

ANNALES SCIENTIFIQUES
DE L'UNIVERSITÉ DE CLERMONT-FERRAND 2
Série Mathématiques

D. LEGRAND

Formes quadratiques et algèbres quadratiques

Annales scientifiques de l'Université de Clermont-Ferrand 2, tome 54, série *Mathématiques*, n° 10 (1975), p. 45-107

http://www.numdam.org/item?id=ASCFM_1975__54_10_45_0

© Université de Clermont-Ferrand 2, 1975, tous droits réservés.

L'accès aux archives de la revue « *Annales scientifiques de l'Université de Clermont-Ferrand 2* » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

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

FORMES QUADRATIQUES ET ALGEBRES QUADRATIQUES

par **D. LEGRAND**

82, rue Meurein 59 000 - LILLE

INTRODUCTION

Ce travail consiste en l'étude de plusieurs problèmes concernant les structures d'algèbre sur un module quadratique.

Notations.

Dans ce travail, A désigne un anneau commutatif d'unité 1. Tous les modules sont des modules unitaires. Les algèbres sont des algèbres non nécessairement associatives mais avec élément unité.

Pour toute forme quadratique Q définie sur un A -module E , on notera en général B_Q la forme bilinéaire symétrique associée à Q .

Notations O.1.1.

A tout A -module quadratique (E, Q) on associe les sous-ensembles H , K et K_1 de E définis comme suit :

$$H = \{X \mid X \in E \text{ et } Q(X) = 0\} \quad (\text{ensemble des éléments isotropes})$$

$$K = \{X \mid X \in E \text{ et } \forall X' \in E, B_Q(X, X') = 0\} \quad (\text{noyau de la forme } B_Q)$$

$$K_1 = K \cap H \quad (\text{noyau du module quadratique } (E, Q))$$

Lorsque 2 est régulier dans A , $K = K_1$.

Définition O.1.2.

On dit qu'une A -algèbre E d'unité e est une Q -algèbre pour une forme quadratique Q définie sur E lorsque $Q(e) = 1$ et que tout élément X de E vérifie l'équation

$$X^2 = -Q(X)e + B_Q(X, e)X.$$

Ceci étant posé, on constate que toute algèbre unitaire projective de rang 2 sur A est une N -algèbre pour la norme N et que toute forme quadratique Q pour laquelle E est une Q -algèbre coïncide avec la norme N .

Un premier problème se pose, le problème de la détermination des structures de Q -algèbre sur un module quadratique (E, Q) projectif de rang 2 sur A . Ce problème est étudié dans le chapitre I, (§ 1). Un théorème d'existence et d'unicité montre en particulier que toute algèbre unitaire projective de rang 2 est déterminée à isomorphisme près par la donnée de la forme norme.

Un idéal d'une telle algèbre est un module quadratique. Un deuxième problème se pose, le problème de la détermination des structures d'idéal de Q -algèbre sur un module quadratique donné. Cette étude est faite dans le chapitre II pour les idéaux libres de rang 2 des algèbres unitaires libres de rang 2, (algèbres quadratiques selon la terminologie de Bourbaki). Elle est suivie d'une application : Une correspondance entre classes d'idéaux libres de rang 2 d'une algèbre quadratique sur A et classes de formes quadratiques binaires à coefficients dans A .

Les propriétés des algèbres unitaires projectives de rang 2 et de leurs idéaux peuvent être étudiées en utilisant leur structure de module quadratique et en particulier les ensembles H , K et K_1 . Cette étude est faite dans le chapitre I, (§ 2).

Le chapitre III est consacré à l'étude des Q -algèbres générales. Une algèbre unitaire dont tout élément vérifie une équation de dépendance intégrale de degré 2 n'est pas nécessairement une Q -algèbre pour une forme Q convenable. Dans ce chapitre on étudie d'abord des conditions d'existence et d'unicité d'une telle forme Q et les premières propriétés qui résultent de cette existence. On étudie ensuite une famille assez générale de Q -algèbres commutatives et on utilise les résultats obtenus pour l'étude des Q -algèbres non nécessairement commutatives et en particulier de celles de ces algèbres qui possèdent des idempotents non triviaux.

Le chapitre IV est consacré à l'étude des formes quadratiques multiplicatives sur les algèbres étudiées dans le chapitre précédent.

Les résultats énoncés dans ces différents chapitres sont les principaux résultats de la thèse [6]. Ils ont été résumés dans des notes ([7] à [10]).

Chapitre I

Algèbres unitaires projectives de rang 2§ 1. Structures d'algèbre unitaire sur un A-module quadratique projectif de rang 2.

On utilisera dans ce paragraphe des méthodes de localisation et globalisation.

Proposition 1.1.1.

Soit E une A -algèbre projective de rang 2, d'unité e . Alors E est associative et commutative. A tout élément X de E , on peut associer sa norme $N(X)$, déterminant de l'endomorphisme $m_X : Y \mapsto XY$ de E , et l'application $N : X \mapsto N(X)$ est une forme quadratique définie sur E telle que $N(e) = 1$.

Tout élément X de E vérifie l'équation

$$X^2 + N(X)e - B_N(X,e)X = 0$$

Corollaire

Toute A -algèbre unitaire E projective de rang 2 est une N -algèbre pour la norme N . Toute forme quadratique Q définie sur E pour laquelle E est une Q -algèbre coïncide avec la norme N .

Preuve de la proposition et du corollairea) Cas des algèbres libres

Toute A -algèbre unitaire libre de rang 2, c'est-à-dire toute A -algèbre quadratique, vérifie la proposition, (B. A. §2 ch. III). Elle est donc une N -algèbre pour la norme N , (déf. 0.1.2).

Soient E une algèbre quadratique sur A , (e,i) une base de E contenant l'unité e , et α et β les éléments de A définis par la relation $i^2 = \alpha e + \beta i$. Alors la norme N est la forme quadratique définie par $N(e) = 1$, $N(i) = -\alpha$ et $B_N(e,i) = \beta$ et toute forme quadratique Q définie sur E telle que E soit une Q -algèbre coïncide avec N . (On a nécessairement $Q(e) = 1$, $Q(i) = -\alpha$ et $B_Q(e,i) = \beta$).

b) Cas général

Si E est une A -algèbre projective de rang 2, d'unité e , alors, pour tout $\mathfrak{p} \in \text{Spec } A$, $E_{\mathfrak{p}}$ est une algèbre quadratique sur $A_{\mathfrak{p}}$ d'unité $e/1$. La proposition et le corollaire s'établissent par localisation et globalisation car la norme se «localise».

On est amené à poser le problème suivant :

Problème 1.

Soit (E,Q) un A -module quadratique projectif de rang 2. Peut-on définir sur E une structure de A -algèbre unitaire telle que, N désignant la norme de l'algèbre, on ait, pour tout élément X de E , $N(X) = Q(X)$?

D'après le corollaire précédent, le problème 1 peut aussi être énoncé comme suit :

Peut-on définir sur (E, Q) une structure de A -algèbre unitaire telle que E soit une Q -algèbre pour cette structure ?

1 - Théorème d'existence et d'unicité

Théorème 1.1.2.

Soit (E, Q) un A -module quadratique projectif de rang 2, alors :

- Pour qu'il existe sur E une structure de Q -algèbre, il faut et il suffit que la forme Q représente 1.

- Si e est l'unité d'une algèbre solution, $Q(e) = 1$. Inversement, à tout élément e de E tel que $Q(e) = 1$, on peut faire correspondre une algèbre solution d'unité e et une seule.

- Les algèbres solutions sont isomorphes.

On peut préciser

Proposition 1.1.3.

Soit (E, Q) un A -module quadratique projectif de rang 2. On suppose qu'il existe deux éléments e et e' de E tels que $Q(e) = Q(e') = 1$ et on désigne par E_e et $E_{e'}$, les Q -algèbres solutions du problème 1 associées à e et e' respectivement. Alors, il y a identité entre l'ensemble $\Sigma_{ee'}$ des isomorphismes d'algèbres de E_e sur $E_{e'}$, et l'ensemble des transformations orthogonales σ de (E, Q) telles que $\sigma(e) = e'$.

Preuve du théorème et de la proposition

a) Preuve pour les modules libres

Soit (E, Q) un A -module quadratique libre de rang 2.

Lemme

Tout élément e de E tel que $Q(e) = 1$ fait partie d'une base du A -module E .

En effet : Soit (e_1, e_2) une base de E et soit $e = m e_1 + n e_2$ tel que $Q(e) = 1$, $(m, n \in A)$. On suppose Q définie par $Q(e_1) = a$, $Q(e_2) = c$ et $B_Q(e_1, e_2) = b$. Alors, m et n vérifient la relation

$$(1) \quad a m^2 + b m n + c n^2 = 1$$

Or, pour que deux éléments $m e_1 + n e_2$ et $p e_1 + q e_2$ de E ($m, n, p, q \in A$), forment une base de E , il suffit que $m q - p n$ soit inversible. Si on choisit par exemple $p = -c n$ et $q = a m + b n$, on a, compte tenu de (1), $m q - p n = 1$ et le couple $(m e_1 + n e_2, p e_1 + q e_2)$ est une base de E .

Preuve du théorème

Pour toute solution d'unité e , $Q(e) = 1$. De plus, toute base (e, i) d'une algèbre solution d'unité e est telle que $i^2 = -Q(i) e + B_Q(e, i)$. Il existe donc au plus une solution d'unité e .

Inversement, soit e un élément de E tel que $Q(e) = 1$. D'après le lemme, e fait partie d'une base (e, i) de E et, pour la structure d'algèbre d'unité e définie par $i^2 = -Q(i)e + B_Q(e, i)i$, la norme N coïncide avec Q , ce qui montre l'existence d'une solution associée à e .

Donc, à tout élément e de E tel que $Q(e) = 1$ correspond une algèbre solution et on obtient ainsi toutes les solutions.

Soit E_e l'algèbre solution associée à e , et soit (e, i) la base utilisée dans le lemme, ($e = m e_1 + n e_2$, $i = -c n e_1 + (a m + b n) e_2$). Compte tenu de (1), $Q(i) = a c$ et $B_Q(e, i) = b$. Comme $a c$ et b ne dépendent pas du choix de e , les algèbres solutions associées aux différents couples (m, n) vérifiant (1) sont isomorphes.

Preuve de la proposition

- Un isomorphisme de A -algèbres de E_e sur E_e , conserve les normes donc est une transformation orthogonale de (E, Q) .

- Inversement, soit σ une transformation orthogonale de (E, Q) telle que $\sigma(e) = e'$ et soit (e, i) une base de E . Le couple $(\sigma(e), \sigma(i))$ est une base de E et $\sigma(e)$ est l'unité de $E_{e'}$. Un calcul immédiat montre que σ est un isomorphisme de A -algèbres.

Remarque 1

La multiplication par e' pour la structure de E_e est une transformation orthogonale de (E, Q) qui transforme e en e' , c'est donc un isomorphisme d'algèbres de E_e sur $E_{e'}$.

b) Preuve pour les modules projectifs

Soit (E, Q) un module quadratique projectif de rang 2 sur A . Si e est l'unité d'une solution, $Q(e) = 1$ et on établit sans difficulté par localisation et globalisation les résultats suivants :

- Pour tout élément e de E tel que $Q(e) = 1$, il existe au plus une algèbre solution d'unité e .
- Les solutions éventuelles sont des A -algèbres isomorphes.

(Pour établir ce dernier point, on utilise la remarque 1)

Il en est de même pour la preuve de la proposition 1.1.3.

Pour prouver le théorème, il reste à montrer que, pour tout $e \in E$ tel que $Q(e) = 1$, il existe une algèbre solution E_e d'unité e . La globalisation n'étant pas immédiate, la preuve de l'existence de E_e est donnée de façon plus détaillée.

Soit $e \in E$ tel que $Q(e) = 1$. Pour qu'il existe sur E une structure de Q -algèbre d'unité e , il faut et il suffit qu'il existe une application A -bilinéaire \sharp de E^2 dans E telle que

$$(2) \quad \forall p \in \text{Spec } A, \quad \forall X, X' \in E, \quad (\sharp(X, X'))/1 = (X/1)(X'/1)$$

pour la structure de l'algèbre quadratique $(E_p)_e$ d'unité $e/1$, de norme Q_p , où Q_p est l'extension de Q à E_p . Alors, E , muni de la multiplication $(X, X') \mapsto XX' = \phi(X, X')$ est une Q -algèbre d'unité e (vérifications immédiates).

Il reste à montrer l'existence d'une telle application ϕ . Cette existence est une conséquence des deux lemmes suivants. Le premier est un lemme trivial sur l'extension des scalaires dans les algèbres quadratiques, le second est un exercice de Bourbaki (B.A.C. Ch II § 5 ex. 9).

Lemme 1

Soient (E, Q) un A -module quadratique et S et T deux parties multiplicatives de A tels que T contienne S et que $S^{-1}E$ soit un $S^{-1}A$ -module libre de rang 2.

On suppose que 0 n'appartient pas à T et qu'il existe $e \in E$ tel que $Q(e) = 1$. Alors $S^{-1}E$, (resp. $T^{-1}E$), est muni de la structure d'algèbre quadratique $(S^{-1}E)_e$ (resp. $(T^{-1}E)_e$), d'unité $f_S(e)$, (resp. $f_T(e)$), de norme Q_S , (resp. Q_T), où f_S , (resp. f_T), est le morphisme canonique de E dans $S^{-1}E$, (resp. $T^{-1}E$), et Q_S , (resp. Q_T), l'extension de la forme Q à $S^{-1}E$, (resp. $T^{-1}E$), et le morphisme canonique de $S^{-1}E$ dans $T^{-1}E$ est compatible avec les multiplications de $(S^{-1}E)_e$ et $(T^{-1}E)_e$.

Lemme 2

Soient A un anneau commutatif unitaire, $(s_i)_{i \in I}$ une famille finie d'éléments de A engendrant l'idéal A et E un A -module. Pour $i, j \in I$, on pose $A[s_i^{-1}] = A_{s_i}$, $E[s_i^{-1}] = E_{s_i}$, $A[(s_i s_j)^{-1}] = A_{s_i s_j}$, $E[(s_i s_j)^{-1}] = E_{s_i s_j}$.

On suppose qu'il existe $(Z_i)_{i \in I} \in \prod_{i \in I} E_{s_i}$ tel que, pour tout couple (i, j) d'éléments de I , les images canoniques de Z_i et Z_j dans $E_{s_i s_j}$ soient égales.

Alors, il existe un élément Z de E et un seul tel que pour tout $i \in I$, l'image canonique de Z dans E_{s_i} soit égale à Z_i .

On montre maintenant l'existence de l'application ϕ . Puisque E est projectif de rang 2, il existe une famille finie $(s_i)_{i \in I}$ d'éléments de A engendrant l'idéal A telle que, pour tout $i \in I$, E_{s_i} soit un A_{s_i} -module libre de rang 2, (B.A.C. § 5 Ch II).

Pour tout $i \in I$ et tout $X \in E$, on note X_i l'image canonique de X dans E_{s_i} et pour tout couple (i, j) d'éléments de I , on note X_{ij} l'image canonique de X dans $E_{s_i s_j}$.

Puisqu'il existe $e \in E$ tel que $Q(e) = 1$, pour tout $i \in I$, E_{s_i} est muni de la structure d'algèbre quadratique $(E_{s_i})_e$ d'unité e_i et de norme Q_{s_i} (extension de Q à E_{s_i}). Soient X et X' deux éléments de E . Pour tout $i \in I$, on note Z_i le produit de X_i et X'_i dans $(E_{s_i})_e$. Alors, la famille $(Z_i)_{i \in I}$ vérifie les hypothèses du lemme 2.

En effet, soient i et j deux éléments de I .

- Lorsque $s_i s_j$ est nilpotent, les images canoniques de Z_i et Z_j dans $E_{s_i s_j}$ sont nulles.
- Lorsque $s_i s_j$ n'est pas nilpotent, $E_{s_i s_j}$ est muni de la structure d'algèbre quadratique $(E_{s_i s_j})_e$ d'unité e_{ij} et de norme $Q_{s_i s_j}$ (extension de Q à $E_{s_i s_j}$) et Z_i et Z_j ont pour image canonique dans $E_{s_i s_j}$ le produit dans $(E_{s_i s_j})_e$ des éléments X_{ij} et X'_{ij} (cela résulte de lemme 1).

Soit Z l'élément de E associé à la famille $(Z_i)_{i \in I}$ par le lemme 2. On pose $\phi(X, X') = Z$.

La condition (2) est vérifiée. En effet, soit $\mathfrak{p} \in \text{Spec } A$. Puisque la famille $(s_i)_{i \in I}$ engendre l'idéal A , il existe $i \in I$ tel que s_i appartienne à $A - \mathfrak{p}$. On sait que dans $(E_{s_i})_e$, $Z_i = X_i X'_i$, on en déduit, en utilisant le lemme 1 avec $T = A - \mathfrak{p}$, que $f_T(Z) = f_T(X) f_T(X')$.

Donc :

$$\forall \mathfrak{p} \in \text{Spec } A, \quad \forall X, X' \in E, \quad (\phi(X, X'))/1 = (X/1)(X'/1)$$

L'application $\phi : E^2 \rightarrow E$ ainsi définie vérifie les conditions (2). Il est immédiat qu'elle est A -bilinéaire.

Remarque 2

(E, Q) désignant un A -module quadratique projectif de rang 2, on suppose que la propriété ci-dessous est vérifiée.

«Il existe une forme bilinéaire B_1 définie sur E^2 telle que, pour tout élément X de E , $Q(X) = B_1(X, X)$.»

Alors, lorsqu'il existe $e \in E$ tel que $Q(e) = 1$, la multiplication de la Q -algèbre associée à e selon le théorème 1.1.2 est l'application $(X, X') \mapsto XX' = -B_1(X, X')e + B_1(X, e)X + B_1(X', e)X$. En effet, la forme bilinéaire symétrique associée à Q est $2 B_1$. Il est immédiat que pour cette multiplication, E est une Q -algèbre d'unité e .

§2. Etude d'une algèbre unitaire projective de rang 2

Dans tout ce paragraphe, E désigne une A-algèbre projective de rang 2, d'unité e, de norme N.

1 - Propriétés préliminaires

Proposition 2.1.1

La norme N de l'algèbre E est multiplicative sur E et l'application σ définie sur E par $\sigma(X) = B_N(X,e)e - X$ est un automorphisme de l'algèbre E tel que $\sigma^2 = 1_E$ et tel que, pour tout $X \in E$, $X \sigma(X) = N(X)e$.

Preuve

- Pour tout élément X de E, on note m_X la multiplication par X. Pour tout couple (X, X') d'éléments de E, $m_X \circ m_{X'} = m_{XX'}$, donc

$$N(X) N(X') = \det(m_X) \det(m_{X'}) = \det(m_{XX'}) = N(XX').$$

- Il est immédiat que $\sigma^2 = 1_E$ et que σ est une transformation orthogonale de (E, N) telle que $\sigma(e) = e$. C'est donc un automorphisme de l'algèbre E, (prop. 1.1.3). La dernière égalité est une conséquence de l'équation $X^2 = -N(X)e + B_N(X,e)X$.

Remarque : Il résulte de la proposition 2.1.1 que :

1 - Pour qu'un élément X de E soit inversible, (resp. régulier), il faut et il suffit que $N(X)$ soit un élément inversible, (resp. régulier), de A.

2 - Pour que E soit égal à son anneau total de fractions, il faut et il suffit que A soit égal à son anneau total de fractions.

2 - Propriétés relatives à l'ensemble des éléments isotropes et au noyau du module quadratique (E,N)

On associe à (E, N) les ensembles suivants (cf. notations 0.1.1)

$$H = \{X \mid X \in E \text{ et } N(X) = 0\}$$

$$K = \{X \mid X \in E \text{ et } \forall X' \in E, B_N(X, X') = 0\}$$

$$K_1 = K \cap H$$

a) Etude des ensembles K et K_1

Proposition 1.2.2

K et K_1 sont des idéaux de E.

Preuve

Comme les ensembles K et K_1 se localisent, on peut se ramener par localisation au cas où E est libre. Soit (e, i) une base de E telle que $i^2 = \alpha e + \beta i$, ($N(i) = -\alpha$, $B_N(e, i) = \beta$). K est l'ensemble des éléments $x e + y i$ de E, ($x, y \in A$), tels que

$$(1) \quad 2x + \beta y = 0 \quad (B_N(xe + yi, e) = 0)$$

$$(2) \quad \beta x - 2\alpha y = 0 \quad (B_N(xe + yi, i) = 0)$$

$K = (0)$ si et seulement si $4\alpha + \beta^2$ est un élément régulier de A .

