# TORSIONS QUADRATIQUES ET BASES NORMALES AUTODUALES

By Eva Bayer-Fluckiger and Jean-Pierre Serre

---

**Introduction.** Soient $K$ un corps de caractéristique $\neq 2$ et $L$ une extension finie séparable de $K$. L'un des invariants les plus souvent étudiés du couple $(L, K)$ est la forme quadratique $q_L : L \to K$, dite *forme trace*, définie par

$$q_L(x) = \mathrm{Tr}_{L/K}(x^2).$$

Lorsque $L/K$ est galoisienne de groupe de Galois $G$, cette forme est invariante par $G$. On obtient ainsi ce que l'on appelle une *$G$-forme quadratique*, cf. n°1.2. C'est un invariant de $L/K$ plus précis que la seule forme $q_L$ (il détermine non seulement $q_L$, mais aussi tous les $q_E$ pour $K \subset E \subset L$, cf. n°1.4). C'est à cet invariant que le présent travail est consacré.

Le cas le plus simple est celui où la $G$-forme quadratique $(L, q_L)$ est la *forme unité*. Cela signifie que $L$ possède une "*base normale autoduale*" (au sens de [4]), autrement dit qu'il existe $e \in L$ ayant les deux propriétés suivantes:

(i) Les $ge$ ($g \in G$) forment une base de $L$ ("base normale");

(ii) On a $\mathrm{Tr}_{L/K}(ge.g'e) = \delta_{g,g'}$ si $g, g' \in G$ (la base $(ge)$ est sa propre duale vis-à-vis de la forme $q_L$).

De telles bases existent lorsque $G$ est d'ordre impair, cf. [4]. Il n'en est plus de même lorsque $G$ est d'ordre pair. Il semble que la question dépende en grande partie des 2-sous-groupes de Sylow de $G$, et de leur "fusion." C'est en tout cas ce qui se passe lorsque ces groupes sont de type $(2, \ldots, 2)$, ou sont quaternioniens d'ordre 8, cf. ci-dessous; dans des cas simples, cela permet de donner des *critères cohomologiques* assurant l'existence d'une base normale autoduale.

Le texte est divisé en onze §§, répartis en trois sections:

Premiers exemples (§§1,2,3).
Groupes de Sylow élémentaires et quaternioniens (§§4,5,6,7,8,9).
Compléments (§§10,11).

Leur contenu est le suivant:

Le §1 contient un certain nombre de préliminaires, en particulier sur les *$G$-algèbres galoisiennes*. Il est en effet essentiel de ne pas se borner aux "extensions

---

Manuscript received July 15, 1992.
*American Journal of Mathematics* 116 (1994), 1–64.

galoisiennes" (qui sont des corps), mais d'accepter des $G$-algèbres quelconques. Cela permet en particulier de remplacer $K$ par une extension convenable de degré impair (ce qui ne change pas le problème, d'après [4]); cette technique nous servira souvent. Si $L$ est une telle $G$-algèbre, la $G$-forme quadratique $(L, q_L)$ est déterminée à isomorphisme près par un élément de $H^1(K, U_G)$, où $U_G$ est le groupe unitaire de l'algèbre $K[G]$, cf. 1.5.1.

Cette interprétation cohomologique est utilisée dans les §§2 et 3:

Dans le §2, on suppose que $K$ est un corps de dimension cohomologique $\leq 1$; dans ce cas, la classe d'isomorphisme de $(L, q_L)$ dépend seulement d'invariants appartenant à $H^1(K, \mathbf{Z}/2\mathbf{Z})$, cf. 2.2.3.

Dans le §3, $K$ est un corps de nombres algébriques. On montre que, si $H^1(G, \mathbf{Z}/2\mathbf{Z}) = H^2(G, \mathbf{Z}/2\mathbf{Z}) = 0$, alors une $G$-algèbre galoisienne $L$ a une base normale autoduale si et seulement si ses "Frobenius réels" sont triviaux.

