

MÉMOIRES DE LA S. M. F.

ANTONIO PAQUES

Sur la cohomologie des formes quadratiques

Mémoires de la S. M. F., tome 59 (1979), p. 101-113

http://www.numdam.org/item?id=MSMF_1979__59__101_0

© Mémoires de la S. M. F., 1979, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (<http://smf.emath.fr/Publications/Memoires/Presentation.html>) 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/>

SUR LA COHOMOLOGIE DES FORMES QUADRATIQUES.

par

Antonio PAQUES

Le but de cet article est de généraliser les résultats obtenus par T.A. Springer [12] sur l'équivalence de formes quadratiques sous un point de vue de cohomologie de groupes.

On supposera toujours que tout anneau est commutatif à élément unité, tout module est unitaire, toute algèbre est associative (non nécessairement commutative) à élément unité et tout homomorphisme d'anneaux (resp. d'algèbres) transforme élément unité en élément unité.

1. Soient R un anneau et M un R -module. Si M est muni d'une forme quadratique q , on dira que (M, q) est un R -module quadratique. Si, de plus, M est projectif de type fini et q est non dégénérée, on dira que (M, q) est un R -espace quadratique. Si $f : R \rightarrow S$ est un homomorphisme d'anneaux et (M, q) est un R -module quadratique, il existe une unique forme quadratique $q^S : \otimes_R M \rightarrow S$ rendant commutatif le diagramme suivant

$$\begin{array}{ccc} M & \xrightarrow{q} & R \\ f \otimes \text{id}_M \downarrow & & \downarrow f \\ S \otimes_R M & \xrightarrow{q^S} & S \end{array} \quad (\text{cf. [6]}).$$

Désignons par $U(R)$ le groupe multiplicatif des éléments inversibles de l'anneau R et considérons les ensembles $R^\circ = \{x \in R \mid 1-4x \in U(R)\}$ et $J = \{x-x^2 \mid x \in R \text{ et } 1-2x \in U(R)\}$. L'ensemble R° , muni de l'opération $(x, y) \mapsto xoy = x+y-4xy$, est un groupe abélien et J est un sous-groupe de R° . On notera $G(R)$ le groupe quotient R°/J de R° par J . Si $2 \in U(R)$, $G(R) = U(R)/U^2(R)$ et si $2 \notin U(R)$, $G(R) = R/\{x-x^2 \mid x \in R\}$ (cf. [7]).

Supposons, maintenant que R soit local et que (M, q) soit un R -espace quadratique. Si $2 \in U(R)$, il existe une base $\{x_1, \dots, x_n\}$ de M telle que

$$q\left(\sum_{i=1}^n \xi_i x_i\right) = \sum_{i=1}^n \alpha_i \xi_i^2, \text{ avec } \alpha_i \in U(R), 1 \leq i \leq n \quad (\text{cf. [7]}).$$

Si $2 \notin U(R)$, le rang de M est pair et il existe une base $\{x_1, \dots, x_{2m}\}$ de M telle que

$$q\left(\sum_{i=1}^{2m} \xi_i x_i\right) = \sum_{i=1}^m (\alpha_i \xi_i^2 + \beta_i \xi_i \xi_{i+m} + \gamma_i \xi_{i+m}^2), \text{ avec } \alpha_i, \beta_i \in U(R), 1 \leq i \leq m$$

(cf. [7]). Le discriminant $\Delta(q)$ de la forme quadratique q est un élément de $G(R)$ décrit par

$$\Delta(q) = \prod_{i=1}^n \alpha_i \pmod{U^2(R)}, \text{ si } 2 \in U(R) \text{ et}$$

$$\Delta(q) = \alpha_1 \gamma_1 \circ \dots \circ \alpha_m \gamma_m \pmod{J}, \text{ si } 2 \notin U(R).$$

Etant donnés deux R-modules quadratiques (M, q) et (M_1, q_1) , on dit que q et q_1 sont équivalentes si il existe un isomorphisme de R-modules $t : M_1 \rightarrow M$ tel que le diagramme

$$\begin{array}{ccc} M_1 & \xrightarrow{t} & M \\ & \searrow q_1 & \swarrow q \\ & R & \end{array}$$

soit commutatif.

Il s'agira dans ce paragraphe, étant donnés deux R-espaces quadratiques (M, q) et (M, q_1) , d'étudier l'existence d'extensions galoisiennes S de R telles que q^S et q_1^S soient équivalentes.

Soient S un anneau, G un groupe fini d'automorphismes de S et $R=S^G$. On dit que S est une extension galoisienne de l'anneau R , de groupe G , si S est une R-algèbre séparable, projective de type fini et de rang $[G:1]$ comme R-module. La notion d'extension quadratique d'un anneau est aussi utilisée dans ce paragraphe. Une R-algèbre S est une extension quadratique de l'anneau R si S est séparable, fidèle, projective de type fini et de rang 2 comme R-module. Toute extension quadratique d'un anneau R est aussi une extension galoisienne de R (cf. [11] et [6]). Dans le cas local, une extension quadratique d'un anneau R est de type $R[x]$, avec $x^2 = bx+c$, où b et c sont éléments dans R tels que $b^2+4c \in U(R)$. Le groupe de Galois de $R[x]$ sur R est cyclique d'ordre 2, dont le générateur est $\sigma : x \mapsto b-x$. Pour d'autres résultats concernant les extensions galoisiennes et quadratiques d'un anneau on renvoie à la bibliographie (cf. [1], [3], [6], [8], [11] et [13]).

Un anneau local R d'idéal maximal \mathfrak{m} est quadratiquement hensélien si tout polynôme de la forme $X^2 + \alpha X + \beta$ dans $R[X]$ admettant deux racines distinctes dans R/\mathfrak{m} , module $\mathfrak{m} R[X]$, admet aussi deux racines (nécessairement distinctes) dans R .

Proposition 1.1 : Soit R un anneau local d'idéal maximal \mathfrak{m} . Toute extension quadratique $R[X]$ de R , avec $x^2 = bx+c$ et telle que le polynôme $X^2 - bX - c$ soit irréductible sur R , est un anneau local si, et seulement si, R est quadratiquement hensélien.

