ANNALES SCIENTIFIQUES DE L'É.N.S.

ARTIBANO MICALI
ORLANDO E. VILLAMAYOR

Algèbres de Clifford et groupe de Brauer

Annales scientifiques de l'É.N.S. 4e série, tome 4, nº 2 (1971), p. 285-310
<http://www.numdam.org/item?id=ASENS_1971_4_4_2_285_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1971, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens) 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/

Ann. scient. Éc. Norm. Sup.,
4e série, t. 4, 1971, p. 285 à 310.

ALGÈBRES DE CLIFFORD ET GROUPE DE BRAUER (1)

PAR ARTIBANO MICALI ET ORLANDO E. VILLAMAYOR.

TABLE DES MATIÈRES.

(1) Ce travail a été réalisé alors que le premier des auteurs séjournait à l'Université de Buenos Aires dans le cadre du Programme Multinational de Mathématiques de l'O. E. A. (1969).

0. Introduction.

Ce papier reprend, dans une certaine mesure, la dernière partie de [9]. Soient A un anneau commutatif à élément unité, $\mathcal{B}_2(A)$ le sous-groupe du groupe de Brauer $\mathcal{B}(A)$ dont tous les éléments sont d'ordre 2 et $\mathfrak{Q}(A)$ le groupe des extensions quadratiques de A (*cf.* 2.2). Désignons encore par $\mathcal{H}_0(A)$ le groupe des classes d'isomorphismes d'algèbres de Clifford de modules projectifs de rang pair défini dans [8] (*cf.* 2.1). On démontre (*cf.* lemme 2 de 2.4) que, comme ensembles, $\mathcal{H}_0(A) = N(A) \times \mathfrak{Q}(A)$, où N(A) est un certain sous-groupe de $\mathcal{B}_2(A)$. Il existe alors un homomorphisme injectif naturel de groupes abéliens $\mathcal{H}_0(A) \hookrightarrow \mathcal{B}_2(A) \times \mathfrak{Q}(A)$. Cela va nous permettre de calculer un certain nombre de groupes $\mathcal{H}$ (*cf.* 5).

Nous présentons ici une autre méthode pour la construction de la structure de groupe dans $\mathcal{B}_2(A) \times \mathfrak{Q}(A)$, méthode qu'on pourrait appeler des *représentants canoniques* (*cf.* 3.2).

Pour tout entier $p \geqq 0$, premier on non, on posera $\mathbf{Z}_p = \mathbf{Z}/(p)$. Tout anneau est commutatif à élément unité, tout module est unitaire et un homomorphisme d'anneaux (resp. algèbres) transforme élément unité en élément unité. Le mot algèbre désignera une algèbre associative à élément unité non nécessairement commutative et, le plus souvent, graduée sur $\mathbf{Z}_2$. Soient $B = B_0 \oplus B_1$ et $C = C_0 \oplus C_1$ deux A-algèbres graduées sur $\mathbf{Z}_2$ (*cf.* 1.2) et $\varphi : B \to C$ un *homomorphisme*. Ceci veut dire que φ est un homomorphisme de A-algèbres et que, de plus, $\varphi(B_i) \subset C_i$ $(i = 0, 1)$, i. e., un homomorphisme d'algèbres graduées est toujours de *degré zéro* (*cf.* 1.2).

Si B et C sont deux A-algèbres graduées sur $\mathbf{Z}_2$, on considère leur produit tensoriel $B \otimes_A C$ en tant que A-modules. Nous désignerons par $B \hat{\otimes} C$ (*produit tensoriel gradué*) la A-algèbre dont sa structure multiplicative est donnée par

$$(b \otimes c) . (b' \otimes c') = (-1)^{d^0(c)\, d^0(b')} (bb') \otimes (cc'),$$

où $b, b' \in B$ et $c, c' \in C$ sont des éléments homogènes et où $d^0(b)$, par exemple, désigne le *degré* de l'élément b. On désignera par $B \otimes C$ (*produit tensoriel ordinaire ou non gradué*) la A-algèbre dont sa structure multiplicative est donnée par

$$(b \otimes c) . (b' \otimes c') = (bb') \otimes (cc').$$

Nous verrons que, sous certaines conditions, le produit tensoriel gradué peut *s'identifier* au non gradué, tout au moins dans le cas des algèbres de Clifford (*cf.* 1.3).

Si A est un anneau, on notera U(A) le groupe multiplicatif des éléments inversibles de A et $U^2(A)$ le sous-groupe de U(A) formé par les carrés d'éléments de $U(A)$. Considérons le groupe $G(A)$ (*cf.* [8], § 7). On sait (*cf.* [8], § 7, lemme 7) qu'il existe un homomorphisme canonique $G(A) \to U(A)/U^2(A)$ qui est un isomorphisme si 2 est inversible dans A.

Si A est local, l'homomorphisme (composé) de groupes

$$W : \mathcal{H}_0(A) \to G(A) \to U(A)/U^2(A)$$

est le *discriminant*.

Étant donnée une A-algèbre C, on désignera par $Z(C)$ le *centre* de C. Pour tout anneau A, $A(n)$ désignera l'anneau des matrices carrées $n \times n$ à coefficients dans A.

Étant donné que la lettre μ désignera fréquemment l'homomorphisme de multiplication $C \otimes C \to C$, on notera par $\sqrt{1}(A)$ le sous-groupe des éléments d'ordre 2 du groupe multiplicatif de l'anneau A [noté habituellement $\mu_2(A)$].

Nous remercions le Referee pour ses suggestions en vue d'améliorer ce texte.

1. Le groupe $\mathcal{H}(A)$.

1.1. Formes quadratiques et algèbres de Clifford. — Soient A un anneau et P un A-module. On dit qu'une application $Q : P \to A$ est une *forme quadratique* sur P si les deux conditions suivantes sont vérifiées :
(FQ_1) pour tout $x \in P$ et pour tout $a \in A$, $Q(ax) = a^2 Q(x)$;
(FQ_2) l'application $\Phi : P \times P \to A$ définie par

$$(x, y) \mapsto Q(x+y) - Q(x) - Q(y)$$

est une forme bilinéaire (nécessairement symétrique).

Un A-module P muni d'une forme quadratique $Q : P \to A$ sera appelé un *module quadratique* et on le note (P, Q). On dira que Φ est la forme bilinéaire *associée* à Q.

Soient (P, Q) un module quadratique, $P^\star = \mathrm{Hom}_A(P, A)$ le dual de P et $\varphi : P \to P^\star$ l'application A-linéaire définie par $\varphi(x)(y) = \Phi(x, y)$, quels que soient $x, y \in P$. On dira que Q (resp. Φ) est *non dégénérée* si $\varphi : P \xrightarrow{\sim} P^\star$ est un isomorphisme de A-modules. Il est clair que si A est un corps et P un A-espace vectoriel de dimension finie, alors $Q : P \to A$ *est non dégénérée si et seulement si la condition suivante est vérifiée :* $\Phi(x, y) = 0$ *pour tout* $y \in P$, *entraîne* $x = 0$ (ce qui est bien la définition classique de forme quadratique non dégénérée).

Supposons maintenant que P soit un A-module de présentation finie. *Alors* $Q : P \to A$ *est non dégénérée si et seulement si, pour tout idéal maximal* $\mathfrak{m}$

de A, *la forme quadratique étendue* $Q_{\mathfrak{m}} : P_{\mathfrak{m}} \to A_{\mathfrak{m}}$ *est non dégénérée.* En effet, ceci résulte du lemme de globalisation et du fait suivant : si P est un A-module de présentation finie et si $A \to A'$ est une A-algèbre plate, il existe un isomorphisme de A'-modules $P^\star \otimes_A A' \xrightarrow{\sim} (P \otimes_A A')^\star$.

Considérons l'application A'-linéaire $P^\star \otimes_A A' \xrightarrow{\theta} (P \otimes_A A')^\star$ définie (comme ci-dessus) par

$$\alpha \otimes a' \mapsto (x \otimes b' \mapsto \alpha(x)\, a' b').$$

Si $P = A$, θ est un isomorphisme, donc c'est aussi un isomorphisme si P est libre de type fini et, par suite, $P^\star \otimes_A A' \xrightarrow{\sim} (P \otimes_A A')^\star$ est un isomorphisme de A'-modules, si P est projectif de type fini (quelle que soit la nature de l'extension $A \to A'$). De ceci, il résulte alors que si P est un A-module projectif de type fini, *une condition nécessaire et suffisante pour qu'une forme quadratique* $Q : P \to A$ *soit non dégénérée est que pour tout idéal maximal* $\mathfrak{m}$ *de* A, *la forme étendue* $Q/\mathfrak{m} : P/\mathfrak{m}P \to A/\mathfrak{m}$ *soit non dégénérée.*

Par la suite (sauf mention expresse du contraire), on supposera toujours, si (P, Q) est un module quadratique, que P est un A-module projectif de type fini et que $Q : P \to A$ est une forme quadratique non dégénérée.

Si (P, Q) est un module quadratique, nous désignerons par C(P, Q) son algèbre de Clifford (*cf.* [4], § 9) et par $C_0(P, Q)$ et $C_1(P, Q)$ ses parties homogènes de degrés 0 et 1 respectivement, C(P, Q) étant considérée comme une algèbre graduée sur $\mathbf{Z}_2$. Pour des propriétés concernant les algèbres de Clifford et utilisées ici, on renvoie le lecteur à ([4], § 9).

Soit (P, Q) un A-module quadratique et supposons que P soit libre ayant $\{e_1, \ldots, e_n\}$ comme base. Si Φ est la forme bilinéaire associée à Q, la matrice $(\Phi(e_i, e_j))_{1 \leq i, j \leq n}$ formée par les $\Phi(e_i, e_j)$ s'appelle la *matrice* de Φ (ou de Q). Dire que Q est non dégénérée équivaut à dire que la matrice de Q est inversible. Finalement, si

$$e_i = \sum_{i=1}^{n} a_{ij} f_j \quad (i = 1, \ldots, n), \qquad a_{ij} \in A \quad (i, j = 1, \ldots, n)$$

est un changement de base, la matrice de Φ en la base $\{e_1, \ldots, e_n\}$ s'écrit $(a_{ij})(\Phi(f_i, f_j))^t(a_{ij})$.