Les §§4 et 5 contiennent divers résultats auxiliaires, notamment sur les formes quadratiques, et sur les foncteurs "induction" et "restriction". Ces résultats sont utilisés aux §§6,7,8, où l'on suppose qu'un 2-sous-groupe de Sylow $S$ de $G$ est abélien élémentaire de rang $r \geq 1$. Le cas le plus simple est celui où le normalisateur de $S$ opère transitivement sur $S - \{1\}$, i.e. où $G$ a une seule classe d'éléments d'ordre 2. Si $L$ est une $G$-algèbre galoisienne, on lui associe alors une *$r$-forme de Pfister*, qui *détermine la $G$-forme quadratique $(L, q_L)$ à isomorphisme près* (cf. 6.6.1—on trouvera un énoncé plus général dans 6.4.1). Ce résultat est particulièrement utile lorsque le rang $r$ de $S$ est $\leq 4$, car il permet de *caractériser* $(L, q_L)$ par un élément du groupe de cohomologie $H^r(K, \mathbf{Z}/2\mathbf{Z})$, cf. 7.5.4. Ainsi, par exemple, si $G$ est égal à $\mathbf{SL}_2(\mathbf{F}_8)$, ou au groupe de Janko $J_1$, l'existence d'une base normale autoduale *équivaut à la nullité d'un certain élément de* $H^3(K, \mathbf{Z}/2\mathbf{Z})$, à savoir l'image de l'unique élément non nul de $H^3(G, \mathbf{Z}/2\mathbf{Z})$.

Le §9 complète les précédents en traitant le cas où un 2-sous-groupe de Sylow de $G$ est quaternionien d'ordre 8. Ici encore, on obtient un invariant dans $H^3(K, \mathbf{Z}/2\mathbf{Z})$.

Le §10 contient deux contre-exemples montrant que l'existence d'une base normale autoduale ne peut pas toujours se lire sur la cohomologie ($\bmod 2$).

Enfin, le §11 explique le rôle de $(L, q_L)$ lorsqu'on utilise $L$ pour *tordre* (au sens galoisien du terme) un espace vectoriel muni de tenseurs: si tous ces tenseurs sont quadratiques, le résultat de la torsion ne dépend que de la $G$-forme quadratique $(L, q_L)$, cf. 11.2.2; en particulier, si $L$ a une base normale autoduale, la torsion par $L$ n'a aucun effet.

L'un des auteurs (E.B-F.) a bénéficié d'une subvention du Fonds National Suisse de la Recherche Scientifique, et l'en remercie.

**Table des matières**

## I. Premiers exemples

### 1. Préliminaires.

**1.1. Notations et conventions.** *Cardinal.* Si $X$ est un ensemble fini, son cardinal est noté $|X|$.

*Corps de base.* On note $K$ un corps commutatif de caractéristique $\neq 2$, $K_s$ une clôture séparable de $K$, et $G_K$ le groupe de Galois $\mathrm{Gal}(K_s/K)$.

*Cohomologie galoisienne.* Si $A$ est un groupe algébrique sur $K$, on note $H^1(K,A)$ l'ensemble pointé $H^1(G_K, A(K_s))$, cf. [19], p. II.3; c'est le "premier ensemble de cohomologie de $G_K$ dans $A$". Si $A$ est commutatif, on pose de même:

$$H^n(K,A) = H^n(G_K, A(K_s)) \quad \text{pour tout } n \geq 0.$$

*Groupes et algèbres de groupes.* On note $G$ un groupe fini, et $K[G]$ l'algèbre de $G$ sur $K$; on munit $K[G]$ de l'involution $K$-linéaire $x \mapsto x^*$ telle que $g^* = g^{-1}$ pour tout $g \in G$.

*Formes quadratiques.* Toutes les formes quadratiques considérées sont supposées non dégénérées. Si $q$ est une telle forme, on note $(x,y) \mapsto q(x,y)$ le produit scalaire correspondant, i.e. l'unique forme bilinéaire symétrique telle que $q(x) = q(x,x)$; on a

$$q(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)).$$

**1.2. $G$-espaces quadratiques.** Un *$G$-espace quadratique* (ou une *$G$-forme quadratique*) est un couple $(V, q)$, où $V$ est un $K$-espace vectoriel de dimension finie muni d'une action $K$-linéaire de $G$ (à gauche), et $q$ est une forme quadratique (non dégénérée, cf. 1.1) sur $V$ invariante par $G$.

L'espace vectoriel $V$ est un $K[G]$-module à gauche, et $q$ définit sur $V$ une $K[G]$-forme hermitienne non dégénérée $H_q : V \times V \to K[G]$ par la formule

$$H_q(x, y) = \sum_{g \in G} q(x, gy)g.$$

(Inversement, une telle forme hermitienne détermine un $G$-espace quadratique.)

*Exemple.* On appelle *$G$-forme unité* la $G$-forme quadratique $(K[G], q)$, où $q$ est telle que $q(g, h) = \delta_{g,h}$ (symbole de Kronecker) si $g, h \in G$. La forme hermitienne correspondante est $(x, y) \mapsto xy^*$.

