Inventiones math. 5, 19—41 (1968)

Formes quadratiques, groupes orthogonaux et algèbres de Clifford

J. Tits (Bonn)

1. Introduction

Dans cet article, nous introduisons une notion de forme quadratique dans les algèbres à involution, et associons à une telle forme une «algèbre de Clifford» correspondant dans le cas classique à l'algèbre des éléments de degré pair de l'algèbre de Clifford usuelle. L'origine de ce travail se trouve dans une recherche visant à étendre aux groupes orthogonaux en caractéristique 2 les résultats d' A. WEIL [15] mettant en relation les formes des groupes classiques avec les algèbres à involution. On verra (§ 3) qu'une fois les définitions posées, cette extension est pratiquement automatique.

Nos résultats sont à rapprocher de ceux de N. JACOBSON [7]; ils en diffèrent cependant par le fait que la caractéristique 2 n'est pas exclue (et ne joue même quasiment plus de rôle particulier), et aussi en ce que notre définition de l'algèbre de Clifford est «rationnelle», indépendante de toute descente galoisienne. Au n° 2.3, on verra aussi le rapport qui existe entre les «formes quadratiques quaternioniennes» de E. A. M. SEIP-HORNIX [10] et les nôtres.

Comme nous l'a signalé T. A. SPRINGER, l'idée, essentielle ici, de considérer une forme quadratique comme une classe de formes bilinéaires modulo l'espace des formes alternées, apparaît déjà dans [8] et [12].

Notons enfin que l'expression du pseudo-discriminant (invariant d'Arf) fournie par notre théorème 4, semble nouvelle, même pour les formes quadratiques usuelles (cf. toutefois la formule (6) de [12]).

2. Espaces de formes bilinéaires

2.1. Dans tout cet article, k désigne un corps, $\bar{k}$ sa clôture algébrique et E une k-algèbre centrale simple, de dimension finie n^2, isomorphe à son opposée, notée E^*. Nous «désidentifions» les ensembles sous-jacents de E et E^* et, pour $e \in E$, nous notons e^* l'élément correspondant de E^*, de sorte que $(e e')^* = e'^* e^*$.

Soit σ: $E \to E$ une involution de première espèce (involution fixant chaque élément du centre k). L'espace $E^\sigma = \{e \in E \mid e^\sigma = e\}$ des éléments symétriques de σ est de dimension $\frac{1}{2}n(n+1)$ ou $\frac{1}{2}n(n-1)$ et seul le premier cas peut se présenter si n est impair ou car $k=2$; pour le montrer, on se ramène par une extension du corps de base au cas où E est une algèbre de matrices et σ est alors de la forme $x \mapsto h \cdot {}^t x \cdot h^{-1}$ où h est une matrice symétrique ou antisymétrique. L'élément de k égal à 1 ou à -1 selon que $\dim E^\sigma = \frac{1}{2}n(n+1)$ ou $\frac{1}{2}n(n-1)$ sera appelé le *type* de σ. L'algèbre E possède en tout cas une involution de type 1. En effet elle possède au moins une involution de première espèce τ: $E \to E$ (cf. [1], p. 161, théorème 19), et si celle-ci n'est pas de type 1, il existe un élément h de la forme $e^\tau - e$ qui soit inversible (si E est une algèbre de matrices, c'est facile à voir, sinon on se ramène à ce cas-là par extension du corps de base et par un argument de densité évident, utilisant le fait que k est infini); l'involution $x \mapsto h \cdot x^\tau \cdot h^{-1}$ est alors de type 1.

Une paire (B, π) formée d'un E-module à droite B isomorphe à E_d (on désigne ainsi l'algèbre E elle-même, avec sa structure de E-module à droite) et d'une application k-linéaire $\pi: B \to B$ sera appelée un *espace de formes bilinéaires* pour E s'il existe un générateur s de B et une involution σ: $E \to E$ de type 1 tels que

$$\pi(s\,e) = s\,e^\sigma \qquad (e \in E). \tag{1}$$

Il est clair *qu'une telle paire existe* (il suffit de prendre $B = E_d$ et $\pi = \sigma$). De plus *elle est unique à isomorphisme (non canonique) près*. En effet, soient (B, π) et (B', π') deux espaces de formes bilinéaires, et soient $s \in B$, $s' \in B'$, σ: $E \to E$, σ': $E \to E$ des générateurs de B et B' et des involutions de type 1 tels qu'on ait (1) et

$$\pi'(s'\,e) = s'\,e^{\sigma'} \qquad (e \in E). \tag{1'}$$

Les involutions σ et σ' étant de première espèce, $\sigma \circ \sigma'$ est un automorphisme intérieur de E (cf. [3], p. 111, corollaire), c'est-à-dire qu'il existe dans E un élément inversible h tel que

$$e^{\sigma'} = h \cdot e^\sigma \cdot h^{-1} \qquad (e \in E).$$

Exprimant que σ' est une involution, on voit que $g = h^\sigma h^{-1} \in k$. Mais $g^\sigma = g^{-1}$, donc $g^2 = 1$ et $g = \pm 1$. D'autre part, un simple calcul montre que l'espace des points fixes de σ' est

$$\{e \in E \mid e^\sigma = g\,e\} \cdot h^{-1}.$$

Cet espace devant avoir $\frac{1}{2}n(n+1)$ dimensions, il s'ensuit que $g=1$, d'où $h^\sigma = h$. Mais alors, l'application α: $B \to B'$ définie par $\alpha(se) = s'he$ est un isomorphisme de E-module tel que $\alpha \circ \pi = \pi' \circ \alpha$, ce qui établit notre assertion.

Les seuls automorphismes du E-module B compatibles avec π sont les homothéties (multiplications par les éléments de k), ainsi qu'on s'en convainc immédiatement en posant $B=E_d$ et $\pi=\sigma$. Nous pouvons résumer tout ceci de façon imagée en disant qu' *à l'algèbre E est associé «canoniquement à homothétie près» un espace de formes bilinéaires.* Ainsi, *l'espace projectif de B est canoniquement associé à E.*

Dans la suite, nous nous donnerons une fois pour toutes un espace de formes bilinéaires (B,π) pour E. Les éléments de B seront appelés *formes*. Le dual de l'espace B sera noté B' et nous désignerons par $\langle,\rangle: B'\times B\to k$ la forme bilinéaire canonique.

2.2. L'espace B a une structure naturelle de E^*-module à gauche définie par

(1) $$\pi(e^*\cdot b)=\pi(b)\cdot e\,.$$

Pour $e\in E$ et $b\in B$, nous poserons

(2) $$b^e=e^*\cdot b\cdot e\,.$$

Posons $S=\{b\in B\,|\,b=\pi(b)\}$, $A=\{b-\pi(b)\,|\,b\in B\}$, $Q=B/A$. Nous appellerons *formes symétriques* (resp. *alternées*; resp. *quadratiques*) les éléments de S (resp. A; resp. Q), *bilinéarisation* l'application β: $Q\to S$ définie par

(3) $$\beta(\bar q+A)=\bar q+\pi(\bar q)\qquad(\bar q\in B)$$

et *quadratisation* la projection canonique γ: $B\to Q$. La composée $\gamma\circ\beta$ est la multiplication par 2.

Pour tout $e\in E$, on a $A^e=A$, donc l'opération de E sur B définie par (2) induit une opération de E sur Q qui sera aussi notée exponentiellement: $(q,e)\mapsto q^e$.

Soit $b\in B$. Alors $\operatorname{Ann} b=\{e\in E\,|\,be=0\}$ est un idéal à droite de E. Si nr est sa dimension, $n-r$ est appelé le *rang* de b. La forme b est dite *non dégénérée* si $\operatorname{Ann} b=\{0\}$, c'est-à-dire si b est un générateur du E-module B. *A toute forme symétrique s non dégénérée, la relation* 2.1 (1) *associe une involution σ: $E\to E$ de type* 1.

Soit $q\in Q$. Un simple calcul montre que $\operatorname{Noy} q=\{e\in\operatorname{Ann}\beta(q)\,|\,q^e=0\}$ est un idéal à droite de E. Si nr et nr' sont les dimensions respectives de $\operatorname{Ann}\beta(q)$ et $\operatorname{Noy} q$, les différences $n-r'$ et $r-r'$ sont appelées respectivement le *rang* et le *défaut* de q. Nous écartant un tant soit peu de la terminologie reçue, nous dirons que la forme q est *non dégénérée* si $r'=0$ et $r\leqq 1$ (si car $k\neq 2$ ou si n est pair, cela signifie simplement que $\beta(q)$ est non dégénérée).

Un idéal à droite I de E est dit *totalement singulier* pour une forme $x\in B$ ou Q si $x^I=\{x^e\,|\,e\in I\}=\{0\}$.

Soit k' une extension du corps k. Pour $X=E, B, S, A$ ou Q, posons ${}_{k'}X=X\otimes_k k'$, et ${}_{k'}\pi=\pi\otimes\mathrm{id}$. Alors $({}_{k'}B, {}_{k'}\pi)$ est un espace de formes bilinéaires pour ${}_{k'}E$ et les espaces de formes symétriques, alternées et quadratiques correspondants sont ${}_{k'}S$, ${}_{k'}A$ et ${}_{k'}Q$ (moyennant identifications canoniques). Si $x\in X=E, B$ etc., le point $x\otimes 1$ de ${}_{k'}X$ sera noté ${}_{k'}x$; cependant, lorsqu'aucune confusion ne sera à craindre, nous omettrons l'indice k' de cette notation, identifiant ainsi X à une partie de ${}_{k'}X$.

