit (M,q,N) un objet de $\mathcal{C}(A)$, où q est strictement non dégénérée. S'il existe une application A-linéaire $f : M \to M$ telle que $\varphi(x,f(x)) = q(x)$ pour tout $x \in M$, alors $(M,q,N) \perp (M,-q,N) \simeq h(M,N)$.

En effet, soient U et V les deux sous-modules suivants de $M \oplus M$: $U = \{(x,x) \mid x \in M\}$ et $V = \{(y - f(y), -f(y)) \mid y \in M\}$. Il est facile de voir que U et V sont deux sous-modules supplémentaires de $M \oplus M$ car l'équation $(x,y) = (z,z) + (t-f(t), -f(t))$ a, pour tout couple (x,y), la solution unique $z = y + f(x-y)$ et $t = x-y$. Calculons $(q \perp -q)((z,z) + (t-f(t), -f(t))) = q(z+t - f(t)) - q(z-f(t)) = q(t) + \varphi(t,z - f(t)) = \varphi(z,t)$. Soit alors $\alpha : M \to \mathrm{Hom}_A(M,N)$ l'isomorphisme associé à q, i.e., $\alpha(x)(y) = \varphi(x,y)$ pour tout $(x,y) \in M \times M$. L'application de $M \oplus M = U \oplus V$ dans $h(M,N)$ qui à $(z,z) + (t-f(t), -f(t))$ associe le couple $(z,\alpha(t))$ est un isomorphisme de modules. De plus, $\alpha(t)(z) = \varphi(z,t) = (q \perp -q)((z,z) + (t-f(t), (f(t)))$; c'est donc un isomorphisme dans $\mathcal{C}(A)$.

Nous pouvons maintenant démontrer le résultat souhaité, à savoir :

Proposition 1.9.3. Soient M un module N-réflexif et $q : M \to N$ une application quadratique. Supposons l'une des deux conditions suivantes réalisées : (1) l'homothétie de rapport 2 est inversible dans N ; (2) M est projectif. Alors les propriétés suivantes sont équivalentes : i) q est strictement non dégénérée ; ii) il existe un isomorphisme $(M,q,N)\perp(M,-q,N) \simeq h(M,N)$.

Comme on l'a déjà remarqué, ii) $\Rightarrow$ i) si M est N-réflexif car l'application linéaire de $M \oplus M$ dans $\mathrm{Hom}_A(M,N) \oplus \mathrm{Hom}_A(M,N)$ associée à $q \perp -q$ a pour matrice $\begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$ et pour que ce soit un isomorphisme, il est nécessaire et suffisant que α en soit un.

En sens contraire, i) $\Rightarrow$ ii) : en vertu des hypothèses, soit $B : M \times M \to N$ une application A-bilinéaire telle que $B(x,x) = q(x)$. Comme l'application A-linéaire $\alpha : M \to \mathrm{Hom}_A(M,N)$ induite par q est un isomorphisme, on sait que pour toute application A-bilinéaire $F : M \times M \to N$, il existe une application $f_F : M \to N$ telle que pour tout $(x,y) \in M \times M$, on ait $F(x,y) = \varphi(x,f_F(y))$. Prenant alors $F = B$, on voit que l'application A-linéaire $f = f_B$ vérifie, en particulier, $\varphi(x,f(x)) = q(x)$. On est alors dans les hypothèses du lemme 1.9.2. et on en conclut l'isomorphisme $(M,q,N)\perp(M,-q,N) \approx h(M,N)$.

Remarque. On n'a pas utilisé le cas 3) du lemme 1.9.1. dont l'intérêt réel n'est pas évident. Si l'on ne suppose pas 2 inversible dans A et si l'on s'intéresse aux couples (M,N), où $\mathrm{Hom}_A(N,N) \approx A$, il sera nécessaire de supposer M projectif, auquel cas il sera aussi nécessaire de supposer N projectif de type fini et de rang 1 pour qu'il soit possible que $\mathrm{Hom}_A(M,N)$ et M soient isomorphes. En effet, on ne voit guère quels sont les modules N non projectifs qui vérifient en plus de $\mathrm{Hom}_A(N,N) \approx A$, la condition 3) du lemme 1.9.1.

La proposition précédente permet de donner une définition un peu différente du groupe de Witt de N. Soit pour cela E(N) l'ensemble des classes d'isomorphismes d'objets de C'(N) et soit dans E(N) la relation suivante : $(M,q) \sim (M',q')$ si et seulement si il existe P_1 et P_2, A-modules projectifs de type fini tels que $(M,q)\perp h(P_1) \simeq (M',q')\perp h(P_2)$.

Il est facile de voir que c'est une relation d'équivalence dans E(N), compatible avec la loi d'addition induite par la somme orthogonale. Ainsi l'ensemble quotient $E'(N) = E(N)/\sim$ hérite d'une structure de monoïde abélien avec élément neutre.

Proposition et Définition 1.9.4. Le groupe universel du monoïde abélien E'(N) est le groupe de Witt de N, W(N). Si 2 est inversible dans A ou si N est un module

projectif de type fini et de rang 1, $E'(N)$ est un groupe abélien et coïncide donc avec $W(N)$.

En effet, la définition donnée plus haut montre que l'application naturelle de $E(N)$ dans $W(N)$ passe au quotient par la relation d'équivalence $\sim$ et ainsi on a un homomorphisme de $E'(N)$ dans $W(N)$. Comme les éléments de $W(N)$ sont différence d'image d'éléments de $E(N)$, ils sont de même différence d'image d'éléments de $E'(N)$. On a donc une application naturelle du groupe universel de $E'(N)$ dans $W(N)$. Inversement, l'application composée $E(N) \to E'(N) \to K(E'(N))$, groupe universel de $E'(N)$, induit un homomorphisme de groupes abéliens de $WG(N)$ dans $K(E'(N))$ qui est nul sur le sous-groupe de $WG(N)$ engendré par les espaces hyperboliques. Par passage au quotient, on obtient ainsi un homomorphisme naturel de $W(N)$ dans $K(E'(N))$. Une vérification facile, laissée au lecteur, montre que ces deux homomorphismes sont inverses l'un de l'autre.

La seconde affirmation est une conséquence immédiate de la proposition 1.8.1. En effet, dans les hypothèses du lemme 1.9.2., on a $(M,q) \perp (M,-q) \simeq h(M)$, donc dans $E'(N)$, la classe (M,q) a pour opposée la classe de $(M,-q)$ et $E'(N)$ est donc un groupe abélien.

Corollaire 1.9.5. Dans les hypothèses de la proposition précédente, si -1 est un carré dans A, en particulier si $2 = 0$ dans A, $W(N)$ est un groupe abélien dans lequel tout élément est d'ordre 2.

En effet, si $-1 = a^2$, alors l'homothétie de rapport a dans M est un isomorphisme de (M,q) sur $(M,-q)$, d'où le résultat annoncé.

1.10. L'HOMOMORPHISME DE DIMENSION

Rappelons certains faits bien connus d'algèbre commutative (cf. [11], ch. 2). Si A est un anneau commutatif et unitaire, on appelle spectre de A et on note $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de A muni de la topologie de Zariski, dans lequel une base d'ouverts est formé des $D_f = \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(A), f \notin \mathfrak{p}\}$, où $f \in A$. Pour cette topologie, $\mathrm{Spec}(A)$ est quasi compact. A tout A-module M projectif de type fini, on associe une fonction de $\mathrm{Spec}(A)$ dans $\mathbb{Z}$, la fonction rang, définie par : $r_M(\mathfrak{p})$ = le rang du $A_{\mathfrak{p}}$-module libre de type fini $M \otimes_A A_{\mathfrak{p}}$. C'est une fonction continue, ce qui équivaut à localement constante, vue la topologie de $\mathrm{Spec}(A)$. L'ensemble $\mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$ est un anneau pour les opérations somme et produit des fonctions. On a alors les propriétés évidentes suivantes : $r_{M \oplus N} = r_M + r_N$ et $r_{M \otimes_A N} = r_M . r_N$, quels que soient M et N, A-modules projectifs de type fini.

Si $f : A \to A'$ est un homomorphisme d'anneaux et $\mathfrak{p}$ un idéal premier de A', $f^{-1}(\mathfrak{p})$ est un idéal premier de A. On en déduit une application continue $\mathrm{Spec}(f) : \mathrm{Spec}(A') \to \mathrm{Spec}(A)$, d'où un homomorphisme naturel d'anneaux de $\mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$ dans $\mathcal{C}(\mathrm{Spec}(A'), \mathbb{Z})$. Si M est un A-module projectif de type fini on a, si $r_{A' \otimes_A M} : \mathrm{Spec}\ A' \to \mathbb{Z}$, la relation $r_{A' \otimes_A M} = r_M \circ \mathrm{Spec}(f)$.

Soit $K_o(A)$ l'anneau de Grothendieck des classes de A-modules projectifs de type fini. Alors r_M induit un homomorphisme naturel $r : K_o(A) \to \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$, fonctoriel en A, en ce sens que si $f : A \to A'$ est un homomorphismes d'anneaux, on a le carré commutatif :

$$\begin{array}{ccc} K_o(A) & \xrightarrow{\ r\ } & \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z}) \\ \Big\downarrow{\scriptstyle K_o(f)} & & \Big\downarrow{\scriptstyle \mathrm{Spec}(f)} \\ K_o(A') & \xrightarrow{\ r'\ } & \mathcal{C}(\mathrm{Spec}(A'), \mathbb{Z}) \end{array}$$

La flèche r est surjective. En effet, si $g \in \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$, comme $\mathrm{Spec}(A)$ est quasi compact, $g(\mathrm{Spec}(A))$ est un ensemble fini et, comme les fonctions constantes sont naturellement dans $r(K_o(A))$, on peut translater g de sorte que $g(\mathrm{Spec}(A))$ soit constitué d'entiers positifs ou nuls $r_1 < r_2 < \ldots < r_p$. Soit alors $X_i = g^{-1}(r_i)$, $i = 1, \ldots, p$. Les X_i forment une partition de $\mathrm{Spec}(A)$ en parties ouvertes et fermées et il existe donc, dans A, des idempotents e_i, $1 \leq i \leq p$, deux à deux orthogonaux et de somme 1 tels que $X_i = \mathrm{Spec}(A\, e_i)$. Il suffit alors de prendre $M = \bigoplus_{i=1}^{p} (A\, e_i)^{r_i}$ et on a bien $r_M = g$.

Dans le cadre des applications quadratiques, considérons (M,q) un objet de $\mathcal{C}'(N)$, où N est projectif de type fini. Nous pouvons lui faire correspondre la classe de M dans le groupe de Grothendieck $K_o(A)$ et on obtient ainsi un homomorphisme de groupes abéliens de $WG(N)$ dans $K_o(A)$ qui est un homomorphisme d'anneaux commutatifs, si $N = A$ (notons que $K_o(A)$ est unitaire, mais que $WG(A)$ ne l'est pas toujours). Cet homomorphisme est fonctoriel en ce sens qu'on a le diagramme commutatif :

$$\begin{array}{ccc} WG(N) & \longrightarrow & K_o(A) \\ \Big\downarrow{\scriptstyle WG(f)} & & \Big\downarrow{\scriptstyle K_o(f)} \\ WG(A' \otimes_A N) & \longrightarrow & K_o(A') \end{array}$$

On appellera homomorphisme de dimension, et on notera dim l'homomorphisme composé $WG(N) \to K_o(A) \to \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$; si $N = A$ c'est un homomorphisme

d'anneaux. Il est fonctoriel en A, i.e., on a le carré commutatif de groupes abéliens (resp. d'anneaux, si N = A) :

$$\begin{array}{ccc} WG(N) & \xrightarrow{\dim} & \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z}) \\ \downarrow{\scriptstyle WG(f)} & & \downarrow{\scriptstyle \mathrm{Spec}(f)} \\ WG(A' \otimes_A N) & \xrightarrow{\dim} & \mathcal{C}(\mathrm{Spec}(A'), \mathbb{Z}) \end{array}$$

On a un homomorphisme naturel de groupes abéliens de $K_o(A)$ dans $WG(N)$ défini de la façon suivante : à M, on associe la classe dans $WG(N)$ de l'espace hyperbolique $h(M,N)$. L'image de $K_o(A)$ est le sous-groupe noté $H(N)$ en 1.8. et le conoyau de cet homomorphisme est donc le groupe de Witt $W(N)$. On a ainsi la suite exacte de groupes abéliens $K_o(A) \to WG(N) \to W(N) \to 0$. Il n'est pas nécessaire ici de supposer que N soit projectif de type fini et de rang 1.

Regardons maintenant l'image par l'application dim du sous-groupe $H(N)$ formé par les espaces hyperboliques. Il s'agit donc d'étudier la fonction $r_{M \oplus \mathrm{Hom}_A(M,N)}$, qui n'est autre que $r_M + r_{\mathrm{Hom}_A(M,N)}$ et comme $\mathrm{Hom}_A(M,N) \approx M^* \otimes_A N$ a même rang que M, $r_{h(M,N)} = 2\, r_M$. Comme de plus, l'application $r : K_o(A) \to \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$ est surjective, l'image de $H(N)$ par l'application dim est le sous-groupe $\mathcal{C}(\mathrm{Spec}(A), 2\,\mathbb{Z})$ de $\mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})$. On a ainsi un homomorphisme naturel de $W(N)$ dans le groupe quotient $\mathcal{C}(\mathrm{Spec}(A), \mathbb{Z})/\mathcal{C}(\mathrm{Spec}(A), 2\,\mathbb{Z})$ et celui-ci est isomorphe à $\mathcal{C}(\mathrm{Spec}(A), \mathbb{Z}/2\,\mathbb{Z})$. L'homomorphisme composé $W(N) \to \mathcal{C}(\mathrm{Spec}(A), \mathbb{Z}/2\,\mathbb{Z})$ est appelé <u>dimension modulo</u> 2.

Soit alors $Ip(A)$ l'ensemble des éléments idempotents de l'anneau A : c'est un anneau commutatif et unitaire si l'on munit des lois de compositions $e \overset{\sim}{+} e' = e + e' - 2\,e\,e'$ (somme booléenne) et $e.e' = e\,e'$, le produit dans l'anneau A. Cet anneau est isomorphe à l'anneau des fonctions continues de $\mathrm{Spec}(A)$ dans $\mathbb{Z}/2\,\mathbb{Z}$ par l'intermédiaire de l'ensemble des parties de $\mathrm{Spec}(A)$ qui sont, à la fois, ouvertes et fermées. En effet, à $e \in Ip(A)$ on associe $X_e = \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(A), e \notin \mathfrak{p}\}$ et l'image de e dans l'anneau local $A_{\mathfrak{p}}$, qui est idempotent, est 0 si $\mathfrak{p} \notin X_e$ et 1 si $\mathfrak{p} \in X_e$. On peut donc associer à $e \in Ip(A)$, la fonction continue de $\mathrm{Spec}(A)$ dans $\mathbb{Z}/2\,\mathbb{Z}$ égale à 0 sur $\complement X_e$ et à 1 sur X_e. On a donc, pour chaque module projectif N de type fini et de rang 1, un homomorphisme de dimension modulo 2, $\dim_2 : W(N) \to Ip(A)$ dont les propriétés fonctorielles, vis à vis de l'extension des scalaires, sont claires.

De plus, si $N = A$, cet homomorphisme est un homomorphisme d'anneaux. Dans le cas général, le noyau, noté $W_o(N)$, est un sous-$W(A)$-module de $W(N)$. Si $N = A$, c'est un idéal de $W(A)$. On a le diagramme commutatif :

$$\begin{array}{ccccc} WG(N) & \longrightarrow & K_o(A) & \xrightarrow{r} & \mathbf{C}(\mathrm{Spec}(A), \mathbb{Z}) \\ \downarrow{\scriptstyle \pi} & & & & \downarrow \\ W(N) & & \xrightarrow{\dim_2} & & \mathbf{C}(\mathrm{Spec}(A), \mathbb{Z}/(2)) = \mathrm{Ip}(A) \end{array} .$$

Le noyau de l'application composée $\dim_2 \circ \pi : WG(N) \to \mathrm{Ip}(A)$ sera noté $WG_o(N)$ et l'application $\dim : WG(N) \to K_o(A) \xrightarrow{r} \mathbf{C}(\mathrm{Spec}(A), \mathbb{Z})$ restreinte à $WG_o(N)$ permet de définir une application, notée $\frac{1}{2}\dim : WG_o(N) \to \mathbf{C}(\mathrm{Spec}(A), \mathbb{Z})$. De plus, si P est un A-module projectif de type fini, $\frac{1}{2}\dim(h(P,N)) = r_P$ et comme l'application r est surjective, il en est de même de $\frac{1}{2}\dim$. Notons $\widetilde{WG}(N) = \mathrm{Ker}(\frac{1}{2}\dim)$; on a la suite exacte de groupes abéliens : $0 \to \widetilde{WG}(N) \to WG_o(N) \xrightarrow{1/2\dim} \mathbf{C}(\mathrm{Spec}(A), \mathbb{Z}) \to 0$.

1.11. DECOMPOSITIONS ORTHOGONALES

Désormais, on appellera A-module quadratique tout couple (P,q), où P est un A-module projectif de type fini et $q : P \to A$ est une forme quadratique strictement non dégénérée, que nous dirons aussi non dégénérée, si aucune confusion n'est à craindre. Notons $\mathrm{Quad}(A)$ la catégorie des A-modules quadratiques, notée $\mathbf{C}'(A)$ dans 1.8., qui est la seule catégorie dans laquelle nous travaillerons désormais.

Lemme 1.11.1. *Soient A un anneau, (P,q) un A-module quadratique, P' un sous-A-module de P et q' la restriction de q à P'. Les conditions suivantes sont équivalentes : (i) (P',q') est un A-module quadratique, i.e., P' est projectif et q' est non dégénérée ; (ii) (P',q') est un facteur orthogonal de (P,q).*

Il est évident que (ii) $\Rightarrow$ (i). Montrons que (i) $\Rightarrow$ (ii). Soient, à cet effet, $j : P' \hookrightarrow P$ l'injection canonique et $\alpha' : P' \xrightarrow{\sim} P'^*$ (resp. $\alpha : P \xrightarrow{\sim} P^*$) l'isomorphisme A-linéaire défini par q'(resp. q). Alors l'application A-linéaire $\alpha'^{-1} \circ {}^t j \circ \alpha$ vérifie $(\alpha'^{-1} \circ {}^t j \circ \alpha) \circ j = \mathrm{id}_{P'}$, donc P' est un facteur direct de P. Si $P'' = \mathrm{Ker}\,(\alpha'^{-1} \circ {}^t j \circ \alpha)$ et q'' est la restriction de q à P'', on a $(P,q) \approx (P',q') \perp (P'',q'')$.

Il est clair que dans ce lemme, on peut oublier la projectivité des modules P et P' et ne retenir que la non dégénérescence des formes quadratiques

q et q'.

Théorème 1.11.2. Soient A un anneau local d'idéal maximal $\mathfrak{m}$ et (P,q) un A-module quadratique. (i) Si 2 est inversible dans A, (P,q) possède une base orthogonale. (ii) Si $2 \in \mathfrak{m}$, (P,q) est de rang pair et possède une décomposition orthogonale en somme de plans (sous-modules de rang 2).

Supposons que 2 est inversible dans A. La démonstration se fait par récurence sur le rang n du A-module P, le résultat étant clair pour $n = 1$. Supposons $n \geq 1$ et considérons le k-espace quadratique $k \otimes_A P$, où $k = A/\mathfrak{m}$ est le corps résiduel de A. Comme la forme quadratique étendue $q' : k \otimes_A P \to k$ est non dégénérée, il existe au moins un vecteur $x \in k \otimes_A P$ tel que $q'(x) \neq 0$. Mais x peut s'écrire sous la forme $x = 1 \otimes e_1$ avec $e_1 \in P$ et $q'(1 \otimes e_1)$ est la classe de $q(e_1)$ dans k. Cela signifie qu'il existe un vecteur $e_1 \in P$ tel que $q(e_1)$ soit inversible dans A. La restriction q" de q au sous-A-module $A e_1$ de P est donc non dégénérée et, par suite (P,q) est la somme orthogonale de $(A e_1, q")$ et d'un A-module quadratique (P',q') de rang n-1. D'après l'hypothèse de récurrence, il existe une base orthogonale $\{e_2,\ldots,e_n\}$ de (P',q') donc $\{e_1,e_2,\ldots,e_n\}$ est une base orthogonale de (P,q).

Si 2 n'est pas inversible dans A, on considère une base $\{e_1,\ldots,e_n\}$ de P, $n \geq 2$, et soit $(\varphi(e_i,e_j))_{1 \leq i,\, j \leq n}$ la matrice de q relativement à cette base, où φ est la forme A-bilinéaire symétrique associée à q. Comme q est non dégénérée, cette matrice est inversible donc il existe au moins un couple d'indices (i,j) tel que $\varphi(e_i,e_j) \notin \mathfrak{m}$. Comme $\varphi(x,x) = 2q(x)$, on a $i \neq j$; on peut supposer que $i = 1$ et $j = 2$. La restriction q' de q au sous-A-module $P' = A e_1 \oplus A e_2$ a pour matrice $\begin{pmatrix} 2\,q(e_1) & \varphi(e_1,e_2) \\ \varphi(e_1,e_2) & 2\,q(e_2) \end{pmatrix}$, qui est inversible. Ceci nous montre que $(P,q) \approx (P',q') \perp (P'^{\perp}, q")$, où q" est la restriction de q à $P'^{\perp}$ et le rang de $P'^{\perp}$ est n-2. Pour le début de la récurrence, il suffit de remarquer que si $n = 0$, il n'y a rien à démontrer et qu'on ne peut pas avoir $n = 1$, car $2 \in \mathfrak{m}$.

Si A est un anneau local dans lequel 2 est inversible et si a est un élément inversible de A, on notera $< a >$ le A-module quadratique (A,q), où $q : A \mapsto A$ est de la forme quadratique définie par $x \mapsto a x^2$. Si $a_1,\ldots,a_n$ sont des éléments inversibles de A, $< a_1 > \perp \ldots \perp < a_n >$ est le A-module quadratique (A^n,q), où $q : A^n \to A$ est de la forme quadratique définie $(x_1,\ldots,x_n) \mapsto \sum_{i=1}^{n} a_i x_i^2$. Le théorème 1.11.2. nous dit que tout A-module quadratique de rang n est de la forme $< a_1 > \perp \ldots \perp < a_n >$, où $a_1,\ldots,a_n$ sont des éléments inversibles de A.

On dira qu'une A-algèbre commutative A' est fidèlement plate si A' est un A-module plat et si pour tout A-module M, la condition $A' \otimes_A M = 0$ entraîne $M = 0$. Ceci équivaut encore à dire qu'une suite de A-modules $M' \to M \to M''$ est exacte si et seulement si la suite de A'-modules $A' \otimes_A M' \to A' \otimes_A M \to A' \otimes_A M''$ est exacte. On dira aussi que A' est une extension fidèlement plate de A. On a les propriétés suivantes : (i) Pour qu'un A-module P soit projectif de type fini il faut et il suffit que le A'-module $A' \otimes_A P$ soit projectif de type fini. (ii) Pour qu'une application A-linéaire $f : M \to N$ soit un isomorphisme, il faut et il suffit que l'application A'-linéaire $id_{A'} \otimes f : A' \otimes_A M \to A' \otimes_A N$ soit un isomorphisme. (iii) Soient P un A-module, $q : P \to A$ une forme A-quadratique et $q' : A' \otimes_A P \to A'$ la forme A'-quadratique obtenue par extension des scalaires. Alors (P,q) est un A-module quadratique si et seulement si $(A' \otimes_A P, q')$ est un A'-module quadratique.

Soit $\{f_1,\ldots,f_n\}$ un ensemble d'éléments de A engendrant l'idéal A, $S_{f_i} = \{1, f_i, f_i^2, \ldots, f_i^n, \ldots\}$ la partie multiplicative engendrée par f_i et $A_{f_i} = S_{f_i}^{-1} A$ l'anneau des fractions de A à dénominateurs dans S_{f_i}. La A-algèbre $A' = \prod_{i=1}^{n} A_{f_i}$ est appelée une extension de Zariski de A.

Si A' est une extension de Zariski de A, alors A' est une extension fidèlement plate de A. En effet, il est évident que A' est un A-module plat, car les A_{f_i} le sont. Soit, de plus, M un A-module tel que $A' \otimes_A M = 0$. Ceci équivaut à dire que $M_{f_i} = 0$ $(i = 1,\ldots,n)$, donc, pour tout idéal maximal $\mathfrak{m}$ de A, $M_{\mathfrak{m}} = 0$. Le lemme de globalisation nous dit alors que $M = 0$.

Le théorème précédent nous permet d'énoncer la proposition suivante :

Proposition 1.11.3. Soient A un anneau et (P,q) un A-module quadratique, où P est un A-module projectif de type fini et de rang constant. (i) Si 2 est inversible dans A, il existe une extension de Zariski A' de A telle que $A' \otimes_A (P,q)$ possède une base orthogonale. (ii) Si 2 n'est pas inversible dans A, il existe une extension de Zariski A' de A telle que $A' \otimes_A (P,q) = (A' \otimes_A P, q')$ a une décomposition en somme orthogonale de sous-modules quadratiques libres de rang 2 et tels que dans chaque sous-module, il existe au moins un vecteur x tel que $q'(x)$ est inversible dans A'.

La démonstration se fait par récurrence sur le rang n de P. Supposons d'abord que 2 est inversible dans A. Pour chaque idéal maximal $\mathfrak{m}$ de A, il existe, dans le $A_{\mathfrak{m}}$-module quadratique $A_{\mathfrak{m}} \otimes_A (P,q)$ une base orthogonale, en particulier,

un vecteur $\frac{x_m}{s_m}$, $x_m \in P$, $s_m \notin m$ tel que $q_m(\frac{x_m}{s_m})$ soit inversible dans A_m. Ceci signifie que pour chaque idéal maximal m de A, il existe un élément $f_m \notin m$ - ici, $f_m = s_m\, q(x_m)$ - tel que dans $P_{f_m} = A_{f_m} \otimes_A P$, il existe un élément y_m avec $q_{f_m}(y_m)$ inversible dans A_{f_m}. L'idéal de A engendré par les f_m n'est contenu dans aucun idéal maximal de A, donc il est égal à A et, par suite, il existe une sous-famille finie $f_1,\dots,f_p$ qui engendre A. Soient $x_i \in P_{f_i}$ l'élément associé à f_i tel que $q_{f_i}(x_i)$ soit inversible dans A_{f_i} $(i = 1,\dots,p)$, $A' = \prod_{i=1}^{p} A_{f_i}$ et $x = (x_i) \in A' \otimes_A P = \prod_{i=1}^{p} P_{f_i}$. On a $q'(x) = (q_{f_i}(x_i))$ qui est inversible dans A'. Comme 2 est inversible dans A, donc dans A', la restriction Q' de q' à $A'x$ est non dégénérée, donc $(A' \otimes_A P, q') = (A' x, Q') \perp (P'',Q'')$, où P'' est un A'-module projectif de rang $n-1$. D'après l'hypothèse de récurrence, il existe une extension de Zariski A'' de A' telle que $A'' \otimes_{A'} P''$ admet une base orthogonale $\{e_2,\dots,e_n\}$. En posant $e_1 = 1 \otimes x \in A'' \otimes_{A'} (A' \otimes_A P) \approx A'' \otimes_A P$, on voit que $\{e_1,e_2,\dots,e_n\}$ est une base orthogonale de $A'' \otimes_A P$. Il reste à remarquer que A'' est une extension de Zariski de A, par transitivité des extensions de Zariski.

Dans le cas où 2 n'est pas inversible, la démonstration se fait de façon analogue. En effet, pour chaque idéal maximal m de A, il existe un élément $f_m \notin m$ et une décomposition orthogonale de $A_{f_m} \otimes_A (P,q)$ en somme de sous-modules libres de rang 2. Comme les f_m engendrent l'idéal A, il existe une sous-famille finie $f_1,\dots,f_p$ qui l'engendre. On pose alors $A' = \prod_{i=1}^{p} A_{f_i}$, $A_{f_i} \otimes_A (P,q) = \perp_{j=1}^{n/2} (P_{ij},q_{ij})$, donc $A' \otimes_A (P,q) \approx \perp_{j=1}^{n/2} (\prod_{i=1}^{p} (P_{ij},q_{ij}))$, où $\prod_{i=1}^{p} P_{ij}$ est un plan de $A' \otimes_A (P,q)$ $(j = 1,\dots,n/2)$. De plus, dans chaque $\prod_{i=1}^{p} P_{ij}$, il existe un vecteur x_j tel que $q'(x_j)$ soit inversible dans A' et pour cela il suffit de prendre dans chaque P_{ij} $(1 \le i \le p)$ un vecteur x_{ij} satisfaisant à la condition voulue dans A_{f_i}. La démonstration s'achève à l'aide du lemme suivant :

Lemme 1.11.4. *Soient A un anneau, (P,q) un A-module quadratique, où P est un A-module projectif de type fini et de rang constant pair et m un idéal maximal de A. Il existe un élément f de A n'appartenant pas à m et une décomposition orthogonale de $A_f \otimes_A (P,q)$ en somme de sous-modules libres de rang 2 et telle que dans chaque plan, il existe au moins un vecteur x avec $q_f(x)$ inversible dans A_f.*

Si $2 \notin m$, $A_m \otimes_A (P,q)$ a une base orthogonale $\{e_1,\dots,e_n\}$ avec

$e_i = \frac{x_i}{s_i}$, $x_i \in P$, $s_i \notin \mathfrak{m}$ et $q(x_i) \notin \mathfrak{m}$ $(i = 1,\ldots,n)$. Il suffit alors de prendre $f = \prod_{i=1}^{n} s_i\, q(x_i)$ et les éléments $e_1,\ldots,e_n$ forment une base orthogonale de $A_f \otimes_A (P,q)$, d'où le résultat voulu.

Supposons maintenant que $2 \in \mathfrak{m}$: il existe dans $A_{\mathfrak{m}} \otimes_A P$ des éléments e_i, f_i $(i = 1,\ldots,n)$, $e_i = \frac{x_i}{s_i}$, $f_i = \frac{y_i}{t_i}$ avec $x_i, y_i \in P$, $s_i, t_i \notin \mathfrak{m}$ et tels que $A_{\mathfrak{m}} \otimes_A (P,q)$ soit la somme orthogonale des plans (P_i,q_i) $(i = 1,\ldots,\frac{n}{2})$, où $P_i = A\, e_i \oplus A\, f_i$ et q_i est la restriction de q à P_i. De plus, $q_{\mathfrak{m}}(e_i)$ est inversible dans $A_{\mathfrak{m}}$. Soit alors $d_i = 4\, q(x_i)\, q(y_i) - \varphi(x_i,y_i)^2$ $(i = 1,\ldots,\frac{n}{2})$, où φ est la forme A-bilinéaire associée à q. Comme la restriction de $q_{\mathfrak{m}}$ à P_i est non-dégénérée, $d_i \notin \mathfrak{m}$ $(i = 1,\ldots,n)$ et il suffit de prendre $f = \prod_{i=1}^{n/2} s_i t_i d_i\, q(x_i)$ pour obtenir un élément qui n'est pas dans $\mathfrak{m}$ et tel que les sous-A_f-modules $A_f\, x_i \oplus A_f\, y_i$ de $A_f \otimes_A P$ sont des plans non dégénérés deux à deux orthogonaux. Ainsi, $A_f \otimes_A (P,q)$ est bien la somme orthogonale de sous-modules libres de rang 2 et tels que dans chacun d'eux il existe un élément x avec $q_f(x)$ inversible dans A_f.

Proposition 1.11.5. Soient A un anneau et (P,q) un A-module quadratique où P est un A-module projectif de type fini et de rang constant pair. Il existe une extension fidèlement plate A' de A telle que $A' \otimes_A (P,q)$ soit un A'-espace hyperbolique.

D'après la transitivité des extensions fidèlement plates, on peut supposer (cf. Proposition 1.11.3.) que P est un A-module libre de rang 2, de base $\{e_1,e_2\}$ avec $q(e_1) \in U(A)$. On a $q(x\, e_1 + y\, e_2) = a\, x^2 + b\, x\, y + c\, y^2$, $a = q(e_1) \in$ $\in U(A)$, $b = q(e_2)$, $c = \varphi(e_1,e_2)$ et $b^2 - 4\, ac \in U(A)$. Alors $A' = A[t]$ avec $t^2 +$ $+ a^{-1} b\, t + a^{-1}\, c = 0$ est une extension quadratique de A (cf. 2.4.) ; A' est une A-algèbre fidèlement plate. Notons $q' = A' \otimes_A P \to A'$ la forme A'-quadratique obtenue par extension des scalaires. On a $q'(t \otimes e_1 + 1 \otimes e_2) = a\, t^2 + b\, t + c = 0$ et si l'on prend $f_1 = t \otimes e_1 + 1 \otimes e_2$ comme vecteur faisant partie d'une base de $A' \otimes_A P$ en tant que A'-module, on a $q'(x\, f_1 + y\, f_2) = b'\, x\, y + c'\, y^2 = y(b'\, x +$ $+ c'\, y)$ avec $b', c' \in A'$ et $b' \in U(A')$. Il suffit maintenant de modifier f_2 pour achever la démonstration.

On voit que, en fait, dans le cas général, il faut faire une extension de Zariski puis une suite d'extensions quadratiques.

Remarquons que si P est un A-module de rang impair, quitte à faire une

extension de Zariski de A, on peut supposer que P est un A-module libre ayant une base orthogonale $\{e_1,\ldots,e_{2n+1}\}$. Soient alors $a_i = q(e_{2i-1})q(e_{2i})$ $(i = 1,\ldots,n)$ et $A' = A[\sqrt{-a_1}, \ldots, \sqrt{-a_n}]$. On voit que $A' \otimes_A (P,q)$ est la somme orthogonale d'un A-espace hyperbolique et d'un A'-module libre de rang 1.

1.12. GROUPES ET TRANSFORMATIONS ORTHOGONALES

Soit (P,q,N) un objet de $\mathcal{C}'(N)$, où N est projectif de type fini et de rang 1. Une application linéaire s de P dans P sera appelée <u>transformation orthogonale</u> de (P,q,N) si pour tout élément x de P, $q(s(x)) = q(x)$. Comme q est strictement non dégénérée, s est un automorphisme de A-modules. En effet, s conserve l'application bilinéaire symétrique φ associée à q et on a le diagramme commutatif :

$$\begin{array}{ccc} P & \xrightarrow{d_\varphi} & \mathrm{Hom}_A(P,N) \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle t_s} \\ P & \xrightarrow{d_\varphi} & \mathrm{Hom}_A(P,N) \end{array}$$

Si s et s' deux transformations orthogonales de (P,q,N), $s \circ s'$ et s^{-1} sont encore des transformations orthogonales ; id_P est aussi une transformation orthogonale. L'ensemble des transformations orthogonales de (P,q,N) est donc un sous-groupe du groupe linéaire de P qu'on appellera <u>groupe orthogonal</u> de (P,q,N) et qu'on notera $\mathcal{O}(P,q)$ (ou $\mathcal{O}(q)$, ou $\mathcal{O}(P)$).

<u>Exemples</u>. 1.12.1. Une homothétie $x \mapsto \lambda x$ est dans $\mathcal{O}(P,q)$ si et seulement si $\lambda^2 = 1$.

1.12.2. Supposons que $N = A$ et soit $x \in P$ un élément tel que $q(x) \in U(A)$. Alors la transformation $t_x : P \to P$ définie par $y \mapsto y - x\, q(x)^{-1} \varphi(x,y)$ est une transformation orthogonale appelée <u>transvection de vecteur</u> x. Si 2 est inversible dans A, $(P,q) \approx (Ax, q_{|Ax}) \perp (P',q')$, car la restriction de q à Ax est strictement non dégénérée ; t_x a alors la décomposition $t_x = -\mathrm{id}_{Ax} \oplus \mathrm{id}_P$, et c'est donc la <u>symétrie par rapport à l'hyperplan orthogonal à</u> x.

1.12.3. Le groupe orthogonal d'une somme $(P,q) \perp (P',q')$ contient un sous-groupe isomorphe au produit direct $\mathcal{O}(P) \times \mathcal{O}(P')$: c'est le sous-groupe formé des matrices $\begin{pmatrix} s & 0 \\ 0 & s' \end{pmatrix}$, où s et s' sont deux transformations orthogonales de P et P' respecti-

vement.

1.12.4. Soit $h(P,N)$ un espace hyperbolique. Alors $\mathcal{O}(h(P,N))$ contient un sous-groupe isomorphe au groupe linéaire de P. En effet, si $u : P \to P$ est un automorphisme de P, ${}^t(u^{-1})(f)(u(x)) = f(u^{-1}(u(x))) = f(x)$, donc la matrice $M(u) = \begin{pmatrix} u & 0 \\ 0 & {}^t(u^{-1}) \end{pmatrix}$ est une transformation orthogonale de $h(P,N)$. L'application $u \mapsto M(u)$ est un isomorphisme de $G\ell(P)$ dans $\mathcal{O}(h(P,N))$.

On appelle $\mathcal{O}(n,A)$ le groupe orthogonal de l'espace hyperbolique $h(A^n)$. L'inclusion naturelle $\varphi_{n,p}$ de $h(A^n)$ dans $h(A^{n+p})$, $p \geq 0$, obtenue en identifiant A^n au sous-module de A^{n+p} dont les p dernières coordonnées sont nulles, induit une injection de $\mathcal{O}(n,A)$ dans $\mathcal{O}(n+p,A)$, $u \mapsto \begin{pmatrix} u & 0 \\ 0 & id_{h(A^p)} \end{pmatrix}$. On appelle groupe orthogonal général et on note $\mathcal{O}(A)$, la limite inductive des groupes $\mathcal{O}(n,A)$ munis des homomorphismes $\varphi_{n,p}$. Tout groupe orthogonal d'un module quadratique (P,q) se plonge dans $\mathcal{O}(A)$. En effet, (P,q) est toujours facteur orthogonal d'un espace $h(A^n)$, car si $P \oplus P' \approx A^n$, on a l'isomorphisme $(P,q) \perp (P,-q) \perp h(P') \approx h(A^n)$.

1.12.5. Déterminant d'un automorphisme orthogonal. Si A est de caractéristique 2 et si (P,q) est un A-module quadratique, la forme bilinéaire symétrique φ associée est alternée : le groupe orthogonal $\mathcal{O}(P,q)$ est un sous-groupe du groupe des transformations linéaires qui laissent φ invariante. Or, on sait (cf. [10], par exemple) que le déterminant d'un tel automorphisme est 1. Le déterminant d'une transformation orthogonale est donc toujours égal à 1 dans ce cas.

Dans le cas général, si $s \in \mathcal{O}(P)$ est si n est un entier, $\Lambda^n s$ est un automorphisme de la puissance extérieure $n^{\text{ième}}$, $(\Lambda^n P, \Lambda^n \varphi)$. En particulier, l'homothétie de rapport dét(s) laisse dét(P,q) invariant. On a donc $(\text{dét } s)^2 = 1$ et le déterminant d'une transformation orthogonale est une racine carrée de l'unité. Si 2 est inversible dans A, on a un isomorphisme naturel entre le groupe $\mu_2(A)$ des racines carrées de l'unité de A et le groupe $Ip(A)$ des idempotents de A par $u \mapsto \frac{1}{2}(1-u)$ et $e \mapsto 1-2e$, $u \in \mu_2(A)$ et $e \in Ip(A)$. On obtient donc par l'homomorphisme déterminant, un homomorphisme de $\mathcal{O}(P,q)$ dans $Ip(A)$. Son noyau est le groupe spécial orthogonal de (P,q) et nous verrons, au chapitre 2, comment on peut se passer de l'hypothèse 2 inversible pour définir cet homomorphisme (cf. 2.8.14.).

Si 2 est inversible dans A, le déterminant d'une transvection t_x est égal à -1, comme le montre la décomposition de t_x en $-id_{AX} \oplus id_{(Ax)^\perp}$. Rappelons le théorème suivant (cf. [17]) :

Théorème 1.12.1. Si A est un corps, le groupe orthogonal d'un A-module quadratique (P,q) est engendré par les transvections. De façon précise, si n est la dimension de P sur A, toute transformation orthogonale est produit d'au plus n transvections, excepté dans le cas où $(P,q) \simeq h((\mathbb{Z}/(2))^2)$.

1.13. THEOREME DE SIMPLIFICATION DE WITT

Avant de passer au théorème de Witt, nous allons démontrer le lemme suivant :

Lemme 1.13.1. Soit x un élément unimodulaire du A-module quadratique (P,q) tel que $q(x) = 0$. Si q est strictement non dégénérée, il existe un élément y de P tel que $q(y) = 0$ et $\varphi(x,y) = 1$. Le sous-module engendré par x et y est strictement non dégénérée et isomorphe à l'espace hyperbolique h(A).

En effet, comme x est unimodulaire (i.e., il existe $f \in P^*$ tel que $f(x) = 1$), il existe $z \in P$ tel que $\varphi(x,z) = 1$, car q est strictement non dégénérée ; il suffit alors de prendre $y = z - q(z)x$ et il est clair que le sous-module engendré par x et y est libre de rang 2. La restriction q' de q à ce sous-module est strictement non dégénérée, car la matrice de $d_{\varphi'}$ est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ en prenant pour base du dual la base duale de $\{x,y\}$. L'isomorphisme de h(A) sur $(Ax \oplus Ay, q')$ s'obtient en envoyant 1 sur x et 1^* sur y. Le couple $\{x,y\}$ s'appelle alors une paire hyperbolique.

Une question naturelle se pose quand on définit le groupe de Witt-Grothendieck d'un anneau A : le monoïde abélien E(A) des classes d'isomorphismes de modules quadratiques est-il simplifiable ? En d'autres termes, ce monoïde s'injecte-t-il dans son groupe universel WG(A), c'est à dire, est-ce que deux modules quadratiques (P_1,q_1) et (P_2,q_2) qui ont même classe dans WG(A) sont isomorphes ? La réponse générale ne peut être que négative ; il y a cependant des cas importants où le résultat est vrai, à savoir si A est un corps ou un anneau semi-local.

Dire que (P_1,q_1) et (P_2,q_2) ont même classe dans WG(A) signifie qu'il existe (P,q) objet de $\mathcal{C}'(A)$ tel que $(P_1,q_1) \perp (P,q) \approx (P_2,q_2) \perp (P,q)$, et le problème est de savoir quand on peut simplifier cet isomorphisme par (P,q). Il est équivalent de dire qu'on peut simplifier quand (P,q) est un espace hyperbolique puisqu'on peut rajouter (P,-q) aux termes de l'isomorphisme et que $h(P) \approx (P,q) \perp (P,-q)$. On peut alors supposer que P est libre de type fini car il

existe P' projectif de type fini tel que $P \oplus P' \approx A^n$ et donc $h(P) \perp h(P') \approx$ $\approx h(A^n)$. Comme $h(A^n)$ est somme orthogonale de n espaces $h(A)$, il suffit finalement de montrer qu'on peut simplifier par le plan hyperbolique $h(A)$. Identifiant les deux modules quadratiques $E_1 = (P_1,q_1) \perp h(A)$ et $E_2 = (P_2,q_2) \perp h(A)$, on voit que le problème de la simplification consiste à montrer que le groupe orthogonal d'un module quadratique opère transitivement sur l'ensemble des paires hyperboliques.

Théorème 1.13.2. Le groupe orthogonal d'un module quadratique sur un corps A opère transitivement sur l'ensemble des paires hyperboliques.

Soient $\{x,y\}$ et $\{x',y'\}$ deux paires hyperboliques dans un module quadratique E et soient P et P' les plans hyperboliques correspondants. Nous allons montrer qu'il existe toujours $\sigma \in \mathcal{O}(E)$ tel que $\sigma(x) = x'$. C'est clair si x et x' sont dépendants car $x' = ax$ et il suffit de prendre pour σ l'identité sur l'orthogonal de P, $\sigma(x) = x'$ et $\sigma(y) = a^{-1}y$. Si x et x' sont indépendants et si $\varphi(x,x')$ n'est pas nul, on note R le plan hyperbolique $Ax \oplus Ax'$ et on prend pour σ l'identité sur $R^\perp$, $\sigma(x) = x'$ et $\sigma(x') = x$. Si x et x' sont indépendants et $\varphi(x,x') = 0$, il existe z dans E tel que $\varphi(x,z)$ et $\varphi(x',z)$ sont tous deux non nuls. Remplaçant z par $z + cx$ avec un c convenable, on peut supposer que $q(z) = 0$. On peut donc envoyer d'abord x sur z puis z sur x' par des transformations orthogonales, d'où le résultat voulu.

On suppose désormais que $x = x'$ et y' s'écrit alors $y' = y+z$. Si $q(z)$ est non nul, la transvection $t_z : E \to E$ définie par $t_z(u) = u - zq(z)^{-1}\varphi(u,z)$ laisse x invariant car $\varphi(x,z) = 0$ et envoie y sur y' car $q(y') = \varphi(y,z) + q(z) = 0$. Si $q(z)$ est nul, z est un élément de $P^\perp$ et il existe t dans $P^\perp$ tel que $Az \oplus At$ est un plan hyperbolique R ; $P \perp R$ est isomorphe à $h(A^2)$ et il suffit de trouver une transformation orthogonale de $P \perp R$ qui conserve x et envoie y sur $y+z$. Il est facile de vérifier que $\sigma : P \perp R \to P \perp R$ définie par $\sigma(x) = x$, $\sigma(y) = y+z$, $\sigma(z) = z$ et $\sigma(t) = t-x$ répond bien à la question, d'où le théorème.

Notons que si la dimension de E est supérieur à 2, on peut se restreindre aux transformations du groupe spécial orthogonal.

En effet, si besoin est, on peut composer la transformation σ trouvée d'après le théorème précédent avec une transvection qui se réduit à l'identité sur P', c'est à dire définie par un vecteur z de $P'^\perp$ tel que $q(z) \neq 0$.

Dans le cas d'un anneau semi-local, on a le théorème suivant :

Théorème 1.13.3. Soient A un anneau semi-local et (P,q) un A-module quadratique. Le groupe orthogonal de (P,q) opère transitivement sur l'ensemble des paires hyperboliques. Si le rang de P est supérieur ou égal à 3, le groupe spécial orthogonal opère aussi transitivement sur les paires hyperboliques.

La seconde assertion est, comme pour les corps, une conséquence immédiate de la première. En ce qui concerne la première question, soit $B = A/\mathrm{Rad}\, A = \prod_{i=1}^{n} A/\mathfrak{m}_i$, où $\mathfrak{m}_i$ décrit l'ensemble fini des idéaux maximaux de A. Soient p et p' deux paires hyperboliques dans P, p_i et p_i' les paires déduites de celles-ci par extension des scalaires à $A/\mathfrak{m}_i$ et on suppose pour l'instant que le rang de P est supérieur ou égal à 3. Alors il existe dans chaque $P \otimes_A A/\mathfrak{m}_i$ une transformation orthogonale σ_i qui envoie p_i sur p_i' et qu'on peut supposer être produit d'un nombre pair de transvections, ce qui permet de supposer que ce nombre est indépendant de l'idéal maximal $\mathfrak{m}_i$ et $\sigma_i = \prod_{j=1}^{2q} t_{x_{i,j}}$. Posons alors $x_j = (x_{i,j})_i \in P \otimes_A B \approx \prod_{i=1}^{n} P \otimes_A A/\mathfrak{m}_i$. On a $q_B(x_j) = (q_{A/\mathfrak{m}_i}(x_{i,j})) \in U(B)$; on peut remonter x_j dans P en y_j et $q(y_j)$ est inversible dans A. Soit alors $\sigma = \prod_{j=1}^{2q} t_{y_j}$. Si l'on pose $p = \{x,y\}$ et $p' = \{x',y'\}$, on a $\sigma(x) \equiv x' \pmod{\mathrm{Rad}(A).P}$ et $\sigma(y) \equiv y' \pmod{\mathrm{Rad}(A).P}$ si bien qu'on est ramené à démontrer le théorème pour deux paires $\{x,y\}$ et $\{x',y'\}$ telles que $x \equiv x'$ et $y \equiv y' \pmod{\mathrm{Rad}(A).P}$. On a alors $q(y-x') = -\varphi(y,x') \in U(A)$ et on vérifie que $t_{y-x'}(x') = y$ et que $t_{x-y}(y) = x$, donc on peut supposer que $x = x'$. On écrit alors $y' = y + ax + t$ avec $t \in (Ax \oplus Ay)^{\perp}$, où $a = -q(t)$ puisque $q(y') = 0$. Soit alors E_t la transformation (introduite par Eichler dans le cas d'un corps ; cf. [45]) définie par : $E_t(x) = x$, $E_t(y) = y - xq(t) + t$, $E_t(z) = z + \varphi(z,t)x$, si $z \in (Ax \oplus Ay)^{\perp}$. Il est immédiat de vérifier que E_t est orthogonale et que $E_t(y + ax + t) = y$. Comme $E_t(x) = x$, la démonstration est achevée dans ce cas. Si le rang de P n'est pas supérieur ou égal à 3, on se ramène tout d'abord au cas où P est de rang constant en décomposant A en un produit d'anneau semi-locaux indécomposables et il ne reste plus que le cas où $P \approx Ax \oplus Ay \approx Ax' \oplus Ay'$; il suffit d'envoyer x sur x' et y sur y' pour obtenir le résultat annoncé.

Corollaire 1.13.4. Si A est semi-local, le monoïde $E(A)$ des classes d'isomorphismes de modules quadratiques s'injecte dans le groupe de Witt-Grothendieck de A.

C'est la réponse à la question que nous nous sommes posés au début du paragraphe.

Dans le cas des corps, le théorème de Witt ramène la classification des

formes quadratiques à celle des formes dites anisotropes. Un A-module quadratique (P,q), où A est un corps, sera dit anisotrope si le seul vecteur x tel que $q(x) = 0$ est le vecteur nul. Sinon P est dit isotrope ou encore, on dit que q représente 0. On a alors la proposition suivante :

Proposition 1.13.5. Si A est un corps, tout A-module quadratique (P,q) possède une décomposition orthogonale $(P,q) \approx h(A^r) \perp (P',q')$, où (P',q') est anisotrope. La classe d'isomorphisme de (P',q') et l'entier r ne dépendent que du module (P,q).

La démonstration se fait par récurrence sur la dimension de P sur A. Elle est claire si le rangde P est 1 ou 2. Si le rang de P est supérieur à 2 et P anisotrope, c'est terminé et $r = 0$. Si q représente 0, le lemme 1.13.1. montre que $(P,q) \approx h(A) \perp (P'',q'')$ et (P'',q'') a, d'après l'hypothèse de récurrence, une décomposition du type voulu, d'où la décomposition orthogonale annoncée. Si on a $(P,q) \approx h(A^{r_1}) \perp (P_1',q_1') \approx h(A^{r_2}) \perp (P_2',q_2')$ et $r_1 \neq r_2$, par exemple $r_1 < r_2$, $h(A^{r_2}) \approx h(A^{r_1}) \perp h(A^{r_2-r_1})$ et d'après le théorème de simplification, $h(A^{r_2-r_1}) \perp (P_2',q_2') \approx (P_1',q_1')$. Mais comme (P_1',q_1') est anisotrope, $h(A^{r_2-r_1}) = 0$, donc $r_1 = r_2$ et $(P_1',q_1') \approx (P_2',q_2')$, d'où la proposition. L'entier r s'appelle l'indice de (P,q).