K et K_1 sont des sous A -modules de E . De plus,

$$\forall X \in K, \quad \forall X' \in E, \quad XX' \in K$$

En effet, si $X = xe + yi$ et $X' = x'e + y'i$, ($x, y, x', y' \in A$),

$$XX' = (xx' + \alpha yy')e + (xy' + x'y + \beta yy')i$$

$$B_N(XX', e) = 2(xx' + \alpha yy') + \beta(xy' + x'y + \beta yy') = B_N(X, e)x' + B_N(X, i)y' + (4\alpha + \beta^2)y y'$$

$$B_N(XX', i) = \beta(xx' + \alpha yy') - 2\alpha(xy' + x'y + \beta yy') = B_N(X, i)x' - B_N(X, e)\alpha y'$$

Lorsque X appartient à K , $B_N(X, e) = B_N(X, i) = 0$ et puisque x et y vérifient les équations

(1) et (2), $(4\alpha + \beta^2)y = 0$. Donc $B_N(XX', e) = 0$, $B_N(XX', i) = 0$ et XX' appartient à K .

Lorsque de plus X appartient à K_1 , $N(XX') = N(X)N(X') = 0$ donc XX' appartient à K_1 .

Proposition 1.2.3

Tout élément du noyau K_1 est de carré nul.

Lorsque 2 est régulier dans A , on a $K_1^2 = K^2 = (0)$.

Preuve

Pour tout élément X de E , $X^2 = -N(X)e + B_N(X, e)X$ et pour tout couple (X, X') d'éléments de E ,

$$2XX' = (X + X')^2 - X^2 - X'^2 = -B_N(X, X')e + B_N(X, e)X' + B_N(X', e)X.$$

Donc, lorsque X appartient à K_1 , $X^2 = 0$ et lorsque X et X' appartiennent à K_1 , $2XX' = 0$.

Lorsque 2 est régulier dans A , $K = K_1$ et pour tout couple (X, X') d'éléments de K , $XX' = 0$.

b) Propriétés liées aux ensembles H , K et K_1

Il résulte du a) que K_1 est un idéal de E contenu dans le nilradical de E . On va étudier quelques cas particuliers.

1) On suppose A réduit

Proposition 1.2.4

Lorsque A est réduit, le nilradical de E est l'ensemble des éléments de carré nul. Cet ensemble est égal au noyau K_1 de (E, N) .

Preuve

Comme pour la preuve de la proposition 1.2.2, on peut se ramener par localisation au cas où E est libre.

Soit $X \in E$. Pour que X soit nilpotent, il faut et il suffit que $N(X) = B_N(X,e) = 0$.

En effet, pour tout élément X de E , $X^2 = -N(X)e + B_N(X,e) = 0$, donc

$$(B_N(X,e) = 0 \text{ et } N(X) = 0) \Rightarrow X^2 = 0$$

Inversement, on suppose qu'il existe $n \in \mathbb{N} - \{0\}$ tel que $X^n = 0$. Puisque N est multiplicative et A réduit, $N(X^n) = 0$ implique $N(X) = 0$. On en déduit successivement, si $n \geq 2$,

$$X^2 = B_N(X,e) X, X^n = (B_N(X,e))^{n-1} X, 0 = B_N(X^n,e) = (B_N(X,e))^n, B_N(X,e) = 0$$

Il en résulte que tout élément nilpotent est de carré nul. Compte tenu de la proposition 1.2.3, il reste à montrer que tout élément de carré nul appartient à K_1 .

Soit (e, i) une base de E telle que $i^2 = \alpha e + \beta i$. Tout élément $X = x e + y i$ qui vérifie les conditions $N(X) = 0$ et $B_N(X,e) = 0$ vérifie aussi la condition $B_N(X,i) = 0$ donc appartient à K_1 . En effet : $N(X) = x^2 + \beta xy - \alpha y^2$, $B_N(X,e) = 2x + \beta y$ et $B_N(X,i) = \beta x - 2\alpha y$, d'où

$$(3) \quad 4\alpha N(X) = (2\alpha y - \beta x)^2 - (4\alpha + \beta^2)x^2$$

$$(4) \quad 4 N(X) = (2x + \beta y)^2 - (4\alpha + \beta^2)y^2$$

$$\text{Puisque } B_N(X,e) = 2x + \beta y = 0, N(X) = -(x^2 + \alpha y^2)$$

$$\text{Puisque } N(X) = 0 \text{ et } B_N(X,e) = 0, x^2 = -\alpha y^2 \text{ et } (4\alpha + \beta^2)y^2 = 0.$$

On en déduit $(4\alpha + \beta^2)x^2 = 0$, $(2\alpha y - \beta x)^2 = 0$ et, puisque A est réduit, $-2\alpha y + \beta x = 0$, c'est-à-dire $B_N(X,i) = 0$.

2) On suppose A intègre

Proposition 1.2.5

On suppose A intègre. Alors :

- H est l'ensemble des éléments non réguliers de E
- Lorsque $K \neq (0)$, $H = K_1$ et H est un idéal premier qui est le nilradical de E .

Preuve

- Le premier point résulte de la proposition 1.2.3.

- On suppose E libre et on reprend les notations précédentes.

Lorsque K est $\neq (0)$, $4\alpha + \beta^2 = 0$. Soit $X = x e + y i \in H$. D'après (3) et (4),

$$0 = 4\alpha N(X) = (\beta x - 2\alpha y)^2 - (4\alpha + \beta^2)x^2$$

$$0 = 4 N(X) = (2x + \beta y)^2 - (4\alpha + \beta^2)y^2$$

Donc $2x + \beta y = \beta x - 2\alpha y = 0$, ce qui montre que H est inclus dans K . Donc $H = H \cap K = K_1$ et H est le nilradical de E , (prop. 1.2.4). De plus, H est un idéal premier car $N(XX') = 0$ implique $N(X) = 0$ ou $N(X') = 0$.

Ces propriétés s'étendent immédiatement à une algèbre E projective.

Pour étudier les idéaux de E , on étudie d'abord rapidement le cas particulier où A est un corps.

On peut distinguer trois cas auxquels correspondent trois types d'anneaux E .

Cas 1 : $H = \{0\}$ E est un corps

Cas 2 : $H \neq \{0\}$, $K = K_1 = \{0\}$

E n'est pas intègre, il est réduit et possède exactement deux idéaux stricts non nuls et dont la réunion est H . (Ils correspondent aux deux familles de solutions de l'équation $N(X) = 0$, $(x^2 + \beta xy - \alpha y^2 = 0$ avec les notations précédentes).)

Cas 3 : $K_1 \neq (0)$, $H = K_1$ (prop. 1.2.5)

E n'est pas réduit, il possède un seul idéal strict non nul K_1 .

On suppose maintenant A simplement intègre. Soient A_0 le corps des fractions de A et E_0 l'algèbre quadratique obtenue par extension des scalaires à A_0 . On identifie A et E à leurs images respectives dans A_0 et E_0 par les injections canoniques. L'extension de tout idéal de E est un idéal de E_0 . On obtient les résultats suivants :

Cas 1 : $H = \{0\}$

E est intègre, les idéaux non nuls sont de rang 2.

Cas 2 : $H \neq \{0\}$, $K = K_1 = (0)$

E n'est pas intègre, il est réduit. Les idéaux de rang 1 sont les idéaux $\neq (0)$ contenus dans H et se répartissent en deux familles comme suit : Il existe deux idéaux premiers de rang 1, I_1 et I_2 , tels que $I_1 \cap I_2 = (0)$ et $I_1 \cup I_2 = H$; les idéaux de rang 1 sont les idéaux non nuls contenus soit dans I_1 , soit dans I_2 .

Cas 3 : $K_1 \neq (0)$, (donc $H = K_1$)

E n'est pas réduit. Les idéaux de rang 1 sont les idéaux $\neq (0)$ contenus dans le nilradical K_1 .

En particulier, lorsque A est principal, E est libre et, pour qu'un idéal de E soit libre de rang 2, il faut et il suffit qu'il contienne un élément de norme non nulle. Il en résulte que le produit de deux idéaux libres de rang 2 est un idéal libre de rang 2.

On revient au cas général (A quelconque).

3) Etude du groupe d'automorphismes de E

Proposition 1.2.6

Le groupe d'automorphismes T de E n'est pas nécessairement commutatif, l'anneau d'invariants contient A e mais l'inclusion peut être stricte.

Lorsque 2 est régulier dans A , T est commutatif et l'anneau d'invariants est A e.

Preuve

On suppose d'abord E libre, de base (e, i) telle que $i^2 = \alpha e + \beta i$. D'après la proposition 1.1.3, les automorphismes de l'algèbre E sont les transformations orthogonales de (E, N) qui laissent e invariant. Un automorphisme σ de E est défini par la donnée d'un élément $j = x e + y i$ de E , ($j = \sigma(i)$), tel que (e, j) soit une base de E et tel que $N(j) = N(i)$ et $B_N(e, j) = B_N(e, i)$. Ces conditions s'écrivent :

$$\left. \begin{array}{l} (5) \quad x^2 + \beta x y - \alpha y^2 = -\alpha \\ (6) \quad 2x + \beta y = \beta \\ (7) \quad y \text{ est inversible} \end{array} \right\} (1.2.7)$$

Le système (1.2.7) admet toujours en particulier les solutions $(x, y) = (0, 1)$ et $(x, y) = (\beta, -1)$. Elles sont confondues lorsque $2 = \beta = 0$. A la première correspond l'automorphisme identique 1_E , à la seconde l'automorphisme $X \mapsto B_N(X, e) e - X$ déjà signalé.

- Soient σ et σ' les automorphismes associés à deux solutions (x, y) et (x', y') du système (1.2.7). Pour que σ et σ' commutent, il faut et il suffit que leurs matrices relatives à la base (e, i) commutent c'est-à-dire que $x'(y-1) = x(y'-1)$.

Les équations $2x + \beta y = \beta$ et $2x' + \beta y' = \beta$ impliquent $2[x'(y-1) - x(y'-1)] = 0$ et $\beta[x'(y-1) - x(y'-1)] = 0$. En particulier, lorsque 2 est régulier, T est commutatif.

Exemple de groupe T non commutatif

On prend pour A l'extension quadratique de l'anneau de séries formelles $k[[t]]$ sur le corps k à deux éléments définie par $A = k[[t]] \oplus k[[t]] u$ avec $u^2 = 0$, et pour algèbre E , une A -algèbre de base (e, i) telle que $i^2 = 0$, ($\alpha = \beta = 0$).

Les couples $(x, y) = (u, y)$ avec y inversible et $(x', y') = (0, 1 + t)$ sont des solutions du système (1.2.7) mais $x'(y-1) = 0$ et $x(y'-1) = u t$ avec $u t \neq 0$.

- Il est évident que l'anneau d'invariants contient A e.

Lorsque 2 est régulier, l'automorphisme $\sigma : X \mapsto B_N(X, e) e - X$ ne laisse invariants que les éléments de A e. En effet, si $X = a e + b i$, $\sigma(X) = (a + \beta b)e - b i$ donc $\sigma(X) = X$ si et seulement si $\beta b = 2b = 0$.

Exemple d'inclusion stricte

On choisit $A = \mathbb{Z}/6\mathbb{Z}$, $\alpha = \beta = 0$. Les automorphismes de E sont associés aux couples $(0, b)$ où $b = \bar{1}$ ou $\bar{5}$. L'élément $\bar{3} i$ est invariant par T et n'appartient pas à A e.

Remarque : Lorsque 2 est régulier, il y a au plus un automorphisme de déterminant γ fixé.

La proposition s'étend immédiatement au cas projectif.

Etude du cas particulier où A est intègre

Proposition 1.2.8

On suppose A intègre.

- Lorsque $K = (0)$, le groupe d'automorphismes T de E a exactement deux éléments, l'identité et l'automorphisme $\sigma : X \mapsto B_N(X,e)e - X$, lorsque de plus H est $\neq \{0\}$, σ transforme tout idéal de rang 1 de l'une des deux familles en un idéal de l'autre famille.

- Lorsque K est $\neq (0)$, pour tout $X \in E$, l'orbite O_X de X est contenue dans $X + H$.

Dans les deux cas, le groupe T est commutatif.

Preuve

On étudie d'abord le cas particulier où A est un corps. Soit (e,i) une base de E telle que $i^2 = \alpha e + \beta i$.

Lorsque $K = (0)$, $(4\alpha + \beta^2 \neq 0)$, le système (1.2.7) a exactement deux solutions $(0,1)$ et $(\beta,-1)$, il leur correspond l'identité et l'automorphisme $\sigma : X \mapsto B_N(X,e)e - X$. On voit facilement que lorsque H est $\neq \{0\}$, σ échange les deux idéaux stricts non nuls de E.

Lorsque $K \neq (0)$, $4\alpha + \beta^2 = 0$. Soit O_i l'orbite de i.

$$O_i = \{j \mid j \in E, j = i + x_1 e + y_1 i, x_1 e + y_1 i \in K_1 \text{ et } 1 + y_1 \neq 0\}$$

En effet : Soient $X_1 = x_1 e + y_1 i$ et $j = i + X_1$. Puisque K est $\neq (0)$, $H = K_1$, (prop. 1.2.5).

$$X_1 \in K_1 \Rightarrow (N(i + X_1) = N(i) \text{ et } B_N(e, i + X_1) = B_N(e, i)).$$

Donc $(X_1 \in K_1 \text{ et } 1 + y_1 \neq 0)$ implique $i + X_1 \in O_i$.

Il reste à établir l'implication opposée. Lorsque $i + X_1$ appartient à O_i , $(e, i + X_1)$ est une base de E donc $1 + y_1$ est $\neq 0$,

$$B_N(e, i + X_1) = B_N(e, i) \Rightarrow B_N(e, X_1) = 0$$

$$B_N(e, X_1) = 0 \Rightarrow 4N(X_1) = 0$$

En effet $4N(X_1) = (B_N(e, X_1))^2 - (4\alpha + \beta^2)y_1^2$ et $4\alpha + \beta^2 = 0$.

Donc lorsque 2 est $\neq 0$, $N(X_1) = 0$. Lorsque 2 = 0, l'équation $N(i + X_1) - N(i) = 0$

s'écrit $x_1^2 - \alpha((y_1 + 1)^2 - 1) = 0$ ou encore $x_1^2 - \alpha y_1^2 = 0$ c'est-à-dire $N(X_1) = 0$.

Conséquence

Lorsque $K \neq (0)$, on a, pour tout élément $X = x e + y i$ de E ,

$$0_X = \left\{ X' \mid X' \in E, X' = X + y(x_1 e + y_1 i), x_1 e + y_1 i \in H, 1 + y_1 \neq 0 \right\}$$

En particulier $0_X \subset X + H$.

- Le groupe T est commutatif.

C'est immédiat lorsque $K = (0)$ ou $H = (0)$.

On suppose maintenant $K_1 \neq (0)$, alors $K \neq (0)$ et $H = K_1$. Soit $X_0 = x_0 e + y_0 i$

un générateur de K_1 .

$$0_i = \left\{ X' \mid X' \in E, X' = i + \mu X_0, \mu \in A, 1 + \mu y_0 \neq 0 \right\}$$

Soient σ_1 et σ_2 les automorphismes associés à μ_1 et μ_2 et $X = x e + y i$ un

élément quelconque de E .

$$(\sigma_1 \circ \sigma_2)(X) = X + y [\mu_1 x_0 + \mu_2 x_0 + \mu_1 \mu_2 y_0 x_0] e + y y_0 [\mu_1 + \mu_2 + \mu_1 \mu_2] i$$

donc $(\sigma_1 \circ \sigma_2)(X) = (\sigma_2 \circ \sigma_1)(X)$. Donc T est commutatif.

Si on suppose simplement A intègre, E se plonge dans l'algèbre E_0 obtenue par extension des scalaires au corps des fractions A_0 de A , tout automorphisme de l'algèbre E se prolonge en un automorphisme de l'algèbre E_0 . Les résultats énoncés résultent immédiatement de l'étude précédente.

Chapitre II

Idéaux libres de rang 2 d'une algèbre quadratique§1. Structures d'idéal d'algèbre quadratique sur un A-module quadratique libre de rang 2

La norme d'une algèbre quadratique induit sur tout idéal libre de rang 2 de cette algèbre une structure de module quadratique libre de rang 2. On est amené à généraliser le problème 1 comme suit :

Problème 2

Soit (E, Q) un A-module quadratique libre de rang 2. Peut-on trouver un idéal E' d'une algèbre quadratique et un isomorphisme quadratique σ de (E, Q) sur (E', N) où N désigne la norme de l'algèbre ?

Lorsque E' et σ existent, E s'identifie par σ à un idéal d'une algèbre quadratique.

On établit d'abord deux résultats préliminaires.

1 - Etude des idéaux libres de rang 2 d'une algèbre quadratique

Soit F une algèbre quadratique d'unité f , de base (f, j) , de norme N . On pose $N(j) = -\alpha$ et $B_N(f, j) = \beta$.

a) Condition nécessaire et suffisante pour qu'un sous-module libre de rang 2 de F soit un idéal de F

Soit E un sous-module de F de base (e_1, e_2) , $(e_1 = u_1 f + v_1 j, e_2 = u_2 f + v_2 j)$.

Le déterminant $\delta = u_1 v_2 - u_2 v_1$ est un élément régulier de A et si on choisit une autre base pour E , le déterminant associé est de la forme δu avec u inversible.

Pour que E soit un idéal de F il faut et il suffit que $j e_1$ et $j e_2$ appartiennent à E . Un calcul facile montre que pour qu'il en soit ainsi, il faut et il suffit qu'il existe des éléments x, y, x', y' de A tels que

$$\left. \begin{aligned} (1) \quad \delta x &= -(u_1 u_2 - \alpha v_1 v_2 + \beta u_2 v_1) \\ (2) \quad \delta y &= u_1^2 + \beta u_1 v_1 - \alpha v_1^2 \\ (3) \quad \delta x' &= -u_2^2 - \beta u_2 v_2 + \alpha v_2^2 \\ (4) \quad \delta y' &= u_1 u_2 - \alpha v_1 v_2 + \beta u_1 v_2 \end{aligned} \right\} (2.1.1)$$

Lorsque 2 est régulier dans A , le système (2.1.1) est équivalent au système (2.1.1)'

$$\left. \begin{aligned} (1') \quad 2 \delta x &= \beta \delta - B_N(e_1, e_2) \\ (2) \quad \delta y &= N(e_1) \\ (3) \quad \delta x' &= -N(e_2) \\ (4') \quad 2 \delta y' &= \beta \delta + B_N(e_1, e_2) \end{aligned} \right\} (2.1.1)'$$

comme on le vérifie aisément.

Pour que le système (2.1.1)' admette une solution (x, y, x', y') il faut et il suffit que δ divise $N(e_1)$, $N(e_2)$ et $B_N(e_1, e_2)$, c'est-à-dire que δ divise la norme de chaque élément de E .

Dans le cas général, pour que le système (2.1.1) admette une solution (x, y, x', y') , il est nécessaire que δ soit un diviseur de la norme sur E . (En effet, ((1) et (4)) $\Rightarrow \delta(y' - x) = B_N(e_1, e_2)$).

b) Condition nécessaire et suffisante d'isomorphie quadratique de deux idéaux libres de rang 2 de l'algèbre quadratique F

On établit un résultat un peu plus général.

Proposition 2.1.2

Soient F une algèbre quadratique d'unité f et de norme N , E et E' deux sous- A -modules de F libres de rang 2, et σ un isomorphisme de E sur E' . On désigne par $S^{-1}F$ l'algèbre quadratique obtenue par extension des scalaires à l'anneau total de fractions $S^{-1}A$ de A et on identifie A et F à leurs images respectives dans $S^{-1}A$ et $S^{-1}F$ par les injections canoniques. Alors,

- σ se prolonge en un automorphisme σ_o du $S^{-1}A$ -module $S^{-1}F$
- Pour qu'il existe deux éléments réguliers k et k' de A tels que, pour tout élément X de E , $k'N(X) = kN(\sigma(X))$, il faut et il suffit que σ_o puisse être mis sous la forme $m_f \circ \tau_o$ où m_f est la multiplication par un élément f' de $S^{-1}F$ de norme $k'k^{-1}$ et τ_o un automorphisme d'algèbre de $S^{-1}F$.

Preuve

- Deux bases homologues (e_1, e_2) et $(\sigma(e_1), \sigma(e_2))$ de E et E' sont aussi des bases du $S^{-1}A$ -module $S^{-1}F$ donc σ se prolonge à un $S^{-1}A$ -automorphisme σ_o de $S^{-1}F$.

- Soit N_o la norme de $S^{-1}F$. Si $k'N(X) = kN(\sigma(X))$ pour tout élément X de E , $k'N_o(Y) = kN_o(\sigma_o(Y))$ pour tout élément Y de $S^{-1}F$, en particulier, $N_o(\sigma_o(f)) = k'k^{-1}$.

Soit $f' = \sigma_o(f)$. Puisque $k'k^{-1}$ est inversible dans $S^{-1}A$, f' est inversible dans $S^{-1}F$, (prop. 1.2.1, remarque). L'application $\tau_o = m_{f',-1} \circ \sigma_o$ est une transformation orthogonale de

$(S^{-1}F, N_o)$ qui conserve f , c'est donc un automorphisme d'algèbre de $S^{-1}F$. La réciproque est immédiate.