2.3. Soit D une k-algèbre à division de centre k, de dimension finie d^2, isomorphe à son opposée. Soient $\delta: D\to D$ une involution de première espèce de type $\varepsilon=\pm 1$, V un espace vectoriel à droite de dimension m sur D, End V l'algèbre des endomorphismes de V (opérant à gauche sur V), Sesq ${}_\delta V$ l'espace des formes sesquilinéaires relatives à δ, c'est-à-dire des applications biadditives b: $V\times V\to D$ telles que

$$(1)\qquad b(x\,d, y\,d')=d^\delta\cdot b(x,y)\cdot d' \qquad (x,y\in V;\ d,d'\in D),$$

et $\pi_{V,\delta}$: Sesq ${}_\delta V\to$ Sesq ${}_\delta V$ l'application définie par

$$(2)\qquad (\pi_{V,\delta}(b))(x,y)=\varepsilon\cdot b(y,x)^\delta \qquad (x,y\in V;\ b\in \mathrm{Sesq}\,{}_\delta V).$$

Alors (Sesq ${}_\delta V$, $\pi_{V,\delta}$) est un espace de formes bilinéaires pour End V pour la structure de module définie par

$$(3)\qquad (b\,e)(x,y)=b(x,e\,y) \qquad (x,y\in V;\ e\in \mathrm{End}\,V;\ b\in\mathrm{Sesq}\,{}_\delta V).$$

Si $D=k$, d'où $\delta=\mathrm{id.}$, on posera Sesq ${}_\delta V=$ Bil V et $\pi_{V,\delta}=\pi_V$. De plus, nous identifierons toujours le dual de Bil V avec $V\otimes V$ à l'aide de la forme bilinéaire $\langle , \rangle$ définie par

$$(4)\qquad \langle x\otimes y, b\rangle=b(x,y) \qquad (x,y\in V;\ b\in\mathrm{Bil}\,V).$$

Supposons que E soit une algèbre de matrices sur D et que $n=md$. Alors il existe des isomorphismes $\lambda: E\to$ End V et $\mu: B\to$ Sesq ${}_\delta V$ compatibles avec les structures envisagées. Notons que l'espace V est associé à $(E, D, \delta; B, \pi)$ «canoniquement au signe près», c'est-à-dire que les seuls automorphismes de V compatibles avec λ, μ *i.e.* induisant l'identité sur End V et Sesq ${}_\delta V$) sont les homothéties de rapports 1 et -1.

Dans la suite de ce numéro, nous supposons que $E=$ End V, $B=$ $=$ Sesq ${}_\delta V$ et $\pi=\pi_{V,\delta}$.

Si $\varepsilon=1$, les formes symétriques (resp. alternées) sont les formes sesquilinéaires hermitiennes (resp. antihermitiennes si car $k\neq 2$ et hermitiennes traciques [6] si car $k=2$). Si $\varepsilon\neq 1$ (d'où $\varepsilon=-1$), les formes symétriques (resp. alternées) sont les formes sesquilinéaires antihermitiennes (resp. hermitiennes).

Posons $D_1 = \{d - \varepsilon\, d^\delta \mid d \in D\}$. A toute forme quadratique $q = \bar{q} + A$ nous pouvons associer une fonction $\varphi(q)\colon V \to D/D_1$ définie par

(5) $$\varphi(q)(x) = \bar{q}(x, x) + D_1.$$

Cette représentation de Q comme espace de fonctions est fidèle. En effet, soit $q = \bar{q} + A \in Q$ telle que $\varphi(q) = 0$. Pour tous $x, y \in V$, on a

$$\begin{aligned}\bar{q}(x, y) &= \bar{q}(x+y, x+y) - \bar{q}(x, x) - \bar{q}(y, y) - \bar{q}(y, x) \equiv \\ &\equiv -\bar{q}(y, x) \equiv -\varepsilon\, \bar{q}(y, x)^\delta \qquad (\operatorname{mod} D_1),\end{aligned}$$

d'où, en remplaçant y par yd pour $d \in D$,

$$\bar{q}(x, y) \cdot d \equiv -\varepsilon \cdot \bar{q}(y, x)^\delta \cdot d \qquad (\operatorname{mod} D_1).$$

Autrement dit, l'idéal à droite de D engendré par $\bar{q}(x, y) + \varepsilon \cdot \bar{q}(y, x)^\delta = \beta(q)\,(x, y)$ est contenu dans D_1, donc est nul puisque $D_1 \neq D$. De sorte que $\beta(q) = 0$. Considérons à présent une base $(\boldsymbol{v}_i)$ de V, posons pour tout i

$$\bar{q}(\boldsymbol{v}_i, \boldsymbol{v}_i) = d_i - \varepsilon\, d_i^\delta \qquad (d_i \in D)$$

et soit $b \in B$ défini par

$$b(\boldsymbol{v}_i, \boldsymbol{v}_j) = \begin{cases} d_i & \text{si } i = j, \\ \bar{q}(\boldsymbol{v}_i, \boldsymbol{v}_j) & \text{si } i < j, \\ 0 & \text{si } i > j. \end{cases}$$

On a alors $\bar{q} = b - \pi(b)$, d'où $q = 0$.

Si $D = k$, on a $D_1 = \{0\}$ d'où $D/D_1 = k$, et l'application φ met en correspondance bijective l'espace Q et l'espace des formes quadratiques sur V au sens usuel.

Supposons que D soit une algèbre de quaternions et que $\varepsilon = -1$ ($= 1$ si car $k = 2$), de sorte que $D_1 = k$. Dans ce cas, les fonctions $V \to D$ dont la composée avec la projection canonique $D \to D/D_1$ appartient à $\varphi(Q)$ ne sont autres que les «formes quadratiques quaternioniennes» de E. A. M. Seip-Hornix [10]. On constatera que dans [10], deux formes quadratiques ne se distinguent «pratiquement pas» si elles ne diffèrent que par une fonction à valeurs dans k.

Soit V_1 un sous-espace de V. On définit de façon évidente la restriction à V_1 d'une forme $x \in B$ ou Q.

L'espace V_1 est *totalement singulier* pour x si cette restriction est nulle; cela revient à dire que l'idéal à droite $I = \{e \in E \mid e\,V \subset V_1\}$ est totalement singulier pour x, au sens du n° 2.2.

Les propositions 1 et 2 généralisent (à peine) des propriétés bien connues (voir par ex. [6]).

Proposition 1. *Tous les espaces totalement singuliers maximaux pour une forme symétrique, alternée ou quadratique donnée ont même dimension.*

En effet, soit b la forme en question ou sa bilinéarisée (cf. 2.2 (3)) selon qu'il s'agit d'une forme bilinéaire (symétrique ou alternée) ou d'une forme quadratique, soient V_1 et V_1' deux espaces totalement singuliers tels que $\dim V_1 < \dim V_1'$ et soit (v_i) $(i=1, \ldots, \dim V_1)$ une base de V_1. Pour des raisons de dimension, l'intersection X des noyaux des restrictions à V_1' des formes linéaires $x \mapsto b(v_i, x)$ n'est pas réduite à $\{0\}$, et l'espace $V_1 + X$ est totalement singulier de dimension strictement plus grande que $\dim V_1$.

La dimension commune des espaces totalement singuliers maximaux d'une forme symétrique, alternée ou quadratique est *l'indice de Witt* de celle-ci.

Nous laissons au lecteur le soin de démontrer la proposition suivante (qui ne sera pas utilisée dans la suite) en s'inspirant des indications données dans [6] (pp. 21, 22 et 36).

Proposition 2. *Soit x une forme alternée non dégénérée ou une forme quadratique dont la bilinéarisée $\beta(x)$ est non dégénérée, soient V_1 et V_1' deux sous-espaces de V et soit $f\colon V_1 \to V_1'$ une application linéaire bijective «transformant la restriction de x à V_1 en la restriction de x à V_1'». Alors, f se prolonge en un automorphisme e de V conservant x (i.e. tel que $x^e = x$).*

Remarquons que ceci n'est en général pas vrai pour une forme symétrique (même non dégénérée) lorsque $\operatorname{car} k = 2$.

2.4. Soit donnée une forme symétrique non dégénérée $s \in S$ et soit $\sigma\colon E \to E$ l'involution qui lui est associée par 2.1 (1). Il est souvent commode d'identifier E^* et B à E par les bijections

$$e^* \mapsto e^\sigma, \qquad b = s\,e \mapsto e. \tag{1}$$

L'application π s'identifie alors avec σ. L'existence dans E de la forme bilinéaire non dégénérée distinguée $(x, y) \mapsto \operatorname{Trd}(xy)$, où Trd désigne la trace réduite [3], permet d'autre part d'identifier E à son dual E', donc aussi, moyennant les identifications (1), au dual B' de B, ce qui se traduit par l'«identité»

$$\langle b', b\rangle = \operatorname{Trd}(b'\,b). \tag{2}$$

Supposons en particulier que $E = \operatorname{End} V$ et $B = \operatorname{Bil} V$, d'où $B' = V \otimes V$ selon 2.3 (4). Moyennant le choix d'une base (v_i) $(i=1, \ldots, n)$ dans V, nous pouvons identifier V à l'espace des matrices à n lignes et une colonne et E à l'algèbre $M_n(k)$ des matrices carrées d'ordre n de telle façon que l'opération (à gauche) de E sur V soit donnée par le produit ordinaire des matrices. Si nous prenons alors pour s la forme définie par

(3) $$s(\boldsymbol{v}_i, \boldsymbol{v}_j) = \delta_{ij} \qquad \text{(symbole de Kronecker)},$$

l'involution σ devient la transposition $m \mapsto {}^t m$ et les éléments $e^* \in E^*$, $b \in B$ et $b' \in B'$ correspondant selon les identifications décrites plus haut à la matrice $m = ((m_{ij})) \in E$ sont donnés par les relations

(4) $$e = {}^t m,$$

(5) $$b(x, y) = {}^t x\, m\, y$$

et

(6) $$b' = \sum_{i,j} m_{ij}\, \boldsymbol{v}_j \otimes \boldsymbol{v}_i .$$

En particulier, $x \otimes y \in B'$ est identifié à la matrice $y \cdot {}^t x$.