Démonstration : Soit $R[x]$, avec $x^2 = bx+c$, une extension quadratique de R . Supposons que R soit quadratiquement hensélien et que le polynôme $X^2 - bX - c$ soit irréductible sur R . Pour montrer que $R[x]$ est un anneau local il suffit de vérifier que tout élément dans $R[x] - \mathfrak{m} R[x]$ est inversible dans $R[x]$. Un élément $y = \alpha + \beta x \in R[x]$ est inversible dans $R[x]$ si et seulement si, sa norme $N(y) = y \sigma(y) = (\alpha + \beta x)(\alpha + \beta(b-x)) = \alpha^2 + \alpha\beta b - \beta^2 c$ est inversible dans R . Remarquons que $c \notin \mathfrak{m}$ car, sinon, nous aurions le polynôme $X^2 - bX - c$ réductible sur R , contrairement à la supposition initiale. Maintenant, on voit aisément que $N(\alpha + \beta x)$ est inversible dans R si, et seulement si, $\alpha \notin \mathfrak{m}$ ou $\beta \notin \mathfrak{m}$, ce qui montre l'assertion.

Réciproquement, soit $X^2 + \alpha X + \beta \in R[X]$ un polynôme admettant deux racines distinctes dans R/\mathfrak{m} , modulo $\mathfrak{m}R[X]$. Donc, $\alpha^2 - 4\beta$ est inversible dans R , ce qui veut dire que $R[x]$, avec $x^2 = -\alpha x - \beta$, est une extension quadratique de R .

D'autre part si un élément $a \in R$ satisfait $a^2 + \alpha a + \beta \equiv 0 \pmod{\mathfrak{m}}$, l'élément $a-x \in R[x] - \mathfrak{m}R[x]$ n'est pas inversible dans $R[x]$, ce qui signifie que $R[x]$ n'est pas local. Donc, le polynôme $X^2 + \alpha X + \beta$ est réductible sur R et, par conséquent, $X^2 + \alpha X + \beta$ admet deux racines dans R . Ceci montre que R est quadratiquement hensélien. ■

Corollaire 1.2 : Soient R un anneau local et $R[x]$, avec $x^2 = bx+c$, une extension quadratique de R . Si R est hensélien et le polynôme $X^2 - bX - c$ est irréductible sur R , alors $R[x]$ est un anneau local et hensélien.

La démonstration de ce corollaire est une conséquence immédiate de la Proposition 1.1 et du corollaire 16, chap. VII, § 43 de [9].

Théorème 1.3 : Soient R un anneau local et (M, q) et (M, q_1) deux R -espaces quadratiques. Alors il existe une extension galoisienne S de R telle que q^S et q_1^S soient équivalentes. Si de plus R est hensélien, S est aussi un anneau local et hensélien.

Démonstration : Dans cette démonstration \otimes signifiera \otimes_R .

i) $2 \in U(R)$: soient $\{x_1, \dots, x_n\}$ et $\{y_1, \dots, y_n\}$ bases de M telles que

$$q\left(\sum_{j=1}^n \xi_j x_j\right) = \sum_{j=1}^n \alpha_j \xi_j^2 \quad \text{et} \quad q_1\left(\sum_{j=1}^n \xi_j y_j\right) = \sum_{j=1}^n \beta_j \xi_j^2$$

avec α_j et β_j inversible dans R (cf. [7]) et considérons les extensions quadratiques $R[\gamma_j]$ et $R[\gamma_{n+j}]$ de R , avec $\gamma_j^2 = \alpha_j$ et $\gamma_{n+j}^2 = \beta_j$, $1 \leq j \leq n$. Soit I l'ensemble des indices i tels que $X^2 - \gamma_i^2$ soit irréductible sur $\otimes_{k \neq i} R[\gamma_k]$ et considérons $S = \otimes_{i \in I} R[\gamma_i]$. L'algèbre S , ainsi obtenue, est une extension galoisienne de R comme produit tensoriel d'extensions galoisiennes de R (cf. [1]) et vérifie la première partie du théorème.

Supposons, maintenant, que R soit hensélien. La vérification que S est un anneau local et hensélien se fait par récurrence sur le cardinal de l'ensemble $I = \{i_1, \dots, i_r \mid 1 \leq r \leq 2n\}$. L'extension quadratique $R[\gamma_{i_1}]$ est, évidemment, un anneau local et hensélien. Soit (par hypothèse de récurrence) $S' = R[\gamma_{i_1}] \otimes \dots \otimes R[\gamma_{i_s}]$ avec $1 \leq s \leq r$, un anneau local et hensélien. L'algèbre $S' \otimes R[\gamma_{i_{s+1}}] \simeq S'[X]/(X^2 - \gamma_{i_{s+1}}^2)$ est une extension quadratique de S' et, puisque

le polynôme $X^2 - \gamma_{i,s+1}^2$ est irréductible sur S' (car il est irréductible sur

$\otimes_{k \neq s+1} R[\gamma_{i,k}]$), alors $S' \otimes R[\gamma_{i,s+1}]$ est un anneau local et hensélien (cf. cor.1.2).

Donc, S est un anneau local et hensélien.

ii) $2 \in U(R)$: Dans ce cas le rang de M est pair et soient $\{x_1, \dots, x_{2m}\}$ et $\{y_1, \dots, y_{2m}\}$ deux bases de M telles que

$$q\left(\sum_{j=1}^{2m} \xi_j x_j\right) = \sum_{j=1}^m (\alpha_j \xi_j^2 + \beta_j \xi_j \xi_{j+m} + \gamma_j \xi_{j+m}^2)$$

et

$$q_1\left(\sum_{j=1}^{2m} \xi_j y_j\right) = \sum_{j=1}^m (\lambda_j \xi_j^2 + \mu_j \xi_j \xi_{j+m} + \nu_j \xi_{j+m}^2),$$

avec $\alpha_j, \beta_j, \lambda_j$ et μ_j inversibles dans R , $1 \leq j \leq m$, (cf [7]). Considérons les extensions quadratiques $R[w_j]$ et $R[w_{j+m}]$ de R , avec $w_j^2 = -\alpha_j^{-1} \beta_j w_j - \alpha_j^{-1} \gamma_j$ et $w_{j+m}^2 = -\lambda_j^{-1} \mu_j w_{j+m} - \lambda_j^{-1} \nu_j$, $1 \leq j \leq m$. Soit I l'ensemble des indices i tels que $X^2 + \alpha_j^{-1} \beta_j X + \alpha_j^{-1} \gamma_j$ (si $i=j$) ou $X^2 + \lambda_j^{-1} \mu_j X + \lambda_j^{-1} \nu_j$ (si $i=j+m$) soit irréductible sur