L'algèbre de Clifford d'un module quadratique (L, Q), où L est libre de rang 2, s'appelle *algèbre de quaternions.* Si Φ est la forme bilinéaire associée à Q et si $\{e_1, e_2\}$ est une base de L sur A, on notera $h_s(a, b) = C(L, Q)$, si $s = \Phi(e_1, e_2)$, $a = Q(e_1)$ et $b = Q(e_2)$, i. e., $h_s(a, b)$ est l'algèbre de quaternions dont la matrice est $\begin{bmatrix} 2a & s \\ s & 2b \end{bmatrix}$.

1.2. Algèbres de Clifford triviales et le groupe $\mathcal{H}(A)$. — On dira qu'un anneau A est *gradué* (sur $\mathbf{Z}_2$) si $A = A_0 \oplus A_1$ avec $A_i A_j \subset A_{i+j}$ ($i+j$ calculé modulo 2) et qu'un A-module P est *gradué* (sur $\mathbf{Z}_2$) si $P = P_0 \oplus P_1$ avec $A_i P_j \subset P_{i+j}$.

Soient P et P′ deux A-modules gradués et $\alpha : P \to P'$ une application additive de P vers P′. On dira que α est A-*linéaire de degré* $d^0(\alpha)$ si $\alpha(P_i) \subset P'_{i+d^0(\alpha)}$ ($i = 0, 1$) et si pour tout $a \in A$ et $x \in P$, on a

$$\alpha(ax) = (-1)^{d^0(\alpha)\, d^0(a)}\, a\, \alpha(x).$$

Désignons par $\mathrm{Hom}_A(P, P')_i$ les applications A-linéaires de P vers P′ de degré i ($i = 0, 1$). On peut donc considérer

$$\mathrm{Hom}_A(P, P') = \mathrm{Hom}_A(P, P')_0 \oplus \mathrm{Hom}_A(P, P')_1$$

comme un A-module gradué (sur $\mathbf{Z}_2$), où

$$\alpha(P_0) \subset P'_0, \quad \alpha(P_1) \subset P'_1 \qquad \text{si} \quad d^0(\alpha) = 0$$

et

$$\alpha(P_0) \subset P'_1, \quad \alpha(P_1) \subset P'_0 \qquad \text{si} \quad d^0(\alpha) = 1.$$

Supposons maintenant que A soit trivialement gradué (i. e., $A_0 = A$ et $A_1 = 0$) et soient (P, Q) un A-module quadratique et C(P, Q) son algèbre de Clifford. On dira que C(P, Q) est une *algèbre de Clifford triviale* s'il existe un A-module gradué (sur $\mathbf{Z}_2$) $P_0 \oplus P_1$ projectif de type fini et un isomorphisme de A-algèbres graduées (sur $\mathbf{Z}_2$),

$$C(P, Q) \xrightarrow{\sim} \mathrm{End}_A(P_0 \oplus P_1).$$

Soit $\mathcal{C}(A)$ l'ensemble des classes d'isomorphismes gradués d'algèbres de Clifford et considérons sur $\mathcal{C}(A)$ la relation d'équivalence suivante : si C et C′ sont deux algèbres de Clifford, on dira C est *équivalente* à C′ ($C \sim C'$) s'il existe deux algèbres de Clifford triviales S, S′ telles que $C \hat{\otimes} S \simeq C' \hat{\otimes} S'$ (isomorphisme d'algèbres graduées). Étant donné que si S et S′ sont deux algèbres de Clifford triviales, il en est de même de $S \hat{\otimes} S'$ (*cf.* [8], lemme 12), il en résulte immédiatement que $\sim$ est bien une relation d'équivalence sur $\mathcal{C}(A)$ et soit $\mathcal{H}(A) = \mathcal{C}(A)/\sim$ l'ensemble quotient.

L'ensemble $\mathcal{H}(A)$ est muni d'une structure naturelle de groupe abélien, l'opération de groupe étant induite par le produit tensoriel gradué. Ceci signifie que si C est une algèbre de Clifford et si $\{C\}$ est l'élément qu'elle définit dans $\mathcal{H}(A)$, alors la loi de groupe de $\mathcal{H}(A)$ est définie par $\{C\} + \{C'\} = \{C \hat{\otimes} C'\}$. La seule chose à vérifier est l'existence de l'inverse et cela résulte du lemme 13 de [8]. Le groupe $\mathcal{H}(A)$ s'appelle le *groupe des classes d'isomorphismes d'algèbres de Clifford.*

Si $\varphi : A \to A'$ est un homomorphisme d'anneaux, il existe un homomorphisme de groupes abéliens $\mathcal{H}(\varphi) : \mathcal{H}(A) \to \mathcal{H}(A')$ défini par

$$\mathcal{H}(\varphi)(\{C\}) = \{C \otimes_A A'\}.$$

Il est clair que pour tout anneau A, $\mathcal{H}(\mathrm{id}_A) = \mathrm{id}_{\mathcal{H}(A)}$ et si $A \xrightarrow{\varphi} A'$ et $A' \xrightarrow{\varphi'} A''$ sont deux homomorphismes d'anneaux, alors

$$\mathcal{H}(\varphi' \circ \varphi) = \mathcal{H}(\varphi') \circ \mathcal{H}(\varphi);$$

$\mathcal{H}$ est ainsi un foncteur covariant défini dans la catégorie des anneaux commutatifs à élément unité à valeurs dans la catégorie des groupes abéliens.

1.3. LE THÉORÈME $\otimes = \hat{\otimes}$. — Si $C = C(P, Q)$ est l'algèbre de Clifford d'un module quadratique (P, Q), où P est projectif de rang pair, on pose

$$X(C) = \{x \mid x \in C,\ xy = -yx,\ \forall y \in P\}.$$

On sait (*cf.* [8], § 9, p. 292) que $X(C)$ est un A-module projectif de type fini et de rang 1. Si $x, x' \in X(C)$, pour tout $y \in P$, on a

$$(xx')y = -xyx' = y(xx'), \qquad \text{donc} \quad xx' \in Z(C) = A.$$

Donc, la multiplication $\mu : X(C) \otimes X(C) \to A$, $x \otimes x' \mapsto xx'$ induit un isomorphisme de A-modules. De plus, il existe une forme quadratique naturelle, notée encore $\mu : X(C) \to A$, donnée par $\mu(x) = x^2$ pour tout $x \in X(C)$ et soit $Q' \star \mu : P' \otimes X(C) \to A$ la forme quadratique définie localement par

$$(Q' \star \mu)(x' \otimes y) = Q'(x')\,\mu(y).$$

THÉORÈME $\otimes = \hat{\otimes}$. — *Soient* A *un anneau,* $C = C(P, Q)$ *et* $C' = C(P', Q')$ *deux algèbres de Clifford où* P *est de rang pair. Il existe alors un isomorphisme d'algèbres de Clifford* $C \otimes C'_\star \xrightarrow{\sim} C \hat{\otimes} C'$, *où*

$$C'_\star = C(P' \otimes_A X(C),\ Q' \star \mu)$$

(*cf.* [8], § 5, théorème 4', p. 283).

Dans le cas où A est local, la « modification » de C' se fait comme suit. Supposons que P soit projectif, donc libre, de rang 2 et soit $\{u_1, u_2\}$ une base de P sur A. Soit Φ la forme bilinéaire associée à Q et posons $\theta = -\Phi(u_1, u_2) + 2u_1u_2$. Si $\{u'_1, u'_2\}$ est une autre base de P sur A, alors $\theta' = \Delta\theta$, où Δ est le déterminant de changement de base. Ainsi, θ est déterminé à moins d'un élément inversible. De plus, θ est inversible car $\theta^2 = -\det(\Phi)$. Puisque A est local,

$$P' \otimes_A X(C) \simeq P' \qquad \text{et} \qquad Q' \star \mu = -\det(\Phi) Q'$$

(*cf.* [8], § 5, théorème 4, p. 283) de telle sorte que

$$C(P, Q) \hat{\otimes} C(P', Q') = C(P, Q) \otimes C(P', -\det(\Phi) Q').$$

C'est sous cette forme que le théorème $\otimes = \hat{\otimes}$ sera souvent utilisé.

2. Le groupe $\mathcal{H}_0(A)$.

2.1. Les groupes Ip(A) et $\mathcal{H}_0(A)$. — Étant donné un anneau A, désignons par Ip(A) l'ensemble des idempotents de A. On munit Ip(A) d'une structure de groupe abélien définie par la somme booléienne, i. e., si $e, e' \in \mathrm{Ip}(A)$, on pose

$$e \mathbin{\bar{+}} e' = e + e' - 2ee'.$$

On obtient ainsi sur Ip(A) une structure de groupe, appelé le *groupe des idempotents* de l'anneau A.

Pour chaque algèbre de Clifford C(P, Q), on associe, localement, l'idempotent 0 si le rang de P est pair et l'idempotent 1 si le rang de P est impair. On définit ainsi un homomorphisme de groupes abéliens $\varphi : \mathcal{H}(A) \to \mathrm{Ip}(A)$ car si

$$\varphi(\{C\}) = e \qquad \text{et} \qquad \varphi(\{C'\}) = e',$$

alors

$$\varphi(\{C\} + \{C'\}) = \varphi(\{C \hat{\otimes} C'\}) = e + e' - 2ee' = e \mathbin{\bar{+}} e'.$$

On pose alors, par définition,

$$\mathcal{H}_0(A) = \mathrm{Ker}(\mathcal{H}(A) \xrightarrow{\varphi} \mathrm{Ip}(A)).$$

Si $\psi : A \to A'$ est un homomorphisme d'anneaux on déduit, par restriction, un homomorphisme de groupes abéliens $\psi|_{\mathrm{Ip}(A)} : \mathrm{Ip}(A) \to \mathrm{Ip}(A')$ donc un homomorphisme $\mathcal{H}_0(\psi) : \mathcal{H}_0(A) \to \mathcal{H}_0(A')$ rendant commutatif le diagramme

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{H}_0(A) \arrow[r] \arrow[d, dashed, "\mathcal{H}_0(\psi)"] & \mathcal{H}(A) \arrow[r] \arrow[d, "\mathcal{H}(\psi)"] & \mathrm{Ip}(A) \arrow[d, "\psi|_{\mathrm{Ip}(A)}"] \\
0 \arrow[r] & \mathcal{H}_0(A') \arrow[r] & \mathcal{H}(A') \arrow[r] & \mathrm{Ip}(A')
\end{tikzcd}$$

Le caractère fonctoriel de $\mathcal{H}_0$ se déduit immédiatement des considérations précédentes.