2.5. Nous introduirons à présent quatre applications bilinéaires $E \times B' \to B'$, $B' \times B \to E$, $B' \times E^* \to B'$ et $B \times B' \to E^*$ que nous appellerons simplement «produits», dont la valeur en une paire (x, y) sera notée $x \cdot y$ ou xy, et qui seront définies par les relations suivantes, où $e \in E$, $b \in B$ et $b' \in B'$:

(1) $$\langle e\, b', b \rangle = \mathrm{Trd}(b'\, b \cdot e) = \langle b', b\, e \rangle,$$

(2) $$\langle b'\, e^*, b \rangle = \mathrm{Trd}(e^* \cdot b\, b') = \langle b', e^*\, b \rangle .$$

Si, moyennant le choix d'une forme symétrique s non dégénérée, on identifie entre eux E, E^*, B et B' de la façon décrite au n° 2.4, tous ces produits viennent coïncider avec le produit ordinaire $E \times E \to E$. Dans la suite, nous ferons librement usage de diverses propriétés des produits en question qui résultent immédiatement de cette observation, par exemple:

i) du fait que les produits $E \times B' \to B'$ et $B' \times E^* \to B'$ font de B' un E-module à gauche et un E^*-module à droite;

ii) de relations d'associativité telles que

(3) $$(e\, b')(b\, e_1) = e \cdot (b'\, b) \cdot e_1 \qquad \text{pour } b \in B,\ b' \in B' \text{ et } e, e_1 \in E,$$

ou encore

(4) $$(b'\, b)\, b'_1 = b'(b\, b'_1) \qquad \text{pour } b \in B \text{ et } b', b'_1 \in B',$$

qui donne un sens à l'expression $b' b b'_1$, etc.;

iii) du fait que toute forme non dégénérée $b \in B$ possède dans B' une «inverse» b^{-1}, caractérisée par chacune des deux relations $b^{-1} \cdot b = 1$ et $b \cdot b^{-1} = 1^*$;

iv) de l'identité suivante, où s désigne comme précédemment une forme symétrique non dégénérée:

$$\langle s^{-1} \cdot s_1 \cdot s^{-1}, a\rangle = 0 \qquad \text{pour } s_1 \in S \text{ et } a \in A \tag{5}$$

(si on pose $a = \pi(b) - b$, avec $b \in B$, les identifications du n° 2.4 transforment (5) en la relation

$$\operatorname{Trd}(s_1 b) = \operatorname{Trd}(s_1 b^\sigma)$$

qui résulte immédiatement de la commutativité de la trace et de son invariance par σ).

2.6. Pour terminer ce paragraphe de généralités, nous rassemblons, en vue d'applications ultérieures, quelques propriétés élémentaires des formes alternées. *Dans ce numéro, le nombre n est toujours supposé pair, et posé $= 2m$.*

Commençons par établir quelques conventions de langage qui auront cours dans la suite de l'article. Etant donné un k-polynôme (k-morphisme) p d'une espace vectoriel X sur k dans un autre Y (c'est-à-dire, étant donné un homomorphisme p^* du dual de Y dans l'algèbre symétrique du dual de X), nous désignerons par ce même symbole p les applications polynomiales $X \otimes k' \to Y \otimes k'$ associées à p pour toute extension k' de k. Par abus de notation, nous parlerons du «k-polynôme p: $X \to Y$». Le k-polynôme de degré n de E dans k dont la valeur pour un élément de $E \otimes \bar{k}$ est la norme réduite de cet élément [3] sera noté Nrd.

Proposition 3. *Soient $a, a' \in A$ deux formes alternées et supposons a non dégénérée. Alors, le polynôme caractéristique* $\operatorname{Nrd}(\lambda \cdot 1 - a^{-1} \cdot a')$ *de $a^{-1} \cdot a'$ est un carré parfait dans $k[\lambda]$.*

Si $E = \boldsymbol{M}_n(k)$, nous pouvons identifier B et B' à $\boldsymbol{M}_n(k)$ de telle façon que π soit la transposition (2.4). Alors

$$\operatorname{Nrd}(\lambda \cdot 1 - a^{-1} \cdot a') = \operatorname{Dét}(\lambda \cdot a - a') / \operatorname{Dét} a\,,$$

et notre assertion résulte d'une propriété bien connue des matrices alternées. Le cas général se ramène à celui-là par extension du corps de base; lorsque $\operatorname{car} k = 2$, l'extension en question doit être separable pour que la propriété à établir se conserve par descente.

Corollaire 1. *Etant donnée une forme alternée a non dégénérée, le k-polynôme v: $A \to k$ défini par $v(x) = \operatorname{Nrd}(a^{-1} \cdot x)$ pour $x \in A \otimes \bar{k}$, est un carré parfait dans l'algèbre $k[A]$ des k-polynômes sur A. En particulier,* $\operatorname{Nrd}(a^{-1} \cdot a') \in k^2$ *pour tout $a' \in A$.*

Il suffit d'appliquer la proposition précédente à $E \otimes K$, où K est une extension transcendante pure de degré suffisamment élevé de k, en prenant pour a' un point générique de A sur k.

Remarque 1. On peut établir directement le corollaire 1 en remarquant que, si $x \in {}_K A$ est un point générique de A sur k, l'intersection du centralisateur de $a^{-1} \cdot x$ avec $a^{-1} \cdot {}_K A$ est une sous-algèbre de ${}_K E$, et que le carré de la norme de $a^{-1} \cdot x$ dans cette sous-algèbre est égal à $\mathrm{Nrd}(a^{-1} \cdot x)$. La proposition 3 se déduit alors à son tour immédiatement du corollaire 1. Cette façon de procéder, moins rapide que celle adoptée plus haut, est par contre plus élémentaire en ce qu'elle ne fait pas intervenir l'existence d'une extension séparable de k déployant E.

On appelle *discriminant* d'une forme $b \in B$, et on note Dis b, la classe $\bmod k^{*2}$ de $(-1)^m \cdot \mathrm{Nrd}(a^{-1} \cdot b)$, où a désigne une forme alternée non dégénérée. C'est donc un élément de $k/k^{*2} = \{0\} \cup k^*/k^{*2}$, qui ne dépend pas du choix de a en vertu du corollaire 1. Le discriminant est toujours défini car il existe effectivement des formes alternées non dégénérées (rappelons que $n = 2m$): si $E \cong \boldsymbol{M}_n(k)$ c'est évident, sinon k est infini et on peut utiliser un argument de densité, l'ensemble des formes alternées non dégénérées étant un ouvert de Zariski de A.

Un sous-espace vectoriel H de A est appelé *sous-espace de Cartan* s'il existe une forme non dégénérée $a \in H$ telle que $a^{-1} \cdot H$ soit une sous-algèbre commutative séparable de dimension m de E; on remarquera que, pour toute forme non dégénérée $a' \in H$, on a alors $a'^{-1} \cdot H = a^{-1} \cdot H$. Si $b \in B$ est une forme non dégénérée, un sous-espace de Cartan $H \subset A$ est dit *b-orthogonal* lorsque $b^{-1} \cdot H$ est une partie commutative de E. La proposition suivante éclaire la signification de ces définitions dans le cas des formes alternées usuelles.

Proposition 4. *Supposons que* $E = \mathrm{End}\, V$ *et* $B = \mathrm{Bil}\, V$, *où* V *est un espace vectoriel à* n *dimensions. Alors, pour toute décomposition*

$$V = \coprod_{j=1}^{m} V_j$$

de V *en somme directe d'espaces* V_j *à deux dimensions, l'espace*

$$\{a \in A \mid a(V_j, V_{j'}) = \{0\} \text{ pour } j \neq j'\} \tag{1}$$

est un sous-espace de Cartan de A. *Cet espace est b-orthogonal (pour* $b \in B$ *non dégénérée) si et seulement si* $b(V_j, V_{j'}) = \{0\}$ *pour* $j \neq j'$. *Si le corps* k *est algébriquement clos, tout sous-espace de Cartan de* A *est de la forme* (1) *pour une décomposition*

$$V = \coprod_{j=1}^{m} V_j \qquad (\dim V_j = 2)$$

convenable.

Soit

$$V=\coprod_{j=1}^{m} V_j \qquad \text{avec } \dim V_j=2.$$

Choisissons dans V une base $(\mathbf{v}_i)_{i=1,\dots,n}$ telle que $V_j=k\cdot \mathbf{v}_{2j-1}+k\cdot \mathbf{v}_{2j}$, et identifions E et B avec $\boldsymbol{M}_n(k)$ au moyen de cette base, selon le n° 2.4. La première assertion de l'énoncé résulte à présent d'un simple calcul.