La proposition s'applique en particulier aux idéaux libres de rang 2 de F et donne une caractérisation des isomorphismes quadratiques entre ces idéaux. Il suffit de prendre $k = k'$.

Corollaire

Les notations sont celles de la proposition 2.1.2. Soit E un sous A -module de F libre de rang 2. Alors les sous-modules de F images de E par les isomorphismes de A -modules compatibles avec la norme sont les sous-modules de F de la forme $f \cdot E$ où f est un élément de $S^{-1}F$ de norme 1 et E'' l'image de E par un automorphisme de l'algèbre $S^{-1}F$.

2 - Etude du problème 2a) Théorème d'existence - Caractérisation des solutionsThéorème 2.1.3 :

Soit (E, Q) un A -module quadratique libre de rang 2. Pour qu'il existe une algèbre quadratique F de norme N , un idéal E' de F et un isomorphisme quadratique σ de (E, Q) sur (E', N) , (autrement dit pour qu'il existe une solution du problème 2), il faut et il suffit qu'il existe δ , élément régulier de A , diviseur de $Q(X)$ pour tout $X \in E$, et $V \in E$ tels que $Q(V) = \delta^2$.

On peut convenir d'identifier deux solutions (F, E', σ) et (F_1, E'_1, σ_1) du problème 2 lorsqu'il existe un isomorphisme τ de l'algèbre F sur l'algèbre F_1 tel que $\tau(E') = E'_1$ et $\tau \circ \sigma = \sigma_1$.

Avec cette convention, il existe une correspondance biunivoque entre les couples (V, δ) vérifiant la condition de ce théorème, définis à un facteur inversible près, et les solutions du problème 2.

(les couples (V, δ) et $(tV, t\delta)$ où t est un élément inversible de A correspondent à la même solution).

Preuve.1 - Critère d'existence de solutions

On utilisera plusieurs lemmes.

Soit (E, Q) un A -module quadratique libre de rang 2. On cherche d'abord s'il existe une algèbre quadratique F de norme N , un sous-module E' de F et un isomorphisme quadratique σ de (E, Q) sur (E', N) . Lorsqu'on fixe une base (e_1, e_2) de E et lorsqu'on se donne un A -module F de base (f, j) , cela revient à chercher un couple (α, β) d'éléments de A qui détermine une multiplication d'unité f sur F par la relation $j^2 = \alpha f + \beta j$ et une base $(\sigma(e_1), \sigma(e_2))$ du sous-module E' .

Le lemme 1 donne une condition d'existence de solutions (F, E', σ) de ce problème préliminaire.

Lemme 1

Soit (E, Q) un A -module quadratique de base (e_1, e_2) . Pour que (E, Q) puisse être identifié

à un sous-module d'une algèbre quadratique par un isomorphisme quadratique, il faut et il suffit qu'il existe un couple (V,W) d'éléments de E , de déterminant δ régulier dans A , et deux éléments α et β de A tels que $Q(V) = \delta^2$, $Q(W) = -\alpha \delta^2$ et $B_Q(V,W) = \beta \delta^2$.

Lorsque cette condition est vérifiée, E peut être identifié à un sous module E' d'une algèbre F d'unité f , de base (f,j) telle que $j^2 = \alpha f + \beta j$, par un isomorphisme quadratique σ tel que $\sigma(V) = \delta f$ et $\sigma(W) = \delta j$.

Preuve

On suppose qu'il existe une solution (F, E', σ) de ce problème préliminaire. F est une algèbre quadratique d'unité f , de base (f,j) telle que $j^2 = \alpha f + \beta j$, E' un sous-module de F de base (e'_1, e'_2) homologue de la base (e_1, e_2) de E . Soient $e'_1 = u_1 f + v_1 j$ et $e'_2 = u_2 f + v_2 j$. $\delta = u_1 v_2 - u_2 v_1$. Le déterminant δ est un élément régulier de A , δf et δj sont des éléments de E' , ($\delta f = v_2 e'_1 - v_1 e'_2$, $\delta j = -u_2 e'_1 + u_1 e'_2$), $N(\delta f) = \delta^2$, $N(\delta j) = -\alpha \delta^2$ et $B_N(\delta f, \delta j) = \beta \delta^2$. Il existe donc un couple (V,W) d'éléments de E tel que $\sigma(V) = \delta f$, $\sigma(W) = \delta j$, $Q(V) = \delta^2$, $Q(W) = -\alpha \delta^2$ et $B_Q(V,W) = \beta \delta^2$.

Le couple (V,W) dépend du choix de la base (f,j) de F . Il est déterminé lorsque cette base est fixée et a pour déterminant δ relativement à (e_1, e_2) . En effet, $V = v_2 e_1 - v_1 e_2$, $W = -u_2 e_1 + u_1 e_2$.

Inversement, soient (V,W) un couple d'éléments de E de déterminant δ régulier et α et β vérifiant les conditions indiquées dans le lemme. Soient $u_1, u_2, v_1, v_2 \in A$ tels que $V = v_2 e_1 - v_1 e_2$ et $W = -u_2 e_1 + u_1 e_2$ et soit $\delta = u_1 v_2 - u_2 v_1$. On considère une algèbre quadratique d'unité f , de base (f,j) telle que $j^2 = \alpha f + \beta j$ et le sous-module E' de F engendré par $e'_1 = u_1 f + v_1 j$ et $e'_2 = u_2 f + v_2 j$. Puisque δ est régulier, E' est libre de rang 2. Alors (F, E', σ) , où σ est défini par $\sigma(e_1) = e'_1$ et $\sigma(e_2) = e'_2$, est une solution de ce problème préliminaire comme on le vérifie aisément.

Remarque 1

Les solutions (F_1, E'_1, σ_1) où une base de F_1 contenant l'unité est fixée et auxquelles correspond le même couple (V,W) sont les triples de la forme $(\tau(F), \tau(E'), \tau \circ \sigma)$ où τ est un isomorphisme d'algèbres.

En effet, puisque la donnée du couple (V,W) détermine α, β, δ et la base de E' , ces solutions sont nécessairement de cette forme et il est immédiat que tout triple de cette forme est une solution à laquelle (V,W) est associé.

Le lemme suivant est une conséquence immédiate du lemme 1 et de l'étude (1,a) du paragraphe 1.

Lemme 2

Soit (E,Q) un A -module quadratique de base (e_1, e_2) . Pour qu'il existe un isomorphisme quadratique de (E,Q) sur un idéal d'une algèbre quadratique, il faut et il suffit qu'il existe un couple $(V = v_2 e_1 - v_1 e_2, W = -u_2 e_1 + u_1 e_2)$, $(u_1, v_1, u_2, v_2 \in A)$, de déterminant δ régulier, vérifiant les conditions suivantes :

$$1 \quad Q(V) = \delta^2 \text{ et il existe } (\alpha, \beta) \in A^2 \text{ tel que } Q(W) = -\alpha \delta^2 \text{ et } B_Q(V,W) = \beta \delta^2$$

2 Le système (2.1.1) du (1,a) admet une solution (x,y,x',y') formée d'éléments de A .

D'après l'étude (1, a), pour que le système (2.1.1) admette une solution, il faut que δ divise $N(X')$ pour tout $X' \in E'$, c'est-à-dire que δ divise $Q(X)$ pour tout $X \in E$.

Le lemme 3 permet d'associer au moins une solution du problème 2 à tout couple (V, δ) tel que $Q(V) = \delta^2$ et tel que δ soit un élément régulier de A qui divise $Q(X)$ pour tout $X \in E$.

Lemme 3

Soit (E,Q) un A -module quadratique de base (e_1, e_2) . On pose $Q(e_1) = a, Q(e_2) = c$ et $B_Q(e_1, e_2) = b$. Soit δ un élément régulier de A diviseur commun à a, b, c . S'il existe $V \in E$ tel que $Q(V) = \delta^2$, il existe $W \in E$ tel que le couple (V, W) ait pour déterminant δ et vérifie les conditions du lemme 2.

Preuve

Soit $V = m e_1 + n e_2, (m,n \in A)$, tel que $Q(V) = \delta^2$. On pose $W = -c' n e_1 + (a' m + b' n) e_2, a', b', c'$ désignant les quotients respectifs de a, b, c par δ . Compte tenu de l'égalité $Q(V) = \delta^2, m(a'm + b'n) + n c' n = \delta, Q(W) = a'c' \delta^2$ et $B_Q(V,W) = b' \delta^2$. Donc le couple (V,W) vérifie la condition 1 du lemme 2 pour $\alpha = -a'c'$ et $\beta = b'$. Pour retrouver les notations précédentes, on pose $m = v_2$ et $n = -v_1$.

Lorsque 2 est régulier, le système (2.1.1) du (1,a) est équivalent au système (2.1.1)' qui s'écrit ici

$$2 \quad \delta x = \beta \delta - b$$

$$\delta y = a$$

$$\delta x' = -c$$

$$2 \quad \delta y' = \beta \delta + b$$

et qui admet la solution évidente $(0, a', -c', b')$.

Lorsque 2 n'est pas régulier, on vérifie directement que $(0, a', -c', b')$ est encore une solution de (2.1.1).

Donc la condition 2 du lemme 2 est vérifiée.

On en déduit le critère d'existence annoncé. En effet :

- s'il existe une solution du problème 2, il existe au moins un couple (V, W) vérifiant les conditions du lemme 2 et par suite un couple (V, δ) vérifiant les conditions du théorème.

- Inversement, à tout couple (V, δ) vérifiant les conditions du théorème, correspond d'après le lemme 3, au moins un couple (V, W) vérifiant les conditions du lemme 2, et par suite une solution du problème 2.

2 - Correspondance entre couples (V, δ) définis à un facteur inversible près et solutions du problème 2 définies à isomorphisme près

- Soit (F, E', σ) une solution du problème 2. Lorsqu'une base (f, j) de F contenant l'unité f est fixée, il lui correspond selon le lemme 1 un couple unique (V, W) d'éléments de E tel que $\sigma(V) = \delta f$ et $\sigma(W) = \delta j$, (où δ est le déterminant de $(\sigma(e_1), \sigma(e_2))$ relatif à (f, j) et aussi le déterminant de (V, W) relatif à (e_1, e_2)), et le couple (V, δ) associé.

Les couples (V_1, W_1) associés à (F, E', σ) et aux différentes bases de F contenant f sont les couples (tV, W_1) de déterminant $t\delta$ tels que t soit un élément inversible de A et (tV, W_1) une base du sous-module $[V, W]$ de E . En effet :

Soit (f, j_1) une autre base de F , $j = sf + tj_1$ ($s, t \in A$, t inversible). Alors,

$$\sigma(e_1) = u_1f + v_1j = (u_1 + sv_1)f + tv_1j_1 \text{ et } \sigma(e_2) = u_2f + v_2j = (u_2 + sv_2)f + tv_2j_1$$

et le couple (V_1, W_1) associé à (F, E', σ) et à la base (f, j_1) est tel que

$$V_1 = tv_2e_1 - tv_1e_2 = tV \text{ et } W_1 = -(u_2 + sv_2)e_1 + (u_1 + sv_1)e_2 = -sV + W.$$

On en déduit que $V_1 = tV$, que (V_1, W_1) est une base du sous-module $[V, W]$ de E et que le déterminant de (V_1, W_1) relatif à (e_1, e_2) est $t\delta$.

Inversement, soit (tV, W_1) un couple d'éléments de E vérifiant ces dernières conditions.

Alors W_1 est de la forme $sV + W$, ($s \in A$), et il est immédiat qu'il est associé à la solution (F, E', σ) et à la base (f, j_1) de F définie par $j = sf + tj_1$.

Il en résulte que les couples (V_1, δ_1) associés à (F, E', σ) et aux différentes bases de F sont les couples $(tV, t\delta)$ où t décrit l'ensemble des éléments inversibles de A .

- Soit (V, δ) un couple vérifiant les conditions du théorème et (F, E', σ) une solution du problème 2 associée à (V, δ) , alors les solutions associées à (V, δ) sont les triples $(\tau(F), \tau(E'), \tau \circ \sigma)$ où τ est un isomorphisme d'algèbres. Cela résulte immédiatement de la remarque 1, (lemme 1), et du lemme ci-dessous.

Lemme 4

Soient (E, Q) un A -module quadratique de base (e_1, e_2) telle que $Q(e_1) = a$, $Q(e_2) = c$, et $B_Q(e_1, e_2) = b$. On suppose qu'il existe δ , élément régulier de A , diviseur commun à a, b , et c , et $V \in E$ tels que $Q(V) = \delta^2$. Si deux couples (V, W) et (V, W') de déterminant δ vérifient les conditions du lemme 2, (V, W') est une base du sous-module $[V, W]$ de E et par suite les solutions associées à (V, W) et (V, W') coïncident.

Preuve

Soient $V = v_2 e_1 - v_1 e_2$, $W = -u_2 e_1 + u_1 e_2$ et $W' = -u'_2 e_1 + u'_1 e_2$ vérifiant les conditions indiquées. Puisque $\delta e_1 = u_1 V + v_1 W$ et $\delta e_2 = u_2 V + v_2 W$,

$\delta W' = (-u'_2 u_1 + u'_1 u_2) V + \delta W$. Pour que (V, W') soit une base du module $[V, W]$, il faut et il suffit que δ divise $-u'_2 u_1 + u'_1 u_2$.

Il suffit de prouver le lemme lorsque W est l'élément utilisé dans le lemme 3. Alors $u_2 = -c' v_2$, $u_1 = a' v_2 - b' v_1$ et $-u'_2 u_1 + u'_1 u_2 = -a' u'_2 v_2 + b' u'_2 v_1 - c' u'_1 v_1$.

Puisque W' vérifie les conditions du lemme 2 relativement à V et δ , on obtient, pour

$$\alpha' = -\frac{Q(W')}{\delta^2} \quad \text{et} \quad \beta' = \frac{B_Q(V, W')}{\delta^2}, \quad a = u_1^2 + \beta' u_1 v_1 - \alpha' v_1^2$$

$$c = u_2^2 + \beta' u_2 v_2 - \alpha' v_2^2, \quad b = 2 u_1 u_2 - 2 \alpha' v_1 v_2 + \beta' (u_1 v_2 - u_2 v_1)$$

En reportant ces valeurs dans $-a' u'_2 v_2 + b' u'_2 v_1 - c' u'_1 v_1$ on obtient

$$-a' u'_2 v_2 + b' u'_2 v_1 - c' u'_1 v_1 = -u'_1 u'_2 + \alpha' v_1 v_2 - \beta' u'_2 v_1.$$

Or le second membre de cette dernière équation est le second membre divisible par δ de l'équation (1) du système (2.1.1) pour les coefficients $v_1, v_2, u'_1, u'_2, \alpha'$ et β' relatifs à V et W' .

Il en résulte que (V, W) et (V, W') sont associés à une même solution, (cf. début de la partie 2), donc que les solutions associées à (V, W) et (V, W') coïncident.

Remarque 2

La solution, (définie à isomorphisme près), associée à un couple (V, δ) vérifiant les hypothèses du théorème 2.1.3 est la solution associée en particulier au couple (V, W) d'éléments de E où W est l'élément utilisé dans la preuve du lemme 3. Pour ce choix, $\alpha = -a'c'$ et $\beta = b'$. Dans la suite, sauf précision contraire, les couples (V, W) utilisés seront de ce type.

On utilisera la même notation (F, E', σ) pour désigner une solution associée à un couple (V, δ) et pour désigner la solution au sens du théorème associée à ce couple (les solutions isomorphes y ont été identifiées).

b) Etude des solutions du problème 2

1) Solutions correspondant à un diviseur δ fixé

Soit (E, Q) un A -module quadratique de base (e_1, e_2) telle que $Q(e_1) = a$, $Q(e_2) = c$ et $B_Q(e_1, e_2) = b$ et soit δ un élément régulier de A diviseur commun à a, b, c . On suppose qu'il existe deux éléments V et V_1 de E tels que $Q(V) = Q(V_1) = \delta^2$ et on désigne par W et W_1 les éléments associés respectivement à V et V_1 selon la remarque 2.

Deux cas peuvent se présenter :

1 - Il existe une transformation orthogonale ϕ de (E, Q) telle que $\phi(V) = V_1$ et $\phi(W) = W_1$. Alors, à (V, δ) et (V_1, δ) correspondent respectivement les solutions (F, E', σ) et (F, E', σ_1) où $\sigma = \sigma_1 \circ \phi$.

2 - Une telle transformation n'existe pas. Alors, à (V, δ) et (V_1, δ) correspondent les solutions (F, E', σ) et (F, E'_1, σ_1) où E' et E'_1 sont deux idéaux distincts d'une même algèbre F .

Preuve

Soient (V, W) et (V_1, W_1) les couples vérifiant les hypothèses de la proposition. Aux deux couples est associée une algèbre F , d'unité f , de base (f, j) telle que $j^2 = -a'c'f + b'j$, (a', b', c' quotients respectifs de a, b, c par δ).

On suppose qu'il existe une transformation orthogonale ϕ de (E, Q) telle que $\phi(V) = V_1$ et $\phi(W) = W_1$. Soit (F, E'_1, σ_1) une solution associée à (V_1, W_1) , alors $\sigma_1 \circ \phi$ est un isomorphisme quadratique de E sur E'_1 tel que $(\sigma_1 \circ \phi)(V) = \sigma_1(V_1) = \delta f$ et $(\sigma_1 \circ \phi)(W) = \sigma_1(W_1) = \delta j$. Donc $(F, E'_1, \sigma_1 \circ \phi)$ est une solution associée à (V, W) , (lemme 1).

Inversement, lorsqu'on peut associer aux couples (V, δ) et (V_1, δ) les solutions (F, E', σ) et (F, E', σ_1) avec le même idéal E' , $\sigma_1^{-1} \circ \sigma$ est une transformation orthogonale de (E, Q) telle que $(\sigma_1^{-1} \circ \sigma)(V) = \sigma_1^{-1}(\delta f) = V_1$, $(\sigma_1^{-1} \circ \sigma)(W) = \sigma_1^{-1}(\delta j) = W_1$ et

$$\sigma = \sigma_1 \circ (\sigma_1^{-1} \circ \sigma).$$

Une étude plus précise montre que le cas 2 peut effectivement se présenter (cf. thèse).

2) Etude des solutions associées à différents diviseurs communs à a, b et c

Si on envisage le cas particulier de deux diviseurs d et δ tels que δ divise d , on vérifie aisément le résultat ci-dessous :

Proposition 2.1.5

Soit (E, Q) un A -module quadratique de base (e_1, e_2) telle que $Q(e_1) = a$, $Q(e_2) = c$ et $B_Q(e_1, e_2) = b$ et d et δ deux éléments réguliers de A diviseurs communs à a, b, c tels que δ divise d . On suppose qu'il existe $V_\delta \in E$ tel que $Q(V_\delta) = \delta^2$. On pose $k = \frac{d}{\delta}$ et $V_d = k V_\delta$. Alors le couple (V_d, d) vérifie les conditions du théorème 2.1.3.

Soient (F_d, E'_d, σ_d) une solution associée à (V_d, d) , W_d l'élément de E associé à V_d selon la remarque 2, et (f_d, j_d) la base de F_d associée à (V_d, W_d) . Alors la sous-algèbre F_δ de F_d de base $(f_d, k j_d)$ forme avec E'_d et σ_d une solution associée à (V_δ, δ) .

Remarques

- Lorsqu'on identifie E à E'_d par σ_d , on munit E à la fois d'une structure d'idéal de F_d et d'une structure d'idéal de F_δ .

- La proposition 2.1.5 permet de ramener la recherche des solutions à la recherche des solutions associées au p.g.c.d de a, b, c lorsque A est un anneau factoriel.

§ 2 - Correspondances entre classes d'idéaux et classes de formes quadratiques binaires**Notations 2.2.1**

Soit E un A -module libre de rang 2. A toute forme quadratique définie sur E et à toute base de E correspond une forme quadratique binaire à coefficients dans A , c'est-à-dire une application de A^2 dans A de la forme $(x, y) \mapsto ax^2 + bxy + cy^2$, $(a, b, c) \in A^3$. Inversement, la donnée d'une telle application et d'une base de E détermine une forme quadratique définie sur E .

L'ensemble des formes quadratiques binaires à coefficients dans A est muni de la relation d'équivalence notée R définie comme suit :

$q R q' \iff$ (Pour tout A -module E libre de rang 2, il existe deux bases (e_1, e_2) et (e'_1, e'_2) de E telles que les formes quadratiques associées à $(q, (e_1, e_2))$ et $(q', (e'_1, e'_2))$ coïncident).

Une forme quadratique au sens du paragraphe 1 est une classe d'équivalence selon R , on la notera en général \bar{Q} au lieu de Q et on réservera la notation Q pour un élément de la classe d'équivalence.