On remarque que si 2 est inversible dans A, alors $\varphi : \mathcal{H}(A) \to \mathrm{Ip}(A)$ est localement surjectif (*cf.* [8], lemme 1), donc surjectif. On a ainsi la suite exacte de groupes abéliens

$$0 \to \mathcal{H}_0(A) \to \mathcal{H}(A) \to \mathrm{Ip}(A)$$

et, si 2 est inversible dans A,

$$0 \to \mathcal{H}_0(A) \to \mathcal{H}(A) \to \mathrm{Ip}(A) \to 0.$$

Il est clair que si A n'a d'autres idempotents que 0 et 1, on a les suites exactes de groupes abéliens

$$0 \to \mathcal{H}_0(A) \to \mathcal{H}(A) \to \mathbf{Z}_2$$

et

$$0 \to \mathcal{H}_0(A) \to \mathcal{H}(A) \to \mathbf{Z}_2 \to 0,$$

si 2 est inversible dans A.

2.2. Le groupe $\mathfrak{Q}(A)$. — Soit A un anneau. On dira qu'une A-algèbre B est une *extension quadratique* de A si B est une A-algèbre séparable et si, de plus, B est un A-module projectif de type fini et de rang 2. On voit que, nécessairement, B est commutative.

Si B est une extension quadratique de A, alors B se plonge dans une extension de Galois B′ de A de rang $2! = 2$ (*cf.* [11]) et, par suite, $B = B'$. Il existe alors un unique automorphisme de A-algèbres $\sigma \neq \mathrm{id}$ de B tel que $B^\sigma = A$.

Soient B_i $(i = 1, 2)$ deux extensions quadratiques de A et désignons par σ_i $(i = 1, 2)$ l'unique automorphisme de A-algèbres de B_i distinct de l'identité. Alors $B_1 \otimes_A B_2$ est une extension de Galois de A de rang 4 ayant comme groupe de Galois $\{\mathrm{id} \otimes \mathrm{id}, \mathrm{id} \otimes \sigma_2, \sigma_1 \otimes \mathrm{id}, \sigma_1 \otimes \sigma_2\}$. Il s'ensuit que $(B_1 \otimes_A B_2)^{\sigma_1 \otimes \sigma_2}$ est alors de rang 2 sur A, donc une extension quadratique de A. Si l'on pose

$$B_1 \star B_2 = (B_1 \otimes B_2)^{\sigma_1 \otimes \sigma_2}$$

alors l'opération $\star$ induit sur l'ensemble $\mathfrak{Q}(A)$ des classes d'isomorphismes des extensions quadratiques de A une structure de groupe abélien, l'élément unité de $\mathfrak{Q}(A)$ étant la classe de l'extension quadratique $I = A \oplus A$ dont l'unique automorphisme distinct de l'identité est $\tau(a, a') = (a', a)$. En effet, si B est une extension quadratique de A et si $\sigma \neq \mathrm{id}$ est l'automorphisme de B, alors

$$B \star I = \{(b, b') \mid (b, b') \in B \oplus B, \sigma(b) = b'\}$$

et il est évident que l'application $B \to B \star I$ définie par $b \mapsto (b, \sigma(b))$ est un isomorphisme d'extensions quadratiques. On dira que $\mathcal{Q}(A)$ est le *groupe des extensions quadratiques de* A.

2.3. Rapports entre les groupes $\mathcal{H}_0(A)$ *et* $\mathcal{Q}(A)$. — Considérons l'application $\beta : \mathcal{H}_0(A) \to \mathcal{B}(A)$, où $\mathcal{B}(A)$ est le *groupe de Brauer* de A, qui à toute algèbre de Clifford C associe C considérée comme A-algèbre centrale séparable. Il est clair que β est bien définie car si C et C′ sont égales dans $\mathcal{H}_0(A)$, il existe deux algèbres de Clifford triviales S et S′ telles que $C \hat{\otimes} S \simeq C' \hat{\otimes} S'$ (isomorphisme d'algèbres graduées sur $\mathbf{Z}_2$) et, d'après le théorème $\otimes = \hat{\otimes}$, on a $C \otimes S \simeq C' \otimes S'$, car S et S′ sont triviales. Donc, C et C′ sont égales dans $\mathcal{B}(A)$, puisque toute algèbre de Clifford triviale est nulle dans $\mathcal{B}(A)$. Ceci démontre que β est bien définie; β n'est pas un homomorphisme de groupes abéliens car, en général, étant données deux algèbres de Clifford C et C′, on a

$$C \hat{\otimes} C' \neq C \otimes C'.$$

Considérons maintenant l'application $\gamma : \mathcal{H}_0(A) \to \mathcal{Q}(A)$ qui à toute algèbre de Clifford C associe $Z(C_0)$, $Z(C_0)$ considéré comme extension quadratique de A (*cf.* [9], § 3, n° 3.1). Montrons que γ est bien définie. En effet, on sait que si C et C′ sont deux algèbres de Clifford quelconques, alors $Z((C \hat{\otimes} C')_0) = Z(C_0) \star Z(C'_0)$ (*cf.* [9], § 3, n° 3.1). Donc, si C et C′ sont égales dans $\mathcal{H}_0(A)$, il existe deux algèbres de Clifford triviales S et S′ telles que $C \hat{\otimes} S \simeq C' \hat{\otimes} S'$, d'où,

$$Z((C \hat{\otimes} S)_0) = Z(C_0) \star Z(S_0) = Z(C_0)$$

et, de même,

$$Z((C' \hat{\otimes} S')_0) = Z(C'_0),$$

étant donnée que si S est triviale, $Z(S_0)$ est l'élément unité de $\mathcal{Q}(A)$. Il s'ensuit que $Z(C_0) = Z(C'_0)$ dans $\mathcal{Q}(A)$. On a aussi montré, du même coup, que γ est un homomorphisme de groupes. De plus, $\gamma : \mathcal{H}_0(A) \to \mathcal{Q}(A)$ est un homomorphisme surjectif de groupes et $\mathrm{Ker}(\gamma) = N(A)$ est le sous-groupe de $\mathcal{H}_0(A)$ formé des classes d'isomorphismes d'algèbres de Clifford C qui admettent un idempotent e définissant la graduation de C, i. e., tel que $ex = xe$ pour tout $x \in C_0$ et $ex + xe = x$ pour tout $x \in C_1$ (*cf.* [9], § 3, n° 3.1).

D'après le théorème 6 de [8], on sait que N(A) est un sous-groupe du groupe de Brauer $\mathcal{B}_2(A)$ dont tous les éléments sont d'ordre 2.

Soit $\sqrt{1}\,(A) = \{ a \mid a \in A,\ a^2 = 1 \}$ le *groupe des racines carrées de* 1 *dans* A et considérons l'homomorphisme de groupes $\mathrm{Ip}(A) \to \sqrt{1}\,(A)$ défini par $e \mapsto 1 - 2e$ [il est clair que si 2 est inversible dans A, $\mathrm{Ip}(A) \xrightarrow{\sim} \sqrt{1}\,(A)$ est un isomorphisme et que si 2 est non diviseur de zéro dans A, alors $\mathrm{Ip}\,(A) \to \sqrt{1}\,(A)$ est injectif]. Il en résulte un homomorphisme de groupes abéliens

$$H^1(\mathfrak{X}, A, \mathrm{Ip}) \xrightarrow{\eta} H^1(\mathfrak{X}, A, \sqrt{1}),$$

où $\mathfrak{X}$ est une topologie convenable (*cf.* [9], § 3, n° 3.1; par exemple, la topologie fidèlement plate de présentation finie). D'autre part, on sait (*cf.* [9], § 3, n° 3.2) que $H^1(\mathfrak{X}, A, \sqrt{1})$ peut s'interpréter comme le groupe $\mathfrak{T}(A)$ des couples (P, μ), où P est un A-module projectif de type fini et rang 1 et $\mu : P \otimes P \xrightarrow{\sim} A$ (où $\otimes = \otimes_A$) est un isomorphisme de A-modules, la loi de groupe abélien de $\mathfrak{T}(A)$ étant la suivante :

$$(P, \mu) + (P', \mu') = (P \otimes P', \mu \star \mu'),$$

où

$$\mu \star \mu' : \quad P \otimes P' \otimes P \otimes P' \xrightarrow{\sim} P \otimes P \otimes P' \otimes P' \xrightarrow{\mu \otimes \mu'} A \otimes A \xrightarrow[\sim]{\mu_A} A$$

est l'isomorphisme composé évident et μ_A est la multiplication de l'anneau A. On dira encore que $(P, \mu) = (P', \mu')$ si et seulement si il existe un isomorphisme de A-modules $\varphi : P \xrightarrow{\sim} P'$ tel que le diagramme

$$\begin{tikzcd} P \otimes P \arrow[rr, "\varphi \otimes \varphi", "\sim"'] \arrow[dr, "\mu"'] & & P' \otimes P' \arrow[dl, "\mu'"] \\ & A & \end{tikzcd}$$

soit commutatif. Il est clair que pour cette structure de groupe, le zéro est le couple (A, μ_A) et l'opposé de (P, μ) est encore (P, μ), car le diagramme commutatif

$$\begin{tikzcd} P \otimes P \otimes P \otimes P \arrow[rr, "\mu \otimes \mu", "\sim"'] \arrow[dr, "\mu \star \mu"'] & & A \otimes A \arrow[dl, "\mu_A"] \\ & A & \end{tikzcd}$$

nous montre que

$$(P, \mu) + (P, \mu) = (P \otimes P, \mu \star \mu) = (A, \mu_A).$$

Pour toute algèbre de Clifford $C = C\,(P, Q)$, on considère le A-module $X(C)$. On sait que $X(C)$ est un A-module projectif de type fini et de rang 1 (*cf.* [8], § 9, p. 292) et si P est de rang pair, l'application $\mu : X(C) \otimes X\,(C) \to A$ définie par $\mu(x \otimes x') = xx'$ est bien définie et est un isomorphisme de A-modules, car $\mu : X(C) \otimes X\,(C) \to A$ est localement un isomorphisme, donc un isomorphisme (global). Ceci nous montre qu'il existe une application $\mathcal{H}_0(A) \xrightarrow{\delta} H^1(\mathfrak{X}, A, \sqrt{1})$ définie par

$$\delta(C) = (X(C), \mu).$$

Si C et C′ sont deux algèbres de Clifford, alors

$$\delta(C \hat{\otimes} C') = (X(C \hat{\otimes} C'), \tilde{\mu})$$

et étant donné que

$$X(C \hat{\otimes} C') = X(C) \otimes X(C'),$$

alors $\tilde{\mu} = \mu \star \mu'$, où

$$\mu : \quad X(C) \otimes X(C) \to A \qquad \text{et} \qquad \mu' : \quad X(C') \otimes X(C') \to A$$

sont les multiplications sur X(C) et X(C′) respectivement. Ceci nous montre que

$$\delta : \quad \mathcal{H}_0(A) \to H^1(\mathfrak{X}, A, \sqrt{1})$$

est un homomorphisme de groupes.