Notons H l'espace (1), soit $a\in H$ une forme non dégénérée et, pour tout $j\in\{1,\dots,m\}$, soit e_j l'endomorphisme de V défini par

$$e_j\left(\sum_{j'=1}^{m} x_{j'}\right)=x_j \qquad \text{pour } x_{j'}\in V_{j'}.$$

Les e_j forment une base de $a^{-1}\cdot H$. Pour que H soit b-orthogonal, il faut et il suffit que $b^{-1}\cdot a$ commute avec $a^{-1}\cdot H$, donc avec chacun des e_j, donc que $(b^{-1}\cdot a)(V_j)=V_j$ pour tout j, d'où la deuxième assertion.

Supposons k algébriquement clos, désignons désormais par H un sous-espace de Cartan *quelconque* de A, soit $a\in H$ une forme non dégénérée, soient $X_j=k\cdot e_j$ $(j=1,\dots,m)$ les facteurs simples de l'algèbre $X=a^{-1}\cdot H$ et posons $V_j=e_j\,V$, de sorte que

$$V=\coprod_{j=1}^{m} V_j.$$

Vu la proposition 3, les valeurs propres d'un élément générique de X sont de multiplicité paire, par conséquent $\dim V_j=2$. Pour tout $a'\in H$ on a $a'\,e_j\in H$ de sorte que, pour $j'\neq j$,

$$\begin{aligned} a'(V_j,V_{j'})&=a'(V_j,e_{j'}V)=(a'\,e_{j'})(V_j,V)=\\ &=(a'\,e_{j'})(V,V_j)=a'(V,e_{j'}V_j)=\{0\}. \end{aligned}$$

L'espace H est donc contenu dans l'espace (1), et il coïncide avec lui pour raison de dimension.

Proposition 5. *Pour toute forme symétrique $s\in S$ non dégénérée, il existe au moins un sous-espace de Cartan de A s-orthogonal. Toute forme alternée non dégénérée est contenue dans au moins un sous-espace de Cartan de A.*

Si E est une algèbre de matrices, c'est évident, vu la proposition 4. Sinon, k est infini et la proposition résulte aussitôt du

Lemme 1. *Soit $b\in A\cup S$ une forme non dégénérée, et soit $U\subset A\otimes\bar{k}$ défini comme suit:*

(i) *si* $\operatorname{car} k\neq 2$ *et $b\in S$, U est l'ensemble des $x\in A\otimes\bar{k}$ tels que le polynôme caractéristique* $\operatorname{Nrd}(\lambda\cdot 1-b^{-1}\cdot x)$ *ait n racines distinctes, deux à deux opposées;*

(ii) *si* car $k=2$ *ou* $b\in A$, *U est l'ensemble des* $x\in A\otimes\bar{k}$ *tels que* $\mathrm{Nrd}(\lambda\cdot 1-b^{-1}\cdot x)$ *ait m racines doubles distinctes.*

Alors U est un ouvert de Zariski non vide de $A\otimes\bar{k}$. *Si* $a\in A\cap U$, *l'ensemble*

$$\{x\in A\,|\,a\cdot b^{-1}\cdot x=x\cdot b^{-1}\cdot a\} \tag{2}$$

est un sous-espace de Cartan b-orthogonal de A.

Nous pouvons supposer $k=\bar{k}$, poser $E=\mathrm{End}\,V$ et $B=\mathrm{Bil}\,V$, et identifier E et B à $\boldsymbol{M}_n(k)$ moyennant choix d'une base $(\boldsymbol{v}_i)_{i=1,\ldots,n}$ dans V.

Si $b\in A$, le polynôme $\mathrm{Nrd}(\lambda\cdot 1-b^{-1}\cdot x)$ n'a, pour tout $x\in A$, que des racines de multiplicités paires (d'après la proposition 3) et l'assertion concernant U résulte alors de ce qu'il existe des x pour lesquels ce polynôme ait m racines doubles distinctes, ce qui se vérifie immédiatement en prenant pour $(\boldsymbol{v}_i)$ une base symplectique de b.

Si $b\notin A$ (d'où $b\in S$), nous pouvons choisir $(\boldsymbol{v}_i)$ de telle façon que b soit identifiée à la matrice unité et l'assertion concernant U exprime alors une propriété connue des matrices alternées.

Démontrons la seconde assertion. Soit $a\in U$ et soient V_j $(j=1,\ldots,m)$ les sous-espaces à deux dimensions de V, invariants par $b^{-1}\cdot a$, et tels que la restriction c_j de $b^{-1}\cdot a$ à V_j ait des valeurs propres opposées ou égales selon qu'on se trouve dans le cas (i) ou le cas (ii) de l'énoncé. Choisissons la base $(\boldsymbol{v}_i)$ de telle façon que $V_j=k\cdot\boldsymbol{v}_{2j-1}+k\cdot\boldsymbol{v}_{2j}$, et écrivons a et b sous forme de matrices carrées d'ordre m $((a_{jj'}))$ et $((b_{jj'}))$ dont les coefficients sont eux-mêmes des matrices d'ordre 2. Nous avons, pour tous $j,j'\in\{1,\ldots,m\}$,

$$a_{jj'}=b_{jj'}\cdot c_{j'}, \tag{3}$$

d'où

$$b_{jj'}\cdot c_{j'}=a_{jj'}=-{}^t a_{j'j}=-({}^t c_j\cdot{}^t b_{j'j})=\varepsilon\cdot{}^t c_j\cdot b_{jj'}, \tag{4}$$

où $\varepsilon=-1$ ou $+1$ selon qu'on se trouve dans le cas (i) ou le cas (ii) de l'énoncé. Si $j\neq j'$, les matrices $c_{j'}$ et ${}^t c_j$ n'ont pas de valeur propre commune et (4) implique que $b_{jj'}=0$. Vu (3), il s'ensuit que $a_{jj'}=0$. Il résulte à présent d'un calcul élémentaire que l'espace (2) de l'énoncé n'est autre que l'espace (1) de la proposition 4. Le lemme et la proposition 5 sont ainsi démontrés.

3. Formes des groupes symplectiques et orthogonaux

Dans cet article, l'expression *k-groupe (algébrique)* est synonyme de *schéma en groupe de type fini sur* Spec k. La composante connexe [5, fasc. 2a] d'un k-groupe G est notée G^0. Soient H, H' deux $\bar{k}$-groupes et soit $\alpha\colon H\to H'$ un $\bar{k}$-homomorphisme; un k-groupe (resp. un k-homomorphisme de groupes algébriques) est alors appelé une *k-forme* de H

(resp. de α) s'il devient isomorphe à H (resp. α) par extension du corps de base de k à $\bar{k}$. Pour toute k-algèbre X, nous désignerons par $GL(X)$, ou encore, s'il y a lieu de spécifier le corps de base, par ${}_kGL(X)$, le «groupe multiplicatif de X considéré comme groupe algébrique», c'est-à-dire le k-groupe algébrique ayant pour groupe de points à valeurs dans une k-algèbre Y le groupe des éléments inversibles de l'algèbre $X \otimes_k Y$.

Reprenons à présent les notations des n$^{\text{os}}$ 2.1 et 2.2. Pour $f \in A$ ou Q, nous désignerons par $SL(E)$, $U(f)$ et $SU(f)$ les k-sous-groupes algébriques de $GL(E)$ définis respectivement par les équations

$$\operatorname{Nrd} x = 1,$$

$$f^x = f,$$

$$\operatorname{Nrd} x = 1 \quad \text{et} \quad f^x = f,$$

où Nrd désigne, rappelons-le, le «polynôme norme réduite». Si k est algébriquement clos et si $a \in A$, $q \in Q$ sont des formes *non dégénérées* (cf. 2.2), nous poserons, par abus de notation, $GL(E) = {}_kGL_n$, $SL(E) = {}_kSL_n$, $U(a) = SU(a) = SU(a)^0 = {}_kSp_n$, $U(q) = {}_kO_n$, $SU(q) = {}_kSO_n$ et $SU(q)^0 = {}_kSO_n^0$ (on a toujours ${}_kSO_n = {}_kSO_n^0$ sauf si $\operatorname{car} k = 2$ et $n = 2m$, auquel cas ${}_kSO_n = {}_kO_n$), et nous appellerons *immersion standard* les inclusions ${}_kSp_n \to {}_kGL_n$, ${}_kO_n \to {}_kGL_n$ et ${}_kSO_n^0 \to {}_kGL_n$. Ces conventions se justifient par le fait que, dans le cas envisagé, les groupes $GL(E)$, $SL(E)$, $U(a) = SU(a)$, $U(q)$, $SU(q)$ et $SU(q)^0$ et les immersions en question ne dépendent pas, à isomorphisme près, de l'algèbre E et des formes a et q, mais seulement de n et du corps k. Il est clair que

Proposition 6. *Quels que soit le corps k, si $a \in A$ et $q \in Q$ désignent des formes non dégénérées, les groupes $U(a) = SU(a)$, $U(q)$ et $SU(q)^0$ sont des k-formes de ${}_{\bar{k}}Sp_n$, ${}_{\bar{k}}O_n$ et ${}_{\bar{k}}SO_n^0$ respectivement.*

Remarque 2. Il est bien connu (et aisément vérifiable) que les groupes ${}_kSp_n$ et ${}_{\bar{k}}SO_n$ sont *réduits* (au sens de la théorie des schémas); par conséquent, le groupe $SU(f)$, pour $f \in A$ ou Q non dégénérée, est absolument réduit (donc «défini sur k» dans la terminologie classique). En fait, le groupe $G = U(f)$ ou $SU(f)$ (donc aussi G^0) est absolument réduit quel que soit $f \in A$ ou Q, sauf dans les deux cas suivants:

car $k = 2$, $G = U(f)$ et f est une forme quadratique défective;

car $k = 2$, $G = SU(f)$ et f est une forme quadratique dégénérée et défective.