Première correspondance**Notations 2.2.2**

On note Φ le sous-ensemble de l'ensemble des formes quadratiques binaires à coefficients dans A caractérisé par la propriété suivante :

Pour tout $Q \in \mathfrak{F}$, il existe d , élément régulier de A et des éléments a_1, b_1, c_1 de A tels que

$$1 \quad \forall (x,y) \in A^2, Q(x,y) = a x^2 + b xy + cy^2 = d(a_1 x^2 + 2 b_1 xy + c_1 y^2)$$

$$2 \quad \text{Il existe } (m,n) \in A^2 \text{ tel que } Q(m,n) = d^2$$

A chaque élément α de A , on fait correspondre le sous-ensemble \mathfrak{F}_α de \mathfrak{F} formé des éléments de \mathfrak{F} pour lesquels $b_1^2 - a_1 c_1 = \alpha$ pour un d convenable, et une algèbre quadratique F_α , d'unité f_α , de base (f_α, j_α) telle que $j_\alpha^2 = \alpha f_\alpha$.

On désigne par N_α la norme de F_α et par $S^{-1}F_\alpha$ l'algèbre obtenue par extension des scalaires à l'anneau total de fractions $S^{-1}A$ de A .

La relation R induit sur \mathfrak{F}_α une relation d'équivalence que l'on note aussi R .

Proposition 2.2.3

Soient $\alpha \in A$ et F_α et \mathfrak{F}_α définis comme ci-dessus. On considère sur l'ensemble I_α des idéaux de F_α qui sont libres de rang 2 la relation d'équivalence T_α définie comme suit :

$E' T_\alpha E'' \iff (E'' \text{ est homologue de } E' \text{ dans une transformation orthogonale de l'algèbre } S^{-1}F_\alpha)$

Alors, il existe une bijection de l'ensemble \mathfrak{F}_α/R sur l'ensemble I_α/T_α .

Preuve

Soit $Q \in \mathfrak{F}_\alpha$ et soit (E, \bar{Q}) un A -module quadratique de base (e_1, e_2) où \bar{Q} est définie sur E par $\bar{Q}(x e_1 + y e_2) = Q(x,y)$. Par hypothèse, il existe un élément régulier d de A , des éléments a_1, b_1, c_1 de A tels que $\bar{Q}(e_1) = d a_1, \bar{Q}(e_2) = d c_1, B\bar{Q}(e_1, e_2) = 2 d b_1$ et $b_1^2 - a_1 c_1 = \alpha$, et $(m,n) \in A^2$ tel que $d^2 = Q(m,n) = \bar{Q}(m e_1 + n e_2)$.

Soit $V = m e_1 + n e_2$, alors le couple (V,d) vérifie les hypothèses du théorème 2.1.3 et l'algèbre F_α est l'algèbre d'une solution du problème 2 associée à (V,d) . En effet, puisqu'elle admet la base (f_α, j_α) où f_α est l'unité et $j_\alpha^2 = \alpha f_\alpha$ avec $\alpha = b_1^2 - a_1 c_1$, elle admet aussi la base (f_α, j'_α) où $j'_\alpha = b_1 f_\alpha - j_\alpha$ et $j_\alpha'^2 = -a_1 c_1 f_\alpha + 2 b_1 j'_\alpha$ qui est la base associée au couple (V,W) , (§ 1, remarque 2). Il existe donc un idéal E' de F_α possédant une base (e'_1, e'_2) telle que, pour tout $(x,y) \in A^2, Q(x,y) = \bar{Q}(x e_1 + y e_2) = N_\alpha(x e'_1 + y e'_2)$.

Les idéaux de F_α qui vérifient cette propriété sont les idéaux homologues de E' dans une transformation orthogonale de l'algèbre $S^{-1}F_\alpha$, (prop. 2.1.2).

Inversement, soit E' un idéal de F_α libre de rang 2. La norme N_α induit une forme quadratique sur E' à laquelle correspond une forme quadratique binaire appartenant à Φ_α dès qu'une base est fixée. En effet, pour toute base (e'_1, e'_2) de E' , le déterminant δ de (e'_1, e'_2) relatif à (f_α, j_α) divise $N_\alpha(x e'_1 + y e'_2)$ pour tout $(x, y) \in A^2$. Avec les notations du système (2.1.1), $(e'_1 = u_1 f_\alpha + v_1 j_\alpha, e'_2 = u_2 f_\alpha + v_2 j_\alpha)$, δ divise $u_1 u_2 - \alpha v_1 v_2$ puisque $\beta = 0$. Comme $B_{N_\alpha}(e'_1, e'_2) = 2(u_1 u_2 - \alpha v_1 v_2)$, B_{N_α} est un multiple de 2δ . De plus, comme $v_2 e'_1 - v_1 e'_2 = \delta f_\alpha$, $N_\alpha(v_2 e'_1 - v_1 e'_2) = \delta^2$. Donc la forme Q définie par $Q(x, y) = N_\alpha(x e'_1 + y e'_2)$ pour tout $(x, y) \in A^2$, appartient à Φ_α .

Les formes quadratiques binaires associées aux différentes bases de E sont les éléments d'une classe d'équivalence selon R .

Il existe donc une bijection de Φ_α/R sur I_α/T_α .

Deuxième correspondance

A chaque élément α de A , on associe l'ensemble Φ_α^1 des formes quadratiques à coefficients dans A de la forme $(x, y) \mapsto a_1 x^2 + 2b_1 xy + c_1 y^2$ qui représentent au moins un élément régulier de A et telles que $b_1^2 - a_1 c_1 = \alpha$, et l'algèbre F_α précédente (notations 2.2.2).

Soit $Q_1 \in \Phi_\alpha^1$. A chaque élément régulier d de A représenté par Q_1 , on fait correspondre la forme $d Q_1$ et les idéaux E de F_α possédant une base (e_1, e_2) de déterminant d , (relatif à (f_α, j_α)), telle que, $\forall (x, y) \in A^2$, $N_\alpha(x e_1 + y e_2) = d Q_1(x, y)$. Il existe au moins un tel idéal E car la forme $d Q_1$ est un élément de Φ_α (correspondance précédente).

Soit E l'un de ces idéaux. Un idéal E' de F_α est associé à Q_1 par l'intermédiaire de la forme $d Q_1$ si et seulement si il existe une base (e'_1, e'_2) de E' de déterminant d relativement à (f_α, j_α) telle que : $\forall (x, y) \in A^2$, $d' N_\alpha(x e'_1 + y e'_2) = d' d Q_1(x, y) = d N_\alpha(x e'_1 + y e'_2)$.

On vérifie facilement qu'une base (e'_1, e'_2) de déterminant d' , (relatif à (f_α, j_α)), d'un idéal E' de F_α libre de rang 2 vérifie cette propriété si et seulement si l'automorphisme σ_0 de $S^{-1}F_\alpha$ qui prolonge l'isomorphisme σ de E sur E' défini par $\sigma(e_1) = e'_1$ et $\sigma(e_2) = e'_2$ peut être mis sous la forme $m_f \circ \tau_0$ où f est un élément de $S^{-1}F_\alpha$ de norme $d' d^{-1}$ et τ_0 un automorphisme de déterminant 1 de l'algèbre $S^{-1}F_\alpha$ (on utilise la proposition 2.1.2).

Lorsque 2 est régulier ou lorsque l'anneau A est intègre, τ_0 est l'identité comme le montre

immédiatement l'étude du système 1.2.7 lorsque $\beta = 0$.

Inversement, soit E un idéal de F_α libre de rang 2. Une base (e_1, e_2) de E étant choisie, on lui associe une forme Q appartenant à Φ_α selon la correspondance précédente et la forme $Q_1 = Q/d$ associée où d désigne le déterminant de (e_1, e_2) relatif à (f_α, j_α) . Il est immédiat que Q_1 appartient à Φ_α^1 .

Lorsqu'on choisit une autre base (e'_1, e'_2) de déterminant d' , on obtient une forme Q' équivalente à Q selon R et la forme $Q'_1 = Q'/d'$ associée. Soit u le déterminant de (e'_1, e'_2) relatif à (e_1, e_2) . Puisque $d' = du$, $u Q'_1 = Q/d$. On voit que, de même que Q et Q' , les formes $Q_1 = Q/d$ et $u Q'_1 = Q/d$ sont associées à une même forme quadratique sur E et aux bases (e_1, e_2) et (e'_1, e'_2) respectivement. De plus, u est le déterminant du changement de base $(e_1, e_2) \mapsto (e'_1, e'_2)$. On résume cette propriété en disant que $u Q'_1$ est équivalente à Q_1 selon R par l'intermédiaire d'un changement de base de déterminant u .

Inversement, toute forme Q'_1 qui appartient à Φ_α^1 et qui vérifie cette dernière propriété correspond de même que Q_1 à une base de E comme on le vérifie aisément.

Théorème 2.2.4

On garde les notations 2.2.2. Soit α un élément de A .

On considère sur l'ensemble I_α des idéaux de F_α qui sont libres de rang 2 la relation binaire T_1 définie comme suit :

$E T_1 E' \iff (E'$ est homologue de E dans un isomorphisme dont l'extension à $S^{-1}F_\alpha$ est de la forme $m_f \circ \tau_0$ où m_f est la multiplication par un élément de $S^{-1}F_\alpha$ et τ_0 un automorphisme de déterminant 1 de l'algèbre $S^{-1}F_\alpha$).

De même, on considère sur l'ensemble Φ_α^1 des formes quadratiques binaires $(x, y) \mapsto a_1 x^2 + 2b_1 xy + c_1 y^2$, $(a_1, b_1, c_1 \in A)$, telles que $b_1^2 - a_1 c_1 = \alpha$ et qui représentent au moins un élément régulier de A la relation binaire R_1 définie comme suit :

$Q_1 R_1 Q'_1 \iff$ (il existe un élément inversible u de A tel que $u Q'_1$ soit une forme équivalente à Q_1 selon R obtenue par l'intermédiaire d'un changement de base de déterminant u).

Alors T_1 et R_1 sont des relations d'équivalence et il existe une bijection de I_α/T_1 sur Φ_α^1/R_1 .

Il est facile de vérifier que T_1 et R_1 sont des relations d'équivalence. Le théorème

résulte alors de l'étude précédente.

Remarque

Lorsque 2 est régulier ou lorsque A est intègre, T_1 est définie par

$$E T_1 E' \iff (\exists f' \in S^{-1}F_\alpha \text{ tel que } E' = f'E)$$

(En effet, dans ce cas τ_0 est l'identité sur $S^{-1}F_\alpha$)

Cas particuliers

a) On suppose que l'anneau A est principal.

Le produit de deux idéaux de F_α libres de rang 2 est un idéal libre de rang 2, (étude p. 11), Puisque A est intègre, T_1 est définie comme dans la remarque ci-dessus, elle est donc compatible avec la multiplication des idéaux. On peut alors munir l'ensemble $\mathfrak{F}_\alpha^1/R_1$ d'une structure de monoïde par l'intermédiaire de la bijection du théorème 2.2.4.

b) On suppose que A est principal, que 2 est inversible dans A et que α est sans facteurs carrés

La norme N_α ne s'annule pas sur $F_\alpha - \{0\}$ donc F_α est intègre, de corps des fractions $S^{-1}F_\alpha$ (prop. 1.2.1, remarque 2). De plus, F_α est intégralement clos. En effet, les hypothèses impliquent que tout $X_0 \in S^{-1}F_\alpha$, tel que $N_0(X_0)$ et $B_{N_0}(X_0, f_\alpha)$ soient des éléments de A, appartient à F_α . Donc F_α est un anneau de Dedekind (B.A.C ch. VII, § 2). Puisque N_α ne s'annule pas sur $F_\alpha - \{0\}$, I_α est l'ensemble des idéaux non nuls de F_α (étude p. 11). D'autre part, T_1 a la forme simplifiée précédente.

L'ensemble I_α/T_1 peut alors être identifié au groupe des classes d'idéaux fractionnaires de F_α modulo le groupe des idéaux principaux et l'ensemble $\mathfrak{F}_\alpha^1/R_1$ est muni d'une structure de groupe par l'intermédiaire de la bijection précédente.

c) On suppose que $A = \mathbb{Z}$, que $\alpha \equiv 2$ ou $3 \pmod{4}$ et que α est sans facteurs carrés

F_α s'identifie à l'anneau des entiers du corps $\mathbb{Q}(\sqrt{\alpha})$. La correspondance entre classes d'idéaux de F_α et classes de formes quadratiques binaires de discriminant 4α donnée par le théorème 2.2.4 n'est pas exactement la correspondance donnée par exemple par Hecke ([3] § 53), (voir aussi [1]), mais on peut déduire cette correspondance de la correspondance du théorème 2.2.4.

Comparaison des deux correspondances

1 - Correspondance du théorème 2.2.4

- L'ensemble d'idéaux est l'ensemble I_α des idéaux $\neq (0)$ de F_α . Il est muni de la relation d'équivalence T_1 définie comme suit :

$E T_1 E' \iff (\exists f' \in \mathbb{Q}(\sqrt{\alpha}) \text{ tel que } E' = f'E)$

- L'ensemble de formes est l'ensemble Φ_α^1 des formes quadratiques binaires à coefficients dans \mathbb{Z} de discriminant 4α . Il est muni de la relation d'équivalence R_1 définie comme suit :

$Q_1 R_1 Q'_1 \iff (Q'_1 \text{ est équivalente à } Q_1 \text{ selon } R \text{ (équivalence ordinaire), par l'intermédiaire d'un changement de base de déterminant } 1 \text{ ou } -Q'_1 \text{ est équivalente à } Q_1 \text{ selon } R \text{ par l'intermédiaire d'un changement de base de déterminant } -1)$

En écriture abrégée : $Q_1 R_1 Q'_1 \iff \begin{pmatrix} Q_1 R Q'_1 & \text{ou } Q_1 R \cdot Q'_1 \\ \text{dét } 1 & \text{dét } -1 \end{pmatrix}$

- Soit E un élément de I_α , la classe de formes associée à la classe de E est l'ensemble des formes Q_1 définies comme suit :

A chaque base (e_1, e_2) de E , on associe la forme $Q_1 : (x, y) \mapsto \frac{N_\alpha(x e_1 + y e_2)}{\delta}$

où δ est le déterminant de (e_1, e_2) relatif à la base $(1, \sqrt{\alpha})$ de F_α .

2 - Correspondance de Hecke

- L'ensemble d'idéaux est l'ensemble I_α , il est muni de la relation d'équivalence T_2 définie comme suit :

$E T_2 E' \iff (\exists f' \in \mathbb{Q}(\sqrt{\alpha}) \text{ tel que } E' = f'E \text{ et } N_\alpha(f') > 0) \text{ (relation restreinte)}$

Il est immédiat que sur I_α , $E T_2 E'$ implique $E T_1 E'$.

- Lorsque $\mathbb{Q}(\sqrt{\alpha})$ est réel, ($\alpha > 0$), l'ensemble de formes est l'ensemble Φ_α^1 précédent. Lorsque $\mathbb{Q}(\sqrt{\alpha})$ est imaginaire, l'ensemble de formes est la partie de Φ_α^1 constituée par les formes définies positives de Φ_α^1 .

Dans les deux cas, l'ensemble de formes est muni de la relation d'équivalence R_2 définie comme suit :

$Q_1 R_2 Q'_1 \iff Q_1 R Q'_1 \quad (\text{relation restreinte})$
dét 1

Il est immédiat que sur Φ_α^1 , $Q_1 R_2 Q'_1$ implique $Q_1 R_1 Q'_1$.

- Soit E un élément de I_α , la classe de formes associée à la classe de E est l'ensemble des formes Q_1 définies comme suit :

A chaque base (e_1, e_2) de E telle que $\frac{e_1 \bar{e}_1 - e_2 \bar{e}_2}{\sqrt{4\alpha}}$ soit > 0 où \bar{e}_1 et \bar{e}_2 désignent les

conjugués de e_1 et e_2 , (c'est-à-dire telle que le déterminant δ de (e_1, e_2) soit < 0), on associe

la forme $Q_1 : (x,y) \mapsto \frac{N_\alpha (x e_1 + y e_2)}{|\delta|}$

Une étude plus précise (cf. thèse) montre que :

a) Les relations R_1 et R_2 sont identiques sur \mathbb{F}_α^1 si et seulement si le corps $\mathbb{Q}(\sqrt{\alpha})$ contient une unité (élément inversible de F_α) de norme -1.

b) Soient E un élément de $I_\alpha(e_1, e_2)$ une base de E de déterminant $\delta < 0$ et

$Q_1 : (x,y) \mapsto \frac{N_\alpha (x e_1 + y e_2)}{\delta}$, alors Q_1 est une des formes associées à E par le théorème

2.2.4 et $-Q_1$ est une des formes associées par Hecke à l'idéal E . Les classes selon R_1 des formes Q_1 et $-Q_1$ sont confondues si et seulement si tout idéal conjugué d'un élément de la classe de E selon T_1 appartient aussi à cette classe.

Ces remarques permettent d'étudier les différents cas et de retrouver la correspondance de Hecke à partir de la correspondance du théorème 2.2.4.

Chapitre III

Q - algèbres générales§ 1 - Problèmes préliminaires - Premières propriétés

Une A-algèbre E d'unité e est une Q-algèbre pour une forme quadratique Q définie sur E si et seulement si

$$Q(e) = 1 \text{ et } \forall X \in E, X^2 = -Q(X)e + B_Q(X,e)X.$$

Il peut arriver qu'une Q-algèbre E puisse être munie d'une forme quadratique Q' distincte de Q telle que E soit une Q'-algèbre.

Exemple

On suppose que A n'est pas réduit. Soient $a \in A - \{0\}$ tel que $a^2 = 0$, F une algèbre quadratique sur A, d'unité e, de base (e, j), de norme Q telle que $Q(j) = -a$ et $B_Q(e, j) = 2$, et E la sous-algèbre monogène de F engendrée par a, j (alors $E = Ae \oplus Aaj$). On note encore Q la restriction de Q à E. Alors E est une Q-algèbre. On munit E de la forme quadratique Q' définie par $Q'(e) = 1$, $Q'(aj) = 0$ et $B_{Q'}(aj, e) = 3a$. Pour tout élément $X = xe + yaj$ de E, ($x, y \in A$) on a

$$X^2 = -Q(X)e + B_Q(X,e)X = -(x^2 + 2xya)e + (2x + 2ay)(xe + yaj)$$

et puisque $a^2 = 0$,

$$X^2 = -(x^2 + 3ayx)e + (2x + 3ay)(xe + yaj) = -Q'(X)e + B_{Q'}(X,e)X.$$

Dans cet exemple, E est à la fois une Q-algèbre et une Q'-algèbre et $Q' \neq Q$. Toutefois :

Proposition 3.1.1

Soient E une A-algèbre, Q et Q' deux formes quadratiques définies sur E telles que E soit à la fois une Q-algèbre et une Q'-algèbre.

Lorsque l'une des propriétés 1 et 2 ci-dessous est vérifiée, $Q = Q'$.

1-E possède une base contenant l'unité e.

2-A est réduit.

Preuve

1- On suppose que 1 est vérifié. Soit $(e_i)_{i \in I}$ une base de E contenant l'unité e. Alors

$Q(e) = 1 = Q'(e)$. Pour tout élément e_i de la base, distinct de e,

$$e_i^2 = -Q(e_i)e + B_Q(e_i,e)e_i = -Q'(e_i)e + B_{Q'}(e_i,e)e_i, \text{ donc } Q(e_i) = Q'(e_i) \text{ et}$$

$$B_Q(e_i,e) = B_{Q'}(e_i,e).$$

Pour tout couple (e_i, e_j) d'éléments de la base, distincts de e,

$$(e_i + e_j)^2 = -Q(e_i + e_j)e + B_Q(e_i + e_j, e)(e_i + e_j)$$

$$(e_i + e_j)^2 = -Q'(e_i + e_j)e + B_{Q'}(e_i + e_j, e)(e_i + e_j)$$

d'où, compte tenu des relations précédentes, $B_Q(e_i, e_j) = B_{Q'}(e_i, e_j)$.

Donc $Q(X) = Q'(X)$ pour tout $X \in E$.

2 - On suppose que A est réduit.

$$\begin{aligned} \text{Puisque } \forall X \in E, X^2 &= -Q(X)e + B_Q(X, e)X = -Q'(X)e + B_{Q'}(X, e)X, \\ (Q(X) - Q'(X))e &= (B_Q(X, e) - B_{Q'}(X, e))X \end{aligned}$$

On en déduit, compte tenu des relations $B_Q(e, e) = B_{Q'}(e, e) = 2$ et $Q(e) = 1$,

$$(Q(X) - Q'(X))^2 = (B_Q(X, e) - B_{Q'}(X, e))^2 Q(X)$$

$$2(Q(X) - Q'(X)) = (B_Q(X, e) - B_{Q'}(X, e)) B_Q(X, e)$$

$$2(Q(X) - Q'(X)) = (B_Q(X, e) - B_{Q'}(X, e)) B_{Q'}(X, e)$$

d'où $(B_Q(X, e) - B_{Q'}(X, e))^2 = 0$ et puisque A est réduit, $B_Q(X, e) - B_{Q'}(X, e) = 0$ et $Q(X) = Q'(X)$.