Une $G$-forme quadratique $(V, q)$ est isomorphe à la $G$-forme unité si et seulement si $V$ possède une *base normale autoduale*, autrement dit s'il existe $e \in V$ tel que:

(a) les $ge$, $g \in G$, forment une base de $V$;

(b) on a $q(e, e) = 1$ et $q(e, ge) = 0$ si $g \neq 1$ (d'où $q(ge, g'e) = \delta_{g,g'}$).

Dans la suite un tel élément $e$ sera appelé un *vecteur basique* de $V$.

**Opérations sur les $G$-formes quadratiques.**

*Restriction.* Si $(V, q)$ est un $G$-espace quadratique et $S$ un sous-groupe de $G$, le groupe $S$ opère sur $V$ en fixant $q$, et l'on obtient ainsi un $S$-espace quadratique noté $\mathrm{Res}_S^G(V, q)$, ou plus simplement $\mathrm{Res}_S^G V$.

*Induction.* Soit $S$ un sous-groupe de $G$, et soit $(V, q)$ un $S$-espace quadratique. Soit $W = K[G] \otimes_{K[S]} V$ le $K[G]$-module induit de $V$. Si $T$ est un système de représentants de $G/S$, $W$ est somme directe des $tV$, $t \in T$. Il existe sur $W$ une forme quadratique $q_W$ et une seule qui ait les propriétés suivantes:

(a) elle est invariante par $G$;

(b) elle coïncide avec $q$ sur $V$;

(c) les sous-espaces $tV$ et $t'V$ sont orthogonaux pour $q$ si $t \neq t'$, $t, t' \in T$.

Le couple $(W, q_W)$ est un $G$-espace quadratique noté $\mathrm{Ind}_S^G(V, q)$.

**1.3. $G$-algèbres galoisiennes.**

*Définition.* Une $G$-algèbre galoisienne est une $K$-algèbre commutative $L$ de dimension $n = |G|$ munie d'une action de $G$ satisfaisant aux conditions équivalentes suivantes:

(1) L est étale (i.e. produit d'extensions séparables de $K$, cf. Bourbaki A V.28), de rang $n$, et l'action de $G$ sur $X(L) = \mathrm{Hom}^{\mathrm{alg}}(L, K_s)$ est simplement transitive.

(2) Après extension des scalaires à $K_s$, $L$ devient isomorphe au produit de $n$ copies de $K_s$, le groupe $G$ permutant de façon transitive les facteurs.

(3) $L$ est l'algèbre affine d'un $G$-torseur $T_L$ sur $K$ (espace principal homogène à droite sous $G$, vu comme groupe algébrique "constant" de dimension 0).

(4) $L$ est étale et la représentation de $G$ dans $L$ est isomorphe à la représentation régulière (i.e. $L$ est un $K[G]$-module libre de rang 1).

*Remarques.* (a) Dans (3), le $G$-torseur $T_L$ est $\mathrm{Spec}(L)$. L'ensemble de ses $K_s$-points est $X(L) = \mathrm{Hom}^{\mathrm{alg}}(L, K_s)$, cf. (1). Sur $X(L)$, il y a une action de $G$ à droite (provenant de celle de $G$ sur $L$) qui en fait un $G$-ensemble principal homogène; il y a aussi une action de $G_K$ à gauche (provenant de celle de $G_K$ sur $K_s$) qui commute à la précédente. Inversement, tout ensemble à $n$ éléments muni d'une action de $G$ à droite simplement transitive, et d'une action (continue) de $G_K$ à gauche commutant à l'action de $G$, définit une $G$-algèbre galoisienne et une seule.

(b) Les $G$-algèbres galoisiennes sont parfois appelées "algèbres galoisiennes de groupe de Galois $G$". Nous n'utiliserons pas cette terminologie, qui pourrait laisser croire que l'on peut reconstituer $G$ à partir de $L$, ce qui n'est pas le cas (sauf bien sûr si $L$ est un corps, cf. ci-dessous).

**1.3.1. L'homomorphisme $\phi_L$.** Si $L$ est comme ci-dessus, choisissons un élément $\chi \in X(L)$. Si $s \in G_K$, on a $s\chi = \chi.g_s$ avec $g_s \in G$ et l'application $s \mapsto g_s$ est un homomorphisme continu $\phi_{L,\chi} : G_K \to G$. La connaissance de $\phi_{L,\chi}$ détermine le couple $(L, \chi)$.