Pour établir ce résultat, on suppose k algébriquement clos (ce qui suffit manifestement) et on compare la dimension du groupe G et celle de son algèbre de Lie; ces dimensions se calculent aisément, par exemple en réduisant f à une forme canonique.

Le théorème suivant complète les résultats obtenus par A. Weil [15]. Comme eux, il s'établit par une simple application des principes de la cohomologie galoisienne (voir aussi [11]), compte tenu du théorème de Grothendieck-Demasure [5, fasc. 6] d'après lequel tout groupe algébrique connexe semi-simple se déploie sur une extension séparable du corps de base.

Théorème 1. *Etant donnée une k-forme G de* $_{\bar{k}}Sp_n$ *(resp.* $_{\bar{k}}SO_n^0$*), il existe une algèbre centrale simple X sur k, isomorphe à son opposée, et une k-immersion* $\rho: G \to GL(X)$ *qui est une k-forme de l'immersion standard. L'algèbre X est unique à isomorphisme près. Si* $X = E$*, il existe une droite* $L \subset A$ *(resp. Q) et une seule telle que* $\rho(G) = SU(f)^0$ *pour tout* $f \in L - \{0\}$*. Les points de* $L - \{0\}$ *sont des formes non dégénérées.*

Remarque 3. Le fait qu'on n'ait pas dû exclure de cet énoncé les «formes trialitaires» des groupes de type D_4 résulte de ce que celles-ci sont nécessairement simplement connexes (formes de Spin_8) ou adjointes (formes de PSO_8^0). D'ailleurs, mises à part ces formes de D_4, le théorème précédent fournit aussi la description complète des groupes des types B_m, C_m et D_m car si G est un k-groupe connexe de type D_m $(m \neq 4)$ (resp. C_m; resp. B_m), il existe une forme H de SO_{2m}^0 (resp. Sp_{2m}; resp. SO_{2m+1}) telle que G soit isomorphe à H, à son revêtement universel $\tilde{H}$ ou au groupe adjoint correspondant $\bar{H}$ (resp. à H ou $\bar{H}$; resp. à H ou $\tilde{H}$).

4. Algèbre de Clifford, discriminant et pseudo-discriminant, groupe spinoriel

4.1. Les notations des n^{os} 2.1, 2.2 et 2.5 sont reprises. Notons Sand: $(B' \otimes B') \times B \to B'$ l'application bilinéaire définie par

$$\mathrm{Sand}(b' \otimes b_1', b) = b_1' \, b \, b'. \tag{1}$$

Etant donnée une forme quadratique $q = \bar{q} + A \in Q$, nous appellerons *algèbre de Clifford* de q et noterons $\mathrm{Cl}(q)$ le quotient de l'algèbre tensorielle $\mathcal{T}(B')$ de l'espace vectoriel B' par l'idéal I engendré par l'ensemble $I_1 \cup I_2$, où

$$I_1 = \{b' - \langle b', \bar{q} \rangle \cdot 1 \mid b' \in B' \text{ et } \langle b', A \rangle = \{0\}\},$$

$$I_2 = \{c - \mathrm{Sand}(c, \bar{q}) \mid c \in B' \otimes B' \text{ et } \mathrm{Sand}(c, A) = \{0\}\}.$$

Théorème 2. *La formation de l'algèbre* $\mathrm{Cl}(q)$ *est compatible avec une extension du corps de base, c'est-à-dire que si k' désigne une extension de k, on a* $\mathrm{Cl}(_{k'}q) = \mathrm{Cl}(q) \otimes_k k'$ *(pour la notation* $_{k'}q$*, cf. 2.2). Si* $E = \mathrm{End}\, V$ *et* $B = \mathrm{Bil}\, V$*, où V est un espace vectoriel sur k, de sorte que q est associée à* *une forme quadratique usuelle* $\varphi(q)$: $V \to k$ (cf. 2.3), *alors* $\mathrm{Cl}(q)$ *est canoniquement isomorphe à l'algèbre des éléments pairs de l'algèbre de Clifford usuelle de* $\varphi(q)$ [4].

Corollaire 2. *L'algèbre* $\mathrm{Cl}(q)$ *a* 2^{n-1} *dimensions. Supposons la forme* q *non dégénérée. Alors, si* n *est impair,* $\mathrm{Cl}(q)$ *est une algèbre simple de centre* k, *et si* n *est pair,* $\mathrm{Cl}(q)$ *est soit la somme directe de deux algèbres simples de dimension* 2^{n-2} *et de centre* k, *soit une algèbre simple dont le centre est une extension quadratique séparable de* k.

Une description «explicite» du centre de $\mathrm{Cl}(q)$ pour n pair sera donnée plus loin (n[os] 4.2 et 4.3).

La première assertion du théorème 2 résulte immédiatement du fait que les ensembles I_1 et I_2 sont des sous-espaces vectoriels de $\mathscr{T}(B')$.

Démontrons la seconde assertion. Pour simplifier, nous noterons simplement q la forme quadratique $\varphi(q)$, de sorte que $q(x)=\bar{q}(x, x)$ pour $x \in V$. L'espace B' étant identifié à $V \otimes V$ par 2.3(4), $\mathscr{T}(B')$ s'identifie à la sous-algèbre $\mathscr{T}^+(V)$ des éléments de degrés pairs de l'algèbre tensorielle de V. Soit $\mathscr{C}^+(q)$ l'algèbre des éléments pairs de l'algèbre de Clifford de q au sens usuel. Le noyau de l'application canonique $\mathscr{T}^+(V) \to \mathscr{C}^+(q)$ est l'idéal I' de $\mathscr{T}^+(V)$ engendré par l'ensemble $I_1' \cup I_2'$, où

$$I_1' = \{x \otimes x - q(x) \cdot 1 \mid x \in V\},$$

$$I_2' = \{x \otimes y \otimes y \otimes z - q(y) \cdot x \otimes z \mid x, y, z \in V\}.$$

En effet, il est clair que I' appartient au noyau en question et d'autre part, le raisonnement classique, fondé sur l'emploi d'une base de V, montre que l'algèbre $\mathscr{T}^+(V)/I'$ a bien la dimension voulue, 2^{n-1}. Le théorème sera démontré si nous prouvons que I_j $(j=1, 2)$ est l'espace vectoriel engendré par I_j', ce qui résultera aussitôt de l'identité

(2) $$\mathrm{Sand}\big((x \otimes y) \otimes (z \otimes t), b\big) = b(z, y) \cdot x \otimes t$$

pour $x, y, z, t \in V$ et $b \in B$, et des deux assertions suivantes:

(3) l'espace $\{b' \in B' \mid \langle b', A\rangle = \{0\}\}$ est engendré linéairement par l'ensemble $\{x \otimes x \mid x \in V\}$;

(4) l'espace $J = \{c \in B' \otimes B' \mid \mathrm{Sand}(c, A) = \{0\}\}$ est engendré linéairement par l'ensemble

$$J' = \{(x \otimes y) \otimes (y \otimes z) \mid x, y, z \in V\}.$$

Pour établir (2), (3), (4), le plus simple est sans doute de choisir une base $(\mathfrak{v}_i)$ $(i=1, \ldots, n)$ dans V et de procéder aux identifications du n^0 2.4.

La relation (2) est alors évidente. Pour prouver (3), il suffit de remarquer qu'une matrice b' vérifie la relation $\mathrm{Tr}(b' a)=0$ pour toute matrice a «alternée» (i. e. antisymétrique et n'ayant que des zéros sur la diagonale) si et seulement si b' est symétrique. Reste à prouver (4). Vu (2), il est clair que J contient J'. Réciproquement, soit

$$c=\sum_{h,i,j,l} c_{hijl}\,\boldsymbol{v}_h\otimes\boldsymbol{v}_i\otimes\boldsymbol{v}_j\otimes\boldsymbol{v}_l\in J.$$

Alors, pour toute matrice alternée $a=((a_{ij}))$, on a

$$\mathrm{Sand}(c,a)=\sum_{h,l}\Big(\sum_{i,j} c_{hijl}\,a_{ji}\Big)\boldsymbol{v}_h\otimes\boldsymbol{v}_l=0,$$

ce qui implique que $c_{hijl}=c_{hjil}$, donc que c est combinaison linéaire des éléments

$$\boldsymbol{v}_h\otimes(\boldsymbol{v}_i\otimes\boldsymbol{v}_j+\boldsymbol{v}_j\otimes\boldsymbol{v}_i)\otimes\boldsymbol{v}_l \qquad (h,i,j,l=1,2,\ldots,n)$$

et

$$\boldsymbol{v}_h\otimes\boldsymbol{v}_i\otimes\boldsymbol{v}_i\otimes\boldsymbol{v}_l \qquad (h,i,l=1,2,\ldots,n),$$

d'où (3). Le théorème est démontré.