Exemple : Les algèbres de Cayley sont des Q-algèbres pour la norme cayleyenne et vérifient la condition 1 de la proposition, chacune d'elles ne peut être une Q-algèbre que pour une seule forme Q.

Soit E une Q-algèbre sur A d'unité e. Tout élément X de E vérifie une équation de dépendance intégrale de degré 2. Une algèbre vérifiant cette dernière condition n'est pas nécessairement une Q-algèbre, toutefois :

Théorème 3.1.2

Soit E une A-algèbre d'unité e. On suppose que 2 est régulier dans A et que l'une des conditions 1 et 2 ci-dessous est vérifiée.

1-E possède une base contenant l'unité

2-A est intègre, E de rang ≥ 2 .

Alors, pour qu'il existe une forme quadratique Q définie sur E telle que E soit une Q-algèbre, il faut et il suffit que tout élément X de E vérifie une équation de la forme

$$(1) \quad X^2 = \alpha(X)e + \beta(X)X, \quad (\alpha(X), \beta(X) \in A).$$

Preuve

- On vient de voir que cette condition est nécessaire

- On suppose maintenant que tout élément X de E vérifie une équation de la forme (1) et que 2 est régulier dans A. On va montrer que lorsque de plus 1 ou 2 est vérifié, il existe une forme Q (nécessairement unique d'après la proposition 3.1.1), telle que E soit une Q-algèbre.

1 - On suppose que E possède une base $(e_i)_{i \in I}$ contenant e

Le résultat est déjà connu lorsque Card I \leq 2. On suppose Card I $>$ 2. Soit $e_{i_0} = e$.

On pose $\alpha_{i_0} = -1$, $\beta_{i_0} = 2$ et pour tout $i \in I - \{i_0\}$, $\alpha_i = \alpha(e_i)$ et $\beta_i = \beta(e_i)$. Pour tout couple (i, j) d'éléments de $I - \{i_0\}$ où $i \neq j$, on pose $\alpha(e_i + e_j) = \gamma_{ij}$ et

$$\beta(e_i + e_j) = \delta_{ij}$$

$$\text{Alors, } e_i e_j + e_j e_i = (e_i + e_j)^2 - e_i^2 - e_j^2 = (\gamma_{ij} - \alpha_i - \alpha_j)e + (\delta_{ij} - \beta_i)e_i + (\delta_{ij} - \beta_j)e_j$$

et, quels que soient les éléments a, a_i , a_j de A,

$$(2) \quad (a e + a_i e_i + a_j e_j)^2 = k e + l(a e + a_i e_i + a_j e_j)$$

où on a posé $k = \alpha(ae + a_i e_i + a_j e_j)$ et $l = \beta(ae + a_i e_i + a_j e_j)$.

k et l dépendent de i, j, a, a_i , a_j .

En identifiant dans les deux membres de (2) les coefficients de e_i et ceux de e_j pour $a_i = 1$ et $a_j = -1$, on obtient après réduction

$$2 \beta_i + 2 a - \delta_{ij} = 1 = -(2 \beta_j - 2 a - \delta_{ij}) \text{ et puisque 2 est régulier, } \delta_{ij} = \beta_i + \beta_j.$$

On considère maintenant la forme quadratique Q définie comme suit sur E :

Pour tout $i \in I$, on pose $Q(e_i) = -\alpha_i$ et $B_Q(e_i, e) = \beta_i$. Pour tout couple (i, j) d'éléments de $I - \{i_0\}$ tel que $i \neq j$, on pose $B_Q(e_i, e_j) = \alpha_i + \alpha_j - \gamma_{ij}$.

Alors pour tout élément X de E, $X^2 = -Q(X)e + B_Q(X, e)X$. En effet :

Soit $X = a e + \sum_{i \in L} a_i e_i$, ($a, a_i \in A$, L fini, $L \subset I - \{i_0\}$).

Puisque pour $i, j \in L$ et $i \neq j$, $\delta_{ij} = \beta_i + \beta_j$,

$$X^2 = a^2 e + \sum_{i \in L} a_i^2 (\alpha_i e + \beta_i e_i) + 2 a \sum_{i \in L} a_i e_i + \sum_{\substack{i, j \in L \\ i \neq j}} a_i a_j [(\gamma_{ij} - \alpha_i - \alpha_j)e + \beta_j e_i + \beta_i e_j]$$

$$\begin{aligned}
X^2 = & - \left[a^2 \cdot \sum_{i \in L} a_i^2 \alpha_i + a \sum_{i \in L} a_i \beta_i + \sum_{\substack{ij \in L \\ i \neq j}} a_i a_j (\alpha_i + \alpha_j - \gamma_{ij}) \right] e + \\
& + (2a^2 + a \sum_{i \in L} a_i \beta_i) e + 2a \sum_{i \in L} a_i e_i + \sum_{i \in L} a_i^2 \beta_i e_i + \sum_{\substack{ij \in L \\ i \neq j}} a_i a_j (\beta_i e_j + \beta_j e_i) \\
X^2 = & - Q(ae + \sum_{i \in L} a_i e_i) e + B_Q(ae + \sum_{i \in L} a_i e_i, e) (ae + \sum_{i \in L} a_i e_i)
\end{aligned}$$

Donc E est une Q-algèbre.

2 - On suppose que A est intègre, ($2 \neq 0$), et E de rang ≥ 2

Comme dans les chapitres précédents, on note E_0 l'algèbre obtenue par extension des scalaires au corps des fractions A_0 de A et f_0 le morphisme canonique de E dans E_0 . L'algèbre E_0 possède une base contenant l'unité $f_0(e)$. Pour tout élément $f_0(X)$ de $f_0(E)$,

$(f_0(X))^2 = \alpha(X) f_0(e) + \beta(X) f_0(X)$, donc tout élément de E_0 vérifie une équation du même type à coefficients dans A_0 . Il existe donc une forme quadratique Q_0 telle que E_0 soit une Q_0 -algèbre (cas 1). Pour tout $X \in E$, on pose $Q(X) = Q_0(f_0(X))$.

On va montrer que Q est une forme quadratique définie sur E et que E est une Q-algèbre.

Puisque E est de rang ≥ 2 , tout élément de E appartient à une sous-algèbre de rang 2.

On est amené à étudier d'abord le problème pour les algèbres de rang 2.

Lemme 1 (cas où E est sans torsion ; E s'identifie à son image canonique dans E_0)

Soit E une algèbre sans torsion de rang 2 sur A, d'unité e. On suppose que tout élément de E vérifie une équation de la forme (1).

Alors, E est une N-algèbre pour la restriction N de la norme N_0 de l'algèbre E_0 à E.

Preuve

Il suffit de montrer que N est à valeurs dans A.

Tout élément X de E est solution dans E_0 des deux équations

$$X^2 = \alpha(X) e + \beta(X) X$$

$$X^2 = -N_0(X) e + B_{N_0}(X, e) X$$

Lorsque e et X forment une base de E_0 , $\alpha(X) = -N_0(X)$ et $\beta(X) = B_{N_0}(X, e)$.

En particulier, $N_O(X)$ appartient à A .

Remarque : $\forall k \in A_O - \{0\}$, e et kX forment une base de E_O et lorsque kX est un élément de E , $\beta(kX) = B_{N_O}(kX, e) = k B_{N_O}(X, e) = k \beta(X)$.

Lorsque e et X ne forment pas une base de E_O , X est de la forme $\frac{a}{b} e$, $((a,b) \in A^2, b \neq 0)$,

et $N_O(X) = \frac{a^2}{b^2}$. Lorsque $a = 0$, $N_O(X) = 0$. On suppose maintenant $a \neq 0$.

Soit $Y \in E$ tel que e et Y forment une base de E_O .

$$(Y + \frac{a}{b} e)^2 = \alpha(Y) e + \beta(Y) Y + 2 \frac{a}{b} Y + \frac{a^2}{b^2} e$$

$$\text{et } (Y + \frac{a}{b} e)^2 = \alpha(Y + \frac{a}{b} e) e + \beta(Y + \frac{a}{b} e) (Y + \frac{a}{b} e)$$

$$\text{d'où } \alpha(Y) + \frac{a^2}{b^2} = \alpha(Y + \frac{a}{b} e) + \frac{a}{b} \beta(Y + \frac{a}{b} e) \text{ et } \beta(Y) + 2 \frac{a}{b} = \beta(Y + \frac{a}{b} e)$$

On en déduit :

$$\alpha(Y) - \alpha(Y + \frac{a}{b} e) - \frac{a}{b} \beta(Y) = \frac{a^2}{b^2}$$

$\alpha(Y)$ et $\alpha(Y + \frac{a}{b} e)$ appartiennent à A . D'autre part, e et $\frac{a}{b} Y$ forment une base de E_O

et $\frac{a}{b} Y$ appartient à E donc, d'après la remarque précédente, $\beta(\frac{a}{b} Y) = \frac{a}{b} \beta(Y)$ et

$\frac{a}{b} \beta(Y)$ est un élément de A . Il en résulte que $\frac{a^2}{b^2}$ appartient à A .

Lemme 2 (cas où le sous-module de torsion T peut être $\neq (0)$)

Soit E une algèbre de rang 2 sur A , d'unité e . On suppose que tout élément X de E vérifie une équation de la forme (1).

Alors, il existe une forme quadratique N telle que E soit une N -algèbre. N est l'unique forme quadratique définie sur E dont l'extension à E_O est la norme de E_O .

Preuve

$f_O(E)$ est sans torsion de rang 2 sur A et tout élément de $f_O(E)$ vérifie une équation de la forme (1), donc la restriction à $f_O(E)$ de la norme N_O de E_O est à valeurs dans A . Pour tout $X \in E$, on pose $N(X) = N_O(f_O(X))$. L'application N ainsi définie est l'unique forme quadratique définie sur E dont l'extension à E_O est N_O . Il reste à montrer que E est une N -algèbre.

$$\forall X \in E, (f_0(X))^2 = \alpha(X) f_0(e) + \beta(X) f_0(X)$$

$$(f_0(X))^2 = -N(X) f_0(e) + B_N(X,e) f_0(X)$$

- Lorsque $f_0(X)$ et $f_0(e)$ forment une base de E_0 ,

$$N(X) = -\alpha(X) \text{ et } B_N(X,e) = \beta(X). \text{ Donc } X^2 = -N(X)e + B_N(X,e)X.$$

- Lorsque $f_0(e)$ et $f_0(X)$ ne forment pas une base de E_0 et que $X \notin T$

Il existe $a, b \in A - \{0\}$ tels que $bX = ae$. Soit $Y \in E$ tel que $(f_0(e), f_0(Y))$ soit une base de E_0 , alors $(f_0(e), f_0(X + bY))$ est aussi une base de E_0 .

On a d'une part, compte tenu de l'équation $bX = ae$,

$$(3) (X + bY)^2 = X^2 + b^2 Y^2 + (bY)X + X(bY) = X^2 + b^2 Y^2 + 2aY$$

et d'autre part,

$$(X + bY)^2 = -N(X + bY)e + B_N(X + bY,e)(X + bY)$$

et après réduction, compte tenu des relations $ae - bX = 0$ et $Y^2 = -N(Y)e + B_N(Y,e)Y$,

$$(4) (X + bY)^2 = -N(X)e + B_N(X,e)X + b^2 Y^2 + 2aY$$

et (3) et (4) impliquent $X^2 = -N(X)e + B_N(X,e)X$

- En particulier, pour tout élément Z du sous-module de torsion T ,

$$(e + Z)^2 = -N(e + Z)e + B_N(e + Z,e)(e + Z) = e + 2Z$$

ce qui implique $Z^2 = 0$ c'est-à-dire $Z^2 = -N(Z)e + B_N(Z,e)Z$.

Cas général : E de rang quelconque ≥ 2 .

On a posé pour tout $X \in E$, $Q(X) = Q_0(f_0(X))$ où Q_0 désigne l'unique forme quadratique définie sur E_0 telle que E_0 soit une Q_0 -algèbre.

Soit X un élément de E et soit F une sous-algèbre de rang 2 de E qui contient X . La restriction de Q_0 à F_0 coïncide avec la norme N_0 de F_0 et $\forall Y \in F$,

$N(Y) = N_0 f_0(Y) = Q_0(f_0(Y)) = Q(Y)$ où N est l'unique forme quadratique définie sur F dont l'extension à F_0 est N_0 (lemme 2). En particulier, la restriction de Q à F est à valeurs dans A

et $X^2 = -Q(X)e + B_Q(X,e)X$ (lemme 2). Donc E est une Q -algèbre.

Remarques

1 - L'hypothèse «2 régulier» n'est pas superflue.

Exemple

A est le corps à deux éléments, E une A -algèbre de base (e_1, e_2, e) d'unité e telle que

$$e_1^2 = e_2^2 = 0, e_1 e_2 = e_1 \text{ et } e_2 e_1 = e_2. \text{ Alors, } (e + e_1)^2 = e, (e + e_2)^2 = e,$$

$$(e + e_1 + e_2)^2 = e + e_1 + e_2 \text{ et } (e_1 + e_2)^2 = e_1 + e_2.$$

Tout élément X de E vérifie donc une équation de la forme (1) mais il n'existe pas de forme quadratique Q telle que E soit une Q -algèbre. En effet :

$$(e_1^2 = 0 \text{ et } e_2^2 = 0) \Rightarrow B_Q(e_1, e) = B_Q(e_2, e) = 0$$

$$(e_1 + e_2)^2 = e_1 + e_2 \Rightarrow B_Q(e_1 + e_2, e) = 1$$

ce qui est incompatible avec la bilinéarité de B_Q .

2 - Toute algèbre unitaire projective de rang 2 est une Q -algèbre (corollaire de la proposition 1.1.1).

Une algèbre non projective et de rang 2 sur un anneau intègre n'est pas nécessairement une Q -algèbre.

Exemple

Soit E_0 l'algèbre quadratique sur \mathbb{Q} d'unité e , de base (e, i) telle que $i^2 = \frac{1}{4} e$, et soit E

la sous \mathbb{Z} -algèbre monogène de E_0 engendrée par i . Alors E est sans torsion de rang 2 sur \mathbb{Z} et toute forme quadratique Q telle que E soit une Q -algèbre est la restriction à E de la norme N_0 de E_0 . Comme $N_0(i) = -\frac{1}{4}$, cette restriction n'est pas à valeurs dans \mathbb{Z} .

3 - Un module sur un anneau intègre dans lequel 2 n'est pas inversible, muni d'une forme quadratique Q qui représente 1, ne peut pas toujours être muni d'une structure de Q -algèbre même lorsqu'il est de rang 2. Le théorème 1.1.2 ne s'étend pas à ces modules quadratiques.

Exemple

Soit A l'ordre du corps quadratique $\mathbb{Q}(\sqrt{3})$ de conducteur 2 (alors $A_0 = \mathbb{Q}(\sqrt{3})$), et soient E_0 un A_0 -module de base (e, i) muni de la forme quadratique Q_0 définie par $Q_0(e) = 1$, $B_{Q_0}(e, i) = 0$ et $Q_0(i) = 3$, et E le sous- A -module de E_0 engendré par $e, i, \sqrt{3} i$. On montre facilement que Q_0 induit une forme quadratique Q sur le A -module E et que les seules solutions dans E de l'équation $Q(X) = 1$ sont $X = e$ et $X = -e$. La multiplication de l'algèbre quadratique $(E_0)_e$, (resp. $(E_0)_{-e}$), d'unité e (resp. $-e$), et de norme Q_0 n'induit pas une loi interne sur E (pour $X = i$ et $X' = \sqrt{3} i$, $XX' = -3\sqrt{3} e$ (resp. $3\sqrt{3} e$)). Il n'y a donc pas de structure de Q -algèbre sur (E, Q) .

Premières propriétés d'une Q -algèbre

Dans la fin de ce paragraphe 1, E désigne une Q -algèbre d'unité e sur un anneau commutatif unitaire A .

E n'est pas nécessairement associative (les algèbres de Cayley de dimension 8 ne sont pas associatives), toutefois :

Proposition 3.1.3

Chaque sous-algèbre monogène de E est associative et commutative.

Preuve (voir aussi [1] pour les algèbres sur des corps)

Soit X un élément de E, alors $X^2 = -Q(X)e + B_Q(X, e)X$. On pose $Q(X) = -a$ et $B_Q(X, e) = b$; X^2 est de la forme $x_2 e + y_2 X$, $X^2 X = a y_2 e + (x_2 + b y_2)X = X X^2$. On note X^3 cette valeur commune qui est de la forme $x_3 e + y_3 X$.

- Hypothèse de récurrence. On suppose que

1 X^k est défini pour tout entier $k \in \{1, \dots, n\}$ (c'est-à-dire que pour k fixé tous les produits formés avec k éléments égaux à X ont la même valeur).

2 Pour tout entier $k \in \{1, \dots, n\}$, il existe x_k et $y_k \in A$ tels que,

$$\forall k \leq n, \quad X^k = x_k e + y_k X$$

$$\forall k < n, \quad X^{k+1} = a y_k e + (x_k + b y_k) X$$

- Alors X^{n+1} est défini et l'hypothèse 2 est vérifiée pour tout entier $k \in \{1, \dots, n+1\}$.

En effet :

Pour montrer que X^{n+1} est défini, il suffit de montrer, compte tenu de l'hypothèse de récurrence, que pour tous entiers r et p tels que $1 \leq r \leq n-1$, $1 \leq p \leq n-1$ et $r+p = n$, on a $X^r X^{p+1} = X^{r+1} X^p$.

- Puisque $p < n$ et $r < n$

$$X^{p+1} = a y_p e + (x_p + b y_p)X, \quad X^{r+1} = a y_r e + (x_r + b y_r) X$$

$$X^r X^{p+1} = [x_r e + y_r X] [a y_p e + (x_p + b y_p) X] = X^{p+1} X^r$$

On obtient après réduction, compte tenu de la relation $X^2 = a e + b X$,

$$X^r X^{p+1} = a [x_r y_p + y_r x_p + b y_r y_p] e + [(a + b^2) y_r y_p + b(y_r x_p + x_r y_p) + x_r x_p] X$$

Le second membre est symétrique en r et p donc $X^r X^{p+1} = X^p X^{r+1}$ et puisque

$$X^p X^{r+1} = X^{r+1} X^p, \quad X^r X^{p+1} = X^{r+1} X^p.$$

Donc X^{n+1} est défini et en particulier $X^{n+1} = X^n X = a y_n e + (x_n + b y_n) X$

ce qui permet de définir x_{n+1} et y_{n+1} tels que l'hypothèse 2 soit vérifiée à l'ordre $n+1$.

On en déduit que X^n est défini pour tout $n \in \mathbb{N}$. Il en résulte que la sous-algèbre engendrée

par X est associative et commutative. On la notera $A[X]$.

Proposition 3.1.4

La forme quadratique Q est multiplicative sur chaque sous-algèbre monogène de E .

Preuve

Soit $A[X]$ l'une de ces sous-algèbres. Puisque $X^2 = -Q(X)e + B_Q(X,e)X$, $A[X] = Ae + A[X]$.

Soient $x e + y X$ et $x'e + y'X$ deux éléments de $A[X]$. On pose $Q(X) = -a$ et $B_Q(X,e) = b$. Alors, $(xe + yX)(x'e + y'X) = (xx' + ay'y')e + (xy' + yx' + by'y')X$ et on vérifie facilement que $Q[(xe + yX)(x'e + y'X)] = Q(xe + yX)Q(x'e + y'X)$.

Remarques

1 $\forall X \in E, \forall n \in \mathbb{N}, Q(X^n) = (Q(X))^n$.

2 Pour qu'un élément X de E soit inversible dans $A[X]$, il faut et il suffit que $Q(X)$ soit inversible dans A .

(immédiat)

Corollaire

Lorsque A est réduit, l'ensemble des éléments nilpotents de E est l'ensemble des éléments X de E tels que $Q(X) = B_Q(X,e) = 0$. C'est donc l'ensemble des éléments de carré nul.

La preuve est analogue à la preuve du début de la proposition 1.2.4 mais ici l'ensemble des éléments nilpotents n'est pas nécessairement égal au noyau du module quadratique (E,Q) .

Autre application de la proposition 3.1.4 :

Recherche des idempotents de E

Pour tout idempotent non trivial a de A , $a e$ est un idempotent non trivial de E . Pour exclure ces idempotents, on suppose dans ce qui suit que A ne possède pas d'idempotents non triviaux.