Si l'on se donne $\phi : G_K \to G$, il y a un couple $(L, \chi)$ et un seul à isomorphisme unique près qui lui correspond, à savoir celui tel que $X(L) = G$, $\chi = 1$, l'action de $G$ à droite sur $X(L)$ étant l'action évidente et l'action à gauche étant donnée par $\phi$.

Ainsi, les $G$-algèbres galoisiennes (à isomorphisme près) correspondent bijectivement aux homomorphismes continus $G_K \to G$ (à conjugaison près).

Dans la suite, on se permettra souvent d'écrire $\phi_L$ pour $\phi_{L,\chi}$.

L'image $L_1 = \chi(L)$ de $L$ par $\chi$ est un sous-corps de $K_s$ qui ne dépend pas du choix de $\chi$ dans $X(L)$. Ce corps est une extension galoisienne de $K$; le groupe de Galois de $L_1$ sur $K$ est $\phi_L(G_K)$. L'algèbre $L$ est isomorphe au produit de $m$ copies de $L_1$, où $m$ est l'indice de $\phi_L(G_K)$ dans $G$. En particulier:

(a) $\phi_L$ est surjectif si et seulement si $L$ est un *corps*; ce corps est alors une extension galoisienne de $K$ de groupe de Galois $G$ (c'est le cas le plus intéressant).

(b) $\phi_L = 1$ si et seulement si $L$ est isomorphe au produit de $n$ copies de $K$ permutées transitivement par $G$. On dit alors que $L$ est *décomposée* (ou *diagonalisable*, cf. Bourbaki, *loc. cit.*). Une telle algèbre sera notée $K^{(G)}$.

**1.3.2. Induction.** Soient $S$ un sous-groupe de $G$ et $M$ une $S$-algèbre galoisienne. A isomorphisme près, il existe un unique couple $(L, \pi)$, où $L$ est une $G$-algèbre galoisienne et $\pi$ un homomorphisme $L \to M$ tel que $\pi(sx) = s\pi(x)$ pour tout $x \in L$ et tout $s \in S$. (On peut prendre pour $L$ l'algèbre des fonctions $f : G \to M$ telles que $f(sg) = sf(g)$ pour tout $s \in S$ et tout $g \in G$; l'action de $G$ sur $L$ est donnée par $(g'f)(g) = f(gg')$ et la projection $\pi$ par $f \mapsto f(1)$.) La $G$-algèbre $L$ est appelée *l'induite* de $M$; on la note $\mathrm{Ind}_S^G M$. (Du point de vue des torseurs, cela correspond à l'opération usuelle d'induction.) Si $\phi_M : G_K \to S$ est associé à $S$ comme ci-dessus, on peut choisir pour $\phi_L : G_K \to G$ le composé de $\phi_M$ et de l'injection $S \to G$. Comme algèbre, $L$ est isomorphe à un produit de $(G : S)$ copies de $M$.

Toute algèbre galoisienne est induite d'une algèbre galoisienne qui est un corps, le groupe $S$ correspondant étant $\phi_L(G_K)$.

**1.4. Forme trace.** Soit $E$ une $K$-algèbre étale de dimension finie $n$. On note $q_E$ la *forme trace* de $E$, définie par $q_E(x) = \mathrm{Tr}_{E/K}(x^2)$ pour $x \in E$, cf. e.g. [20], n°1.4. C'est une forme quadratique de rang $n$. Si $X(E) = \mathrm{Hom}^{\mathrm{alg}}(E, K_s)$, on a

$$q_E(x, y) = \mathrm{Tr}_{E/K}(xy) = \sum_{\chi \in X(E)} \chi(x)\chi(y).$$

Si $L$ est une $G$-algèbre galoisienne, $q_L$ est invariante par $G$, et le couple $(L, q_L)$ est une $G$-forme quadratique au sens du n°1.2. On dit que $L$ a une *base normale autoduale* (cf. [4]) si $(L, q_L)$ est isomorphe à la $G$-forme unité, i.e. s'il existe $e \in L$ tel que:

(a) les $(ge)$, $g \in G$, forment une base de $L$ sur $K$;

(b) on a $q_L(ge, g'e) = \delta_{g,g'}$ si $g, g' \in G$.

Un tel $e$ sera appelé un *vecteur basique* de $L$, cf. n°1.2.

*Remarques*. En fait, la propriété (b) entraîne la propriété (a); il suffit même que l'on ait $q_L(e, ge) = \delta_{1,g}$ pour tout $g \in G$.