$\otimes_{k \neq i} R[w_k]$. Soit $S = \otimes_{i \in I} R[w_i]$. On vérifie, comme dans i), que S satisfait l'assertion du théorème. ■ $i \in I$

Etant donné une extension galoisienne S d'un anneau R et deux R -modules quadratiques (M, q) et (M, q_1) , si q^S et q_1^S sont équivalentes on dit que les formes quadratiques q et q_1 sont S -équivalentes.

2. Soient R un anneau et (M, q) un R -module quadratique. L'algèbre de Clifford de (M, q) , qu'on note $C(M, q)$, est le quotient de l'algèbre tensorielle $T(M)$ par l'idéal bilatère $I(q)$ engendré par les éléments $x^2 - q(x)1_{T(M)}$, $x \in M$.

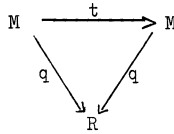
Remarquons que $C(M, q)$ est la solution du problème universel posé par les applications R -linéaires $g: M \rightarrow A$, où A est une R -algèbre, telles que $g(x)^2 = q(x)1_A$, $x \in M$.

Si on gradue $T(M)$ sur $\mathbb{Z}/2\mathbb{Z}$ par $T_0(M) = \otimes_{i \geq 0} T^{2i}(M)$ et $T_1(M) = \otimes_{i \geq 0} T^{2i+1}(M)$ (où $T^j(M) = \otimes_{\mathbb{R}}^j M$), alors $I(q)$ est homogène vis à vis de cette gradation et $C(M, q) = C_0(M, q) \oplus C_1(M, q)$; $C_0(M, q)$ est une sous-algèbre de $C(M, q)$ engendrée par les éléments $xy \pmod{I(q)}$, $x, y \in M$. Si (M, q) est un R -espace quadratique, M s'identifie à un sous-module de $C_1(M, q)$.

Etant donné deux R -espaces quadratiques (M_1, q_1) et (M, q) , tout homomorphisme de R -modules $t: M_1 \rightarrow M$ qui satisfait $q_1(x) = q(t(x))$, s'étend à un homomorphisme de R -algèbres $C(t): C(M_1, q_1) \rightarrow C(M, q)$ tel que $C(t)(M_1) \subset M$. Inversement, tout homomorphisme de R -algèbres $t': C(M_1, q_1) \rightarrow C(M, q)$ tel que $t'(M_1) \subset M$ donne lieu, par restriction à M_1 , à un homomorphisme de R -modules $t = t'|_{M_1}: M_1 \rightarrow M$ vérifiant $q(t(x)) = q_1(x)$, $x \in M_1$. De plus, puisque q et q_1 sont non dégénérées, $C(t)$ est injectif (resp. surjectif, bijectif) si, et seulement si, t est injectif (resp. surjectif, bijectif).

Ensuite supposons que R soit local et que (M, q) soit un R -espace quadratique. On dira qu'un R -automorphisme t de M est orthogonal si le

diagramme suivant



est commutatif. L'ensemble des

R -automorphismes orthogonaux de (M, q) forme un groupe, appelé le groupe orthogonal de (M, q) et on le désignera par $O(M, q)$ (ou $O(q)$). Le groupe orthogonal unimodulaire de (M, q) , qu'on note $SO(M, q)$ (ou $SO(q)$) est le sous-groupe de $O(M, q)$ défini par $SO(M, q) = \{t \mid t \in O(M, q) \text{ et } C(t)|_{Z(C_0)} = \text{id}\}$ si $2 \notin U(R)$, où $Z(C_0)$ désigne le centre de $C_0(M, q)$. Dans le cas $2 \in U(R)$, $SO(M, q) = \{t \mid t \in O(M, q) \text{ et } d(t) = 1\}$, où $d(t)$ désigne le déterminant de t .

Soient, maintenant, (M, q_1) un autre R -espace quadratique et S une extension galoisienne de R telle que les formes quadratiques q et q_1 soient S -équivalentes. Désignons par G le groupe de Galois de S sur R .

Etant donnés $\sigma \in G$ et une application η de $S \otimes_R M$ dans S (resp. $S \otimes_R M$), on définit l'application $\sigma\eta$ de $S \otimes_R M$ dans S (resp. $S \otimes_R M$) par $\sigma\eta(x) = \sigma(\eta(\sigma^{-1}(x)))$, où $\sigma : S \otimes_R M \rightarrow S \otimes_R M$ est donné par $\sigma(s \otimes m) = \sigma(s) \otimes m$, $s \in S$, $m \in M$. Remarquons que si $t \in O(q^S)$ il y en a de même de σt . Maintenant, si $t : S \otimes_R M \rightarrow S \otimes_R M$ est un isomorphisme de S -modules tel que $q^S(t(x)) = q_1^S(x)$, $x \in S \otimes_R M$, puisque $\sigma q^S = q^S$ et $\sigma q_1^S = q_1^S$, on a $q^S(t(x)) = q_1^S(x) = \sigma q_1^S(x) = \sigma(q_1^S(\sigma^{-1}(x))) = \sigma q^S(\sigma t(x)) = q^S(\sigma t(x))$ et alors il existe $u_\sigma \in O(q^S)$ tel que $u_\sigma t = \sigma t$, quel que soit $\sigma \in G$. En outre, $(\sigma\tau)t = \sigma(\tau t) = \sigma(u_\tau t) = (\sigma u_\tau) u_\sigma t$, d'où $u_{\sigma\tau} = (\sigma u_\tau) u_\sigma$, $\sigma, \tau \in G$.