Notons que l'image de (P,q) dans le groupe de Witt de A est la même que celle de (P',q'). Ainsi, le groupe de Witt d'un corps A peut être défini comme l'ensemble des classes d'isomorphismes de modules quadratiques anisotropes.

1.14. AUTOUR DU SATZ 7 DE WITT

L'existence, pour un A-module quadratique sur un anneau local de caractéristique résiduelle différente de 2, d'une base orthogonale (cf. 1.11.), montre que l'anneau de Witt-Grothendieck $WG(A)$ est le quotient de l'anneau de groupe $\mathbb{Z}[U(A)/U^2(A)]$ par l'idéal engendré par les éléments de la forme $(\bar{a}_1+\ldots+\bar{a}_n) - (\bar{b}_1+\ldots+\bar{b}_n)$, où les a_i et b_i sont dans $U(A)$ et où la barre désigne la classe modulo $U^2(A)$. De plus, les formes quadratiques $\langle a_1,\ldots,a_n\rangle : A^n \to A$ et $\langle b_1,\ldots,b_n\rangle : A^n \to A$ définie respectivement par $(x_1,\ldots,x_n) \mapsto \sum_{i=1}^{n} a_i x_i^2$ et $(x_1,\ldots,x_n) \mapsto \sum_{i=1}^{n} b_i x_i^2$ ont même classe dans le groupe de Witt-Grothendieck. Remarquons que cette dernière assertion est naturellement équivalente à dire que les A-modules quadratiques $(A^n, \langle a_1,\ldots,a_n\rangle)$ et $(A^n, \langle b_1,\ldots,b_n\rangle)$ sont isomorphes, d'après le théorème de simplification pour les formes quadratiques (cf. 1.13.).

Nous voulons montrer ici que l'idéal noyau de l'homomorphisme $\mathbb{Z}[U(A)/U^2(A)] \to WG(A)$ est engendré (en tant que groupe abélien) par les éléments de la forme $(\bar{a}_1 + \bar{a}_2) - (\bar{b}_1 + \bar{b}_2)$ et pour cela, nous allons montrer un résultat dû à Witt.

Soit (P,q) un A-module quadratique, $B = \{e_1,\dots,e_n\}$ et $B' = \{e'_1,\dots,e'_n\}$ deux bases orthogonales de (P,q). On dira que B et B' sont contiguës s'il existe une suite de bases orthogonales $B_0 = B, B_1,\dots,B_p = B'$ telle que B_{i+1} ne diffère de B_i que par deux éléments au plus. Notons que la contiguïté est une relation d'équivalence sur l'ensemble des bases orthogonales de (P,q).

Proposition 1.14.1. Deux bases orthogonales d'un A-module quadratique (P,q) sur un anneau local A de caractéristique résiduelle différente de 2 sont contiguës.

Soit n le rang de P ; le résultat est clair si $n \leq 2$. Supposons-le vrai pour n-1 et soient B et B' deux bases orthogonales de P sur A, $B = \{e_1,\dots,e_n\}$ et $B' = \{e'_1,\dots,e'_n\}$. Parmi les bases contiguës à B, choisissons $\bar{B} = \{\bar{e}_1,\dots,\bar{e}_n\}$ l'une des bases dans lesquelles e'_1 est combinaison linéaire du plus petit nombre p de vecteurs de $\bar{B}$. Alors $p = 1$. En effet, si p était égal à 2 et $e'_1 = a_1 \bar{e}_1 + a_2 \bar{e}_2$, par exemple, alors le sous-A-module $A\,\bar{e}_1 \oplus A\,\bar{e}_2$ de P possèderait une base orthogonale $\{e'_1, e''_2\}$ et la base orthogonale $\{e'_1, e''_2, \bar{e}_3,\dots,\bar{e}_n\}$ serait contiguë à B, contredisant la minimalité de p. Supposons donc $p > 2$ et soit $e'_1 = a_1 \bar{e}_1 + \dots + a_p \bar{e}_p$. Comme $q(e'_1)$ est inversible, l'un des a_i au moins est inversible car sinon $q(e'_1) = \sum_{i=1}^{p} a_i^2 q(\bar{e}_i)$ serait dans l'idéal maximal $\mathfrak{m}$ de A. Supposons donc $a_1,\dots,a_q \notin \mathfrak{m}$ et $a_{q+1},\dots,a_p \in \mathfrak{m}$. Alors $q = p$. En effet, si cela n'est pas le cas, on considère le vecteur $e''_1 = a_1 \bar{e}_1 + a_p \bar{e}_p$; $q(e''_1)$ est inversible dans A et $A\,\bar{e}_1 \oplus A\,\bar{e}_p$ a une base orthogonale de la forme $\{e''_1, e''_p\}$. Alors $\{e''_1, \bar{e}_2,\dots,\overline{e_{p-1}}, e''_p, \overline{e_{p+1}},\dots,\bar{e}_n\}$ est une base orthogonale contiguë à B et $e'_1 = e''_1 + a_2 \bar{e}_2 + \dots + a_{p-1} \overline{e_{p-1}}$, ce qui contredit la minimalité de p. On a donc $q = p$, c'est à dire que tous les a_i sont inversibles. Considérons alors les trois vecteurs $f_1 = a_2 \bar{e}_2 + a_3 \bar{e}_3$, $f_2 = a_3 \bar{e}_3 + a_1 \bar{e}_1$ et $f_3 = a_1 \bar{e}_1 + a_2 \bar{e}_2$. Dans ces conditions, l'un des trois éléments $q(f_1)$, $q(f_2)$ ou $q(f_3)$ est inversible, car sinon, la somme $q(f_1) + q(f_2) + q(f_3)$ serait aussi dans $\mathfrak{m}$ et comme 2 est inversible dans A, il en serait de même de $a_1^2 q(\bar{e}_1) + a_2^2 q(\bar{e}_2) + a_3^2 q(\bar{e}_3)$. Or, $q(f_1) = a_2^2 q(\bar{e}_2) + a_3^2 q(\bar{e}_3) \in \mathfrak{m}$, donc $a_1^2 q(\bar{e}_1) \in \mathfrak{m}$ et par suite $a_1 \in \mathfrak{m}$ ce qui est impossible comme on l'a vu plus haut.

Supposons donc $q(f_3) \notin \mathfrak{m}$; $A\,\bar{e}_1 \oplus A\,\bar{e}_2$ possède une base orthogonale $\{f_3, f'_3\}$ et dans la base $\{f_3, f'_3, \bar{e}_3,\dots,\bar{e}_n\}$ contiguë à B, $e'_1 = f_3 + a_3 \bar{e}_3 + \dots + a_p \bar{e}_p$ n'est combinaison linéaire que de p-1 vecteurs ce qui contredit la minimalité de p. On a donc montré que $p = 1$, c'est à dire que B est contiguë

à une base $B'' = \{e'_1, e''_2, \ldots, e''_n\}$. Mais alors $\{e'_2, \ldots, e'_n\}$ et $\{e''_2, \ldots, e''_n\}$ sont deux bases orthogonales d'un même module quadratique de rang n-1, l'orthogonal dans P de $A\,e'_1$. D'après l'hypothèse de récurrence, ces deux bases orthogonales sont contiguës, ce qui entraîne que B'' et B' le sont aussi, d'où le résultat voulu.

L'argument est encore valable pour les modules quadratiques sur les anneaux semi-locaux dans lesquels 2 est inversible.

Proposition 1.14.2. *Le noyau de l'homomorphisme* $\mathbb{Z}[U(A)/U^2(A)] \to WG(A)$ *est engendré par les éléments de la forme* $(\bar{a}_1 + \bar{a}_2) - (\bar{b}_1 + \bar{b}_2)$ *tels que les* A*-modules quadratiques* $\langle a_1\rangle \perp \langle a_2\rangle$ *et* $\langle b_1\rangle \perp \langle b_2\rangle$ *sont isomorphes (éléments du type* α_2*).*

On a vu plus haut que le noyau de cet homomorphisme était engendré par les éléments $\alpha = (\bar{a}_1 + \ldots + \bar{a}_n) - (\bar{b}_1 + \ldots + \bar{b}_n)$, où $a_i, b_i \in U(A)$ et les formes quadratiques $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^{n} a_i x_i^2$ et $(y_1, \ldots, y_n) \mapsto \sum_{j=1}^{n} b_j y_j^2$ sont isomorphes. Dans $(P,q) = \langle a_1\rangle \perp \ldots \perp \langle a_n\rangle$, l'isomorphisme précédent signifie que nous avons deux bases orthogonales $B = \{e_1, \ldots, e_n\}$ et $B' = \{f_1, \ldots, f_n\}$ avec $q(e_i) = a_i$ et $q(f_j) = b_j$. D'après la proposition précédente, il existe une suite $B_0 = B, B_1, \ldots, B_p = B'$ de bases orthogonales telles que B_{i+1} ne diffère de B_i que par deux éléments au plus. A B_i est associé un élément u_i de $\mathbb{Z}[U(A)/U^2(A)]$ comme suit : si $B_i = \{e_1^{(i)}, \ldots, e_n^{(i)}\}$, $u_i = \sum_{j=1}^{n} q(e_{j_{p-1}}^{(i)})$, de sorte que $u_0 = \bar{a}_1 + \ldots + \bar{a}_n$ et $u_p = \bar{b}_1 + \ldots + \bar{b}_n$. Alors $\alpha = u_0 - u_p = \sum_{i=0} (u_i - u_{i+1})$. Or, par définition $u_i - u_{i+1}$ est du type α_2. On a donc bien montré que les éléments du type α_2 engendrent le noyau de l'homomorphisme $\mathbb{Z}[U(A)/U^2(A)] \to WG(A)$.

Remarquons que dans aucune des deux propositions précédentes, nous n'avons utilisé le théorème de simplification.

En caractéristique 2, il existe un résultat analogue à la proposition 1.14.1, signalé dans un article de I. Kaplansky et R. Shaker (cf. [25]). Nous supposerons pour simplifier que A est un corps de caractéristique 2 bien que le résultat soit vrai pour un anneau local de caractéristique résiduelle 2. Soient alors (P,q) un A-module quadratique, $\mathcal{P} = (P_1,q_1) \perp \ldots \perp (P_n,q_n)$ et $\mathcal{P}' = (P'_1,q'_1) \perp \ldots \perp (P'_n,q'_n)$ deux décompositions orthogonales de (P,q) en somme de plans (i.e., sous-modules de dimension 2). On définit, comme au paragraphe précédent, une équivalence entre $\mathcal{P}$ et $\mathcal{P}'$ en disant que $\mathcal{P}$ et $\mathcal{P}'$ sont *contiguës* s'il existe une suite $\mathcal{P}_0 = \mathcal{P}, \mathcal{P}_1, \ldots, \mathcal{P}_m = \mathcal{P}'$ de décompositions orthogonales de (P,q) et si l'on passe de $\mathcal{P}_i$ à $\mathcal{P}_{i+1}$ en changeant au plus deux éléments de la décomposition orthogonale $\mathcal{P}_i$. On a alors :

Proposition 1.14.3. Si A est un corps de caractéristique 2, deux décompositions orthogonales d'un A-module quadratique sont contiguës.

Rappelons tout d'abord que dans un A-module quadratique (P,q) pour que deux vecteurs x et y engendrent un plan facteur orthogonal de P, il faut et il suffit que $\varphi(x,y)$ soit non nul. Cela provient de ce que la forme bilinéaire symétrique φ associée à la forme quadratique q est alternée.

La démonstration se fait par récurrence sur le rang $2n$ de P, le résultat étant clair pour $n \leq 2$. On supposera donc le résultat vrai pour le rang $2n-2$ et il suffit, d'après l'hypothèse de récurrence, de montrer qu'il existe une décomposition orthogonale $\mathcal{P}'' = (P_1',q_1') \perp (P_2'',q_2'') \perp \ldots \perp (P_n'',q_n'')$ équivalente à $\mathcal{P} = (P_1,q_1) \perp (P_2,q_2) \perp \ldots \perp (P_n,q_n)$. Pour cela, soit $\{e_i,f_i\}$ une base de P_i et $\{e_j',f_j'\}$ une base de P_j' pour lesquelles on imposera $\varphi(e_i,f_i) = \varphi(e_j',f_j') = 1$, $1 \leq i, j \leq n$. Considérons e_1' : il existe un indice i et un vecteur $x = e_i$ ou f_i tel que $\varphi(e_1',x) \neq 0$. Quitte à permuter les P_i puis e_1 et f_1, on peut supposer que $x = f_1$. Cela signifie que $e_1' = a\,e_1 + b\,f_1 + p_2 + \ldots + p_n$ avec a et b dans A, $a \neq 0$ et $p_i \in P_i$ pour $i \geq 2$. On peut changer de base dans P_1 (i.e., remplacer e_1 par $e_1 + b\,a^{-1} f_1$) et supposer que $e_1' = a\,e_1 + p_2 + \ldots + p_n$. Posons alors $e_1^{(k)} = e_1 + a^{-1}(p_2 + \ldots + p_k)$, $2 \leq k \leq n$. Le sous-espace $P_1^{(2)} = A\,e_1^{(2)} \oplus A\,f_1$ est un sous-espace non dégénéré de $P_1 \perp P_2$ qui s'écrit donc $P_1^{(2)} \perp P_2^{(2)}$; $\mathcal{P}$ est donc équivalente à la décomposition $P_1^{(2)} \perp P_2^{(2)} \perp P_3 \ldots \perp P_n$ et e_1' s'écrit alors $a\,e_1^{(2)} + p_3 + \ldots + p_n$. Considérant maintenant $P_1^{(3)} = A\,e_1^{(3)} \oplus A\,f_1$, on peut continuer et ainsi on trouve finalement une décomposition $R_1 \perp \ldots \perp R_n$ équivalente à $\mathcal{P}$ avec $R_1 = A\,e_1^{(n)} \oplus A\,f_1$, c'est à dire avec $e_1' = a\,e_1^{(n)}$. Quitte à remplacer f_1 par $a^{-1}f_1$, on suppose $e_1' = e_1^{(n)}$. Alors f_1' s'écrit $\alpha\,e_1^{(n)} + f_1 + q_2 + \ldots + q_n$, où $q_i \in R_i$ pour $i \geq 2$. Posant alors $f_1^{(k)} = \alpha\,e_1^{(n)} + f_1 + q_2 + \ldots + q_k$, $2 \leq k \leq n$, on peut à l'aide de $A\,e_1' \oplus A\,f_1^{(k)}$ trouver une suite de décompositions orthogonales équivalentes à $\mathcal{P}$ dont l'aboutissement est $P_1'' \perp \ldots \perp P_n''$ avec $P_1'' = P_1'$.

Corollaire 1.14.4. Soit E l'ensemble des classes d'isomorphismes de A-modules quadratiques de rang 2. Le groupe $WG(A)$ est le quotient du groupe libre $\mathbb{Z}^{(E)}$ par le sous-groupe H engendré par les éléments de la forme $[P_1] + [P_2] - [P_3] - [P_4]$ tels que $P_1 \perp P_2 \simeq P_3 \perp P_4$ avec $[P_i] \in E$ $(i = 1,2,3,4)$.

On n'a malheureusement pas de critères simples permettant de savoir si deux formes de rang 4 sont équivalentes. Il est bien entendu nécessaire que

invariants d'Arf et algèbres de Clifford soient les mêmes mais cela n'est pas suffisant (cf. 2.7.).

1.15. GROUPES DE WITT D'UN CORPS DE CARACTERISTIQUE 2

Si A est un corps de caractéristique 2, l'existence d'une décomposition d'un module quadratique en somme orthogonale de plans (modules quadratiques de rang 2) montre que WG(A) est un quotient du groupe abélien $\mathbb{Z}^{(E(A))}$ où E(A) est l'ensemble des classes d'isomorphismes de plans (cf. 1.14.4). Nous donnons ici, en nous inspirant de [53], une présentation de WG(A) et de W(A) par générateurs et relations.

Si (P,q) est un A-module quadratique où A est un corps de caractéristique 2 et si φ est la forme A-bilinéaire symétrique associée à q, alors $\varphi(x,x) = 2q(x)$ nous dit que φ est alternée et (P,q) se décompose en somme orthogonale de plans (cf. 1.11.2) et tout plan possède une base $\{e_1, e_2\}$ avec $\varphi(e_1,e_2) = 1$ et $q(x\,e_1 + y\,e_2) = ax^2 + xy + by^2$ avec $a,b \in A$.

Lemme 1.15.1. *L'ensemble E(A) des classes d'isomorphismes de modules quadratiques de rang 2 est en bijection avec l'ensemble quotient de $A \times A$ modulo la relation d'équivalence engendrée par :*

(1) $(a,b) \sim (b,a)$
(2) $(a,b) \sim (\alpha^2 a, \alpha^{-2} b)$
(3) $(a,b) \sim (a + \beta + b\beta^2, b)$

où $a,b,\beta \in A$ et $\alpha \in A - \{0\}$.

Il y a une surjection naturelle de $A \times A$ sur E(A) obtenue en associant au couple (a,b) la forme quadratique $q_{(a,b)} : A^2 \to A$ définie par $q_{(a,b)}(xe_1 + ye_2) = ax^2 + xy + by^2$. Les relations (1), (2) et (3) sont manifestement nécessaires. Pour voir qu'elles sont suffisantes, considérons deux couples (a,b) et (c,d) qui ont même image dans E(A). Cela signifie que les formes $q_{(a,b)}$ et $q_{(c,d)}$ sont isométriques et donc qu'il existe des scalaires λ, μ, λ' et μ' tels que $q_{(a,b)}(\lambda e_1 + \mu e_2) = c$, $q_{(a,b)}(\lambda' e_1 + \mu' e_2) = d$ et $\varphi_{(a,b)}(\lambda e_1 + \mu e_2$, $\lambda' e_1 + \mu' e_2) = 1$; cette dernière égalité équivaut à $\lambda\mu' - \lambda'\mu = 1$ car $\varphi_{(a,b)}$ est une forme alternée et que le groupe symplectique $\mathrm{Sp}\,\varphi_{(a,b)}$ est le groupe spécial linéaire $\mathrm{SL}_2(A)$. Notons alors, utilisant (2) puis (3) que l'on a $(a,b) \sim (a\lambda^2, b\lambda^{-2}) \sim (a\lambda^2 + \lambda\mu + b\lambda^{-2}(\lambda\mu)^2, b\lambda^{-2}) = (c, b\lambda^{-2})$, en supposant λ non nul. Utilisant (1), on a $(a,b) \sim (b\lambda^{-2}, c)$ et un calcul facile donne $f_2 = \lambda' e_1 + \mu' e_2 = \lambda' f_1 + (\lambda^{-1} e_2)$, d'où en appliquant q, $d = b\lambda^{-2} + \lambda' + c\lambda'^2$.

On trouve à l'aide de (3) avec $\beta = \lambda'$, $(b\mu^{-2},c) \sim (b\lambda^{-2} + \lambda' + c\lambda'^{2},c) \sim (d,c) \sim$ $\sim (c,d)$ ce qui achève la démonstration.

Proposition 1.15.2. Le groupe $WG(A)$ est le quotient du groupe abélien libre G de base $A \times A$ par le sous-groupe I engendré par les éléments :

(1) $(a,b) - (b,a)$
(2) $(a,b) - (a\alpha^2, b\alpha^{-2})$
(3) $(a,b)-(a + \beta + b\beta^2,b)$
(4) $(a,b) + (c,d) - (a+c, d) - (c,b+d)$

En effet, il suffit de montrer que si (5) $\perp_{i=1}^{n} q_{(a_i,b_i)} \simeq \perp_{i=1}^{n} q_{(c_i,d_i)}$, alors $\sum_{i=1}^{n} (a_i,b_i) \equiv \sum_{i=1}^{n} (c_i,d_i)$ modulo I et le résultat se démontre par récurrence sur n. Pour $n = 1$, c'est le lemme précédent ; soit $n > 1$ et supposons que le résultat est vrai pour $n-1$. L'isomorphisme (5) signifie que l'on a un module quadratique (P,q) et deux bases symplectiques $\{e_1,\ldots,e_n,f_1,\ldots,f_n\}$ et $\{e'_1,\ldots, e'_n, f'_1,\ldots,f'_n\}$ de sorte que q restreinte à $\{e_i,f_i\}$ (resp. $\{e'_j,f'_j\}$) est $q_{(a_i,b_i)}$ (resp. $q_{(c_j,d_j)}$). Après renumérotation des $\{e_i,f_i\}$, on peut écrire $e'_1 = \sum_{i=1}^{r} g_i$ avec $g_i \in Ae_i \oplus Af_i - \{0\}$. Appliquant q, on a $c_1 = q(e'_1) = \sum_{i=1}^{r} \alpha_i$ avec $q(g_i) = \alpha_i$. On a, avec des β_i convenables, $\sum_{i=1}^{n} (a_i,b_i) \equiv \sum_{i=1}^{r} (\alpha_i,\beta_i) +$ $+ \sum_{i=r+1}^{n} (a_i,b_i)$ modulo I, du fait du lemme précédent. Une application répétée de (4) montre que $\sum_{i=1}^{r} (\alpha_i,\beta_i) \equiv (c_1,\beta_1) + \sum_{i=2}^{r} (\alpha'_i, \beta'_i)$ mod I. Considérons maintenant le vecteur f''_1 tel que $\varphi(e''_1,f''_1) = 1$ et $q(f''_1) = \beta_1$; du fait de $\varphi(e'_1,f'_1) =$ $= 1$, $f'_1 - f''_1$ est dans l'orthogonal de $P''_1 = Ae'_1 \oplus Af''_1$. Appelons P''_i le sous-espace de P donnant (α'_i, β'_i), $2 \leq i \leq r$; en décomposant f'_1 selon les P''_i et les P_i, $i > r$, on a $f'_1 = f''_1 + \sum_{i=2}^{n} h_i$. En utilisant (1), $\sum_{i=1}^{n} (a_i,b_i) \equiv$ $\equiv (q(f''_1),c_1) + \sum_{i=2}^{r} (\alpha'_i, \beta'_i) + \sum_{r+1}^{n} (a_i,b_i)$; on isole alors les P''_i, $i \geq 2$, tels que $h_i \neq 0$ et, en raisonnant comme pour e'_1 avec le lemme 1.15.1 et la relation (4), on trouve que $\sum_{i=1}^{n} (a_i,b_i) \equiv (c_1,d_1) + \sum_{i=2}^{n} (r_i,s_i)$. Par construction même $\perp_{i=2}^{n} q_{(r_i,s_i)}$ est une décomposition orthogonale de $(P'_1)^{\perp}$. D'après le théorème de simplification de Witt, $\perp_{i=2}^{n} q_{(r_i,c_i)} \simeq \perp_{i=2}^{n} q_{(c_i,d_i)}$ et l'hypothèse de récurrence nous donne $\sum_{i=2}^{n} (r_i,s_i) \equiv \sum_{i=2}^{n} (c_i,d_i)$ modulo I, ce qui achève la démonstration de la proposition.

Remarquons que pour obtenir le groupe de Witt de A, il suffit d'ajouter à I l'élément $(0,0)$ dont l'image dans $WG(A)$ est la forme hyperbolique de rang 2. De plus l'application $\psi : A \times A \to W(A)$ qui au couple (a,b) associe la classe de $q_{(a,b)}$ dans $W(A)$ est $\mathbb{F}_2$-bilinéaire (symétrique). En effet $(a,b) + (a,c) \equiv$ $\equiv (0,b) + (a,b+c) \equiv (0,0) + (a,b+c)$ modulo I et donc dans $W(A)$, $\psi(a,b+c) =$ $= \psi(a,b) + \psi(a,c)$. Ainsi la proposition 1.15.2 peut se traduire par : $W(A)$ est le groupe universel pour les applications $\mathbb{F}_2$-bilinéaires symétriques ψ de $A \times A$ dans les $\mathbb{F}_2$-espaces vectoriels vérifiant $\psi(ax^2, b\alpha^2) = \psi(a,b)$, $\psi(a,b) =$ $= \psi(a + \beta + b\beta^2, b)$ et $\psi(a,b) + \psi(c,d) = \psi(a+c,b) + \psi(c,b+d)$. La deuxième relation peut du fait de l'additivité de ψ s'écrire $\psi(a,b) = \psi(a,ab^2)$; la troisième est une conséquence de la biadditivité de ψ. En effet $\psi(b,c) = \psi(b,a + a + c) = \psi(a,b)$ $+ \psi(a+c,b) = \psi(b + d+d,c) = \psi(c,d) + \psi(c,b+d)$, soit finalement $\psi(a,b) + \psi(c,d) =$ $= \psi(a+c,b) + \psi(c,b+d)$. On a ainsi la proposition suivante :

Proposition 1.15.3. *Le groupe de Witt $W(A)$ est la solution du problème universel posé par les applications $\mathbb{F}_2$-bilinéaires symétriques $\psi : A \times A \to G$ où G est un $\mathbb{F}_2$-espace vectoriel, qui vérifient les conditions $\psi(a,b) = \psi(a,ab^2)$ et $\psi(a,b) =$ $\psi(a\alpha^2, b\alpha^{-2})$, quels que soient a et b dans A et $\alpha \in A^*$.*

La démonstration de la proposition 1.15.2. s'apparente à celle de 1.14.3.

1.16. ANNEAU DE WITT D'UN ANNEAU DE PRÜFER

Soit (P,q,N) un objet de $\mathbf{C}(N)$, où N est un A-module projectif de type fini et de rang 1. On a :

Lemme 1.16.1. *Pour que (P,q,N) soit un espace hyperbolique, il faut et il suffit qu'il existe un facteur direct M de P tel que la restriction de q à M soit 0 et que $M = \{y \mid y \in P, \varphi(x,y) = 0, \forall x \in M\}$.*

La condition est bien nécessaire car si $(P,q,N) \simeq h(P',N)$ alors le sous-A-module P' de P satisfait aux conditions exigées de M. Pour montrer la suffisance, considérons un supplémentaire M' de M dans P ; on note i l'injection naturelle de M dans P, p (resp. p') la projection de $\mathrm{Hom}_A(P,N)$ sur $\mathrm{Hom}_A(M,N)$ (resp. $\mathrm{Hom}_A(M',N)$). Par hypothèse $p \circ d_\varphi \circ i$ est un isomorphisme de A-modules car $d_\varphi : P \to \mathrm{Hom}_A(P,N)$ en est un. Il en résulte que M' est isomorphe à $\mathrm{Hom}_A(M,N)$ et si $z = x + f \in P$, $q(z) = F(x,f) + q_0(f)$, où q_0 est la restriction de q à M' et où F est une application bilinéaire de $M \times \mathrm{Hom}_A(M,N)$ dans N qui induit par $f \mapsto (x \mapsto F(x,f))$ un automorphisme de $\mathrm{Hom}_A(M,N)$. Quitte à changer l'identification de M et de $\mathrm{Hom}_A(M,N)$, on peut supposer que $F(x,f) = f(x)$.

On a vu dans le lemme 1.9.1. qu'il existe une application bilinéaire

$\psi : M' \times M' \to N$ telle que $\psi(f,f) = -q_o(f)$; soit alors $\alpha : M' \to \mathrm{Hom}_A(M',N) \approx N$ l'application linéaire induite par ψ telle que $\psi(f,g) = f(\alpha(g))$; on a $q_o(f) + f(\alpha(f)) = 0$ par construction de α. Soit alors M'' le sous-module de P formé des éléments $\alpha(f) + f$ où f décrit M' ; c'est un supplémentaire de M et on a $q(x + \alpha(f) + f) = f(x) + f(\alpha(f)) + q_o(f) = f(x)$. L'application $(x,f) \mapsto x + \alpha(f) + f$ de $h(M,N)$ dans P est l'isomorphisme cherché.

Supposons maintenant que A soit un anneau de Prüfer, c'est à dire un anneau intègre dans lequel tout idéal de type fini est projectif ; on désigne par K son corps des fonctions et soit N un A-module projectif de type fini et de rang 1, i.e., un idéal de type fini de A. Il existe un homomorphisme naturel de $W(N)$ dans $W(N \otimes_A K)$ qui est, quand on choisit un générateur de $N \otimes_A K$, isomorphe à $W(K)$. On a alors la proposition suivante :

Proposition 1.16.2. L'homomorphisme naturel de groupes abéliens $W(N) \to W(N \otimes_A K)$ est injectif.

Il suffit de montrer que si (M,q,N) et (M',q',N) sont tels que $(M,q,N) \otimes K$ et $(M',q',N) \otimes_A K$ sont isomorphes, alors (M,q,N) et (M',q',N) ont même classe dans le groupe de Witt de N. Pour cela, considérons $(M,q,N) \perp \perp (M',-q',N) = (P,q,N)$ dont l'image dans $W(K)$ est 0 : il s'agit de montrer que (P,q,N) est un espace hyperbolique. Or, $(P,q,N) \otimes_A K \simeq h(V,K)$ et P s'identifie à un sous-A-module de $V \oplus V^*$. On a la suite exacte de K-espaces vectoriels $0 \to V \xrightarrow{i} V \oplus V^* \xrightarrow{p} V^* \to 0$. Soit alors M' l'image de P dans V^* par la projection p ; M' est un A-module de type fini sans torsion donc projectif et on en déduit la suite exacte scindée de A-modules

$$0 \to P \cap V \xrightarrow{i'} P \xrightarrow{p'} M' \to 0 .$$

On peut alors appliquer le lemme précédent à $M = P \cap V$, ce qui démontre la proposition.

Considérons le cas où $N = A$; si B est un sous-anneau intermédiaire entre A et K, B est de Prüfer et du fait de la proposition précédente, on a les inclusions naturelles $W(A) \hookrightarrow W(B) \hookrightarrow W(K)$. Si maintenant $\mathfrak{m}$ est un idéal maximal de A et $A_{\mathfrak{m}}$ l'anneau local de A en $\mathfrak{m}$, $W(A) \hookrightarrow W(A_{\mathfrak{m}}) \hookrightarrow W(K)$ et la question se pose de savoir si $W(A)$ coïncide avec $\bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} W(A_{\mathfrak{m}})$ dans $W(K)$, où $\mathrm{Max}(A)$ désigne l'ensemble des idéaux maximaux de A. La réponse est affirmative et on a la proposition suivante :

Proposition 1.16.3. L'homomorphisme naturel de groupes abéliens $W(A) \to \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} W(A_{\mathfrak{m}})$ est un isomorphisme.

Le lecteur pourra consulter [22], pour la démonstration. En fait, un résultat analogue à celui de la proposition 1.16.3. est encore vrai dans le cas où A est un anneau semi-héréditaire (cf. [23]).

En général, si A est un anneau intègre de corps de fractions K, l'homomorphisme naturel de groupes abéliens $W(A) \to W(K)$ n'est pas injectif. Ainsi, si A est régulier et noéthérien intégre, le noyau de $W(A) \to W(K)$ est un nilidéal de $W(A)$ (cf. [15]). Par contre, si A est un anneau local régulier complet et noéthérien avec 2 inversible, alors $W(A) \to W(K)$ est injectif (cf. [15]).

1.17. EXEMPLES

Nous rassemblons ici un certain nombre d'exemples d'anneaux de Witt.

1.17.1. L'anneau de Witt d'un corps K quadratiquement clos

Si K est quadratiquement clos et de caractéristique différente de 2, $U(K)/U^2(K)$ est réduit à un élément et la proposition 1.14.2. montre que l'homomorphisme $\mathbb{Z} = \mathbb{Z}[U(K)/U^2(K)] \to WG(K)$ est un isomorphisme d'anneaux, inverse de l'homomorphisme $\dim : WG(K) \to \mathbb{Z}$ (cf. 1.10.). En caractéristique 2, on voit encore que $E(A)$ est réduit à un élément si bien que $WG(K)$ s'identifie encore à $\mathbb{Z}$ par l'homomorphisme $\frac{1}{2}\dim$. On en déduit immédiatement que $W(K) = (0)$ en caractéristique 2 et $\mathbb{Z}/(2)$ dans le cas contraire.

1.17.2. L'anneau de Witt d'un corps K ordonné maximal

On sait que le groupe $U(K)/U^2(K)$ est alors réduit à deux éléments, classes de -1 et de $+1$. Le noyau de l'homomorphisme $\mathbb{Z}[U(K)/U^2(K)] \to WG(K)$ de 1.14.2. est manifestement réduit à (0), de sorte que $WG(K)$ est isomorphe à $\mathbb{Z} \oplus \mathbb{Z}$ avec pour produit $(s,t) \circ (s',t') = (ss' + tt', st' + s't)$, ce qui n'est autre chose que la loi d'inertie. L'homomorphisme naturel $WG(K) \to W(K)$ n'est alors pas autre chose que la signature $\sigma[(s,t)] = s-t$ car le sous-groupe formé par les espaces hyperboliques est le sous-groupe diagonal $H = \{(s,s) \mid s \in \mathbb{Z}\}$ et $W(K)$ s'identifie en tant qu'anneau à $\mathbb{Z}$.

1.17.3. Cas de l'anneau des entiers

L'anneau de Witt de $\mathbb{Z}$ s'obtient à l'aide de l'homomorphisme $\mathbb{Z} \to \mathbb{R}$ qui fournit un homomorphisme injectif $W(\mathbb{Z}) \hookrightarrow W(\mathbb{R}) \approx \mathbb{Z}$ (cf. [51]);donc $W(\mathbb{Z})$ est un idéal de $\mathbb{Z}$. Comme tous les modules quadratiques sur $\mathbb{Z}$ de rang inférieur ou égal à 8 sont hyperboliques sauf celui fourni par la matrice de Milnor (cf. [28]), on voit que $W(\mathbb{Z}) \approx 8\,\mathbb{Z}$.

Des considérations analogues permettent le calcul de $W(\mathbb{Q})$ et de tout

corps de nombres ainsi que celui de l'anneau de ses entiers algébriques (cf. [26]).

1.17.4. L'anneau de Witt d'un corps $C_1(2)$

Soit K un corps et supposons que toute forme quadratique sur K à plus de deux variables représente 0 ; le corps K est dit $C_1(2)$. Cela équivaut à dire que toute forme quadratique non dégénérée à deux variables représente tout élément non nul de K et en particulier l'élément unité. Nous distinguons deux cas suivant la caractéristique de K.

(i) Le corps K n'est pas de caractéristique 2

On voit alors aisément, par récurrence sur le rang de la forme quadratique q que q est équivalente à la forme $\langle 1\rangle \perp \ldots \perp \langle 1\rangle \perp \langle \text{dét } q\rangle$. Ainsi les deux homomorphismes dim : $WG(K) \to \mathbb{Z}$ et dét : $WG(K) \to U(K)/U^2(K)$ suffisent à déterminer les formes quadratiques sur K, c'est à dire l'homomorphisme de groupes abéliens $u = (\dim, \text{dét}) : WG(K) \to \mathbb{Z} \oplus U(K)/U^2(K)$ est injectif. D'autre part, il est bien clair que u est surjectif et le produit dans $WG(K)$ est donné par

$$(m_1, \bar{a}_1).(m_2, \bar{a}_2) = (m_1 m_2, \overline{a_1^{m_2}.a_2^{m_1}}).$$

Considérons maintenant l'anneau de Witt de K : deux cas sont à considérer. Supposons d'abord que $-1 \in U^2(K)$. L'anneau de Witt est le quotient de $WG(K)$ par l'idéal des formes hyperboliques, sous-groupe cyclique infini engendré par $H_1 = \langle 1\rangle \perp \langle -1\rangle$ dont l'image par u est $(2,\bar{1})$. On a donc $W(K) \approx \mathbb{Z}/(2) \oplus \oplus U(K)/U^2(K)$.

Si -1 n'est pas un carré dans K, $WG(K)$ est le quotient de $\mathbb{Z} \oplus \oplus U(K)/U^2(K)$ par le sous-groupe engendré par $(2,\overline{-1})$. Comme $(2,\overline{-1}) + (2,\overline{-1}) = (4,\bar{1})$, $W(K)$ est un quotient de $\mathbb{Z}/4\mathbb{Z} \oplus U(K)/U^2(K)$. En fait on a la suite exacte non scindée de groupes abéliens : $0 \to W_o(K) \to W(K) \xrightarrow{\alpha} \mathbb{Z}/(2)$ où α est l'homomorphisme de dimension modulo 2. Le groupe $W_o(K)$ s'identifie à $U(K)/U^2(K)$ et la somme dans $W(K) = W_o(K) \underset{\text{s.d.}}{\times} \mathbb{Z}/(2)$; $(\bar{a},1) + (\bar{b},1)$ est $(\overline{-ab},0)$.

(ii) Le corps K est de caractéristique 2

Notant H_1 l'espace hyperbolique de dimension 2 sur K, on voit que comme dans le premier cas toute forme quadratique q s'écrit $H_1 \perp H_1 \perp \ldots \perp H_1 \perp A(q)$ où $A(q) \in E(K)$ est déterminée de manière unique par q. De plus l'ensemble $E(K)$ se trouve naturellement muni d'une loi de groupe abélien de la façon suivante : soient q_1 et q_2 deux éléments de $E(K)$ et posons $q_1 * q_2 = A(q_1 \perp q_2)$. On a donc comme dans (i), deux homomorphismes de groupes abéliens $\frac{1}{2}\dim : WG(K) \to \mathbb{Z}$ et $A : WG(K) \to E(K)$ qui suffisent à déterminer $WG(K)$: c'est le groupe abélien somme directe de $\mathbb{Z}$ et de $E(K)$. L'élément neutre de $E(K)$ étant

H_1, le groupe $W(K)$ s'identifie naturellement à $E(K)$. Intéressons-nous maintenant au groupe $E(K)$. Les éléments de $E(K)$ correspondent aux formes quadratiques $q_{(1,a)}$ (cf. 1.15.) et 1.15.2. montre que $q_{(1,a)} * q_{(1,b)} = q_{(1,a+b)}$. On voit donc que $E(K)$ est un quotient du groupe additif de K par le sous-groupe H formé des éléments a tels que $q_{(1,a)} \approx H_1$. A l'aide de 1.15.1., on voit immédiatement que $H = \{x + x^2 | x \in K\} = \wp(K)$ où $\wp$ est l'homomorphisme de groupes abéliens $\wp : K \to K$ défini par $\wp(x) = x + x^2$. Le groupe $E(K)$ est donc le groupe $K/\wp K$ que nous retrouverons au chapitre 2 comme groupe des extensions quadratiques de K. L'invariant $A(q)$ est l'<u>invariant d'Arf</u> de q (cf. 2.6.).

Les résultats que nous venons d'obtenir peuvent être obtenus directement à partir de 1.15. dans le cas particulier des corps parfaits de caractéristique 2. Comme un corps fini est $C_1(2)$, les résultats présents s'appliquent à eux.

1.17.5. <u>Anneau de Witt d'un corps et d'un anneau fini</u>

On sait que tout corps fini K est C_1, donc $C_1(2)$, d'après le théorème de Warning-Chevalley (cf. [9]). Dans tous les cas, $WG(K) \approx \mathbb{Z} \oplus \mathbb{Z}/(2)$. Pour $W(K)$, on a les trois cas suivants :

(i) Card $K \equiv 0(2)$: $W(K) \approx E(K) = \mathbb{Z}/(2)$.
(ii) Card $K \equiv 1(4)$: $W(K) \approx \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.
(iii) Card $K \equiv 3(4)$: $W(K) \approx \mathbb{Z}/(4)$.

Dans le premier cas, K est parfait de caractéristique 2 ; dans le second cas, $-1 \in U^2(K)$ et dans le troisième $-1 \notin U^2(K)$.

Soit maintenant A un anneau fini : c'est un anneau semi-local dont le radical est nilpotent , c'est donc un produit d'anneaux locaux complets de corps résiduels finis. Soient alors r_1 le nombre des idéaux maximaux $\mathfrak{m}$ de A tels que Card $(A/\mathfrak{m}) \equiv 0(2)$, r_2 le nombre de ceux pour lesquels Card $(A/\mathfrak{m}) \equiv 1(4)$ et r_3 celui de ceux pour lesquels Card $(A/\mathfrak{m}) \equiv 3(4)$. Alors $WG(A)$ (resp. $W(A)$) est le produit des $WG(A/\mathfrak{m})$ (resp. des $W(A/\mathfrak{m})$) où $\mathfrak{m}$ parcourt l'ensemble fini des idéaux maximaux de A, si bien que :

$$WG(A) \approx \mathbb{Z}^{r_1 + r_2 + r_3} \oplus (\mathbb{Z}/(2))^{r_1 + r_2 + r_3}$$

$$W(A) \approx (\mathbb{Z}/(4))^{r_3} \oplus (\mathbb{Z}/(2))^{r_1 + 2r_2}$$

2. ALGEBRES DE CLIFFORD

2.1. DEFINITIONS

Soient A un anneau, M un A-module et $q : M \to A$ une forme quadratique sur M. L'algèbre de Clifford de l'objet (M,q) est, par définition, le quotient de l'algèbre tensorielle $T(M)$ par l'idéal bilatère $I(q)$ de $T(M)$ engendré par les éléments $x \otimes x - q(x)\, 1_{T(M)}$, où x parcourt M. On la note $C(M,q) = T(M)/I(q)$.

Il est clair que dans la définition de l'algèbre de Clifford de (M,q), on n'est pas tenu à supposer que M soit projectif et q non dégénérée. Aussi, les objets (M,q) où M est un A-module et $q : M \to A$ est une forme quadratique, seront aussi appelés modules quadratiques, si aucune confusion n'est à craindre.

Remarquons que si q est la forme nulle, $C(M,q)$ est l'algèbre extérieure $\Lambda(M)$. L'algèbre $C(M,q)$ est la solution du problème universel suivant : on considère les couples (E,α) où E est une A-algèbre associative et unitaire et $\alpha : M \to E$ une application A-linéaire telle que $\alpha(x)^2 = q(x)\, 1_E$. L'algèbre $C(M,q)$ et l'application ρ de M dans $C(M,q)$, composée de l'injection naturelle de M dans $T(M)$ et de la surjection π de $T(M)$ sur $C(M,q)$, est un objet initial de la catégorie formée des paires (E,α). Notons qu'on a dans $C(M,q)$, $\rho(x)^2 = q(x) 1_{C(M,q)}$ par construction et, pour tout couple (x,y) d'éléments de M, $\rho(x)\rho(y) + \rho(y)\rho(x) = \varphi(x,y)\, 1_{C(M,q)}$, φ étant la forme A-bilinéaire symétrique associée à q. Si ρ est injective, on identifiera M à son image par ρ dans $C(M,q)$ (en général, ρ n'est pas injective). On dira que $\rho : M \to C(M,q)$ est l'application A-linéaire canonique.

Soit $\rho' : M \to C(M,q)$ l'application A-linéaire définie par $x \mapsto -\rho(x)$: on a $(\rho'(x))^2 = q(x)\, 1_{C(M,q)}$ et on obtient ainsi, d'après la propriété universelle de $C(M,q)$ un homomorphisme qu'on notera σ_C de $C(M,q)$ dans elle-même. Comme le couple $(C(M,q), \rho')$ est aussi solution du problème universel posé ci-dessus, σ_C est un automorphisme, involutif puisque $\sigma_C(\rho(x)) = -\rho(x)$, qu'on appelle automorphisme principal. De même, soit $D = C(M,q)^o$ l'algèbre opposée de $C(M,q)$, c'est à dire que D a même groupe abélien sous-jacent mais que sa multiplication $*$ est définie par $x * y = y\,x$, x et y parcourant D. L'application $\rho : M \to D$ vérifie la condition $\rho(x) * \rho(x) = q(x)\, 1_D$, d'où un homomorphisme τ de $C(M,q)$ dans $C(M,q)^o$ qui est un isomorphisme, donc un antiautomorphisme de $C(M,q)$ appelé l'antiautomorphisme principal. Ces deux isomorphismes σ_C et τ

proviennent d'applications analogues définies sur $T(M)$ et qui laissent globalement invariant l'idéal $I(q)$.

Le caractère universel de $C(M,q)$ entraîne un certain nombre de propriétés fonctorielles. Ainsi, soit $u : (M,q) \to (M',q')$ un morphisme de modules quadratiques et $\rho' : M' \to C(M',q')$ l'application canonique. On a $(\rho' \circ u(x))^2 = q'(u(x))\, 1_{C(M',q')} = q(x)\, 1_{C(M',q')}$ et l'application $\rho' \circ u : M \to C(M',q')$ induit donc un unique homomorphisme de A-algèbres $C(u)$ de $C(M,q)$ dans $C(M',q')$. Il est évident que $C(id_{(M,q)}) = id_{C(M,q)}$; si $v : (M',q') \to (M'',q'')$ est un second morphisme de modules quadratiques, on obtient deux homomorphismes de $C(M,q)$ dans $C(M'',q'')$, à savoir , $C(v) \circ C(u)$ et $C(v \circ u)$ qui coïncident du fait de l'universalité de $C(M,q)$. Ceci nous montre que $C : (M,q) \mapsto C(M,q)$ est un foncteur de la catégorie des A-modules quadratiques dans la catégorie des A-algèbres associatives.

De plus, soit (M,q) la limite inductive d'une famille $(M_i,q_i)_{i\in I}$ de A-modules quadratiques. L'assertion donnée ci-dessus montre que la famille des algèbres $(C(M_i,q_i))_{i\in I}$ munie des homomorphismes $C(u_{ij})$ induits par les $u_{ij} : M_i \to M_j$ pour chaque $i \leq j$ forme un système inductif. Alors $C(M,q)$ s'identifie à la limite inductive des algèbres $C(M_i,q_i)$.

Soit maintenant $A \to A'$ un homomorphisme d'anneaux (commutatifs). La A'-algèbre $C(A' \otimes_A M,q')$ où $q' : A' \otimes_A M \to A'$ est la forme A'-quadratique obtenue de q par extension des scalaires, s'identifie naturellement à la A'-algèbre $A' \otimes_A C(M,q)$.

L'algèbre tensorielle $T(M)$ est graduée sur $\mathbb{N}$ par $T^n(M) = \overset{n}{\otimes} M$, mais l'idéal $I(q)$ n'est pas homogène pour cette graduation. Cependant, graduons $T(M)$ sur $\mathbb{Z}/2\mathbb{Z}$ en posant $T_0(M) = \bigoplus_{p\geq 0} T^{2p}(M)$ et $T_1(M) = \bigoplus_{p\geq 0} T^{2p+1}(M)$. Alors l'idéal $I(q)$ est homogène car $x \otimes x - q(x)\, 1_{T(M)} \in T_0(M)$ $(x \in M)$ et $C(M,q)$ se trouve ainsi graduée sur $\mathbb{Z}/2\mathbb{Z}$: $C(M,q) = C_0(M,q) \oplus C_1(M,q) = C_0 \oplus C_1$, $C_0(M,q)$ est une sous-algèbre de $C(M,q)$, la sous-algèbre engendrée sur A par les produits $\rho(x)\,\rho(y)$, $x,y \in M$ et $\rho(M)$ est contenu dans le A-module $C_1(M,q)$.

Remarquons que σ_C et τ -automorphisme et antiautomorphisme principaux- respectent la graduation. En particulier $\sigma_C = id_{C_0} \oplus - id_{C_1}$. Notons que $(M,q) \mapsto$ $\mapsto C(M,q)$ est un foncteur de la catégorie des A-modules quadratiques dans la catégorie des A-algèbres associatives graduées sur $\mathbb{Z}/2\mathbb{Z}$, les morphismes étant les homomorphismes de degré zéro. Il suffit, pour cela, de remarquer que si u est un morphisme de modules quadratiques, de (M,q) dans (M',q'), $C(u)$ est un morphisme d'algèbres graduées, homogène de degré zéro. En particulier, si l'on note $C_0(u)$

la restriction de $C(u)$ à $C_o(M,q)$ et en restreignant le codomaine de $C_o(u)$ à $C_o(M',q')$, alors on a $C_o(id_{(M,q)}) = id_{C_o(M,q)}$ et $C_o(v \circ u) = C_o(v) \circ C_o(u)$. Ainsi, $(M,q) \mapsto C_o(M,q)$ est aussi un foncteur de la catégorie des A-modules quadratiques dans la catégorie des A-algèbres associatives.

Notons encore que l'extension des scalaires est compatible avec C_o, c'est à dire que $C_o(A' \otimes_A M, q')$ s'identifie naturellement à $A' \otimes_A C_o(M,q)$.

2.2. PRODUIT TENSORIEL GRADUE ET ALGEBRE DE CLIFFORD D'UNE SOMME

Soient $E = E_o \oplus E_1$ et $F = F_o \oplus F_1$ deux A-algèbres associatives, graduées sur $\mathbb{Z}/(2)$. Le produit tensoriel gradué de E par F, noté $E \hat{\otimes} F$, est la A-algèbre associative graduée sur $\mathbb{Z}/(2)$ dont le A-module sous-jacent est $E \otimes F$, gradué par $(E \otimes F)_o = (E_o \otimes F_o) \oplus (E_1 \otimes F_1)$ et $(E \otimes F)_1 = (E_o \otimes F_1) \oplus (E_1 \otimes F_o)$ et dont la multiplication est donnée, sur les éléments homogènes $x \in E_i$, $x' \in E_{i'}$, $y \in F_j$, $y' \in F_{j'}$, par $(x \otimes y)(x' \otimes y') = (-1)^{ji'}(xx') \otimes (yy')$, où $\otimes$ désigne le produit tensoriel sur l'anneau A.

Le produit tensoriel $E \otimes F$ peut être aussi muni d'une structure de A-algèbre graduée sur $\mathbb{Z}/(2)$, en posant $(x \otimes y)(x' \otimes y') = (xx') \otimes (yy')$, où $x,x' \in E$ et $y,y' \in F$ et en graduant $E \otimes F$ comme ci-dessus. Notons que si E_1 (ou F_1) est réduit à 0, $E \hat{\otimes} F$ et $E \otimes F$ coïncident en tant que A-algèbres graduées sur $\mathbb{Z}/(2)$. De même, en caractéristique 2, le produit tensoriel gradué et le produit tensoriel ordinaire coïncident. Remarquons enfin que si x est dans E_1 et y dans F_1, on a, dans $E \hat{\otimes} F$, $(x \otimes 1)(1 \otimes y) = x \otimes y$ et $(1 \otimes y)(x \otimes 1) = -x \otimes y$. Les images canoniques de E et de F dans $E \hat{\otimes} F$ ne commutent donc pas, en général.

Proposition 2.2.1. L'algèbre de Clifford de la somme orthogonale de deux modules quadratiques est le produit tensoriel gradué des algèbres de Clifford de chaque composante.