*Exemple*. La $G$-forme quadratique associée à une $G$ algèbre décomposée est isomorphe à la $G$-forme unité. Plus précisément, si $L = K \times \cdots \times K$, l'élément $e = (1, 0, \ldots, 0)$ est un vecteur basique.

*Forme trace d'une sous-algèbre de points fixes*. Soit $S$ un sous-groupe de $G$, et soit $E = L^S$ la sous-algèbre de $L$ fixée par $S$. Nous allons voir que la $G$-forme quadratique $(L, q_L)$ *détermine la forme trace* $q_E$ à isomorphisme près. De facon plus précise:

PROPOSITION 1.4.1. (a) *Soit $y \in E$. Il existe $y' \in L$ tel que $y = \sum_{s \in S} sy'$.*

(b) *Pour un tel choix de $y'$, on a $q_E(x, y) = q_L(x, y')$ pour tout $x \in E$.*

(Cet énoncé montre bien que l'on peut reconstituer $q_E$ à partir de $S$ et de la $G$-forme quadratique $(L, q_L)$.)

L'assertion (a) résulte de ce que $L$ est un $K[S]$-module libre; tout élément invariant est une trace.

Démontrons (b). Si l'on pose $X = X(L)$, alors $X(E)$ s'identifie à $X/S$. Choisissons un système de représentants $\Omega$ de $X/S$ dans $X$. On a:

$$\begin{aligned} q_E(x,y) &= \mathrm{Tr}_{E/K}(xy) = \mathrm{Tr}_{E/K}(x\sum_{s\in S} sy') = \sum_{\omega\in\Omega}\omega(x)\omega(\sum_{s\in S} sy') \\ &= \sum_{\omega\in\Omega}\sum_{s\in S}\omega(x)\omega(sy') = \sum_{\omega\in\Omega}\sum_{s\in S}(\omega s)(x).(\omega s)(y') \\ &= \sum_{\chi\in X}\chi(x)\chi(y') = \mathrm{Tr}_{L/K}(xy') = q_L(x,y'). \qquad \square \end{aligned}$$

*Remarque*. Lorsque $L$ est un *corps*, toutes ses sous-algèbres sont de la forme $L^S$ (théorie de Galois) et la prop. 1.4.1 montre comment leurs formes trace peuvent se déduire de la $G$-forme $(L, q_L)$.

PROPOSITION 1.4.2. *Supposons que $L$ ait une base normale autoduale, et soit $S$ un sous-groupe de $G$ comme ci-dessus.*

(i) *La forme trace $q_E$ de l'algèbre $E = L^S$ est isomorphe à la forme unité $\langle 1, \ldots, 1\rangle$.*

(ii) *Si $S$ est normal dans $G$, la $G/S$-algèbre galoisienne $E$ a une base normale autoduale.*

Soit $e$ un vecteur basique de $L$, et soit $T$ un système de représentants de $S\backslash G$, contenant 1. Pour tout $t \in T$, posons

$$e_t = \sum_{s\in S} st(e).$$

L'assertion (i) résulte du lemme plus précis suivant:

LEMME 1.4.3. *La famille $(e_t)_{t\in T}$ est une base autoduale de $(E, q_E)$, i.e. on a*

$$q_E(e_t, e_{t'}) = \delta_{t,t'} \text{ pour } t, t' \in T.$$

En effet, d'après la prop. 1.4.1, on a:

$$q_E(e_t, e_{t'}) = q_L(e_t, t'e) = \sum_{s\in S} q_L(ste, t'e) = \sum_{s\in S}\delta_{st,t'} = \delta_{t,t'}.$$

L'assertion (ii) résulte de:

LEMME 1.4.4. (cf. [4], p. 369). *Si $S$ est normal dans $G$, l'élément $e_1 = \sum_{s\in S}$ se est un vecteur basique de la $G/S$-algèbre galoisienne $E$.*

Du fait que $S$ est normal dans $G$, on a $e_t = \sum_{s\in S} ts(e) = te_1$: l'élément $e_t$ est le transformé de $e_1$ par l'élément de $G/S$ correspondant à $t$. D'après 1.4.3, on a $q_E(e_t, e_{t'}) = \delta_{t,t'}$; cela montre que $e_1$ est un vecteur basique de $E$.

*Remarque.* Plus généralement, soient $L$ et $L'$ deux $G$-algèbres galoisiennes telles que les $G$-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ soient isomorphes. Soit $S$ un sous-groupe normal de $G$, et soient $E = L^S$, $E' = L'^S$. Alors *les $G/S$-formes quadratiques $(E, q_E)$ et $(E', q_{E'})$ sont isomorphes*. Cela se voit, soit par un raisonnement analogue à celui fait ci-dessus, soit en utilisant les résultats du §11 sur la torsion des tenseurs quadratiques.