D'autre part, si $t' : S \otimes_R M \rightarrow S \otimes_R M$ est un autre automorphisme de S -modules tel que $q^S(t'(x)) = q_1^S(x)$, $x \in S \otimes_R M$, alors on a aussi $\sigma t' = u'_\sigma t'$, avec $u'_\sigma \in O(q^S)$ et il existe $u \in O(q^S)$ tel que $u'_\sigma = (\sigma u) u_\sigma^{-1}$, quel que soit $\sigma \in G$.

Donc, toute forme quadratique q_1 sur M , qui est S -équivalente à q , donne lieu à une classe de cohomologie, notée par $c_S(q, q_1)$, de l'ensemble $H^1(G, O(q^S))$ de 1-cohomologie non abélienne de G à valeurs dans $O(q^S)$, représentée par le cocycle $f : G \rightarrow O(q^S)$ tel que $f(\sigma) = (\sigma t) t^{-1}$, $\sigma \in G$, où t est un S -automorphisme de $S \otimes_R M$ vérifiant $q^S(t(x)) = q_1^S(x)$, $x \in S \otimes_R M$. Remarquons que la représentation de la classe $c_S(q, q_1)$ ne dépend pas de l'automorphisme t .

Théorème 2.1 : Soient R un anneau local, S une extension galoisienne de R de groupe G et (M, q) un R -espace quadratique. Il existe une correspondance bijective entre les classes d'équivalence de formes quadratiques q_1 sur M , qui sont S -équivalentes à q et les éléments de l'ensemble $H^1(G, O(q^S))$.

Démonstration : Soient q_1 et q_2 formes quadratiques S -équivalentes à q . Supposons que $c_S(q, q_1) = c_S(q, q_2)$. Alors on a $q_i^S(x) = q^S(t_i(x))$, $x \in S \otimes_R M$, ($i=1,2$) où t_1 et t_2 sont des S -automorphismes de $S \otimes_R M$. On peut choisir ces automorphismes tels que $\sigma t_i = h(\sigma)t_i$ ($i=1,2$), où $h: G \rightarrow O(q^S)$ est un cocycle représentant de la classe $c_S(q, q_1) = c_S(q, q_2)$. Donc, $\sigma(t_2^{-1}t_1) = t_2^{-1}t_1$, quel que soit $\sigma \in G$ et alors il existe un R -automorphisme t de M tel que $t_2^{-1}t_1 = \text{id}_S \otimes t$ (cf. [5]). C'est évident que $q_2(t(x)) = q_1(x)$, $x \in M$, ce qui montre que q_1 et q_2 sont équivalentes.

Inversement si q_1 et q_2 sont équivalentes, il est trivial que $c_S(q, q_1) = c_S(q, q_2)$.

Finalement, si c est un élément arbitraire de $H^1(G, O(q^S))$, représenté par le cocycle $h: G \rightarrow O(q^S)$, il existe un S -automorphisme t de $S \otimes_R M$ tel que $h(\sigma) = (\sigma t)t^{-1}$, $\sigma \in G$ (cf. [5]). Soit $q': S \otimes_R M \rightarrow S$ la forme quadratique donnée par $q'(x) = q^S(t(x))$, $x \in S \otimes_R M$. Alors, puisque $\sigma q' = q'$, quel que soit $\sigma \in G$, on a, tout de suite, $q' = q_1^S$, pour quelque forme quadratique $q_1: M \rightarrow R$. Ceci achève la démonstration du théorème. ■

Théorème 2.2 : Soient R un anneau local, S une extension galoisienne locale de R , de groupe G et (M, q) un R -espace quadratique. Il existe une correspondance bijective entre les classes d'équivalence de formes quadratiques q_1 sur M , qui sont S -équivalentes à q et ont même discriminant que q , et les éléments de l'ensemble $H^1(G, SO(q^S))$.

Démonstration : Soient q_1 une forme quadratique S -équivalente à q et $f: G \rightarrow O(q^S)$, donné par $f(\sigma) = (\sigma t)t^{-1}$, $\sigma \in G$, le cocycle représentant de la classe de 1-cohomologie $c_S(q, q_1) \in H^1(G, O(q^S))$, où t est un S -automorphisme de $S \otimes_R M$ vérifiant $q^S(t(x)) = q_1^S(x)$, $x \in S \otimes_R M$.

Il s'agit de montrer que $f(\sigma) \in SO(q^S)$, quel que soit $\sigma \in G$, si, et seulement si, $\Delta(q) = \Delta(q_1)$ dans $G(R)$ et pour cela il faut distinguer le cas où $2 \in U(R)$ de celui où $2 \notin U(R)$.

i) $2 \in U(R)$: Dans ce cas $G(R) = U(R)/U^2(R)$ et supposons que $\Delta(q) = \Delta(q_1) \pmod{U^2(R)}$. Alors il existe $\lambda \in U(R)$ tel que $\Delta(q_1) = \Delta(q)\lambda^2$. En outre, de $q_1^S(x) = q^S(t(x))$, $x \in S \otimes_R M$, on a $\Delta(q_1^S) = \Delta(q^S)(d(t))^2$, où $d(t)$ désigne le déterminant de t . Comme $\Delta(q^S) = \Delta(q)$ et $\Delta(q_1^S) = \Delta(q_1)$, on a $\lambda^2 = d(t)^2$ et, puisque S est un anneau local, il s'ensuit que $d(t) = \pm \lambda \in U(R)$. Ainsi, $\sigma(d(t)) = d(t)$ et, comme $d(\sigma t) = \sigma(d(t))$, on a $d(f(\sigma)) = 1$ ou $f(\sigma) \in SO(q^S)$, quel que soit $\sigma \in G$. Réciproquement, si $f(\sigma) \in SO(q^S)$, quel que soit $\sigma \in G$, on peut voir trivialement que $\Delta(q_1) = \Delta(q) \pmod{U^2(R)}$.