Soient (M,q) et (M',q') deux modules quadratiques, D le produit tensoriel gradué $C(M,q) \hat{\otimes} C(M',q')$ et ρ l'application de $M \oplus M'$ dans D définie par $\rho(x,x') = x \otimes 1 + 1 \otimes x'$. Nous voulons montrer que (D,ρ) est la solution du même problème universel que $C((M,q) \perp (M',q'))$. Soit donc E une A-algèbre associative et $\alpha : M \oplus M' \to E$ une application linéaire telle que $(\alpha(x,x'))^2 = (q(x) + q'(x'))\, 1_E$. Considérant les restrictions de α à M et à M' respectivement, on en déduit deux homomorphismes de A-algèbres $\alpha_M : C(M,q) \to E$ et $\alpha_{M'} : C(M',q') \to E$ et soit $\beta : C(M,q) \otimes C(M',q') \to \xrightarrow{\alpha_M \otimes \alpha_{M'}} E \otimes E \xrightarrow{\mu} E$

l'application A-linéaire composée, où μ est la multiplication de E. En prenant pour multiplication sur le A-module $C(M,q,) \otimes C(M',q')$ la multiplication du produit tensoriel gradué, β est un homomorphisme de A-algèbres. Pour cela, il suffit de vérifier que $\beta((x \otimes x')(y \otimes y')) = \beta(x \otimes x') \beta(y \otimes y')$, où $x,y \in C(M,q)$ et $x',y' \in C(M',q')$ sont des éléments homogènes. On a donc à vérifier que

$(-1)^{d^o(x')d^o(y)} \alpha_M(x) \alpha_M(y) \alpha_{M'}(x') \alpha_{M'}(y') = \alpha_M(x) \alpha_{M'}(x') \alpha_M(y) \alpha_{M'}(y')$, i.e., il suffit de montrer que $\alpha_M(y) \alpha_{M'}(x') = (-1)^{d^o(x') d^o(y)} \alpha_{M'}(x') \alpha_M(y)$, pour tout $x' \in C(M',q')$ et $y \in C(M,q)$. Comme M engendre $C(M,q)$ en tant que A-algèbre, il suffit de vérifier la relation ci-dessus pour $x' \in \rho'(M')$ et $y \in \rho(M)$, où $\rho : M \to C(M,q)$ et $\rho' : M' \to C(M',q')$ sont les applications A-linéaires canoniques. Mais alors, on sait que $(\alpha(y,x'))^2 - (\alpha(y,0))^2 - (\alpha(0,x'))^2 = \varphi((y,0),(0,x')) = 0$, où φ est la forme A-bilinéaire symétrique associée à la forme quadratique $q \perp q' : M \oplus M' \to A$, $(x,x') \mapsto q(x) + q'(x')$, ce qui est exactement la relation demandée.

Le résultat précédent fournit des renseignements sur la structure de module de l'algèbre de Clifford de certains modules quadratiques.

Proposition 2.2.2. Soit (M,q) un module quadratique, libre de type fini et possédant une base orthogonale (e_i), $1 \leq i \leq n$; $C(M,q)$ est un module libre de type fini et une base de $C(M,q)$ est formée des éléments $\rho(e_{i_1}) \ldots \rho(e_{i_q})$, où $1 \leq i_1 < \ldots < i_q \leq n$. L'application ρ est injective et le module $C(M,q)$ est isomorphe à l'algèbre extérieure de M.

La démonstration se fait par récurrence sur n. Si $n = 1$, $T(M)$ s'identifie à l'anneau des polynômes $A[X]$ et $I(q)$ est l'idéal principal engendré par $X^2 - q(e_1)$. Ainsi, $C(M,q)$ est un A-module libre de rang 2 dont une base est formée de 1 et de $\rho(e_1)$. Supposons le résultat vrai pour n-1 et soit M' le sous-module engendré par $e_1,\ldots,e_{n-1}$. On a $(M,q) = (M', q_{|M'}) \perp (A\, e_n, q_{|A\, e_n})$ et en appliquant la proposition 2.2.1., $C(M,q)$ en tant que A-module, s'identifie à $C(M', q_{|M'}) \otimes C(A\, e_n, q_{|A\, e_n})$. Les résultats voulus sont clairs en appliquant l'hypothèse de récurrence à $C(M', q_{|M'})$ et (le cas où le module est de rang 1) à $C(A\, e_n, q_{|A\, e_n})$.

Corollaire 2.2.3. Soient A un corps et (M,q) un A-module quadratique, où M est de dimension finie n sur A. Alors, $C(M,q)$ est un A-espace vectoriel de dimension finie égale à 2^n.

En effet, si A est de caractéristique différente de 2, la proposition s'applique directement, même si la forme quadratique est dégénérée. En caractéristique 2, la chose se complique légèrement car le module quadratique (M,q) est la somme orthogonale de tois facteurs : son radical M_1, un sous espace vectoriel M_2 sur lequel la forme quadratique est une application semi-linéaire de M_2 dans A vis-à-vis de l'isomorphisme $x \mapsto x^2$ de A sur son sous-corps A^2 et un troisième M_3 sur lequel la forme quadratique est non dégénérée. Ainsi $(M,q) = \perp_{i=1}^{3} (M_i,q_i)$ et il suffit de regarder ce qui se passe sur chaque M_i. Pour $M_1, q_1 = 0$ et $C(M_1,q_1)$ est l'algèbre extérieure $\Lambda(M_1)$. Pour M_2, il existe une base orthogonale (toute base l'est !). Reste M_3 qui est somme orthogonale de sous-espace de rang 2. Il suffit donc de montrer le lemme suivant :

Lemme 2.2.4. L'algèbre de Clifford d'un A-module quadratique (M,q) libre de rang 2 est un A-module libre de rang 4.

En effet, c'est le quotient de l'algèbre tensorielle à deux générateurs e_1 et e_2 par l'idéal engendré par les éléments $(a\,e_1 + b\,e_2)^2 - q(a\,e_1 + b\,e_2)$ avec a et b dans A, soit finalement par les éléments $e_1^2 - q(e_1)$, $e_2^2 - q(e_2)$, et $e_1\,e_2 + e_2\,e_1 - \varphi(e_1,e_2)$, où φ est la forme A-bilinéaire symétrique associée à q. On considère le A-module $E = A^4$ dont on note $\{\varepsilon_0,\varepsilon_1,\varepsilon_2,\varepsilon_3\}$ la base canonique et on définit sur E une structure de A-algèbre associative en posant : (i) ε_0 est élément unité de E ; (ii) $\varepsilon_1^2 = q(e_1)\,\varepsilon_0$, $\varepsilon_2^2 = q(e_2)\,\varepsilon_0$, $\varepsilon_1\varepsilon_2 = \varepsilon_3$ et $\varepsilon_2\,\varepsilon_1 = \varphi(e_1,e_2)\,\varepsilon_0 - \varepsilon_3$. On a $(a\,\varepsilon_1 + b\,\varepsilon_2)^2 = q(a\,e_1 + b\,e_2)\varepsilon_0$, donc l'application ρ de M dans E qui à $a\,e_1 + b\,e_2$ associe $a\,\varepsilon_1 + b\,\varepsilon_2$ induit un homomorphisme de A-algèbres de $C(M,q)$ dans E. Inversement si $\alpha : M \to D$ est une application A-linéaire telle que $(\alpha(x))^2 = q(x)\,1_D$, pour tout $x \in M$, où D est une A-algèbre associative à élément unité, on définit $\beta : E \to D$, $\beta(\varepsilon_0) = 1_D$, $\beta(\varepsilon_i) = \alpha(e_i)$ $(i=1,2)$ et $\beta(\varepsilon_3) = \alpha(e_1)\,\alpha(e_2)$. Il est immédiat de vérifier que β est un homomorphisme de A-algèbres, donc E est isomorphe à l'algèbre de Clifford de (M,q). Ceci nous montre bien que $\{1,e_1,e_2,e_1e_2\}$ est une base de l'algèbre de Clifford $C(M,q)$. De plus, $\{1,e_1e_2\}$ est une base de $C_0(M,q)$ et $\{e_1,e_2\}$ est une base de $C_1(M,q)$. Donc, en particulier, on a un isomorphisme de A-modules $C_1(M,q) \approx M$, dès que M est un A-module projectif de type fini et de rang 2.

2.3. STRUCTURE DE MODULE DE L'ALGEBRE DE CLIFFORD

Le but de ce paragraphe est de donner dans un cas général des renseignements sur le A-module $C(M,q)$ (cf. [10]). Comme cette méthode s'applique à d'au-

tres algèbres, sans complications excessives, nous avons donné les démonstrations dans le cadre le plus général.

Soient M un A-module et $x \in M$. On note $e_x : T(M) \to T(M)$ la multiplication à gauche par x, i.e., $e_x(u) = xu$ pour tout $u \in T(M)$, où $x\,u$ désigne le produit de x par u dans l'algèbre tensorielle $T(M)$. Désignons $+1$ ou -1 par ε.

Lemme 2.3.1. Soit $f \in \mathrm{Hom}_A(M,A) = M^*$. Il existe une unique application A-linéaire j_f^ε de $T(M)$ dans $T(M)$ telle que : (i) $j_f^\varepsilon(1) = 0$; (ii) $j_f^\varepsilon \circ e_x + \varepsilon\, e_x \circ j_f^\varepsilon = f(x)\, 1_{T(M)}$, pour tout x dans M. De plus, $f \mapsto j_f$ est une application A-linéaire de M^* dans $\mathrm{Hom}_A(T(M), T(M))$; si $T_n(M)$ désigne le module des éléments de $T(M)$ de degré au plus égal à n, $j_f^\varepsilon\ (T_n(M)) \subset T_{n-1}(M)$. Si f et g sont des éléments de M^*, $j_f^\varepsilon \circ j_g^\varepsilon + \varepsilon\, j_g^\varepsilon \circ j_f^\varepsilon = 0$ et $(j_f^1)^2 = 0$.

En effet, la condition (ii) s'écrit $j_f^\varepsilon(x\,u) = -\varepsilon\, x\, j_f^\varepsilon(u) + f(x)\, u$ pour x dans M et u dans $T(M)$. Comme (i) détermine j_f^ε sur $T_0(M)$ et que (ii) montre que j_f^ε est connu sur $T_n(M)$ si l'on connait ses valeurs sur $T_{n-1}(M)$, l'application j_f^ε se trouve déterminée et de manière unique par les deux conditions, en raisonnant par récurrence sur l'entier n. On a clairement alors $j_f^\varepsilon\ (T_n(M)) \subset T_{n-1}(M)$ pour la même raison. De plus, si $g = a_1 f_1 + a_2 f_2$, $a_i \in A$, $f_i \in M^*$, j_g^ε et $a_1 j_{f_1}^\varepsilon + a_2 f_{f_2}^\varepsilon$ vérifient les condition (i) et (ii), donc sont égales. La dernière affirmation se démontre différemment suivant ε : si $\varepsilon = 1$, $(j_f^1)^2 \circ e_x = -\, j_f^1 \circ e_x \circ j_f^1 + f(x)\, j_f^1 = (-\, j_f^1 \circ e_x + f(x)\, 1_{T(M)}) \circ j_f^1 = e_x \circ (j_f^1)^2$. Comme $(j_f^1)^2(1) = 0$, $(j_f^1)^2$ est nul sur $T(M)$ puisque $T(M)$-linéaire à gauche. Remplaçant alors f par $f+g$, on obtient $j_f^1 \circ j_g^1 + j_g^1 \circ j_f^1 = 0$.

Dans le cas $\varepsilon = -1$, le résultat est clair pour les éléments de degré 0 car $j_f^{-1} \circ j_g^{-1}\ (1) = 0$. Le résultat général s'obtient par récurrence sur n. En effet, supposons que $j_f^{-1} \circ j_g^{-1} = j_g^{-1} \circ j_f^{-1}$ sur $T_{n-1}(M)$ et soit $v = xu \in T_n(M)$. On a $(j_f^{-1} \circ j_g^{-1})(v) = x\,(j_f^{-1} \circ j_g^{-1})(u) + f(x)\, j_g^{-1}(u) + g(x)\, j_f^{-1}(u)$ et $(j_g^{-1} \circ j_f^{-1})(v) = x\,(j_g^{-1} \circ j_f^{-1})(u) + g(x)\, j_f^{-1}(u) + f(x)\, j_g^{-1}(u)$. De l'hypothèse de récurrence, on déduit le résultat cherché.

On remarque que les conditions(i) et (ii), jointes au fait que $j_f^\varepsilon(x) = f(x)\, 1_{T(M)}$ pour $x \in M$ signifient que j_f^ε est l'unique $(-\varepsilon)$ - dérivation de $T(M)$ dans $T(M)$ qui prolonge f. On en déduit aisément que j_f^ε est nulle sur la

sous-algèbre de $T(M)$ engendrée par le noyau de la forme linéaire f.

Soit maintenant $F : M \times M \to A$ une forme A-bilinéaire. On note F_x l'élément de M^* défini par $F_x(y) = F(x,y)$ et $j^{\epsilon}_{F,x}$ l'application $j^{\epsilon}_{F_x}$ de $T(M)$ dans $T(M)$ associée à F_x suivant le lemme 2.3.1. On a alors le lemme suivant :

Lemme 2.3.2. *Il existe une application A-linéaire λ^{ϵ}_F et une seule de $T(M)$ dans $T(M)$ telle que : (i) $\lambda^{\epsilon}_F(1) = 1$; (ii) $\lambda^{\epsilon}_F \circ e_x = (e_x + j^{\epsilon}_{F,x}) \circ \lambda^{\epsilon}_F$. De plus, λ^{ϵ}_F est une bijection de $T(M)$ sur $T(M)$ qui commute avec les j^{ϵ}_f, $f \in M^*$, qui respecte la filtration de $T(M)$ et qui induit l'identité par passage au gradué associé à $T(M)$. Si G est une seconde forme A-bilinéaire, $\lambda^{\epsilon}_F \circ \lambda^{\epsilon}_G = \lambda^{\epsilon}_{F+G}$ et λ^{ϵ}_o est l'identité de $T(M)$.*

L'existence et l'unicité de λ^{ϵ}_F se démontrent comme dans le lemme 2.3.1. pour j^{ϵ}_f, à partir de (i) et (ii). En particulier, pour $x \in M$ et $u \in T(M)$, on a $\lambda^{\epsilon}_F(x\,u) = x\,\lambda^{\epsilon}_F(u) + j^{\epsilon}_{F,x}(\lambda^{\epsilon}_F(u))$. Montrons que λ^{ϵ}_F et j^{ϵ}_f commutent. Pour ce faire, on procède par récurrence sur le degré. C'est vrai en degré 0 car $j^{\epsilon}_f \circ \lambda^{\epsilon}_F(1) = j^{\epsilon}_f(1) = 0$ et $\lambda^{\epsilon}_F \circ j^{\epsilon}_f(1) = \lambda^{\epsilon}_F(0) = 0$. Supposons-le vrai jusqu'au degré $n-1$ et soit $v = xu$, de degré n avec $x \in M$ et $u \in T_{n-1}(M)$. Alors,

$\lambda^{\epsilon}_F \circ j_f(v) = \lambda^{\epsilon}_F \circ (j^{\epsilon}_f \circ e_x)(u) = \lambda^{\epsilon}_F \circ (-\epsilon\, e_x \circ j^{\epsilon}_f + f(x)\, 1_{T(M)})(u) =$

$= -\epsilon\, \lambda^{\epsilon}_F \circ e_x \circ j^{\epsilon}_f(u) + f(x)\, \lambda^{\epsilon}_F(u) = -\epsilon\,(e_x + j^{\epsilon}_{F,x}) \circ \lambda^{\epsilon}_F \circ j^{\epsilon}_f(u) + f(x)\, \lambda^{\epsilon}_F(u)$.

D'après l'hypothèse de récurrence, on a $\lambda^{\epsilon}_F \circ j^{\epsilon}_f(v) = -\epsilon\, e_x \circ j^{\epsilon}_f \circ \lambda^{\epsilon}_F(u) +$

$+ f(x)\, \lambda^{\epsilon}_F(u) - \epsilon\, j^{\epsilon}_{F,x} \circ j^{\epsilon}_f \circ \lambda^{\epsilon}_F(u) = (f(x)\, 1_{T(M)} - \epsilon\, e_x \circ j^{\epsilon}_f)(\lambda^{\epsilon}_F(u)) + j^{\epsilon}_f \circ$

$\circ\, j^{\epsilon}_{F,x} \circ \lambda^{\epsilon}_F(u) = (j^{\epsilon}_f \circ e_x \circ \lambda^{\epsilon}_F)(u) + j^{\epsilon}_f \circ j^{\epsilon}_{F,x} \circ \lambda^{\epsilon}_F(u) = j^{\epsilon}_f \circ (e_x + j^{\epsilon}_{F,x}) \circ$

$\circ\, \lambda^{\epsilon}_F(u) = j^{\epsilon}_f \circ \lambda^{\epsilon}_F \circ e_x(u) = j^{\epsilon}_f \circ \lambda^{\epsilon}_F(v)$, d'où le résultat annoncé.

Les autres assertions se démontrent aisément : λ^{ϵ}_F respecte la filtration de $T(M)$ à cause de la formule qui donne $\lambda^{\epsilon}_F(x\,u)$, $x \in M$, en utilisant $\lambda^{\epsilon}_F(1) = 1$. Pour voir que λ^{ϵ}_F induit l'identité sur le gradué associé qui est $T(M)$ lui même, il suffit de montrer que si u est homogène de degré n, $\lambda^{\epsilon}_F(u) - u$ est de degré inférieur ou égal à $n-1$, ce qui se démontre par récurrence sur le degré de u ; ceci est vrai si $n = 0$ car $\lambda^{\epsilon}_F(1) = 1$. Supposons-le vrai pour n et soit $v = x\,u$, $x \in M$ où u est homogène de degré n. On a $\lambda^{\epsilon}_F(v) - v = \lambda^{\epsilon}_F(x\,u) -$

$- x\,\lambda^{\epsilon}_F(u) + x\,\lambda^{\epsilon}_F(u) - x\,u = j^{\epsilon}_{F,x}(\lambda^{\epsilon}_F(u)) + x(\lambda^{\epsilon}_F(u) - u)$. Or, d'après le lemme 2.3.1., le degré de $j^{\epsilon}_{F,x}(\lambda^{\epsilon}_F(u))$ est inférieur ou égal à $n-1$ et, d'après l'hypothèse de récurrence, il en est de même de celui de $\lambda^{\epsilon}_F(u) - u$. Donc le degré de $\lambda^{\epsilon}_F(v) - v$ est inférieur ou égal à n. Ceci montre que λ^{ϵ}_F est une bijection de

$T(M)$ dans $T(M)$.

Pour la dernière assertion, λ_o^ε est clairement l'identité car $j_{0,x}^\varepsilon$ est l'application nulle et la condition (ii) signifie que λ_o^ε est $T(M)$-linéaire à gauche ; comme $\lambda_o^\varepsilon(1) = 1$, $\lambda_o^\varepsilon = 1_{T(M)}$. Soit G une seconde forme A-bilinéaire. On vérifie aisément que $\lambda_F^\varepsilon \circ \lambda_G^\varepsilon$ vérifie les mêmes conditions (i) et (ii) que $\lambda_{F+G}^\varepsilon$, d'où leur égalité, en utilisant le fait que λ_F^ε et j_f^ε commutent. Remarquons qu'alors $(\lambda_F^\varepsilon)^{-1} = \lambda_{-F}^\varepsilon$. Ceci achève la démonstration du lemme.

Soit φ une forme A-bilinéaire alternée sur le A-module M. On notera $R(M,\varphi)$ la A-algèbre $T(M)/I(\varphi)$, où $I(\varphi)$ est l'idéal bilatère de $T(M)$ engendré par les éléments $x\,y - y\,x - \varphi(x,y)$, x et y parcourant M. Cette algèbre possède des propriétés fonctorielles analogues à celles de l'algèbre de Clifford d'une forme quadratique, que nous ne donnerons pas ici (cf. [38]).

Notons cependant que si φ est la forme nulle, l'algèbre $R(M,\varphi)$ est l'algèbre symétrique $S_A(M)$ du A-module M. Signalons le complément suivant au lemme 2.3.1. où q désigne une forme quadratique sur M et φ une forme alternée :

Lemme 2.3.3. Soit $f \in M^*$. L'idéal $I(q)$ est stable par l'application j_f^1 et l'idéal $I(\varphi)$ est stable par j_f^{-1}.

En effet, la condition (ii) du lemme 2.3.1. montre que l'ensemble des éléments u de $I(q)$ (resp. $I(\varphi)$) tels que $j_f^1(u) \in I(q)$ (resp. $j_f^{-1}(u) \in I(\varphi)$) est un idéal à gauche. Il suffit donc de montrer que pour $u = (x^2 - q(x))\,v$ (resp. $u = (x\,y - y\,x - \varphi(x,y))\,v$), où v est dans $T(M)$, $j_f^1(u) \in I(q)$ (resp. $j_f^{-1}(u) \in I(\varphi)$).

Regardons le premier cas : $j_f^1(u) = j_f^{1\prime} \circ e_x \circ e_x(v) - q(x)\,j_f^1(v) = (-e_x \circ j_f^1 \circ e_x + f(x)\,1_{T(M)} \circ e_x)(v) - q(x)\,j_f^1(v)$ et en appliquant à nouveau la condition (ii) du lemme 2.3.1., on trouve $j_f^1(u) = (x^2 - q(x))\,j_f^1(v) \in I(q)$. La démonstration est identique dans le second cas.

Soit F une forme A-bilinéaire sur M. On notera $\widetilde{F}$ la forme A-bilinéaire définie sur M par $\widetilde{F}(x,y) = F(x,y) - F(y,x)$. On a alors le résultat suivant :

Lemme 2.3.4. L'application λ_F^1 applique l'idéal $I(q)$ sur l'idéal $I(q')$ où q' est la forme quadratique sur M définie par $x \mapsto q(x) - F(x,x)$. L'application λ_F^{-1} applique l'idéal $I(\varphi)$ sur l'idéal $I(\varphi')$ où φ est la forme alternée $\varphi - \widetilde{F}$.

Comme λ_F^ε est une bijection dont l'inverse est λ_{-F}^ε, il suffit de montrer que $\lambda_F^1(I(q))$ est contenu dans $I(q')$ (resp. $\lambda_F^{-1}(I(\varphi)) \subset I(\varphi')$). Comme $I(q')$ (resp. $I(\varphi')$) est stable par j_f^1 (resp. j_f^{-1}), l'ensemble des u de $T(M)$

tels que $\lambda_F^1(u) \in I(q')$ (resp. $\lambda_F^{-1}(u) \in I(\varphi')$) est un idéal à gauche d'après la condition (ii) du lemme 2.3.2. Il suffit donc de considérer, dans le premier cas, $\lambda_F^1((x^2 - q(x))\, v)$ et dans le second, $\lambda_F^{-1}((x\,y - y\,x - \varphi(x,y))\, v)$. Or, $\lambda_F^1((x^2 - q(x))\, v) = \lambda_F^1 \circ e_x \circ e_x(v) - q(x)\, \lambda_F^1(v) = (e_x + j_{F,x}^1)^2 \circ \lambda_F^1(v) - q(x)\, \lambda_F^1(v) = (e_x \circ e_x - q(x)\, 1_{T(M)})\,(\lambda_F^1(v)) + (e_x \circ j_{F,x}^1 + j_{F,x}^1 \circ e_x)(\lambda_F^1(v))$. Le second terme est, par définition de $j_{F,x}^1$, $F(x,x)\, 1_{T(M)}$, donc $\lambda_F^1((x^2 - q(x))v) = (x^2 - q'(x))\, \lambda_F^1(v)$.

Dans le second cas, calculons $\lambda_F^{-1} \circ (e_x \circ e_y - e_y \circ e_x)$. D'après le lemme 2.3.2., c'est $((e_x + j_{F,x}^{-1}) \circ (e_y + j_{F,y}^{-1}) - (e_y + j_{F,y}^{-1}) \circ (e_x + j_{F,x}^{-1})) \circ \lambda_F^{-1} = (e_x \circ e_y - e_y \circ e_x) \circ \lambda_F^{-1} + (e_x \circ j_{F,y}^{-1} - j_{F,y}^{-1} \circ e_x) \circ \lambda_F^{-1} - (e_y \circ j_{F,x}^{-1} - j_{F,x}^{-1} \circ e_y) \circ \lambda_F^{-1}$ car $j_f^\varepsilon \circ j_g^\varepsilon = j_g^\varepsilon \circ j_f^\varepsilon$. Mais on a $e_x \circ j_{F,y}^{-1} - j_{F,y}^{-1} \circ e_x = -F_y(x)\, 1_{T(M)} = -F(y,x)\, 1_{T(M)}$ et $e_y \circ j_{F,x}^{-1} - j_{F,x} \circ e_y = F(x,y)\, 1_{T(M)}$, donc $\lambda_F^{-1}((x\,y - y\,x - \varphi(x,y))\, v) = (x\,y - y\,x - \varphi'(x,y))\, \lambda_F^{-1}(v)$ et le lemme est ainsi démontré.

Le lemme 2.3.4. peut s'énoncer ainsi :

Lemme 2.3.4'. L'application λ_F^1 induit, par passage aux quotients, un isomorphisme de A-modules filtrés entre $C(M,q)$ et $C(M,q')$; l'application λ_F^{-1} induit, par passage aux quotients, un isomorphisme de A-modules filtrés entre $R(M,\varphi)$ et $R(M,\varphi')$.

On sait que $C(M,q)$ et $R(M,\varphi)$ sont des A-algèbres filtrées par la filtration induite par la filtration canonique de $T(M)$ et les algèbres graduées associées sont engendrées sur A par l'image de M ; ce sont des quotients de $T(M)$. Comme $\rho(x)^2 = q(x)$ (resp. $\rho(x)\,\rho(y) - \rho(y)\,\rho(x) = \varphi(x,y)$) dans $C(q)$ (resp. $R(M,\varphi)$), où $\rho : M \to C(M,q)$ (resp. $\rho : M \to R(M,\varphi)$) est l'application A-linéaire canonique, ces algèbres graduées sont quotients de $\wedge(M)$ et de $S(M)$ respectivement. On a alors le résultat suivant :

Théorème 2.3.5. Supposons que le A-module M soit libre ou bien que 2 soit inversible dans A. Alors, pour toute forme quadratique q sur M et pour toute forme alternée φ sur M, il existe un isomorphisme de A-modules filtrés de $C(M,q)$ sur $\wedge(M)$ et de $R(M,\varphi)$ sur $S(M)$.

Montrons que, dans les conditions du théorème, il existe $F : M \times M \to A$, A-bilinéaire telle que l'on ait $F(x,x) = q(x)$ dans le cas d'une forme quadratique q et qu'il existe $G : M \times M \to A$ telle que $G(x,y) - G(y,x) = \varphi(x,y)$ dans le cas d'une forme alternée φ sur M. Si 2 est inversible dans A, il est clair qu'il

suffit de prendre $F(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$ et $G(x,y) = \frac{1}{2}\varphi(x,y)$, x et y parcourant M. Si M est libre, soit $(x_i)_{i \in J}$ une base de M et ordonnons totalement l'ensemble des indices J. Posons alors $F(x_i,x_j) = q(x_i + x_j) - q(x_i) - q(x_j)$ si $i > j$, $F(x_i,x_i) = q(x_i)$ pour tout $i \in I$ et $F(x_i,x_j) = 0$, sinon ; et $G(x_i,x_j) = \varphi(x_i,x_j)$ si $i > j$ et $G(x_i,x_j) = 0$, sinon. Dans le second cas, on a bien $\tilde{G} = \varphi$; dans le premier cas, $F(\sum_{i\in J} a_i x_i , \sum_{i\in J} a_i x_i) =$

$= \sum_{i\in J} a_i^2 F(x_i,x_i) + \sum_{i<j} a_i a_j (F(x_i,x_j) + F(x_j,x_i))$ et $q(\sum_{i \in J} a_i x_i) =$

$= \sum_{i\in J} a_i^2 q(x_i) + \sum_{i<j} a_i a_j F_q(x_i,x_j)$, où $F_q(x_i,x_j) = q(x_i+x_j) - q(x_i) - q(x_j)$ est bien égal à $F(x_i,x_j) + F(x_j,x_i)$, donc $q(x) = F(x,x)$ pour tout x dans M. Le lemme 2.3.4'. nous donne alors le résultat. Notons que $\Lambda(M)$ et $S(M)$ sont des algèbres filtrées et graduées, donc que les isomorphismes du théorème précédent induisent des isomorphismes de A-modules gradués entre $\mathrm{Gr}\, C(M,q)$ et $\Lambda(M)$ (resp. $\mathrm{Gr}\, R(M,\varphi)$ et $S(M)$).

Corollaire 2.3.6. Dans les hypothèses du théorème précédent, les algèbres graduées associées à $C(M,q)$ et à $R(M,\varphi)$ sont respectivement isomorphes à $\Lambda(M)$ et $S(M)$.

Corollaire 2.3.7. Supposons M libre et soit $(e_i)_{i \in J}$ une base de M avec J totalement ordonné. Alors $C(M,q)$ est un A-module libre dont une base est constituée des produits $\rho(e_{i_1}) \ldots \rho(e_{i_q})$ pour toute suite strictement croissante d'indices $i_1 < \ldots < i_q$. En particulier $C(M,q)$ est une A-algèbre fidèle et l'application canonique $\rho : M \to C(M,q)$ est injective.

Notons F^n l'image dans $C(M,q)$ de la filtration de $T(M)$: $A = F^0 \subset F^1 \subset \ldots \subset F^n \subset F^{n+1} \subset \ldots$ On a la suite exacte $0 \to F^{n-1} \to F^n \to F^n/F^{n-1} \to 0$ et F^n/F^{n-1} est, d'après le corollaire 2.3.6., isomorphe à $\Lambda^n M$. Chaque F^n est libre (démonstration par récurrence sur n, à l'aide de la suite exacte précédente) et une base de F^n s'obtient en ajoutant à une base de F^{n-1} un système de représentants R_n de F^n modulo F^{n-1}. La réunion des R_n est une base de $C(M,q)$ car la filtration F^n est exhaustive. Il suffit donc de voir que les images des $\rho(e_{i_1}) \ldots \rho(e_{i_n})$ pour $i_1 < \ldots < i_n$ forment une base de F^n modulo F^{n-1}. Or, $\lambda^1_F(e_{i_1} \ldots e_{i_n}) = e_{i_1} \ldots e_{i_n} + r_n$, où r_n est de degré inférieur ou égal à n-1. En passant à $C(M,q)$ et $\Lambda(M)$, on a $\lambda^1_F(\rho(e_{i_1}) \ldots \rho(e_{i_n})) = \overline{e_{i_1}} \ldots \overline{e_{i_n}}$, où les $\overline{e_i}$ sont les images des e_i dans $C(M,q)$ et le produit, le produit extérieur. Vu les résultats bien connus sur la base de l'algèbre extérieure d'un module

libre, le corollaire est démontré.

Dans le cas d'un module plat, on a le corollaire suivant :

Corollaire 2.3.8. Soient (M,q) un A-module quadratique où M est un A-module plat. Alors, $C(M,q)$ est une A-algèbre plate et l'application A-linéaire canonique $\rho : M \to C(M,q)$ est injective.

Il suffit de remarquer que M est limite inductive de modules libres et d'appliquer le corollaire précédent.

2.4. EXTENSIONS QUADRATIQUES

Soient A un anneau commutatif à élément unité, B une A-algèbre associative à élément unité et B^0 la A-algèbre opposée de B. La loi de composition $(b \otimes c^0)z = b\,z\,c$ avec $b \in B$, $c^0 \in B^0$ et $z \in B$ fait de B un $B \otimes B^0$-module à gauche, où le produit tensoriel est pris sur A. On dira que B est une A-algèbre séparable si B est un $B \otimes B^0$-module projectif. Comme la multiplication $\mu : B \otimes B^0 \to B$, $b \otimes c^0 \mapsto b\,c$ est $B \otimes B^0$-linéaire, si B est un $B \otimes B^0$-module projectif, il est nécessairement de type fini.

On dira qu'une A-algèbre B est une extension quadratique de A si B est une A-algèbre séparable et si B est un A-module projectif de type fini et de rang 2.

Une conséquence immédiate de cette définition est qu'une extension quadratique B de A est une algèbre commutative : il suffit pour cela de le voir localement. En effet, B est engendrée sur A par un seul élément car $1_B (= 1_A)$ est élément de base du A-module B.

Exemples. 2.4.1. Supposons que A est un corps : B est une A-algèbre de rang 2. Si B est sans diviseurs de zéro, c'est un corps, extension séparable de A. Si B a des diviseurs de zéro, B est sans radical, donc sans éléments nilpotents et s'identifie au produit $A \times A$. Dans les deux cas B possède un seul A-automorphisme distinct de l'identité.

2.4.2. Supposons que A est un anneau local d'idéal maximal $\mathfrak{m}$. Alors $B = A[x]$ avec $x^2 = bx + c$ avec b et c dans A et B est une extension quadratique de A si $B/\mathfrak{m}B$ est une extension quadratique du corps $A/\mathfrak{m}$. Or, dans le cas d'un corps, la séparabilité signifie que l'équation a son discriminant non nul. Donc une condition nécessaire est que $b^2 + 4c \notin \mathfrak{m}$. Si 2 est inversible dans A, B peut s'écrire $A[y]$ avec $y^2 = \alpha \notin \mathfrak{m}$ (on prend $y = x - \frac{b}{2}$) ; si 2 est dans l'idéal maximal de A, alors $b \notin \mathfrak{m}$ et, en posant $z = b^{-1}x$, on a $B = A[z]$ avec $z^2 - z + \alpha = 0$ et $\alpha \in A$. Le cas où 2 est inversible peut se ramener à celui-là

en posant $z = -x + \frac{1}{2}$ et on a alors $1 - 4\alpha \notin \mathfrak{m}$. Il s'agit donc de vérifier la séparabilité de $A[z]$ avec $z^2 = z - \alpha$ et $1 - 4\alpha \notin \mathfrak{m}$; soit donc $B \otimes B = A[z,t]$ avec $z^2 = z - \alpha$ et $t^2 = t - \alpha$. On montre aisément que l'élément $\varepsilon = (1 - 4\alpha)^{-1}((1 - 2\alpha) - (z + t) + 2zt)$ vérifie $\varepsilon^2 = \varepsilon$, $\mu(\varepsilon) = 1$ et $\mathrm{Ker}(\mu)\varepsilon = 0$. Ceci montre que B s'identifie, en tant que $B \otimes B$-module, à $(B \otimes B)\varepsilon$ et est séparable sur A.

Pour tout entier $n \geq 0$, considérons l'ensemble $A(n) = \{a \mid a \in A, 1 - n\,a \in U(A)\}$. La loi de composition $a \tilde{+} b = a + b - n\,a\,b$, $a,b \in A(n)$, munit $A(n)$ d'une structure de groupe abélien d'élément neutre 0 ; $A(0) = A^+$, le groupe abélien additif sous-jacent à A. L'application $\varphi : A(2) \mapsto A(4)$ définie par $x \mapsto x - x^2$ est un morphisme de groupes abéliens dont le noyau $\mathrm{Ip}(A)$ est le groupe des idempotents de l'anneau A. Si $G(A)$ désigne le conoyau de cet homomorphisme, on a la suite exacte de groupes abéliens $0 \to \mathrm{Ip}(A) \to A(2) \xrightarrow{\varphi} A(4) \to G(A) \to 0$. Le caractère fonctoriel de Ip, $.(n)$ et G est facile à établir.

On a ainsi une application de $A(4)$ dans l'ensemble $\mathfrak{D}(A)$ des classes d'isomorphismes d'extensions quadratiques de A définie par $a \mapsto A[x]$ avec $x^2 = x + a$ et la discussion précédente montre que si A est local, cette application est surjective. Cherchons maintenant à quelle condition a et a', éléments de $A(4)$, ont la même image dans $\mathfrak{D}(A)$. Il s'agit, si $B = A[x]$ avec $x^2 = x - a$, de chercher $y = \alpha x + \beta$, tel que $B = A[y]$ et $y^2 = y - a' \in A$. Or, $y - y^2 = (1 - (\alpha + 2\beta))x + \beta - \beta^2 + a\alpha^2$ et comme on veut que $B = A[y]$, α doit être inversible et $\alpha = 1 - 2\beta$, soit $\beta \in A(2)$. On voit donc que a et a', éléments de $A(4)$, ont même image dans $\mathfrak{D}(A)$ si et seulement si il existe $\beta \in A(2)$ tel que $a' - a = (\beta - \beta^2)(1 - 4a)$. On en déduit un isomorphisme de groupes abéliens $G(A) \xrightarrow{\sim} \mathfrak{D}(A)$.

2.4.3. Soit $A \to A'$ un homomorphisme d'anneaux commutatifs à élément unité. $A' \otimes_A B$ est une extension quadratique de A' si B l'est de A. La réciproque est vraie si A' est une extension fidèlement plate de A.

Au sujet des extensions séparables d'un anneau, on a le résultat suivant (cf. [54]) : une A-algèbre commutative et séparable, qui est un A-module projectif de type fini et fidèle et de rang n, peut être plongé dans une extension galoisienne de A, projective de type fini et de rang $n!$. Appliquant ceci à une extension quadratique de l'anneau A, on obtient :

Proposition 2.4.4. *Etant donnée une extension quadratique B d'un anneau A, il existe un seul A-automorphisme σ de B linéairement indépendant de l'identité et l'anneau des invariants $B^\sigma = \{x \mid x \in B \text{ et } \sigma(x) = x\}$ coïncide avec A.*

Cette propriété peut se voir directement de la manière suivante : locale-

ment, $B = A[x]$ avec $x^2 - x + a = 0$ et $1 - 4a \in U(A)$. Localement signifie que pour tout idéal premier $\mathfrak{p}$ de A, il existe un voisinage (affine) de $\mathfrak{p}$ dans Spec (A) au dessus duquel B a la forme annoncée. Si $\sigma : B \mapsto B$ est un A-automorphisme linéairement indépendant de l'identité, il est déterminé par $\sigma(x) = \alpha x + \beta$, $\alpha \in U(A)$ et $(\sigma(x))^2 = \sigma(x) - a$, d'où, après calculs et en utilisant le fait que $1 - 4a \in U(A)$, $\sigma(x) = 1 - x$. Ceci montre l'existence et l'unicité de σ.

Ceci permet de définir la <u>norme</u> $N : B \to A$ sur B par $N(x) = x\,\sigma(x)$: c'est une forme quadratique sur le A-module B car $N(c\,x) = c^2 N(x)$ si $c \in A$ et $N(x + y) - N(x) - N(y) = x\,\sigma(y) + y\,\sigma(x)$ dépend linéairement de x et de y. Il est facile de voir que c'est une forme non dégénérée : on regarde localement et si $B = A[x]$ avec $x^2 = x - a$, $N(\alpha + \beta x) = \alpha^2 + \alpha\beta + a\beta^2$ a pour matrice $\begin{pmatrix} 2 & 1 \\ 1 & 2a \end{pmatrix}$ de déterminant $-(1 - 4a)$, qui est inversible.

On définit, de même, la <u>trace</u> $Tr : B \to A$ sur B par $Tr(u) = u + \sigma(u)$ qui est une application A-linéaire de B dans A et surjective comme on le voit localement. Un invariant intéressant est le noyau de la trace $X(B)$: on a la suite exacte de A-modules $0 \to X(B) \to B \xrightarrow{Tr} A \mapsto 0$ ce qui montre que B s'identifie, en tant que A-module, à $A \oplus X(B)$ et que $X(B)$ est un A-module projectif de type fini et de rang 1, isomorphe à $\Lambda^2 B$.

<u>Exemples</u>. 2.4.5. Si $2 = 0$ dans A, $X(B) = \operatorname{Ker} Tr = \{x \mid x \in B, \sigma(x) + x = 0\} = \{x \mid x \in B, \sigma(x) = x\} = B^\sigma = A$, donc B est un A-module libre de rang 2. Ainsi toute extension quadratique B de A s'écrit $A[x]$ avec $x^2 = b\,x - c$ et $b^2 - 4c = b^2 \in U(A)$, d'où, en posant $y = b^{-1}x$, $B = A[y]$ avec $y^2 = y - b^{-2}c$. L'ensemble des classes d'isomorphismes d'extensions quadratiques de A est en bijection avec A modulo la relation d'équivalence $a \sim b$ si et seulement si il existe un élément $c \in A$ tel que $a - b = c + c^2$. Notons que cette situation ressemble au cas local et qu'on aurait pu supposer seulement que 2 est dans le radical de Jacobson de l'anneau A.

2.4.6. Dans le cas général, soient x et x' dans $X(B)$: $\sigma(x\,x') = \sigma(x)\sigma(x') = (-x)(-x') = x\,x'$, donc $x\,x' \in B^\sigma = A$. On obtient ainsi une application A-bilinéaire $X(B) \times X(B) \to A$, c'est à dire, une application A-linéaire notée μ_B : $X(B) \otimes X(B) \to A$. Pour montrer que c'est un isomorphisme, nous allons regarder localement. Soit $B = A[t]$ avec $t^2 = t - \alpha$ et $1 - 4\alpha \in U(A)$. On a $Tr(at + b) = at + b + a(1 - t) + b = a + 2b$, donc $X(B) = \{b(1 - 2t) \mid b \in A\}$. L'application μ_B envoie $b(1 - 2t) \otimes b'(1 - 2t)$ sur $b\,b'(1 - 2t)^2$ et $(1 - 2t)^2 = 1 - 4(t - t^2) = 1 - 4\alpha$, soit μ_B est surjective, donc c'est un isomorphisme.

2.4.7. Supposons maintenant que $2 \in U(A)$: l'automorphisme σ de l'extension quadratique B de A vérifie $\sigma^2 = id_B$. On a donc la décomposition $id_B = \frac{id_B + \sigma}{2} + \frac{id_B - \sigma}{2}$ de l'identité de B en somme de deux idempotents orthogonaux et B est somme directe de $\mathrm{Ker}\,(\frac{id_B + \sigma}{2}) = X(B)$ et de $\mathrm{Ker}\,(\frac{id_B - \sigma}{2}) = B^{\sigma} = A\,1_B$. La multiplication de B est alors donnée par l'application μ_B. On a la formule $b\,b' = (a,x)\,(a',x') = (aa' + \mu_B\,(x \otimes x'),\ a\,x' + a'\,x)$, où a et a' sont dans A et x et x' dans X(B). On a alors $\sigma(a,x) = (a, -x)$, $N(a,x) = a^2 - \mu_B\,(x \otimes x)$ et $\mathrm{Tr}\,(a,x) = 2a$.

Inversement, soit P un A-module projectif de type fini et de rang 1 et $\mu : P \otimes P \to A$ un isomorphisme de A-modules. Le A-module $B = A \oplus P$ est muni d'une structure de A-algèbre par $(a,x)\,(a',x') = (a\,a' + \mu(x \otimes x'),\ a\,x' + a'\,x)$ et B est une extension quadratique séparable de A car 2 est inversible dans A. Localement, B est la forme $A[x]$ avec $x^2 \in U(A)$.

2.4.8. Structure de groupe sur l'ensemble $\mathfrak{D}(A)$. Soient B et B' deux extensions quadratiques de A. L'algèbre $C = B \otimes B'$ est une extension galoisienne de A de groupe de Galois $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ formé de l'identité, $\sigma_B \otimes id_{B'}$, $id_B \otimes \sigma_{B'}$ et $\sigma_B \otimes \sigma_{B'}$. Comme G possède trois sous-groupes (distingués) isomorphes à $\mathbb{Z}/2\mathbb{Z}$, C possède trois sous-extensions quadratiques B, B' et l'anneau des invariants de $\sigma_B \otimes \sigma_{B'}$ qu'on notera $B * B'$. Il est clair que la classe d'isomorphisme de $B * B'$ ne dépend que de celles de B et de B', donc que la loi $*$ est une loi de composition interne commutative sur l'ensemble $\mathfrak{D}(A)$. L'anneau $B_o = A \times A$ ayant comme unique A-automorphisme linéairement indépendant de l'identité $\sigma(a,b) = (b,a)$ pour a et b parcourant A, est une extension quadratique de A et un calcul trivial montre que $B * B_o$ (et $B_o * B$) est isomorphe à B.

Pour montrer l'associativité de la loi $*$, considérons trois extensions quadratiques B_1, B_2 et B_3 ; $(B_1 * B_2) * B_3$ est, dans $D = B_1 \otimes B_2 \otimes B_3$, l'anneau des invariants du sous-groupe de Galois engendré par $\sigma_{B_1} \otimes \sigma_{B_2} \otimes id_{B_3}$ et $(\sigma_{B_1} \otimes id_{B_2}) \otimes \sigma_{B_3}$ en notant que $\sigma_{B_1 * B_2}$ n'est autre que la restriction à $B_1 * B_2$ de $\sigma_{B_1} \otimes id_{B_2}$ (ou de $id_{B_1} \otimes \sigma_{B_2}$). Ainsi, $(B_1 * B_2) * B_3 = (B_1 \otimes B_2 \otimes B_3)^H$ où H est le sous-groupe formé des éléments id_D, $\sigma_{B_1} \otimes \sigma_{B_2} \otimes id_{B_3}$, $\sigma_{B_1} \otimes id_{B_2} \otimes \sigma_{B_3}$ et $id_{B_1} \otimes \sigma_{B_2} \otimes \sigma_{B_3}$. On voit bien ici que cette condition est invariante par permutation de B_1, B_2 et B_3, d'où l'associativité. On a donc sur

l'ensemble $\mathfrak{D}(A)$ une loi de composition interne qui en fait un groupe abélien.

Considérons maintenant $B \otimes_A B$; en tant que B-algèbre c'est isomorphe à $B[e]$ avec $e^2 = e$, donc cela contient les trois extensions quadratiques de A suivantes: $B \otimes 1$, $1 \otimes B$ et $A[e]$ avec $e^2 = e$. Nécessairement, on a $B * B \simeq$ $\simeq A[e] \simeq A \times A$. Ceci montre que dans le groupe $\mathfrak{D}(A)$, tout élément est d'ordre 2.

La propriété suivante est claire : $\mathfrak{D}$ est un foncteur covariant défini dans la catégorie des anneaux commutatifs unitaires à valeurs dans la catégorie des groupes abéliens. De plus, comme il a été vu ci-dessus, la classe de B est toujours dans le noyau de l'homomorphisme $\mathfrak{D}(A) \to \mathfrak{D}(B)$.

Exemples. 2.4.9. Si A est un corps de caractéristique différente de 2, $\mathfrak{D}(A)$ s'identifie au groupe $U(A)/U^2(A)$ quotient du groupe multiplicatif des éléments non nuls de A par le groupe des carrés de ces mêmes éléments. En effet, une extension quadratique de A est un anneau $B = A[x]$ avec $x^2 = a$, $a \neq 0$ et a est déterminé à un carré près car si $A[y] \simeq A[x]$ et $y^2 = b \in A$, $y = \alpha x$ et $\alpha^2 a = b$. De plus, $A[x] * A[x']$, $x^2 = a$, $x'^2 = a'$, est l'anneau $A[x \otimes x']$ avec $(x \otimes x')^2 = a a'$.

2.4.10. Si A est un anneau de caractéristique 2, on a vu que si B est une extension quadratique de A, B est de la forme $A[x]$ avec $x^2 + x + \alpha = 0$, $\alpha \in A$. Si $A[x]$ et $A[x']$ sont isomorphes et $x'^2 + x' + \alpha' = 0$, comme $Tr(x) = Tr(x') = 1$, $x - x' \in A$ et $x' = x + a$ et on a aisément $\alpha' = \alpha + a + a^2$. Ainsi, notant $\mathfrak{p}$ l'homomorphisme de A dans A défini par $\mathfrak{p}(a) = a + a^2$, on a $\mathfrak{D}(A) = A/\mathfrak{p}A$.

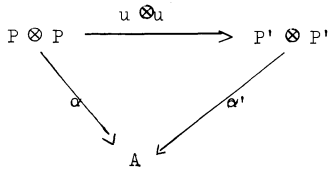
2.4.11. Supposons que A est un anneau local. On a vu que $\mathfrak{D}(A)$ est l'ensemble quotient de l'ensemble $A(4)$ par la relation d'équivalence $a' \sim a$ si et seulement si il existe $b \in A(2)$ tel que $a' - a = (b - b^2)(1 - 4a)$. Or, si $B = A[x]$ avec $x^2 = x - a$ et $B' = A[x']$ avec $x'^2 = x' - a'$, $a, a' \in A(4)$, $B * B'$ se calcule aisément : $B * B' = A[t]$ avec $t = -(2x \otimes x' - x \otimes 1 - 1 \otimes x')$ et $t^2 = t - (a + a' - 4 a a')$. De plus, la relation d'équivalence entre éléments de $A(4)$ vue en 2.4.2. est exactement la relation d'équivalence modulo le sous-groupe H de $A(4)$ formé des éléments $b - b^2$ où $b \in A(2)$. Ainsi $\mathfrak{D}(A)$ s'identifie au quotient $G(A)$ de $A(4)$ par H. En caractéristique 2, $A(4) \simeq A$, $A(2) \simeq A$ et on retrouve le résultat précédent. Si, par contre, 2 est inversible dans A, $A(4)$ (resp. $A(2)$) s'identifie à $U(A)$ par $a \mapsto 1 - 4a$ (resp. $b \mapsto 1 - 2b$) et dans cette identification μ est l'élévation au carré. Ainsi, $\mathfrak{D}(A)$ $(= G(A))$ s'identifie à $U(A)/U^2(A)$, comme pour un corps de caractéristique différente de 2.

2.4.12. Le groupe $\mathfrak{D}(\mathbb{Z})$ est réduit à zéro. En effet, si B est une extension

quadratique de $\mathbb{Z}$, $B = \mathbb{Z}[x]$ avec $x^2 + b\,x + c = 0$ et $b^2 - 4\,c$ inversible, c'est à dire, $b^2 - 4\,c = \pm 1$. Seul le cas $+1$ est possible car tout carré est congru à 0 ou 1 modulo 4. De plus, b est impair, $b = 2\,n+1$ et $c = n(n+1)$. On a donc $B = \mathbb{Z}[x]$ avec $x^2 + (2\,n+1)x + n(n+1) = 0$ soit $(x + n)(x + n + 1) = 0$. Posant $y = x + n + 1$, $y(y - 1) = 0$. Donc $B = \mathbb{Z}[y]$ avec $y^2 = y$.

On aurait pu remarquer que pour toute extension quadratique non triviale B de $\mathbb{Z}$ (i.e., B non nécessairement séparable sur $\mathbb{Z}$ et $B \neq \mathbb{Z} \times \mathbb{Z}$), $K = \mathbb{Q} \otimes_{\mathbb{Z}} B$ est un corps extension quadratique de $\mathbb{Q}$. Mais alors B s'injecte dans K et même, dans la clôture intégrale de $\mathbb{Z}$ dans K. Or, l'anneau des entiers d'un corps quadratique n'est jamais séparable sur $\mathbb{Z}$ car il y a toujours au moins un nombre premier qui se ramifie.

2.4.13. Le groupe $\mathcal{P}(A)$. On considère les paires (P,α), où P est un A-module projectif de type fini et de rang 1 et α un A-isomorphisme de $P \otimes P$ sur A. Deux paires (P,α) et (P',α') sont dites isomorphes s'il existe un isomorphisme $u : P \xrightarrow{\sim} P'$ de A-modules tel que le diagramme



est commutatif. On appelle $\mathcal{P}(A)$ l'ensemble des classes d'isomorphismes de ces objets.

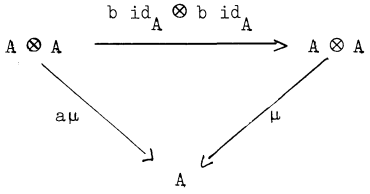
Soient (P,α) et (P',α') deux objets comme ci-dessus. Alors $Q = P \otimes P'$ est un A-module projectif de type fini et de rang 1 et il existe un isomorphisme naturel de $Q \otimes Q$ avec A défini à l'aide de α et α'. Soit, pour cela, la flèche composée $\beta : P \otimes P' \otimes P \otimes P' \xrightarrow{id_P \otimes \tau \otimes id_{P'}} P \otimes P \otimes P' \otimes P' \xrightarrow{\alpha \otimes \alpha'} A \otimes A \xrightarrow{\mu} A$, où μ est la multiplication de A et τ la transposition des facteurs dans le produit tensoriel. Il est clair que (Q,β) dépend, à isomorphisme près, de (P,α) et de (P',α') et on définit ainsi sur l'ensemble $\mathcal{P}(A)$ une loi de composition interne qui en fait, de façon évidente, un groupe abélien. L'élément neutre est la paire (A,μ) et tout élément est son propre inverse car si (Q,β) est le produit $(P,\alpha)\,(P,\alpha)$ l'isomorphisme de A-modules α de $Q = P \otimes P$ avec A est aussi un isomorphisme de (Q,β) avec (A,μ).