Les idempotents de E sont les solutions de l'équation $Y^2 = Y$ c'est-à-dire de l'équation
(5) $-Q(Y)e + B_Q(Y,e)Y = Y$

Pour toute solution Y de (5), $(Q(Y))^2 = Q(Y^2) = Q(Y)$ donc $Q(Y)$ est un idempotent de A et, compte tenu de l'hypothèse faite sur A , $Q(Y) = 0$ ou $Q(Y) = 1$.

- Lorsque $Q(Y) = 1$, (5) s'écrit $Y(B_Q(Y,e) - 1) = e$, ce qui implique

$$(B_Q(Y,e) - 1)^2 = Q(e) = 1 \text{ et } B_Q(Y,e)(B_Q(Y,e) - 1) = B_Q(e, e) = 2.$$

On en déduit $B_Q(Y,e) = 2$ donc $Y = e$.

- Lorsque $Q(Y) = 0$, (5) s'écrit $Y(B_Q(Y,e) - 1) = 0$, ce qui implique $B_Q(Y,e)(B_Q(Y,e) - 1) = 0$ et puisque A n'a pas d'idempotents non triviaux, $B_Q(Y,e) = 1$ ou $B_Q(Y,e) = 0$. Lorsque $B_Q(Y,e) = 0$, $Y = 0$ et lorsque $B_Q(Y,e) = 1$, Y est un idempotent non trivial. En définitive :

Proposition 3.1.5

On suppose que A n'a pas d'idempotents non triviaux. Alors, pour qu'un élément Y de E soit un idempotent non trivial, il faut et il suffit que $Q(Y) = 0$ et $B_Q(Y, e) = 1$.

Propriété immédiate :

Proposition 3.1.6

Pour que E soit une algèbre de Jordan, il faut et il suffit que E soit flexible.

En effet une algèbre unitaire F est une algèbre de Jordan si et seulement si les deux conditions ci-dessous sont vérifiées ([4], chap. V, 3)

$$1 \quad \forall X, Y \in F, \quad (X Y)X - X(Y X) = 0 \quad (\text{condition de flexibilité})$$

$$2 \quad \forall X, Y \in F, \quad (X Y) X^2 - X(Y X^2) = 0$$

Or pour tout couple (X, Y) d'éléments de E

$$(X Y) X^2 - X(Y X^2) = B_Q(X, e)((X Y) X - X(Y X))$$

La proposition en résulte immédiatement.

Dans le paragraphe suivant, on étudie une famille de Q -algèbres commutatives.

§ 2 - Q-algèbres associées à une forme bilinéaire symétrique**Hypothèses et définitions 3.2.1**

Soient E un A -module et B_1 une forme bilinéaire symétrique définie sur E^2 . A tout élément e de E tel que $B_1(e, e) = 1$, on peut associer la structure d'algèbre sur E dont la multiplication est définie pour tout couple (X, X') d'éléments de E par

$$(1) \quad X X' = -B_1(X, X')e + B_1(X, e)X' + B_1(X', e)X.$$

Pour tout $X \in E$, on pose $Q(X) = B_1(X, X)$. Alors E est une Q -algèbre commutative pour la forme quadratique Q ainsi définie.

Lorsque E est muni de cette structure, on dit que E est la Q -algèbre d'unité e associée à la forme B_1 .

Lorsque 2 est régulier, la donnée de la forme Q détermine B_1 ; lorsque 2 est inversible, le calcul de $(X + X')^2 - X^2 - X'^2$ montre que toutes les Q -algèbres commutatives sont de ce type.

1 - Propriétés complémentaires immédiates

Toute Q -algèbre associée à une forme bilinéaire symétrique est une algèbre de Jordan commutative (prop. 3.1.6), de plus :

Proposition 3.2.2

Soit E une Q -algèbre d'unité e associée à une forme bilinéaire symétrique B_1 . Alors, la forme linéaire $X \mapsto B_1(X, e)$ est associative

En effet, $\forall X, X', X'' \in E$

$$(X X') X'' - X(X' X'') = [-B_1(X, e)B_1(X', X'') + B_1(X'', e)B_1(X, X')] e + \\ + [B_1(X, e)B_1(X', e) - B_1(X, X')] X'' + [-B_1(X'', e)B_1(X', e) + B_1(X'', X')] X$$

donc $B_1((X X') X'', e) - B_1(X(X' X''), e) = 0$

2 - Etude d'une Q-algèbre sur A associée à une forme bilinéaire symétrique B_1 qui possède des idempotents non triviaux

Soit E une telle algèbre d'unité e. Si on suppose que A n'a pas d'idempotents non triviaux, tout idempotent non trivial Y de E est solution du système ($Q(Y) = 0, 2 B_1(Y, e) = 1$) et par suite 2 est inversible dans A.

A tout idempotent non trivial Y de E, on associe la décomposition de Peirce

$E = E'_Y \oplus E''_Y \oplus E'''_Y$ (somme directe de sous A-modules), où

$$E'_Y = \{X \mid X \in E \text{ et } X Y = X\}, E''_Y = \{X \mid X \in E \text{ et } X Y = 0\}, E'''_Y = \{X \mid X \in E \text{ et } 2 X Y = X\}$$

Tout élément X de E s'écrit de façon unique $X = X' + X'' + X'''$, ($X' \in E'_Y, X'' \in E''_Y,$

$X''' \in E'''_Y$), avec

$$X' = 2(XY)Y - XY, \quad X'' = X - 3XY + 2(XY)Y, \quad X''' = 4XY - 4(XY)Y$$

(L'existence d'une telle décomposition est montrée par exemple dans [1], ch IV pour les algèbres de Jordan commutatives sur un corps de caractéristique $\neq 2$. On vérifie facilement que cette décomposition existe aussi pour la A-algèbre E)

On étudie cette décomposition.

Proposition 3.2.3

On suppose que A n'a pas d'idempotents non triviaux. Soit E une Q-algèbre sur A, d'unité e, associée à une forme bilinéaire symétrique B_1 et qui possède un idempotent non trivial Y, et soit $E = E'_Y \oplus E''_Y \oplus E'''_Y$ la décomposition de Peirce associée à Y. Alors, $E'_Y \oplus E''_Y$ est une sous-algèbre quadratique de E de norme non dégénérée, c'est une sous-algèbre associative maximale, on a $E'_Y = AY, E''_Y = A(e - Y), E'_Y$ et E''_Y sont totalement isotropes et E'''_Y est l'orthogonal de $E'_Y \oplus E''_Y$ dans (E, Q).

Preuve

Pour simplifier, on néglige l'indice Y et on pose $M = E' \oplus E''$ et $B = 2 B_1$.

M est une sous-algèbre de E. En effet :

Puisque Y et $e - Y$ sont des éléments de M, e appartient à M et pour tout couple (X_1, X_2)

d'éléments de M, $X_1 X_2 = -B_1(X_1, X_2)e + B_1(X_1, e) X_2 + B_1(X_2, e) X_1$ donc $X_1 X_2$

appartient à M.

(e, Y) est une base de M. En effet :

$$\forall X \in E, X = X' + X'' + X''' \text{ avec } X''' = 4XY - 4(XY)Y$$

$$X \in M \Leftrightarrow 4XY - 4(XY)Y = 0$$

ce qui s'écrit après réduction, puisque $Y^2 = Y$ et $B(Y,e) = 1$,

$$(2) \quad X \in M \Leftrightarrow X = [B(X,e) - 2B(X,Y)]Y + B(X,Y)e$$

D'autre part, e et Y sont linéairement indépendants. En effet,

$$(ae + bY = 0, (a,b) \in A^2) \Rightarrow (B(ae + bY,e) = B(ae + bY,Y) = 0)$$

ou encore, puisque $Q(Y) = 0$ et $B(Y,e) = 1$,

$$(ae + bY = 0, (a,b) \in A^2) \Rightarrow (2a + b = a = 0)$$

Donc (e,Y) est une base de M, ainsi que (Y, e-Y).

Plus précisément : $E' = AY$ et $E'' = A(e - Y)$. En effet :

Soit X un élément de E' , $XY = X$ implique $X = -B(X,Y)e + B(X,e)Y$ et, compte tenu de (2), $2B(X,Y)(e - Y) = 0$. Puisque (e,Y) est une base de M, $B(X,Y) = 0$ et $X = B(X,e)Y$ et puisque Y est un élément de E' , $E' = AY$.

On voit de même que $E'' = A(e - Y)$ et que $\forall X \in E'', X = B(X,e)(e - Y)$.

Il en résulte que E' et E'' sont des sous-modules isotropes de (E,Q) .

M est une sous-algèbre associative maximale de E. En effet :

M est une algèbre quadratique, elle est donc associative. D'autre part, pour tout $X \in E - M$, $XY \neq (XY)Y$ et $XY = XY^2$ donc $(XY)Y \neq XY^2$ et les sous-algèbres de E qui contiennent strictement M ne sont pas associatives.

$E''' = M^\perp$. En effet :

$$\forall X \in E, X = X' + X'' + X''' \text{ avec } X' = XY - 2(XY)Y \text{ et } X'' = X - 3XY + 2(XY)Y$$

$$X \in E''' \Leftrightarrow XY = 2(XY)Y \text{ et } X = 3XY - 2(XY)Y \text{ et après réduction,}$$

$$X \in E''' \Leftrightarrow -B(X,Y)e + B(X,e)Y = 0$$

ce qui équivaut à $B(X,Y) = B(X,e) = 0$ puisque (e,Y) est une base de M.

Donc, $X \in E''' \Leftrightarrow X$ est orthogonal à M.

Il en résulte que la restriction de Q à M est non dégénérée.

Remarques

1 e - Y est un idempotent non trivial de E. La décomposition associée à e - Y est obtenue en échangeant E' et E'' dans la décomposition associée à Y.

2 Lorsque A possède des idempotents non triviaux, la proposition reste vraie pour les idempotents Y de E solutions du système $(Q(Y) = 0, B(Y,e) = 1)$.

Conséquences de la proposition 3.2.3

On suppose dans cette partie que E possède un idempotent Y tel que $Q(Y) = 0$ et

$B(Y,e) = 1$ et on désigne par $E' \oplus E'' \oplus E'''$ la décomposition de Peirce associée à Y .

Le noyau K_1 du module quadratique (E,Q) (déf 0.1.1) est un sous-module de E .

De plus,

$$\forall X \in K_1, \forall Z \in E, 2 XZ = B(Z,e)X \quad (XZ = B_1(X,e)Z).$$

En particulier : $\forall X \in K_1, 2 XY = X$.

Donc K_1 est un idéal de E contenu dans E''' .

Proposition 3.2.4

Soit E une Q -algèbre d'unité e associée à une forme bilinéaire symétrique B_1 . On suppose que E possède un idempotent Y tel que $Q(Y) = 0$ et $2 B_1(Y,e) = 1$ et on désigne par $E' \oplus E'' \oplus E'''$ la décomposition de Peirce associée à Y et par K_1 le noyau du module quadratique (E,Q) . Les propriétés suivantes sont équivalentes

1- $K_1 = E'''$

2- E''' est un idéal de E

3- La forme Q est multiplicative sur E .

Preuve

1 \Leftrightarrow 2. En effet :

Pour tout couple (X_1, X_2) d'éléments de E''' , $X_1 X_2 = -\frac{1}{2} (B(X_1, X_2)e)$.

Lorsque E''' est un idéal de E , $X_1 X_2 \in E'''$ donc $B(X_1, X_2) = 0$.

Puisque $E''' = M^\perp$, $E''' = K_1$. La réciproque est immédiate.

2 \Leftrightarrow 3. En effet :

- On suppose Q multiplicative sur E .

$$\forall X_1, X_2 \in E''', B(X_1, X_2) = B(2 X_1 Y, 2 X_2 Y) = 4 Q(Y) B(X_1, X_2) = 0$$

donc $E''' = K_1$

- On suppose que $E''' = K_1$.

Soient X_1 et X_2 deux éléments de E , $X_1 = Z_1 + X'''_1$, $X_2 = Z_2 + X'''_2$

($Z_1, Z_2 \in M, X'''_1, X'''_2 \in E'''$).

$$X_1 X_2 = Z_1 Z_2 + X'''_1(Z_2 + X'''_2) + X'''_2 Z_1$$

Dans le second membre $Z_1 Z_2$ appartient à M et les deux autres termes à l'idéal K_1 .

Donc $Q(X_1 X_2) = Q(Z_1 Z_2) = Q(Z_1) Q(Z_2) = Q(X_1) Q(X_2)$.

Corollaire

On reprend les hypothèses de la proposition 3.2.4. On suppose de plus que A est intègre et E de rang 2. Alors E est somme directe d'un module libre de rang 2 et de son sous-module

de torsion T .

En effet, Q est multiplicative sur E ($\forall X \in E, Q(X) = N_0(f_0(X))$) où N_0 est la norme de l'extension E_0). Donc $K_1 = E'''$ et K_1 est de rang zéro. Comme $T \subset K_1, T = K_1 = E'''$.

3 - Etude des automorphismes d'une Q-algèbre associée à une forme bilinéaire symétrique B_1

Dans cette partie, on suppose \mathfrak{A} régulier. Alors B_1 est déterminée par la donnée de la forme Q associée. La proposition 1.1.3 ne s'étend pas en général aux Q-algèbres commutatives quelconques.

Proposition 3.2.5

On suppose que \mathfrak{A} est régulier dans A . Soit E une Q-algèbre sur A , d'unité e , associée à une forme bilinéaire symétrique B_1 .

Le groupe des automorphismes de E contient le groupe des transformations orthogonales de (E, Q) qui laissent e invariant. Ces deux groupes peuvent être distincts.

Toutefois, lorsque l'une des conditions a, b, c ci-dessous est vérifiée, les deux groupes coïncident.

- a) A est réduit
- b) E possède une base contenant e
- c) E possède des idempotents non triviaux, A n'en possède pas.

Preuve

Toute transformation orthogonale de (E, Q) qui laisse e invariant est un automorphisme de l'algèbre E . En effet, la multiplication de l'algèbre E est déterminée par la donnée de e et de la forme Q .

Exemple d'inclusion stricte

On suppose que A n'est pas réduit. On reprend l'exemple du § 1 p. 30. Soit $a \in A - \{0\}$ tel que $a^2 = 0$ et soit F l'algèbre quadratique d'unité e , de base (e, j) , de norme Q telle que $Q(j) = -a$ et $B_Q(e, j) = 2$. On prend pour E la sous A -algèbre monogène de F engendrée par a, j , (E est associée à e et à la forme bilinéaire $\frac{B}{2}$). L'automorphisme τ du A -module F défini par $\tau(e) = e$ et $\tau(j) = e + j$ induit un automorphisme τ' de E compatible avec la multiplication de E , ($\tau'((aj)^2) = a^2 \tau'(j^2) = 0 = a^2 (\tau'(j))^2 = (\tau'(aj))^2$ puisque $a^2 = 0$). Mais τ' n'est pas une transformation orthogonale de (E, Q) . En effet, $B(a, j, e) = 2a$ et $B(\tau'(aj), \tau'(e)) = 4a$. (τ' n'est pas compatible avec la multiplication de F).

Etude des cas a, b, c

- Chacune des conditions a) et b) assure l'unicité de la forme Q telle que E soit une Q-algèbre (prop. 3.1.1). Il en résulte que lorsque a) ou b) est vérifié, tout automorphisme de l'algèbre E

est une transformation orthogonale de (E, Q) .

- On suppose maintenant que c) est vérifié. Soient σ un automorphisme de l'algèbre E , Y un idempotent non trivial de E et $E' \oplus E'' \oplus E'''$ la décomposition de Peirce associée à Y . Il est immédiat que $\sigma(Y)$ est un idempotent non trivial de E et que $\sigma(E') \oplus \sigma(E'') \oplus \sigma(E''')$ est la décomposition associée à Y . Soient $X_1 = Z_1 + T_1$, $X_2 = Z_2 + T_2$ ($Z_1, Z_2 \in M$, $T_1, T_2 \in E'''$), on a $B(X_1, X_2) = B(Z_1, Z_2) + B(T_1, T_2)$ car $E''' = M^\perp$. De même, $B(\sigma(X_1), \sigma(X_2)) = B(\sigma(Z_1), \sigma(Z_2)) + B(\sigma(T_1), \sigma(T_2))$. Comme Y et $\sigma(Y)$ sont des idempotents non triviaux, on a $Q(Y) = 0 = Q(\sigma(Y))$ et $B(Y, e) = 1 = B(\sigma(Y), e)$. Par suite, $B(Z_1, Z_2) = B(\sigma(Z_1), \sigma(Z_2))$.

D'autre part, pour tout couple (T_1, T_2) d'éléments de E''' , $2 T_1 T_2 = -B(T_1, T_2) e$ donc $2 \sigma(T_1) \sigma(T_2) = -B(T_1, T_2) e$.

Puisque dans $\sigma(E''')$, $2 \sigma(T_1) \sigma(T_2) = -B(\sigma(T_1), \sigma(T_2)) e$, on a aussi $B(T_1, T_2) = B(\sigma(T_1), \sigma(T_2))$, (car e est libre).

Donc $\forall (X_1, X_2) \in E^2$, $B(X_1, X_2) = B(\sigma(X_1), \sigma(X_2))$ et puisque 2 est nécessairement inversible on a aussi $\forall X \in E$, $Q(X) = Q(\sigma(X))$.

Remarques

1 Les deux groupes peuvent coïncider sans que l'une au moins des conditions a, b, c soit vérifiée. Ils coïncident toujours par exemple lorsque E est projectif de rang 2.

2 Tout automorphisme du A -module E compatible avec la forme B_1 et qui laisse e invariant est un automorphisme de l'algèbre E même lorsque 2 n'est pas régulier.

§3 - Q-algèbres non nécessairement commutatives - Q-algèbres alternatives

Soit E une Q -algèbre d'unité e .

$$\forall X \in E, X^2 = -Q(X) e + B_Q(X, e) X$$

$$\forall X, X' \in E, XX' + X'X = -B_Q(X, X') e + B_Q(X, e) X' + B_Q(X', e) X$$

Lorsqu'il existe une forme bilinéaire symétrique B_1 telle que pour tout $X \in E$, $Q(X) = B_1(X, X)$, on peut munir E de la structure de Q -algèbre commutative E_+ associée à e et à la forme B_1 . ($\forall X, X' \in E$, $X \circ X' = X' \circ X = -B_1(X, X') e + B_1(X, e) X' + B_1(X', e) X$).

Lorsque 2 est inversible dans A , B_1 existe et l'algèbre E_+ est uniquement déterminée par l'algèbre E , ($X \circ X' = \frac{1}{2} (XX' + X'X)$). Il en est de même par exemple lorsque B_1 existe et que 2 est régulier et E libre.

1 - Etude des Q-algèbres non nécessairement commutatives qui possèdent des idempotents non triviaux

Soit E une Q -algèbre sur A d'unité e . On suppose que A ne possède pas d'idempotents non triviaux et qu'il existe une forme bilinéaire B_1 telle que $B_Q = 2 B_1$.

Tout idempotent non trivial Y de E est solution du système $(Q(Y) = 0, B_Q(Y, e) = 1)$. Si un tel idempotent Y existe, 2 est inversible, l'algèbre E_+ est déterminée par l'algèbre E et Y est un idempotent de E_+ . On peut donc associer à Y la décomposition de Peirce $E = E' \oplus E'' \oplus E'''$. La proposition 3.2.3 s'étend à E , à cette différence près que $E' \oplus E''$, qui est une sous-algèbre associative de E , n'est pas nécessairement une sous-algèbre associative maximale. Il existe par exemple des algèbres de quaternions sur un corps de caractéristique $\neq 2$ qui possèdent des idempotents non triviaux. De telles algèbres sont associatives et de dimension 4.

On va étudier plus particulièrement parmi les algèbres E celles qui sont alternatives.
Décomposition de Peirce dans les Q-algèbres alternatives

On suppose que A ne possède pas d'idempotents non triviaux et que 2 est inversible dans A . Soit E une Q -algèbre alternative sur A .

A tout idempotent non trivial Y de E , on associe la décomposition de Peirce $E = E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ (somme directe de sous-modules) où $\forall i, j \in \{0, 1\}, E_{ij} = \{X \mid X \in E, YX = iX \text{ et } XY = jX\}$

(E_{ij} dépend de Y , on a supprimé l'indice Y pour simplifier).

Tout élément X s'écrit de façon unique $X = X_{11} + X_{00} + X_{10} + X_{01}$ où $X_{ij} \in E_{ij}$, $X_{11} = YXY, X_{00} = X - XY - YX + YXY, X_{10} = YX - YXY, X_{01} = XY - YXY$ (puisque E est flexible, on peut poser $XYX = (XY)X = X(YX)$).

De plus, avec les notations de la proposition 3.2.3,

$$(2) \quad E' = E_{11}, \quad E'' = E_{00}, \quad E''' = E_{10} \oplus E_{01}$$

$$(3) \quad \forall i, j, k \in \{0, 1\}, \quad E_{ij} E_{jk} \subset E_{ik}, \quad E_{ij} E_{ij} \subset E_{ji}$$

Ces propriétés sont établies par exemple dans [4], ch. III pour les algèbres alternatives sur un corps de caractéristique $\neq 2$ et s'étendent facilement à une algèbre alternative sur l'anneau A .