4.2. *Dans ce numéro et le suivant, le nombre n est supposé pair et posé $=2m$.*

Les foncteurs «algèbre symétrique» et «m-ième puissance symétrique» sont respectivement notés $\mathscr{S}$ et $\mathscr{S}_m$.

Soit H un sous-espace de Cartan de l'espace A des formes alternées (2.6). Il résulte de la proposition 4 que l'espace $\overline{H}=H\otimes\bar{k}$ se décompose de façon unique en une somme directe

$$\coprod_{j=1}^{m}\overline{H}_j$$

de sous-espaces de dimension 1 dont les éléments non nuls sont des formes de rang 2. Cela étant, nous noterons δ_H le k-polynôme de H dans $\mathscr{S}_m H$ défini par

$$\delta_H\Big(\sum_{j=1}^{m} h_j\Big)=\prod_{j=1}^{m} h_j \qquad \text{pour } h_j\in\overline{H}_j. \tag{1}$$

Un raisonnement standard de descente galoisienne montre que δ_H est bien «défini sur k», mais on peut aussi arriver à ce resultat par les considérations suivantes, qui fournissent une définition «rationnelle» de δ_H. Soit U l'ensemble des formes non singulières contenues dans H et soit H' le sous-espace linéaire de B' engendré par U^{-1}. Posons $X=H'\cdot H$ $(=a^{-1}\cdot H$ pour tout $a\in U)$. Notons N_X et T_X le «polynôme norme» et le «polynôme trace» de l'algèbre X. L'espace H' s'identifie canoniquement au dual de H par la forme bilinéaire $(h', h) \mapsto T_X(h' h)$. Le k-polynôme

$$(h', h) \mapsto N_X(h' h) \qquad (h' \in H' \otimes \bar{k},\ h \in H \otimes \bar{k})$$

de $H' \times H$ dans k est homogène de degré m «en chacune des variables h', h». Il y correspond donc, de façon évidente, un polynôme de degré m de H dans l'espace des k-polynômes homogènes de degré m sur H', lequel espace s'identifie canoniquement avec $\mathscr{S}_m H$. Le polynôme $H \to \mathscr{S}_m H$ ainsi défini n'est autre que δ_H. (Ces diverses affirmations doivent seulement être vérifiées lorsque $k = \bar{k}$, auquel cas elles résultent de calculs immédiats, compte tenu de la proposition 4.)

Théorème 3. *On suppose la caractéristique de k différente de 2. Soient $q \in Q$ une forme quadratique non dégénérée, $s = \beta(q)$ la forme symétrique correspondante et $H \subset A$ un sous-espace de Cartan s-orthogonal de A* (2.6). *Alors, l'image canonique de $\mathscr{T}(s^{-1} H s^{-1}) \subset \mathscr{T}(B')$ dans* $\mathrm{Cl}(q)$ *est une sous-algèbre commutative séparable maximale de* $\mathrm{Cl}(q)$. *En particulier, l'application canonique $\mathscr{T}(s^{-1} H s^{-1}) \to \mathrm{Cl}(q)$ est composée de l'application canonique $\mathscr{T}(s^{-1} H s^{-1}) \to \mathscr{S}(s^{-1} H s^{-1})$ et d'une application η: $\mathscr{S}(s^{-1} H s^{-1}) \to \mathrm{Cl}(q)$. Soit ζ_H: $H \to \mathrm{Cl}(q)$ le composé du polynôme δ_H: $H \to \mathscr{S}_m H$, de l'application linéaire $\mathscr{S}_m H \to \mathscr{S}_m(s^{-1} H s^{-1})$ induite par $h \mapsto s^{-1} h s^{-1}$ (pour $h \in H$) et de l'application η. Alors, $k \cdot \zeta_H(H)$ est une droite distincte de $k \cdot 1$, l'espace $k \cdot \zeta_H(H) + k \cdot 1$ est le centre de* $\mathrm{Cl}(q)$, *et on a, pour tout $h \in H$,*

$$(\zeta_H(h))^2 = (-1)^m \cdot \mathrm{Nrd}(s^{-1} \cdot h) \cdot 1. \tag{2}$$

Vu la proposition 5 (n° 2.6), on en déduit assitôt le

Corollaire 3. *Soit* $\operatorname{car} k \neq 2$, *soit $q \in Q$ une forme quadratique non dégénérée, et soit d un représentant du discriminant* $\mathrm{Dis}\, s$ *de $s = \beta(q)$ dans k^** (2.6). *Alors, le centre de* $\mathrm{Cl}(q)$ *est isomorphe à $k[x]/(x^2 - d)$. En particulier,* $\mathrm{Cl}(q)$ *se décompose en une somme de deux algèbres simples si et seulement si* $\mathrm{Dis}\, s = 1$.

Démontrons le théorème 3 en supposant pour commencer que $k = \bar{k}$, et que $E = \mathrm{End}\, V$, $B = \mathrm{Bil}\, V$ et $B' = V \otimes V$, où V est un espace vectoriel à n dimensions. Soient V_j ($j = 1, \ldots, m$) les sous-espaces à deux dimensions de V tels que H soit l'espace (1) de la proposition 4 (n° 2.6). Choisissons dans V une base $(\mathbf{v}_i)_{i=1,\ldots,n}$ telle que

$$s(\mathbf{v}_i, \mathbf{v}_{i'}) = \delta_{i i'} \qquad \text{(symbole de KRONECKER)} \tag{3}$$

et que

$$V_j = k \cdot \mathbf{v}_{2j-1} + k \cdot \mathbf{v}_{2j} \qquad \text{pour } j = 1, \ldots, m,$$

ce qui est possible vu la proposition 4 et le fait que l'espace H a été supposé s-orthogonal. Soit h_j l'unique élément de H tel que

$$h_j(\boldsymbol{v}_{2j'-1}, \boldsymbol{v}_{2j'}) = \delta_{jj'} \qquad \text{(symbole de Kronecker)}.$$

Il résulte d'un calcul élémentaire, et pratiquement immédiat lorsqu'on identifie E, B, B' avec $\boldsymbol{M}_n(k)$ selon le n° 2.4, que

$$s^{-1} h_j s^{-1} = \boldsymbol{v}_{2j} \otimes \boldsymbol{v}_{2j-1} - \boldsymbol{v}_{2j-1} \otimes \boldsymbol{v}_{2j}. \tag{4}$$

Identifions $\mathrm{Cl}(q)$ et V avec leurs images canoniques dans l'algèbre de Clifford usuelle C de la forme quadratique $\varphi(q)$ (cf. 2.3 et le théorème 2). L'image canonique de $s^{-1} h_j s^{-1}$ dans C est alors, vu (3) et (4),

$$z_j = \boldsymbol{v}_{2j} \boldsymbol{v}_{2j-1} - \boldsymbol{v}_{2j-1} \boldsymbol{v}_{2j} = 2\boldsymbol{v}_{2j} \boldsymbol{v}_{2j-1}. \tag{5}$$

On note que, pour $j, j' \in \{1, \ldots, m\}$,

$$z_j z_{j'} = z_{j'} z_j \tag{6}$$

et

$$z_j^2 = -1. \tag{7}$$

L'image canonique U de $\mathscr{T}(s^{-1} Y s^{-1})$ dans $\mathrm{Cl}(q)$ étant engendrée par les z_j, on déduit de (5), (6), (7) et des propriétés connues de l'algèbre de Clifford C que l'application produit induit un isomorphisme d'algèbre du produit tensoriel des algèbres $k \cdot z_j + k \cdot 1 \cong k \otimes k$ sur l'algèbre U. Celle-ci est donc une algèbre commutative séparable de dimension 2^m, ce qui établit notre première assertion.

Soit

$$h = \sum_{j=1}^{m} c_j h_j$$

un élément quelconque de H. Utilisant par exemple les identifications du n° 2.4, on voit que $s^{-1} h$ est l'endomorphisme de V défini par

$$\boldsymbol{v}_{2j-1} \mapsto -c_j \boldsymbol{v}_{2j}, \qquad \boldsymbol{v}_{2j} \mapsto c_j \boldsymbol{v}_{2j-1},$$

de sorte que

$$\mathrm{Nrd}(s^{-1} h) = \prod_{j=1}^{m} c_j^2.$$

Mais

$$\delta_H(h) = \prod_{j=1}^{m} c_j \cdot \prod_{j=1}^{m} h_j$$

donc

$$\zeta_H(h) = \prod_{j=1}^{m} c_j \cdot \prod_{j=1}^{m} z_j.$$

La relation (2) en résulte, vu (6) et (7). D'autre part, il est bien connu que le produit

$$z=\prod_{j=1}^{m} z_j=(-2)^m\cdot\prod_{i=1}^{n} \boldsymbol{v}_i$$

appartient au centre Z de $\mathrm{Cl}(q)=C^+$ et que $Z=k\cdot z+k\cdot 1$.

Le théorème 3 est ainsi établi dans le cas où $k=\bar{k}$. Pour passer au cas général, il suffit d'observer que toutes les assertions de l'énoncé se conservent par descente du corps de base, à ceci près toutefois que l'inclusion

$$(k\cdot\zeta_H(H))\otimes\bar{k}\subset\zeta_H(H\otimes\bar{k})$$

pourrait *a priori* être stricte. Mais comme $\zeta_H(H\otimes\bar{k})$ est un espace de dimension 1, cela voudrait dire que $\zeta_H(H)=\{0\}$, ou encore, vu la relation (2) déjà établie, que H ne contiendrait que des formes dégénérées, ce qui est absurde. Ceci achève la démonstration.