Le groupe $\mathcal{P}(A)$, qui dépend fonctoriellement de A, s'exprime aisément

en fonction de groupes mieux connus.

Proposition 2.4.14. Pour tout anneau commutatif à élément unité A, on a la suite exacte de groupes abéliens $U(A) \xrightarrow{2} U(A) \xrightarrow{f} \mathcal{P}(A) \xrightarrow{\tau} Pic(A) \xrightarrow{2} Pic(A)$, où $\xrightarrow{2}$ désigne la multiplication par 2, f l'application définie par $a \mapsto (A, a\mu)$ et τ l'application qui à la classe de (P,α) associe la classe de P dans Pic(A), groupe des classes d'isomorphismes de A-modules projectifs de type fini et de rang 1.

Il est clair que τ est un homomorphisme de groupes et que $2 \circ \tau = 0$. Inversement si $P \in Ker(2)$, cela signifie que $P \otimes P$ est isomorphe à A ; choisissant un isomorphisme α particulier, on obtient une pair (P,α) qui donne un élément de $\mathcal{P}(A)$ dont l'image est P dans Pic(A). Reste à regarder le début de la suite exacte. On a $\tau \circ f = 0$ par construction et si $(P,\alpha) = 0$, P est libre et isomorphe à A ; choisissant un isomorphisme particulier, $P = Ae$ et en posant $a = \alpha(e \otimes e)$, on a immédiatement $f(a) = (P,\alpha)$, d'où l'exactitude en $\mathcal{P}(A)$. Reste à voir l'exactitude en U(A). Si $f(a) = (A,\mu)$ cela signifie qu'il existe $b \in U(A)$ tel que le diagramme



est commutatif. Cela signifie que $a = b^2 \in U^2(A)$, d'où le résultat.

La suite exacte, ci-dessus construite, peut encore s'écrire sous la forme $0 \to U/U^2(A) \to \mathcal{P}(A) \to Pic_2(A) \to 0$, où Pic_2 est le groupe des éléments d'ordre 2 dans Pic. Notons que tous ces groupes sont des espaces vectoriels sur $\mathbb{Z}/(2)$, donc que la suite exacte est sciendée, en tant que suite exacte de $\mathbb{Z}/(2)$-espaces vectoriels.

Proposition 2.4.15. Soit A un anneau commutatif à élément unité. L'application $\mathcal{D}(A) \to \mathcal{P}(A)$ définie par $B \mapsto (X(B), \mu)$ est un homomorphisme de groupes abéliens, fonctoriel en A. Si 2 est inversible dans A, cet homomorphisme est un isomorphisme et si $2 = 0$ dans A, il est nul.

Il est clair que $(X(B), \mu)$ définit un élément de $\mathcal{P}(A)$. Montrons que l'application $B \mapsto (X(B), \mu)$ est un homomorphisme de groupes. Soient pour cela B et B' deux extensions quadratiques de A. Comme X(B) et X(B') sont facteurs directs respectivement de B et de B', $X(B) \otimes X(B')$ s'identifie à un facteur direct de $B \otimes B'$. De plus, $(\sigma \otimes \sigma')(x \otimes x') = \sigma(x) \otimes \sigma'(x') = (-x) \otimes (-x') = x \otimes x'$,

si $x \in X(B)$, $x' \in X(B')$. Cela montre que $X(B) \otimes X(B')$ est un sous-module de $B * B'$ et comme $\sigma_{B * B'}$ est la restriction de $\sigma_B \otimes id_{B'}$ à $B * B'$, $\sigma_{B * B'}(x \otimes x') = \sigma_B(x) \otimes x' = -x \otimes x'$ et $X(B) \otimes X(B')$ s'identifie à un sous-module de $X(B * B')$. On voit alors facilement qu'on a, en fait, l'égalité et que $(X(B), \mu)(X(B'), \mu')$ est égal à $(X(B * B'), \mu_{B * B'})$ car μ n'est autre que la restriction à $X(B)$ de la multiplication de B, d'où la première assertion. Si 2 est inversible, l'homomorphisme de groupes est en fait un isomorphisme à cause de 2.4.7. Si $2 = 0$, $X(B) = B^{\sigma} = A\,1$, donc $(X(B), \mu)$ est l'élément neutre de $\mathcal{P}(A)$.

Les propositions 2.4.14. et 2.4.15. nous donnent un procédé de calcul de $\mathcal{D}(A)$, si 2 est inversible dans A.

2.4.16. L'algèbre de Clifford $C(B,N_B)$. On a vu que la norme, qu'on notera N_B, d'une extension quadratique B est une forme quadratique non dégénérée sur le A-module B. On notera C_B l'algèbre de Clifford de (B,N_B). D'après des résultats de 2.3., c'est un A-module projectif de type fini et de rang 4 et c'est la somme directe de $(C_B)_0$ et de $(C_B)_1$ qui sont chacun de rang 2. Comme $B \to C_B$ est injectif et que B s'identifie à un facteur direct de $(C_B)_1$, B et $(C_B)_1$ sont des A-modules isomorphes. Notons aussi que B est un anneau unitaire et que $N(1_B) = 1$. Donc, si $u \in (C_B)_1$ est l'image canonique de 1_B, on a $u^2 = 1$ dans C_B. Ainsi l'application $C_B \to C_B$ définie par $x \mapsto u\,x$ est un isomorphisme de A-modules qui, comme u est de degré 1, réalise un isomorphisme de $(C_B)_0$ sur $(C_B)_1$.

On pourrait alors montrer que $(C_B)_0$ est isomorphe à B en tant que A-algèbre. Nous allons cependant procéder différemment. Soit $C = B[\sigma]$ l'algèbre associative tordue sur B du groupe $\mathbb{Z}/(2)$, c'est-à-dire, $C = B \oplus B\,\sigma$ en tant que A-module avec pour multiplication $(b_1, b_2\,\sigma)(b_1', b_2'\,\sigma) = (b_1 b_1' + b_2\,\sigma(b_2'), (b_1 b_2' + b_2\,b_1')\,\sigma)$, soit $\sigma b = \sigma(b)\,\sigma$ pour tout $b \in B$. L'algèbre C contient B comme sous-algèbre et elle est $\mathbb{Z}/(2)$-graduée par $C_0 = B\,1$ et $C_1 = B\,\sigma$. Soit u l'application de B dans C définie par $u(b) = b\,\sigma$. On a alors $(u(b))^2 = (b\,\sigma)(b\,\sigma) = N(b)\,1_C$ et il en découle l'existence d'un homomorphisme $\bar{u} : C_B \to C$ qui est surjectif car C est engendré en tant que A-algèbre par $B\,\sigma$. Comme les deux A-modules sous-jacents à C_B et C sont projectifs de type fini et de même rang, $\bar{u}$ est un isomorphisme.

Nous allons montrer maintenant que $C = B[\sigma]$ est isomorphe à l'algèbre des endomorphismes du A-module B. En effet, soient $C' = \mathrm{End}_A(B)$ et $f : B \oplus B\,\sigma \to C'$ l'application définie par $f(b\,1) = \mu_b$ et $f(b\,\sigma) = \mu_b \circ \sigma$ où μ_b désigne la multiplication par b dans B. C'est une application A-linéaire injective car, si $f(b_1 + b_2\sigma) = 0$, avec $b_1, b_2 \in B$, cela signifie $b_1\,id_B + b_2\sigma = 0$ dans $\mathrm{End}_A(B)$, ce qui implique $b_1 = b_2 = 0$. Cela se voit localement. En effet, si A est local,

$B = A[x]$ avec $\sigma(x) = 1-x$ et $b_1\,id_B + b_2\sigma = 0$ équivaut à $b_1 + b_2 = 0$ et $b_1 x + b_2(1-x) = 0$, soit $b_1(1-2x) = b_2(1-2x) = 0$. Or, $x^2 = x-a$ avec $1-4a$ inversible dans A et comme $(1-2x)^2 = 1-4a$, $1-2x$ est aussi inversible dans B. Ceci nous dit que $b_1 = b_2 = 0$. C'est un homomorphisme d'algèbres comme on le vérifie aisément en vérifiant, par exemple, que $f((b\,\sigma)(b'\,\sigma)) = f(b\,\sigma(b'))$ et $f(b\,b') = f(b)f(b')$. Pour voir que c'est un isomorphisme, il suffit de le voir localement, c'est à dire qu'il suffit de montrer que c'est un isomorphisme modulo tout idéal maximal. Mais alors on a un homomorphisme injectif et deux espaces vectoriels de même dimension, c'est donc un isomorphisme. On remarque, à cet effet, que si $\mathfrak{m}$ est un idéal maximal de A, $(A/\mathfrak{m}) \otimes_A B$ est une extension quadratique du corps $A/\mathfrak{m}$.

2.4.17. De l'homomorphisme naturel $\mathfrak{D}(A) \xrightarrow{f} \mathfrak{P}(A)$ et de la suite exacte de groupes abéliens, $0 \to U/U^2(A) \to \mathfrak{P}(A) \xrightarrow{p} Pic_2(A) \to 0$, on déduit la suite exacte $0 \to \mathfrak{D}'(A) \to \mathfrak{D}(A) \xrightarrow{p\,o\,f} Pic_2(A)$ où il se trouve que $\mathfrak{D}'(A)$ est le sous-groupe de $\mathfrak{D}(A)$ formé des extensions quadratiques libres en tant que A-module. De plus, on obtient un homomorphisme naturel $t : \mathfrak{D}'(A) \to U/U^2(A)$, qui est un isomorphisme si 2 est inversible dans A alors qu'en caractéristique 2, $\mathfrak{D}'(A) \simeq Q(A)$ et $t = 0$. Il est intéressant de savoir quand t est injectif (ou ce qui revient au même, f) ; c'est le cas, par exemple, 2 étant nul, si A est intégralement clos. Cela montre par exemple que $\mathfrak{D}(A)$ est fini si A est un anneau d'entiers algébriques. En effet, le théorème des unités montre que $U/U^2(A)$ est un groupe fini et, comme $Pic(A)$ est fini, $\mathfrak{D}(A)$ l'est.

2.5. EXTENSIONS QUADRATIQUES GRADUEES

Soient A un anneau commutatif à élément unité et B une A-algèbre graduée sur $\mathbb{Z}/(2)$, i.e., B est un A-module gradué sur $\mathbb{Z}/(2)$, $B = B_0 \oplus B_1$ vérifiant $B_i\,B_j \subset B_{i+j}$, où $i+j$ est calculé modulo 2. Si B est une extension quadratique de A (dans le sens du § 2.4.), on dira que B est une <u>extension quadratique graduée</u> de A.

Une conséquence de la définition est que B_0, qui est une sous-algèbre de B, et B_1 sont des A-modules projectifs de type fini et que $A.\,1_B$ est contenu dans B_0 et en est, en fait, facteur direct. Ainsi B_1 est un A-module projectif de type fini de rang inférieur ou égal à 1.

<u>Exemples</u>. 2.5.1. Soit B une extension quadratique de A ; posant $B_0 = B$ et $B_1 = (0)$, on obtient une extension quadratique (trivialement) graduée de A.

2.5.2. Soit (P,μ) un élément de $\mathfrak{P}(A)$ et B l'extension quadratique $A \oplus P$ dont la multiplication est définie à l'aide de μ (cf. 2.4.7.) ; posant $B_0 = A$

et $B_1 = P$, on définit sur B une structure d'extension quadratique graduéede A.

Comme B_1 est un A-module projectif de type fini et de rang inférieur ou égal à 1, on peut lui associer un idempotent e de A en le définissant localement par $e = 1$ en $\mathfrak{p} \in \operatorname{Spec} A$ si $A_{\mathfrak{p}} \otimes_A (B_1)$ est non nul et $e = 0$ en $\mathfrak{p} \in \operatorname{Spec} A$ si $A_{\mathfrak{p}} \otimes_A (B_1)$ est réduit en 0. On notera $e(B)$ l'idempotent ainsi construit ; on a aisément les résultats suivants : $e(B) = 0$ si et seulement si B est trivialement graduée et $e(B) = 1$ si et seulement si B est de la forme $A \oplus P$, avec $B_0 = A$ et $B_1 = P$ car alors B_0 est A-projectif de rang 1 et $B_0 \simeq A\,1_B$.

On remarque que si $e(B)_{\mathfrak{p}} = 1$, alors $2 \notin \mathfrak{p}$, i.e., $2 \in U(A_{\mathfrak{p}})$. En effet, il suffit de s'intéresser à $B_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_A B$: c'est une extension quadratique de $A_{\mathfrak{p}}$, donc un $A_{\mathfrak{p}}$-module libre de rang 2 et $(B_{\mathfrak{p}})_1 \neq 0$, soit $B_{\mathfrak{p}} = A_{\mathfrak{p}}[x]$ avec $x^2 = a \in U(A_{\mathfrak{p}})$ où x est un générateur de $(B_{\mathfrak{p}})_1$. La séparabilité de l'équation $x^2 = a$ implique que 2 est inversible dans $A_{\mathfrak{p}}$. En conséquence, si e est un idempotent associé à une extension quadratique B, $2e \in U(Ae)$, comme on le voit aisément par un raisonnement local.

Soit maintenant B une extension quadratique graduée et σ l'unique A-automorphisme non trivial de B. Alors σ respecte la graduation de B. En effet, il suffit de le montrer localement. Supposons donc A local. Si 2 est dans l'idéal maximal de A, $B_1 = (0)$ et le problème ne se pose pas ; si 2 est inversible dans A et $B_1 \neq (0)$, alors $B = A[x]$ avec $x^2 = a \in U(A)$ et $d^0x = 1$. On vérifie immédiatement que $\sigma = \mathrm{id}_{B_0} \oplus - \mathrm{id}_{B_1}$ respecte la graduation de B.

Soient maintenant B et B' deux extensions quadratiques graduées de A et σ et σ' leurs seuls A-automorphismes non triviaux : $B \hat{\otimes} B'$ est une A-algèbre graduée, non nécessairement commutative et $\sigma \otimes \sigma'$ un A-automorphisme qui respecte la graduation de $B \hat{\otimes} B'$. On en déduit que $B * B' = (B \hat{\otimes} B')^{\sigma \otimes \sigma'}$ est encore une extension quadratique graduée de A. Ainsi la loi $*$ induit sur l'ensemble des classes d'isomorphismes d'extensions quadratiques graduées de A une loi de composition interne, associative et commutative. On vérifie bien qu'il y a un élément neutre, l'anneau $A \times A$, muni de la graduation triviale et ayant comme unique A-automorphisme non trivial, la transposition.

On note $\mathfrak{D}_2(A)$ le groupe ainsi défini ; comme le montre l'exemple 2.5.1., $\mathfrak{D}(A)$ apparaît comme un sous-groupe de $\mathfrak{D}_2(A)$.

Proposition 2.5.3. La suite de groupes abéliens $0 \to \mathfrak{D}(A) \to \mathfrak{D}_2(A) \xrightarrow{e} \mathrm{Ip}(A)$ est exacte et l'image de $\mathfrak{D}_2(A)$ est l'ensemble des idempotents e tels que $2e$ est inversible dans Ae.

Pour montrer la première partie, il faut montrer que si $e(B)$ et $e(B')$ sont les idempotents associés aux extensions B et B', alors à $B * B'$ est associé $e(B) \tilde{+} e(B')$. Pour cela il suffit de regarder localement. Si $e(B) = e(B') = 0$, $B \hat{\otimes} B'$ est trivialement gradué et il en est donc de même de $B * B'$. Pour le second cas, supposons $e(B) = 1$ et $e(B') = 0$; cela implique que 2 est inversible dans A et on a $B = A[x]$ avec $x^2 = a$, $d^0 x = 1$ et $B' = A[x']$ avec $x'^2 = a'$, $d^0 x' = 0$. On a alors $B * B' = A[x \otimes x']$ avec $d^0(x \otimes x') = 1$, donc $e(B * B') = e(B) \tilde{+} e(B')$. Si $e(B) = e(B') = 1$ rien de changé à la situation antérieure sinon que $B' = A[x']$ avec $d^0x' = 1$. Alors $B * B' = A[x \otimes x']$ et $d^0(x \otimes x') = d^0x + d^0x' = 0$. Le noyau de l'homomorphisme e n'est autre que $\mathfrak{D}(A)$ car dire que $e(B) = 0$ signifie que B est munie de la graduation triviale, d'où la suite exacte annoncée.

Pour voir que l'image par e est bien le sous-groupe de $Ip(A)$ annoncé, il suffit de considérer l'extension quadratique $B = A \times A$ graduée par $(A \times A)_0 = \{(a,b) \mid e(b - a) = 0\}$ et $(A \times A)_1 = \{(a,-a) \mid (1-e)\, a = 0\}$. Il est facile de voir que B est une extension quadratique graduée de A en utilisant le fait que $2e$ est inversible dans Ae ; on a alors bien $e(B) = e$.

On remarque que si B et B' sont deux extensions quadratiques graduées, alors $B \hat{\otimes} B'$ n'est pas nécessairement une A-algèbre commutative. Ainsi, supposons 2 inversible dans A et soient a et a' dans $U(A)$, $B = A[x]$ avec $x^2 = a$, $d^0x = 1$, $B' = A[x']$ avec $x'^2 = a'$, $d^0x' = 1$. Alors $B \hat{\otimes} B'$ est l'algèbre de Clifford du A-module quadratique $(A \times A, q)$ où $q : A \times A \to A$ est la forme quadratique définie par $(x,x') \mapsto a x^2 + a'x'^2$ et $B * B'$ sa somposante de degré 0, $A[t]$ avec $t^2 = -a a'$.

On définit de la même façon que dans le cas non gradué un groupe $\mathcal{P}_2(A)$ des paires (P,α) où P est un A-module projectif de type fini et de rang 1, gradué sur $\mathbb{Z}/(2)$ et $\alpha : P \otimes P \to A$ un isomorphisme de A-modules gradués (A trivialement gradué)(cf. [32]). On a alors la suite exacte de groupes abéliens $0 \to \to \mathcal{P}(A) \to \mathcal{P}_2(A) \to Ip(A) \to 0$, car la flèche $\mathcal{P}_2(A) \to Ip(A)$ est surjective.

On peut de la même façon que dans le cas non gradué définir un homomorphisme de $\mathfrak{D}_2(A)$ dans $\mathcal{P}_2(A)$ qui est l'homomorphisme nul si $2 = 0$ et un isomorphisme si 2 est inversible dans A (cf. 2.4.15.).

Nous allons montrer que les groupes $\mathcal{P}(A)$ et $\mathcal{P}_2(A)$ opèrent naturellement sur $W(A)$ et $WG(A)$. Pour cela nous recherchons d'abord le groupe $U(Bil(A))$ des éléments inversibles de l'anneau $Bil(A)$. De l'homomorphisme d'anneaux $\dim : Bil(A) \to \mathcal{C}(Spec(A), \mathbb{Z})$, on déduit qu'un élément α de $Bil(A)$ est inversible si et seulement si $\dim \alpha \in \mathcal{C}(Spec(A), \{\pm 1\}) \approx Ip(A)$. On a donc un homomorphisme

dim : $U(Bil(A)) \to Ip(A)$ dont on vérifie immédiatement qu'il est surjectif. Soit alors $U_0(Bil(A))$ le noyau de cet homomorphisme : on a la suite exacte de groupes abéliens $0 \to U_0(Bil(A)) \to U(Bil(A)) \to Ip(A) \to 0$ et $U_0(Bil(A))$ est le sous-groupe formé de paires (P,α) avec P projectif de type fini et de rang 1 et α une forme bilinéaire symétrique non dégénérée sur P. Deux éléments (P,α) et (P',α') ont même image dans $Bil(A)$ s'il existe un module bilinéaire (M,φ) tel que $(P,\alpha) \perp (M,\varphi) \approx (P',\alpha') \perp (M,\varphi)$. Il en résulte en prenant les déterminants, que (P,α) et (P',α') sont isomorphes. Ceci montre que le groupe $U_0(Bil(A))$ s'identifie au groupe $\mathcal{P}(A)$ défini en 2.4. et la suite $0 \to \mathcal{P}(A) \to U(Bil(A)) \to$ $\to Ip(A) \to 0$ de groupes abéliens est exacte. Alors il est facile de montrer que $U(Bil(A))$ s'identifie au groupe $\mathcal{P}_2(A)$ défini ci-dessus.

Du fait de la structure de $Bil(A)$-module définie sur $WG(A)$ et sur $W(A)$ (cf. 1.8.4.), on a une action naturelle de $\mathcal{P}_2(A)$ et de $\mathcal{P}(A)$ sur ces deux groupes abéliens. Elle se décrit, dans le cas de $\mathcal{P}(A)$, de la façon suivante : à une paire $((P,\alpha),(M,q))$, on associe le module quadratique $(P \otimes M, q')$ où $q' : P \otimes M \to A$ est donnée par $q'(x \otimes y) = \alpha(x \otimes x)\, q(y)$ (on notera $\alpha\, q$ la forme quadratique q'). Si A est un corps, $\mathcal{P}(A) \approx U(A)/U^2(A)$ et l'opération de $U(A)/U^2(A)$ sur $WG(A)$ et $W(A)$ consiste en la multiplication de la forme quadratique par un scalaire.

2.5.4. Notons une propriété de l'opération de $\mathcal{P}(A)$ sur $WG(A)$ concernant l'algèbre C_0 : quels que soient le module quadratique (M,q) et l'élément (P,α) de $\mathcal{P}(A)$, $C_0(P \otimes M, \alpha\, q) \approx C_0(M,q)$. Cela se montre aisément (comme dans 2.3.) en remarquant que les algèbres $T_0(M) = \bigoplus_{p \geq 0} (\overset{2p}{\otimes} M)$ et $T_0(P \otimes M) = \bigoplus_{p \geq 0} (\overset{2p}{\otimes} (M \otimes P))$ sont isomorphes et que dans cet isomorphisme les traces des idéaux $I(q)$ et $I(\alpha\, q)$ se correspondent.

2.6. ALGEBRES D'AZUMAYA ET ALGEBRES DE CLIFFORD

Soient A un anneau commutatif à élément unité, B une A-algèbre associative et B^0 son algèbre opposée. On dira que B est une A-<u>algèbre d'Azumaya</u> si B est un A-module projectif de type fini et fidèle et si l'homomorphisme naturel $B \otimes_A B^0 \to End_A(B)$ défini par $b \otimes c^0 \mapsto (z \mapsto b\, z\, c)$ est un isomorphisme de A-algèbres.

Au vu de cette définition, un certain nombre de propriétés sont claires : si B est une A-algèbre d'Azumaya et $A \to A'$ un homomorphisme d'anneaux, $A' \otimes_A B$ est une A'-algèbre d'Azumaya. Inversement, si $A' \otimes_A B$ est une A'-algèbre d'Azumaya et si $A \to A'$ est fidèlement plat, alors B est une A-algèbre d'Azumaya. Si B

et C sont deux A-algèbres d'Azumaya, $B \otimes_A C$ en est une. Un exemple important est le suivant : soit P un A-module projectif de type fini et fidèle. Alors $\mathrm{End}_A(P)$ est une A-algèbre d'Azumaya. Il suffit de vérifier la seconde condition car on sait que $B = \mathrm{End}_A(P)$ est isomorphe à $P \otimes_A P^*$ au moyen de l'homomorphisme $P \otimes_A P^* \to \mathrm{End}_A(P)$ défini par $x \otimes f \mapsto (y \mapsto f(y)x)$. Alors $B^0 \simeq \mathrm{End}_A(P^*)$ et $B \otimes_A B^0 = \mathrm{End}_A(P) \otimes_A \mathrm{End}_A(P^*)$ s'identifie à $\mathrm{End}_A(P \otimes_A P^*)$. Il est alors facile de montrer que ce dernier isomorphisme n'est autre que l'isomorphisme $B \otimes_A B^* \to \mathrm{End}_A(B)$, en identifiant $\mathrm{End}_A(P)$ à $P \otimes P^*$ par l'isomorphisme déjà cité : pour cela on peut procéder localement en prenant une base dans P, la base duale dans P^*, d'où des bases dans $\mathrm{End}_A(P)$, $\mathrm{End}_A(P^*)$, $\mathrm{End}_A(P \otimes P^*)$ et on vérifie qu'elles se correspondent dans l'homomorphisme $B \otimes_A B^0 \to \mathrm{End}_A(B)$.

Les propriétés suivantes sont bien connues (cf. [5], [52], [11] chapitre II, Exercice 13 et suivants, § 5).

2.6.1. Le centre d'une A-algèbre d'Azumaya s'identifie à l'anneau A. Le résultat est bien connu pour l'algèbre des endomorphismes d'un module projectif de type fini et fidèle. Dans le cas général, si x est dans le centre de B, $x \otimes 1_{B^0}$ est dans le centre de $B \otimes_A B^0 \simeq \mathrm{End}_A(B)$, c'est à dire une homothétie, ce qui montre que x est un scalaire.

2.6.2. Les idéaux bilatères d'une algèbre d'Azumaya B sont tous de la forme $I B$ où I est un idéal de A. Ainsi, soit $f : B \to C$ un homomorphisme d'algèbres où B est d'Azumaya et C est fidèle en tant que A-module, alors f est injectif.

2.6.3. Supposons que A est un corps. Une A-algèbre B de rang fini est d'Azumaya si et seulement si B est une A-algèbre centrale simple.

2.6.4. Soient C une algèbre et B une sous-algèbre de C qui est une A-algèbre d'Azumaya ; on notera $C^B = \{x \mid x \in C, xy = yx, \forall\, y \in B\}$ le commutant de B dans C qui est une sous-algèbre de C. Alors C s'identifie en tant qu'algèbre, au produit tensoriel $B \otimes_A C^B$.

2.6.5. Les automorphismes d'une algèbre d'Azumaya peuvent être décrits comme suit : si A est un corps, le théorème de Skolem-Noether dit que tout automorphisme d'une algèbre centrale simple est intérieur. Dans le cas général, il existe une suite exacte de groupes $\{1\} \to \mathrm{Int\ Aut}(B) \to \mathrm{Aut}(B) \xrightarrow{\tau} \mathrm{Pic}(A)$, où $\mathrm{Int\ Aut}(B)$ est le groupe des automorphismes intérieurs de l'algèbre d'Azumaya B et où τ est défini de la façon suivante : si $u \in \mathrm{Aut}(B)$, on note $P_u = \{x \mid x \in B,\ y\,x = x\,u(y),\ \forall\, y \in B\}$. Alors P_u est un sous-A-module de B et c'est un A-module

projectif de type fini et de rang 1, libre si et seulement si u est intérieur. On définit $\tau(u)$ comme étant la classe de P_u dans $\mathrm{Pic}(A)$.

Soit P un A-module projectif de type fini et $h(P)$ l'espace hyperbolique de P, i.e., $h(P) = (P \oplus P^*, q)$ où $q : P \oplus P^* \to A$ est la forme quadratique définie par $(x,f) \mapsto f(x)$. On a alors le théorème suivant :

Théorème 2.6.6. *L'algèbre de Clifford de $h(P)$ est isomorphe à l'algèbre des endomorphismes de A-module de l'algèbre extérieure $\Lambda(P)$ de P. De plus, il s'agit d'un isomorphisme de A-algèbres graduées sur $\mathbb{Z}/(2)$.*

On remarque, tout d'abord, que $\Lambda(P)$ est une A-algèbre graduée sur $\mathbb{Z}/(2)$ par $\Lambda(P)_0 = \bigoplus_{p\geq 0}^{\infty} \Lambda^{2p}(P)$ et $\Lambda(P)_1 = \bigoplus_{p=0}^{\infty} \Lambda^{2p+1}(P)$ et que $\mathrm{End}_A(\Lambda(P))$, en tant que A-algèbre, est graduée sur $\mathbb{Z}/(2)$ par $\mathrm{End}_A(\Lambda(P))_i = \{f \mid f(\Lambda(P)_j) \subset \subset \Lambda(P)_{i+j}\}$, $i = 0,1$, où $i + j$ est calculé modulo 2. C'est de cette graduation-là qu'il s'agit dans l'énoncé du théorème. Passons maintenant à sa démonstration.

Soient $x \in P$ et $f \in P^*$. On note $\mu_x : \Lambda(P) \to \Lambda(P)$ la multiplication à gauche par x et $d_f : \Lambda(P) \to \Lambda(P)$ la dérivation qui prolonge la forme linéaire f, c'est à dire, si $x_1,\ldots,x_n$ sont des éléments de P, $\mu_x(x_1 \wedge \ldots \wedge x_n) = x \wedge x_1 \wedge \ldots \wedge x_n$ et $d_f(x_1 \wedge \ldots \wedge x_n) = \sum_{i=1}^{n} (-1)^{i+1} f(x_i)\, x_i \wedge \ldots \wedge \hat{x}_i \wedge \ldots \wedge x_n$. Notons alors $L : P \oplus P^* \to \mathrm{End}_A(\Lambda(P))$ l'application A-linéaire définie par $(x,f) \mapsto L(x,f) = \mu_x + d_f$. Un calcul facile montre que $(L(x,f))^2 = f(x)\mathrm{id}_{\Lambda(P)}$: on regarde ce qui se passe sur les générateurs $x_1 \wedge \ldots \wedge x_n$ de $\Lambda(P)$.
Du fait de la propriété universelle de l'algèbre de Clifford, L se prolonge en un homomorphisme d'algèbres noté $\varphi_P : C(h(P)) \to \mathrm{End}(\Lambda(P))$ qui respecte les $\mathbb{Z}/(2)$-graduations, car $d^o\, \mu_x = d^o\, d_f = 1$.

Pour montrer que φ_P est un isomorphisme, il suffit de procéder localement. On peut donc supposer P libre et soient $(e_i)_{1\leq i\leq n}$ une base de P et $(e'_i)_{1\leq i\leq n}$ la base duale. Identifions les e_i avec leur image dans $C(h(P))$. Si H est une partie de $I = \{1,\ldots,n\}$, on notera e_H le produit, dans $C(h(P))$, des e_i, $i \in H$, rangés dans l'ordre croissant et e^*_H le produit correspondant des e'_i. On notera, de plus, f_H le produit des e_i dans $\Lambda(P)$, $i \in H$, H' le complémentaire de H dans I et $x_{H,K} = e_H\, e^*_I\, e_{K'} \in C(h(P))$. Si H,K,L sont trois parties de I, $\varphi_P(x_{H,K})(f_L) = 0$ si $K \neq L$ et $\varphi_P(x_{H,K})(f_L) = \varepsilon\, f_H$ si $K = L$, ε étant égal à $+1$ ou -1 suivant H et K. En effet, notons que $\varphi_P(e_A)(f_B) = \varepsilon\, f_{A \cup B}$ si A et B sont deux parties de I, disjointes, et 0 sinon. Ainsi si $K = L$, $\varphi_P(e_{K'})(f_L) = \varepsilon\, f_I$ donc $\varphi_P(e^*_I\, e_{K'})(f_L) = \varepsilon\, \varphi_P(e_{I*})(f_I) = \varepsilon'\, \mathrm{id}_{\Lambda(P)}$,

d'où l'un des résultats voulus. Si, par contre, L diffère de K, $\varphi_P(e_K')(f_L)$ est soit nul, soit un f_J avec Card $J < n$. Comme $\varphi_P(e_I^*)(f_J)$ est nul, on a bien 0 dans tous les cas. Ceci montre que $\varphi_P : C(h(P)) \to \mathrm{End}(\wedge(P))$ est surjectif et comme il s'agit de modules projectifs de type fini et de même rang, à savoir 2^{2n}, si n est le rang de P, cette surjection est un isomorphisme.

Le fait que cet isomorphisme soit gradué, nous renseigne sur $C_0(h(P))$. En effet, $C_0(h(P)) \approx \mathrm{End}_A(\wedge(P)_0) \times \mathrm{End}_A(\wedge(P)_1)$ et $Z(C_0(h(P))) \approx A \times A$. Rappelons que $Z(C)$ est l'anneau A car A est le centre de $\mathrm{End}_A(\wedge(P))$. Soit maintenant B le commutant de $C_0(h(P))$ dans $C(h(P))$. Il s'agit de chercher dans $\mathrm{End}_A(\wedge(P))$ le commutant de la partie homogène de degré 0. Les éléments de $\mathrm{End}_A(\wedge(P))$ étant représentés par des matrices 2×2 du fait de la décomposition $\wedge(P) = \wedge(P)_0 \oplus \wedge(P_1)$, on cherche $\left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \forall \lambda \in \mathrm{End}_A(\wedge(P)_0), \right.$

$\left. \forall \mu \in \mathrm{End}(\wedge(P)_1) \right\}$. Il est immédiat de voir que ce commutant est formé des matrices $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ où α et δ sont des homothéties, c'est à dire que c'est le centre de la partie homogène de degré 0, pourvu que P soit toujours de rang strictement positif. Notons ici que $C = C(h(P))$.

Une <u>algèbre d'Azumaya</u> est une A-algèbre projective de type fini de centre A et séparable. Un produit d'algèbres séparables est séparable et la séparabilité se conserve par extension plate ; si $A \to A'$ est une extension fidèlement plate et si $A' \otimes_A B$ est séparable et projective de type fini, alors B est une A-algèbre séparable et projective de type fini.

On déduit du théorème précédent, le résultat suivant :

<u>Théorème</u> 2.6.7. <u>Soit</u> (P,q) <u>un</u> A-<u>module quadratique de rang pair non nul</u>. <u>Alors</u> $C(P,q)$ <u>est une</u> A-<u>algèbre d'Azumaya et, en particulier, son centre est égal à</u> A. <u>De plus</u>, $C_0(P,q)$ <u>est une</u> A-<u>algèbre séparable</u>, <u>son centre est une extension quadratique de</u> A <u>et le commutant</u> C^{C_0} <u>de</u> $C_0(P,q)$ <u>dans</u> $C(P,q)$ <u>est le centre</u> $Z(C_0)$ <u>de</u> $C_0(P,q)$.

C'est une simple traduction du théorème 2.6.6. et des remarques qui le suivent. En effet, il existe une extension fidèlement plate A' de A telle que $A' \otimes_A (P,q)$ est un espace hyperbolique de rang strictement positif. En conséquence, $A' \otimes_A C(P,q) \approx C(A' \otimes_A (P,q))$ est l'algèbre des endomorphismes d'un A-module projectif de type fini, donc une A'-algèbre d'Azumaya ; $C(P,q)$ est donc une A-algèbre d'Azumaya car A' est A-fidèlement plate. Les résultats sur $C_0(P,q)$ découlent aussi des résultats du théorème 2.6.6. sur $A' \otimes_A C_0(P,q)$.

Théorème 2.6.8. Soit (P,q) un A-module quadratique de rang impair, somme orthogonale d'un espace hyperbolique $h(P')$ et d'un A-module quadratique $(Au,q")$ libre de rang 1 avec $q"(u) = -1$: (i) l'algèbre $C_o = C_o(P,q)$ est isomorphe à l'algèbre des endomorphismes d'un A-module projectif de type fini ; (ii) l'algèbre $C = C(P,q)$ est le produit tensoriel de C_o et du centre $Z(C)$ de C qui est une extension quadratique de A.

Remarquons tout d'abord que 2 est inversible dans A car P est de rang impair et soit $(P,q) = h(P') \perp (Au,q")$. On identifie les éléments de P à leurs images dans $C(P,q)$. Si $x \in h(P')$ et φ est la forme A-bilinéaire symétrique associée à q, $\varphi(x,u) = 0$ donc $xu + ux = 0$ dans $C(P,q)$. De plus, $(xu)^2 = (xu)(xu) = -x^2u^2 = q(x)$. Considérons l'application A-linéaire $\alpha : h(P') \to C_o(P,q)$ définie par $x \mapsto xu$. Comme $(\alpha(x))^2 = q(x)$ pour tout $x \in h(P')$, α se prolonge en un homomorphisme de A-algèbre $\bar{\alpha} : C(h(P')) \to C_o$. Cet homomorphisme est surjectif car C_o est engendré sur A par les produits $(x + au)(y + bu)$, $x,y \in h(P')$, $a,b \in A$, c'est à dire $xy + bxu - ayu - ab$. Il suffit de montrer que xy est dans $\bar{\alpha}(C(h(P')))$, ce qui est évident, car $xy = (xu)(yu)$. Comme $\bar{\alpha}$ est surjectif et que $C(h(P'))$ et $C_o(P,q)$ sont des A-modules projectifs de type fini et de même rang, $\bar{\alpha}$ est un isomorphisme. Le théorème 2.6.6. nous dit alors que C_o est bien l'algèbre des endomorphismes du A-module projectif $\Lambda(P')$. On aurait pu montrer que $\bar{\alpha}$ est injectif en utilisant la propriété 2.6.2. des algèbres d'Azumaya.

Pour montrer la deuxième partie du théorème, remarquons, d'après la propriété 2.6.4. des algèbres d'Azumaya, que $C \approx C_o \otimes_A {}^{C_o}C$. Comme C_o et ${}^{C_o}C$ sont des A-modules projectifs de type fini et fidèles, il en est de même de ${}^{C_o}C$ qui, pour des questions de rang, est un A-module projectif de type fini et de rang 2 ; c'est donc une A-algèbre commutative et comme C_o a pour centre A, c'est le centre de C. Pour voir que c'est une extension quadratique de A, il suffit de montrer que c'est une A-algèbre séparable et pour cela il suffit de le montrer si A est local : P' est alors libre et on peut prendre dans $h(P')$ une base orthogonale $\{e_1,\ldots,e_{2n}\}$ avec $e_i^2 = 1$ si $i \leq n$, $e_j^2 = -1$ si $j \geq n+1$. L'élément $x = u\, e_1 \ldots e_{2n}$ commute à chaque e_i et à u donc c'est un élément du centre de $C(P,q)$. On voit aisément que $x^2 = -(e_1 \ldots e_{2n})^2$. Par récurrence sur p, on montre que $(e_1 \ldots e_p)^2 = (-1)^{\frac{p(p-1)}{2}} q(e_1) \ldots q(e_p)$, donc $x^2 = (-1)^{\frac{2n(2n-1)}{2} + n+1} = -1$.

Ainsi, $B = A \oplus A\,x$ est une extension quadratique de A qui est dans le centre de $C(P,q)$. Pour voir que c'est le centre, il suffit de remarquer que $C_o \otimes_A B$ s'identifie à C car u ainsi que chaque e_i est produit de x et d'un élément de

$C_o(P,q)$, à savoir, $x\, e_1 \ldots e_{2n} = u$ et $x(u\, e_1 \ldots \hat{e}_i \ldots e_n) = (-1)^{i-1}\, q(e_i)e_i$, $i = 1,\ldots,n$. Comme $d^o x = +1$, B est une extension quadratique graduée, non triviale sur $\mathbb{Z}/(2)$. Notons qu'on peut montrer que, quel que soit le module quadratique (M,q), $C_o((M,q) \perp (Ae,q')) \approx C(M,q)$ si $q'(e) = -1$, ce qu'on a démontré dans le cas particulier où (M,q) est hyperbolique.

On peut alors énoncer le théorème suivant :

Théorème 2.6.9. Soit (P,q) un A-module quadratique de rang impair. Alors : (i) $C_o(P,q)$ est une A-algèbre d'Azumaya ; (ii) $C(P,q)$ est isomorphe à $C_o(P,q) \otimes_A Z$, où Z est son centre ; Z est une extension quadratique de A. C'est aussi le commutant de $C_o(P,q)$ dans $C(P,q)$. Le centre Z est gradué sur $\mathbb{Z}/(2)$ où $Z_o = A$ et Z_1 est un A-module projectif de type fini et de rang 1.

Dans les théorèmes précédents, on a supposé que les modules étaient projectifs de type fini et de rang constant. Dans le cas général, on considère la fonction $e : \mathrm{Spec}(A) \to \mathbb{Z}/(2)$ qui à un point $\mathfrak{p}$ associe le rang du A-module P modulo 2. Alors $\{\mathfrak{p} \mid e(\mathfrak{p}) = 1\}$ définit un idempotent e de A, d'où une décomposition en produit d'anneaux $A = Ae \times A(1-e)$ et une décomposition en somme directe de modules $P = Pe \oplus P(1-e)$ où Pe est un Ae-module projectif de rang impair et $P(1-e)$ un $A(1-e)$-module projectif de rang pair. On a alors $C_A(P,q) = C_{Ae}(Pe, qe) \times C_{A(1-e)}(P(1-e), q(1-e))$ et les théorèmes des paragraphes précédents s'appliquent aux modules quadratiques (Pe, qe) et $(P(1-e),q(1-e))$.

Soit (P,q) un A-module quadratique de rang pair non nul et $C = C(P,q)$. On pose $X(C) = \{x \mid x \in C,\ x\, z + z\, x = 0,\ \forall\, z \in C_1\}$. En fait, cela signifie que x est dans $X(C)$ si x commute à C_o et anticommute à C_1. On a donc, si σ est l'automorphisme principal de C, $\sigma = \mathrm{id}_{C_o} \oplus -\mathrm{id}_{C_1}$, $X(C) = \{x \mid x \in C,\ yx = x\,\sigma(y),\ \forall\, y \in C\}$, ce qui montre que $X(C)$ est un A-module projectif de type fini et de rang 1 (cf. 2.6.5.). On voit, en général, que $X(C)$ est contenu dans le commutant C^{C_o} de C_o dans C, c'est à dire, $Z(C_o)$. Dans le cas hyperbolique, $X(C)$ est formé de matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ et la condition d'anticommutation avec C_1 donne $\lambda + \mu = 0$. Il en résulte que $X(C)$ est exactement égal à $X(Z(C_o))$ (cf. 2.4.).

Soit maintenant (P',q') un second A-module quadratique de rang pair non nul et considérons l'algèbre de Clifford de la somme orthogonale $(P,q) \perp (P',q')$. D'après 2.2., c'est le produit tensoriel gradué de $C = C(P,q)$ et de $C' = C(P',q')$. Comme C est une A-algèbre d'Azumaya et qu'elle s'identifie à une sous-algèbre de $C \hat{\otimes} C'$, d'après 2.6.4., on a $C \hat{\otimes} C' \simeq C \otimes C'_*$ où C'_* est le commutant de C dans

$C \hat{\otimes} C'$. On a, de même, $C \hat{\otimes} C' \simeq C_* \otimes C'$ et C_* et C'_* ne dépendent que de C et de C'.

Soit, dans $C \hat{\otimes} C'$, le sous-module $X(C) \otimes P'$ engendré par les éléments de la forme $x \otimes y'$, $x \in X(C)$, $y' \in P'$. On a $(x \otimes y')^2 = x^2 \otimes y'^2$ car x est de degré 0, soit $x \otimes y' = \mu(x)\, q'(y')$. Sur $X(C) \otimes P'$, on a ainsi une forme quadratique non dégénérée, d'où on déduit un homomorphisme de $C(X(C) \otimes P', \mu\, q')$ dans $C \hat{\otimes} C'$. Notons que les éléments de $X(C) \otimes P'$ commutent à C : si $y \in P$, $(x \otimes y')(y \otimes 1) = - x\, y \otimes y'$ car $d^0 y = d^0 y' = 1$ et $(y \otimes 1)(x \otimes y') = y\, x \otimes y'$ et ces deux éléments de $C \hat{\otimes} C'$ sont égaux, car $xy + y\, x = 0$. En conséquence, les images de $C(X(C) \otimes P', \mu\, q')$ et de C dans $C \hat{\otimes} C'$ commutent. Comme ce sont deux algèbres d'Azumaya, ainsi que $C \hat{\otimes} C'$, $C \hat{\otimes} C' \simeq C \otimes C(X(C) \otimes P', \mu\, q') \otimes D$ où D est une A-algèbre projective et de rang 1, donc isomorphe à A. On a donc $C \hat{\otimes} C' \simeq$ $\simeq C \otimes C(X(C) \otimes P', \mu\, q')$.

Mutatis mutandis, $C \hat{\otimes} C' \simeq C(X(C') \otimes P, \mu'\, q) \otimes C'$ et de plus, chacun de ces isomorphismes est un isomorphisme d'algèbres graduées sur $\mathbb{Z}/(2)$. On peut alors énoncer le résultat suivant :

Théorème 2.6.10. *Soient C et C' deux algèbres de Clifford de modules quadratiques de rang pair non nuls. Il existe une algèbre de Clifford C'_* telle que $C \hat{\otimes} C'$ est isomorphe à $C \otimes C'_*$, isomorphisme d'algèbres graduées sur $\mathbb{Z}/(2)$.*

Soient $C = C(P,q)$ et $C' = C(P',q')$ deux algèbres de Clifford de modules quadratiques de rang quelconque > 0. On s'intéresse au commutant de la partie homogène de degré 0, $(C \hat{\otimes} C')_0$, somme directe de $C_0 \otimes C'_0$ et de $C_1 \otimes C'_1$. Ce commutant est donc contenu dans celui de $C_0 \otimes C'_0$ qui n'est autre que $C^{C_0} \hat{\otimes} C'^{C'_0}$. Il y a alors trois cas distincts à considérer : P et P' sont tous deux de rang pair, tous deux de rang impair, l'un de rang pair, l'autre de rang impair. Dans les trois, nous allons voir que le commutant de $(C \hat{\otimes} C')_0$ est le produit $C^{C_0} * C'^{C'_0}$ dans le groupe $\mathfrak{Q}_2(A)$ est extensions quadratiques graduées.

(i) P *et* P' *sont de rang pair*. On sait que C^{C_0} et $C'^{C'_0}$ sont les centres respectifs de C_0 et C'_0 et commutent dans $C \hat{\otimes} C'$. Le commutant de $(C \hat{\otimes} C')_0$ est donc une sous-extension quadratique (trivialement graduée) de $Z(C_0) \otimes Z(C'_0)$, distincte de $Z(C_0)$ et de $Z(C'_0)$ car si $Z(C_0)$ commute à C'_1, elle ne commute pas à C_1 donc pas à $C_1 \otimes C'_1$. Il s'ensuit que $(C \hat{\otimes} C')_0$ a pour commutant l'extension quadratique composée de $Z(C_0)$ et de $Z(C'_0)$.

(ii) P *et* P' *sont de rang impair*. Si P est de rang impair, soit $X(C) = \{x \mid x \in C_1,\ xy = yx,\ \forall\, y \in C\} = C_1 \cap Z(C) = Z(C)_1$. On a ici $C^{C_0} = Z(C) =$

$= A \oplus Z(C)_1$ et, de même, $C'^{C'}{}_o = Z(C') = A \oplus Z(C')_1$. Comme $Z(C)$ et $Z(C')$ sont graduées non trivialement, la partie homogène de degré 0 de $Z(C) \hat{\otimes} Z(C')$ n'est autre que $Z(C) * Z(C')$. Or, $(P,q) \perp (P',q')$ est de rang pair, donc le commutant de $(C \hat{\otimes} C')_o$ est une sous-algèbre de $Z(C) \hat{\otimes} Z(C')$ concentrée en degré 0 et cela ne peut donc être que $Z(C) * Z(C')$.

(iii) P de rang pair et P' de rang impair. Remarquons que 2 est inversible dans A et qu'on a les décompositions $C^{C}{}_o = Z(C_o) = A \oplus X(C)$ et $C'^{C'}{}_o \approx Z(C') = A \oplus X(C')$ où $X(C)$ est formé d'éléments de degré 0 et $X(C')$ d'éléments de degré 1. Le produit tensoriel gradué $C^{C}{}_o \hat{\otimes} C'^{C'}{}_o$ est, en tant qu'algèbre, le produit ordinaire. Il est clair que $X(C) \otimes X(C')$ commute non seulement à $C_o \otimes C'_o$ mais aussi à $C_1 \otimes C'_1$. En effet, $(x \otimes x')(y \otimes y') = - x y \otimes x'y'$ et $(y \otimes y')(x \otimes x') = y x \otimes y' x'$, car $d^o x' = d^o y' = 1$ et $xy + yx = 0$, $x'y' = y'x'$. Le commutant de $X(C) \otimes X(C')$ ne peut donc être que $A \oplus (X(C) \otimes X(C'))$, où le second terme est homogène de degré 1. On a encore ici $(C \hat{\otimes} C')^{(C \hat{\otimes} C')}{}_o = C^{C}{}_o * C'^{C'}{}_o$.

On a déjà vu que si P est un module projectif de rang strictement positif, $C(h(P))^{C_o(h(P))}$ est l'extension quadratique triviale de A. Soit maintenant (P,q) un A-module quadratique, où P n'est pas nécessairement fidèle ; on veut lui associer une extension quadratique graduée de A. Quand P est fidèle, il suffit de prendre l'extension $C(P,q)^{C_o(P,q)}$. Dans le cas général, ajoutons à (P,q) un espace hyperbolique $h(M)$ où M est de rang strictement positif. Alors on sait associer à $(P,q) \perp h(M)$ une extension quadratique graduée : le commutant $C^{C}{}_o$ où $C = C((P,q) \perp h(M))$. Il s'agit de voir que cela ne dépend pas de l'espace hyperbolique $h(M)$ et soit $C' = C((P,q) \perp h(M'))$ où M' est un second module projectif de type fini et de rang strictement positif. Considérons alors $D = C((P,q) \perp h(M) \perp h(M'))$: $D \approx C \hat{\otimes} C(h(M')) \approx C' \hat{\otimes} C(h(M))$. Comme les extensions quadratiques associées à $h(M)$ et à $h(M')$ sont l'extension triviale et comme l'extension associée à un produit tensoriel gradué est l'extension produit dans le groupe $\mathfrak{D}_2(A)$ d'après la discussion qui suit 2.6.10., on a les isomorphismes $D^{D}{}_o \approx C^{C}{}_o$ et $D^{D}{}_o \approx C'^{C'}{}_o$. Cela montre que $C^{C}{}_o$ ne dépend pas du choix du module projectif de type fini M mais du module quadratique (P,q) et en fait seulement de sa classe dans le groupe de Witt de A. Cet invariant que nous appellerons discriminant gradué de (P,q) définit une application de $W(A)$ dans le groupe $\mathfrak{D}_2(A)$ des extensions quadratiques graduées de A. Nous pouvons alors énoncer le théorème suivant :

Théorème 2.6.11. L'application qui à un A-module quadratique (P,q) associe la classe d'isomorphisme dans le groupe $\mathfrak{D}_2(A)$ de l'extension quadratique graduée C^{C_o} induit un homomorphisme (discriminant gradué) de groupes abéliens $d : W(A) \to \mathfrak{D}_2(A)$ dont la restriction à $W_o(A)$ est un homomorphisme (discriminant ordinaire) $d_o : W_o(A) \to \mathfrak{D}(A)$. De plus, d et d_o sont des homomorphismes surjectifs.

En effet, d_o est surjectif d'après 2.4.16, donc d l'est aussi car le diagramme

$$\begin{array}{ccccccc} 0 & \to & W_o(A) & \to & W(A) & \xrightarrow{r_2} & Ip(A) \\ & & \downarrow{\scriptstyle d_o} & & \downarrow{\scriptstyle d} & & \\ 0 & \to & \mathfrak{D}(A) & \to & \mathfrak{D}_2(A) & \xrightarrow{e} & Ip(A) \end{array}$$

est commutatif, où r_2 désigne l'application rang modulo 2. Il est clair que les images de $W(A)$ et de $\mathfrak{D}_2(A)$ dans $Ip(A)$ sont égales car c'est le groupe des idempotents e tels que $2e$ est inversible dans Ae. Comme d_o est surjectif, d l'est aussi.