Puisque toute extension quadratique de A peut s'exprimer par un $Z(C_0)$ pour une algèbre de Clifford convenable C (*cf.* [9], § 3, n° 3.2), alors l'homomorphisme

$$\delta : \quad \mathcal{H}_0(A) \to H^1(\mathfrak{X}, A, \sqrt{1})$$

se factorise par $\mathfrak{Q}(A)$, i. e., il existe un homomorphisme de groupes

$$\mathfrak{Q}(A) \xrightarrow{\eta} H^1(\mathfrak{X}, A, \sqrt{1})$$

tel que le diagramme

$$\begin{tikzcd} \mathcal{H}_0(A) \arrow[r, "\gamma"] \arrow[d, "\delta"'] & \mathfrak{Q}(A) \arrow[r] \arrow[dl, dotted, "\eta"] & 0 \\ H^1(\mathfrak{X}, A, \sqrt{1}) & & \end{tikzcd}$$

soit commutatif. Il est évident que l'homomorphisme $\mathfrak{Q}(A) \to H^1(\mathfrak{X}, A, \sqrt{1})$ est induit par l'homomorphisme de groupes $Ip(A) \xrightarrow{\eta} \sqrt{1}(A)$ défini par $e \mapsto 1 - 2e$, car

$$\mathfrak{Q}(A) = H^1(\mathfrak{X}, A, Ip)$$

(*cf.* [9], § 3, n° 3.1).

2.4. La fonction $\alpha : \mathcal{H}_0(A) \times \mathcal{H}_0(A) \to \mathcal{H}_0(A)$. — On sait (*cf.* [9], § 3, n° 3.3, lemme 1) que, quels que soient C et C′ dans $\mathcal{H}_0(A)$, il existe une algèbre de Clifford dans $\mathcal{H}_0(A)$, qu'on notera $\alpha(C, C')$, telle que

$$C' \otimes \alpha(C, C') \simeq C'_\star \otimes \mathrm{End}_A(A \oplus X(C))$$

(isomorphisme d'algèbres centrales séparables) et, de même,

$$C \otimes \alpha(C', C) \simeq C_* \otimes \mathrm{End}_A(A \oplus X(C')).$$

Il s'ensuit que

$$\beta(C \hat{\otimes} C') = \beta(C) + \beta(C') + \beta(\alpha(C, C'))$$

et, en particulier,

$$\beta(\alpha(C, C')) = \beta(\alpha(C', C)).$$

D'autre part, la suite exacte de groupes abéliens

$$E : \quad 0 \to N(A) \to \mathcal{H}_0(A) \to \mathcal{Q}(A) \to 0$$

(*cf.* [9], § 3, n° 3.1, théorème 2) nous dit que $E \in \mathrm{Ext}^1(\mathcal{Q}(A), N(A))$ et l'extension reste parfaitement déterminée si l'on fixe la fonction $\alpha : \mathcal{H}_0(A) \times \mathcal{H}_0(A) \to \mathcal{H}_0(A)$ telle que

$$\beta(C \hat{\otimes} C') = \beta(C) + \beta(C') + \beta(\alpha(C, C')),$$

où C et C′ parcourent $\mathcal{H}_0(A)$.

Lemme 1. — *Pour tout couple d'algèbres* $(C, D) \in \mathcal{H}_0(A) \times \mathcal{H}_0(A)$, $\beta(\alpha(C, D))$ *ne dépend que des images de* C *et* D *dans* $H^1(\mathfrak{X}, A, \sqrt{1})$.

En effet,

$$\begin{aligned}\beta(\alpha(C, D)) &= \beta(C \hat{\otimes} D) - \beta(C) - \beta(D) = \beta(C \otimes D_*) - \beta(C) - \beta(D)\\ &= \beta(C) + \beta(D_*) - \beta(C) - \beta(D) = \beta(D_*) - \beta(D) = \beta(D_* \otimes D)\end{aligned}$$

et si $D = C(P, Q)$, alors on sait que $D_* = C(P \otimes_A X(C), Q \star \mu)$, où l'on désigne encore par $\mu : X(C) \to A$ la forme quadratique sur $X(C)$ définie par l'application A-linéaire $\mu : X(C) \otimes X(C) \to A$, i. e., $\mu(x) = x^2$ pour tout $x \in X(C)$. Il est évident maintenant que $\beta(\alpha(C, D))$ ne dépend pas de C mais de son image dans $H^1(\mathfrak{X}, A, \sqrt{1})$, i. e., du couple $(X(C), \mu)$. En effet, si C et C′ ont même image dans $H^1(\mathfrak{X}, A, \sqrt{1})$, i. e., si

$$(X(C), \mu) = (X(C'), \mu'),$$

alors

$$D_* = C(P \otimes_A X(C), Q \star \mu) = C(P \otimes_A X(C'), Q \star \mu').$$

Comme $\beta(\alpha(C, D)) = \beta(\alpha(D, C))$, il en est de même de D.

Lemme 2. — *En tant qu'ensembles*, $\mathcal{H}_0(A) = N(A) \times \mathcal{Q}(A)$.

Considérons l'application $\omega : \mathcal{H}_0(A) \to \mathcal{B}_2(A) \times \mathcal{Q}(A)$ définie par

$$\omega(C) = (\beta(C), \gamma(C))$$

pour tout $C \in \mathcal{H}_0(A)$. Comme application d'ensembles, ω est injective. En effet, si $\omega(C) = \omega(C')$, ceci entraîne $\beta(C) = \beta(C')$, $\gamma(C) = \gamma(C')$, donc $\beta(C - C') = 0$ et $C - C' \in N(A)$. D'après [8], théorème 6, $C - C'$ est une algèbre de Clifford triviale, donc $C = C'$ dans $\mathcal{H}_0(A)$. De plus, l'image de ω est exactement $N(A) \times \mathcal{Q}(A)$. En effet, si $q \in \mathcal{Q}(A)$, existe une algèbre de Clifford $C \in \mathcal{H}_0(A)$ telle que $\omega(C) = (0, q)$ (*cf.* [9], § 3, nº 3.1, démonstration du théorème 2). Si maintenant $(b, q) \in N(A) \times \mathcal{Q}(A)$, alors il existe une algèbre de Clifford C' dans $N(A)$ telle que $b = \beta(C')$, donc

$$\omega(C \hat{\otimes} C') = (\beta(C \otimes C'), \gamma(C \hat{\otimes} C')) = (\beta(C'), \gamma(C)) = (b, q),$$

car C' étant dans $N(A)$, on a

$$C \hat{\otimes} C' = C \otimes C' \qquad \text{et} \qquad \gamma(C') = 0.$$

De plus, $\beta(C) = 0$ par construction de C. On a donc montré que $\mathrm{Im}(\omega) = N(A) \times \mathcal{Q}(A)$. Par la suite on identifiera $\mathcal{H}_0(A) = N(A) \times \mathcal{Q}(A)$ et toute algèbre de Clifford $C \in \mathcal{H}_0(A)$ peut se représenter comme une paire $C = (\beta(C), \gamma(C))$.

PROPOSITION 1. — *Si* $2 = 0$ *dans* A, *on a un isomorphisme de groupes* $\mathcal{H}_0(A) = N(A) \times \mathcal{Q}(A)$.

On remarque tout d'abord (sans aucune hypothèse sur le 2 dans A) que si A est local et si t est un générateur de $X(C)$ sur A, où $C \in \mathcal{H}_0(A)$, alors $t^2 \in U(A)$ et l'image de t^2 dans $U(A)/U^2(A)$ est le discriminant de C. Dans ce cas (A local),

$$U(A)/U^2(A) = H^1(\mathfrak{X}, A, \sqrt{1})$$

car $\mathrm{Pic}(A) = 0$ (*cf.* [9], § 3, nº 3.2, proposition 1).

Supposons maintenant que $2 = 0$ et soit $C \in \mathcal{H}_0(A)$. Si $x \in X(C)$, $xy = -yx$ pour tout $y \in P$, où $C = C(P, Q)$ et comme $2 = 0$, alors $xy = -xy$ pour tout $y \in P$. Donc, $xy = yx$ pour tout $y \in P$ et ceci entraîne que $x \in Z(C) = A$. Donc, $X(C) = A$. De plus, si A est local et t est un générateur de $X(C)$, alors l'image de t^2 dans $U(A)/U^2(A)$ est le discriminant de C. Dans le cas $2 = 0$, il en résulte que $t^2 = a^2$ avec $a \in U(A)$ et ceci veut dire que $(X(C), \mu) = (A, \mathrm{id})$. Donc, $\beta(\alpha(C, C')) = 0$ quels que soient C et C' dans $\mathcal{H}_0(A)$ et, par suite, l'application $\beta : \mathcal{H}_0(A) \to \mathcal{B}_2(A)$ est un homomorphisme de groupes abéliens. Ceci nous montre que $\mathcal{H}_0(A)$ est isomorphe au produit direct de groupes $N(A) \times \mathcal{Q}(A)$.

3. Le calcul quaternionien.

3.1. Trivialisations. — Soit A un anneau. On dira qu'une A-algèbre centrale et séparable C est *triviale* si C est l'algèbre des endomorphismes d'un module projectif de type fini sur A, i. e., si C est zéro dans le groupe de Brauer $\mathcal{B}(A)$.

Soit C une A-algèbre. On dira qu'un idempotent $e \in C$ est *non trivial* (resp. *trivial*) si 1 et e sont A-linéairement indépendants (resp. dépendants). Il est clair que 0 et 1 sont des idempotents triviaux de C et que, plus généralement, tout idempotent de A est un idempotent trivial de C. Donc, si $e \in C$ *est non trivial, alors* $e \notin A$. Et, il est facile de voir que $e \in C$ est non trivial si et seulement si pour tout idéal premier $\mathfrak{p}$ de A, $e_{\mathfrak{p}}$ est un idempotent non trivial de $C_{\mathfrak{p}}$, $e_{\mathfrak{p}}$ désignant l'image de e par la flèche canonique $C \to C_{\mathfrak{p}} = C \otimes_A A_{\mathfrak{p}}$.