ii) $2 \notin U(R)$: Supposons que $\Delta(q_1) = \Delta(q)$ dans $G(R)$. Alors il existe $\lambda \in R$ tel que $\Delta(q_1) = \Delta(q) + (\lambda - \lambda^2)(1 - 4\Delta(q))$. De $q_1^S(x) = q^S(t(x))$, $x \in S \otimes_R M$, il s'ensuit que $C(t) : S \otimes_R C(M, q_1) \rightarrow S \otimes_R C(M, q)$ est un isomorphisme de S -algèbres, d'où $C_0(t) = C(t) \Big|_{S \otimes_R Z(C_0(M, q_1))} : S \otimes_R Z(C_0(M, q_1)) \rightarrow S \otimes_R Z(C_0(M, q))$ est aussi un isomorphisme de S -algèbres. Comme $Z(C_0(M, q_1))$ (resp. $Z(C_0(M, q))$) est l'extension quadratique $R[x]$ (resp. $R[y]$) de R , avec $x^2 = x - \Delta(q_1)$ (resp. $y^2 = y - \Delta(q)$) (cf. [4] et [7]) on peut écrire $C_0(t)(1 \otimes x) = \alpha 1 \otimes 1 + \beta 1 \otimes y$, avec $\alpha \in S$ et $\beta \in U(S)$. De l'équation $x^2 - x + \Delta(q_1) = 0$, on a $(\alpha 1 \otimes 1 + \beta 1 \otimes y)^2 - (\alpha 1 \otimes 1 + \beta 1 \otimes y) + \Delta(q_1) 1 \otimes 1 = 0$, d'où $\beta(\beta + 2\alpha - 1) = 0$ et $(\alpha^2 - \alpha) - \Delta(q)(\beta^2 - 1) = (\lambda^2 - \lambda)(1 - 4\Delta(q))$. Puisque S est un anneau local et $\beta \in U(S)$ on a, finalement, $\alpha = \lambda$ ou $\alpha = 1 - \lambda$ et $\beta = 1 - 2\alpha$, ce qui donne $\alpha, \beta \in R$. Alors $C_0(t) = \sigma C_0(t) = C_0(\sigma t)$ et $C(f(\sigma)) \Big|_{S \otimes_R Z(C_0(M, q))} = \text{id}$, ce qui signifie $f(\sigma) \in SO(q^S)$, quel que soit $\sigma \in G$. Réciproquement, de $f(\sigma) \in SO(q^S)$ il s'ensuit que $C_0(t) = C(t) \Big|_{S \otimes_R Z(C_0(M, q_1))} : S \otimes_R Z(C_0(M, q_1)) \rightarrow S \otimes_R Z(C_0(M, q))$ est un isomorphisme de S -algèbres vérifiant $\sigma C_0(t) = C_0(t)$, quel que soit $\sigma \in G$. Donc, il existe un isomorphisme de R -algèbres $t' : Z(C_0(M, q)) \rightarrow Z(C_0(M, q))$ tel que $C_0(t) = \text{id}_S \otimes t'$ (cf. [5]), d'où $\Delta(q_1) = \Delta(q)$ dans $G(R)$ (cf. [4]). ■

3. Pour les résultats de ce paragraphe nous aurons besoin des deux premières propositions suivantes.

Proposition 3.1 : Soient R un anneau local et (M, q) un R -espace quadratique. Alors, à tout R -automorphisme orthogonal t de (M, q) correspond un élément inversible a_t de $C(M, q)$ tel que $t(x) = d(t)a_t x a_t^{-1}$, $x \in M$, où $d(t)$ désigne le déterminant de t . L'élément a_t est déterminé à un facteur inversible près.

Pour la démonstration de cette proposition voir [2].

Proposition 3.2 : Soient R un anneau local d'idéal maximal \mathfrak{m} , (M, q) un R -espace quadratique et S une extension galoisienne locale de R , de groupe G . Alors, les éléments $a_t \in C(S \otimes_R M, q^S)$ qui satisfont la Prop. 3.1, pour chaque $t \in O(q^S)$, peuvent être choisis de manière à vérifier $a_{\sigma t} = \sigma(a_t)$, quel que soit $\sigma \in G$.

Remarque : Comme $C(S \otimes_R M, q^S) = S \otimes_R C(M, q)$, le groupe G opère sur $C(S \otimes_R M, q^S)$ de manière habituelle en identifiant $\sigma = \sigma \otimes \text{id}_{C(M, q)}$.

Démonstration : (de la prop. 3.2)

De $t(x) = d(t)a_t x a_t^{-1}$, on a $(\sigma t)(x) = d(t)(\sigma(a_t))x(\sigma(a_t^{-1}))$, $x \in S \otimes_R M$ et alors il existe $\lambda_{\sigma,t} \in U(S)$ tel que $\sigma(a_t) = \lambda_{\sigma,t} a_{\sigma t}$, quel que soit $\sigma \in G$.

Le corps $S/\mathfrak{m}S = R/\mathfrak{m} \otimes_R S$ est une extension galoisienne de R/\mathfrak{m} , dont le groupe de Galois est $\bar{G} = \{\bar{\sigma} = \text{id}_{R/\mathfrak{m}} \otimes \sigma \mid \sigma \in G\} \simeq G$ (cf. [3]). Pour l'indépendance linéaire des $\bar{\sigma} \in \bar{G}$, il existe $\lambda \in S$ tel que $\sum_{\tau \in \bar{G}} \bar{\lambda}_{\tau, \tau^{-1}t} \bar{\tau}(\bar{\lambda}) \neq 0 \pmod{\mathfrak{m}S}$, ce qui signifie $\lambda_t = \sum_{\tau \in G} \lambda_{\tau, \tau^{-1}t} \tau(\lambda) \in U(S)$. Alors, $\sigma(\lambda_t) = \lambda_{\sigma,t}^{-1} \lambda_{\sigma t}$

où $\lambda_{\sigma t} = \sum_{\tau \in G} \lambda_{\tau, \tau^{-1}\sigma t} \tau(\lambda)$ et, par suite, $\sigma(\lambda_t a_t) = \lambda_{\sigma t} a_{\sigma t}$. Donc, en remplaçant

$\lambda_{\sigma t} a_{\sigma t}$ par $a_{\sigma t}$, on a $\sigma(a_t) = a_{\sigma t}$, quels que soient $\sigma \in G$ et $t \in O(q^S)$. Ceci achève la démonstration. ■

Soient, maintenant, R un anneau local, S une extension galoisienne locale de R , avec groupe G et considérons deux R -espaces quadratiques (M, q) et (M, q_1) tels que q et q_1 soient S -équivalentes.