Comme on l'a vu en 2.5.4., si $(P,\alpha) \in \mathcal{P}(A)$, pour tout module quadratique (M,q), $C_o(P \otimes M, \alpha q) \approx C_o(M,q)$. En conséquence, si (M,q) est un module de rang pair, $d_o(M,q) = d_o(P \otimes M, \alpha q)$ quel que soit (P,α) dans $\mathcal{P}(A)$. Supposons maintenant que A est un corps de caractéristique différente de 2 : le discriminant gradué est alors un couple formé d'un élément de $U(A)/U^2(A)$ et d'un entier modulo 2. Ainsi on a $d(\langle a_1\rangle \perp \ldots \perp \langle a_n\rangle) = ((-1)^{\frac{n(n-1)}{2}} a_1 \ldots a_n, n \bmod 2)$ car $C^{C_o} = A\,1_C \oplus A(e_1 \ldots e_n)$ où $e_1, \ldots, e_n$ est une base orthogonale du module quadratique.

Dans ces conditions, soient φ et ψ deux formes quadratiques non dégénérées de rang pair. Comme 2 est inversible dans A, $\mathfrak{D}(A)$ et $\mathcal{P}(A)$ sont isomorphes et le théorème 2.6.10. s'exprime de la façon suivante : $C(\varphi \perp \psi) \approx C(\varphi) \otimes C(d(\varphi)\psi) \approx C(d(\psi)\varphi) \otimes C(\psi)$.

En caractéristique 2, d se réduit à d_o. Comme $\mathfrak{D}(A) \approx A/\wp A$, $d((P,q))$ est un scalaire déterminé à un élément de la forme $a + a^2$, $a \in A$, près. L'invariant d est alors appelé invariant d'Arf (cf. 2.4.10).

2.7. ALGEBRES DE QUATERNIONS

On appelle algèbre de quaternions, l'algèbre de Clifford d'un module de rang 2. D'après les théorèmes de structure des algèbres de Clifford, une algèbre de quaternions C est une algèbre d'Azumaya de rang 4 en tant que A-module.

Si (P,q) est le A-module quadratique correspondant à C, la sous-algèbre $C_o(P,q)$ de C est une algèbre commutative de rang 2, extension quadratique de A et $C_1(P,q)$ s'identifie à P en tant que A-module.

Considérons l'antiautomorphisme principal τ de C : c'est l'identité sur $C_1 = P$ et un automorphisme sur C_o. Comme τ n'est pas l'identité car C n'est pas commutative, la restriction de τ à C_o ne peut être que σ l'unique automorphisme linéairement indépendant de l'identité de C_o. Soit alors σ_C l'automorphisme principal $id_{C_o} \oplus - id_{C_1}$ et notons $z \mapsto \bar{z}$ l'antiautomorphisme involutif $\sigma_C \circ \tau \ (= \tau \circ \sigma_C)$ qui est la somme directe $\sigma \oplus - id_{C_1}$. Si 2 est inversible dans A, $C_o(P,q) = A\,1_{C_o} \oplus X(C)$ et $\sigma = id_A \oplus - id_{X(C)}$. L'algèbre $C(P,q)$ est somme directe de $X(C) \oplus C_1$ et de $A\,1_C$ et l'antiautomorphisme $z \mapsto \bar{z}$ s'écrit $id_{A\,1_C} \oplus - id_{X(C) \oplus C_1}$. Les éléments de $X(C) \oplus C_1$ sont appelés <u>quaternions purs</u>.

Dans le cas général, si $z \in C(P,q)$, le produit $z\bar{z}$ est dans A. En effet, $z\bar{z} = (z_o + z_1)(\sigma(z_o) - z_1) = z_o\sigma(z_o) - z_1^2 + z_1\,\sigma(z_o) - z_o z_1 = N_{C_o}(z_o) - q(z_1)$ car $z_o z_1 = z_1\sigma(z_o)$ comme le montre le calcul local suivant : on prend P libre de base $\{e_1, e_2\}$ de sorte que $e_1^2 = a$, $e_2^2 = b$ et $e_1 e_2 + e_2 e_1 = 1$. On a $C_o = A\,1 \oplus A\,e_1 e_2$ et $\sigma(\alpha + \beta\, e_1 e_2) = \alpha + \beta(1 - e_1 e_2)$ et il suffit de vérifier la relation $z_o z_1 = z_1\,\sigma(z_o)$ pour $z_o = e_1 e_2$ et $z_1 = e_1$ ou bien $z_1 = e_2$. On a $(e_1 e_2)e_1 = e_1(e_2 e_1) = e_1\,\sigma(e_1 e_2)$ et $(e_1 e_2)e_2 = e_1 e_2^2 = e_2^2 e_1 = e_2(e_2 e_1) = e_2\,\sigma(e_1 e_2)$. Le produit $z\bar{z}$ est appelé <u>norme réduite</u> de z et noté $Nrd(z)$. Comme $z \mapsto \bar{z}$ est un antiautomorphisme et que $Nrd(z) \in A\,1$ est dans le centre de C, on a $Nrd(zz') = (zz')(\overline{zz'}) = z(\overline{z'z'})\bar{z} = Nrd(z)\,Nrd(z')$. La norme réduite est une forme quadratique $Nrd : C \to A$ non dégénérée car le A-module quadratique (C, Nrd) est la somme orthogonale des deux A-modules quadratiques $(C_o, N_{C_o/A})$ et $(P, -q)$. C'est une forme quadratique de discriminant 1 car C_o et C_1 $(=P)$ sont de rang pair et ont même discriminant gradué ; $(P,-q)$ est de rang 2 et donc son discriminant gradué est $C_o(P,-q) \approx C_o(P,q)$. De même, le discriminant de $(C_o, N_{C_o/A})$ est C_o (cf. 2.4.16.).

<u>Lemme</u> 2.7.1. <u>La forme quadratique</u> Nrd <u>de l'algèbre de quaternions</u> $C(h(P))$ <u>où</u> P <u>est un</u> A<u>-module projectif de type fini et de rang</u> 1, <u>coïncide avec la forme quadratique</u> dét : $C(h(P)) \to A$ <u>obtenue en identifiant</u> $C(h(P))$ <u>avec l'algèbre des endomorphismes de</u> $\Lambda(P)$.

La démonstration se fait aisément à l'aide du cas local. Soit $\{e_1, e_2\}$ la base naturelle de $h(P)$ d'où une base $\{1, e_1, e_2, e_1\ e_2\}$ de $C(h(P))$. Dans l'isomorphisme $C(h(P)) \to \mathrm{End}\ (\Lambda(P))$, e_1 donne la matrice $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et e_2 la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. L'image de l'élément $\alpha 1 + \beta e_1 + \gamma e_2 + \delta e_1\ e_2$ est donc la matrice $\begin{pmatrix} \alpha & \gamma \\ \beta & \alpha + \delta \end{pmatrix}$ de déterminant $\alpha(\alpha + \delta) - \beta\gamma$. Or, $\mathrm{Nrd}(\alpha 1 + \beta e_1 + \gamma e_2 + \delta e_1\ e_2) = N_{C_o/A}(\alpha 1 + \delta e_1\ e_2) - q(\beta e_1 + \gamma e_2) = \alpha(\alpha + \delta) - \beta\gamma$, d'où le lemme.

Soit maintenant C une algèbre de quaternions et supposons que $C = C(P,q) = C(P',q')$. On a donc deux normes réduites définies sur C associées respectivement à (P,q) et à (P',q'). Alors on a le lemme suivant :

Lemme 2.7.2. La norme réduite d'une algèbre de quaternions C ne dépend pas du module quadratique, mais seulement de la classe d'isomorphisme de l'algèbre C.

Cela revient à dire que les normes réduites $\mathrm{Nrd}_P : C = C(P,q) \to A$ et $\mathrm{Nrd}_{P'} : C = C(P',q') \to A$ coïncident. Or, remarquons tout d'abord que si $A \to B$ est un homomorphisme d'anneaux commutatifs, $\mathrm{Nrd} : C(B \otimes_A P, q_B) \to B$ est l'extension à B de la forme quadratique Nrd sur $C(P,q)$. De plus, il existe une extension fidèlement plate A' de A telle que $A' \otimes_A (P,q) \approx h(A')$ et $A' \otimes_A (P',q') \approx h(A')$. Ceci nous donne, par extension des scalaires, deux isomorphismes $u : A' \otimes_A C \to M_2(A')$ et $u' : A' \otimes_A C \to M_2(A')$ qui transportent chacun la norme réduite correspondante sur le déterminant $\det : M_2(A') \to A'$. De plus, $\varphi = u' \circ u^{-1}$ est un automorphisme de $M_2(A')$ et puisque A' est une extension fidèlement plate de A, φ est un automorphisme intérieur. Ainsi comme $\varphi \circ u = u'$, on a $\det(u(1 \otimes z)) = \det(\varphi \circ u(1 \otimes z)) = \det(u'(1 \otimes z))$, pour tout z dans C. Comme $\det(u(1 \otimes z))$ est exactement $1 \otimes \mathrm{Nrd}_P(z)$, on a bien $\mathrm{Nrd}_P(z) = \mathrm{Nrd}_{P'}(z)$, pour tout $z \in C$.

Ce lemme a la conséquence importante suivante :

Proposition 2.7.3. Soient (P,q) et (P',q') deux A-modules quadratiques de rang 2 tels que $C(P,q) \approx C(P',q')$ et $C_o(P,q) \approx C_o(P',q')$. Alors (P,q) et (P',q') ont même classe dans le groupe de Witt-Grothendieck de l'anneau A.

En effet, d'après le lemme 2.7.2., $C(P,q)$ et $C(P',q')$ ont la même norme réduite, ce qui donne l'isomorphisme de A-modules quadratiques $(P,-q) \perp (C_o(P,q), N_{C_o/A}) \approx (P',-q') \perp (C_o(P',q'), N_{C_o/A})$. Comme $C_o(P,q)$ et $C_o(P',q')$

sont des extensions quadratiques isomorphes, elles ont même norme. On a donc l'égalité $[(P,-q)] = [(P',-q')]$, dans $WG(A)$, d'où l'assertion annoncée.

Notons que la réciproque n'est pas vraie : si $[(P,q)] = [(P',q')]$ dans $WG(A)$, alors les extensions quadratiques $C_o(P,q)$ et $C_o(P',q')$ sont égales dans le groupe $\mathfrak{D}(A)$, donc ces algèbres sont isomorphes. Pour $C(P,q)$ et $C(P',q')$, il existe un A-module quadratique (P'',q''), que l'on peut supposer hyperbolique, tel que $(P,q) \perp (P'',q'') \approx (P',q') \perp (P'',q'')$ et on a donc un isomorphisme d'algèbres graduées sur $\mathbb{Z}/(2)$, $C(P,q) \hat{\otimes} C(P'',q'') \simeq C(P',q') \hat{\otimes} C(P'',q'')$ où le $\hat{\otimes}$ peut être remplacer par le produit tensoriel ordinaire car (P'',q'') est hyperbolique. Nous ne pouvons pas en conclure l'isomorphisme entre $C(P,q)$ et $C(P',q')$ car il n'y a pas, en général, de théorème de simplification pour les algèbres d'Azumaya. Cependant, si A est un anneau local (ou même semi-local), il y a simplification, d'après le théorème de Skolem-Noether, et la réciproque de la proposition précédente est vraie. Supposons que la caractéristique résiduelle de A diffère de 2 ; si $q : A^2 \to A$ est la forme quadratique définie par $(x,y) \mapsto a\,x^2 + b\,y^2$, q est non dégénérée de rang 2 et on notera $(\frac{a,b}{A})$ la classe, dans le groupe de Brauer de A, de l'algèbre de quaternions $C = C(A^2,q)$. Comme on l'a vu au début de 2.7., C est somme orthogonale de $A\,1_C$ et de C_+, sous-module formé des quaternions purs, car 2 est inversible dans A. Si $z \in C_+$, $z^2 = -\,z\,\bar{z} = -\,\mathrm{Nrd}(z)$. Comme A est local, on voit immédiatement que si $C \approx (\frac{a,b}{A})$, $(C_+, \mathrm{Nrd}_{C_+}) \approx \langle -a\rangle \perp \langle -b\rangle \perp \langle ab\rangle$. Soit alors P' le sous-module libre de rang 2 engendré par les deux derniers vecteurs et q' la restriction de la forme quadratique $-\,\mathrm{Nrd}$ à P' de sorte que $(P',q') \approx \langle b\rangle \perp \langle -ab\rangle$. L'injection naturelle i de P' dans C vérifie par construction $(i(z))^2 = q'(z)$ et cela induit un homomorphisme de $C(P',q')$ dans C qui est un isomorphisme de A-algèbres. Cela signifie que dans le groupe de Brauer de A, $(\frac{a,b}{A}) = (\frac{b,-ab}{A}) = (\frac{a,-ab}{A})$. On a un résultat analogue si A est un anneau quelconque dans lequel 2 est inversible. Soit (X,μ) et (X',μ') deux éléments de $P(A)$ et notons (P,q) le module quadratique suivant : $P = X \oplus X'$ et $q((x,x')) = \mu(x \otimes x) + \mu'(x' \otimes x')$. L'algèbre $C = C(P,q)$ est somme de $A\,1_C$ et de C_+ où $C_+ \approx (X, -\bar{\mu}) \perp (X', -\bar{\mu}') \perp (X \otimes X', \overline{\mu \otimes \mu'})$, où $\bar{\mu}$ désigne la restriction de μ à la diagonale. On vérifie alors, comme plus haut, que $C((X,\bar{\mu}) \perp (X',\bar{\mu}')) \approx C((X,\bar{\mu}) \perp \perp (X \otimes X', -\mu \otimes \mu'))$.

D'après les remarques précédentes, on voit que $\langle a\rangle \perp \langle b\rangle \approx \langle c\rangle \perp \langle d\rangle$ si et seulement si $ab \equiv cd$ (modulo $U^2(A)$) et $(\frac{a,b}{A}) = (\frac{c,d}{A})$. Ceci nous permet d'énoncer le théorème suivant :

Théorème 2.7.4. *L'anneau de Witt-Grothendieck d'un anneau local A dans lequel 2 est inversible est le quotient de l'anneau de groupes $\mathbb{Z}[U(A)/U^2(A)]$ par l'idéal*

engendré par les éléments $\bar{a} + \bar{b} - \bar{c} - \bar{d}$, où $a, b, c, d \in U(A)$, $\bar{a}\,\bar{b} = \bar{c}\,\bar{d}$ dans $U(A)/U^2(A)$ et $(\frac{a,b}{A}) = (\frac{c,d}{A})$ dans le groupe de Brauer de A.

Dans le même ordre d'idées, on a la proposition suivante :

Proposition 2.7.5. Soit A un corps. (i) Si (P,q) est un A-module quadratique de rang 4, tel que $C(P,q) = 0$ dans $Br(A)$ et $Z(C_0(P,q)) = 0$ dans $\mathfrak{D}(A)$, alors (P,q) est hyperbolique. (ii) Soient (P,q) et (P',q') deux A-modules quadratiques de rang 3 tels que $C_0(P,q) \approx C_0(P',q')$ et $C(P,q) \approx C(P',q')$. Alors (P,q) et (P',q') sont isomorphes.

Dans le premier cas, soit $(P,q) = (P_1,q_1) \perp (P_2,q_2)$ une décomposition orthogonale en somme de A-modules quadratiques de rang 2. En caractéristique 2, $C(P,q) = M_4(A) = C(P_1,q_1) \otimes C(P_2,q_2)$, l'anneau des matrices carrées d'ordre 4. Comme $C(P_1,q_1) \approx C(P_1,q_1)^0$ et que $C(P_1,q_1) \otimes C(P_1,q_1)^0 = \mathrm{End}_A(C(P_1,q_1)) = M_4(A)$, on a $C(P_1,q_1) \approx C(P_2,q_2)$. De plus, indépendamment de la caractéristique, $0 = Z(C_0(P,q)) = C_0(P_1,q_1) * C_0(P_2,q_2)$ dans le groupe $\mathfrak{D}(A)$ des extensions quadratiques, donc $C_0(P_1,q_1) = C_0(P_2,q_2)$ et la proposition précédente permet d'affirmer, en caractéristique 2, que (P_1,q_1) et (P_2,q_2) sont isomorphes, donc que (P,q) est hyperbolique.

En caractéristique différente de 2, il faut montrer que (P_1,q_1) et $(P_2,-q_2)$ sont isomorphes. Or, $M_4(A) = C(P,q) = C(P_1,q_1) \hat{\otimes} C(P_2,q_2) = C(P_1,q_1) \otimes C(P_2, d(q_1)\,q_2)$. Comme $C_0(P_1,q_1) = C_0(P_2,q_2)$ et $C_0(P_2,q_2) = C_0(P_2, a\,q_2)$ pour tout $a \in U(A)$, on a $C(P_1,q_1) \approx C(P_2, d(q_1)\,q_2)$ et $C_0(P_1,q_1) \simeq C_0(P_2, d(q_1)\,q_2)$, donc $(P_1,q_1) \approx (P_2, d(q_1)\,q_2)$. Si $(P_1,q_1) = \langle a\rangle \perp \langle b\rangle$, $d(q_1) = -\,a\,b$ modulo $U^2(A)$ alors $(P_2,q_2) = (P_1, d(q_1)\,q_1) = -\,a\,b\,(\langle a\rangle \perp \langle b\rangle) = \langle -a\rangle \perp \langle -b\rangle = (P_1, -q_1)$ ce qui achève la démonstration de (i).

En ce qui concerne l'assertion (ii), A est de caractéristique différente de 2 car P et P' sont de rang impair. On a, de plus, $C(P,q) = C_0(P,q) \otimes Z(C(P,q))$ où $C_0(P,q)$ est une A-algèbre centrale séparable de rang 4 et $Z(C(P,q))$ est somme directe de A 1 et de $X(C)$. On a un isomorphisme donné par la multiplication $C_1(P,q) \approx C_0(P,q) \otimes X(C)$ ainsi que $C_0(P,q) \approx C_1(P,q) \otimes X(C)$. Ainsi on a les deux décompositions $C_0(P,q) = A\,1 \oplus P \otimes X(C)$ et $C_1(P,q) = X(C) \oplus P$ et les décompositions correspondantes pour (P',q'). Comme $Z(C(P,q)) \approx Z(C(P',q'))$, $X(C)$ et $X(C')$ sont isomorphes. Soit $\langle a_1\rangle \perp \langle a_2\rangle \perp \langle a_3\rangle$ une décomposition orthogonale de (P,q) et e_1, e_2, e_3 les éléments correspondants de P. Alors $P \otimes X(C)$ est l'espace vectoriel de base $\{e_2\,e_3,\ e_3\,e_1,\ e_1\,e_2\}$. On voit que $C_0(P,q)$ est une algèbre de quaternions, c'est l'algèbre de Clifford de l'espace quadratique $\langle -a_1\,a_2\rangle \perp \langle -a_1\,a_3\rangle$. La norme réduite de cette algèbre est la forme quadratique $\langle 1\rangle \perp \langle a_1\,a_2\rangle \perp \langle a_2\,a_3\rangle \perp \langle a_3\,a_1\rangle$. Si $\{f_1, f_2, f_3\}$ est une base orthogonale de

(P',q') et $q'(f_i) = a'_i$ $(i = 1,2,3)$, le théorème de simplification de Witt appliqué aux algèbres C_o nous dit qu'il existe un isomorphisme de A-modules quadratiques $\langle a_1\ a_2\rangle \perp \langle a_2\ a_3\rangle \perp \langle a_3\ a_1\rangle \approx \langle a'_1\ a'_2\rangle \perp \langle a'_2\ a'_3\rangle \perp \langle a'_3\ a'_1\rangle$. L'isomorphismes $Z(C(P,q) \approx Z(C(P',q'))$ entraîne que $a_1\ a_2\ a_3 \equiv a'_1\ a'_2\ a'_3 \pmod{U^2(A)}$ et en multipliant les deux membres de l'isomorphisme ci-dessus par $a_1\ a_2\ a_3$, on obtient un isomorphisme de (P,q) sur (P',q').

2.8. LE GROUPE DES CLASSES D'ALGEBRES DE CLIFFORD

Une A-algèbre associative S, graduée sur $\mathbb{Z}/(2)$ sera dite <u>triviale</u> s'il existe deux A-modules projectifs de type fini P_1 et P_2 tels que S soit isomorphe, en tant qu'algèbre graduée, à l'élgèbre $\mathrm{End}_A(P_1 \oplus P_2)$ et si, de plus, $P_1 \oplus P_2$ est fidèle.

<u>Lemme</u> 2.8.1. <u>Soit</u> S <u>une</u> A-<u>algèbre triviale et</u> R <u>une</u> A-<u>algèbre graduée sur</u> $\mathbb{Z}/(2)$. <u>Alors</u>, $S \hat{\otimes} R$ <u>et</u> $S \otimes R$ <u>sont isomorphes en tant qu'algèbres graduées</u>.

On se ramène aisément au cas où P_1 et P_2 sont de rang constant. Si P_1 ou P_2 est réduit à 0, le résultat est clair car $S_1 = 0$, c'est à dire que S est trivialement graduée. On les supposera donc tous deux non nuls. Dans ce cas, S_o s'identifie à $\mathrm{End}(P_1) \times \mathrm{End}(P_2)$ et son centre à $A \times A$, c'est à dire à l'anneau des matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec λ et μ dans A. On note $X(S) = \{\begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix} \mid \lambda \in A\}$, qui est un A-module libre de rang 1, de générateur $\varepsilon = \mathrm{id}_{P_1} \oplus -\mathrm{id}_{P_2}$ et on a $\varepsilon\, s_i = (-1)^i\, s_i \varepsilon$ si $s_i \in S_i$ $(i = 0,1)$. Notons alors R' la sous-algèbre graduée de $S \hat{\otimes} R$ somme directe de $R'_o = 1 \otimes R_o$ et de $R'_1 = X(S) \otimes R_1$, dont les éléments sont de la forme $1 \otimes r_o + \varepsilon \otimes r_1$, $r_i \in R_i$ $(i = 0,1)$. Elle est isomorphe à R par $r_o + r_1 \mapsto 1 \otimes r_o + \varepsilon \otimes r_1$ car $\varepsilon^2 = 1_S$ et $\varepsilon \otimes 1$ commute à $1 \otimes r_o$. De plus, $S \otimes 1$ et R' commutent dans $S \hat{\otimes} R$. En effet, c'est bien clair pour les éléments de S_o et de R' et pour S_1 et R'_o. Il reste à montrer que $(s_1 \otimes 1)(\varepsilon \otimes r_1) = (\varepsilon \otimes r_1)(s_1 \otimes 1)$. Or, le premier membre est $s_1\, \varepsilon \otimes r_1$ et le second $-\varepsilon\, s_1 \otimes r_1$ car $d^o r_1 = d^o s_1 = 1$. Comme $s_1\, \varepsilon = -\varepsilon\, s_1$ pour tout $s_1 \in S_1$, on a bien l'égalité voulue. De plus, $S \hat{\otimes} R$ est bien engendré par les images de $S \otimes 1$ et de R', ce qui montre l'isomorphisme cherché.

<u>Lemme</u> 2.8.2. <u>Le produit tensoriel gradué de deux algèbres triviales est une algèbre triviale</u>.

C'est bien clair vu le lemme 2.8.1. et l'isomorphisme $\mathrm{End}_A(P) \otimes_A \otimes_A \mathrm{End}_A(P') \approx \mathrm{End}_A(P \otimes_A P')$, où P et P' sont des A-modules projectifs de type fini.

Soient (P,q) et (P',q') deux A-modules quadratiques. On dira que les algèbres $C = C(P,q)$ et $C' = C(P',q')$ sont <u>équivalentes</u> s'il existe deux algèbres triviales S et S' telles que $C \hat{\otimes} S \approx C' \hat{\otimes} S'$, isomorphisme d'algèbres graduées sur $\mathbb{Z}/(2)$.

<u>Théorème</u> 2.8.3. <u>Le produit tensoriel gradué induit sur l'ensemble des classes d'équivalence d'algèbres de Clifford de</u> A-<u>modules quadratiques une loi de composition interne qui en fait un groupe abélien. L'élément neutre est la classe des algèbres de Clifford triviales et l'opposé de la classe de</u> $C(P,q)$ <u>est la classe de</u> $C(P,-q)$.

Pour voir qu'on a bien une loi de composition interne, il faut montrer que si C_1 et C_1' sont équivalentes de même que C_2 et C_2', alors $C_1 \hat{\otimes} C_2$ est équivalente à $C_1' \hat{\otimes} C_2'$. Or, l'hypothèse signifie qu'il existe des algèbres triviales S_1, S_1', S_2 et S_2' telles que $C_1 \hat{\otimes} S_1 \simeq C_1' \hat{\otimes} S_1'$ et $C_2 \hat{\otimes} S_2 \simeq C_2' \hat{\otimes} S_2'$ et donc par associativité et commutativité du produit tensoriel gradué $(C_1 \hat{\otimes} C_2) \hat{\otimes} (S_1 \hat{\otimes} S_2) \approx (C_1' \hat{\otimes} C_2') \hat{\otimes} (S_1' \hat{\otimes} S_2')$. Comme $S_1 \hat{\otimes} S_2$ et $S_1' \hat{\otimes} S_2'$ sont triviales, d'après le lemme 2.8.2., on a bien l'équivalence voulue.

L'associativité et la commutativité de la loi de composition interne ainsi définie proviennent des propriétés analogues du produit tensoriel gradué. La classe des algèbres de Clifford triviales (équivalentes à une algèbre triviale) -non vide car elle contient les algèbres de Clifford des espaces hyperboliques - est bien élément neutre. En effet, si C est équivalente à une algèbre triviale, $C \hat{\otimes} S \approx S'$ avec S et S' triviale et si D est une algèbre de Clifford, $D \hat{\otimes} S' \simeq (D \hat{\otimes} C) \hat{\otimes} S$, c'est à dire que la classe de D égale la classe de $D \hat{\otimes} C$.

Soient maintenant $C = C(P,q)$ et $C' = C(P,-q)$; $C \hat{\otimes} C = C(P,q) \hat{\otimes} C(P,-q) = C((P,q) \perp (P,-q)) = C(h(P))$ est une algèbre triviale, donc la classe de C' est l'opposé de la classe de C. Ainsi l'ensemble de ces classes d'équivalence est bien un groupe abélien pour la loi induite par le produit tensoriel gradué.

On notera $\mathcal{H}(A)$ le groupe ainsi obtenu, appelé <u>groupe des classes d'algèbres de Clifford</u>. Il dépend fonctoriellement de A. En effet, soit $A \to B$ un homomorphisme d'anneaux, C une A-algèbre de Clifford et $C_B = B \otimes_A C$ la B-algèbre de Clifford obtenue par extension des scalaires. Comme l'image d'une algèbre triviale est triviale, l'équivalence se conserve par extension des scalaires. De plus, $B \otimes_A (C \hat{\otimes}_A C') \simeq (B \otimes_A C) \hat{\otimes}_B (B \otimes_A C')$ ce qui montre que l'application de $\mathcal{H}(A)$ dans $\mathcal{H}(B)$ ainsi obtenue est un homomorphisme de groupes abéliens. C' est donc un foncteur covariant défini dans la catégorie des anneaux commutatifs et unitaires à valeurs dans la catégorie des groupes abéliens.

Théorème 2.8.4. Le foncteur qui à un A-module quadratique associe son algèbre de Clifford, induit un homomorphisme de groupes abéliens du groupe de Witt $W(A)$ dans le groupe $\mathcal{H}(A)$, qui est surjectif.

Le résultat provient de ce que l'algèbre de Clifford d'un espace hyperbolique est une algèbre triviale et que l'algèbre d'une somme orthogonale est le produit tensoriel gradué des algèbres de Clifford des deux facteurs. Si (P_1,q_1) et (P_2,q_2) ont même classe dans le groupe $W(A)$, $(P_1,q_1) \perp h(R_1) \approx (P_2,q_2) \perp h(R_2)$ et $C(P_1,q_1) \hat{\otimes} S_1 \approx C(P_2,q_2) \hat{\otimes} S_2$ où S_1 et S_2 sont les algèbres triviales $C(h(R_1))$ et $C(h(R_2))$, d'où l'homomorphisme noté C_A de $W(A)$ dans $\mathcal{H}(A)$, surjectif par construction.

Notons que C_A dépend fonctoriellement de A, c'est à dire que si $f : A \to B$ est un homomorphisme d'anneaux, on a le carré commutatif :

$$\begin{array}{ccc} W(A) & \xrightarrow{W(f)} & W(B) \\ \downarrow{\scriptstyle C_A} & & \downarrow{\scriptstyle C_B} \\ \mathcal{H}(A) & \xrightarrow{\mathcal{H}(f)} & \mathcal{H}(B) \end{array}$$

En d'autres termes, $C : W \to \mathcal{H}$ est une transformation naturelle de foncteurs.

Soient C une algèbre de Clifford et C^{C}_{o} l'extension quadratique graduée associée à C. Montrons que si C et C' sont deux algèbres de Clifford équivalentes, C^{C}_{o} et $C'^{C'}_{o}$ ont même classe dans le groupe $\mathfrak{D}_2(A)$ des extensions quadratiques graduées. Pour cela il suffit de montrer que si S est une algèbre triviale le commutant de $(C \hat{\otimes} S)_o$ dans $C \hat{\otimes} S$ est isomorphe à C^{C}_{o}. On peut toujours supposer que $S = \mathrm{End}_A(P_1 \oplus P_2)$ où P_1 et P_2 sont projectifs de type fini et fidèles : S_o a pour commutant son centre, l'algèbre des matrices

$$\begin{pmatrix} \lambda \mathrm{id}_{P_1} & 0 \\ 0 & \mu \mathrm{id}_{P_2} \end{pmatrix}$$

où λ et μ parcourent A. Une démonstration analogue à celle qui suit le théorème 2.6.10. montre que le commutant de $(C \hat{\otimes} S)_o$ est $C^{C}_{o} * Z(S_o)$, isomorphe à C^{C}_{o}. Il en résulte que si C et C' sont deux algèbres de Clifford équivalentes, C^{C}_{o} et $C'^{C'}_{o}$ sont isomorphes en tant qu'algèbres graduées sur $\mathbb{Z}/(2)$. Or, le

commutant de $(C \hat{\otimes} C')_o$ dans $C \hat{\otimes} C'$ est le produit ${}^{C}C^{o} * {}^{C'}C'^{o}$. Comme si C est une algèbre triviale, ${}^{C}C^{o}$ est l'élément neutre de $\mathfrak{D}_2(A)$, on a la proposition suivante :

Proposition 2.8.5. *L'application qui à une algèbre de Clifford C associe l'extension quadratique graduée ${}^{C}C^{o}$ induit un homomorphisme du groupe $\mathfrak{H}(A)$ dans le groupe $\mathfrak{D}_2(A)$, qui est surjectif.*

La surjectivité est claire. En effet, l'homomorphisme composé $W(A) \to \mathfrak{H}(A) \to \mathfrak{D}_2(A)$ n'est autre que le discriminant gradué (cf. théorème 2.6.11.) qui est surjectif. On déduit, de l'homomorphisme $\mathfrak{H}(A) \to \mathfrak{D}_2(A)$, un homomorphisme de $\mathfrak{H}(A)$ dans $Ip(A)$ en composant avec l'application $e : \mathfrak{D}_2(A) \to Ip(A)$. Notons que si $C = C(P,q)$, l'idempotent e associé à C est caractérisé par la propriété suivante : $C(1-e)$ est une $A(1-e)$-algèbre d'Azumaya et $C_o e$ est une Ae-algèbre d'Azumaya.

On désignera par $\mathfrak{H}_o(A)$ le noyau de l'homomorphisme $\mathfrak{H}(A) \to Ip(A)$: c'est l'ensemble des classes d'algèbres de Clifford des A-modules quadratiques de rang pair, ou encore l'image dans $\mathfrak{H}(A)$ du sous-groupe $W_o(A)$ de $W(A)$. Les algèbres intervenant dans $\mathfrak{H}_o(A)$ sont des algèbres d'Azumaya. On a le diagramme commutatif

$$\begin{array}{ccccccc} 0 & \to & \mathfrak{H}_o(A) & \to & \mathfrak{H}(A) & \to & Ip(A) \\ & & \downarrow & & \downarrow & & \| \\ 0 & \to & \mathfrak{D}(A) & \to & \mathfrak{D}_2(A) & \to & Ip(A) \end{array} ,$$

où les deux lignes sont exactes. De plus, le noyau de $\mathfrak{H}_o(A) \to \mathfrak{D}(A)$ est le même que celui de $\mathfrak{H}(A) \to \mathfrak{D}_2(A)$.

Considérons maintenant C et C' deux algèbres de Clifford équivalentes dont la classe est dans $\mathfrak{H}_o(A)$. Cela signifie que C et C' sont deux A-algèbres d'Azumaya et qu'il existe deux algèbres triviales S et S' telles que $C \hat{\otimes} S \approx C' \hat{\otimes} S'$. Le lemme 2.8.1. et la définition des algèbres triviales montrent qu'il existe P et P', A-modules projectifs de type fini et fidèles et un isomorphisme d'algèbres $C \otimes End_A(P) \approx C \otimes End_A(P')$. On voit donc que la classe, dans le groupe de Brauer $Br(A)$, d'une algèbre de Clifford d'un A-module quadratique de rang pair ne dépend que de la classe de cette même algèbre dans le groupe $\mathfrak{H}_o(A)$. On définit ainsi une application $\beta : \mathfrak{H}_o(A) \to Br(A)$, qui n'est pas, en général, un homomorphisme de groupes. En effet, les algèbres $C \hat{\otimes} C'$ et $C \otimes C'$ ne sont pas, en général,

équivalentes dans le groupe de Brauer de A. Notons tout de suite que $\beta(\mathcal{H}_o(A))$ est contenu dans $Br_2(A)$, le sous-groupe des éléments d'ordre 2 du groupe de Brauer. En effet, si C est une algèbre de Clifford, C est isomorphe à C^o par l'antiautomorphisme principal, soit $C \otimes C \approx C \otimes C^o \approx End_A(C)$, donc $2\,\beta(C) = 0$ dans $Br(A)$. Cependant, on a le résultat suivant :

Théorème 2.8.6. *La restriction de l'application β au noyau de l'homomorphisme $\mathcal{H}_o(A) \to \mathcal{D}(A)$ est un homomorphisme injectif de groupes abéliens.*

Que cette restriction est un homomorphisme, cela provient du théorème 2.6.10. (théorème $\otimes = \hat{\otimes}$). En effet, si $C \in Ker(\mathcal{H}_o(A) \to \mathcal{D}(A))$, $X(C)$ est trivial et $C \hat{\otimes} C'$ s'identifie à $C \otimes C'$, donc $\beta(C \hat{\otimes} C') = \beta(C \otimes C') = \beta(C) + \beta(C')$. Pour voir que β est injectif, il faut montrer que si C est dans le noyau de l'homomorphisme $\mathcal{H}_o(A) \to \mathcal{D}(A)$ et si $\beta(C) = 0$, alors C est équivalente à une algèbre triviale.

Pour cela, considérons une A-algèbre D graduée sur $\mathbb{Z}/(2)$ qui est, soit une algèbre de Clifford dont la classe est dans le noyau de l'homomorphisme $\mathcal{H}_o(A) \to \mathcal{D}(A)$, soit une algèbre triviale $End_A(P_1 \oplus P_2)$ où chacun des P_i est projectif de type fini et fidèle. Dans l'un et l'autre cas le commutant de D_o est le centre $Z(D_o)$, extension quadratique triviale de A. Soient alors e_1 et e_2 les deux idempotents de $Z(D_o)$, A-linéairement indépendants avec l'élément unité de D. Alors, $z \in D_o$ si et seulement si $e_i z = z\, e_i$ $(i = 1,2)$ et $z \in D_1$ si et seulement si $e_i\, z + z\, e_i = 1_D$ $(i = 1,2)$. En effet, il suffit de le montrer pour les algèbres triviales, car par extension fidèlement plate, l'algèbre de Clifford d'un module quadratique de rang pair peut être rendue triviale et les idempotents considérés plus haut sont conservés par extension. Or, dans la représentation matricielle de $End_A(P_1 \oplus P_2)$, e_1 et e_2 sont représentés par les matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Si $z = z_o + z_1$, $z_i \in D_i$ $(i = 0,1)$, on a $z_o = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ et $z_1 = \begin{pmatrix} 0 & \gamma \\ \delta & 0 \end{pmatrix}$ et il suffit de calculer $e_i\, z_j - z_j\, e_i$ et $e_i\, z_j + z_j\, e_i$ pour conclure.

Soit donc C une algèbre de Clifford telle que $C \in Ker(\mathcal{H}_o(A) \to \mathcal{D}(A))$ et $\beta(C) = 0$. Il existe deux A-modules projectifs de type fini et fidèles P et Q et un isomorphisme $\varphi : C \otimes End_A(P) \approx End_A(Q)$ d'algèbres graduées sur $\mathbb{Z}/(2)$. Soient e_o et e_1 les deux idempotents de $Z(C_o) \approx A \times A$. Le A-module Q est somme directe de $Q_o = e_o\, Q$ et $Q_1 = e_1\, Q$ et $End_A(Q) \approx End_A(Q_o \oplus Q_1)$. Graduons $End_A(P)$ trivialement et $End_A(Q)$ à l'aide de la décomposition $Q = Q_o \oplus Q_1$; $C \otimes End_A(P)$ étant muni de la graduation produit tensoriel, on voit que φ est un

isomorphisme gradué. Il suffit pour cela d'appliquer l'assertion ci-dessous $(C \otimes \mathrm{End}_A(P))_0 \approx C_0 \otimes \mathrm{End}_A(P)$, $(C \otimes \mathrm{End}_A(P))_1 \approx C_1 \otimes \mathrm{End}_A(P)$. Or, les éléments de C_0 commutent à e_0 et e_1, donc aussi œux de $C_0 \otimes \mathrm{End}_A(P)$ et $\varphi(C_0 \otimes \mathrm{End}_A(P)) \subset (\mathrm{End}_A(Q))_0$. Les éléments de C_1 vérifient $e_i z + z e_i = z$ $(i = 0,1)$, donc ceux de $C_1 \otimes \mathrm{End}_A(P)$ vérifient la même relation ; on a ainsi $\varphi(C_1 \otimes \mathrm{End}_A(P)) \subset (\mathrm{End}_A(Q))_1$ et, par suite φ est un isomorphisme gradué. Cela montre que la classe de C est nulle dans le groupe $\mathcal{H}(A)$, d'où le théorème.

Théorème 2.8.7. *Tout élément de $\mathcal{H}(A)$ a un ordre diviseur de 8 et tout élément de $\mathcal{H}_0(A)$ a un ordre diviseur de 4.*

En effet, si C est un élément de $\mathcal{H}(A)$ (resp. $\mathcal{H}_0(A)$), $4C$ (resp. $2C$) est dans le noyau de l'homomorphisme $\mathcal{H}(A) \to \mathfrak{B}_2(A)$ (resp. $\mathcal{H}_0(A) \to \mathfrak{B}(A)$). Comme ce noyau est un sous-groupe du groupe de Brauer dont tous les éléments sont d'ordre 2, $8C = 0$ (resp. $4C = 0$).

Exemples. 2.8.8. Soit k un corps $C_1(2)$. On a vu (cf. 1.17.4.) que l'homomorphisme $W(k) \to \mathfrak{B}_2(k)$ est un isomorphisme, donc $\mathcal{H}(k)$ s'identifie à $\mathfrak{B}_2(k)$ et $\mathcal{H}_0(k)$ à $\mathfrak{B}(k)$.

2.8.9. Si k est un corps ordonné maximal, $W(k)$ s'identifie à $\mathbb{Z}$ par l'homomorphisme signature. Le groupe $\mathcal{H}(k)$ est donc un quotient de $\mathbb{Z}$, dont tout élément est d'ordre 8 au plus : c'est donc un quotient de $\mathbb{Z}/8\mathbb{Z}$. Comme l'algèbre de Clifford de la forme quadratique $-x_1^2 - x_2^2 - x_3^2 - x_4^2$ n'est pas une algèbre de matrices sur k, car isomorphe à $M_2(\mathbb{H})$ (cf. [37]), où $\mathbb{H}$ est le corps des quaternions construit sur k, $\mathcal{H}(k)$ est isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

Théorème 2.8.10. *Soient (P,q) et (P',q') deux A-modules quadratiques de rang pair, C et C' leurs algèbres de Clifford et B' et B' les extensions quadratiques $Z(C_0)$ et $Z(C_0')$ correspondantes. Il existe alors un isomorphisme de A-algèbres graduées sur $\mathbb{Z}/(2)$, $(C \hat{\otimes} C') \otimes C(B,N) \otimes C(B',N') \approx C \otimes C' \otimes C((B,N) \perp (B',N'))$.*

Rappelons que N et N' désignent les normes des algèbres B et B' qui sont des formes quadratiques non dégénérées et $C(B,N)$ et $C(B',N')$ sont des algèbres de classe nulle dans le groupe de Brauer de A car isomorphes à $\mathrm{End}_A(B)$ et $\mathrm{End}_A(B')$ respectivement (cf. 2.4.16.). Ainsi, le théorème signifie que dans le groupe de Brauer de A, $\beta(C \hat{\otimes} C') - (\beta(C) + \beta(C'))$ est la classe de l'algèbre de Clifford de $(B,N) \perp (B',N')$.

Pour démontrer ce résultat, remarquons que l'invariant X associé à $C(P,q)$, P de rang pair, et celui associé à l'extension quadratique $B = Z(C_0)$ sont les mêmes (cf. 2.6.10.). De même, on a $X(C(B,N)) \approx X(B)$ et les applications $\mu : X \otimes X \to A$ sont les mêmes dans les deux cas. Appliquant le théorème 2.6.10.

plusieurs fois de suite, on a les isomorphismes suivants en notant $\bar{\mu}_C$ (resp. $\bar{\mu}_{C'}$) la restriction de $\mu : X(C) \otimes X(C) \to A$ (resp. $\mu' : X(C') \otimes X(C') \to A$) à la diagonale : $C \hat{\otimes} C' \otimes C(B,N) \otimes C(B',N') \approx C \otimes C'(P' \otimes X(C), q'\bar{\mu}_C) \otimes C(B,N) \otimes \otimes C(B',N') \approx C \otimes (C' \hat{\otimes} C(B,N)) \otimes C(B',N') \simeq C \otimes C' \otimes C(B \otimes X(C'), N\bar{\mu}_{C'}) \otimes \otimes C(B',N') \simeq C \otimes C' \otimes (C(B,N) \hat{\otimes} C(B',N'))$ et le dernier terme n'est autre que $C(B,N) \perp (B',N'))$.

Remarquons encore que cette dernière algèbre est équivalente à une algèbre de quaternions, d'après le théorème 2.6.10., à savoir, $C(B \otimes X(C'), N\bar{\mu}_{C'})$ où $C(B' \otimes X(C), N'\bar{\mu}_C)$.

Supposons que les A-modules quadratiques (P,q) et (P',q') sont de rang impair et soient $C = C(P,q)$ et $C' = C(P',q')$. Les algèbres $C_o(P,q)$, $C_o(p',q')$ et $C \hat{\otimes} C' = C((P,q) \perp (P',q'))$ sont toutes trois d'Azumaya. De plus, $C_o(P,q)$ et $C_o(P',q')$ sont deux sous-algèbres de $C \hat{\otimes} C'$ qui commutent, donc $C \hat{\otimes} C' = C((P,q) \perp (P',q')) \approx C_o(P,q) \otimes C_o(P',q') \otimes D$ où D est une A-algèbre centrale séparable de rang 4. Soit alors $D' = A \oplus (X(C) \otimes 1_{C'}) \oplus (1_C \otimes X(C')) \oplus \oplus (X(C) \otimes X(C'))$. Il est clair que c'est une sous-algèbre de $C \otimes C'$ et que c'est l'algèbre de Clifford de $(X(C), \bar{\mu}_C) \perp (X(C'), \bar{\mu}_{C'})$ car $X(C)$ et $X(C')$ sont formés d'éléments de degré un. De plus, cet A-module quadratique est muni d'une forme quadratique non dégénérée car 2 est inversible dans A, puisque (P,q) est un A-module quadratique de rang impair. De plus, D' commute à $C_o(P,q)$ et à $C_o(P',q')$. Comme D' et D sont de même rang, elles sont égales et on a $C((P,q) \perp (P',q')) \approx \approx C_o(P,q) \otimes C_o(P',q') \otimes C(X(C), \bar{\mu}_C) \perp (X(C'), \bar{\mu}_{C'}))$.

Supposons maintenant (P,q) de rang pair et (P',q') de rang impair ; $C_o(P',q')$ est une sous-algèbre d'Azumaya de $C_o((P,q) \perp (P',q'))$, donc $(C \hat{\otimes} C')_o \approx \approx C_o(P',q') \otimes C$. Les éléments de $P \otimes X(C')$ sont de degré 0 dans $C \hat{\otimes} C'$ et commutent à $C_o(P',q')$. De plus $(y \otimes x')^2 = - y^2 x'^2 = - q(y) \bar{\mu}_{C'}(x')$ pour tout $y \in P$ et $x' \in X(C')$. On a donc $(C \hat{\otimes} C')_o \simeq C_o(P',q') \otimes C(P \otimes X(C'), - q \bar{\mu}_{C'})$.

La loi de groupe dans $\mathcal{H}_o(A)$ se décrit comme suit. Désignons par $N(A)$ le sous-groupe de $\mathcal{H}_o(A)$ noyau de l'homomorphisme $\mathcal{H}_o(A) \to \mathcal{B}(A)$ qui s'identifie par restriction de l'application β à un sous-groupe du groupe de Brauer de A. On a la suite exacte de groupes abéliens $0 \to N(A) \to \mathcal{H}_o(A) \to \mathcal{B}(A) \to 0$, non scindée, en général. Un élément de $\mathcal{H}_o(A)$ apparaît comme un couple (C,B) où C est la classe de l'algèbre de Clifford dans le groupe de Brauer de A et B l'extension quadratique $Z(C_o)$. Notons pour B et B' dans $\mathcal{B}(A)$, $B \cup B'$ la classe, dans le groupe Brauer de A, de $C((B,N) \perp (B',N'))$. Dans ces conditions, si (C,B) et (C',B') sont deux éléments de $\mathcal{H}_o(A)$, leur somme est, d'après le théorème de 2.8.10.,

$(C + C' + B \cup B', B * B')$.

Notons que ceci permet de décrire aisément le groupe $2\,\aleph_0(A)$. En effet, comme le montre la formule ci-dessus, $2\,\aleph_0(A)$ est le sous-groupe de $N(A)$ formée des classes, dans le groupe de Brauer de A, des algèbres $C((B,N)\perp(B,N)) = B \cup B$ où B décrit le groupe $\mathfrak{D}(A)$. Il apparaît clairement que $2\,\aleph_0(A)$ est dans l'intersection de $N(A)$ avec le noyau de l'homomorphisme naturel $Br_2(A) \to Br_2(A[i])$ où $i^2 = -1$. En effet, $(B,N)\perp(B,N)$ devient, par extension des scalaires de A à $A[i]$, un espace hyperbolique, puisque -1 y est un carré et (B,N) isomorphe à $(B,-N)$. Ce sous-groupe est formé de quaternions car $B \cup B = C(B,N) \hat{\otimes} C(B,N) \simeq$ $\simeq C(B,N) \otimes C(B \otimes X(B), N\,\bar{\mu}_B)$. Il est clair aussi que l'application qui à $B \in \mathfrak{D}(A)$ associe $B \cup B \in 2\,\aleph_0(A)$ est un homomorphisme de groupes. On a donc un homomorphisme surjectif de $\mathfrak{D}(A)$ dans $2\,\aleph_0(A)$, dont le noyau contient le noyau de l'homomorphisme naturel $\mathfrak{D}(A) \to \mathcal{P}(A)$. En effet $B \cup B$ est la classe de l'algèbre de quaternions $C(B \otimes X(B), N\,\bar{\mu}_B)$ qui est nulle si $(X(B), \mu_B)$ est l'élément 0 de $\mathcal{P}(A)$ car $C(B,N) \simeq End_A(B)$. Supposons maintenant 2 inversible dans A. On sait que le A-module quadratique (B,N) est somme orthogonale de (A,m) et de $(X(B), -\bar{\mu}_B)$. Ainsi on a $B \cup B' = C((B,N)\perp(B',N')) = C((A,m)\perp(A,m)\perp(X(B), -\bar{\mu}_B)\perp(X(B'), -\bar{\mu}_{B'})) \approx C((A,m)\perp(A,m)) \hat{\otimes}$ $\hat{\otimes}\ C((X(B), -\bar{\mu}_B)\perp(X(B'), -\bar{\mu}_{B'})) \simeq C((A,m)\perp(A,m)) \otimes C((X(B), \bar{\mu}_B)\perp(X(B'), \bar{\mu}_{B'}))$ car l'invariant X de $(A,m)\perp(A,m)$ est $(A, -m)$. L'algèbre de Clifford de $(A,m)\perp(A,m)$ est triviale car $(A,m)\perp(A,m) = (A[i], N)$ et $A[i]$ est une extension séparable de A car $2 \in U(A)$. Donc $B \cup B'$ est la classe de l'algèbre de Clifford $C((X(B), \bar{\mu}_B)\perp(X(B'), \bar{\mu}_{B'}))$. On définit ainsi une application de $\mathfrak{D}(A) \times$ $\times\, \mathfrak{D}(A)$ dans $Br_2(A)$ dont les propriétés sont entièrement analogues à celles des symboles locaux (cf. [50], Ch. XIV) : l'antisymétrie (ici symétrie car dans $Br_2(A)$ tout élément est d'ordre 2), $B \cup -B = 0$, en notant $-B$ l'extension quadratique associée à $(X(B), -\bar{\mu}_B)$, ainsi que la biadditivité de $B \cup B'$ par rapport à B et B'. En effet, rappelons (cf. 2.7.3.) que si (X,μ) et (X',μ') sont deux éléments de $\mathcal{P}(A)$, $C((X,\bar{\mu})\perp(X', \bar{\mu}')) \approx C((X,\bar{\mu})\perp(X \otimes X', -\overline{\mu \otimes \mu'}))$. Il s'agit alors de montrer que si (X,μ), (X',μ') et (X'',μ'') sont trois éléments de $\mathcal{P}(A)$, $C((X,\bar{\mu})\perp$ $\perp(X', \bar{\mu}')) \otimes C((X,\bar{\mu})\perp(X'',\bar{\mu}''))$ est équivalente dans le groupe de Brauer à $C((X,\bar{\mu})\perp(X' \otimes X'', \overline{\mu' \otimes \mu''})$. Or, appliquant le théorème $\otimes = \hat{\otimes}$, la première algèbre est isomorphe à $C((X,\bar{\mu})\perp(X',\bar{\mu}')) \hat{\otimes} C((X,\bar{\mu}).(X \otimes X', -\overline{\mu \otimes \mu'})\perp(X'',\bar{\mu}'').$ $(X \otimes X', -\overline{\mu \otimes \mu'}))$ soit l'algèbre de Clifford du A-module quadratique de rang 4 $(X, \bar{\mu})\perp(X', \bar{\mu}')\perp(X', -\bar{\mu}')\perp(X \otimes X' \otimes X'', -\overline{\mu \otimes \mu' \otimes \mu''}) = (X,\bar{\mu})\perp(X \otimes X' \otimes$ $\otimes X'', -\overline{\mu \otimes \mu' \otimes \mu''})\perp h(X')$. Comme $C(h(X'))$ est triviale, cela nous donne, dans le groupe de Brauer, $C(X,\bar{\mu})\perp(X \otimes X' \otimes X'', -\overline{\mu \otimes \mu' \otimes \mu''}))$ qui est, d'après la remarque ci-dessus, isomorphe à $C((X,\bar{\mu})\perp(X \otimes X' \otimes X'' \otimes X, \overline{\mu \otimes \mu' \otimes \mu'' \otimes \mu}))$ soit, comme $(X \otimes X, \mu \otimes \mu)$ est l'élément neutre de $\mathcal{P}(A)$, $C(X,\bar{\mu})\perp(X' \otimes X'', \overline{\mu' \otimes \mu''}))$,

d'où la biadditivité du symbole.