Lemme 1. — *Toute algèbre centrale séparable de rang 4 admettant un idempotent non trivial est triviale.*

En effet, soit C une A-algèbre centrale séparable de rang 4 et soit $e \in C$ un idempotent non trivial. On peut écrire $C = Ce \oplus C(1-e)$ et montrons que Ce et $C(1-e)$ sont des A-modules projectifs de rang 2. On peut supposer A local de corps résiduel k, donc $C \otimes k$ (où $\otimes = \otimes_A$) est une k-algèbre centrale simple. Il s'ensuit que $C \otimes k$ est une algèbre de matrices sur un corps (gauche) D. Puisque C a un idempotent, alors $C \neq D$ et, pour des raisons de dimension on a $D = k$. Dans ce cas, un idempotent dans l'anneau des matrices 2×2 à coefficients dans k engendre un sous-k-espace vectoriel de dimension 2.

Puisque C est de rang 4 et Ce de rang 2 alors $\mathrm{End}_C(Ce)$ est un A-module projectif de rang 1, i. e., $\mathrm{End}_C(Ce) \simeq A$. Il s'ensuit que $C \simeq \mathrm{End}_A(Ce)$.

Corollaire 1. — *Toute algèbre de quaternions admettant un idempotent non trivial est triviale.*

Corollaire 2. — *Si* C *est une algèbre de quaternions sur* A, *alors* $C \otimes C_0$ *est triviale sur* C_0.

En effet, on sait (*cf.* [9], § 1, n° 1.4, lemme 6) que $Z(C_0)$ est une extension quadratique de A, donc $C \otimes Z(C_0)$ admet un idempotent. Comme $C \otimes Z(C_0)$ est de rang 4 sur $Z(C_0)$, alors $C \otimes Z(C_0)$ est triviale sur $Z(C_0)$. Comme $Z(C_0) = C_0$, le corollaire est démontré.

Le corollaire 2 nous dit, en particulier, que toute algèbre de quaternions sur A se trivialise dans une extension quadratique convenable de A.

Pour d'autres résultats sur les trivialisations, on renvoie à [9], § 1, n° 1.5.

3.2. Représentants canoniques.

Lemme 2. — *Si* $B \in \mathfrak{Q}(A)$, *il existe, à isomorphisme près, une et une seule algèbre de quaternions* C *telle que* $C_0 = B$ *et il existe* $e \in C_1$ *avec* $e^2 = 1$.

Soit $D = B$; $\overline{D} = B \otimes_A D$ est une extension quadratique triviale de B, car isomorphe à $B \oplus B$. Si ε_0, $\varepsilon_1 : \overline{D} \to B \otimes_A B \otimes_A D$ se déduisent des applications $B \rightrightarrows B \otimes_A B$ définies par $x \mapsto 1 \otimes x$ et $x \mapsto x \otimes 1$ respectivement, il existe un isomorphisme $\alpha : \varepsilon_0 \overline{D} \to \varepsilon_1 \overline{D}$ tel que $D = \operatorname{Ker}(\varepsilon_1 - \alpha\varepsilon_0)$, où $\varepsilon_1 - \alpha\varepsilon_0 : \overline{D} \to \varepsilon_1 \overline{D}$. Comme $\overline{D}$ est triviale, il existe une algèbre de quaternions $\overline{C}$ (algèbre de matrices 2×2 sur B) telle que $\overline{C}_0 = \overline{D}$ et il existe un $\bar{e} \in \overline{C}_1$ avec $\bar{e}^2 = 1$. En effet, comme $\overline{C}_0$ est la sous-algèbre de $\overline{C}$ formée des matrices $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ et $\overline{C}_1$ est le sous-module de $\overline{C}$ formé des matrices $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$, x et y parcourant B, il suffit de prendre $\bar{e} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Il s'ensuit que α s'étend à $\beta : \varepsilon_0 \overline{C} \to \varepsilon_1 \overline{C}$ par la condition $\beta(\varepsilon_0 \bar{e}) = \varepsilon_1 \bar{e}$, i. e.,

$$\beta \varepsilon_0 (x + ye) = \alpha \varepsilon_0 (x) + \alpha \varepsilon_0 (y)\, \varepsilon_1 (\bar{e}),$$

x et y parcourant $\overline{C}_0$. Comme $\varepsilon_2 \beta . \varepsilon_0 \beta = \varepsilon_1 \beta : B^{\otimes 3} \otimes D \to B^{\otimes 3} \otimes D$, si l'on pose $C = \operatorname{Ker}(\varepsilon_1 - \beta\varepsilon_0)$, C satisfait aux conditions imposées. Pour voir que C est une algèbre de quaternions, on procède comme suit. On sait que $\varepsilon_1 - \alpha\varepsilon_0$ est homogène, donc C est graduée sur $\mathbf{Z}_2$. De plus, $C_0 = D$ et si l'on considère la multiplication $\mu : C_1 \to A$, alors $C = C(C_1, \mu)$. Ceci démontre l'existence de C.

Pour voir qu'elle est unique, on remarque que si C et C′ sont deux algèbres de quaternions telles que $\alpha : C_0 \xrightarrow{\sim} C'_0$ est un isomorphisme et il existe $e \in C_1$ et $e' \in C'_1$ tels que $e^2 = e'^2 = 1$, alors il existe un isomorphisme $\rho : C \to C'$ défini par $\rho(xe) = \alpha(x)\, e'$ pour tout $x \in C_0$. En effet, il suffit d'observer que $C_1 = C_0 e$ et que $C'_1 = C'_0 e'$. Ceci achève la démonstration.

Pour tout $B \in \mathfrak{Q}(A)$, on note $h(B)$ l'algèbre de quaternions, à isomorphisme près, définie par le lemme 2. On l'appellera le *représentant canonique de* B.

Lemme 3. — *Pour tout* $B \in \mathfrak{Q}(A)$, $\beta(h(B)) = 0$.

Soient $B \in \mathfrak{Q}(A)$, $C = h(B)$ et D la sous-algèbre commutative maximale de C engendrée par $\{1, e\}$, où $e \in C_1$ obéit à la condition $e^2 = 1$. Comme $D \approx A \oplus A$, D est séparable, donc C est une algèbre D-projective.

Il s'ensuit (*cf.* [5], proposition 2.4, p. 37), que l'homomorphisme de D-algèbres $\theta : C \otimes_A D \to \mathrm{End}_D(C)$ défini par $\theta(c \otimes b)(x) = cxb$ est un isomorphisme. Si l'on considère la contraction $\varphi : D \to A$ définie par $\varphi(1) = 1$ et $\varphi(e) = 1$, alors l'application composée évidente $A \to D \xrightarrow{\varphi} A$ est l'identité de A et, par suite, $C \approx (C \otimes_A D) \otimes_D A \approx \mathrm{End}_A(C \otimes_D A)$. Donc, C est triviale dans $\mathcal{B}(A)$.

3.3. Calcul de $\beta(\alpha(C, C'))$. — Soient C et C′ dans $\mathcal{H}_0(A)$. On sait que $\beta(\alpha(C, C'))$ ne dépend que des images de C et C′ dans $H^1(\mathfrak{X}, A, \sqrt{1})$ et, *a fortiori*, que des images de C et C′ dans $H^1(\mathfrak{X}, A, \mathrm{Ip})$, i. e., de $B = Z(C_0)$ et $B' = Z(C'_0)$, Donc,

$$\beta(\alpha(C, C')) = \beta(\alpha(h(B), h(B'))\qquad \text{et} \qquad \beta(h(B) \hat{\otimes} h(B')) = \beta(\alpha(h(B), h(B'))).$$

D'autre part,

$$h(B) \hat{\otimes} h(B') \approx h(B) \otimes h(B')_*$$

et, par suite,

$$\beta(\alpha(C, C')) = \beta(h(B')_*).$$

Supposons maintenant que A soit local et soient

$$h(B) = h_1(1, m), \qquad h(B') = h_1(1, m') \qquad \Delta = 1 - 4m \qquad \text{et} \qquad \Delta' = 1 - 4m'.$$

Alors

$$h(B')_* = h_\Delta(\Delta, \Delta m').$$

Supposons, de plus, que 2 soit inversible dans l'anneau (local) A. Si le quaternion $h(B')_*$ est engendré par u_1, u_2 avec

$$u_1^2 = \Delta, \qquad u_2^2 = \Delta m', \qquad u_1 u_2 + u_2 u_1 = \Delta,$$

on fait le changement de base suivant :

$$v_1 = u_1, \qquad v_2 = 1 - \frac{2}{\Delta} u_1 u_2.$$

Il est clair qu'on change la graduation mais du point de vue du groupe de Brauer, ceci n'a aucune importante. On a alors $v_1^2 = \Delta$, $v_2^2 = \Delta'$ et $v_1 v_2 + v_2 v_1 = 0$. Ceci nous montre que

$$\beta(\alpha(C, C')) = \beta(h_0(\Delta, \Delta'))$$

et notre construction coïncide avec celle de Wall (*cf.* [12]).