Proposition 3.3.1

On suppose que A n'a pas d'idempotents non triviaux et que 2 est inversible dans A .

Soit E une Q -algèbre alternative sur A , d'unité e , qui possède un idempotent non trivial Y , et soit $E = E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ la décomposition de Peirce associée à Y . Alors :

$E_{11} = AY, E_{00} = A(e - Y)$, les ensembles E_{ij} ($i, j \in \{0,1\}$) sont des sous-modules totalement isotropes de (E, Q) et $E_{10} \oplus E_{01}$ est l'orthogonal de $E_{11} \oplus E_{00}$ dans (E, Q) .

Preuve

On sait que $E_{11} = E', E_{00} = E''$ et $E_{10} \oplus E_{01} = E'''$ (notations de la proposition 3.2.3). Compte tenu de cette proposition, il reste à montrer que les modules E_{10} et E_{01} sont totalement isotropes. On précise d'abord les propriétés de la multiplication dans E .

Soient X et X' deux éléments de E . On étudie différents cas.

- $X \in E_{10}, X' \in E_{01}$

Puisque $E_{10} \oplus E_{01} = (E_{11} \oplus E_{00})^\perp$, $B(X, e) = B(X', e) = 0$
 et $XX' + X'X = -B_Q(X, X')e = -B_Q(X, X')Y - B_Q(X, X')(e - Y)$.

Compte tenu de (3), $XX' = -B_Q(X, X')Y$ et $X'X = -B_Q(X, X')(e - Y)$

- $X \in E_{10}, X' \in E_{10}$

$XX' + X'X = -B_Q(X, X')e$, $XX' \in E_{01}$ et $X'X \in E_{01}$. Donc $XX' + X'X = 0$
 et puisque e est libre, $B_Q(X, X') = 0$.

En particulier, pour tout élément X de E_{10} , $X^2 = 0$ et $Q(X) = 0$

- $X \in E_{01}, X' \in E_{01}$

Les résultats sont analogues aux précédents, $XX' \in E_{10}$ et $X'X \in E_{10}$

- $X \in E_{10}, X' \in E_{11} \oplus E_{00}$

Si $X' = aY + b(e - Y)$, $XX' = bX$ et $X'X = aX$

- $X \in E_{01}, X' \in E_{11} \oplus E_{00}$

Si $X' = aY + b(e - Y)$, $XX' = aX$ et $X'X = bX$

Conséquences

La multiplication d'un élément de E_{ij} par un élément de E_{kl} ($i, j, k, l \in \{0,1\}$), est déterminée par la donnée de la forme Q sauf lorsque $(i, j) = (k, l)$ avec $i \neq j$.

Les sous-modules E_{ij} sont totalement isotropes. En effet, on sait déjà que E_{11} et E_{00} sont totalement isotropes et l'étude du deuxième et du troisième cas montre qu'il en est de même pour E_{10} et E_{01} .

Proposition 3.3.2

On garde les hypothèses et notations de la proposition 3.3.1 et on note K_1 le noyau de (E, Q) . Alors, les deux propriétés suivantes sont équivalentes.

$$1 \quad E_{10} \oplus E_{01} = K_1$$

2 $E_{10} \oplus E_{01}$ est un idéal bilatère de E .

Preuve

$E_{10} \oplus E_{01} = E'''$ et tout idéal bilatère de E est un idéal de l'algèbre commutative associée E_+ . Donc si E''' est un idéal bilatère de E , $E''' = K_1$ (prop. 3.2.4).

Inversement, les calculs précédents montrent que lorsque $K_1 = E'''$, E''' est un idéal bilatère de E .

Remarque

Lorsque $K_1 = E'''$, la forme Q est multiplicative sur E mais elle peut être multiplicative sur E sans que K_1 soit égal à E''' . En effet, la norme réduite d'une algèbre de quaternions est multiplicative et non dégénérée, donc les algèbres de quaternions sur un corps de caractéristique $\neq 2$ qui possèdent des idempotents non triviaux fournissent des contre-exemples ($E''' \neq (0)$ et $K_1 = (0)$).

La proposition 3.2.2 s'étend aux Q -algèbres que l'on vient d'étudier :

Proposition 3.3.3

On suppose que l'anneau A et la Q -algèbre E vérifient les hypothèses de la proposition 3.3.1. Alors, la forme linéaire $X \mapsto B_Q(X, e)$ est associative sur E , autrement dit, elle s'annule sur les commutateurs et les associateurs de E .

Preuve

- $\forall (X', X'') \in E^2$, $B_Q(X'X'', e) = B_Q(X''X', e)$. En effet :

soient $X' = X'_{11} + X'_{00} + X'_{10} + X'_{01}$ et $X'' = X''_{11} + X''_{00} + X''_{10} + X''_{01}$

les décompositions de X' et X'' . On obtient après réduction

$$\begin{aligned} B_Q(X'X'', e) &= B_Q((X'_{11} + X'_{00})(X''_{11} + X''_{00}), e) - B_Q(X'_{10}, X''_{01}) - B_Q(X'_{01}, X''_{10}) \\ &= B_Q(X''X', e) \text{ car la sous-algèbre } E_{11} \oplus E_{00} \text{ est commutative.} \end{aligned}$$

- $\forall (X, X', X'') \in E^3$, $B_Q((XX')X'', e) = B_Q(X(X'X''), e)$. En effet :

Puisque E est flexible, $X(X'X'') + X''(X'X) = (XX')X'' + (X''X')X$,

(identité obtenue par linéarisation des identités de la forme $(XY)X = X(YX)$), donc

$$(4) \quad B_Q(X(X'X''), e) + B_Q(X''(X'X), e) = B_Q((XX')X'', e) + B_Q((X''X')X, e)$$

de plus, puisque la forme $X \mapsto B_Q(X, e)$ est associative sur E_+ ,

$$B_Q(X \circ (X' \circ X''), e) = B_Q(X'' \circ (X \circ X'), e)$$

d'où $2 B_Q(X(X' \circ X''), e) = 2 B_Q(X''(X \circ X'), e)$ c'est-à-dire

$$(5) \quad B_Q(X(X'X''),e) + B_Q(X(X'X''), e) = B_Q(X''(XX'),e) + B_Q(X''(X'X),e)$$

$$(4) \text{ et } (5) \text{ impliquent } 2[B_Q(X(X'X''),e) - B_Q((XX')X'', e)] = 0$$

Remarque

Toute Q-algèbre flexible sur un corps de caractéristique $\neq 2$ possède aussi cette propriété [1].

Automorphismes des Q-algèbres non nécessairement commutatives

On suppose que 2 est inversible dans A. Soit E une Q-algèbre sur A d'unité e et soit E_+ la Q-algèbre commutative associée.

Lorsque l'une des conditions ci-dessous est vérifiée

- a) A est réduit
- b) E possède des idempotents non triviaux, A n'en possède pas
- c) E possède une base contenant l'unité e

le groupe des automorphismes de l'algèbre E_+ coïncide avec le groupe τ_e des transformations orthogonales de (E,Q) qui laissent e invariant (prop. 3.2.5). Comme tout automorphisme et tout antiautomorphisme de l'algèbre E est un automorphisme de l'algèbre E_+ , le groupe d'automorphismes de l'algèbre E est contenu dans τ_e . Cette inclusion est stricte par exemple pour les algèbres de quaternions sur un corps de caractéristique $\neq 2$ et pour les algèbres E non commutatives qui vérifient les hypothèses de la proposition 3.3.1 (on vérifie facilement que l'application $\sigma : X \mapsto B_Q(X, e) e - X$ est une involution).

Chapitre IV

Formes quadratiques multiplicatives sur une Q-algèbre

On étudiera essentiellement les formes quadratiques multiplicatives sur une Q-algèbre E commutative ou alternative dans le cas où l'anneau de base A est intègre et $2 \neq 0$ et dans le cas où E possède des idempotents non triviaux, A n'en possédant pas. On examine d'abord le cas particulier des algèbres quadratiques.

§ 1 - Formes quadratiques multiplicatives sur une algèbre quadratique
(algèbre unitaire libre de rang 2).

La norme est multiplicative sur toute algèbre quadratique. De plus :

Proposition 4.1.1

Soit E une algèbre quadratique. S'il existe une forme quadratique multiplicative Q' définie sur E et distincte de la norme, la forme bilinéaire associée $B_{Q'}$ est dégénérée.

Preuve

Soit (e, i) une base de E contenant l'unité e et soit $(\alpha, \beta) \in A^2$ tel que $i^2 = \alpha e + \beta i$. La norme Q est la forme quadratique définie par $Q(e) = 1$, $Q(i) = -\alpha$ et $B_Q(e, i) = \beta$.

Par définition, une forme quadratique Q' définie sur E est multiplicative si et seulement si $Q'(e) = 1$ et

$$\forall x_1, x_2, y_1, y_2 \in A, Q'((x_1 e + y_1 i)(x_2 e + y_2 i)) = Q'(x_1 e + y_1 i) Q'(x_2 e + y_2 i).$$

On pose $Q'(i) = -\alpha'$ et $B_{Q'}(e, i) = \beta'$. L'équation ci-dessus s'écrit après réduction, lorsque $Q'(e) = 1$:

$$\begin{aligned} & [2(\alpha' - \alpha) + \beta'(\beta' - \beta)] x_1 x_2 y_1 y_2 + [\beta'(\alpha' - \alpha) - 2\alpha'(\beta' - \beta)] (y_1^2 x_2 y_2 + y_2^2 x_1 y_1) + \\ & + (\alpha'^2 - \alpha^2 - \alpha\beta\beta' + \alpha'\beta'^2) y_1^2 y_2^2 = 0 \end{aligned}$$

Déterminer les formes quadratiques multiplicatives Q' revient à déterminer les couples (α', β') solutions du système

$$(4.1.1) \quad \begin{cases} 2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0 & (1) \\ \beta'(\alpha' - \alpha) - 2\alpha'(\beta' - \beta) = 0 & (2) \\ \alpha'^2 - \alpha^2 - \alpha\beta\beta' + \alpha'\beta'^2 = 0 & (3) \end{cases}$$

Lorsque le système formé par les équations (1) et (2) admet une solution non nulle en $\alpha' - \alpha$, $\beta' - \beta$, le déterminant $(4\alpha'^2 + \beta'^2)$ n'est pas régulier. Autrement dit, s'il existe une forme quadratique Q' multiplicative sur E et distincte de Q, le noyau K' de $B_{Q'}$ est $\neq (0)$.

Etude du problème lorsque A est intègre

Proposition 4.1.2

Soit E une algèbre sur l'anneau intègre A, d'unité e, de base (e, i) telle que $i^2 = \alpha e + \beta i$. Il existe exactement une ou trois formes quadratiques multiplicatives sur E. Il n'en existe qu'une, la norme Q, lorsque le noyau K de B_Q est $\neq (0)$.

On suppose de plus β multiple de 2 et $2 \neq 0$. Alors, pour qu'il existe trois formes quadratiques multiplicatives sur E, il faut et il suffit que $4\alpha + \beta^2$ soit le carré d'un élément non nul de A.

Preuve

Lorsque $2 = 0$, le système (4.1.1) s'écrit

$$\beta'(\beta + \beta') = 0$$

$$\beta'(\alpha + \alpha') = 0$$

$$\alpha'^2 + \alpha^2 + \alpha\beta\beta' + \alpha'\beta^2 = 0$$

Pour toute solution (α', β') distincte de (α, β) , $\beta' = 0$ et $\alpha'^2 + \alpha^2 + \alpha'\beta^2 = 0$.

Lorsque $\beta = 0$, c'est-à-dire lorsque $K \neq (0)$, la seule solution est (α, β) . Lorsque $\beta \neq 0$, les solutions distinctes de la solution (α, β) sont les couples $(\alpha', 0)$ tels que

$$\alpha'^2 + \alpha^2 + \alpha'\beta^2 = 0. \text{ Lorsqu'il en existe, il en existe deux.}$$

Lorsque $2 \neq 0$, le système (4.1.1) est équivalent au système

$$2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0$$

$$(4\alpha' + \beta'^2)(\beta' - \beta) = 0$$

$$(\alpha' - \alpha)(2(\alpha' + \alpha) + \beta\beta') = 0$$

Un couple (α', β') est une solution si et seulement si il vérifie

$$(4.1.1)' \left\{ \begin{array}{l} 2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0 \\ (4\alpha' + \beta'^2)(\beta' - \beta) = 0 \\ \alpha' - \alpha = 0 \end{array} \right. \text{ ou } (4.1.1)'' \left\{ \begin{array}{l} 2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0 \\ (4\alpha' + \beta'^2)(\beta' - \beta) = 0 \\ 2(\alpha + \alpha') + \beta\beta' = 0 \end{array} \right.$$

Lorsque le système (4.1.1)' admet une solution (α', β') distincte de (α, β) ,

$\alpha' = \beta' = 0$. Ce cas ne peut se présenter que lorsque $\alpha = 0$ et $\beta \neq 0$, B_Q est alors non dégénérée.

Les solutions du système (4.1.1)'' distinctes de la solution éventuelle (α, β) sont les solutions distinctes de (α, β) du système

$$\left[\begin{array}{l} \beta'^2 - 2\beta\beta' - 4\alpha = 0 \\ 4\alpha' + \beta'^2 = 0 \end{array} \right.$$

Pour que ce dernier système admette une solution, il faut que $4\alpha + \beta^2$ soit le carré d'un élément de A.

Lorsque $4\alpha + \beta^2 = 0$, la seule solution est (α, β) .

Lorsque $4\alpha + \beta^2 \neq 0$ et lorsqu'il existe une solution, il en existe deux et elles sont distinctes de (α, β) .

En particulier, lorsque β est multiple de 2, le système (4.1.1)'' admet deux solutions distinctes de (α, β) exactement lorsque $4\alpha + \beta^2$ est le carré d'un élément non nul de A.

Lorsque $\alpha = 0$ et $\beta \neq 0$, le système (4.1.1)'' redonne la solution $(0, 0)$ du système (4.1.1)'.

Corollaire 1

On suppose A intégralement clos et $2 \neq 0$. Soit E une A-algèbre quadratique de norme Q telle que 2 divise B_Q . Alors, pour qu'il existe trois formes quadratiques multiplicatives sur E, il faut et il suffit que $K_1 = (0)$ et que H soit $\neq (0)$, (K_1 noyau de (E, Q) , H ensemble des éléments isotropes de (E, Q)).

Preuve

Avec les notations de la proposition, $K_1 = (0)$ et $H \neq (0)$ si et seulement si $4\alpha + \beta^2$ est le carré d'un élément non nul de A. En effet :

- Si $4\alpha + \beta^2$ est le carré d'un élément non nul de A, $K_1 = (0)$ et l'équation

$$\left(x + \frac{\beta}{2}y\right)^2 - \frac{4\alpha + \beta^2}{4}y^2 = 0, \quad (Q(xe + yi) = 0), \text{ admet des solutions } (x, y) \text{ non nulles.}$$

- Lorsque $H \neq (0)$, $\frac{4\alpha + \beta^2}{4}$ est un carré dans le corps des fractions de A donc est le carré d'un élément de A qui n'est pas nul lorsque $K_1 = (0)$.

Le corollaire résulte alors de la proposition 4.1.2.

Corollaire 2

Soit E une algèbre quadratique de norme Q sur un corps de caractéristique $\neq 2$. Alors, pour qu'il existe trois formes quadratiques multiplicatives sur E, il faut et il suffit que l'une des conditions équivalentes ci-dessous soit vérifiée

1 $K_1 = (0)$ et $H \neq (0)$

2 E possède des idempotents non triviaux.

1 \Leftrightarrow 2. En effet :

Lorsque $K_1 = (0)$ et $H \neq (0)$, il existe $X \in E$ tel que $Q(X) = 0$ et $B_Q(X, e) \neq 0$. Alors

$\frac{X}{B_Q(X, e)}$ est un idempotent non trivial de E (prop. 3.1.5).

Inversement, lorsque E possède un idempotent non trivial, H n'est pas nul et $K_1 = (0)$ (prop. 3.2.3).

Le corollaire 2 résulte alors du corollaire 1.

Remarque

A toute forme quadratique Q' multiplicative sur E et distincte de la norme Q , on peut associer l'algèbre quadratique E' , d'unité e , de module sous-jacent E , de norme Q' . Alors, Q n'est pas multiplicative sur E' . En effet B_Q est dégénérée (prop. 4.1.1) et Q' est la seule forme quadratique multiplicative sur E' (prop. 4.1.2).

Propriétés des formes quadratiques multiplicatives sur une A-algèbre quadratique (A intègre)

Proposition 4.1.3

Soit E une algèbre quadratique sur l'anneau intègre A . On suppose qu'il existe deux formes quadratiques Q' et Q'' , multiplicatives sur E et distinctes de la norme Q de E . Alors, pour tout élément X de E , $(Q(X))^2 = Q'(X) Q''(X)$.

Preuve

Avec les notations de la proposition 4.1.2, les formes Q' et Q'' sont associées aux deux solutions (α', β') et (α'', β'') distinctes de (α, β) du système (4.1.1).

Lorsque $2 = 0$, $\beta' = \beta'' = 0$ et α' et α'' sont les racines de l'équation en t
 $t^2 + t \beta^2 + \alpha^2 = 0$. Soit $X = x e + y i$ un élément de E . Puisque $\alpha' + \alpha'' = \beta^2$ et $\alpha' \alpha'' = \alpha^2$,

$$Q'(X)Q''(X) = (x^2 + \alpha' y^2)(x^2 + \alpha'' y^2) = (x^2 + \beta xy + \alpha y^2)^2 = (Q(X))^2$$

Lorsque $2 \neq 0$, $4\alpha' + \beta'^2 = 4\alpha'' + \beta''^2 = 0$ et β' et β'' sont les racines de l'équation $t^2 - 2\beta t - 4\alpha = 0$ (en particulier $\beta' + \beta'' = 2\beta$ et $\beta' \beta'' = -4\alpha$).

$$16 Q'(X) Q''(X) = (2x + \beta'y)^2 (2x + \beta''y)^2 = 16(x^2 + \beta xy - \alpha y^2)^2 = 16 (Q(X))^2$$

Soient H (resp. H'), ($\text{resp. } H''$), l'ensemble des éléments de E isotropes pour Q (resp. Q'), ($\text{resp. } Q''$). Il est immédiat que H' et H'' sont des idéaux premiers de E , que $H' \cup H'' = H$ et $H' \cap H'' = (0)$. H' et H'' sont les idéaux I_1 et I_2 de l'étude p. 11.

Soient E' (resp. E'') l'algèbre quadratique associée à Q' (resp. Q'') selon la remarque précédente, et T' (resp. T''), le groupe d'automorphismes de l'algèbre E' (resp. E''). Alors, l'automorphisme $\sigma : X \mapsto B_Q(X, e) e - X$ est un isomorphisme de l'algèbre E' sur l'algèbre E'' , $T' = \sigma T'' \sigma$ et $T'' = \sigma T' \sigma$, comme on le vérifie facilement.

Extension aux algèbres unitaires projectives de rang 2

La proposition 4.1.1, le début de la proposition 4.2.1, le corollaire 1 et les propriétés ci-dessus sont vrais aussi pour les algèbres unitaires projectives de rang 2 (preuves par localisation et globalisation).

§ 2 - Formes quadratiques multiplicatives sur les Q-algèbres commutatives associées à une forme bilinéaire symétrique

1 - Cas des algèbres qui possèdent des idempotents non triviaux

Proposition 4.2.1

On suppose que A ne possède pas d'idempotents non triviaux. Soit E une Q-algèbre d'unité e, associée à une forme bilinéaire symétrique B_1 , qui possède un idempotent non trivial Y, et soit $E' \oplus E'' \oplus E'''$ la décomposition de Peirce associée à Y.

Alors, ou bien il n'existe pas de forme quadratique multiplicative sur E, ou bien il en existe exactement trois.

Pour que les trois formes existent, il faut et il suffit que l'une des conditions équivalentes ci-dessous soit vérifiée

- (i) Q est multiplicative sur E
- (ii) E''' est un idéal de E
- (iii) $E''' = K_1(K_1 \text{ noyau de } (E, Q))$.

Preuve

L'équivalence des trois conditions résulte de la proposition 3.2.4. Les hypothèses impliquent que 2 est inversible dans A.

Pour qu'une forme quadratique Q' définie sur E soit multiplicative, il faut que

$$(4) (Q'(Y))^2 = Q'(Y^2) = Q'(Y)$$

$$(5) (Q'(e - Y))^2 = Q'((e - Y)^2) = Q'(e - Y)$$

$$(6) 0 = Q'(Y(e - Y)) = Q'(Y) Q'(e - Y)$$

Puisque 1 et 0 sont les seuls idempotents de A, (4) et (5) impliquent $(Q'(Y) = 0$ ou $Q'(Y) = 1)$ et $(Q'(e - Y) = 0$ ou $Q'(e - Y) = 1)$.