Etant donnée la classe $c_S(q, q_1) \in H^1(G, O(q^S))$, représentée par le cocycle $f : G \rightarrow O(q^S)$, tel que $f(\sigma) = u_\sigma$, il existe des éléments inversibles a_u dans $C(S \otimes_R M, q^S)$ tels que $u_\sigma(x) = d(u_\sigma) a_u x a_u^{-1}$, $x \in S \otimes_R M$, $\sigma \in G$ (cf. Prop. 3.1).

On vérifie, avec l'aide des Prop. 3.1 et 3.2, que l'application $\alpha : G \times G \rightarrow U(S)$ donnée par $\alpha(\sigma, \tau) = a_{u_{\sigma\tau}} a_{u_\sigma}^{-1} \sigma(a_{u_\tau}^{-1})$, $\sigma, \tau \in G$, est un 2-cocycle de G à valeurs dans $U(S)$ (avec G opérant sur $U(S)$ de manière habituelle). On voit aussi que si $f'(\sigma) = u'_\sigma$, $\sigma \in G$, est un autre cocycle représentant de la même classe $c_S(q, q_1)$ et si $\alpha'(\sigma, \tau) = a_{u'_{\sigma\tau}} a_{u'_\sigma}^{-1} \sigma(a_{u'_\tau}^{-1})$, $\sigma, \tau \in G$, est le 2-cocycle correspondant alors α et α' diffèrent par un cobord. Ceci montre qu'il existe une application T de l'ensemble $H^1(G, O(q^S))$ dans le groupe de 2-cohomologie $H^2(G, U(S))$ de G à valeurs dans $U(S)$, définie par $T(c_S(q, q_1)) = \alpha_S(q, q_1)$.

Proposition 3.3 : Soient R un anneau local, (M, q) et (M, q_1) deux R -espaces quadratiques et S une extension galoisienne de R de façon que $\alpha_S(q, q_1)$ soit définie.

- i) Si q et q_1 sont équivalentes alors $\alpha_S(q, q_1) = 1$
- ii) $\alpha_S(q, q_1)^2 = 1$

La démonstration de cette proposition est immédiate.

Théorème 3.4 : Soient R un anneau local d'idéal maximal \mathfrak{m} et S une extension galoisienne locale de R , de groupe G et de corps résiduel, $S/\mathfrak{m}S$ infini. Soient (M, q) et (M, q_1) deux R -espaces quadratiques, avec q et q_1

S-équivalentes. Si $\Delta(q_1) = \Delta(q)$ et $\alpha_S(q, q_1) = 1$, alors les R-algèbres $C(M, q)$ (resp. $C_0(M, q)$) et $C(M, q_1)$ (resp. $C_0(M, q_1)$) sont isomorphes.

Pour la démonstration de ce théorème la proposition suivante est nécessaire.

Proposition 3.5 : Soient R, S et G comme dans l'énoncé du Théorème 3.4.

Soit A une S-algèbre, libre et de type fini comme S-module. Si G se prolonge à un groupe d'automorphismes de A, alors $H^1(G, U(A)) = 0$.

Démonstration : Soit $f \in H^1(G, U(A))$ et considérons l'élément

$\sum_{\sigma \in G} f(\sigma) X_\sigma$ dans la $S[X_\sigma \mid \sigma \in G]$ -algèbre $A[X_\sigma \mid \sigma \in G]$. La norme $N(\sum_{\sigma \in G} f(\sigma) X_\sigma)$ de

cet élément, relativement à $S[X_\sigma \mid \sigma \in G]$, est un polynôme dans $S[X_\sigma \mid \sigma \in G]$.

D'autre part, le corps $S/\mathfrak{m}S = R/\mathfrak{m} \otimes_R S$ est une extension galoisienne de R/\mathfrak{m} ,

le groupe $\bar{G} = \{\bar{\sigma} = \text{id}_{R/\mathfrak{m}} \otimes \sigma \mid \sigma \in G\} \simeq G$ (cf. [3]) et, de l'indépendance algébrique des $\bar{\sigma} \in \bar{G}$, on a un élément s_0 de S vérifiant $N(\sum_{\sigma \in G} f(\sigma) X_\sigma)(s_0) \neq 0$

(mod $\mathfrak{m}S$), ce qui donne $N(\sum_{\sigma \in G} f(\sigma) \sigma(s_0)) = N(\sum_{\sigma \in G} f(\sigma) X_\sigma)(s_0) \in U(S)$.

Alors l'élément $a = \sum_{\sigma \in G} f(\sigma) \sigma(s_0)$ est inversible dans A et on voit

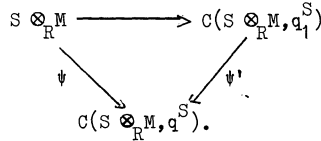
aisément que $f(\sigma) = \sigma(a^{-1})a$, quel que soit $\sigma \in G$, ce qui montre l'assertion de la proposition.

Démonstration : (du Théorème 3.4) De $\Delta(q_1) = \Delta(q)$ on a $c_S(q, q_1) \in H^1(G, SO(q^S))$ (cf. Th. 2.2). Soit $f: G \rightarrow SO(q^S)$, donnée par $f(\sigma) = u_\sigma$, $\sigma \in G$, le cocycle représentant de $c_S(q, q_1)$. Rappelons que $u_\sigma = (\sigma t)^{-1}$, où t est un S-automorphisme de $S \otimes_R M$ tel que $q^S(t(x)) = q_1^S(x)$, $x \in S \otimes_R M$.

Comme $\alpha_S(q, q_1) = 1$, on peut considérer le cocycle correspondant $\alpha: G \times G \rightarrow U(S)$ donné par $\alpha(\sigma, \tau) = 1$, ce qui entraîne que les éléments inversibles a_{u_σ} de $C(S \otimes_R M, q^S)$ satisfont $a_{u_{\sigma\tau}} = \sigma(a_{u_\tau}) a_{u_\sigma}$, quels que soient $\sigma, \tau \in G$.