3.4. L'homomorphisme $\omega : \mathcal{H}_0(A) \to \mathcal{B}_2(A) \tilde{\times} \mathcal{Q}(A)$. — Considérons le produit cartésien (d'ensembles) $\mathcal{B}_2(A) \times \mathcal{Q}(A)$. On peut le munir d'une structure de groupe abélien en posant

$$(b, q) + (b', q') = (b + b' + \beta(\alpha(C, C')), q + q') \quad \text{si} \quad q = \gamma(C) \quad \text{et} \quad q' = \gamma(C')$$

et on le notera $\mathcal{B}_2(A) \tilde{\times} \mathcal{Q}(A)$. Il est clair que l'application $\omega : \mathcal{H}_0(A) \to \mathcal{B}_2(A) \tilde{\times} \mathcal{Q}(A)$ (*cf.* 2.4, lemme 2) est un homomorphisme de groupes car

$$\begin{aligned}\omega(C \hat{\otimes} C') &= (\beta(C \hat{\otimes} C'), \gamma(C \hat{\otimes} C')) \\ &= (\beta(C) + \beta(C') + \beta(\alpha(C, C')), \gamma(C) + \gamma(C')) = \omega(C) + \omega(C').\end{aligned}$$

De plus, ω est injectif en tant que application d'ensembles, donc aussi en tant que homomorphisme de groupes abéliens. Muni de cette structure, on identifiera toujours $\mathcal{H}_0(A)$ à un sous-groupe abélien de $\mathcal{B}_2(A) \tilde{\times} \mathcal{Q}(A)$, à savoir,

$$\mathcal{H}_0(A) = N(A) \tilde{\times} \mathcal{Q}(A).$$

4. Cas local avec 2 inversible.

Dans tout ce paragraphe, sauf mention expresse du contraire, on supposera que A est un anneau local et que 2 est inversible dans A. Donc, la transformation naturelle $\mathrm{Ip} \xrightarrow{\sim} \sqrt{1}$ est un isomorphisme et, par suite, elle induit un isomorphisme

$$\mathcal{Q}(A) = H^1(\mathcal{X}, A, \mathrm{Ip}) \xrightarrow{\sim} H^1(\mathfrak{X}, A, \sqrt{1}).$$

4.1. Calcul de $\beta(\alpha(C, C'))$. — D'après l'hypothèse faite, on sait qu'il existe des quaternions de la forme $h_0(a, b)$. En particulier $h_0(1, -\Delta)$ est un quaternion de discriminant 4Δ et $\beta(h_0(1, -\Delta)) = 0$ car $h_0(1, -\Delta)$ a $\frac{1}{2}(1 + u_1)$ comme idempotent, si

$$u_1^2 = 1, \qquad u_2^2 = -\Delta \qquad \text{et} \qquad u_1 u_2 + u_2 u_1 = 0.$$

Puisque $H^1(\mathfrak{X}, A, \sqrt{1}) = U(A)/U^2(A)$, car $\mathrm{Pic}(A) = 0$, et que les couples $(P, \mu) \in H^1(\mathfrak{X}, A, \sqrt{1})$ s'écrivent (A, μ) avec $\mu : A \otimes A = A \to A$, alors $\mu(1 \otimes 1) = a \in U(A)$ est déterminé à moins d'un carré. De plus, si $a = b^2$, le diagramme

$$\begin{tikzcd} A \otimes A \arrow[r, "a"] \arrow[d, "b \otimes b"'] & A \arrow[d, "\mathrm{id}"] \\ A \otimes A \arrow[r, "1"] & A \end{tikzcd}$$

est commutatif, donc $(A, a) = (A, 1)$. Ceci nous montre que $\beta(\alpha(C, C'))$ dépend seulement du discriminant de C et C′ et l'on note $\beta(\alpha(\Delta, \Delta'))$.

On peut calculer $\beta(\alpha(\Delta, \Delta'))$ comme suit. On a

$$\beta(h_0(-1, \Delta) \hat{\otimes} h_0(1, -\Delta')) = \beta(h_0(-1, \Delta)) + \beta(\alpha(\Delta, \Delta'))$$

et

$$\beta(h_0(-1, \Delta) \hat{\otimes} h_0(1, -\Delta')) = \beta(h_0(-1, \Delta)) + \beta(h_0(\Delta, -\Delta\Delta')),$$

car $\beta(h_0(1, -\Delta')) = 0$. Donc,

$$\beta(\alpha(\Delta, \Delta')) = \beta(h_0(\Delta, -\Delta\Delta')).$$

Si l'on change la graduation de $h_0(\Delta, -\Delta\Delta')$ en prenant comme nouvelle base

$$v_1 = u_1, \qquad v_2 = \frac{1}{\Delta} u_1 u_2,$$

on a

$$\beta(h_0(\Delta, -\Delta\Delta')) = \beta(h_0(\Delta, \Delta')),$$

donc

$$\beta(\alpha(\Delta, \Delta')) = \beta(h_0(\Delta, \Delta')) \quad (cf.\ [12]).$$

On peut encore écrire

$$\beta(\alpha(\Delta, \Delta')) = \beta(h_0(\Delta, \Delta')) = \beta(h_0(-1, -\Delta\Delta'))$$

et si $-1 \in U^2(A)$, alors

$$\beta(h_0(-1, -\Delta\Delta')) = \beta(h_0(1, -\Delta\Delta')) = 0.$$

Donc, pour tout C, $C' \in \mathcal{H}_0(A)$, $\beta(\alpha(C, C')) = 0$. Ceci démontre le résultat suivant :

Proposition 1. — *Si* $2 \in U(A)$ *et si* $-1 \in U^2(A)$, *on a un isomorphisme de groupes* $\mathcal{H}_0(A) = N(A) \times \mathfrak{Q}(A)$ (2).

Dans le cas particulier où $\Delta' = \Delta$, on a

$$h_0(\Delta, -\Delta^2) = h_0(-1, \Delta),$$

donc on peut prendre

$$\beta(\alpha(\Delta, \Delta)) = \beta(h_0(-1, \Delta)).$$

4.2. Nullité de $\beta(h_0(-1, \Delta))$.

---

(2) En fait, si A est un anneau commutatif à élément unité (non nécessairement local) et -1 est un carré dans A, alors les groupes $\mathcal{H}(A)$, $\mathcal{H}_0(A)$ et le groupe de Witt $\mathcal{W}(A)$ sont des $\mathbf{Z}_2$-espaces vectoriels. En effet, pour tout module quadratique (P, Q), on a $(P, Q) \cong (P, -Q)$ et par suite, $(P, Q) \perp (P, Q)$ est un espace hyperbolique. La proposition 1 s'ensuit.

THÉORÈME 1. — *Pour un quaternion de la forme* $h_0(-1, \Delta)$, *les conditions suivantes sont équivalentes :*

(i) $\beta(h_0(-1, \Delta)) = 0$;

(ii) Δ *est une somme de deux carrés.*

Démontrons que (i) $\Rightarrow$ (ii). En effet, supposons donné l'isomorphisme

$$h_0(-1, \Delta) \xrightarrow{\theta} \mathrm{End}_A(A^2)$$

et soit $\varphi = \theta(u_1)$, où

$$u_1^2 = -1, \qquad u_2^2 = \Delta \qquad \text{et} \qquad u_1 u_2 + u_2 u_1 = 0.$$

Alors $\varphi^2 = -\theta(1)$ et étant donné que, modulo l'idéal maximal $\mathfrak{m}$ de A, φ n'est pas un scalaire, il existe $t \in A^2$ tel que $\{t, \varphi(t)\}$ soit une base du A-module libre A^2. En effet, modulo $\mathfrak{m}$, $\{\bar{t}, \overline{\varphi(t)}\}$ est une base de $A^2/\mathfrak{m}A^2$.

Si l'on prend $t_1 = t$, $t_2 = \varphi(t)$, φ se représente par la matrice $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Soit

$$\theta(u_2) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \text{avec} \quad a, b, c, d \in A.$$

On a

$$\theta(u_1 u_2) = \theta(u_1)\,\theta(u_2) = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix} \qquad \text{et} \qquad \theta(u_2 u_1) = \theta(u_2)\,\theta(u_1) = \begin{bmatrix} b & -a \\ d & -c \end{bmatrix},$$

donc, à cause de $u_1 u_2 + u_2 u_1 = 0$, on en déduit que

$$\theta(u_2) = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}.$$

Ceci nous montre que

$$\Delta = u_2^2 = a^2 + b^2.$$

Montrons que (ii) $\Rightarrow$ (i). En effet, si $\Delta = a^2 + b^2$, on a un homomorphisme d'algèbres $\theta : h_0(-1, \Delta) \to A(2)$ défini par

$$\theta(u_1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad \theta(u_2) = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}.$$

Puisqu'il s'agit d'un homomorphisme d'algèbres d'Azumaya et que $\theta|_A$ est injectif, alors θ est injectif. D'autre part, modulo $\mathfrak{m}$, θ est surjectif, donc θ est lui-même surjectif et, par suite, un isomorphisme.

PROPOSITION 2. — *Si* $2 \in U(A)$ *et si* $-1 \in U^2(A)$, *alors*

$$2\mathcal{H}_0(A) = 0.$$

(i) On remarque, tout d'abord, sans supposer que 2 soit inversible dans A, que si $C \in \mathcal{H}_0(A)$ et si $h_1(1, m)$ est un représentant canonique de C dans $H^1(\mathfrak{X}, A, \sqrt{1})$, alors

$$\begin{aligned}\beta(2C) &= \beta(C \hat{\otimes} C) = \beta(C) + \beta(C) + \beta(\alpha(C, C)) \\ &= \beta(\alpha(C, C)) = \beta(h_1(1, m)_*) = \beta(h_\Delta(\Delta, \Delta m)),\end{aligned}$$

où $\Delta = 1 - 4m$. Il existe alors un $t \in h_\Delta(\Delta, \Delta m)$ tel que $t^2 = -1$. En effet, si $u_1^2 = \Delta$, $u_2^2 = \Delta m$ et $u_1 u_2 + u_2 u_1 = \Delta$, alors $t = \frac{1}{\Delta}(u_1 - 2u_2)$ satisfait à la condition $t^2 = -1$.

(ii) Si, de plus, 2 est inversible dans A et il existe un $a \in U(A)$ tel que $a^2 = -1$, alors il existe un idempotent $e \in h_\Delta(\Delta, \Delta m)$. En effet, $e = \frac{1}{2}\left(1 - \frac{t}{a}\right)$ obéit à la condition $e^2 = e$. Donc, $\beta(h_\Delta(\Delta, \Delta m)) = 0$, i. e. $\beta(2C) = 0$.

(iii) Étant donné que $2\mathcal{H}_0(A) \subset N(A) \subset \mathcal{B}_2(A)$, alors pour tout $C \in \mathcal{H}_0(A)$ on a $2C = 0$ dans $\mathcal{B}_2(A)$, donc $2\mathcal{H}_0'(A) = 0$.

Proposition 3. — (i) *Si* $2 \in U(A)$ *et si* $-1 \in U^2(A)$, *tout élément de* $\mathcal{H}(A)$ *est d'ordre* 2.

(ii) *Si* $2 \in U(A)$, $-1 \notin U(A)$ *et si* -1 *est une somme de deux carrés, tout élément de* $\mathcal{H}(A)$ *est d'ordre* 2 *ou* 4.

(iii) *Si* $2 \in U(A)$, $-1 \notin U(A)$ *et si* -1 *n'est pas une somme de deux carrés, il existe un élément de* $\mathcal{H}(A)$ *d'ordre* 8.

Soit $C = C(A, \mu)$, où $\mu : A \to A$ est la forme quadratique définie par $\mu(a) = a^2$ pour tout a dans A. Alors $2C = h_0(1, 1)$ et $W(2C) = -1$.