Soient B, B' et B" trois extensions quadratiques de A, N, N' et N" leurs normes ; montrons que $B \cup B' + B \cup B" = B \cup (B' * B")$ dans $N(A) \subset Br_2(A)$. Or, $B \cup B' = C((B,N) \perp (B',N'))$ est égale, d'après le théorème 2.6.10, à la classe de $C(B \otimes X(B'), N \bar{\mu}')$ que nous abrégerons en $C(B\ X')$. Il s'agit donc de montrer que $C(B\ X') + C(B\ X") = C(B(X' \otimes X"))$ ou encore que $D = C(B\ X') \otimes C(B\ X")$ est équivalente à l'algèbre $C(B(X' \otimes X"))$. Si $b \in B$, $x' \in X'$, $x" \in X"$ et u désigne l'élément unité de B, $(b\ x' \otimes u\ x")^2 = N(b)\ \bar{\mu}'(x')\ \bar{\mu}"(x") = N(b)\ \overline{\mu' \otimes \mu"}\ (x' \otimes x")$. Le sous-module de D engendré par les éléments $b\ x' \otimes u\ x"$ est $B(X' \otimes X")$, donc D contient la sous-algèbre $C(B(X' \otimes X"))$. Notons que D est graduée sur $\mathbb{Z}/(2)$ et $C(B(X' \otimes X"))$ est formée d'éléments de degré 0 car $d^0(b\ x') = 1$ et $d^0(u\ x") = 1$, donc $D_0 \tilde{\approx} C(B(X' \otimes X")) \otimes D'_0$ où D'_0 est une A-algèbre de rang 2 donc une A-algèbre commutative et c'est le centre de D_0. C'est une extension quadratique séparable de A , car D est une algèbre de Clifford. Or, $C(B\ X) \otimes C(B\ X") \simeq$ $\simeq C(B\ X' \perp B(X \otimes X"))$ a un discriminant trivial, donc $D'_0 = A \times A$ est l'extension quadratique triviale de A. Il s'ensuit que $C(B\ X') \otimes C(B\ X") \approx C(B(X' \otimes X")) \otimes C_1$ où C_1 est une algèbre d'Azumaya qui contient l'extension quadratique triviale D'_0. Alors C_1 est une algèbre d'endomorphismes, car si e est l'un des idempotents non triviaux de D'_0, $C_1 = C_1\ e \oplus C_1(1-e)$ et ces deux A-modules projectifs sont de rang 2 et $End_{C_1}(C_1\ e)$ est un A-module projectif de rang 1, donc $End_{C_1}(C_1\ e) = A$. Il s'ensuit que $C_1 \approx End_A(C_1\ e)$, d'où la biadditivité du symbole $B \cup B'$. Ceci montre bien que l'application $\mathfrak{B}(A) \to N(A)$ définie par $B \mapsto B \cup B$ est un homomorphisme de groupes abéliens.

On remarque que si $2 = 0$ dans A, $\otimes = \hat{\otimes}$, donc $B \cup B' = 0$ dans $Br_2(A)$, quels que soient B et B' dans $\mathfrak{B}(A)$.

Nous allons montrer le résultat suivant :

Proposition 2.8.11. Soit A un corps de caractéristique différente de 2. Alors $2\,\mathcal{H}_0(A)$ s'identifie à $Br_2(A[i]/A)$ qui est isomorphe au quotient de A^* par $A^{**} + A^{**}$, sous-groupe du groupe des éléments inversibles, formé des sommes de deux carrés.

La dernière assertion de la proposition est un résultat élémentaire de cohomologie : si R est un groupe abélien sur lequel opère un groupe cyclique fini G, la cohomologie est périodique modulo 2 et $H^2(G,R)$ est isomorphe au quotient de R^G par le sous-groupe $N(R)$. Ainsi, en prenant $R = A[i]^*$ et $G = Gal(A[i]/A)$, on a $H^2(G,A[i]^*) \approx A^*/N(A[i]^*)$ et $H^2(G,A[i]^*)$ est exactement le groupe de Brauer relatif $Br_2(A[i]/A)$.

En ce qui concerne la première affirmation, notons que $2\,\mathcal{H}_0(A)$ est un sous-groupe de $Br_2(A)$ formé des classes d'algèbres de quaternions $B \cup B$. Si $B = A[x]$ avec $x^2 = a$, (B,N_B) est le module quadratique $\langle 1\rangle \perp \langle -a\rangle$ et $B \cup B$ l'algèbre de Clifford $C(\langle 1\rangle \perp \langle -a\rangle) \hat{\otimes} C(\langle 1\rangle \perp \langle -a\rangle) \approx C(\langle 1\rangle \perp \langle -a\rangle) \otimes \otimes C(\langle a\rangle \perp \langle -1\rangle)$, d'après 2.6.10. La classe de $B \cup B$ dans $Br_2(A)$ est donc l'algèbre de quaternions $(\frac{a,-1}{A})$. Il est facile de voir qu'on a un homomorphisme surjectif dans A^* dans $2\,\mathcal{H}_0(A)$ donné par $a \mapsto (\frac{a,-1}{A})$. On en détermine le noyau en se rappelant qu'une algèbre de quaternions sur un corps est une algèbre de matrices si et seulement si sa norme réduite représente 0. Comme $\mathrm{Nrd}\,(\frac{a,-1}{A}) = \langle 1\rangle \perp \langle 1\rangle \perp \perp \langle -a\rangle \perp \langle -a\rangle$, cette forme représente 0 si et seulement si a est une somme de deux carrés. On a donc bien d'isomorphisme $2\,\mathcal{H}_0(A) \approx A^*/A^{**} + A^{**}$.

Proposition 2.8.12. Si A est un corps $C_2(2)$, la surjection $W(A) \xrightarrow{C} \mathcal{H}(A)$ est un isomorphisme.

Rappelons qu'un corps $C_2(2)$ est un corps dans lequel toute forme quadratique à plus de quatre variables représente 0. Pour un corps $C_1(2)$, cas particulier de celui-ci, on a vu que $W(A) \to \mathfrak{D}_2(A)$ est un isomorphisme, ce qui montre que $W(A) \to \mathcal{H}(A)$ en est un. Dans le cas qui nous occupe, les éléments de $W(A)$ sont représentés par les classes d'isomorphismes de formes anisotropes, donc par des classes d'isomorphismes de formes de rang inférieur ou égal à 4. Supposons d'abord que A est de caractéristique 2 et soient (P,q) et (P',q') deux A-modules quadratiques de même rang tels que $C(P,q)$ et $C(P',q')$ ont même classe dans $\mathcal{H}(A)$. Alors $(P,q) \perp (P',q') \approx H \perp (P'',q'')$ où q'' est anisotrope de rang 0, 2 ou 4 et H un espace hyperbolique. L'algèbre de Clifford de (P'',q'') est triviale dans le groupe $\mathcal{H}(A)$ car $C((P,q) \perp (P',q')) = C(P,q) \hat{\otimes} C(P',q')$ est 0 dans $\mathcal{H}(A)$. Comme (P'',q'') est de rang 0,2 ou 4, (P'',q'') est hyperbolique (cf. 2.7.5.), donc $q \oplus q'$ est hyperbolique et q isomorphe à q' ($2 = 0$ dans A).

Supposons maintenant A de caractéristique différente de 2. On considère le module quadratique $(P,q) \perp (P',-q') \approx H \perp (P'',q'')$ où H est un espace hyperbolique et q'' une forme anisotrope de rang pair inférieur ou égal à 4. On suppose que P et P' sont deux espaces vectoriels de même dimension inférieure ou égale à 4 et que $C(P,q)$ et $C(P',q')$ ont même classe dans $\mathcal{H}(A)$. Il s'agit maintenant de montrer que $(P'',q'') = 0$ dans $W(A)$, en montrant que $C(P'',q'') = 0$ dans $\mathcal{H}(A)$, ce qui revient au même que de montrer que $C((P,q) \perp (P',-q')) = 0$ dans $\mathcal{H}(A)$. En dimension 1,2,3, on sait bien que si $C(P,q) = C(P',q')$ dans $\mathcal{H}(A)$, (P,q) et (P',q') sont isomorphes (cf. 2.7.). On suppose donc P et P' de dimension 4 : $C(P,q) \approx \approx C(P',q')$ et $Z(C_0(P,q)) \approx Z(C_0(P',q'))$ puisque A est un corps. On a donc $d(q) = d(q')$ et le discriminant gradué de q'' est nul. Maintenant calculons $C(P'',q'')$: d'après les résultats précédents $C(P'',q'') = C(P,q) + C(P',-q') +$

$+ (\frac{d(q),d(q')}{A})$ et comme $C(P,-q') = C(P,q') + (\frac{-1,d(q')}{A})$, on a $C(P'',q'') =$
$= C(P,q) + C(P',q') + (\frac{-d(q),d(q')}{A}) = 0$ puisque $C(P,q) = C(P',q')$ dans $Br_2(A)$ et $d(q) = d(q')$ dans $\mathfrak{D}(A)$. Maintenant, si la dimension de P'' n'est pas nulle, elle est 2 ou 4. Quand elle vaut 2, $d(q') = 0$ entraîne q'' hyperbolique. Quand elle vaut 4, il suffit d'appliquer la proposition 2.7.5. pour voir que q'' est hyperbolique. On a donc $(P,q) \perp (P',q') \approx H$, espace hyperbolique, ce qui signifie que (P,q) et (P',q') ont même image dans $W(A)$.

Les exemples classiques où s'applique 2.8.12. sont ceux des corps locaux : corps de séries formelles à corps résiduel fini et corps p-adiques, obtenus par complétion d'un corps de nombres suivant une valuation discrète.

On a le diagramme commutatif de groupes abéliens avec les lignes et les colonnes exactes

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & N(A) & = & N(A) & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{H}_0(A) & \longrightarrow & \mathfrak{H}(A) & \longrightarrow & Ip(A) \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{D}(A) & \longrightarrow & \mathfrak{D}_2(A) & \longrightarrow & Ip(A) \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

où $N(A)$ est un sous-groupe de $Br_2(A)$.

Cela permet d'avoir des renseignements sur $\mathfrak{H}$ à partir de la connaissance du groupe de Brauer et du groupe des extensions quadratiques. Ainsi si A est l'anneau des entiers d'un corps de nombres, $Br_2(A)$ est fini (cf. [21]). De même, on a vu en 2.4.17. que $\mathfrak{D}(A)$ était fini ; on peut donc énoncer la proposition suivante:

Proposition 2.8.13. Le groupe $\mathfrak{H}(A)$ de l'anneau A des entiers d'un corps de nombres est fini.

Si K est un corps p-adique, $\mathfrak{D}(K) = K^*/K^{*2}$ est fini avec 4 éléments si la caractéristique résiduelle diffère de 2 et avec 8 éléments dans le cas contraire (cf. [51]). De plus $Br(K) \approx \mathbb{Q}/\mathbb{Z}$, donc $Br_2(K) \approx \mathbb{Z}/(2)$, ce qui montre que $\mathfrak{H}_0(K)$ a respectivement 8 ou 16 éléments et que $\mathfrak{H}(K) \approx W(K)$ a respectivement 16 ou 32 éléments.

On peut de la même façon calculer le nombre d'éléments de $\mathfrak{H}(K)$ et de

$W(K)$ pour un corps de séries formelles K sur un corps fini.

2.8.14. Comme nous l'avons signalé en 1.12., on peut définir un homomorphisme, noté dis, de $\mathbb{O}(P,q)$ dans le groupe $Ip(A)$. Cet homomorphisme est défini ainsi : pour $\sigma \in \mathbb{O}(P,q)$, $C(\sigma)$ est un automorphisme de l'algèbre d'Azumaya graduée $C(P,q)$. Ainsi $C(\sigma)$ induit un automorphisme $t(\sigma)$ de l'extension quadratique $\overset{C}{C}{}^{o}$. On définit alors, localement, un idempotent noté dis (σ) par : $(\text{dis}\ (\sigma))_{\mathfrak{p}} = 0$ si $(t(\sigma))_{\mathfrak{p}}$ est l'identité de $\overset{C}{C}{}^{o}$ localisé en $\mathfrak{p}$, $\mathfrak{p} \in \text{Spec}\ (A)$ et $(\text{dis}(\sigma))_{\mathfrak{p}} = 1$ dans le cas contraire. Le fait que cela induise un homomorphisme de groupes provient immédiatement de $C(\sigma \circ \sigma') = C(\sigma) \circ C(\sigma')$. Le composé de dis et de l'homomorphisme naturel $e \mapsto 1-2e$ de $Ip(A)$ dans $\mu_2(A)$, groupe de racines carrées de A, est l'homomorphisme dét : $\mathbb{O}(P,q) \to \mu_2(A)$. On voit, par exemple, que dis (-1_P) est le rang de P modulo 2 ; si P est de rang impair, donc $\frac{1}{2} \in A$, dis est surjectif. Si $x \in P$ et $q(x) \in U(A)$, la transvection t_x (cf. 1.12.2) a pour discriminant 1 et dis est encore surjectif : la démonstration se fait localement. Le groupe spécial orthogonal $S\mathbb{O}(P,q)$ est défini dans le cas général, 2 inversible ou pas, connu étant noyau de l'homomorphisme dis.

3. PRODUITS VECTORIELS ET VARIETES DE STIEFEL

3.1. PRODUITS VECTORIELS REELS

Soient $\mathbb{R}$ le corps des nombres réels, $E = \mathbb{R}^n$ un $\mathbb{R}$-espace vectoriel de dimension n muni, d'un produit scalaire, noté $(\ |\ )$. On dira qu'une application $\mathbb{R}$-linéaire $u : \Lambda^2 E \to E$ est un produit vectoriel sur E si les conditions suivantes sont vérifiées :

PV 1) Orthogonalité : quels que soient x et y dans E, $(u(x \wedge y) \mid x) = 0$;
PV 2) Théorème de Pythagore : quels que soient x et y dans E, $\|u(x \wedge y)\|^2 + (x|y)^2 = \|x\|^2 \|y\|^2$, où $\|x\| = \sqrt{(x|x)}$ désigne la norme du vecteur x. Le théorème suivant est bien connu (cf. [57]) :

Théorème 3.1.1. *Les seules dimensions de E pour lesquelles il existe un produit vectoriel sur E sont $n = 1, 3, 7$, où l'on suppose $n \geq 1$.*

Dans [18], Eckmann a défini la notion de r-produit vectoriel, où r est un entier vérifiant la condition $1 \leq r \leq n-1$. Précisément, on dira qu'une application $\mathbb{R}$-linéaire $u : \Lambda^r E \to E$ est un r-produit vectoriel sur E si les conditions suivantes sont vérifiées : PV 1r) Orthogonalité : quels que soient $x_1, \ldots, x_r$ dans E, $(u(x_1 \wedge \ldots \wedge x_r) \mid x_i) = 0$; PV 2r) Déterminant de Gram : quels que soient $x_1, \ldots, x_r$ dans E, $\|u(x_1 \wedge \ldots \wedge x_r)\|^2 = \det((x_i|x_j)_{1 \leq i,\, j \leq r})$.

Théorème 3.1.2. *Les seules valeurs de r et n pour lesquelles il existe un r-produit vectoriel sur E sont les suivantes : 1) $r = 1$ et n pair ; 2) $r = 2$ et $n = 7$; 3) $r = 3$ et $n = 8$; 4) $r = n-1$.*

Voyons comment, dans une certaine mesure, ce théorème se réduit au précédent et pour cela, nous allons établir le théorème de réduction :

Théorème 3.1.3. (théorème de réduction). *S'il existe sur le $\mathbb{R}$-espace vectoriel euclidien $E = \mathbb{R}^n$ un r-produit vectoriel, alors il existe sur $F = \mathbb{R}^{n-1}$ un $(r-1)$-produit vectoriel.*

En effet, écrivons $E = F \oplus F^{\perp}$, donc $\Lambda^r E = \bigoplus_{p+q=r} (\Lambda^p F \otimes \Lambda^q F) \approx \Lambda^r F \oplus \oplus \Lambda^{r-1} F$ et il est clair maintenant que la restriction du r-produit vectoriel $u : \Lambda^r E \to E$ sur E à $\Lambda^{r-1} F$ est un $(r-1)$ produit vectoriel sur F.

En appliquant successivement le théorème de réduction, il existe un

2-produit vectoriel sur $\mathbb{R}^{n-r+2}$, donc $n-r+2 = 1, 3, 7$. Or, pour $n-r+2 = 1$, le produit vectoriel doit être nul, car $r = n+1$. Pour $n-r+2 = 3$, soit $r = n-1$, le r-produit vectoriel existe toujours. Dans le dernier cas, $n-r+2 = 7$, on a $n = r+5$. Des considérations sur les variétés de Stiefel, montrent (cf. [57]) que l'on ne peut pas avoir $r \geq 4$, donc $r = 1, 2, 3$. Pour $r = 1$, il est nécessaire et suffisant que n soit pair ; pour $r = 2$, $n = 7$ et pour $r = 3$, $n = 8$. Pour la construction de ces différents produits vectoriels, on renvoie à la bibliographie citée.

3.2. PRODUIT VECTORIEL ALGEBRIQUE

Soit A un anneau dans lequel 2 est inversible et (V,q) un A-module quadratique. Pour x et y dans V, on note $(x \mid y)$ l'élément $\frac{1}{2}\varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$ et on appelle <u>déterminant de Gram</u> des r vecteurs $x_1, \ldots, x_r$ de V l'élément de A, $g(x_1, \ldots, x_r) = \det((x_i \mid x_j))_{1 \leq i, j \leq r}$ (où φ est la forme A-bilinéaire symétrique associée à q).

Une application linéaire $u : \Lambda^r V \to V$ est un <u>r-produit vectoriel sur</u> V si elle satisfait aux deux conditions suivantes, pour $x_1, \ldots, x_r$ parcourant V : (P V r 1) : $\varphi(u(x_1 \wedge \ldots \wedge x_r), x_i) = 0$ et (P V r 2) : $q(u(x_1 \wedge \ldots \wedge x_r)) = g(x_1, \ldots, x_r)$.

La problème algébrique dont nous allons parler ici est le suivant : pour un entier r donné, à quelles conditions sur (V,q) existe-t-il sur V un r-prosuit vectoriel ? On peut toujours supposer V de rang constant n et l'entier r sera supposé compris strictement entre 0 et n. Notons tout d'abord les propriétés élémentaires suivantes dont la vérification est laissée au lecteur :

<u>Proposition</u> 3.2.1. (i) <u>Si</u> $f : A \to A'$ <u>est un homomorphisme d'anneaux et</u> u <u>un r-produit vectoriel sur</u> (V,q), $1' \otimes u$ <u>est un r-produit vectoriel sur</u> $(A' \otimes_A V, q')$ <u>où</u> $q' : A' \otimes_A V \to A'$ <u>est la forme quadratique étendue</u>. (ii) <u>Soient</u> u <u>un r-produit vectoriel sur</u> (V,q) <u>et</u> $x_o \in V$ <u>tel que</u> $q(x_o) = 1$. <u>L'orthogonal</u> (V',q') <u>de</u> $A\,x_o$ <u>possède un</u> $(r-1)$-<u>produit vectoriel</u> u' <u>défini par</u> $u'(y_1, \ldots, y_{r-1}) = u(x_o, y_1, \ldots, y_{r-1})$, <u>pour</u> $y_1, \ldots, y_{r-1}$ <u>parcourant</u> V'. (iii) <u>Soient</u> u <u>un r-produit vectoriel sur</u> (V,q) <u>avec</u> $r = 2p+1$ <u>et</u> a <u>un élément inversible de</u> A. <u>Alors</u> (V, aq) <u>possède un r-produit vectoriel</u> $u' = a^p u$.

Nous cherchons donc pour quels couples (r,n), $0 < r < n$, il n'y a pas de module quadratique de rang n possédant un r-produit vectoriel et, dans le cas contraire, à quelles conditions supplémentaires sur (V,q) il y a effectivement un r-produit vectoriel. Ainsi, si $r = 1$, il est nécessaire que n soit pair mais il y a une condition supplémentaire. Si $r = 2$, le rang n de V doit être 3 ou 7. Or, l'assertion (i) de la proposition ci-dessus montre que si un couple (r,n) convient

pour un anneau A, alors il existe un corps algébriquement clos pour lequel (r,n) convient aussi. On peut alors appliquer (ii) au module quadratique ainsi obtenu, donc quel que soit l'entier k plus petit que r, le couple $(r-k, n-k)$ convient. Ceci montre que si (r,n) convient et si r est supérieur à 2, $(2, n-r+2)$ convient. L'étude du cas $r = 2$ conduit alors aux deux possibilités $n = r+1$ et $n = r+5$. Dans le premier cas, il existe toujours des modules quadratiques convenables ; dans le second cas, on trouve bien des modules quadratiques de rang 8 muni d'un 3-produit vectoriel. Brown et Gray (cf. [14]) ont montré que si $r = 4$ et $n = 9$, il n'existe pas de produits vectoriels sur un corps algébriquement clos, donc sur un anneau commutatif à élément unité, d'après (i) de la proposition 3.2.1.

Lemme 3.2.2. *Il existe sur* (V,q) *un* 1*-produit vectoriel si et seulement si il existe un automorphisme* u *de* (V,q) *tel que* $u^2 + id_V = 0$.

En effet, d'après (P V 1) et (P V 2), si (V,q) a un 1-produit vectoriel, c'est une application linéaire $u : V \to V$ telle que $q(u(x)) = q(x)$ et $\varphi(x,u(x)) = 0$ pour tout x dans V. On a donc $u \in \mathbb{O}(V)$ et, en polarisant la seconde relation, $\varphi(x,u(y)) + \varphi(u(x),y) = 0$ pour x et y parcourant V. Comme u est automorphisme de φ, on a $\varphi(x,u(y)) = \varphi(u^{-1}(x),y)$, donc $\varphi(u(x) + u^{-1}(x),y) = 0$ quels que soient x et y dans V, d'où $u^2 + id_V = 0$ car φ est non dégénérée.

Inversement, si $u \in \mathbb{O}(V)$ et $u^2 = -id_V$, une vérification facile montre que $u : V \to V$ est un 1-produit vectoriel sur (V,q).

Soit alors B l'extension quadratique de A, $A[X]/(X^2+1)$. Dans les conditions du lemme 3.2.2., on munit V d'une structure de B-module par $(a+b\,i)(x) = a\,x + b\,u(x)$, où i désigne l'image de X dans B et on voit aisément que V est un B-module projectif de type fini. En effet, soient pour cela $\varphi_k : V \to A$ des formes linéaires, en nombre fini, et x_k des éléments de V tels que $x = \sum_k \varphi_k(x)\, x_k$ pour tout x dans V. Posons $\psi_k(x) = \frac{1}{2}(\varphi_k(x) - i\,\varphi_k(u(x)))$; on vérifie immédiatement que $\psi_k : V \to B$ est une forme B-linéaire et que, quel que soit x dans V, $x = \sum_k \psi_k(x)\, x_k$.

Soit maintenant l'application $h : V \times V \to B$ définie par $h(x,y) = \frac{1}{2}(\varphi(x,y) + i\,\varphi(x,u(y)))$. Il est facile de voir que h est une forme hermitienne non dégénérée vis-à-vis de l'involution de B, $a + i\,b \mapsto a - i\,b$, où a et b sont dans A. Notons que $h(x,x) = \frac{1}{2}\varphi(x,x) = q(x)$, pour tout $x \in V$.

Inversement, si V est un B-module projectif de type fini et $h : V \times V \to B$ une forme hermitienne non dégénérée, notons $Re(h) : V \times V \to A$ l'application A-bilinéaire définie par $Re(h)(x,y) = \frac{1}{2}(h(x,y) + h(y,x))$ et $Im(h) : V \times V \to A$ celle

définie par $Im(h)(x,y) = \frac{1}{2i}(h(x,y) - h(y,x))$, de sorte que $h(x,y) = Re(h)(x,y) + i\,Im(h)(x,y)$. L'application $q : V \to A$ définie par $x \mapsto h(x,x)$ est une forme quadratique non dégénérée sur le A-module V et la forme A-bilinéaire symétrique φ associée à q n'est autre que $2Re(h)$. Il est clair aussi que $Im(h)$ est une forme alternée non dégénérée. Considérons alors l'homothétie du B-module V, $u : V \to V$, $x \mapsto i\,x$ qui est une application A-linéaire. On a $q(i\,x) = h(i\,x, i\,x) = -i^2\,h(x,x) = q(x)$ et $\varphi(x, i\,x) = Re(h)(x, i\,x) = h(x, i\,x) + h(i\,x, x) = 0$ quel que soit x dans V. Ainsi u vérifie les conditions du lemme 3.2.2. et définit sur l'espace quadratique (V,q) un 1-produit vectoriel. On a ainsi démontré la proposition suivante :

Proposition 3.2.3. Soit (V,q) un A-module quadratique. Pour que (V,q) possède un 1-produit vectoriel, il est nécessaire et suffisant qu'il existe sur V une structure de A[i]-module projectif ($i^2 = -1$) et une forme hermitienne non dégénérée $h : V \times V \to A[i]$ telle que $q(x) = h(x,x)$ pour tout $x \in V$. Le 1-produit vectoriel est alors la multiplication par i.

On remarque que, comme le rang V sur A est le produit du rang de V sur A[i] par le rang de A[i] sur A, il est nécessaire que le rang de V soit pair.

Dans le cas d'un corps (ou d'un anneau local) la proposition se simplifie comme suit : pour que (V,q) possède un 1-produit vectoriel, il faut et il suffit qu'il existe un A-module quadratique (V_1,q_1) tel que $(V,q) \simeq (V_1,q_1) \perp (V_1,q_1)$. L'application $u : V_1 \oplus V_1 \to V_1 \oplus V_1$ est alors donnée par $u(x_1,x_2) = (x_2, -x_1)$.

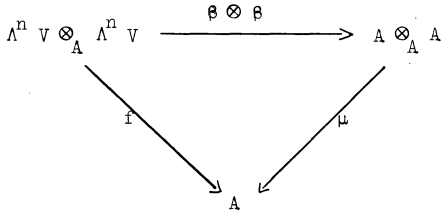
En effet, si $(V,q) \approx (V_1,q_1) \perp (V_1,q_1)$, l'application u indiquée plus haut vérifie bien $u^2 = -id_V$. Inversement, s'il existe $u \in \mathcal{O}(V)$ telle que $u^2 + id_V = 0$, on procède par récurrence sur la dimension de V. Si V est de rang 2 et si x est un vecteur tel que $q(x) \neq 0$, $\{x,u(x)\}$ est une base orthogonale de V et $(V,q) \approx (A\,x, q_{|A\,x}) \perp (A\,u(x), q_{|A\,u(x)})$; les deux facteurs de la décomposition orthogonale sont isomorphes et l'application orthogonale u a bien la forme annoncée. Si $\dim V > 2$, on choisit un vecteur x tel que $q(x) \neq 0$ et on considère $W = Ax \oplus Au(x)$; $V = W \perp V'$ et comme $U(V') \subset V'$, la restriction v de u à V' est un élément de $\mathcal{O}(V')$ tel que $v^2 = -id_{V'}$ et il suffit alors d'appliquer l'hypothèse de récurrence à V', si bien que $(V', q_{|V'}) \approx (V_1',q_1') \perp (V_1',q_1')$. L'espace quadratique cherché (V_1,q_1) est alors $(V_1',q_1') \perp (A\,x, q_{|A\,x})$ et u a bien la forme annoncée.

Avant d'étudier les cas $r = 2$ et $r = 3$, nous allons montrer que si $r = n-1$, il existe toujours un r-produit vectoriel pourvu que (V,q) vérifie une condition supplémentaire simple.

Supposons tout d'abord qu'il existe sur le A-module quadratique (V,q) de rang n, un $(n-1)$-produit vectoriel u et définissons une application $\alpha : V^n \to A$ par $(x_1,\dots, x_n) \mapsto (u(x_1 \wedge \dots \wedge x_{n-1})|x_n)$. C'est une application n-linéaire et alternée, à cause de (P V 1) et (P V 2) et elle induit une application A-linéaire $\psi : \Lambda^n V \to A$. Un calcul local montre que ψ est un isomorphisme de A-modules. En effet, V possède dans ce cas une base orthogonale $(e_i)_{1\leq i\leq n}$ car 2 est inversible ; de plus, $\psi(e_1 \wedge \dots \wedge e_n) = (u(e_1 \wedge \dots \wedge e_{n-1})|e_n)$ et comme $u(e_1 \wedge \dots \wedge e_{n-1})$ est orthogonal à tous les e_i pour $i \leq n-1$, $u(e_1 \wedge \dots \wedge e_{n-1}) = a\, e_n$, où a est un scalaire. On a alors $\psi(e_1 \wedge \dots \wedge e_n) = a\, q(e_n)$ et d'après (P V 2), $a^2\, q(e_n) = q(e_1) \dots q(e_{n-1})$, donc finalement $\psi(e_1 \wedge \dots \wedge e_n)$ est inversible dans A et $(\psi(e_1 \wedge \dots \wedge e_n))^2 = q(e_1) \dots q(e_n) = \det((e_i|e_j))$. Ainsi ψ est un isomorphisme et on a, de plus, la formule $(\psi(x_1 \wedge \dots \wedge x_n))^2 = g(x_1,\dots, x_n) = \det((x_i|x_j))_{1 \leq i,\, j \leq n}$ pour toute famille (x_i) de n éléments de V.

Comme 2 est inversible dans A, nous utiliserons, dans ce chapitre, la notion de <u>déterminant</u> d'un A-module quadratique (V,q) suivante : c'est le couple $(\Lambda^n V, f)$, où $f : \Lambda^n V \otimes_A \Lambda^n V \to A$ est l'isomorphisme composé des applications A-linéaires $\mathrm{id}_{\Lambda^n V} \otimes \Lambda^n(d_\varphi) : \Lambda^n V \otimes_A \Lambda^n V \to \Lambda^n V \otimes_A \Lambda^n V^*$ et $\mathrm{tr} : \Lambda^n V \otimes_A \Lambda^n V^* \to A$ ($d_\varphi : V \to V^*$ étant l'isomorphisme induit par φ).

Le déterminant est alors dit <u>trivial</u> s'il existe un isomorphisme $\beta : \Lambda^n V \to A$ tel que le triangle



soit commutatif, où μ est la multiplication de l'anneau A. Il est alors clair que dans notre situation le diagramme ci-dessus commute en prenant $\beta = \psi$. Ainsi, s'il existe sur (V,q) un $(n-1)$-produit vectoriel, le déterminant de (V,q) est trivial.

Réciproquement, supposons ce déterminant trivial et soit $\beta : \Lambda^n V \to A$ l'application A-linéaire qui fait commuter le triangle ci-dessus. Notons e l'élément $\beta^{-1}(1)$; à e, on associe l'application $d_\varphi^{-1} \circ t_e$ de $\Lambda^{n-1} V$ dans V

définie par $\Lambda^{n-1} V \xrightarrow{t_e} V^* \xrightarrow{d_\varphi^{-1}} V$, où d_φ est l'isomorphisme induit par q et t_e l'isomorphisme défini par e, i.e., $t_e(x_1 \wedge \ldots \wedge x_{n-1})(x_n) = e^*(x_1 \wedge \ldots \wedge x_n)$. Montrons que l'application $d_\varphi^{-1} \circ t_e$ est un $(n-1)$-produit vectoriel sur (V,q). On a bien $(d_\varphi^{-1} \circ t_e(x_1 \wedge \ldots \wedge x_{n-1}) | x_i) = t_e(x_1 \wedge \ldots \wedge x_{n-1})(x_i) = 0$ car $x_1 \wedge \ldots \wedge x_{n-1} \wedge x_i = 0$ dans $\Lambda^n V$. Pour vérifier la seconde condition, on raisonne localement et il suffit de montrer que si $\{e_1, \ldots, e_n\}$ est une base orthogonale de (V,q), $q(d_\varphi^{-1} \circ t_e(e_1 \wedge \ldots \wedge e_{n-1})) = q(e_1) \ldots q(e_{n-1})$. Or, comme $(d_\varphi^{-1} \circ t_e(e_1 \wedge \ldots \wedge e_{n-1}) | e_i) = 0$ si $1 \leq i \leq n-1$, $d_\varphi^{-1} \circ t_e(e_1 \wedge \ldots \wedge e_{n-1}) = a\, e_n$ et $t_e(e_1 \wedge \ldots \wedge e_{n-1}) = b\, \varepsilon_n$ où $\{\varepsilon_1, \ldots, \varepsilon_n\}$ est la base duale de la base $\{e_1, \ldots, e_n\}$ et a et b des éléments de A. Etant donné que $d_\varphi^{-1}(\varepsilon_n) = (q(e_n))^{-1} e_n$, on a $q(d_\varphi^{-1} \circ t_e(e_1 \wedge \ldots \wedge e_{n-1})) = a^2 q(e_n) = b^2 (q(e_n))^{-1}$. Comme le diagramme

$$\begin{array}{ccc} \Lambda^n V \otimes_A \Lambda^n V & \xrightarrow{\beta \otimes \beta} & A \otimes_A A \\ & {\scriptstyle f} \searrow \quad \swarrow {\scriptstyle \mu} & \\ & A & \end{array}$$

est commutatif, $b^2 = q(e_1) \ldots q(e_n)$, donc $q(d_\varphi^{-1} \circ t_e(e_1 \wedge \ldots \wedge e_{n-1})) = q(e_1) \ldots q(e_{n-1})$. On a ainsi démontré la proposition suivante :

Proposition 3.2.4. Le A-module quadratique (V,q) de rang n possède un $(n-1)$-produit vectoriel si et seulement si son déterminant est trivial.

Notons que pour tout anneau A et pour tout entier $n > 0$, il existe des A-modules quadratiques vérifiant la condition demandée : il en est ainsi de A^n muni de la forme quadratique $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i^2$.

3.3. ALGEBRES CAYLEYENNES ET PRODUIT VECTORIEL

Le produit vectoriel classique dans $\mathbb{R}^3$ (resp. $\mathbb{R}^7$) est intimement lié à l'algèbre des quaternions (resp. des octonions). Cette situation n'est pas particulière aux réels et nous voulons montrer ici comment la méthode employée en topologie (cf. [1]), combinée à des résultats sur certaines algèbres, donne des

résultats presque complets sur l'existence de 2- et 3- produits vectoriels.

On appelle algèbre cayleyenne sur A un couple (E,s) où E est une A-algèbre non nécessairement associative à élément unité e et s un autiautomorphisme de E telque $x + s(x)$ et $x\,s(x)$ sont dans Ae quel que soit x dans E.

Comme $s(e) = e$, $s(x + s(x)) = x + s(x)$ pour tout $x \in E$, donc s^2 est l'identité de E, si bien que s est une antiinvolution de E qu'on appelle conjugaison de E et qu'on note $x \mapsto \bar{x}$. Les propriétés élémentaires de ces algèbres sont données dans [12], Chapitre III, et nous ne ferons que rappeler celles que nous utiliserons. En général, $x \mapsto x\bar{x}$ est une forme Ae-quadratique notée $N_E : E \to Ae$, appelée norme (cayleyenne) et l'application $x \mapsto x + \bar{x}$ une forme Ae-linéaire $Tr : E \to Ae$ appelée trace, qui n'est autre que le produit scalaire induit par la norme de x avec l'élément unité e de E. Tout élément u de E vérifie l'équation du second degré $X^2 - Tr(u)\,X + N_E(u)\,e = 0$ à coefficients dans Ae.

Exemples. 3.3.1. Le couple formé d'une extension quadratique B de A et de son unique A-automorphisme non trivial (cf. 2.4.) est une algèbre cayleyenne ; la norme N_B n'est autre que la norme de B considérée comme extension galoisienne de A.

3.3.2. Soit $C = C(P,q)$ une algèbre de quaternions sur A et $s : z \mapsto \bar{z}$ l'antiautomorphisme involutif de C (cf. 2.7.). Alors (C,s) est une algèbre cayleyenne dont la norme est la norme réduite. Cet exemple se généralise aisément au cas d'une algèbre d'Azumaya (centrale séparable) de rang 4.

3.3.3. Soient (E,s) une A-algèbre cayleyenne, $\gamma \in A$ et $F = E \oplus E$. Définissons sur F une multiplication par $(x,y)(x',y') = (x\,x' + \gamma\,\bar{y}'y,\ y\,\bar{x}' + y'\,x)$ et posons $t(x,y) = (\bar{x}, -y)$. Alors le couple (F,t) est une algèbre cayleyenne et on a les résultats suivants (cf. [12]) : (i) E s'identifie à une sous-algèbre cayleyenne de F. (ii) Le A-module quadratique (F,N_F) est somme orthogonale de (E,N_E) et de $(E,\gamma\,N_E)$; la norme N_F est non dégénérée si et seulement si N_E l'est et γ est inversible dans A. (iii) F est associative si et seulement si E est associative et commutative. (iv) F est alternative (i.e., quels que soient $x,y \in F$, $x^2y = x(x\,y)$ et $y\,x^2 = (y\,x)x$) si et seulement si E est associative. Ici, du fait de l'antiinvolution t, F est alternative si et seulement si $x^2y = x(x\,y)$ pour x et y parcourant F.

3.3.4. Soit C une A-algèbre centrale séparable de rang 4 munie de son antiinvolution naturelle et γ un élément inversible de A. On appelle algèbre d'octonions l'algèbre cayleyenne construite à partir de C et de γ suivant le procédé de l'exemple précédent. C'est donc une algèbre alternative, de rang 8 en tant que module,

et sa norme cayleyenne N est une forme quadratique non dégénérée et multiplicative en ce sens que $N(xy) = N(x)\,N(y)$ pour x et y parcourant C (cf. [12]).

Il existe une réciproque partielle à ce résultat (cf. [29]) qui s'énonce ainsi :

Proposition 3.3.5. Soit E une A-algèbre non nécessairement associative à élément unité, qui est un A-module projectif de type fini. Si E est munie d'une forme quadratique $q : E \to A$ multiplicative et non dégénérée, alors E est une A-algèbre cayleyenne alternative.

Soit $x \in E$ et désignons par u_x la multiplication par x à gauche (ou à droite). Du fait de la multiplicativité de la forme quadratique q, on a les deux relations suivantes : $q(u_x(y)) = q(x)\,q(y)$ et $\varphi(u_x(y),y) = \varphi(x,1)\,q(y)$ quel que soit l'élément y de E, où φ est la forme A-bilinéaire symétrique associée à q. En polarisant par rapport à y les deux relations, on a $\varphi(u_x(y), u_x(y')) = q(x)\,\varphi(y,y')$ et $\varphi(u_x(y), y') + \varphi(u_x(y'), y) = \varphi(x,1)\,\varphi(y,y')$ quels que soient y et y' dans E. Posons $y' = u_x(z)$ dans la seconde égalité et utilisons alors la première relation ; on obtient la relation $\varphi((u_x \circ u_x - \varphi(x,1)\,u_x + q(x)\,id_E)(z), y) = 0$ quels que soient y et z dans E. Comme q est non dégénérée, cela signifie que $u_x \circ u_x - \varphi(x,1)\,u_x + q(x)\,id_E = 0$. On a donc $x^2 = \varphi(x,1)\,x - q(x)$, ce qui entraîne aussi $u_{x^2} = \varphi(x,1)\,u_x - q(x)id_E$, donc $u_x \circ u_x = u_{x^2}$ et ceci signifie exactement que E est une algèbre alternative.

Pour voir que E est une algèbre cayleyenne, il faut trouver l'antiautomorphisme de conjugaison. L'équation $x^2 = \varphi(x,1)x - q(x)$ nous incite à poser $\bar{x} = -x + \varphi(x,1)$. Il est immédiat de vérifier que $x \mapsto \bar{x}$ est une involution linéaire et il reste à voir que c'est bien un antiautomorphisme (comme E est un A-module projectif de type fini, il existe au plus une antiinvolution qui fait de E une algèbre cayleyenne (cf. [12]). Remarquons tout d'abord que $x\,\bar{x} = \bar{x}\,x = q(x)$ par définition de $\bar{x}$, donc $\varphi(x,y) = x\,\bar{y} + y\,\bar{x}$. Ainsi $\varphi(x,\bar{y}) = x\,y + \bar{y}\bar{x}$ et $\varphi(x\,y,\,1) = x\,y + \overline{x\,y}$. Pour démontrer la proposition, il suffit donc de montrer que $\varphi(x,\bar{y}) = \varphi(x\,y,1)$, quels que soient x et y dans E. Or, calculons $\varphi((x\,y)\bar{y},\bar{y})$. D'une part, c'est égal à $q(\bar{y})\,\varphi(x\,y,1) = q(y)\,\varphi(x\,y,1)$ et d'autre part, comme E est alternative, $(x\,y)\bar{y} = x(y\,\bar{y}) = x\,q(y)$, c'est égal à $\varphi(x,\bar{y})\,q(y)$. Comme $q(y) = q(\bar{y})$, pour tout couple (x,y) d'éléments de E, $(\varphi(x,\bar{y}) - \varphi(x\,y,\,1))\,q(y) = 0$. Fixant x, nous souhaitons montrer que la forme A-linéaire $\psi : E \to A$ définie par $y \mapsto \varphi(x,\bar{y}) - \varphi(x\,y,1)$ est nulle. Pour cela on raisonne localement : E est alors un module libre qui possède une base e_i, $1 \leq i \leq n$, avec $q(e_i)$ inversible dans A. Or, $\psi(e_i)\,q(e_i) = 0$, donc $\psi(e_i) = 0$ pour chaque i et ψ est identiquement

nulle, ce qui démontre le résultat.

Les algèbres cayleyennes alternatives vont nous fournir des exemples de 2- et 3- produits vectoriels. Nous supposons désormais 2 inversible dans A et soit C une algèbre alternative cayleyenne qui est un A-module projectif de type fini et dont la norme N est non dégénérée. On appelle C_+ le sous-A-module de C formé des z de C tels que $\bar{z} = -z$; c'est l'orthogonal de l'élément unité de C et l'on a la décomposition orthogonale de A-modules quadratiques $(C,N) = (A\,1, N_{|A\,1}) \perp (C_+, N_{|C_+})$. Remarquons que si x et y sont dans C_+, $N(x) = x\bar{x} = -x^2$ et $2(x|y) = \varphi(x,y) = x\bar{y} + y\bar{x} = -(xy + yx)$. On a alors :

Proposition 3.3.6. (i) Sur le A-module quadratique $(C_+, N_{|C_+})$, il existe un 2-produit vectoriel u donné par $u(x \wedge y) = xy + (x|y)$, pour x et y parcourant C_+. (ii) Sur le A-module quadratique (C,N) il existe un 3-produit vectoriel v donné par $v(x \wedge y \wedge z) = x(\bar{y}\,z) - x(y|z) + y(z|x) - z(x|y)$, pour x,y et z parcourant C.

Pour (i), la démonstration est une simple vérification. On notera encore N la restriction de N à C_+. Remarquons que l'application $(x,y) \mapsto xy + (x|y)$ est, pour l'instant, simplement une application A-bilinéaire de $C_+ \times C_+$ dans C. Elle est en fait alternée car $x^2 + (x|x) = -N(x) + N(x) = 0$, étant donnée que $x \in C_+$; en conséquence, $u(x \wedge y) = -u(y \wedge x)$. Or, $\overline{u(x \wedge y)} = \overline{xy + (x|y)} = \overline{xy} + \overline{(x|y)} = \bar{y}\,\bar{x} + (x|y) = yx + (y|x) = u(y \wedge x) = -u(x \wedge y)$, donc $u(x \wedge y) \in C_+$ ce qui montre que u est bien une application A-bilinéaire alternée de $C_+ \times C_+$ dans C_+. Il suffit maintenant de montrer que $(u(x \wedge y)|x) = 0$ et $N(u(x \wedge y)) = N(x)\,N(y) - (x|y)^2$ quels que soient x et y dans C_+. En effet, $(u(x \wedge y)|x) = \frac{1}{2}(x\,u(x \wedge y) + u(x \wedge y)x) = \frac{1}{2}(x(xy + (x|y)) + (xy + (x|y))x) = \frac{1}{2}(x(xy + yx) + 2x(x|y)) = 0$ car $2(x|y) = -(xy + yx)$ et, de même, $N(u(x \wedge y)) = (xy + (x|y))(yx + (x|y)) = (xy)(yx) + (x|y)(xy + yx + (x|y)) = (xy)(yx) - (x|y)^2$. Comme C est alternative, on a aussi $(xy)(yx) = xy^2x = x^2y^2 = (-N(x))(-N(y)) = N(x)\,N(y)$, d'où le résultat voulu.

En ce qui concerne (ii), la vérification est un peu plus longue (cf.[59]). Montrons que v, manifestement A-trilinéaire, est alternée. En effet, $v(x,x,z) = x(\bar{x}\,z) - z(x|x)$ et comme $x(\bar{x}\,z) = (x\,\bar{x})z = N(x)z = (x|x)z$, on a $v(x,x,z) = 0$. De même $v(x,y,x) = x(\bar{y}\,x) - 2x(x|y) + y(x|x) = x(\bar{y}\,x) - x(\bar{x}\,y + \bar{y}\,x) + y(x|x) = -x(\bar{x}\,y) + y(x|x) = 0$ et la dernière assertion se vérifie aussi facilement. Vérifions maintenant que $(x|v(x \wedge y \wedge z)) = 0$. Or, on a $2(x|v(x \wedge y \wedge z)) = \varphi(x, x(\bar{y}\,z)) - \varphi(x, x\,\varphi(y,z)) = N(x)(\varphi(1, \bar{y}\,z) - \varphi(y,z)) = 0$, d'après ce qu'on a vu dans la démonstration de la proposition 3.3.5. Comme v est alternée, on a,

de même, $(y|v\ (x \wedge y \wedge z)) = (z|v(x \wedge y \wedge z)) = 0$ et en développant, on obtient les relations : $(y|x(\bar{y}\ z)) = 2(x|y)(z|y) - N(y)\ (x|z)$ et $(z|x(\bar{y}\ z)) = N(z)(x|y)$. Il nous reste à calculer $N(v(x \wedge y \wedge z))$. D'après les calculs précédents, $v(x \wedge y \wedge z) = x(\bar{y}\ z) + t$, où t est orthogonal à $v(x \wedge y \wedge z)$. Ainsi, $N(v(x \wedge y \wedge z)) = (v(x \wedge y \wedge t)|x(\bar{y}\ z)) = N(x(\bar{y}\ z)) - (x(y|z)|x(\bar{y}\ z)) + (y(z|x)|x(\bar{y}\ z)) - (z(x|y)|x(\bar{y}\ z))$ et les deux formules ci-dessus jointes à la multiplicativité de la norme nous donnent $N(v(x \wedge y \wedge z)) = N(x)\ N(y)\ N(z) - N(x)\ (y|z)^2 - N(y)\ (z|x)^2 - N(z)\ (x|y)^2 + 2(x|y)(y|z)(z|x)$ soit, comme $N(x) = (x|x)$,

$$N(v(x \wedge y \wedge z)) = \begin{vmatrix} (x|x) & (y|x) & (z|x) \\ (x|y) & (y|y) & (z|y) \\ (x|z) & (y|z) & (z|z) \end{vmatrix}$$

ce qui achève de montrer que v est un 3-produit vectoriel.

Nous allons voir qu'inversement, étant donné un 2 (resp. un 3)-produit vectoriel sur un module quadratique, il existe toujours (resp. localement) une algèbre cayleyenne alternative qui lui correspond. Cela nous permettra ensuite de montrer que le rang n du module correspondant est 3 ou 7 si $r = 2$, 4 ou 8 si $r = 3$.

Soit donc (V,q) un A-module quadratique possédant un 2-produit vectoriel u ; u est une application linéaire de $\Lambda^2 V$ dans V telle que $(u(x \wedge y)|\ |\ x) = 0$ et $q(u(x \wedge y)) = q(x)\ q(y) - (x|y)^2$ quels que soient x et y dans V. Soit alors B le module $A \oplus V$ muni de la forme quadratique non dégénérée $N : B \to A$ donnée par $N((a,x)) = a^2 + q(x)$. Sur B, nous définissons la multiplication $(a,x)(b,y) = (ab - (x|y), ay + bx + u(x \wedge y))$, dont $(1,0)$ est l'élément unité. Un calcul facile montre que $N((a,x)(b,y)) = N(a,x)\ N(b,y)$ du fait des propriétés du produit vectoriel u. Ainsi B vérifie les hypothèses de la proposition 3.3.5. : c'est donc une algèbre alternative cayleyenne dans laquelle B_+ coïncide avec V et on a $u(x \wedge y) = x\ y + (x|y)$ pour x et y dans V. On a donc la proposition suivante :

Proposition 3.3.7. *Pour que* (V,q) *possède un* 2*-produit vectoriel, il faut et il suffit qu'il existe une algèbre alternative cayleyenne* B *telle que* $(V,q) \simeq B_+$ *muni de la norme cayleyenne ; le produit vectoriel est alors donné par la formule* $u(x \wedge y) = x\ y + (x\ |\ y)$.

Le fait que B est une algèbre alternative montre que l'on a $u(x \wedge u(x \wedge y)) = x(x|y) - y\ q(x)$ quels que soient x et y dans V. En effet, $u(x \wedge y) = x\ y + (x|y)$, donc $u(x \wedge u(x \wedge y)) = x\ u(x \wedge y) = x(x\ y) + x(x|y)$ et,

comme B est alternative, on écrit $x(x\,y) = x^2 y = -q(x)\,y$ car x est dans B_+. Cela donne par polarisation en x, $u(x \wedge u(y \wedge z)) + u(y \wedge u(x \wedge z)) = x(y|z) + y(x|z) - 2z(x|y)$. Si l'on cherche alors à quelle condition B est associative, on trouve qu'il faut que $u(x \wedge u(y \wedge z)) - u(y \wedge u(x \wedge z)) = y(x|z) - x(y|z)$, pour (x,y,z) parcourant B^3. Utilisant la relation ci-dessus, on a :

Corollaire 3.3.8. Pour que B soit associative, il faut et il suffit que le produit vectoriel u vérifie la formule du double produit vectoriel, à savoir $u(x \wedge u(y \wedge z)) = y(x|z) - z(x|y)$, quels que soient x,y et z dans V.

Pour préciser encore les modules quadratiques (V,q) qui possèdent un 2-produit vectoriel, on a la proposition suivante :

Proposition 3.3.9. Soit E une algèbre alternative cayleyenne dont la norme est non dégénérée. Si E est un module projectif de type fini et de rang constant, ce rang est 1,2,4 ou 8. Si E n'est pas associative, le rang est 8 et si E n'est pas commutative, le rang est 4 ou 8.