Alors, il existe un élément inversible $a \in C(S \otimes_R M, q^S)$ tel que $a_{u_\sigma} = \sigma(a)^{-1} a$ (cf. Prop. 3.5) et, puisque $u_\sigma \in SO(q^S)$, on a $(\sigma t)(x) = u_\sigma(t(x)) = a_{u_\sigma} t(x) a_{u_\sigma}^{-1} = \sigma(a)(a^{-1} t(x) a) \sigma(a^{-1})$, $x \in S \otimes_R M$, $\sigma \in G$.

Soit $\psi: S \otimes_R M \rightarrow S \otimes_R C(M, q)$ l'application définie par $\psi(x) = a^{-1} t(x) a$, $x \in S \otimes_R M$. Comme ψ est S-linéaire et $\psi(x)^2 = q_1^S(x)$, $x \in S \otimes_R M$, il existe un homomorphisme de S-algèbres $\psi': C(S \otimes_R M, q_1^S) \rightarrow C(S \otimes_R M, q^S)$ rendant commutatif le diagramme suivant



Comme $S \otimes_R M$ engendre $C(S \otimes_R M, q^S)$ et ψ est injectif, alors $\psi'(S \otimes_R M) = \psi(S \otimes_R M)$ engendre $C(S \otimes_R M, q^S)$, ce qui montre que ψ' est surjectif. Mais, $C(S \otimes_R M, q^S)$ et $C(S \otimes_R M, q_1^S)$ sont des S -modules libres de type fini et ont même rang, donc ψ' est un isomorphisme. Puisque $\sigma\psi = \psi$, on a $\sigma\psi' = \psi'$, quel que soit $\sigma \in G$ et, par suite, il existe un isomorphisme de R -algèbres $\theta : C(M, q_1) \rightarrow C(M, q)$ vérifiant $\psi' = \text{id}_S \otimes \theta$ (cf. [5]). La vérification de ce que les R -algèbres $C_0(M, q)$ et $C_0(M, q_1)$ sont aussi isomorphes est immédiate. ■

Théorème 3.6 : Soient R un anneau local et (M, q) et (M, q_1) deux R -espaces quadratiques. Si le rang de M est 2 ou 3, $\Delta(q_1) = \Delta(q)$ et les R -algèbres $C(M, q)$ et $C(M, q_1)$ sont isomorphes, alors les formes quadratiques q et q_1 sont équivalentes.

Pour la démonstration de ce théorème voir [10].

Corollaire 3.7 : Soient $R, S, (M, q)$ et (M, q_1) comme dans l'énoncé du Théorème 3.4. Si le rang de M est 2 ou 3 alors les formes quadratiques q et q_1 sont équivalentes si et seulement si $\Delta(q) = \Delta(q_1)$ et $\alpha_S(q, q_1) = 1$.

La démonstration de ce corollaire est une conséquence triviale de la Prop. 3.3i) et des Théorèmes 3.4 et 3.6.

4. Dans tout ce paragraphe R désignera un anneau local où $2 \in U(A)$, de corps résiduel infini.

Soient $a, b \in U(R)$ et S une extension faloisienne locale de R , de groupe G et contenant les éléments λ et μ tels que $\lambda^2 = a$ et $\mu^2 = b$. Puisque S est un anneau local et $2 \in U(S)$, on a $\sigma(\lambda) = (-1)^{a_\sigma} \lambda$ et $\sigma(\mu) = (-1)^{b_\sigma} \mu$, où a_σ et b_σ sont des nombres entiers égaux à 0 et 1, quel que soit $\sigma \in G$. Considérons les applications $f, g : G \times G \rightarrow U(S)$ définies par

$$f(\sigma, \tau) = b, \text{ si } a_{\sigma\tau} = 1 \text{ et } f(\sigma, \tau) = 1, \text{ sinon}$$

et

$$g(\sigma, \tau) = (-1)^{a_\sigma b_\tau}$$

quels que soient $\sigma, \tau \in G$. Ces applications sont des 2-cocycles de G à valeurs dans $U(S)$ et on notera par (a, b) (resp. $[a, b]$) la classe de 2-cohomologie dans $H^2(G, U(S))$ représentée par f (resp. g).

Proposition 4.1 : Soient $a, b, c \in U(R)$. Alors

i) $(a^2, b) = 1$

ii) $(a, b) = (b, a)$

iii) $(ab, c) = (a, c)(b, c)$

iv) $(a, a) = (a, \neq 1)$

v) $(a, b) = [a, b]$

vi) $(a, b) = 1$ si et seulement si il existe des éléments x, y et z dans R tels que $x^2 - ay^2 - bz^2 = 0$ et un parmi eux est inversible.

Les propriétés de (a, b) énoncés dans cette proposition sont de vérification immédiate.

Etant donné un R -espace quadratique et une base $\{x_1, \dots, x_n\}$ de M telle que $q(\sum_{1 \leq i \leq n} \xi_i x_i) = \sum_{1 \leq i \leq n} a_i \xi_i^2$, avec $a_i \in U(R)$, considérons l'élément

$$h(q) = \prod_{i < j} (a_i, a_j) \in H^2(G, U(S)) \text{ où } S \text{ est une extension galoisienne locale de } R,$$

de groupe G et contenant les racines carrées des éléments $a_i, 1 \leq i \leq n$.

On peut montrer que cet élément $h(q)$ ne dépend pas du choix d'une base pour M et on l'appelle l'invariant de Hasse.

Soient, maintenant, (M, q) et (M, q_1) deux R -espaces quadratiques et $\{x_1, \dots, x_n\}$ une base de M telle que $q(\sum_{1 \leq i \leq n} \xi_i x_i) = \sum_{1 \leq i \leq n} a_i \xi_i^2$, avec $a_i \in U(R)$,

$1 \leq i \leq n$. En remplaçant q_1 par une forme quadratique équivalente, on peut aussi supposer que $q_1(\sum_{1 \leq i \leq n} \xi_i x_i) = \sum_{1 \leq i \leq n} b_i \xi_i^2$, avec $b_i \in U(R), 1 \leq i \leq n$.