Remarque 4. Examinons brièvement ce qu'il advient du théorème 3 lorsque car $k=2$. Dans ce cas, $H\subset S$, de sorte que l'image canonique de $\mathscr{T}(s^{-1}Hs^{-1})$ dans $\mathrm{Cl}(q)$ est contenue dans $k\cdot 1$; il résulte en effet de la formule 2.5 (5) et de la définition de $\mathrm{Cl}(q)$ que l'image canonique de $\mathscr{T}(s^{-1}Ss^{-1})$ dans $\mathrm{Cl}(q)$ est $k\cdot 1$ (ceci en toute caractéristique d'ailleurs). On peut donc, comme dans l'énoncé du théorème 3, définir l'application η et le polynôme ζ_H. A présent, $k\cdot\zeta_H(H)=k\cdot 1$, de sorte que $k\cdot\zeta_H(H)+k\cdot 1$ n'est plus le centre de $\mathrm{Cl}(q)$. Par contre, la formule (2) reste valable. Elle se démontre de la même façon qu'en caractéristique $\neq 2$ à ceci près qu'on doit choisir pour $(\boldsymbol{v}_i)$ non plus une base orthogonale pour s, une telle base n'existant pas, mais par exemple une base symplectique. La modification essentielle qui intervient dans les calculs est que, cette fois, l'image canonique de $s^{-1}h_j s^{-1}$ dans C est égale à 1.

Remarque 5. Il existe un k-polynôme $\zeta\colon A\to\mathrm{Cl}(q)$ dont la restriction à tout sous-espace de Cartan H de A est ζ_H. Pour le voir, on considère un point générique $a\in A\otimes K$ de A sur k, où K désigne une extension transcendante pure de k, et on définit ζ par la relation $\zeta(a)=\zeta_{H_a}(a)$, où $H_a=\{x\in A\otimes K\,|\,a\cdot s^{-1}\cdot x=x\cdot s^{-1}\cdot a\}$ (cf. 2.6, lemme 1). La formule (2) peut s'écrire

$$(2')\qquad \zeta(a)^2=\mathrm{Nrd}(s^{-1}a)\cdot 1\qquad\text{pour } a\in A.$$

Lorsque car $k=2$, le polynôme ζ est à valeurs dans $k\cdot 1$ et (2′) est une nouvelle preuve du corollaire 1 du n° 2.6.

4.3. *Rappelons que* $n=2m$.

Théorème 4. *Soit k de caractéristique 2. Soient $q=\bar{q}+A\in Q$ une forme quadratique non dégénérée, $s=\beta(q)$ la forme symétrique correspon-*

dante et z l'image canonique de $s^{-1}\cdot\bar{q}\cdot s^{-1}\in B'$ *dans* $\mathrm{Cl}(q)$. *Pour* $e\in E$, *notons* $T_2(e)$ *le coefficient de* λ^{n-2} *dans le polynôme caractéristique* $\mathrm{Nrd}(e+\lambda\cdot 1)$. *Alors,* $z\notin k\cdot 1$, *le centre de* $\mathrm{Cl}(q)$ *est* $k\cdot z+k\cdot 1$, *et on a*

$$z^2+z=\left(T_2(s^{-1}\cdot\bar{q})+\binom{m}{2}\right)\cdot 1, \tag{1}$$

où

$$\binom{m}{2}=\tfrac{1}{2}m(m-1).$$

Soit $\bar{q}'=\bar{q}+a$ un autre représentant de q dans B et soit z' l'image canonique de $s^{-1}\cdot\bar{q}'\cdot s^{-1}$ dans $\mathrm{Cl}(q)$. Vu la relation 2.5 (5), l'élément

$$s^{-1}\cdot\bar{q}'\cdot s^{-1}+s^{-1}\cdot\bar{q}\cdot s^{-1}+\langle s^{-1}\cdot a\cdot s^{-1},\bar{q}\rangle\cdot 1$$

de B' appartient à l'ensemble I_1 du n° 4.1, de sorte qu'on a, dans $\mathrm{Cl}(q)$,

$$z'=z+\langle s^{-1}\cdot a\cdot s^{-1},\bar{q}\rangle\cdot 1.$$

Il résulte alors de la relation (1) que

Corollaire 4. *Si* Δ *désigne le quotient du groupe additif de* k *par le sous-groupe* $\{x^2+x\mid x\in k\}$, *l'image canonique de* $T_2(s^{-1}\cdot\bar{q})$ *dans* Δ *dépend seulement de* q *et non du représentant* $\bar{q}$ *choisi.*

L'image de

$$T_2(s^{-1}\cdot\bar{q})+\binom{m}{2}\cdot 1$$

dans Δ est appelée le *pseudo-discriminant* ou *invariant d'Arf* de la forme quadratique q, et noté $\mathrm{Arf}\, q$.

Corollaire 5. *Soit* d *un représentant de* $\mathrm{Arf}\, q$ *dans* k. *Alors, le centre de* $\mathrm{Cl}(q)$ *est isomorphe à* $k[x]/(x^2+x+d)$. *En particulier,* $\mathrm{Cl}(q)$ *se décompose en un produit de deux algèbres simples si et seulement si* $\mathrm{Arf}\, q=0$.

Démontrons le théorème 4. Quitte à étendre le corps de base, nous pouvons supposer que celui-ci est algébriquement clos, et que $E=\mathrm{End}\, V$, $B=\mathrm{Bil}\, V$ et $B'=V\otimes V$, où V est un espace vectoriel à n dimensions. Choisissons dans V une base $(\boldsymbol{v}_i)_{i=1,\dots,n}$ telle qu'on ait, avec les notations du n° 2.3,

$$\varphi(q)(\boldsymbol{v}_i)=0 \qquad \text{pour } i\in\{1,\dots,n\}, \tag{2}$$

et

$$s(\boldsymbol{v}_i,\boldsymbol{v}_{i'})=\begin{cases}1 & \text{si } (i,i')=(2j-1,2j) \text{ ou } (2j,2j-1)\\ 0 & \text{dans les autres cas}.\end{cases} \tag{3}$$

Faisant usage de cette base, nous pouvons, selon le n° 2.4, identifier E, B et B' à $\boldsymbol{M}_n(k)$. Identifions aussi $\mathrm{Cl}(q)$ et V à leurs images canoniques dans l'algèbre de Clifford usuelle C de la forme quadratique $\varphi(q)$. Notons $s_{i\,i'}$, $\bar{q}_{i\,i'}$, et $z_{i\,i'}$ les coefficients des matrices s, $\bar{q}$ et $s^{-1}\,\bar{q}\,s^{-1}$ respectivement. On a, pour $i, i' \in \{1, \dots, n\}$,

$$\bar{q}_{i\,i'} + \bar{q}_{i'\,i} = s_{i\,i'} = s(\boldsymbol{v}_i, \boldsymbol{v}_{i'}), \tag{4}$$

et aussi, vu (2),

$$\bar{q}_{i\,i} = 0. \tag{5}$$

L'image canonique de $s^{-1}\,\bar{q}\,s^{-1}$ dans $\mathrm{Cl}(q)$ est

$$z = \sum_{i, i'=1}^{n} z_{i\,i'}\,\boldsymbol{v}_{i'} \cdot \boldsymbol{v}_i = \sum_{i<i'} (z_{i\,i'} + z_{i'\,i})\,\boldsymbol{v}_i \cdot \boldsymbol{v}_{i'} + \sum_{i<i'} z_{i\,i'} \cdot s_{i\,i'} \cdot 1,$$

d'où, en remplaçant les $z_{i\,i'}$ par leurs valeurs en fonction des $\bar{q}_{i\,i'}$, et tenant compte de (3),

$$z = z' + \left(\sum_{j=1}^{m} \bar{q}_{2j,\,2j-1} \right) \cdot 1, \tag{6}$$

où on a posé

$$z' = \sum_{j=1}^{m} \boldsymbol{v}_{2j-1} \cdot \boldsymbol{v}_{2j}.$$

Le fait que $k \cdot z + k \cdot 1$ est le centre de $\mathrm{Cl}(q)$ résulte à présent de [9] (cf. notamment *d*). (Une alternative à la démonstration de [9] consiste à montrer que z' est central dans $\mathrm{Cl}(q)$ — il suffit de montrer qu'il commute avec tous les produits $\boldsymbol{v}_i \cdot \boldsymbol{v}_{i'}$ — et à utiliser le fait, établi *a priori* dans [4], que le centre de $\mathrm{Cl}(q)$ est bidimensionnel.)

Il est facile de calculer $T_2(s^{-1}\,\bar{q})$ en fonction des $\bar{q}_{i\,i'}$, par la formule bien connue

$$T_2(((e_{i\,i'}))) = \sum_{i<i'} (e_{i\,i}\,e_{i'\,i'} - e_{i\,i'}\,e_{i'\,i}).$$

On trouve, toutes réductions faites et compte tenu de (3), (4) et (5), que

$$T_2(s^{-1}\,\bar{q}) = \sum_{j=1}^{m} (\bar{q}^2_{2j,\,2j-1} + \bar{q}_{2j,\,2j-1}) + \binom{m}{2} \cdot 1.$$

Vu (6), la relation (1) se ramène donc à

$$z'^2 = z',$$

dont la vérification est immédiate. Le théorème est ainsi démontré.