Si $-1 \in U^2(A)$, $\mathcal{H}_0(A)$ est un $\mathbf{Z}_2$-module et la suite exacte de groupes abéliens $0 \to \mathcal{H}_0(A) \to \mathcal{H}(A) \to \mathbf{Z}_2 \to 0$ nous montre que $\mathcal{H}(A)$ est aussi un $\mathbf{Z}_2$-module. En effet, l'application qui envoie l'unité de $\mathbf{Z}_2$ dans l'élément $\{C\}$ de $\mathcal{H}(A)$ est bien définie, car $\{C\}$ est d'ordre 2, et scinde la suite exacte ci-dessus. Ceci démontre (i).

Supposons maintenant que $W(2C) = -1 \notin U^2(A)$. Alors $2C \notin N(A)$, donc $4C \in N(A)$. Il s'ensuit que

$$4C = \beta(4C) = \beta(h_0(1, 1) \hat{\otimes} h_0(1, 1)) = \beta(h_0(1, 1) \otimes h_0(-1, -1)) = \beta(h_0(-1, -1)),$$

car $\beta(h_0(1, 1)) = 0$ (*cf.* 4.1). Ou bien -1 est une somme de deux carrés et $\beta(h_0(-1, -1)) = 0$, donc $4\{C\} = 0$, ou bien -1, n'est pas une somme de deux carrés et alors $\beta(h_0(-1, -1)) \neq 0$, donc, $4\{C\} \neq 0$, $8\{C\} = 0$. Ceci démontre (iii).

En ce qui concerne (ii), on remarque que comme tous les éléments de $\mathcal{H}_0(A)$ sont d'ordre 4, il suffit d'étudier les éléments de $\mathcal{H}(A)$ dont l'image dans $\mathbf{Z}_2$ et 1. Si $C' = C(P, Q)$ représente un élément de $\mathcal{H}(A)$, où P est de rang impair, alors $C \hat{\otimes} C'$ représente un élément de $\mathcal{H}_0(A)$, donc $0 = 4(\{C\} + \{C'\}) = 4\{C'\}$, car $4\{C\} = 0$.

Remarque. — Si K est un corps totalement ordonné de caractéristique zéro, il existe dans $\mathcal{H}(K)$ un élément d'ordre 8 [*cf.* proposition 3, (iii)].

4.3. Le groupe $\mathcal{H}_0(A)$. — On sait (*cf.* [8], théorème 7) que $\mathcal{H}_0(A)$ est un 2-groupe fini dont les éléments sont d'ordre 2 ou 4. D'après le théorème de décomposition de groupes abéliens d'ordre borné $\mathcal{H}_0(A)$ est la somme directe d'un module libre L sur $\mathbf{Z}_4$ et d'un espace vectoriel V sur $\mathbf{Z}_2$. Si $O_2(A) = \{x \mid x \in \mathcal{H}_0(A),\ 2x = 0\}$, L a pour base un ensemble de représentants d'une base de $\mathcal{H}_0(A)/O_2(A)$ et $V = O_2(A)/2\,\mathcal{H}_0(A)$. La suite exacte de groupes abéliens

$$0 \to N(A) \to \mathcal{H}_0(A) \xrightarrow{\theta} U(A)/U^2(A) \to 0$$

et $N(A) \subset \mathcal{B}_2(A)$ nous montrent que $N(A) \subset O_2(A)$ et

$$\mathcal{H}_0(A)/O_2(A) = (U(A)/U^2(A))/\theta(O_2(A)).$$

Soit $U^d(A)$ le sous-groupe de $U(A)$ formé par les éléments qui sont somme de deux carrés. Le théorème 1 nous dit alors que

$$\theta(O_2(A)) = U^d(A)/U^2(A), \qquad \text{donc} \quad \mathcal{H}_0(A)/O_2(A) = U(A)/U^d(A).$$

Puisque $2\,\mathcal{H}_0(A) \subset N(A)$, la suite exacte

$$0 \to N(A) \to O_2(A) \to \theta(O_2(A)) \to 0$$

nous fournit la suite exacte de $\mathbf{Z}_2$-espaces vectoriels

$$0 \to N(A)/2\,\mathcal{H}_0(A) \to V \to U^d(A)/U^2(A) \to 0$$

et, par suite,

$$V = (N(A)/2\,\mathcal{H}_0(A)) \oplus (U^d(A)/U^2(A)).$$

Il nous suffit alors de calculer $2\,\mathcal{H}_0(A)$.

Or, $2\,\mathcal{H}_0(A) \subset \mathcal{B}_2(A)$ et $2\,\mathcal{H}_0(A)$ est alors l'ensemble des éléments de la forme $\beta(h_0(-1, \Delta))$. Si $A[i] = A[X]/(X^2+1)$, alors il est clair que

$$\beta(h_0(-1, \Delta) \otimes_A A[i]) = 0 \quad \text{dans } \mathcal{B}(A[i])$$

et, par suite, $2\mathcal{H}_0(A) \subset \mathcal{B}_2(A[i]/A) \cap N(A)$, où

$$\mathcal{B}_2(A[i]/A) = \operatorname{Ker}(\mathcal{B}_2(A) \to \mathcal{B}_2(A[i]))$$

(*groupe de Brauer relatif*).

Lemme 1. — *Soient* A *un corps de caractéristique* $\neq 2$ *et*

$$h \in \mathcal{B}_2(A[\sqrt{d}]/A) = \operatorname{Ker}(\mathcal{B}_2(A) \to \mathcal{B}_2(A[\sqrt{d}])).$$

Il existe alors un élément $t \in h$ *tel que* $t^2 = d$.

En effet, si $e = r \otimes 1 + s \otimes \sqrt{d} \in h \otimes A[\sqrt{d}]$ est un idempotent, où $r, s \in h$, la condition $e^2 = e$ entraîne

$$r^2 + s^2 d = r \quad \text{et} \quad rs + sr = s.$$

Il existe une base orthogonale $\{u, v\}$ et soient

$$r = a + bu + cv + duv \quad \text{et} \quad s = a' + b'u + c'v + d'uv,$$

où $a, b, c, d, a', b', c', d'$ sont dans A. Donc,

$$s^2 = a'^2 + b'^2 u^2 + c'^2 v^2 - d'^2 u^2 v^2 + 2a'(s - a').$$

Si $a' = 0$, alors $s^2 \in A$. On peut supposer $s \neq 0$ car si $s = 0$, $r = r^2$ est un idempotent de h et h est une algèbre de matrices. Mais dans ce cas, il existe déjà dans h un élément de carré d $\left(\text{v. g.}, \begin{vmatrix} 0 & d \\ 1 & 0 \end{vmatrix}^2 = \begin{vmatrix} d & 0 \\ 0 & d \end{vmatrix} = d\right)$. Si $s \neq 0$, $\left(\frac{1}{s^2} rs\right)^2 = d$.

Supposons $a' \neq 0$. Ou bien $s = a'$ est un scalaire, donc $r = \frac{1}{2}$ et $\left(\frac{1}{2a'}\right)^2 = d$; ou bien s n'est pas un scalaire et étant donné que $(1 - 2a)^2 = 4d(s - a')^2$, alors $1 - 2a \neq 0$ (car sinon $s = a'$) et le vecteur $t = \frac{2d}{1 - 2a}(s - a')$ satisfait à la condition $t^2 = d$.

On remarque (d'après le lemme 1) que s'il existe $u \in h$ tel que $u^2 = d$, alors il existe $v \in h$ tel que $\{u, v\}$ engendre h et $uv + vu = 0$. Il s'ensuit que $h = h_0(d, v^2)$.

Lemme 2. — *Si* A *est un corps de caractéristique* $\neq 2$, $2\mathcal{H}_0(A)$ *est le sous-groupe de* $\mathcal{B}_2(A[i]/A)$ *dont les éléments sont représentés par des quaternions.*

On effet, on sait que pour tout $C \in \mathcal{H}_0(A)$,

$$2C = \beta(\alpha(C, C)) = \beta(h_0(-1, \Delta)),$$

donc $2C \underset{\mathcal{B}}{\sim} h_0(-1, \Delta)$, où $\underset{\mathcal{B}}{\sim}$ désigne l'*équivalence de Brauer* (équivalence d'algèbres centrales séparables).

Réciproquement, soit $h \in \mathcal{B}_2(A[i]/A)$ un quaternion. On peut écrire (*cf.* lemme 1), $h = h_0(-1, \Delta)$, donc

$$\begin{aligned}\beta(h \hat{\otimes} h) &= \beta(h \otimes h_\star) = \beta(h_0(-1, \Delta) \otimes h_0(-\Lambda, \Delta^2))\\ &= \beta(h_0(-1, \Delta)) + \beta(h_0(1, -\Delta)) = \beta(h),\end{aligned}$$

car $\beta(h_0(1, -\Delta)) = 0$. Donc $h \underset{\mathcal{B}}{\sim} h \hat{\otimes} h$ et par suite, $h \in 2\mathcal{H}_0(A)$, si l'on identifie $2\,\mathcal{H}_0(A)$ à un sous-groupe de $\mathcal{B}_2(A)$.

Remarque. — Il est clair que si A est un anneau local tel que 2 y soit inversible et si, de plus, le lemme 1 est vérifié pour A, alors le lemme 2 est aussi vrai pour l'anneau A.

5. Étude de quelques exemples.

5.1. L'anneau des entiers.

PROPOSITION 1. — *Le groupe de Brauer de* $\mathbf{Z}$ *est trivial.*

Pour une démonstration de cette proposition (*voir* [7], proposition 2.4, p. 95).

COROLLAIRE. — $\mathcal{H}_0(\mathbf{Z}) = 0$ *et* $\mathcal{H}(\mathbf{Z}) = 0$.

En effet, on sait déjà que $\mathcal{Q}(\mathbf{Z}) = 0$ (*cf.* [9], § 1, n° 1.6, proposition 4). Donc, d'après 3.5 et la proposition 1, $\mathcal{H}_0(\mathbf{Z}) = 0$. La suite exacte de groupes abéliens $0 \to \mathcal{H}_0(\mathbf{Z}) \to \mathcal{H}(\mathbf{Z}) \to \mathbf{Z}_2$ nous donne alors la suite exacte $0 \to \mathcal{H}(\mathbf{Z}) \to \mathbf{Z}_2$ et comme 2 n'est pas inversible dans $\mathbf{Z}$, alors $\mathcal{H}(\mathbf{Z}) = 0$.