Soit S une extension galoisienne locale de R , de groupe G et contenant les racines carrées des éléments a_i et $b_i, 1 \leq i \leq n$.

Il est évident que les formes quadratiques q et q_1 sont S -équivalentes. Un S -automorphisme t de $S \otimes_R M$ vérifiant $q^S(t(x)) = q_1^S(x), x \in S \otimes_R M$, peut être décrit, dans ce cas, par $t(1 \otimes x_i) = \gamma_i (1 \otimes x_i)$, où $\gamma_i^2 = b_i a_i^{-1}, 1 \leq i \leq n$. D'autre part il existe $u_\sigma \in O(q^S)$ tel que $u_\sigma t = \sigma t$, quel que soit $\sigma \in G$ (cf. Th. 2.1).

Alors, puisque $\sigma(\gamma_i) = (-1)^{i\sigma} \gamma_i$ ($\epsilon_{i\sigma} = 0, 1$), on a $u_\sigma(1 \otimes x_i) = (-1)^{\epsilon_{i\sigma}} (1 \otimes x_i)$ et on peut voir que $u_\sigma = t_1^{\epsilon_{1\sigma}} \dots t_n^{\epsilon_{n\sigma}}$, où $t_i \in O(q^S)$ est donné par

$$t_i(x) = x - \frac{\varphi^S(x, 1 \otimes x_i)}{q^S(1 \otimes x_i)} (1 \otimes x_i), x \in S \otimes_R M, 1 \leq i \leq n, \text{ avec } \varphi^S \text{ désignant la forme } S\text{-bilinéaire symétrique associée à } q^S.$$

Puisque $t_i(x) = -(1 \otimes x_i) x (1 \otimes x_i)^{-1}$ dans $C(S \otimes_R M, q^S)$, un élément a_n de $C(S \otimes_R M, q^S)$ qui vérifie la Prop. 3.1 par $u_\sigma, \sigma \in G$, est $a_\sigma = 1 \otimes (x_1^{\epsilon_{1\sigma}} \dots x_n^{\epsilon_{n\sigma}})$

Comme $\alpha_S(q, q_1)^2 = 1$ dans $H^2(G, U(S))$ (cf. Prop. 3.3), cette classe $\alpha_S(q, q_1)$ peut être aussi représentée par le cocycle $\alpha(\sigma, \tau) = \sigma(a_\tau) a_\sigma^{-1}$, quels que soient $\sigma, \tau \in G$. Alors, en calculant $\alpha(\sigma, \tau)$, on a

$$\alpha(\sigma, \tau) = (-1)^{\sum_{i < j} \epsilon_i \sigma \epsilon_j \tau} \cdot \epsilon_{i\sigma} \prod_{i\tau=1}^{a_i} \epsilon_i$$

ou

$$\alpha(\sigma, \tau) = \prod_{i < j} g_{ij}(\sigma, \tau) \prod_{i=1}^n f_i(\sigma, \tau)$$

quels que soient $\sigma, \tau \in G$, où g_{ij} (resp. f_i) est le cocycle représentant de $[a_i^{-1} b_i, a_j^{-1} b_j]$ (resp. $a_i^{-1} b_i, a_i$). Donc,

$$\alpha_S(q, q_1) = \prod_{i < j} [a_i^{-1} b_i, a_j^{-1} b_j] \prod_{i=1}^n (a_i^{-1} b_i, a_i)$$

et par conséquent, on a le résultat suivant

Lemme 4.2 : $\alpha_S(q, q_1) = (\Delta(q), -\Delta(q_1))h(q_1)h(q)$

Corollaire 4.3 : Soient (M, q) et (M, q_1) deux R -espaces quadratiques. Si le rang de M est 2 ou 3, alors les formes quadratiques q et q_1 sont équivalentes si et seulement si $\Delta(q) = \Delta(q_1)$ et $h(q) = h(q_1)$.

La démonstration de ce corollaire est une conséquence immédiate du Corollaire 3.7 et du Lemme ci-dessus.

BIBLIOGRAPHIE

- [1] M. AUSLANDER and O. GOLDMAN, The Brauer group of a commutative ring, Trans. Amer. Math. Soc., 97 (1960), 367-409.
- [2] H. BASS, Clifford algebras and Spinor norms over a commutative ring, Am. J. Math. (1974) 156-206.
- [3] S.U. CHASE, D.K. HARRISON and A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, Mem. Am. Math. Soc., 52 (1965).
- [4] E.A.M. HORNIX, Stiefel-Whitney invariants of quadratic forms over local rings, Journal of Algebra, 26 (1973), 258-279.
- [5] M.A. KNUS et M. OJANGUREN, Théorie de la descente et algèbres d'Azumaya, Lectures Notes in Math., 389, Springer Verlag, Berlin (1974).
- [6] A. MICALI et Ph. REVOY, Modules Quadratiques, Cahiers Mathématiques 10 (1977), MONTPELLIER.

- [7] A. MICALI et O.E. VILLAMAYOR, Sur les algèbres de Clifford, Ann. Sc. Ec. Norm. Sup. 4^{ème} Sér. 1 (1968), 271-304.
- [8] A. MICALI et O.E. VILLAMAYOR, Algèbres de Clifford et groupe de Brauer, Ann. Sc. Ec. Norm. Sup. 4^{ème} Sér. 4(1971), 285-310.
- [9] M. NAGATA, Local rings, Interscience Publishers, New York (1962).
- [10] Ph. REVOY, Autour des formes quadratiques, Thèse de Doctorat d'Etat, Math. Montpellier, (1975).
- [11] C. SMALL, The group of quadratic extensions, Journal of Pure and Applied Algebra, 2 (1973), 83-105.
- [12] T.A. SPRINGER, On the equivalence of quadratic forms, Kon. Ned. Akad. Wet. Proc., Ser. A, 62 (1959), 241-253.
- [13] O.E. VILLAMAYOR, Separable algebras and Galois extensions, Osaka J. Math., 4 (1963), 161-171.

Instituto de Matematica
Universidade Estadual de Campinas
C.P. 1170
CEP 13100 Campinas, SP, Brésil