Nous ne démontrons le résultat que si 2 est inversible dans A (pour le cas général, le lecteur pourra consulter [29]). Dans ce cas, E est somme orthogonale de $A\,1_E$ et de E_+ et l'application linéaire $u_x : E \to E$ définie par $u_x(y) = x\,y$ vérifie $u_x^2 = -N(x)\,1_E$ pour tout $x \in E_+$. On obtient ainsi un homomorphisme $\rho : E_+ \to End_A(A)$ qui vérifie la relation $(\rho(x))^2 = -N(x)$ pour tout $x \in E_+$; il se prolonge donc en un homomorphisme d'algèbres $\bar{\rho} : C(E_+,-N) \to End_A(E)$ qui fait de E un $C(E_+,-N)$-module à gauche.

Si E est de rang impair 2q+1, E_+ est de rang pair 2q et $C = C(E_+,-N)$ est une A-algèbre centrale séparable. On a donc une décomposition $End_A(E) \approx \bar{\rho}(C) \otimes D$ où D est le commutant de $\bar{\rho}(C)$ dans $End_A(E)$, d'où l'égalité $(2q+1)^2 = h\,2^{2q}$ où h est le rang de D en tant que A-module. La seule solution possible est q = 0 et le rang de E est 1.

Si E est de rang pair 2q, E_+ est de rang impair 2q-1 et $C_o(E_+,-N)$ est centrale séparable. On a une décomposition analogue à celle du cas impair et $End_A(E) \approx \bar{\rho}(C_o(E_+,-N)) \otimes D$ où D est le commutant de $\bar{\rho}(C_o(E_+,-N))$ dans $End_A(E)$. On a donc l'égalité $(2q)^2 = h\,2^{2(q-1)}$ dont les seules solutions sont q = 1 et h = 4, q = 2 et h = 4, q = 4 et h = 1, d'où les rangs 2, 4 et 8 possibles pour E. Il est facile de voir (cf. Exemples 3.3.1., 3.2.2. et 3.3.4.) que ces rangs sont effectivement atteints. Pour les résultats concernant associativité et commutativité, on se reportera à [29].

Corollaire 3.3.10. Soit (V,q) un A-module quadratique de rang constant qui possède un 2-produit vectoriel. Alors V est de rang 3 ou 7 ; V est de rang 3 si

et seulement si la formule du double produit vectoriel est vraie.

C'est une conséquence de la proposition précédente appliquée à $B = A \oplus V$.

On remarque que, d'après la proposition 3.2.4., un module quadratique de rang 3 possède un 2-produit vectoriel si et seulement si son déterminant est trivial.

Dans le cas de rang 7, il existe un homomorphisme de $C(V,-q)$ dans $End_A(A \oplus V)$. Comme le rang de V est impair, $C(V,-q) \approx C_o(V,-q) \otimes_A D$ où D est l'extension quadratique centre de $C(V,-q)$. D'autre part, les rangs de $C_o(V,-q)$ et de $End_A(A \oplus V)$ sont égaux et ce sont des algèbres centrales séparables ; elles sont donc isomorphes et D est l'extension quadratique triviale de A. On sait que $C_o(V,-q)$ et $C_o(V,q)$ sont des A-algèbres isomorphes, donc $C_o(V,q)$ et $End_A(A \oplus V)$ sont nécessairement isomorphes. La condition portant sur le centre de $C(V,-q)$ signifie, puisque 2 est inversible dans A, que le déterminant de (V,q) est trivial (cf. 3.2.). On a donc :

Proposition 3.3.11. Une condition nécessaire pour qu'un module quadratique (V,q) de rang 7 possède un 2-produit vectoriel est que son déterminant soit trivial et que son algèbre de Clifford C_o soit de classe nulle dans le groupe de Brauer de A. Si A est un corps, la condition est suffisante.

La première assertion vient d'être démontrée. Pour la seconde, c'est une conséquence directe du fait que la norme d'une algèbre alternative cayleyenne de rang 8 sur un corps est de la forme $q_1 \otimes q_2 \otimes q_3$ où q_1, q_2 et q_3 sont des formes quadratiques de rang 2 qui représentent 1, donc (V,q) possède un 2-produit vectoriel si et seulement si $(V,q) \perp \langle 1 \rangle = q_1 \otimes q_2 \otimes q_3$. Or, d'après [41], une forme de rang 8 est de la forme $q_1 \otimes q_2 \otimes q_3$ si et seulement si discriminant et algèbre de Clifford sont triviaux. Il suffit alors d'en regarder la conséquence sur (V,q). Les remarques qui suivent 3.2.1. montrent que :

Corollaire 3.3.12. Pour que le module quadratique (V,q) possède un 3-produit vectoriel, il est nécessaire que le rang de V soit 4 ou 8.

Dans le cas de rang 4, 3.2.4. donne la condition nécessaire et suffisante pour l'existence d'un 3-produit vectoriel.

Proposition 3.3.13. Soit (V,q) un module quadratique qui possède un 3-produit vectoriel u. S'il existe e dans V tel que $q(e)$ est inversible, alors il existe sur V une structure de A-algèbre cayleyenne alternative dont la norme cayleyenne est proportionnelle à q.

Notons que si $v : V \times V \times V \to V$ est l'application trilinéaire définie par $v(x,y,z) = u(x \wedge y \wedge z) + x(y|z) - y(z|x) + z(x|y)$, on a $q(v(x,y,z)) =$

$= q(x)\,q(y)\,q(z)$ du fait des axiomes (P V 1) et (P V 2). Considérons maintenant V' l'orthogonal de Ae dans V, muni de la forme quadratique $q(e)^{-1}\,q$; V' possède un 2-produit vectoriel $u' : (x,y) \mapsto u(x \wedge e \wedge y)$. Considérons alors sur $B = A \oplus V'$ la structure d'algèbre alternative cayleyenne associée au 2-produit vectoriel u' de V'. Il est immédiat de vérifier que, en identifiant $V = Ae \oplus V'$ avec B, la norme cayleyenne s'identifie à $q(e)^{-1}\,q$ ce qui est le résultat annoncé. Si A est un corps, il est donc nécessaire et suffisant que q soit de la forme $q_1 \otimes q_2 \otimes q_3$ où les q_i sont des formes de rang 2. Dans ce cas, Brown et Gray (cf. [14]) ont montré qu'il existe sur $(V, q_1 \otimes q_2 \otimes q_3)$ deux 3-produits vectoriels non isomorphes ; c'est ce qui leur permet ensuite de montrer que pour $r = 4$ et $n = 9$, il n'y a pas de produits vectoriels.

3.4. VARIETES DE STIEFEL ALGEBRIQUES

Soit (P,q) un A-module quadratique où P est un module projectif de type fini et notons q l'élément de la composante homogène de degré 2, $S_2(P^*)$, de l'algèbre symétrique du dual de P, canoniquement associé à la forme quadratique q de φ l'élément de $P^* \otimes_A P^*$ associé à la forme A-bilinéaire symétrique associée à q.

Soient alors r un entier positif et $A_r(P)$ l'algèbre symétrique de $P_1^* \oplus \ldots \oplus P_r^*$, où chaque P_i est une copie de P. On désigne par $J_r(P,q)$ l'idéal de $A_r(P)$ engendré par les éléments $q_i - 1$, $1 \leq i \leq r$ et φ_{ij}, $1 \leq i \leq j \leq r$, où q_i est l'image de q dans $S_2(P_i^*)$ et φ_{ij} l'image de φ dans $P_i^* \otimes_A P_j^*$, sous-A-module de $A_r(P)$.

On appelle <u>variété de Stiefel d'ordre</u> r, de (P,q) et on note $V_r(P,q)$ la A-algèbre quotient $A_r(P)/J_r(P,q)$.

<u>Exemple</u> 3.4.1. Supposons P libre de rang n et soit $(e_i)_{1 \leq i \leq n}$ une base de P. Posons, pour $i \neq j$, $a_{ij} = \varphi(e_i,e_j)$ et $a_{ii} = q(e_i)$. On voit facilement que $V_r(P,q) = A[x_{ij}]$ avec $1 \leq i \leq n$, $1 \leq j \leq r$ et les relations

$$\sum_{1 \leq i \leq j \leq n} a_{ij}\, x_{ih}\, x_{ij} = 1, \text{ pour } h = 1,\ldots,r \text{ et } 2 \sum_{i=1}^{n} a_{ii}\, x_{ih}\, x_{ik} +$$

$$+ \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n \\ i \neq j}} a_{ij}\, x_{ih}\, x_{jk} = 0 \quad \text{pour } h \neq k.$$

Si B est une A-algèbre commutative, on note $\mathcal{V}_{r,B}(P,q)$ l'ensemble des r-uples ordonnés $(x_1,\ldots,x_r)$ d'éléments de $P \otimes_A B$ vérifiant $(q \otimes B)(x_i) = 1$

pour $1 \leq i \leq r$ et $(\varphi \otimes B)(x_i, x_j) = 0$, si $i \neq j$.

Théorème 3.4.2. (Théorème fondamental). Il existe une bijection naturelle entre $\mathrm{Hom}_{A\text{-alg}}(V_r(P,q), B)$ et $\mathcal{U}_{r,B}(P,q)$.

Se donner un homomorphisme de A-algèbres de $V_r(P,q)$ dans B revient à se donner un homomorphisme de $A_r(P)$ dans B nul sur l'idéal $J_r(P,q)$, c'est-à-dire, r homomorphismes $\psi_i : P \to B$ de A-modules tels que : (i) $S_2(\psi_i)(q) = 1$, $i = 1, \ldots, r$; (ii) $(\psi_i \otimes \psi_j)(\varphi) = 0$, $i,j = 1,\ldots,r$ et $i \neq j$. Comme P est projectif de type fini, $\mathrm{Hom}_A(P^*,B)$ est naturellement isomorphe à $P \otimes_A B$ et soit x_i l'élément de $P \otimes_A B$ associée à ψ_i par cet isomorphisme. La condition (i) équivaut à $(q \otimes B)(x_i) = 1$; il suffit pour le voir de regarder ce qui se passe si P est libre. Soit $(e_j)_{1 \leq j \leq n}$ une base de P et $(X_j)_{1 \leq j \leq n}$ la base duale; q s'écrit $\sum_{1 \leq j \leq k \leq n} a_{jk} X_j X_k + \sum_{i=1}^{n} a_{ii} X_i^2$, avec $a_{jk} = \varphi(e_j, e_k)$ et $a_{ii} = q(e_i)$. L'homomorphisme ψ_i est donné par les $b_j = \psi_i(X_j)$ et l'élément x_i, associé à ψ_i, est $\sum_{j=1}^{n} b_j(e_j \otimes 1)$. On a alors $(q \otimes \mathrm{id}_B)(x_i) = \sum_{1 \leq j \leq k \leq n} a_{jk} b_j b_k$ et $S_2(\psi_i)(q) = \sum_{1 \leq j \leq k \leq n} a_{jk} b_j b_k$, d'où le résultat. On montre de la même manière que la condition (ii) est équivalente à $(\varphi \otimes B)(x_i, x_j) = 0$, si $i \neq j$.

Avant d'énoncer des corollaires du théorème fondamental, donnons la définition suivante. Si B est un anneau, sur le B-module libre B^n de rang n, on appelle produit intérieur la forme quadratique $(b_1,\ldots,b_n) \mapsto \sum_{i=1}^{n} b_i^2$. On a alors :

Corollaire 3.4.3. Soit B une A-algèbre commutative et supposons que $2 \in U(B)$ et que $\mathrm{Hom}_{A\text{-alg}}(V_r(P,q),B)$ soit non vide. Alors $P \otimes_A B$ possède un facteur orthogonal libre de rang r sur lequel la restriction de $q \otimes B$ est le produit intérieur.

Comme $\mathrm{Hom}_{A\text{-alg}}(V_r(P,q),B)$ est non vide, il existe dans $P \otimes_A B$ des éléments $x_1, \ldots, x_r$ qui forment un système orthonormé vis-à-vis de la forme quadratique $q \otimes B$. Comme 2 est inversible dans B, le sous-B-module M qu'ils engendrent est libre de rang r et la restriction de $q \otimes B$ à ce sous-module est le produit intérieur, qui est une forme non dégénérée ; M muni de ce produit intérieur est donc facteur direct orthogonal de $P \otimes_A B$.

Corollaire 3.4.4. Si $2 \in U(A)$ et si $r > \sup_{\mathfrak{p} \in \mathrm{Spec}(A)} r_P(\mathfrak{p})$, alors $V_r(P,q) = \{0\}$.

Rappelons que $r_P(\mathfrak{p})$ est le rang de $A_{\mathfrak{p}}$-module libre $P_{\mathfrak{p}} = P \otimes_A A_{\mathfrak{p}}$. Dans les hypothèses du corollaire supposons $V_r(P,q)$ non réduit à 0. Il existe alors une A-algèbre commutative B telle que $\mathrm{Hom}_{A\text{-alg}}(V_r(P,q),B)$ est non vide

à laquelle on peut appliquer le corollaire 3.4.3. .

En tout point de Spec(B), le rang de $P \otimes_A B$. est donc supérieur ou égal à r ce qui est impossible puisque r est supérieur au rang de P. Ceci démontre le corollaire.

L'hypothèse 2 inversible est nécessaire. En effet, si A est un corps de caractéristique 2 et (P,q) un A-module quadratique qui représente 1 (i.e., il existe x, $x \in P$, tel que $q(x) = 1$), alors $\mathcal{V}_{r,A}(P,q)$ est non vide quel que soit l'entier r car le r-uple $(x, \ldots, x)$ en est un élément, étant donné que $\varphi(x,x) = 2q(x) = 0$. Ainsi $V_r(P,q)$ n'est pas résuit à $\{0\}$.

Si (P,q) est un A-module quadratique et $r \leq \sup_{\mathfrak{p} \in \mathrm{Spec}(A)} r_P(\mathfrak{p})$, $V_r(P,q)$ n'est pas résuit à $\{0\}$, car il existe un corps k et un homomorphisme d'anneaux $u : A \to k$ tel que $P \otimes_A k$ soit de rang supérieur ou égal à r. Il est clair que, si par exemple k est pris algébriquement clos, $\mathcal{V}_{r,k}(P,q)$ est non vide et $V_r(P,q)$ non réduit à $\{0\}$.

Corollaire 3.4.5. *Supposons P de rang constant n, 2 inversible dans la A-algèbre commutative B et $\mathrm{Hom}_{A\text{-alg}}(V_n(P,q),B)$ non vide. Alors $(P \otimes_A B, q \otimes B)$ est isomorphe à B^n muni du produit intérieur et il y a une bijection entre $\mathrm{Hom}_{A\text{-alg}}(V_n(P,q),B)$ et le groupe $\mathcal{O}_n(B)$ des automorphismes de B^n muni du produit intérieur.*

Comme nous sommes dans les hypothèses du corollaire 3.4.3., et que P est de rang n, $P \otimes_A B$ possède un facteur orthogonal libre de rang n, donc lui est égal, d'où le premier résultat. La bijection entre $\mathcal{V}_{n,B}(P,q)$ et $\mathcal{O}_n(B)$ se définit comme dans le cas topologique. Soient $(x_1, \ldots, x_n)$ un élément fixé de $\mathcal{V}_{n,B}(P,q)$ et $u \in \mathcal{O}_n(B)$. Alors $(u(x_1), \ldots, u(x_n))$ est élément de $\mathcal{V}_{n,B}(P,q)$. Réciproquement, à $(y_1, \ldots, y_n)$ élément de $\mathcal{V}_{n,B}(P,q)$ on associe la matrice des y_j dans la base de $P \otimes_A B$ formée des x_i qui est visiblement un élément de $\mathcal{O}_n(B)$.

Notons enfin des propriétés fonctorielles bien claires de V_r. Soit $u : (P,q) \to (P',q')$ un morphisme de A-modules quadratiques et ${}^t u : P'^* \to P^*$. On en déduit un homomorphisme $A_r(u)$ de A-algèbres de $A_r(P')$ dans $A_r(P)$; si les A-modules P et P' sont projectifs de type fini, alors $A_r(u)$ envoie $J_r(P',q')$ sur $J_r(P,q)$ car $q = q' \circ u$, d'où par passage aux quotients, un homomorphisme de A-algèbres $V_r(u) : V_r(P',q') \to V_r(P,q)$. On vérifie aisément que V_r est un foncteur contravariant de la catégorie des A-modules quadratiques, dont le module sous-jacent est projectif de type fini dans la catégorie des A-algèbres commutatives.

La variété de Stiefel $V_r(P,q)$ se comporte bien vis-à-vis de l'extension des scalaires. Ainsi, il est immédiat de vérifier que si $A \to A'$ est un homomor-

phisme d'anneaux, $V_r(P \otimes_A A', q')$ s'identifie naturellement à $V_r(P,q) \otimes_A A'$, car un résultat analogue est vrai pour l'algèbre symétrique $A_r(P \otimes_A A')$, où q' : $P \otimes_A A' \to A'$ est la forme A'-quadratique étendue.

Dans les mêmes hypothèses que ci-dessus, appliquons le théorème fondamental à $B = V_r(P,q)$ supposé non réduit à $\{0\}$. Ainsi $\mathrm{Hom}_{A\text{-alg}}(V_r(P,q), V_r(P,q))$ est en bijection avec $\mathcal{U}_{r,V_r(P,q)}(P)$; à l'identité de $V_r(P,q)$ correspond donc une famille ordonné $(x_{1,r}, \ldots, x_{r,r})$ de r vecteurs orthonormés de $P \otimes_A V_r(P,q)$. Soit alors B une A-algèbre commutative et $\psi : V_r(P,q) \to B$ un homomorphisme de A-algèbres ; il induit une application $\mathrm{id}_P \otimes \psi : P \otimes_A V_r(P,q) \to P \otimes_A B$ et la famille ordonnée des r vecteurs $y_i = (\mathrm{id}_P \otimes \psi)(x_{i,r})$ est un élément de $\mathcal{U}_{r,B}(P,q)$. C'est exactement l'élément de $\mathcal{U}_{r,B}(P,q)$ associé à ψ suivant le théorème de 3.4.2. Supposons maintenant $V_{r+1}(P,q)$ **non réduit à** 0 et considérons la famille ordonnée des vecteurs $(x_{1,r+1}, \ldots, x_{r+1,r+1})$ de $P \otimes_A V_{r+1}(P,q)$ associée à l'identité de $V_{r+1}(P,q)$, comme on vient de le voir pour $V_r(P,q)$. Ne considérant que les r premiers vecteurs, on a un élément de $\mathcal{U}_{r,V_{r+1}(P,q)}(P,q)$, c'est à dire, du fait de 3.4.2., un homomorphisme naturel qu'on notera $\theta_{r,1} : V_r(P,q) \to V_{r+1}(P,q)$. On notera $\theta_{r,k} : V_r(P,q) \to V_{r+k}(P,q)$, l'homomorphisme composé $\theta_{r,k} = \theta_{r+k-1,1} \circ \ldots \circ \theta_{r,1}$, défini si $V_{r+k}(P,q)$ est non réduit à 0. Remarquons que $\theta_{r,k}$ est susceptible d'une définition directe à partir des considérations du début de ce paragraphe.

Pour toute A-algèbre commutative B, $\theta_{r,k}$ induit une application $\tilde{\theta}_{r,k}$ de $\mathrm{Hom}_{A\text{-alg}}(V_{r+k}(P,q),B)$ dans $\mathrm{Hom}_{A\text{-alg}}(V_r(P,q),B)$ par $\tilde{\theta}_{r,k}(\varphi) = \varphi \circ \theta_{r,k}$. D'après le théorème fondamental, $\tilde{\theta}_{r,k}$ définit une application qu'on notera $\theta_{r,k} : \mathcal{U}_{r+k,B}(P,q) \to \mathcal{U}_{r,B}(P,q)$. L'utilisation de la définition de $\theta_{r,k}$ montre que cette dernière application $\theta_{r,k}$ n'est autre que la projection naturelle qui à la famille $(y_1, \ldots, y_r, y_{r+1}, \ldots, y_{r+k})$ de r+k vecteurs orthonormés de $P \otimes_A B$ associe la famille $(y_1, \ldots, y_r)$ formée des r premiers.

La relation vue plus haut entre $V_r(P,q)$ et $V_{r+k}(P,q)$ peut s'exprimer de manière géométrique si l'on suppose 2 inversible dans A. Soit alors P'_r le sous-$V_r(P,q)$-module de $P \otimes_A V_r(P,q)$ engendré par les vecteurs $(x_{i,r})_{1 \le i \le r}$.

D'après le corollaire 3.4.3., P'_r est facteur orthogonal du $V_r(P,q)$-module quadratique $P \otimes_A V_r(P,q)$. Appelons P''_r l'orthogonal de P'_r et soit $V_k(P''_r,q)$ la variété de Stiefel d'ordre k associée au $V_r(P,q)$-module quadratique P''_r.

Théorème 3.4.6. $V_{r+k}(P,q)$ s'identifie canoniquement à $V_k(P''_r,q)$.

Considérons l'injection naturelle de $A_r(P)$ dans $A_{r+k}(P)$. Elle identifie $A_{r+k}(P)$ à l'algèbre symétrique $S_{A_r(P)}(M_1 \oplus \dots \oplus M_k)$ où M_i est une copie du $A_r(P)$-module projectif $P^* \otimes_A A_r(P)$. L'idéal $J_r(P,q)$ (en fait, son image dans $A_{r+k}(P)$) est contenu dans $J_{r+k}(P,q)$ ce qui donne l'homomorphisme naturel $\theta_{r,k}$: $V_r(P,q) \to V_{r+k}(P,q)$. Ainsi $V_{r+k}(P,q)$ apparaît comme un quotient de l'algèbre symétrique $C = S_{V_r(P,q)}(T_1 \oplus \dots \oplus T_k)$ où T_i est le $V_r(P,q)$-module projectif $P^* \otimes_A V_r(P,q) \approx (P \otimes_A A_r(P)) \otimes_{A_r(P)} V_r(P,q)$ par un idéal dont les générateurs sont les images dans C des générateurs de $J_{r+k}(P,q)$, c'est à dire ici les $\varphi_{i,r+h}$, $1 \le i \le r$, $1 \le h \le k$, les $q_{r+h} - 1$, $1 \le h \le k$ et les $\varphi_{r+h_1,\, r+h_2}$, $1 \le h_1 < h_2 \le k$. Or, en tant que fonction sur $P_h \otimes_A V_r(P,q)$, $\varphi_{i,r+h}$ est la forme linéaire $y \mapsto (\varphi \otimes V_r(P,q))(x_{i,r}, y)$. Ecrivons $(P \otimes V_r(P,q),\ q \otimes V_r(P,q))$ comme somme orthogonale de $(P'_r,\ q'_r)$ et de $(P''_r,\ q''_r)$; passer au quotient par les images des $\varphi_{i,r+h}$ revient en fait à se placer dans l'orthogonal de P'_r, c'est à dire, que $V_{r+k}(P,q)$ est quotient de l'algèbre $C' = S_{V_r(P,q)}(M)$ où M est la somme directe de k copies du dual de P''_r. Du fait de la décomposition orthogonale de $P \otimes_A V_r(P,q)$, $q \otimes V_r(P,q)$ est somme de $q'_r \in S^2(P'^*_r)$ et de $q''_r \in S^2(P''^*_r)$ et l'image de q'_r est nulle dans C'. Ainsi l'élément q_{r+h} donne dans C' l'élément $q''_{r,h}$, image de $q''_r \in S^2(P''^*_r)$ dans la $h^{\text{ième}}$ copie de $S^2(P''^*_r)$. De la même façon on voit que les $\varphi_{r+h_1, r+h_2}$ ont pour image dans C', l'image dans le produit tensoriel de la $h^{\text{ième}}$ copie de P''_r par $h^{\text{ième}}$ copie de P''_r de la forme bilinéaire symétrique associée à la forme quadratique q''_r. Ainsi $V_{r+k}(P,q)$ s'identifie bien à $V_k(P''_r,\ q''_r)$.

Géométriquement, cela signifie que si B est une A-algèbre, $\mathcal{V}_{r+k,B}(P,q) \to \mathcal{V}_{r,B}(P,q)$ est une fibration dont la fibre au-dessus d'un point x de $\mathcal{V}_{r,B}(P,q)$ est de la forme $\mathcal{V}_{k,B}(P''_r, q''_r)$ où B est considérée comme une $V_r(P,q)$-algèbre au moyen de x.

Exemples. 3.4.7. Supposons que (P,q) est l'espace hyperbolique de A ; $V_1(P,q)$ est l'anneau de l'hyperbole $A[x,y]$ avec $x\,y = 1$. Si (P,q) est l'espace hyperbolique d'un module projectif P_o de type fini et de rang constant, on peut décrire de façon analogue $V_1(P,q)$: $S_A(P^*)$ est l'anneau $S_A(P_o) \otimes_A S_A(P_o^*)$ en identifiant P_o à son bidual et l'idéal $J_1(P,q)$ est engendré par les éléments $x \otimes f - f(x)$, $x \in P_o$, $f \in P_o^*$. En effet, la forme quadratique q, élément de $S_2(P^*) \approx S_2(P_o) \oplus P_o \otimes_A P_o^* \oplus S_2(P_o^*)$ n'est autre que le triple, $(0, \alpha, 0)$ où α est le générateur canonique de $P_o \otimes_A P_o^*$, i.e., si $u : P_o \otimes_A P_o^* \to A$ est l'isomorphisme $u(x \otimes f) = f(x)$, $\alpha = u^{-1}(1)$. Ainsi $x \otimes f = f(x)\alpha$ par définition même de α et

comme $\alpha - 1 = q - 1$ est le générateur de $J_1(P,q)$, $x \otimes f - f(x) = f(x)(\alpha - 1)$ est dans $J_1(P,q)$. Comme les éléments $x \otimes f$ engendrent $P_o \otimes_A P_o^*$, on a bien le résultant annoncé.

Graduons maintenant $S_A(P^*)$ sur $\mathbb{Z}$ par $d^o x = 1$ si $x \in P_o - \{0\}$, et $d^o f = -1$ si $f \in P_o^* - \{0\}$. Alors $J_1(P,q)$ est un idéal homogène et $V_1(P,q)$ est naturellement muni d'une graduation sur $\mathbb{Z}$. L'anneau gradué $V_1(P,q)$ s'identifie à la somme directe graduée $\bigoplus_{n \in \mathbb{Z}} (P_o^{\otimes n})$, où $P_o^{-1} = P_o^*$, avec le produit $P_o^{\otimes m} \times$ $\times P_o^{\otimes n} \to P_o^{\otimes (n+m)}$. En effet, $S_A(P) = \bigoplus_{m,n \geq 0} (P_o^{\otimes n}) \otimes (P_o^{*\otimes m})$ et soit $u = x_1 \otimes \ldots \otimes x_n \otimes f_1 \otimes \ldots \otimes f_m$ un élément de $P_o^{\otimes n} \otimes P_o^{*\otimes m}$; si $n > m$, $u \equiv f_1(x_1) \ldots f_m(x_m)\, x_{m+1} \otimes \ldots \otimes x_n$ modulo $J_1(P,q)$; si $n = m$, $u \equiv \prod_{i=1}^{n} f_i(x_i)$ et si $n < m$, $u \equiv f_1(x_1) \ldots f_n(x_n)\, f_{n+1} \otimes \ldots \otimes f_m$ modulo $J_1(P,q)$, ce qui montre l'isomorphisme annoncé de $V_1(P,q)$ avec $\bigoplus_{n \in \mathbb{Z}} (P_o^{\otimes n})$.

3.4.8. Soit P un A-module projectif de type fini et de rang 1 muni d'une forme quadratique non dégénérée q ; donc 2 est nécessairement inversible dans A. Le corollaire 3.4.4. montre que seul $V_1(P,q)$ n'est pas réduit à 0. Cet anneau est le quotient de $S_A(P^*)$ par l'idéal principal $(q-1)$ et, en fait, $V_1(P,q)$ n'est autre que l'algèbre de Clifford du module quadratique (P,q). Considérons, en effet, l'application naturelle ρ de P dans $V_1(P,q)$ composée de $P \xrightarrow{\alpha} P^* \to S_A(P^*) \xrightarrow{\pi}$ $\xrightarrow{\pi} V_1(P,q)$ où α est l'isomorphisme induit par q et π la projection de $S_A(P^*)$ sur $V_1(P,q) = S_A(P^*)/(q-1)$. Un calcul local facile montre que $(\rho(x))^2 = q(x)1$, donc que ρ se prolonge en un homomorphisme naturel $C(\rho)$ de $C(P,q)$ dans $V_1(P,q)$. Comme P est projectif de rang 1 et que q est un générateur du module libre de rang 1, $S_2(P^*)$, $V_1(P,q)$ en tant que module est isomorphe à $A \oplus P^*$, ou encore du fait de α à $A \oplus P$. Il est clair que $C(\rho)$ est un isomorphisme de A-algèbres et que $V_1(P,q)$ est une extension quadratique de A.

Supposons maintenant que (P,q) est un espace quadratique de rang n, 2 étant toujours inversible et soit $r < n$: $P'_r \approx r < 1 >$. Ainsi $(P \otimes_A V_r(P,q),$ $q \otimes V_r(P,q)) \approx r < 1 > \perp (P''_r, q''_r)$ et $(\Lambda^n P, \Lambda^n q) \otimes_A V_r(P,q) \approx (\Lambda^{n-r} P''_r, \Lambda^{n-r} q''_r)$, en passant aux puissances extérieures. Prenons en particulier $r = n-1$: P''_{n-1} est projectif de type fini et de rang 1, donc on a l'isomorphisme $(\Lambda^n P, \Lambda^n q) \otimes_A V_{n-1}(P,q) \approx$ $\approx (P''_{n-1}, q''_{n-1})$. L'exemple précédent montre que $V_n(P,q)$ n'est autre que le

produit tensoriel $V_{n-1}(P,q) \otimes_A B$, où B est l'extension quadratique de A, $C(\Lambda^n P, \Lambda^n q)$.

3.5. ANNEAUX FACTORIELS ET SPHERES

Rappelons qu'un anneau factoriel est un anneau de Krull dont le groupe des classes d'idéaux divisoriels est nul ou encore, dont tout idéal divisoriel est principal (cf. [13]). On a alors les propriétés suivantes : (i) un anneau de Krull A est factoriel si et seulement si $A[X]$ l'est ; (ii) si S est une partie multiplicative de A et A est factoriel, $S^{-1}A$ est factoriel ; (iii) réciproquement si $S^{-1}A$ est factoriel et A est de Krull et si S est engendré dans des éléments p_i tels que les idéaux $A\,p_i$ soient premiers, alors A est factoriel (théorème de Nagata).

Enfin nous utilisons aussi le résultat suivant : on suppose que A est une k-algèbre graduée sur $\mathbb{N}$, où $A_o = k$ est un corps. Si A est de Krull et s'il existe une extension k' de k telle que $A \otimes_k k'$ est un anneau factoriel, alors A est factoriel.

Considérons un corps k et $F \in k[X_1, \ldots, X_n]$ un polynôme homogène du second degré qui représente une forme quadratique non dégénérée et de rang n. On peut alors considérer deux k-algèbres, $A_F = k[X_1, \ldots, X_n]/(F(X_1,\ldots,X_n))$ et $A'_F = k[X_1, \ldots, X_n]/(F(X_1,\ldots,X_n)-1)$. Les résultats concernant la factorialité de ces algèbres sont presque tous connus et nous allons les rappeler et les compléter, résolvant ainsi une question posée par R. FOSSUM (cf. [20]; voir [39] pour une solution indépendante de la nôtre). Nous aurons besoin de la proposition suivante :

Proposition 3.5.1. *Soient k un corps et k' une extension quadratique séparable de k. Le noyau de l'homomorphisme naturel $W(k) \to W(k')$ est le sous-Bil(k)-module engendré par la classe dans $W(k)$ du k-module quadratique $(k', N_{k'})$.*

C'est un résultat dont on trouvera la démonstration en caractéristique différente de 2 dans [30] et qui résulte du lemme suivant :

Lemme 3.5.2. *Soit F une forme quadratique anisotrope sur k telle que $F_{k'}$ représente 0. Alors F a une décomposition orthogonale $F_1 \perp F_2$ où F_1 est une forme de rang 2 proportionnelle à $N_{k'}$.*

Nous démontrerons ce lemme en supposant k de caractéristique 2, la démonstration générale en étant une copie. Le corps k' est de la forme $k[x]$ avec $x^2 + x + a = 0$ et $N_{k'}(u + v\,x) = u^2 + u\,v + a\,v^2$, $u,v \in k$. Dire que $F_{k'}$ représente 0 signifie qu'il existe des vecteurs α et β dont les composantes sont

dans k tels que $F_{k'}(\alpha + x\,\beta) = 0$. On a donc $F(\alpha) + x\,\varphi(\alpha,\beta) + x^2 F(\beta) = 0$, soit :

$$F(\alpha) + a\,F(\beta) = 0$$

$$\varphi(\alpha,\beta) + F(\beta) = 0$$

Comme ni α, ni β ne sont nuls, $F(\alpha)$ et $F(\beta)$ diffèrent de 0 ; α et β sont linéairement indépendants et le plan qu'ils engendrent est non dégénéré car $\varphi(\alpha,\beta) \neq 0$. On a donc une décomposition orthogonale $F = F_1 \perp F_2$ où F_1 est la restriction de F au plan $k\,\alpha \oplus k\,\beta$. Il suffit de voir maintenant que F_1 est proportionnelle à $N_{k'}$. En effet $F_1(u\,\beta + v\,\alpha) = F(\beta)\,(u^2 + u\,v + a\,v^2) = F(\beta)\,N_{k'}(u + v\,x)$ ce qui est le résultat souhaité.

La proposition 3.5.1. se démontre maintenant de la façon suivante : soit F une forme quadratique anisotrope sur k telle que $F_{k'}$ est hyperbolique ; on voit alors que F est de la forme $N_{k'} \otimes \phi$ où ϕ est une forme bilinéaire symétrique non dégénérée en appliquant le lemme 3.5.2. et en raisonnant par récurrence sur le rang de F. Nous utiliserons le cas particulier suivant du lemme 3.5.2. :

Corollaire 3.5.3. Soit F une forme quadratique anisotrope de rang 4. Il existe une extension quadratique séparable k' de k telle que $F_{k'}$ est hyperbolique si et seulement si le discriminant de F est trivial.

Si $F_{k'}$ est hyperbolique, $F \approx N_{k'} \otimes \phi$ a son discriminant trivial car ϕ est de rang 2. Si le discriminant de F est trivial, $F \approx \langle a \rangle \perp \langle b \rangle \perp \langle c \rangle \perp \langle d \rangle$ avec $ab = cd$ en caractéristique différente de 2. Si $k' = k(\sqrt{-ab})$, $F_{k'}$ est hyperbolique. En caractéristique 2, cela signifie que $F = F_1 \perp F_2$ où F_1 et F_2 ont même invariant d'Arf a. Il suffit alors de prendre $k' = k[\mathcal{P}^{-1}(a)] = k[x]$ avec $x^2 + x + a = 0$.

Proposition 3.5.4. Si $n \geq 5$ ou si $n = 4$ et le discriminant de F est non trivial, alors A_F est factoriel.

En effet, dans l'un et l'autre cas, il existe une extension quadratique k' de k telle que $F \otimes k'$ représente 0 donc, quitte à faire un changement de variables linéaires, F s'écrit $Y_1\,Y_2 + G(Y_3, \ldots, Y_n)$ où G représente une forme non dégénérée à $n-2$ variables. Si $n \leq 5$, $n-2 \geq 3$ et G est irréductible dans $k[Y_1, Y_2, \ldots, Y_n]$; si $n = 4$, G est aussi irréductible, car sinon G pourrait s'écrire $Y_3\,Y_4$ et $F \otimes k'$ serait hyperbolique, ce qui est impossible à cause du corollaire 3.5.3. Dans l'algèbre $A_F \otimes_k k'$, l'image y_1 de Y_1 est donc un élément premier. Si on localise par rapport à la partie multiplicative $S = \{1, y_1, y_1^2, \ldots, y_1^n, \ldots\}$, on obtient un anneau de polynômes en $y_1, y_3, \ldots, y_n$ localisé par rapport à y_1, donc un anneau factoriel. Appliquant le théorème de

Nagata, on en déduit que A_F est factoriel.

Si $n < 3$, il n'est bien entendu pas question que A_F soit factoriel ; si $n = 3$, on sait (cf. [46]) que A_F est factoriel si et seulement si la forme quadratique F n'a pas de zéro non trivial dans k. Dans le cas contraire il est bien clair que $A_F = k[x, y, z]$ avec la relation $x\,y = z^2$, ne peut pas être factoriel. Reste le cas où $n = 4$ et où le discriminant de F vaut 1. Alors le résultat est le suivant : A_F n'est pas factoriel.

En effet, en caractéristique différente de 2, A_F est de la forme $k[x_1, x_2, x_3, x_4]$ avec la relation $x_1^2 + a\,x_2^2 + b(x_3^2 + a\,x_4^2) = 0$. Soit alors $k' = k[w]$ avec $w^2 = -a$. On a $A_F \otimes_k k' \approx k'[y_1, y_2, y_3, y_4]$ avec $y_1y_2 - y_3y_4 \mp = 0$, où $y_1 = x_1 + w\,x_2$, $y_2 = x_1 - w\,x_2$, $y_3 = -b(x_3 + w\,x_4)$ et $y_4 = x_3 - w\,x_4$. Dans $A_F \otimes_k k'$, on a les deux idéaux premiers de hauteur 1, $P_1 = (y_1, y_3)$ et $P_2 = (y_2, y_4)$ qui sont non principaux et engendrent le groupe des classes d'idéaux de $A_F \otimes_k k'$. L'idéal $P_1\,P_2$ a pour interxection avec A_F l'idéal engendré par $x_1^2 + a\,x_2^2$, $x_3^2 + a\,x_4^2$, $x_1\,x_3 + a\,x_2\,x_4$ et $x_2\,x_3 - x_1\,x_4$ qui est un idéal premier divisoriel puisque P_1 et P_2 le sont et que $A_F \otimes_k k'$ est entier sur A_F. L'anneau A_F n'est donc pas factoriel. D'après [20], le groupe des classes de diviseurs de A_F est $\mathbb{Z}$.

En caractéristique 2, F s'écrit, dans une base convenable, $X_1^2 + X_1\,X_2 + a\,X_2^2 + b(X_3^2 + X_3\,X_4 + a\,X_4^2)$. Notant x_i l'image de X_i dans A_F, on voit comme plus haut que l'idéal $(x_1^2 + x_1\,x_2 + a\,x_2^2, x_3^2 + x_3\,x_4 + a\,x_4^2, x_1\,x_3 + a\,x_2\,x_4, x_1x_4 + x_2\,x_3 + x_3\,x_4)$ est un idéal premier de hauteur 1 non principal ce qui montre encore que A_F n'est pas factoriel. En caractéristique 2, le discriminant est l'invariant d'Arf.

Etudions maintenant la k-algèbre A'_F. Soit $\tilde{F}(Y_1, \ldots, Y_n, T) = F(Y_1, \ldots, Y_n) - T^2$ et considérons l'anneau $S^{-1}\,A_{\tilde{F}}$ où S est la partie multiplicative formée des puissances de t, image de T dans $A_{\tilde{F}}$. Considérons alors l'homomorphisme $\varphi : k[X_1, \ldots, X_n] \to S^{-1}\,A_{\tilde{F}}$ défini par $\varphi(X_i) = y_i\,t^{-1}$, où y_i est l'image de Y_i dans $A_{\tilde{F}}$. On a $\varphi(F(X_1, \ldots, X_n)) = t^{-2}\,F(y_1, \ldots, y_n) = 1$ donc φ passe au quotient en un homomorphisme injectif de A'_F dans $S^{-1}\,A_{\tilde{F}}$. Il est alors facile de voir que $A'_F[X, X^{-1}]$ s'identifie à $S^{-1}\,A_{\tilde{F}}$ en envoyant X sur t. Si F est irréductible dans $k[X_1, \ldots, X_n]$, c'est à dire si $n > 2$ ou si $n = 2$ et F ne

représente pas 0, t est un élément premier de $A_F^{\sim}$. La factorialité de A'_F équivaut dans ce cas à celle de $A_F^{\sim}$. Donc si $n \geq 4$ ou si $n = 3$ et dét $F \neq -1$, A'_F est factoriel ; si $n = 3$ et dét $F = -1$, A'_F ne peut pas être factoriel. Ainsi par exemple $R[x, y, z]$ avec $x^2 + y^2 + z^2 + 1 = 0$ n'est pas factoriel.

Reste le cas où $n = 2$. Si F ne représente pas 0, il ne faut pas que $\tilde{F}$ représente 0, c'est à dire que F représente 1. Par contre si F représente 0, $A'_F = k[x,y]$ avec $x\,y = 1$ est factoriel. On obtient ainsi la proposition suivante :

Proposition 3.5.5. A'_F est factoriel sauf dans les deux cas suivants : (i) $n = 3$ et dét $F = -1$; (ii) $n = 2$ et F représente 1 sans représenter 0.

Remarquons que si $n = 1$, A'_F est soit un corps, soit le produit de deux exemplaires de k, soit les nombres duaux en caractéristique 2.

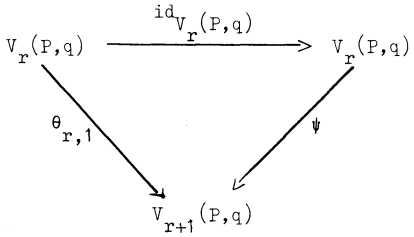
Nous supposons maintenant que A est un anneau factoriel de corps des fractions K et que (P,q) est un A-module quadratique de rang n et nous nous intéressons à la factorialité de la A-algèbre $V_1(P,q)$. Or, $S = A - \{0\}$ est engendrée par des éléments premiers, aussi bien dans $V_1(P,q)$ que dans A. La factorialité de $V_1(P,q)$ est donc entraînée par celle de $V_1(P,q) \otimes_A K \approx V_1(P \otimes K, q \otimes K) = A'_q$. Notons, de plus, comme A est factoriel, que la condition dét $(q \otimes K) = -1$ équivaut à la condition dét $q = -1$. On a alors :

Proposition 3.5.6. Soit A un anneau factoriel. La A-algèbre $V_1(P,q)$ est un anneau factoriel si le rang de P est ≥ 4 ou s'il est égal à 3 et dét $q \neq -1$.

La proposition 3.5.6. permet d'étudier la factorialité de $V_r(P,q)$ pour $r > 1$. En effet, $V_r(P,q)$ est de la forme $V_1(P''_{r-1}, q''_{r-1})$ sur l'anneau $V_{r-1}(P,q)$. On déduit donc aisément de la proposition précédente, le corollaire suivant :

Corollaire 3.5.7. Soit A un anneau factoriel dans lequel 2 est inversible et (P,q) un A-module quadratique de rang n. Alors $V_r(P,q)$ est factoriel si $r \leq n-3$. Si $r = n-2$ et dét$(q) = -1$, $V_r(P,q)$ n'est pas factoriel.

On suppose donné un A-module quadratique (P,q) muni d'un r-produit vectoriel u (et donc 2 est inversible dans A) et considérons la variété de Stiefel $V_r(P,q)$ et l'espace quadratique $(P \otimes V_r(P,q), q \otimes V_r(P,q))$ muni du produit vectoriel $\bar{u}$ déduit de u. Si l'on considère le vecteur $y = \bar{u}(x_{1,r} \wedge \ldots \wedge x_{r,r})$ le $(r+1)$-uple $(x_{1,r}, \ldots, x_{r,r}, y)$ est une famille ordonnée de $(r+1)$-vecteurs orthonormés de $P \otimes_A V_r(P,q)$ et définit donc un homomorphisme ψ : $V_{r+1}(P,q) \to V_r(P,q)$. Comme les r premiers vecteurs de ce $(r+1)$-uple sont les $x_{i,r}$, $1 \leq i \leq r$, on a le triangle commutatif



et on peut énoncer la proposition suivante :

Proposition 3.5.8. Pour que le A-module quadratique (P,q) possède un r-produit vectoriel, il est nécessaire que l'homomorphisme de A-algèbres $\theta_{r,1} : V_r(P,q) \to V_{r+1}(P,q)$ possède un inverse à gauche.

La variété de Stiefel $V_1(P,q)$ d'un A-module quadratique (P,q), avec 2 inversible dans A, est l'équivalent algébrique naturel de la sphère topologique. Il est donc intéressant, par analogie avec le cas topologique, de s'intéresser au $V_1(P,q)$-module des A-dérivations de la A-algèbre $V_1(P,q)$ qui est l'équivalent du fibré tangent à la sphère. On a alors :

Proposition 3.5.9. Le $V_1(P,q)$-module D_1 des A-dérivations de $V_1(P,q)$ est l'orthogonal dans $(P \otimes_A V_1(P,q),\ q \otimes V_1(P,q))$ du sous-espace $V_1(P,q)\, x_{11}$.

Une A-dérivation de $V_1(P,q)$ provient d'une A-dérivation de $S_A(P^*)$ nulle sur q. Il suffit alors d'écrire ce que cela signifie pour obtenir la proposition. En conséquence D_1 est un $V_1(P)$-module projectif de type fini.

La proposition précédente permet de montrer deux résultats partiels.

Proposition 3.5.10. Soit k un corps de caractéristique différente de 2, q une forme quadratique non dégénérée de rang n et $R = k[X_1,\ldots,X_n]/(q(X_1,\ldots,X_n)-1)$ la sphère algèbrique. Alors le R-module des k-dérivations de R est un R-module libre de rang n-1 si q représente 0.

La proposition 3.5.10. est conséquence des deux lemmes suivants dont le premier est bien connu :

Lemme 3.5.11. Soit A un anneau, n un entier et $\{e_1, \ldots, e_n\}$ la base canonique de A^n. Pour un élément unimodulaire x de A^n, les conditions suivantes sont équivalentes : (i) tout supplémentaire de A x est libre ; (ii) il existe un A-automorphisme $f : A^n \to A^n$ tel que $f(x) = \sum_{i=1}^{n} b_i e_i$ avec b_1 inversible dans A.

Lemme 3.5.12. Soit dans A^n un élément unimodulaire $x = \sum_{i=1}^{n} a_i e_i$. Pour que Ax ait un supplémentaire libre, il suffit que l'un des n vecteurs $x - a_i e_i$ soit unimodulaire.

La condition du lemme 3.5.12. peut se dire de la façon suivante : l'idéal engendré par n-1 des a_i est égal à A. Supposons donc que l'on ait la relation $1 = a_1 b_1 + \sum_{i=3}^{n} a_i b_i$ et définissons l'application linéaire f de A^n dans A^n par $f(e_1) = (\alpha + 1)e_1 + \alpha e_2$, $f(e_2) = e_1 + e_2$, $f(e_j) = \lambda b_j e_1 + e_j$ pour $j \geq 3$, où α et λ sont des scalaires qu'on choisira par la suite.

L'application f est un automorphisme de A^n car sa matrice a pour déterminant 1. La première composante de $f(x)$ est $c = a_1(\alpha + 1) + a_2 + \sum_{j=3}^{n} a_j(\lambda b_j)$; utilisant la relation $a_1 b_1 + \sum_{j=3}^{n} a_j b_j = 1$, on obtient $c = a_1(\alpha + 1 - \lambda b_1) + \lambda + a_2$. On choisit alors $\lambda = 1 - a_2$ et $\alpha = (1 - a_2)b_1 - 1$, si bien que $c = 1$; appliquant le lemme 3.5.11., on obtient le résultat annoncé.

Montrons maintenant que le lemme 3.5.12. entraîne la proposition 3.5.10. D'après la proposition 3.5.9., il suffit de montrer qu'il existe une base de $k^n \otimes_k R$ dans laquelle le vecteur x_{11} a des composantes $(y_1, \ldots, y_n)$ telles que n-1 des y_i engendrent R en tant qu'idéal. Or, comme q représente 0, on peut, en changeant de variables, mettre q **sous la forme** $q(Y_1, \ldots, Y_n) = Y_1 Y_2 + q'(Y_3, \ldots, Y_n)$; R est la k-algèbre $k[y_1, y_2, y_3, \ldots, y_n]$ avec $y_1 y_2 + q'(y_3, \ldots, y_n) = 1$ et $x_{11} = (y_1, y_2, \ldots, y_n)$. Il est bien clair maintenant que l'idéal engendré par $y_1, y_3, \ldots, y_n$ dans R est R tout entier, d'où la proposition.

Corollaire 3.5.13. Soit k un corps de caractéristique différente de 2 et q une forme quadratique non dégénérée sur k^n. Soit $R = k[X_1, \ldots, X_n]/(q(X_1, \ldots, X_n)-1)$ et D le R-module des k-dérivations de R. Alors $D \oplus D$ est un R-module libre de rang $2(n-1)$.

En effet, du moment que $n \geq 2$, il existe une extension quadratique k' de k telle que $q \otimes k'$ représente 0. Alors $D \otimes_k k' = D \oplus D$ est un $R \otimes_k k'$-module libre de rang n-1 , d'après la proposition 3.5.10.. En tant que R-module , $D \oplus D$ est donc libre de rang $2(n-1)$. Si $n = 1$, D est réduit à 0.

Nous allons encore donner un résultat sur le fibré tangent. On suppose toujours 2 inversible dans A et soit E une A-algèbre alternative cayleyenne dont le module sousjacent est projectif de type fini et dont la norme cayleyenne N est une forme quadratique non dégénérée (cf. 3.3.). Soit alors R la A-algèbre $V_1(E,N)$.

On a :

Proposition 3.5.14. Le R-module des A-dérivations de R est isomorphe à $E_+ \otimes_A R$.

Pour cela, montrons tout d'abord le lemme suivant :

Lemme 3.5.15. Soit E une A-algèbre non nécessairement associative à élément unité e, munie d'une forme quadratique multiplicative $q : E \to A$ telle que $q(e) = 1$. Alors, pour tout élément x inversible dans E, l'orthogonal de x dans E est isomorphe, en tant que A-module, à l'orthogonal de l'élément unité e.

En effet, comme q est multiplicative, $q(x^{-1}) = (q(x))^{-1}$ et $q(x)$ est inversible dans A. De plus, $\varphi(x,y) = q(x)\,\varphi(e, x^{-1}y)$, donc l'application $y \mapsto x^{-1}y$ est un isomorphisme de l'orthogonal de x sur l'orthogonal de e.

La proposition 3.5.14. découle du lemme précédent car le R-module cherché est l'orthogonal dans $(E \otimes_A R, N \otimes R)$ de x_{11}, élément inversible, car de norme 1. Comme l'orthogonal de e dans (E,N) est le sous-module E_+, on a le résultat annoncé.

Corollaire 3.5.16. Soit k un corps de caractéristique différente de 2 et q une forme quadratique non dégénérée de rang n qui représente 1. Alors le module des dérivations de $V_1(k^n,q)$ est libre dans les deux cas suivants : (i) $n = 4$ et le discriminant de q est 1 ; (ii) $n = 8$, le discriminant de q est 1 et l'algèbre de Clifford $C(k^n,q)$ est une algèbre de matrices.

En effet, dans les deux cas on peut appliquer la proposition 3.5.14. car il existe sur k^n une structure de k-algèbre cayleyenne alternative dont la norme est q.