5.2. CAS D'UN CORPS ALGÉBRIQUEMENT CLOS. — Soit K un corps algébriquement clos. Alors $\mathcal{Q}(K) = 0$ et $\mathcal{B}(K) = 0$, donc $\mathcal{H}_0(K) = 0$. La suite exacte de groupes abéliens $0 \to \mathcal{H}(K) \to \mathbf{Z}_2$ nous montre alors que $\mathcal{H}(K) = 0$ si la caractéristique de K est 2 et que $\mathcal{H}(K) = \mathbf{Z}_2$ si la caractéristique de K est $\neq 2$. En particulier, $\mathcal{H}_0(\mathbf{C}) = 0$ et $\mathcal{H}(\mathbf{C}) = \mathbf{Z}_2$, $\mathbf{C}$ étant le corps des nombres complexes.

5.3. Corps des nombres réels. — Soit $\mathbf{R}$ le corps des nombres réels. Puisque $\frac{1}{2} \in \mathbf{R}$, on a la suite exacte de groupes abéliens $0 \to \mathcal{H}_0(\mathbf{R}) \to \mathcal{H}(\mathbf{R}) \to \mathbf{Z}_2 \to 0$. Étant donné que $\mathcal{B}(\mathbf{R}) = \mathbf{Z}_2$ et que $G(\mathbf{R}) = \mathbf{Z}_2$, alors $\mathcal{H}(\mathbf{R})$ a au plus 8 éléments. Pour montrer que $\mathcal{H}(\mathbf{R}) = \mathbf{Z}_8$, il suffit d'exhiber une algèbre de Clifford d'ordre 8. Considérons la forme quadratique $Q : \mathbf{R} \to \mathbf{R}$ définie par $x \mapsto -x^2$ et soit $C = C(\mathbf{R}, Q)$ son algèbre de Clifford. Il est clair que $2C = C \hat{\otimes} C = h_0(-1, -1)$ est l'algèbre des quaternions ordinaire, donc $\gamma(2C) = \mathbf{C}$ ($=$ corps des complexes) est $\neq 0$ dans $\mathcal{Q}(\mathbf{R})$. Ceci nous montre que $2C \neq 0$ dans $\mathcal{H}_0(\mathbf{R})$. D'autre part, $4C \in N(\mathbf{R}) \subset \mathcal{B}_2(\mathbf{R})$, donc

$$\begin{aligned} 4C = \beta(4C) &= \beta(\alpha(2C, 2C)) = \beta(\alpha(h_0(-1, -1), h_0(-1, -1))) \\ &= \beta(\alpha(h_0(1, 1), h_0(1, 1))) = \beta(h_0(-1, -1)) \neq 0 \end{aligned}$$

car $h_0(-1, -1)$ n'est pas triviale dans $\mathcal{B}(\mathbf{R})$. Il s'ensuit que $4C \neq 0$ dans $\mathcal{H}(\mathbf{R})$, donc C est d'ordre 8. Ceci nous montre que $\mathcal{H}(\mathbf{R}) = \mathbf{Z}_8$, donc $\mathcal{H}_0(\mathbf{R}) = \mathbf{Z}_4$.

5.4. Cas d'un corps fini. — Soit k un corps fini. On sait (*cf.* [10]) que $\mathcal{B}(k) = 0$. Si la caractéristique de k est p, alors k a p^n éléments, où n est un entier convenable. Soit K une extension quadratique de k; K est un k-espace vectoriel de dimension 2 donc K a $(p^n)^2 = p^{2n}$ éléments. On sait que $K = k[x]$, où $x^2 - x = m \in k$ et $1 + 4m \neq 0$, donc K peut s'écrire comme quotient d'un anneau de polynômes, $K = k[X]/(X^2 - X - m)$. Ou bien le polynôme $X^2 - X - m$ est irréductible et dans ce cas, K est un corps fini de caractéristique p et a p^{2n} éléments, ou bien le polynôme $X^2 - X - m$ se décompose en facteurs de degré 1, donc $K = k \oplus k$ est une extension triviale. Ceci nous montre bien que $\mathcal{Q}(k) = \mathbf{Z}_2$ et par suite, $\mathcal{H}_0(k) = \mathbf{Z}_2$.

Supposons $p \neq 2$. Alors la suite de groupes abéliens

$$0 \to \mathcal{H}_0(k) \to \mathcal{H}(k) \to \mathbf{Z}_2 \to 0$$

est exacte et le générateur de $\mathbf{Z}_2$ est représenté dans $\mathcal{H}(k)$ par l'algèbre de Clifford $C = C(k, \mu)$, où $\mu : k \to k$ est la forme quadratique définie par $x \mapsto x^2$. Étant donné que $2C = h_0(1, 1)$, le discriminant de $2C$ est $W(2C) = W(h_0(1, 1)) = -1$, donc $2C = 0$ dans $\mathcal{H}_0(k)$ si et seulement si $-1 \in U^2(k)$. On peut alors résumer comme ceci :

$$\mathcal{H}(k) = \mathbf{Z}_2 \oplus \mathbf{Z}_2, \qquad \text{si} \quad -1 \in U^2(k)$$

et

$$\mathcal{H}(k) = \mathbf{Z}_4, \qquad \text{si} \quad -1 \notin U^2(k).$$

Si $p = 2$, l'homomorphisme de groupes $\mathcal{H}(k) \to \mathbf{Z}_2$ est l'homomorphisme trivial, donc $\mathcal{H}(k) = \mathcal{H}_0(k) = \mathbf{Z}_2$.

5.5. Le corps des rationnels. — On sait (*cf.* [1], chap. 9, § 14, th. 32) que $\mathcal{B}_2(\mathbf{Q})$ est engendré par des quaternions, donc $\mathcal{B}_2(\mathbf{Q}) = \mathrm{N}(\mathbf{Q})$ (*cf.* [9], § 1, nº 1.7, lemme 11). D'après le lemme 2 de 4.3, on en déduit que

$$2\mathcal{H}_0(\mathbf{Q}) = \mathcal{B}_2(\mathbf{Q}(i)/\mathbf{Q}).$$

D'autre part, $\mathrm{U}(\mathbf{Q})/\mathrm{U}^2(\mathbf{Q})$ est un $\mathbf{Z}_2$-espace vectoriel engendré par -1 et les nombres premiers > 0. Or, on sait qu'un produit de nombres premiers distincts est somme de deux carrés si et seulement si chaque facteur est $\equiv 1 \pmod 4$. Ceci nous montre que $\mathrm{U}^d(\mathbf{Q})/\mathrm{U}^2(\mathbf{Q})$ est le sous-$\mathbf{Z}_2$-espace vectoriel de $\mathrm{U}(\mathbf{Q})/\mathrm{U}^2(\mathbf{Q})$ engendré par les nombres premiers $p \equiv 1 \pmod 4$. On le note G_2.

En prenant $\mathrm{C} = \mathrm{C}(\mathbf{Q}, \mu)$, où $\mu : \mathbf{Q} \to \mathbf{Q}$, $\mu(x) = -x^2$ pour tout $x \in \mathbf{Q}$, comme représentant de $\mathcal{H}(\mathbf{Q})/\mathcal{H}_0(\mathbf{Q})$, alors $2\mathrm{C} = h_0(-1, -1)$, donc le générateur -1 est représenté par $2\mathrm{C}$. D'après 4.3, on a alors

$$\mathcal{H}(\mathbf{Q}) = \mathbf{Z}_8 \oplus \mathrm{G}_4 \oplus \mathrm{G}_2 \oplus (\mathcal{B}_2(\mathbf{Q})/\mathcal{B}_2(\mathbf{Q}(i)/\mathbf{Q}))$$

et

$$\mathcal{H}_0(\mathbf{Q}) = 2\mathbf{Z}_8 \oplus \mathrm{G}_4 \oplus \mathrm{G}_2 \oplus (\mathcal{B}_2(\mathbf{Q})/\mathcal{B}_2(\mathbf{Q}(i)/\mathbf{Q})),$$

où G_4 est le $\mathbf{Z}_4$-module libre engendré par les nombres premiers $p \not\equiv 1 \pmod 4$ et où $2\mathbf{Z}_8 (\simeq \mathbf{Z}_4)$ est l'ensemble des nombres pairs de $\mathbf{Z}_8$, ou encore, le $\mathbf{Z}_4$-module libre engendré par le quaternion $h_0(-1, -1)$.

6. BIBLIOGRAPHIE.

[1] A. A. Albert, *Structure of algebras* (*Amer. Math. Soc. Coll. Publ.*, vol. 24, New York, 1939).

[2] M. Auslander et O. Goldman, *The Brauer group of a commutative ring* (*Trans. Amer. Math. Soc.*, vol. 97, 1960, p. 367-409).

[3] H. Bass, *Lectures on topics in Algebraic* K-*theory*, Tata Institute of Fundamental Research, Bombay, 1967.

[4] N. Bourbaki, *Algèbre*, chap. 9, Hermann, Paris, 1959.

[5] S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and cohomology of commutative rings* (*Memoirs Amer. Math. Soc.*, nº 52, 1965).

[6] M. Deuring, *Algebren* (*Ergeb. Math.*, 4, Springer, Berlin, 1935).

[7] A. Grothendieck, *Le groupe de Brauer III. Dix exposés sur la cohomologie des schémas*, North-Holland Publis. Co., Amsterdam et Masson et Cie, Paris, 1968.

[8] A. MICALI et O. E. VILLAMAYOR, *Sur les algèbres de Clifford* (*Ann. scient. Éc. Norm. Sup.*, 4e série, t. 1, 1968, p. 271-304).

[9] A. MICALI et O. E. VILLAMAYOR, *Sur les algèbres de Clifford*, II (*J. Reine und And. Math.* 242, 1970, p. 61-90).

[10] J.-P. SERRE, *Homologie des groupes. Applications arithmétiques*, Cours au Collège de France, 1968-1969.

[11] O. E. VILLAMAYOR, *Separables algebras and Galois extensions* (*Osaka J. Math.*, vol. 4, 1967, p. 161-171).

[12] C. T. C. WALL, *Graded Brauer Groups* (*Journal de Crelle*, t. 213, 1964, p. 187-199).

(Manuscrit reçu le 12 mars 1970.)

A. MICALI,
Université des Sciences et Techniques du Languedoc,
U. E. R. de Mathématiques,
Place Eugène Bataillon,
34-Montpellier, France.

O. E. VILLAMAYOR,
Facultad de Ciencias Exactas y Naturales,
Departemento de Matematicas,
Universidad de Buenos Aires,
Buenos Aires, Argentina.