4.4. Pour terminer, nous donnerons encore quelques brèves indications sur les groupes spinoriels. Pour le détail des démonstrations, le lecteur pourra par exemple se reporter aux notes [13a] le jour où elles existeront.

Dans ce numéro, q désigne toujours une forme quadratique *non dégénérée*.

Soient X une k-algèbre commutative quelconque et x un point de $SU(q)^0_X$ (point de $SU(q)^0$ à valeurs dans X). Considérons l'application linéaire de $B' \otimes X$ dans lui-même définie par

$$b' \mapsto x\, b'\, x^*.$$

Elle induit un automorphisme de $\mathscr{T}(B') \otimes X$ dont on vérifie qu'il conserve le noyau de l'application canonique $\mathscr{T}(B') \otimes X \to \mathrm{Cl}(q) \otimes X$, et induit donc finalement un automorphisme

$$\alpha(x)\colon\ \mathrm{Cl}(q) \otimes X \to \mathrm{Cl}(q) \otimes X\,.$$

Nous avons ainsi défini un homomorphisme de groupes algébriques

$$\alpha\colon\ SU(q)^0 \to \mathrm{Aut}(\mathrm{Cl}(q)) \cong PGL(\mathrm{Cl}(q))\,.$$

Si $\mathrm{Spin}\, q$ désigne le revêtement universel de $SU(q)^0$ (cf. [13], n° 2.6.1), α se relève de façon unique en un homomorphisme

$$\tilde{\alpha}\colon\ \mathrm{Spin}\, q \to GL(\mathrm{Cl}(q))$$

qui est en fait une immersion, appelée *représentation spinorielle* de $\mathrm{Spin}\, q$.

Supposons $n=2m$. Si le centre Z de $\mathrm{Cl}(q)$ est isomorphe à $k \otimes k$ (i.e. si $\mathrm{Dis}\, q=1$ ou $\mathrm{Arf}\, q=0$ selon que car $k \neq 2$ ou $=2$), alors $\mathrm{Cl}(q)$ est somme directe de deux algèbres simples Cl_1 et Cl_2 et $\tilde{\alpha}$ est somme directe de deux représentations

$$\tilde{\alpha}_i\colon\ \mathrm{Spin}\, q \to GL\,(\mathrm{Cl}_i) \qquad (i=1,2)$$

appelées représentations *semi-spinorielles* de $\mathrm{Spin}\, q$.

Soient λ_0 et λ_i $(i=1,2)$ les poids dominants respectifs de la «représentation naturelle» $\mathrm{Spin}\, q \to GL(E)$ (composée de $\mathrm{Spin}\, q \to SU(q)^0 \to \to GL(E)$) et des représentations $\tilde{\alpha}_i$. Ces poids satisfont aux congruences suivantes modulo le groupe des poids de $\mathrm{Spin}\, q$ qui sont combinaisons linéaires de racines:

si m est pair, $2\lambda_1 \equiv 2\lambda_2 \equiv \lambda_1 + \lambda_2 + \lambda_0 \equiv 0$;

si m est impair, $\lambda_1 \equiv -\lambda_2,\ 2\lambda_1 \equiv 2\lambda_2 \equiv \lambda_0$.

Il résulte alors de théorèmes généraux sur les représentations linéaires des groupes semi-simples [13a] qu'on a la

Proposition 7. *Soit $n=2m$, supposons que $\mathrm{Cl}(q)$ soit la somme directe de deux algèbres simples Cl_1 et Cl_2 et soient $|\mathrm{Cl}_i|$ et $|E|$ les images respectives de Cl_i et E dans le groupe de Brauer. Alors*

si m est pair, $2|\mathrm{Cl}_1| = 2|\mathrm{Cl}_2| = |\mathrm{Cl}_1| + |\mathrm{Cl}_2| + |E| = 0$;

si m est impair, $2|\mathrm{Cl}_i| = |E|, \quad |\mathrm{Cl}_1| + |\mathrm{Cl}_2| = 0$.

Cette proposition peut évidemment aussi être démontrée directement, sans faire appel à la théorie des groupes algébriques. (On trouvera dans [7] une démonstration de la relations $|\mathrm{Cl}_1|+|\mathrm{Cl}_2|+|E|=0$ pour m pair, sous l'hypothèse que car $k \neq 2$.)

Enonçons encore la

Proposition 8. *Soit $n=2m$, et supposons l'indice de Witt de la forme q* (n° 2.3) *égal à m. Alors,* $\mathrm{Cl}(q)$ *est la somme directe de deux algèbres simples dont l'une est une algèbre de matrices (d'ordre 2^{m-1}) et l'autre a même image que E dans le groupe de Brauer**.

C'est une conséquence immédiate du corollaire 2, de la proposition 7 et du fait suivant: si I désigne un idéal à droite totalement singulier de E, de dimension $nm=2m^2$, alors la m-ième puissance symétrique de $IB'I^*(\subset B')$ a pour image canonique dans l'algèbre $\mathrm{Cl}(q)$ un sous-espace à une dimension $\rho(I)$, engendrant un idéal à gauche $\mathrm{Cl}(q)\cdot\rho(I)$ de dimension 2^{m-1}. Pour établir cette assertion, on peut évidemment supposer k algébriquement clos, auquel cas elle résulte d'une simple vérification, pratiquement faite dans [4] (p. 43).

Supposons $\mathrm{Cl}(q)=\mathrm{Cl}_1+\mathrm{Cl}_2$. Nous pouvons représenter Cl_i comme l'algèbre des endomorphismes d'un espace vectoriel W_i sur une algèbre à division. Si $|\mathrm{Cl}_i|=0$, l'espace W_i est un espace vectoriel sur k, dont les points sont appelés *semi-spineurs* de i-ième espèce.

Supposons en particulier la forme q d'indice de Witt m. A tout idéal à droite totalement singulier I de dimension nm de E, nous avons associé plus haut une droite $\rho(I)$ de $\mathrm{Cl}(q)$. Cette droite est contenue dans l'un des facteurs simples de $\mathrm{Cl}(q)$, soit Cl_i; l'espace W_i correspondant est un espace de semi-spineurs (i.e. $|\mathrm{Cl}_i|=0$), et $\overline{\omega}(I)=\rho(I)$. W_i est une droite de W_i. Un *semi-spineur* x est dit *pur* s'il existe un idéal I tel que $x\in\overline{\omega}(I)$.

Pour une étude détaillée de ces questions dans le cas où E est une algèbre de matrices sur une algèbre de quaternions, voir [14] (dont la terminologie est toutefois un peu différente de la nôtre).

* *Note ajoutée aux épreuves.* Ce résultat a été obtenu indépendamment par D.C. van Drooge et (pour car $k \neq 2$) par H.P. Allen. Sous l'hypothèse car $k \neq 2$, elle est déjà annoncée dans les propositions («Stellingen») annexées à [14] (Stelling IV).

Bibliographie

1. Albert, A.A.: Structure of algebras. A.M.S. Colloquium Publications, vol. 24, 1939.
2. Borel, A., et J. Tits: Groupes réductifs. Publ. Math. I.H.E.S. **27**, 55—151 (1965).
3. Bourbaki, N.: Algèbre, chap. 8: Modules et anneaux semi-simples. Actu. Sci. et Ind., No. 1261. Paris: Hermann 1958.
4. Chevalley, C.: The algebraic theory of spinors. New York: Columbia U. Press 1954.

5. Demazure, M., et A. Grothendieck: Schémas en groupes. Séminaire de Géom. Alg., I.H.E.S., Paris, 1963/64.
6. Dieudonné, J.: La géométrie des groupes classiques. Ergebnisse d. Math., N.F. 5, 2e éd. Berlin-Göttingen-Heidelberg: Springer 1963.
7. Jacobson, N.: Clifford algebras for algebras with involution of type *D*. Journal of Algebra **1**, 288—300 (1964).
8. Klingenberg, W., u. E. Witt: Über die Arfsche Invariante quadratischer Formen mod 2. J. reine angew. Math. **193**, 121—122 (1954).
9. Kneser, M.: Bestimmung des Zentrums der Cliffordschen Algebren einer quadratischen Form über einem Körper der Charakteristik 2. J. reine angew. Math. **193**, 123—125 (1954).
10. Seip-Hornix, E.A.M.: Clifford algebras of quadratic quaternion forms. Proc. Kon. Ned. Akad. Wet. A **68**, 326—363 (1965).
11. Serre, J.P.: Cohomologie galoisienne. Lecture Notes in Math. No. 5. Berlin-Heidelberg-New York: Springer 1964.
12. Springer, T.A.: Note on quadratic forms in characteristic 2. Nieuw Archief voor Wiskunde (3), **10**, 1—10 (1962).
13. Tits, J.: Classification of algebraic semisimple groups. Proc. Symp. Pure Math., vol. 9 (Algebraic groups and discontinuous subgroups), Amer. Math. Soc. 1966, 33—62. Voir aussi
13a. — Même titre. Notes de séminaire, Yale University, 1967, à paraître.
14. van Drooge, D.C.: Spinor theory of quadratic quaternion forms. Proc. Kon. Ned. Akad. Wet. A **70**, 487—523 (1967).
15. Weil, A.: Algebras with involution and the classical groups. J. Indian Math. Soc. **24**, 589—623 (1960).

Prof. Dr. J. Tits
Mathematisches Institut der Universität
5300 Bonn, Wegelerstr. 10

(Reçu le 7 Décembre 1967)