Supposons que (P,q) soit un A-module quadratique de rang 2. La proposition 3.5.9. dit que le A-module des dérivations de $V_1(P,q)$ est le sous-$V_1(P,q)$-module de $(P \otimes V_1(P,q), q \otimes V_1(P,q))$, orthogonal de x_{11}. Comme on l'a vu dans l'exemple 3.4.8., cet orthogonal est naturellement isomorphe à $\Lambda^2 P \otimes_A V_1(P,q)$. On a ainsi le résultat suivant :

Proposition 3.5.17. Le $V_1(P,q)$-module des A-dérivations de $V_1(P,q)$, où (P,q) est un module quadratique de rang 2, est isomorphe à $\Lambda^2 P \otimes_A V_1(P,q)$.

En particulier, si A est un corps, ce module des dérivations est toujours libre.

4. CLASSES DE STIEFEL-WHITNEY

4.1. INTRODUCTION

Dans ce chapitre, on montre comment il est possible de généraliser aux anneaux semi-locaux, la construction des invariants de Stiefel-Whitney des formes quadratiques sur un corps de caractéristique différente de 2, faite par J. Milnor dans [35]. Chronologiquement, c'est A. Delzant (cf. [16]) qui est l'initiateur de cette construction. Soit F un corps dans lequel $2 \neq 0$, $\bar{F}$ sa clôture séparable et G le groupe de Galois de $\bar{F}$ sur F. Faisant opérer G trivialement sur $\mathbb{Z}/2\,\mathbb{Z}$, on a la suite exacte de G-modules $0 \to \mathbb{Z}/2\,\mathbb{Z} \to \bar{F}^* \xrightarrow{2} \bar{F}^* \to 0$ qui donne les isomorphismes suivants, à l'aide de la suite exacte longue de cohomologie :

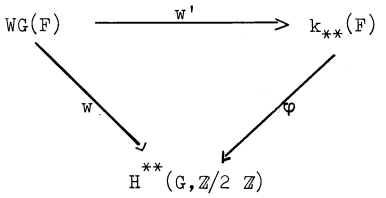
$$H^1(G,\ \mathbb{Z}/2\,\mathbb{Z}) \approx F^*/F^{*2}$$

$$H^2(G,\ \mathbb{Z}/2\,\mathbb{Z}) \approx Br_2(F)\ .$$

Ceci dit, considérons l'anneau de cohomologie $H^*(G,\mathbb{Z}/2\,\mathbb{Z})$ et soit $\tilde{H}(G,\mathbb{Z}/2\,\mathbb{Z})$ l'anneau $\prod_{i=0}^{\infty} H^i(G,\mathbb{Z}/2\,\mathbb{Z})$ dont on notera $H^{**}(G,\mathbb{Z}/2\,\mathbb{Z})$ le groupe des éléments inversibles : ce sont des éléments qui s'écrivent $1 + \sum_{i=1}^{\infty} h_i$, $h_i \in H^i(G,\mathbb{Z}/2\,\mathbb{Z})$ et qui se multiplient à l'aide du cup-produit. L'<u>invariant de Stiefel-Whitney</u> d'une forme quadratique est défini à l'aide d'un homomorphisme de groupes abéliens $w : WG(F) \to H^{**}(G,\mathbb{Z}/2\,\mathbb{Z})$ donné sur les formes de rang 1 par $w(< a >) = 1 + \bar{a}$, $\bar{a} \in H^1(G,\mathbb{Z}/2\,\mathbb{Z}) \approx F^*/F^{*2}$. Si η est un élément de $WG(F)$, on écrit $w(\eta) = 1 + \sum_{i=1}^{\infty} w_i(\eta)$ et $w_i(\eta)$ est appelée la $i^{\text{ème}}$ <u>classe de Stiefel-Whitney</u> de η. La première classe est liée au discriminant et la seconde à l'algèbre de Clifford. W. Scharlau a étudié systématiquement cette construction dans [47] et, en particulier, le problème de l'injectivité de w qui avait été résolu par A. Delzant dans le cas des corps de nombres algébriques (cf. [16]).

En 1970, J. Milnor s'est intéressé à la question dans le cadre de la K-théorie algébrique (définition de $K_n(F)$ pour un corps F, $n \geq 2$) dans [35] et a posé les notations suivantes : soit $k_*(F) = S_{\mathbb{Z}/2\,\mathbb{Z}}(F^*/F^{*2})/I = \bigoplus_{n \in \mathbb{N}} k_n(F)$ où I est l'idéal de $S_{\mathbb{Z}/2\,\mathbb{Z}}(F^*/F^{*2})$ engendré par les éléments de la forme $\bar{x}.\overline{1-x}$, $x \in F - \{0,1\}$. Soit alors $k_\pi(F)$ l'anneau produit $\prod_{n \in \mathbb{N}} k_n(F)$ et $k_{**}(F)$ le groupe des éléments inversibles de $k_\pi(F)$. Il est facile de voir maintenant que, comme $\bar{a} \cup (\overline{1-a}) = 0$ dans $H^2(G,\mathbb{Z}/2\,\mathbb{Z})$ (cf. [50], ch. XIV, Prop. 4), il existe

un homomorphisme naturel d'anneaux de $k_*(F)$ dans $H^*(G,\mathbb{Z}/2\ \mathbb{Z})$, qui induit un homomorphisme φ de $k_{**}(F)$ dans $H^{**}(G,\mathbb{Z}/2\ \mathbb{Z})$. J. Milnor définit alors (cf. [35], lemme 3.1.) un homomorphisme de groupes abéliens que nous noterons $w' : WG(F) \to k_{**}(F)$ de sorte que le triangle



est commutatif, en posant $w'(< a >) = 1 + \bar{a}$ et c'est l'homomorphisme w' qui devient alors la base de la construction des invariants de Stiefel-Whitney.

Notre but est de construire des remplaçants pour $k_*(F)$ et $k_{**}(F)$ dans le cas des anneaux semi-locaux, en nous inspirant d'une construction analogue pour les anneaux locaux faite par E. Hornix dans [24]. Nous aurons tout d'abord besoin de certaines propriétés des formes quadratiques sur les anneaux semi-locaux, puis nous donnerons l'anneau qui jouera le rôle de $k_*(F)$ et nous justifierons ce choix à l'aide de résultats techniques simples.

4.2. MODULES QUADRATIQUES SUR LES ANNEAUX SEMI-LOCAUX

Nous nous restreignons pour toute la suite au cas des anneaux semi-locaux indécomposables, ce que nous omettrons de préciser ; les énoncés et démonstrations sont plus simples et le lecteur pourra sans difficultés retrouver le cas général. Dans notre cas les modules projectifs de type fini sont de rang constant, donc libres. Une généralisation facile des résultats de 1.11., dans le cas local est donnée par la proposition suivante :

Proposition 4.2.1. Tout module quadratique sur un anneau semi-local A est somme orthogonale de modules quadratiques de rang 1, i.e., possède une base orthogonale, si 2 est inversible dans A et de rang 2 dans le cas contraire.

Pour pouvoir définir des invariants de Stiefel-Whitney, il est nécessaire de posséder un analogue de Satz 7 de Witt qui a été établi pour les anneaux locaux dans 1.14. Une démonstration analogue peut se faire dans le cas semi-local, ce qui donne le résultat suivant :

Proposition 4.2.2. (i) Si 2 est inversible dans A, deux bases orthogonales d'un module quadratique sont équivalentes. (ii) Si 2 n'est pas inversible dans A, deux décompositions d'un module quadratique en somme orthogonale de modules de rang 2 sont équivalentes.

A partir de cette proposition on a des corollaires immédiats :

Corollaire 4.2.3. (i) Si 2 est inversible dans A, l'anneau de Witt-Grothendieck de A est isomorphe au quotient de l'anneau de groupe $\mathbb{Z}[U(A)/U^2(A)]$ par l'idéal engendré par les éléments $(\bar{a}+\bar{b}) - (\bar{c}+\bar{d})$, où a, b, c, d parcourent $U(A)$ et où les formes quadratiques $< a > \perp < b >$ et $< c > \perp < d >$ sont isomorphes. (ii) Si 2 n'est pas inversible dans A, soit $E(A)$ l'ensemble des classes d'isomorphismes de modules quadratiques de rang 2. Le groupe $WG(A)$ est le quotient du groupe libre $\mathbb{Z}^{(E(A))}$ par le sous-groupe engendré par les éléments $([P_1] + [P_2]) - ([P_3] + [P_4])$ où $P_i \in E(A)$ et $P_1 \perp P_2 \simeq P_3 \perp P_4$.

La démonstration de la proposition 4.2.2. utilise le fait que $A/\mathrm{Rad}\, A$ est un produit fini de corps et comme on sait remonter des bases orthogonales ou plus généralement des décompositions orthogonales de $A/\mathrm{Rad}\, A$ à A, on se ramène au cas où les décompositions orthogonales considérées coïncident modulo le radical. La démonstration est alors calquée sur celle du cas local (cf. 1.14.). On peut rajouter à la proposition précédente la précision suivante, qui nous servira par la suite : deux décompositions orthogonales sont équivalentes par une suite de transformations admissibles du type $P_i \perp P_j \simeq P'_i \perp P'_j$ où $P_i \cap P'_i = Ax$ et où x est unimodulaire, ou encore, Ax est facteur direct dans P_i et dans P'_i.

Pour poursuivre, nous avons besoin d'étudier de plus près les formes quadratiques de rang 2. On a alors le lemme suivant :

Lemme 4.2.4. Soit (P,q) un A-module quadratique de rang 2. (i) Il existe $x \in P$ tel que $q(x) \in U(A)$; (ii) il existe $y \in P$ tel que $\varphi(x,y) = 1$, $P = Ax \oplus Ay$ et $q(y) \notin \mathfrak{m}$, pour tout idéal maximal $\mathfrak{m}$ de A tel que $\mathrm{Card}\,(A/\mathfrak{m}) \geq 4$.

Par réduction modulo le radical de A, on se ramène au cas où A est un corps. Si A diffère de $\mathbb{Z}/2\,\mathbb{Z}$ et $\mathbb{Z}/3\,\mathbb{Z}$, il existe toujours une base $\{x,y\}$ de P avec $q(x)\,q(y)\,\varphi(x,y)$ non nul. Si $A = \mathbb{Z}/2\,\mathbb{Z}$, il n'y a que deux formes quadratiques à isomorphisme près, à savoir, $q(ae_1 + be_2) = ab$ et $q(ae_1 + be_2) = a^2 + ab + b^2$. Pour la seconde, toute base convient et pour la première il existe un seul vecteur x tel que $q(x) \neq 0$, d'où la restriction $A/\mathfrak{m} \neq \mathbb{Z}/2\,\mathbb{Z}$. Si $A/\mathfrak{m} = \mathbb{Z}/3\,\mathbb{Z}$ et si q est hyperbolique, il n'y a que deux droites portant des vecteurs non isotropes et elles sont orthogonales, d'où la seconde restriction, $A/\mathfrak{m} \neq \mathbb{Z}/3\,\mathbb{Z}$.

Cela signifie que si $q : A^2 \to A$ est une forme quadratique non dégénérée, il existe une base $\{e_1, e_2\}$ telle que $q(xe_1 + ye_2) = ax^2 + xy + by^2$ avec a inversible dans A et b n'est dans aucun des idéaux maximaux $\mathfrak{m}$ de A tels que $\mathrm{Card}(A/\mathfrak{m}) > 3$. On a donc $q(xe_1 + ye_2) = a(x^2 + x.ya^{-1} + ab(ya^{-1})^2)$ et comme q est non dégénérée, $1 - 4\,ab = \varphi(e_1, e_2)^2 - 4\,q(e_1)\,q(e_2)$ est inversible. Cela signifie qu'en prenant pour base de A^2, e_1 et $a\,e_2$, $q(xe_1 + y(ae_2)) = a(x^2 + xy + ab\,y^2)$. Considérons maintenant la A-algèbre $B = A[t]$ avec $t^2 - t + ab = 0$. Il est clair que B est une extension quadratique(séparable) de A (cf. 2.4.) et que $q(xe_1 + y(ae_2)) = a\,N_{B/A}(x\,1_B + y\,t)$. Inversement soit B une extension quadratique de A. A a, élément inversible de A et à B, on associe naturellement une forme quadratique non dégénérée q sur A^2 en posant sur B, $q(z) = a\,N_{B/A}(z)$. On a donc une surjection de l'ensemble $U(A) \times \mathfrak{D}(A)$ sur l'ensemble E(A) des classes d'isomorphismes de modules quadratiques de rang 2. Il est facile d'établir sous quelles conditions deux couples (a,B) et (a',B') ont même image dans E(A). En effet, on a l'isomorphisme de A-algèbres $C_o(B, a\,N_{B/A}) \simeq B$ et donc il est nécessaire que $B = B'$ dans $\mathfrak{D}(A)$. Ensuite, pour que $a\,N_{B/A} \simeq a'\,N_{B/A}$ il est nécessaire et suffisant que a et a' appartiennent à la même classe dans le groupe $U(A)/N_{B/A}(U(B))$ où $N_{B/A}(U(B))$ est le sous-groupe de U(A), image de U(B) par l'homomorphisme $N_{B/A}$.

Ceci nous amène à chercher le groupe $\mathfrak{D}(A)$ des extensions quadratiques de l'anneau semi-local A, comme l'a montrée la discussion précédente. Rappelons, tout d'abord, le lemme suivant (cf. [6]) :

Lemme 4.2.5. Soient A un anneau semi-local, $a \in A$ et I un idéal de A tel que $aA + I = A$. Il existe alors $v \in I$ tel que $a + v \in U(A)$.

Lemme 4.2.6. Le groupe $\mathfrak{D}(A)$ des extensions quadratiques de A est isomorphe au groupe G(A) défini en 2.4.

En effet, une extension quadratique B de A est un A-module projectif de type fini et de rang 2, donc $B = A[t]$ avec $t^2 - bt + c = 0$ et $b^2 - 4c \in U(A)$.

En appliquant le lemme 4.2.5. à b et à l'idéal $I = 2A$, on obtient h dans A tel que $b + 2h \in U(A)$. Considérons alors $z = (t+h)(b+2h)^{-1}$ et $B = A[z]$ avec $z^2 - z + d = 0$. Ceci nous montre que l'homomorphisme de groupes abéliens $\varphi : A(4) \to \mathfrak{D}(A)$ défini par $\varphi(a) = A[z]$ avec $z^2 - z + a = 0$ est surjectif. On vérifie alors comme dans 2.4.2. que cet homomorphisme a pour noyau l'image de A(2) dans A(4) par l'application naturelle $x \mapsto x - x^2$.

Ceci nous permet de remplacer l'application considérée plus haut de $U(A) \times \mathfrak{D}(A)$ dans E(A) par une application de $U(A) \times A(4)$ dans E(A). Comme

il y a une certaine indétermination sur l'élément dont on a besoin dans $A(4)$, il est possible de chercher à quelle condition un tel élément peut être pris dans $U(A)$. On a alors le lemme :

Lemme 4.2.7. *Si* $a \in A(4)$, *il existe* $b \in U(A) \cap A(4)$ *tel que* a *et* b *ont même image dans* $G(A) = \mathfrak{D}(A)$ *si et seulement si* a *n'est dans aucun des idéaux maximaux* $\mathfrak{m}$ *de* A *tels que* $\mathrm{Card}(A/\mathfrak{m}) \leq 3$.

En effet, dire que a et b ont même image dans $G(A)$ signifie qu'il existe $c \in A(2)$ tel que $b = a + (c - c^2)(1 - 4a)$. On se ramène en faisant le quotient modulo le radical de A au cas où A est un corps et il faut alors montrer qu'il existe $c \in A(2)$ tel que $a + (c-c^2)(1-4a) \neq 0$. Si $a = 0$, il existe toujours un élément c tel que $1-2c \neq 0$ et $c-c^2 \neq 0$ à condition que $\mathrm{Card}(A) > 3$.

Notons que l'application surjective de $U(A) \times \mathfrak{D}(A)$ dans $E(A)$ induit une application de $U(A) \times \mathfrak{D}(A)$ dans le sous-groupe $\mathrm{Br}_2(A)$ des éléments d'ordre 2 du groupe de Brauer de A en associant à (a,B) la classe de l'algèbre des quaternions $C(a\, N_{B/A})$. De plus, cette application est biadditive (cf. 2.8.). Remarquons que l'on peut dans cette discussion remplacer $U(A)$ par le groupe quotient $U(A)/U^2(A)$ car $(B, a\, N_{B/A}) \approx (B, ab^2\, N_{B/A})$ quel que soit b inversible dans A. Nous noterons alors $[\bar{a}, B]$ pour $a \in U(A)$, $B \in \mathfrak{D}(A)$, la classe de l'algèbre $C(a\, N_{B/A})$ dans $\mathrm{Br}_2(A)$. On a l'homomorphisme de groupes abéliens de $(U(A)/U^2(A)) \otimes_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathfrak{D}(A)$ dans $\mathrm{Br}_2(A)$. Si A est un corps, on obtient des symboles locaux (cf. [50], Ch. XIV, § 2 et § 5). Supposons que $a \in U(A) \cap A(4)$. On note a^0 l'image de a élément de $A(4)$ dans $G(A) = \mathfrak{D}(A)$, c'est à dire, la A-algèbre $B = A[t]$ avec $t^2 - t + a = 0$. On a alors le résultat suivant : $[\bar{a}, a^0) = 0$ dans $\mathrm{Br}_2(A)$ car $a\, N_{B/A} \approx N_{B/A}$ et la classe de $C(N_{B/A})$ dans $\mathrm{Br}_2(A)$ est nulle.

4.3. INVARIANTS DE STIEFEL-WHITNEY D'UN PLAN

Nous nous intéressons, comme au paragraphe 4.2., aux applications biadditives f de $U(A)/U^2(A) \times \mathfrak{D}(A)$ dans un groupe abélien G telles que $f(\bar{a}, a^0) = 0$ pour tout a dans $U(A) \cap A(4)$. On désigne par $h_2(A)$ le groupe universel défini par les couples (G,f) : c'est le quotient de $(U(A)/U^2(A)) \otimes_{\mathbb{Z}} \mathfrak{D}(A)$ par le sous-groupe engendré par les éléments $\bar{a} \otimes a^0$ où a décrit $U(A) \cap A(4)$. Si 2 est inversible dans A, l'homomorphisme $t : \mathfrak{D}(A) = G(A) \to U(A)/U^2(A)$ défini par $t(a^0) = \overline{1-4a}$ est un isomorphisme et $h_2(A)$ est isomorphe au quotient de $(U(A)/U^2(A)) \otimes_{\mathbb{Z}} (U(A)/U^2(A))$ par le sous-groupe engendré par les éléments $\bar{a} \otimes \overline{1-4a} = \bar{x} \otimes \overline{1-x}$ avec $x = 4a$ et $x(1-x) \in U(A)$. On retrouve ainsi, quand A est un corps de caractéristique différente de 2, le k_2 introduit par J. Milnor (cf. [35]).

Nous allons déduire de la relation (1) : $f(\bar{a},a^0) = 0$ quelques conséquences. L'inverse de a dans $A(4)$ étant $a' = -a(1-4a)^{-1}$, on a $f(-a(1-4a)^{-1},a^0)=0$ soit, (2) : $f(\overline{1-4a}, a^0) = f(-\bar{1},a^0)$. Soient maintenant a et b dans $U(A) \cap A(4)$ et supposons qu'il existe c dans $U(A) \cap A(4)$ tel que $c^0 = a^0 * b^0$ (on note * la loi de composition dans $\mathfrak{D}(A)$). On a, du fait de (2), $f(\overline{-(1-4aob)},c^0) = 0$ soit, en utilisant la biadditivité de f et la relation (1), (3) : $f(\overline{1-4a},b^0) = f(\overline{1-4b}, a^0)$. Supposons, par exemple, tous les corps résiduels $A/\mathfrak{m}$ distincts de $\mathbb{Z}/2\,\mathbb{Z}$ et de $\mathbb{Z}/3\,\mathbb{Z}$. Le lemme 4.2.7. nous dit que tout élément de $\mathfrak{D}(A)$ est de la forme a^0 où $a \in U(A) \cap A(4)$. En notant encore t l'application naturelle de $\mathfrak{D}(A)$ dans $U(A)/U^2(A)$, la relation (3) s'écrit : (3') : $f(t(B),B') = f(t(B'),B)$ pour tout couple (B,B') d'éléments de $\mathfrak{D}(A)$. Remarquons que les relations (2) et (3) n'entraînent pas en général (1). En effet, si $2 = 0$ dans A, t est l'homomorphisme nul et les relations (2), (3) et (3') sont trivialement vérifiées.

Pour définir les invariants de Stiefel-Whitney d'un module quadratique, nous considérons un quotient $g_*(A)$ de l'algèbre symétrique $S_{\mathbb{Z}/2\,\mathbb{Z}}((U(A)/U^2(A)) \oplus \mathfrak{D}(A))$ par un idéal homogène I dont nous préciserons un système de générateurs au fur et à mesure. Comme I est homogène, $g_*(A)$ sera gradué sur $\mathbb{N}$: $g_*(A) = \bigoplus_{n \in \mathbb{N}} g_n(A)$ et on pose $g_\pi(A) = \prod_{n=0}^{\infty} g_n(A)$ le complété de l'anneau $g_*(A)$ pour la filtration associée à cette graduation. L'invariant de Stiefel-Whitney sera la donnée d'un homomorphisme de groupes abéliens $w : WG(A) \to U(g_\pi(A))$, groupe des éléments inversibles de $g_\pi(A)$, qui s'écrira $w(P,q) = 1 + \sum_{i=1}^{\infty} w_i(P,q)$. Du fait des résultats du paragraphe 4.2., il suffira de définir l'image par w des modules quadratiques de rangs 1 et 2 et de vérifier, en prolongeant la définition de w à $WG(A)$ tout entier par additivité, que ce prolongement ne dépend pas de la décomposition orthogonale choisie. D'après 4.2.2., il suffira d'étudier les modules quadratiques de rang 4 si 2 n'est pas inversible et ceux de rang 2 dans le cas contraire.

Si 2 est inversible dans A, pour tout $a \in U(A)$, on définit la classe de $q_a : A \to A$, $x \mapsto ax^2$, comme étant $w(q_a) = 1 + t^{-1}(\ddot{a})$ où t^{-1} est l'isomorphisme réciproque de $t : \mathfrak{D}(A) \to U(A)/U^2(A)$ et $t^{-1}(\bar{a})$ est la classe dans $\mathfrak{D}(A)$ de l'algèbre de Clifford de la forme quadratique q_a. En rang 2, on a $w(q_a \perp q_b) = (1 + t^{-1}(\bar{a}))(1 + t^{-1}(b)) = 1 + t^{-1}(\overline{ab}) + t^{-1}(\bar{a}).t^{-1}(\bar{b})$ et nous verrons plus loin, en regardant directement (i.e. sans hypothèse sur 2) le cas des modules quadratiques de rang 2, que $w(q_a \perp q_b)$ ne dépend pas de la base orthogonale choisie.

On suppose maintenant que tous les corps résiduels $A/\mathfrak{m}$ ont plus de trois

éléments et on ne fait aucune hypothèse sur l'inversibilité de 2 dans A. Soit (A^2,q) un module quadratique de rang 2 et $\{e_1,e_2\}$ une base dans laquelle q s'écrit $q(xe_1 + ye_2) = ax^2 + xy + by^2 = a\, N_{B/A}(x.1 + a^{-1}y\, t)$ avec $a,b \in U(A)$, $ab \in A(4)$ et B est l'extension quadratique $(ab)^\circ$ (on sait, d'après le paragraphe 4.2., qu'une telle base existe toujours). On pose alors $w(A^2,q)) = 1 + \overline{-1} + (ab)^\circ + \bar{a}.(ab)^\circ$.

Il est nécessaire de vérifier que cette définition coïncide avec celle donnée dans le cas où 2 est inversible et il faudra ensuite montrer que $w((A^2,q))$ ne dépend que de q.

Pour cela, nous allons commencer à imposer des relations dans $g_*(A)$, la première étant : (1) $\bar{a}\ .\ a^\circ = 0$ pour tout a dans $U(A) \cap A(4)$. Comme on l'a vu au début de ce paragraphe, cela implique les relations (2) : $\overline{1-4a}.a^\circ = \overline{-1}.a^\circ$ et (3) : $\overline{1-4a}.b^\circ = \overline{1-4b}.a^\circ$. De plus, si 2 est inversible dans A, nous imposons la relation (4) : $\overline{-1} = t^{-1}(\overline{-1})$, c'est à dire que nous identifions $\overline{-1} \in U(A)/U^2(A)$ avec la classe dans $\mathfrak{D}(A)$ de l'algèbre $B = A[i]$ avec $i^2 + 1 = 0$. Ainsi, si 2 est inversible dans A, $\overline{-1} + (ab)^\circ$ est la classe dans $\mathfrak{D}(A)$ de $A[z]$ avec $z^2 + (1-4ab) = 0$; si $q(xe'_1 + ye'_2) = a'x^2 + b'y^2$ où $\{e'_1, e'_2\}$ est une base orthogonale pour q, le terme de degré 1 de w(q) donné plus haut est $t^{-1}(\overline{a'b'})$. Le calcul du discriminant de q, suivant les deux bases $\{e_1,e_2\}$ et $\{e'_1,e'_2\}$, donne $\overline{a'b'} = \overline{-(1-4ab)}$, soit l'égalité $\overline{-1} + (ab)^\circ = t^{-1}(a'b')$ d'où la cohérence pour le premier terme $w_1(q)$.

Il faut maintenant comparer les seconds invariants $t^{-1}(\bar{a}').t^{-1}(\bar{b}')$ et $\bar{a}.(ab)^\circ$. Pour montrer qu'ils sont égaux, nous sommes amenés à imposer dans $g_*(A)$ la relation (5) : $B.B' = t(B).B' = t(B').B$ pour tout couple (B,B') d'éléments de $\mathfrak{D}(A)$. Avec les notations précédentes $t^{-1}(\bar{a}')\ t^{-1}(\bar{b}') = \bar{a}'.t^{-1}(\bar{b}') = \bar{a}'.t^{-1}(\overline{-a'b'}) = \bar{a}'.(ab)^\circ$. Il s'agit donc de montrer que $\bar{a}.(ab)^\circ = \bar{a}'(ab)^\circ$; comme q est proportionnel à $N_{B/A}$ pour B extension quadratique de A, $a' = a\, N_{B/A}(z)$ avec $z \in U(B)$ et il suffit de montrer que $\overline{N_{B/A}(z)}.B = 0$ dans $g_*(A)$ ce que nous ferons plus loin.

Remarques. (i) Les relations (2) et (5) donnent dans $g_*(A)$ la relation (5') : $B.B = t(B).B = \overline{-1}.B$ pour tout élément B de $\mathfrak{D}(A)$. (ii) La relation (5) a une justification algébrique simple : le second invariant $w_2(q)$ est lié à l'algèbre de Clifford et ce que l'on souhaite obtenir en faisant le produit de deux extensions quadratiques dans $g_*(A)$ c'est la classe de l'algèbre de Clifford $C((B,N_B) \perp \perp (B',N_{B'}))$. On doit avoir la formule $w_2((P,q) \perp (P',q')) = w_2((P,q)) + w_2((P',q')) + w_1((P,q))\, w_1((P',q'))$ et on sait que dans $Br_2(A)$, $C((P,q) \perp (P',q')) = C(P,q) + C(P',q') + C((B,N_B) \perp (B',N'_B))$. Ainsi on a $C((B,N_B) \perp (B',N_{B'})) = C(B,t(B')N_B) =$

$= C(B', t(B)N_{B'})$ (cf. suite au théorème 2.8.12.), ce qui explique la relation (5). Notons que l'homomorphisme $\mathfrak{D}(A) \otimes_{\mathbb{Z}} \mathfrak{D}(A) \to Br_2(A)$, induit par l'application $B \times B' \mapsto C((B,N_B) \perp (B',N_{B'}))$, se factorise de deux façons différentes par l'homomorphisme de groupes abéliens : $(U(A)/U^2(A)) \otimes_{\mathbb{Z}} \mathfrak{D}(A) \xrightarrow{f} Br_2(A)$, $\bar{a} \otimes B \mapsto [\bar{a},B)$. Nous avons alors le carré commutatif :

$$\begin{array}{ccc} \mathfrak{D}(A) \otimes_{\mathbb{Z}} \mathfrak{D}(A) & \xrightarrow{t \otimes id_{\mathfrak{D}(A)}} & (U(A)/U^2(A)) \otimes_{\mathbb{Z}} \mathfrak{D}(A) \\ \downarrow{\scriptstyle id_{\mathfrak{D}(A)} \otimes t} & & \downarrow{\scriptstyle f} \\ \mathfrak{D}(A) \otimes_{\mathbb{Z}} (U(A)/U^2(A)) & \xrightarrow{f} & Br_2(A) \end{array}$$

Il nous reste à montrer maintenant que $\overline{N_{B/A}(z)}.B = 0$ dans $g_*(A)$ si $z \in U(B)$. Notons que cela montrera du même coup que la définition donnée plus haut pour $w(q)$ ne dépend pas de la base $\{e_1,e_2\}$ choisie.

En effet, changer de vecteur e_1 revient à remplacer a par $\alpha \in U(A)$ tel que $a\, N_B \simeq \alpha\, N_B$, c'est à dire, $\alpha = a\, N_B(z)$ et $\bar{\alpha}\, B = \bar{a}\, B + \overline{N_B(z)}.B$ où $z \in U(B)$. Nous avons alors le lemme suivant :

Lemme 4.3.1. *Si tous les corps résiduels* $A/\mathfrak{m}$ *sont dfférents de* $\mathbb{Z}/2\,\mathbb{Z}$, $\mathbb{Z}/3\,\mathbb{Z}$, *et* $\mathbb{Z}/5\,\mathbb{Z}$, *alors pour tout élément* B *de* $\mathfrak{D}(A)$ *et pour tout* z *inversible dans* B, *on a* $\overline{N_{B/A}(z)}.B = 0$ *dans* $g_*(A)$.

Supposons d'abord $Tr_{B/A}(z)$ inversible et $B = A[z]$. Si $y = z(Tr_{B/A}(z))^{-1}$, $B = A[y]$ avec $y^2 - y + d = 0$ et $d = Tr_{B/A}(z)^{-2}N_{B/A}(z)$ est inversible. On a donc $\overline{N_{B/A}(z)}.B = \bar{d}.N = 0$ car $B = d^0$.

Dans le cas général, soit $B = A[x]$ avec $x^2 - x + a = 0$, $a \in U(A) \cap A(4)$ et $z = \alpha + \beta x$ tel que $N_{B/A}(z) = \alpha^2 + \alpha\beta + a\beta^2$ est inversible. Soient h dans $A(2)$ et y dans B tels que $x = (1 - 2h)y + h$; alors $B = A[y]$ avec $y^2 - y + (a-h+h^2)(1-2h)^2 = 0$. Posant $d = N_{B/A}(y)$, on a $\bar{d}.B = 0$ d'après le cas précédent si $a-h+h^2 \in U(A)$ et donc $\overline{N_{B/A}(z)}.B = \overline{N_{B/A}(yz)}.B$.

On va montrer que, dans les conditions du lemme, il existe h tel que $B = A[yz]$ avec $Tr(yz) \in U(A)$ et $a-h+h^2 \in U(A)$: appliquant à nouveau le premier cas, on en déduira le lemme. Or, $yz = (\alpha + \beta(1-h))y - d\,\beta(1-2h)$ et $Tr(yz) = \alpha + \beta(1-h) - 2d\,\beta(1-2h)$. L'élément h cherché doit donc satisfaire aux conditions

suivantes : (i) $1-2h \in U(A)$; (ii) $a-h+h^2 \in U(A)$; (iii) $\alpha + \beta(1-h) \in U(A)$; (iv) $\alpha + \beta(1-h) - 2d\beta(1-2h) \in U(A)$ avec $d = (a-h+h^2)(1-2h)^{-2}$ et $\alpha,\beta \in A$ tel que $\alpha^2 + \alpha\beta + a\beta^2 \in U(A)$. Pour trouver h dans A, il suffit de le trouver dans chaque corps résiduel. Supposons donc que A est un corps de caractéristique 2 : (iii) et (iv) sont les mêmes et (i) est automatiquement vérifiée. Pour (ii), il suffit de prendre $h = 0$ ou 1 et il est clair que l'une des deux valeurs convient pour (iii) car on ne peut avoir à la fois $\alpha+\beta$ et α nuls. En caractéristique différente de 2, la condition (ii) exclut deux valeurs de h ; les autres conditions en excluent une. Il suffit donc que le corps considéré ait plus de cinq éléments, d'où la restriction signalée dans le lemme.

Remarques. (i) La réciproque de ce lemme est claire : soit $a \in U(A)$ tel que $\bar{a}.B = 0$. Du fait de l'homomorphisme de $(U(A)/U^2(A)) \otimes_{\mathbb{Z}} \mathfrak{D}(A)$ dans le groupe de Brauer de A, $C(a\, N_{B/A}) = 0$ dans $Br_2(A)$. Ainsi, les formes quadratiques $a\, N_{B/A}$ et $N_{B/A}$ ont même discriminant et même algèbre de Clifford et sont donc isométriques. Il en résulte que $a = N_{B/A}(z)$ pour un $z \in U(B)$.

(ii) Nous venons de voir que l'invariant de Stiefel-Whitney d'un espace quadratique de rang 2 est bien défini. La suite de la proposition 2.7.3. nous dit alors que si $w(Q) = w(Q')$, Q et Q' sont isométriques.

4.4. L'INVARIANT DE STIEFEL-WHITNEY POUR UN ESPACE QUELCONQUE

Dans le paragraphe précédent, nous avons défini $w(P,q)$ pour tout A-module quadratique (P,q) de rang inférieur ou égal à 2 ; en vertu de 4.2.2., c'est suffisant si 2 est inversible dans A. Dans le cas général, il est nécessaire de montrer que si $(P,q) = (P_1,q_1) \perp (P_2,q_2) = (P_1',q_1') \perp (P_2',q_2')$ est un A-module quadratique de rang 4, $w(P_1,q_1)\, w(P_2,q_2) = w(P_1',q_1')w(P_2',q_2')$ et ainsi $w(P,q)$ sera défini sans ambiguité. On sait que l'on peut toujours se ramener au cas où $P_1 \cap P_1' = Ax$ où x est unimodulaire et $q(x)$ inversible dans A. Soit alors $\{e_i,f_i\}$ (resp. $\{e_j',f_j'\}$ une base de P_i (resp. P_j') fournie par le lemme 4.2.4. On suppose, vu ce qui précède, que $e_1' = e_1$ et on a alors $f_1' = f_1 + a(e_1 - 2q(e_1)\, f_1) + p_2$ avec $p_2 \in P_2$. Supposons tout d'abord que $q(p_2)$ soit inversible dans A. On peut alors choisir $p_2 = e_2$ et $e_2 - 2q(e_2)f_2$ peut être pris comme e_2' car il est bien orthogonal à $e_1 = e_1'$ et à f_1' et, de plus, $q(e_2') = q(e_2)(1-4q(e_2)q(f_2)) \in U(A)$. Posons $\delta_i = (q(e_i)q(f_i))^{\circ}$ et $\delta_j' = (q(e_j')q(f_j'))^{\circ} \in G(A) = \mathfrak{D}(A)$ et soit β définie par $\delta_1' = \delta_1 \circ \beta$ (et $\delta_2' = \delta_2 \circ \beta$ car $\delta_1 \circ \delta_2 = \delta_1' \circ \delta_2'$). On trouve $\beta = ((1-4\delta_1)^{-1}\, q(e_1)q(e_2) + aq(e_1) - a^2q(e_1)^2)^{\circ}$ et on a $w(P_1,q_1) = 1 + \overline{-1} + \delta_1 + \overline{q(e_1)}\delta_1$, $w(P_2,q_2) = 1 + \overline{-1} + \delta_2 + \overline{q(e_2)}\delta_1$, $w(P_1',q_1') =$

$= 1 + \overline{-1} + \delta_1 \circ \beta + \overline{q(e_1)}(\delta_1 \circ \beta)$ et $w(P_2',q_2') = 1 + \overline{-1} + \delta_2 \circ \beta + \overline{q(e_2')}(\delta_2 \circ \beta)$.

Calculons $w(P_1,q_1)\, w(P_2,q_2) - w(P_1',q_1')\, w(P_2',q_2')$ dans $g_*(A)$. Comme il s'agit d'un anneau gradué, on regarde enchaque degré, ici 2, 3, ou 4. Remarquons que $\overline{q(e_2)}\delta_2 = \overline{q(e_2')}\delta_2$ et en degré 2 on a $\beta(\delta_1 \circ \delta_2 \circ \beta + \overline{q(e_1)q(e_2')})$ soit en utilisant la formule (5), $\beta\overline{(1-4\delta_1)q(e_1)q(e_2)}$. Or β n'est autre que l'extension quadratique $B = A[z]$ avec $z^2 - z + \beta = 0$ et pour montrer que $\beta.\bar{u} = 0$, il suffit de voir que $u = N_{B/A}(v)$, $v \in A[z]$. Or, $N_{B/A}(b+cz) = b^2 + bc + \beta c^2$ et on a donc à résoudre $b^2 + bc + c^2\beta = (1-4\delta_1)q(e_1)q(e_2)$ dont une solution est donnée par $b = -(1-4\delta_1)\, aq(e_1)$ et $c = 1-4\delta_1$. En degré 3, on a $\beta(\delta_1 \circ \delta_2 \circ \beta + \overline{-1})\overline{q(e_1)q(e_2')}$. Du fait de la nullité du terme de degré 2, ceci est égal à $\beta(\delta_1 \circ \delta_2 \circ \beta + \overline{-1})\delta_1 \circ \delta_2 \circ \beta$ ce qui fait 0 d'après la formule (5'). En degré 4, on trouve $\beta(\delta_1 \circ \delta_2 \circ \beta)\, \overline{q(e_1)}\, \overline{q(e_2')}$ soit $\beta\, \overline{q(e_1)}\, \overline{q(e_2')}\, \overline{q(e_1)q(e_2')}$. Pour que ce terme s'annule, nous imposons une nouvelle relation (6) : $(\bar{a})^2 = \overline{-1}\, \bar{a}$ pour tout $a \in U(A)$. Ceci donne, en particulier, $(\bar{a}^2)\bar{b} = \bar{a}\,(\bar{b}^2)$ pour a et b parcourant $U(A)$ et montre que le terme de degré 4 est nul.

Pour montrer que l'on peut toujours supposer $q(p_2)$ inversible, nous allons démontrer le lemme suivant, avec les notations introduites ci-dessus :

Lemme 4.4.1. Il existe $x = x_1 + x_2$, $x_i \in P_i$ $(i = 1,2)$ vérifiant les conditions : (i) $q(x_2 + p_2) \in U(A)$; (ii) le sous-module P_1'' engendré par e_1 et $f_1 + p_2 + x_1 + x_2$ est non dégénéré et $\varphi(e_1,x_1) = 0$; (iii) $y = x - a(e_1 - 2q(e_1)f_1) \in P_2'$; (iv) $q(y) \in U(A)$.

En admettant ce lemme, (P,q) s'écrit $(P_1'',q_1'') \perp (P_2'',q_2'')$. Les résultats ci-dessus s'appliquent aux couples de décompositions orthogonales de (P,q), $(P_1,q_1) \perp (P_2,q_2)$ et $(P_1'',q_1'') \perp (P_2'',q_2'')$, $(P_1',q_1') \perp (P_2',q_2')$ et $(P_1'',q_1'') \perp (P_2'',q_2'')$ car $q(x_2 + p_2) \in U(A)$, $q(y) \in U(A)$ et $f_1'' = (f_1 + x_1) + (x_2 + p_2) = f_1' + y$. On a donc $w(P_1,q_1)\, w(P_2,q_2) = w(P_1',q_1')\, w(P_2',q_2')$; reste à démontrer le lemme. La condition (ii) donne $x_1 = e_1 - 2q(e_1)f_1$ et $1-4q(e_1)q(f_1 + x_1 + x_2 + p_2) \in U(A)$. Pour (iii), y étant toujours orthogonal à $e_1 = e_1'$, on a la seule condition $\varphi(y, f_1') = 0$, soit $\varphi(x_2,p_2) + (\alpha-a)(1-4\delta_1)(1-2aq(e_1)) = 0$. Pour trouver x, on est, comme on l'a déjà vu, ramené au cas où A est un corps. Si A est de caractéristique 2, (P_1'',q_1'') est toujours nondégénérée, $x_1 = \alpha\, e_1$ et on a alors le système des trois relations :

(1) $\varphi(x_2,p_2) = a - \alpha$

(2) $q(p_2) + q(x_2) \neq a - \alpha$

(3) $(a-\alpha)^2\, q(e_1) + q(x_2) \neq 0$.

Si $p_2 = 0$, on prend $a = \alpha$ et $x_2 \in P_2$ tel que $q(x_2) \neq 0$. Si $P_2 \neq 0$, soit $x' \in P_2$ tel que $\varphi(x',p_2) = 1$. La relation (1) donne $x_2 = (a-\alpha)x' + \lambda\, p_2$ et on obtient alors deux inéquations $F_1(\lambda,a-\alpha) \neq 0$ et $F_2(\lambda,a-\alpha) \neq 0$ où F_1 et F_2 sont deux polynômes quadratiques : il est alors facile de voir que si $\mathrm{Card}(A) > 2$, le système possède toujours une solution, d'où α et λ. En caractéristique différente de 2, on a trois inéquations qui possèdent une solution pourvu que A ait au moins 6 éléments.

Pour résumer, nous avons obtenu le résultat suivant : soit A un anneau semi-local dans lequel ou bien 2 est inversible, ou bien pour tout idéal maximal $\mathfrak{m}$ de A, $\mathrm{Card}(A/\mathfrak{m}) \neq 2$, 3 et 5. Alors il existe un homomorphisme $w : WG(A) \to U(g_\pi(A))$ où $g_\pi(A)$ est le complété de l'anneau gradué $g_*(A) = S_{\mathbb{Z}/2\,\mathbb{Z}}(U/U^2(A) \oplus \mathfrak{D}(A))/I$ et où I est l'idéal de l'anneau $S_{\mathbb{Z}/2\,\mathbb{Z}}(U/U^2(A) \oplus \mathfrak{D}(A))$ engendré par les éléments de la forme :

(1) $\bar{a}.a^0$ pour a parcourant $U(A) \cap A(4)$;
(4) $\overline{-1} - t^{-1}(\overline{-1})$ si $2 \in U(A)$;
(5) $B.B' - t(B).B'$ pour B et B' parcourant $\mathfrak{D}(A)$;
(6) $\bar{a}^2 - \overline{-1}.\bar{a}$ pour a parcourant $U(A)$.

L'homomorphisme w est fonctoriel. En effet, si $A \to B$ est un homomorphisme d'anneaux semi-locaux et si A vérifie les conditions indiquées plus haut, alors B les vérifie aussi. De plus, comme U/U^2 et $\mathfrak{D}$ sont des foncteurs de la catégorie des anneaux commutatifs à élément unité dans celle des groupes abéliens, il existe un morphisme naturel de $g_\pi(A)$ dans $g_\pi(B)$ et il est clair que l'application qu'on en déduit de $U(g_\pi(A))$ dans $U(g_\pi(B))$ fait commuter le diagramme :

$$\begin{array}{ccc} WG(A) & \longrightarrow & WG(B) \\ \downarrow & & \downarrow \\ U(g_\pi(A)) & \longrightarrow & U(g_\pi(B)) \end{array} .$$

Remarques. (i) En caractéristique 2, $t : \mathfrak{D}(A) \to U/U^2(A)$ est l'application nulle et on a $B.B' = 0$ quels que soient $B,B' \in \mathfrak{D}(A)$. Ainsi, $w_i(P,q) = 0$ pour tout A-module quadratique (P,q) et pour tout $i \geq 3$. Dans le cas d'un corps, on obtient des classes de Stiefel-Whitney sans supposer le corps parfait (cf. [47]).

(ii) Si $t : \mathfrak{D}(A) \to U/U^2(A)$ est surjectif, (6) peut être supprimé. En effet, nous avons besoin de $B.\bar{a}^2 = B\,\overline{-1}\,\bar{a}$. Or, si $\bar{a} = t(B')$, une application répétée de (5) et (5') donne la relation voulue.

BIBLIOGRAPHIE

[1] J.F. Adams, Vector fields on spheres, Ann. of Math. 75 (1962), 603-632.

[2] C. Arf, Untersuchungen über quadratische Formen in Körpern der Charakteristik 2, Journal für R. und A. Math. 183 (1941), 148-167.

[3] M. Auslander and O. Goldman, The Brauer group of a commutative ring, Transactions of the A.M.S. 97 (1960), 367-409.

[4] A. Bak, K-theory of forms, Annals of Math. Studies, Princeton.

[5] H. Bass, Lectures on Topics in Algebraic K-theory, Tata Institute of Fundamental Research, Bombay 1967.

[6] H. Bass, K-theorie and stable algebra, Publications Mathématiques I.H.E.S. n° 22, pages 1-60.

[7] H. Bass, Unitary algebraic K-theory, Lecture Notes in Math. 343 (1973), 57-265, Springer-Verlag.

[8] H. Bass, Clifford algebras and spinor norms over a commutative ring, Amer. J. Math. 46 (1974), 156-206.

[9] Z.I. Borevitch et I.R. Chafarevitch, Théorie des Nombres, Gauthier-Villars, Paris, 1967.

[10] N. Bourbaki, Algèbre, Chap. 9. Hermann, Paris 1973.

[11] N. Bourbaki, Algèbre Commutative, Chap. 1 et 2, Hermann, Paris 1961.

[12] N. Bourbaki, Algèbre, Chap. 1 à 3, Hermann, Paris 1970.

[13] N. Bourbaki, Algèbre Commutative, Chap. 7, Hermann, Paris 1965.

[14] R.R. Brown and A. Gray, Vector cross products, Comm. Math. Helv. 41 (1967), 222-236.

[15] T.C. Craven, A. Rosenberg and R. Ware, The map of the Witt ring of a domain into the Witt ring of its field of fractions, Proc. Amer. Math. Soc. 51 (1975), 25-30.

[16] A. Delzant, Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de caractéristique différente de 2, C.R. Acad. Sci. Paris 255 (1962), 1366-1368.

[17] J. Dieudonné, Sur les groupes classiques, Hermann, Paris, 1958.

[18] B. Eckmann, Stetige Lösungen linearer Gleichungsysteme, Comm. Math. Helv. 15 (1942-3), 318-339.

[19] M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer-Verlag,1952.

[20] R. Fossum, The divisor class group of a Krull domain, Ergebnisse der Mathematik, Band 74, Springer-Verlag 1973.

[21] A. Grothendieck, Dix exposés sur la cohomologie des schémas, North-Holland, Amsterdam, 1968.

[22] C. Hostmaelingen, Sur l'anneau de Witt d'un anneau de Prüfer, C.R. Acad. Sci. Paris 280 (1975), 69-71.

[23] C. Hostmaelingen, Sur l'anneau de Witt d'un anneau semi-héréditaire, Anais da Academia Brasileira de Ciências, à paraître.

[24] E. Hornix, Stiefel-Whitney invariants of quadratic forms over local rings, J. of Algebra 26 (1973), 258-279.

[25] I. Kaplansky and R. Shaker, Abstract quadratic forms, Canadian Journal of Math. 21 (1969), 1218-1233.

[26] O. Laborde, Formes quadratiques, algèbres de Clifford et signatures, C.R. Acad. Sci. Paris 278 (1974), 1599-1602.

[27] T.Y. Lam, The algebraic theory of quadratic forms, W.R. Benjamin, Inc., Reading 1973.

[28] A. Larotonda, A. Micali et O.E. Villamayor, Sur le groupe de Witt, Symposia Mathematica 11 (1973), 211-219.

[29] D. Legrand, Formes quadratiques et algèbres quadratiques, Thèse de doctorat, n° d'ordre C.N.R.S. 803, 1971.

[30] F. Lorenz, Quadratische Formen über Körpern, Lecture Notes in Math. 130, Springer-Verlag 1970.

[31] A. Micali et O.E. Villamayor, Sur les algèbres de Clifford, Ann. Sc. Ec. Normale Sup. 1 (1968), 271-304.

[32] A. Micali et O.E. Villamayor, Sur les algèbres de Clifford II, Journal für R. und A. Math., 242 (1970), 61-90.

[33] A. Micali et O.E. Villamayor, Algèbres de Clifford et groupe de Brauer, Ann. Sc. Ec. Normale Sup. 4 (1971), 285-310.

[34] J. Milnor, On simply connected manifolds, Symp. Mexico (1958), 122-128.

[35] J. Milnor, Algebraic K-theory and quadratic forms, Inventiones Math. 9 (1970), 318-344.

[36] J. Milnor and D. Husemoller, Symmetric bilinear forms, Ergebnisse der Mathematik, Band 73, Springer-Verlag 1973.

[37] A. Morris, On a generalized Clifford algebra (II), Quart. Journal of Math. 19 (1968), 289-299.

[38] Y. Nouazé et Ph. Revoy, Algèbres de Weyl généralisées, Bull. Sc. Math. 96 (1972), 27-47.

[39] T. Ogama, On a problem of Fossum, Proc. Japan Academy 50 (1974), 266-267.

[40] O.T. O'Meara, Introduction to quadratic forms, Springer-Verlag, 1963.

[41] A. Pfister, Quadratische Formen in beliebigen Körpern, Inventiones Math. 1 (1966), 116-132.

[42] Ph. Revoy, Sur les deux premiers invariants d'une forme quadratique, Ann. Sc. Ec. Normale Sup. 4 (1971), 311-319.

[43] Ph. Revoy, Groupes de Witt d'un corps de caractéristique 2, Journal für R. und A. Math. 296 (1977), 33-36.

[44] Ph. Revoy, Autour des formes quadratiques, thèse de doctorat, N° d'enregistrement au C.N.R.S. A.O. 8580, Université de Montpellier II, 1975.

[45] A. Roy, Cancellation of quadratic forms over commutative rings, J. of Algebra 10 (1968), 286-298.

[46] P. Samuel, Lectures on unique factorization domains, Tata Institut of Fundamental Research, Bombay, 1964.

[47] W.Scharlau, Quadratische Formen und Galois Cohomologie, Inventiones Math. 4 (1967), 238-264.

[48] W.Scharlau, Quadratic reciprocity laws, Journal of Number Theory 4 (1972),78-97.

[49] J.P. Serre, Modules projectifs et espaces fibrés à fibre vectorielle, Séminaire P. Dubreil 1957/58, Exposé 23 du 5 mai 1958.

[50] J.P. Serre, Corps locaux, Hermann, Paris 1968.

[51] J.P. Serre, Cours d'Arithmétique, PUF, Paris 1970.

[52] C. Small, The Brauer group of a commutative ring, Transactions of the A.M.S. 156 (1971), 455-491.

[53] U. Tietze, Zur theorie quadratischer Formen über Körpern der Charakteristik 2, Journal für R. und A. Math., 268-269 (1974), 388-390.

[54] O.E. Villamayor, Separable algebras and Galois extensions, Osaka J. Math. 4 (1967), 161-171.

[55] G. Vranceanu, Sur les vecteurs tangents aux sphères, Revue Roumaine de Math. Pures et Appliquées 10 (1965), 895-914.

[56] C.T.C. Wall, Graded Brauer groups, Journal dür R. und A. Math. 213 (1964), 187-199.

[57] G.W. Whitehead, Note on cross sections in Stiefel manifolds, Comm. Math. Helv. 37 (1963), 239-240.

[58] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, Journal für R. und A. Math. 176 (1937), 31-44.

[59] P. Zvengrovoski, A 3-fold vector product in R^8, Comm. Math. Helv. 40 (1966), 148-152.