Il y a trois cas à examiner

$$a) Q'(Y) = 0 \text{ et } Q'(e - Y) = 0$$

$$b) Q'(Y) = 0 \text{ et } Q'(e - Y) = 1$$

$$c) Q'(Y) = 1 \text{ et } Q'(e - Y) = 0$$

(le cas $Q'(Y) = Q'(e - Y) = 1$, incompatible avec la condition 6, est à exclure.)

- Le noyau de toute forme quadratique Q' multiplicative sur E contient E''' . En effet :

$$\forall X''' \in E''', X''' = 2 X''' Y = 2 X'''(e - Y)$$

$$Q'(X''') = 4 Q'(Y) Q'(X''') = 4 Q'(e - Y) Q'(X''') \text{ donc,}$$

puisque Q' vérifie les conditions a), b) ou c), $Q'(X''') = 0$.

$$\forall X''' \in E''', B_{Q'}(Y, X''') = 2 B_{Q'}(Y^2, YX''') = 2 Q'(Y) B_{Q'}(Y, X''')$$

$$B_{Q'}(e - Y, X''') = 2 B_{Q'}((e - Y)^2, (e - Y)X''') = 2 Q'(e - Y) B_{Q'}(Y, X''')$$

ce qui implique $B_Q(Y, X''') = B_Q(e - Y, X''') = 0$ dans le cas a), $B_Q(Y, X''') = 0$ dans le cas b), et $B_Q(e - Y, X''') = 0$ dans le cas c).

D'autre part, dans le cas b), puisque $Q'(e - Y) = 1$,
 $B_Q(e - Y, X''') = Q'(e - Y) B_Q(e - Y, X''') = B_Q((e - Y)^2, (e - Y)X''') = \frac{1}{2} B_Q(e - Y, X''')$
 donc $B_Q(e - Y, X''') = 0$.

De même dans le cas c), $B_Q(Y, X''') = 0$.

On en déduit que E''' est contenu dans le noyau de (E, Q') .

Il existe exactement trois formes quadratiques Q' définies sur E dont le noyau contient E''' , telles que a), b) ou c) soit vérifié, et telles que $Q'(e) = 1$. Elles admettent pour noyaux respectifs E''' , $AY \oplus E'''$ et $A(e - Y) \oplus E'''$. Il reste à examiner si les trois formes peuvent effectivement être multiplicatives.

Soit Q' l'une des trois formes. Pour que Q' soit multiplicative, il faut que pour tout couple (Z_1, Z_2) d'éléments de E''' , $Q'(Z_1 Z_2) = Q'(Z_1) Q'(Z_2)$ et
 $Q'((e + Z_1)(e + Z_2)) = Q'(e + Z_1) Q'(e + Z_2)$.

Puisque $Z_1 Z_2 = -\frac{1}{2} B_Q(Z_1, Z_2)e$ et $Q'(Z_1) = Q'(Z_2) = 0$, il faut que

$$0 = Q'(Z_1) Q'(Z_2) = \frac{1}{4} B_Q^2(Z_1, Z_2)$$

et puisque $Q'(Z_1 + e) = Q'(Z_2 + e) = 1$, il faut que

$$1 = Q'(e + Z_1) Q'(e + Z_2) = Q'(e + Z_1 + Z_2 - \frac{1}{2} B_Q(Z_1, Z_2)e) = 1 + \frac{1}{4} B_Q^2(Z_1, Z_2) - B_Q(Z_1, Z_2).$$

Donc, pour que l'une au moins des trois formes soit multiplicative, il faut que pour tout couple (Z_1, Z_2) d'éléments de E''' , $B_Q(Z_1, Z_2) = 0$, c'est-à-dire, puisque E''' est orthogonal à $E' \oplus E''$ pour Q , que $K_1 = E'''$.

Il est immédiat que lorsque cette condition est vérifiée, les trois formes sont multiplicatives sur E et que la première, (cas a)), est la forme Q .

Remarques

1 - Lorsqu'il existe trois formes quadratiques multiplicatives Q, Q', Q'' sur la Q -algèbre E on a, $\forall X \in E, (Q(X))^2 = Q'(X) Q''(X)$.

2 - La proposition 4.2.1 s'étend au cas où A possède des idempotents non triviaux pour les algèbres E qui possèdent un idempotent solution du système $(Q(Y) = 0, 2 B_1(Y, e) = 1)$ à ceci près que lorsqu'il existe des formes quadratiques multiplicatives sur E , il en existe plus de trois.

2 - Formes quadratiques multiplicatives sur une Q-algèbre commutative lorsque A est intègre et $2 \neq 0$

Proposition 4.2.2

On suppose A intègre et $2 \neq 0$. Soit E une Q-algèbre commutative sur A. On note E_0 l'algèbre obtenue par extension des scalaires au corps des fractions A_0 de A, Q_0 l'extension de Q à E_0 et $K_{1,0}$ le noyau de (E_0, Q_0) . Alors :

1 - Pour que Q soit multiplicative sur E, il faut et il suffit que $K_{1,0}$ soit de codimension 1 ou 2 dans E_0 .

2 - Il existe au plus trois formes quadratiques multiplicatives sur E. Pour qu'il en existe au moins deux, il faut que K_1 soit distinct de H et $K_{1,0}$ de codimension 2 dans E_0 .

Lorsque de plus 2 est inversible dans A, il existe exactement zéro, une ou trois formes quadratiques multiplicatives sur E.

Preuve

Lorsque E est de rang 1, il existe une seule forme quadratique multiplicative sur E. On peut supposer que E est de rang ≥ 2 .

a) On établit d'abord la proposition dans le cas où A est un corps de caractéristique $\neq 2$ (Alors $E = E_0$, $K_1 = K_{1,0}$ et 2 est inversible dans A).

- Il est connu que toute algèbre commutative unitaire sur le corps A sur laquelle il existe une forme quadratique multiplicative non dégénérée est de dimension 1 ou 2 (voir par exemple [5]). Puisque l'unité e de E n'appartient pas à K_1 , il existe une décomposition $E = M \oplus K_1$ où M contient e. De plus M est une sous-algèbre de E, ($\forall X, X' \in E, XX' = \frac{1}{2} [-B_Q(X, X')e + B_Q(X, e)X' + B_Q(X', e)X]$), et il est immédiat que Q n'est pas dégénérée sur M. Il en résulte que lorsque Q est multiplicative sur E, M est de dimension 1 ou 2. Inversement, lorsque M est de dimension 1 ou 2, il est immédiat que Q est multiplicative sur E.

- Lorsqu'il existe deux formes quadratiques multiplicatives sur E, il existe au moins une sous-algèbre de dimension 2 sur laquelle ces formes sont distinctes donc (prop. 4.1.2, cor. 2), E possède au moins un idempotent non trivial Y et $K_1 = E'''_Y$ (prop. 4.2.1).

Donc K_1 est de codimension 2 et $K_1 \neq H$.

Inversement, lorsque K_1 est de codimension 2 et $H \neq K_1$, E admet une décomposition de la forme $Ae \oplus Ai \oplus K_1$ où $Q(i) = 0$ et $B_Q(e, i) \neq 0$. L'élément $Y = \frac{i}{B_Q(e, i)}$ est un idempotent non trivial et $K_1 = E'''_Y$ (en effet $K_1 \subset E'''_Y$ et E'''_Y

est de codimension 2). Il existe alors trois formes quadratiques multiplicatives sur E (prop. 4.2.1).

b) Preuve de la proposition (cas A intègre et $2 \neq 0$)

Une forme quadratique Q' définie sur E est multiplicative sur E si et seulement si son extension à E_0 est multiplicative sur E_0 . Les propriétés 1 et 2 résultent de l'étude a) précédente.

On suppose maintenant que 2 est inversible dans A.

Lorsqu'il existe au moins deux formes quadratiques multiplicatives sur E, E_0 possède un idempotent non trivial Y_0 . Soit $f_0 : E \rightarrow E_0$ le morphisme canonique et soit

$E_0 = A_0 Y_0 \oplus A_0(e_0 - Y_0) \oplus K_{1,0}$ la décomposition de Peirce associée à Y_0 . Tout élément $f_0(X)$ de $f_0(E)$ se met de façon unique sous la forme $f_0(X) = a_X Y_0 + b_X(e_0 - Y_0) + Z_0$, ($a_X, b_X \in A_0, Z_0 \in K_{1,0}$).

Soit $Q^{(2)}$ une forme quadratique multiplicative sur E distincte de Q. Le noyau $K_{1,0}^{(2)}$ de $(E_0, Q^{(2)})$ où $Q^{(2)}$ est l'extension de $Q^{(2)}$ à E_0 , est soit $A_0 Y_0 \oplus K_{1,0}$, soit $A_0(e_0 - Y_0) \oplus K_{1,0}$ (preuve de la proposition 4.2.1). Soit par exemple $K_{1,0}^{(2)} = A_0 Y_0 \oplus K_{1,0}$, alors :

$$B_Q(X,e) = B_{Q_0}(f_0(X), e_0) = a_X + b_X, B_{Q^{(2)}}(X,e) = B_{Q^{(2)}}(f_0(X), e_0) = 2b_X, Q^{(2)}(X) = b_X^2$$

Puisque 2 est inversible et puisque $a_X + b_X$ et $2b_X$ appartiennent à A, a_X et b_X appartiennent à A.

On vérifie facilement que l'application $Q^{(3)}$ définie sur E par $Q^{(3)}(X) = a_X^2$ est une forme quadratique multiplicative sur E distincte de Q et $Q^{(2)}$. Le raisonnement est analogue lorsqu'on remplace $A_0 Y_0 \oplus K_{1,0}$ par $A_0(e_0 - Y_0) \oplus K_{1,0}$.

Donc, lorsqu'il existe deux formes quadratiques multiplicatives sur E, il en existe trois.

§ 3 - Formes quadratiques multiplicatives sur une Q-algèbre alternative

Soit E une Q-algèbre sur A. Lorsque 2 est inversible dans A, on peut associer à E la Q-algèbre commutative E_+ , mais la recherche des formes quadratiques multiplicatives sur E ne se ramène pas à la recherche des formes quadratiques multiplicatives sur E_+ . Par exemple, la norme réduite d'une algèbre de quaternions E sur un corps de caractéristique $\neq 2$ est multiplicative sur E et non dégénérée, elle n'est donc pas multiplicative sur E_+ .

1 - Formes quadratiques multiplicatives sur une Q-algèbre alternative qui possède un idempotent non trivial

Proposition 4.3.1

On suppose que A ne possède pas d'idempotents non triviaux et que 2 est inversible dans A. Soit E une Q-algèbre alternative qui possède un idempotent non trivial Y et soit $E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ la décomposition de Peirce associée à Y.

Il existe exactement zéro, une ou trois formes quadratiques multiplicatives sur E. Dans les deux derniers cas, Q est multiplicative. Pour qu'il existe trois formes quadratiques multiplicatives sur E, il faut et il suffit que $E_{10} \oplus E_{01} = K_1$. Lorsque cette condition est vérifiée, les trois formes sont multiplicatives sur E_+ .

Preuve

Soit e l'unité de E. Comme dans le cas commutatif, toute forme quadratique Q' multiplicative sur E vérifie l'une des conditions

a) $Q'(Y) = 0$ et $Q'(e - Y) = 0$

b) $Q'(Y) = 0$ et $Q'(e - Y) = 1$

c) $Q'(Y) = 1$ et $Q'(e - Y) = 0$

Q' est nulle sur les sous-espaces E_{10} et E_{01} . En effet, puisque

$$E_{10} = \{X \mid X \in E, YX = X \text{ et } X(e-Y) = X\} \text{ et } E_{01} = \{X \mid X \in E, (e-Y)X = X \text{ et } XY = X\},$$

$$Q'(X) = Q'(Y)Q'(X) = Q'(e-Y)Q'(X) \text{ pour tout élément } X \text{ de } E_{10} \cup E_{01}.$$

Puisque Q' vérifie a), b) ou c), $Q'(X) = 0$.

- Lorsqu'une forme quadratique multiplicative vérifie la condition a), elle coïncide avec Q.
En effet, soit Q' une telle forme.

Puisque $Q(e) = 1 = Q'(e)$ et $Q'(Y) = Q'(e-Y) = 0 = Q(Y) = Q(e-Y)$, Q et Q' coïncident sur $E_{11} \oplus E_{00}$.

Q est nulle sur $E_{10} \cup E_{01}$ (prop. 3.3.1). Donc Q et Q' coïncident sur $E_{10} \cup E_{01}$.

$E_{10} \oplus E_{01}$ est orthogonal à $E_{11} \oplus E_{00}$ pour Q (prop. 3.3.1). D'autre part, pour tout élément X de E_{10} , $B_Q(Y, X) = B_Q(Y^2, YX) = Q'(Y) B_Q(Y, X) = 0$ et

$B_Q(e-Y, X) = B_Q((e-Y)^2, X(e-Y)) = 0$. Donc E_{10} est orthogonal à $E_{11} \oplus E_{00}$ pour Q'; de même E_{01} est orthogonal à $E_{11} \oplus E_{00}$ pour Q'.

Il reste à comparer $B_Q(X, X')$ et $B_Q(X, X')$ pour X dans E_{10} et X' dans E_{01} . Soient $X_{10} \in E_{10}$ et $X_{01} \in E_{01}$. D'après le § 3, chap. III, $X_{01} X_{10} = -B_Q(X_{10}, X_{01})(e-Y)$.

$$\text{Puisque } Q'(X_{01} + Y) = Q'(X_{01}Y + Y^2) = 0,$$

$$0 = Q'(X_{01} + Y) Q'(X_{10} + Y) = Q' \left[-B_Q(X_{10}, X_{01}) (e-Y) + X_{01} + X_{10} + Y \right]$$

d'où, compte tenu de ce qui précède,

$$0 = -B_Q(X_{10}, X_{01}) + B_Q(X_{10}, X_{01}).$$

- Toute forme quadratique multiplicative Q' qui vérifie b) admet pour noyau $E_{11} \oplus E_{10} \oplus E_{01}$.

En effet, on sait déjà que les sous-espaces E_{11} , E_{10} et E_{01} sont totalement isotropes pour Q' . De plus, pour tout élément X de E_{10} ,

$$B_Q(Y, X) = B_Q(Y^2, YX) = Q'(Y) B_Q(Y, X) = 0$$

$$\text{et } B_Q(e-Y, X) = B_Q((e-Y)^2, (e-Y)X) = Q'(e-Y) B_Q(e-Y, X) = 0.$$

Donc E_{10} est orthogonal à $E_{11} \oplus E_{00}$ pour Q' . De même, E_{01} est orthogonal à $E_{11} \oplus E_{00}$ pour Q' .

D'autre part, pour tout élément X_{10} de E_{10} et tout élément X_{01} de E_{01} ,

$$Q'(X_{10} + e) = 1, \quad Q'(X_{01} + e) = 1$$

$$Q'(X_{10} + e) Q'(X_{01} + e) = Q' \left[-B_Q(X_{10}, X_{01}) Y + X_{10} + X_{01} + e \right]$$

$$1 = 1 + B_Q(X_{10}, X_{01})$$

$$\text{Donc } B_Q(X_{10}, X_{01}) = 0.$$

Il reste à voir si inversement la forme Q' qui vérifie b), $Q'(e) = 1$, et admet pour noyau $E_{11} \oplus E_{10} \oplus E_{01}$ peut effectivement être multiplicative.

Pour tout élément X_{10} de E_{10} et tout élément X_{01} de E_{01} ,

$$Q'[(X_{01} + Y) X_{01}] = Q'[-B_Q(X_{10}, X_{01}) (e-Y) + X_{10}] = B_Q^2(X_{10}, X_{01})$$

$$Q'[(X_{01} + e-Y) (X_{10} + e-Y)] = Q'[-B_Q(X_{10}, X_{01})(e-Y) + e-Y] = B_Q^2(X_{10}, X_{01}) - 2B_Q(X_{10}, X_{01}) + 1$$

$$\text{et } Q'(X_{01} + Y) = 0, \quad Q'(X_{01} + e-Y) = Q'(X_{10} + e-Y) = 1.$$

Il en résulte que lorsque Q' est multiplicative, on a, pour tout élément X_{01} de E_{01} et tout élément X_{10} de E_{10} , $B_Q(X_{10}, X_{01}) = 0$, ce qui implique que $E_{10} \oplus E_{01} = K_1$, (K_1 est le noyau de (E, Q) et $E_{10} \oplus E_{01} = E'''$).

Inversement, il est immédiat que lorsque $K_1 = E'''$, Q' est multiplicative sur E .

En échangeant les rôles de Y et $e-Y$, on voit que toute forme quadratique multiplicative Q' qui vérifie c) admet pour noyau $E_{00} \oplus E'''$ et que l'unique forme quadratique Q' qui vérifie c), $Q'(e) = 1$, et admet pour noyau $E_{00} \oplus E'''$, est multiplicative sur E si et seulement si $K_1 = E'''$.

En définitive :

Lorsque $K_1 \neq E''''$, il existe au plus une forme quadratique multiplicative sur E.

Lorsqu'elle existe, cette forme est la forme Q.

- Lorsque $K_1 = E''''$, il existe exactement trois formes quadratiques multiplicatives sur E qui sont les formes quadratiques multiplicatives sur E_+ .

2 - Formes quadratiques multiplicatives sur une Q-algèbre alternative sur A lorsque A est intègre et $2 \neq 0$

Proposition 4.3.2

On suppose A intègre et $2 \neq 0$. Soit E une Q-algèbre alternative sur A. On note E_0 l'algèbre obtenue par extension des scalaires au corps des fractions A_0 de A, Q_0 l'extension de Q à E_0 , et $K_{1,0}$ le noyau de (E_0, Q_0) .

Il existe au plus trois formes quadratiques multiplicatives sur E. Lorsqu'il existe au moins deux formes quadratiques multiplicatives sur E, Q est multiplicative sur E, K_1 est distinct de H et $K_{1,0}$ est de codimension 2.

Lorsque de plus 2 est inversible dans A, il existe exactement zéro, une ou trois formes quadratiques multiplicatives sur E.

Preuve

Puisque E est alternative, E_0 est une A_0 -algèbre alternative.

- Lorsqu'il existe au moins deux formes quadratiques Q' et Q'' multiplicatives sur E, les extensions Q'_0 et Q''_0 sont multiplicatives et distinctes sur E_0 . Il existe donc une sous-algèbre quadratique de E_0 sur laquelle Q'_0 et Q''_0 sont distinctes, E_0 possède un idempotent non trivial (prop. 4.1.2, cor. 2). Donc d'après la proposition 4.3.1, il existe sur E_0 trois formes quadratiques multiplicatives, H_0 est $\neq K_0$ (donc $H \neq K$), $K_{1,0}$ est de codimension 2, Q_0 est multiplicative sur E_0 , (donc Q est multiplicative sur E), et il existe au plus trois formes quadratiques multiplicatives sur E.

- On suppose maintenant que 2 est inversible dans A. Lorsque $K_{1,0}$ est de codimension 2 et $H_0 \neq K_{1,0}$, E_0 admet un idempotent non trivial Y_0 et $K_{1,0} = E''''_{0,Y_0}$ (raisonnement analogue au raisonnement de la proposition 4.2.2). Il existe donc sur E_0 trois formes quadratiques multiplicatives qui sont aussi les trois formes quadratiques multiplicatives sur $(E_0)_+$. Lorsqu'il existe deux formes quadratiques multiplicatives sur E, ces deux formes sont multiplicatives sur

E_+ car leurs extensions sont multiplicatives sur E_0 et $(E_0)_+$, il existe donc trois formes quadratiques multiplicatives sur E_+ (prop. 4.2.3). Comme leurs extensions sont multiplicatives sur E_0 , ces trois formes sont multiplicatives sur E .

REFERENCES

- B. A. BOURBAKI N. - Algèbre
B.A.C. BOURBAKI N. - Algèbre commutative
- [1] BOREVITCH-CHAFAREVITCH - Théorie des nombres
[2] BRAUN H. et KOECHER M. - Jordan Algebren (Springer 1966)
[3] HECKE E. - Algebraische Zahlen (Chelsea)
[4] SCHAFER R.D. - An introduction to non associative algebras
(Academic Press 1966)
[5] SCHAFER R.D. - Forms permitting composition
(Advances in Mathematics, Vol 4 n° 2, avril 1970)
[6] LEGRAND D. - Formes quadratiques et algèbres quadratiques
(Thèse Orsay 1971)
- LEGRAND D. - Comptes rendus
- [7] t. 265 p. 764-767 (6 décembre 1967)
[8] t. 267 p. 433-436 (23 septembre 1968)
[9] t. 273 p. 479-482 (20 septembre 1971)
[10] t. 273 p. 548-550 (27 septembre 1971)

(Manuscrit reçu le 9 septembre 1974)