**1.4.5. Induction.** L'opération d'induction *commute* avec le foncteur $L \mapsto (L, q_L)$: si $S$ est un sous-groupe de $G$, si $M$ est une $S$-algèbre galoisienne, et si $L = \mathrm{Ind}_S^G M$ (cf. 1.3.2), la $G$-forme $(L, q_L)$ est isomorphe à l'induite $\mathrm{Ind}_S^G(M, q_M)$, cf. n°1.2.

**1.5. Le groupe unitaire $U_G$.** On note $U_G$ le *groupe unitaire* de l'algèbre à involution $K[G]$, cf. n°1.1. C'est un groupe algébrique linéaire sur $K$. Si $K'$ est une $K$-algèbre commutative, le groupe $U_G(K')$ des $K'$-points de $U_G$ est égal au groupe multiplicatif des éléments $x$ de $K'[G]$ tels que $xx^* = 1$. Du fait que $K$ est de caractéristique $\neq 2$, ce groupe est lisse; il est réductif si $K$ est de caractéristique 0, ou si la caractéristique de $K$ ne divise pas $|G|$. On peut considérer $U_G$ comme le *schéma des automorphismes* de la forme hermitienne unité, et donc aussi de la $G$-forme quadratique unité, cf. n°1.2.

Soit $H^1(K, U_G)$ le premier ensemble de cohomologie de $G_K$ dans $U_G$, i.e., $H^1(G_K, U_G(K_s))$, cf. n°1.1. D'après [19], chap. III, §1, les éléments de cet ensemble correspondent aux classes d'isomorphisme des *$G$-formes quadratiques qui deviennent isomorphes à la forme unité après extension des scalaires à $K_s$* (ou à une clôture algébrique de $K$, cela revient au même du fait que $U_G$ est lisse).

(On peut montrer que de telles formes $(V, q)$ sont caractérisées par le fait que la représentation de $G$ dans $V$ est isomorphe à la représentation régulière. Nous n'utiliserons pas ce résultat.)

Soit maintenant $L$ une $G$-algèbre galoisienne. D'après ce qui précède, la classe de la $G$-forme quadratique $(L, q_L)$ s'identifie à un élément de $H^1(K, U_G)$. Cet élément sera noté $u(L)$. On a par construction:

PROPOSITION 1.5.1. *Soient $L$ et $L'$ deux $G$-algèbres galoisiennes. Les $G$-formes associées $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes si et seulement si $u(L) = u(L')$ dans $H^1(K, U_G)$.*

COROLLAIRE 1.5.2. *Pour que $L$ ait une base normale autoduale il faut et il suffit que $u(L) = 0$.*

Nous allons voir comment on peut déterminer $u(L)$. Choisissons un homomorphisme $\varphi_L : G_K \to G$ définissant $L$. Identifions $G$ à un sous-groupe de $U_G(K)$ par $g \mapsto g$ (ce qui est licite puisque $gg^* = 1$). Soit $f_L : G_K \to U_G(K_s)$ le composé de $\varphi_L$ par ce plongement de $G$ dans $U_G(K_s)$. On peut considérer $f_L$ comme un 1-cocycle de $G_K$ à valeurs dans $U_G(K_s)$. Il définit donc une classe de cohomologie $(f_L)$ dans $H^1(G_K, U_G(K_s)) = H^1(K, U_G)$.

THÉORÈME 1.5.3. *On a $u(L) = (f_L)$.*

Soit $(V, q)$ une $G$-forme quadratique qui est $K_s$-isomorphe à la $G$-forme unité. Choisissons un vecteur basique $e \in K_s \otimes_K V$. Alors pour tout $s \in G_K$, $s(e) = u_s e$ avec $u_s \in K_s[G]$. On vérifie facilement que:

(a) $u_s$ appartient à $U_G(K_s)$ pour tout $s \in G$;

(b) l'application $s \mapsto u_s^{-1}$ est un 1-cocycle dont la classe dans $H^1(K, U_G)$ est celle de $(V, q)$.

On applique ceci à la $G$-forme $(L, q_L)$ de la façon suivante: soit $\chi$ un élément de $X(L)$ et soit $\phi = \phi_{L,\chi}$ l'homomorphisme de $G_K$ dans $G$ correspondant. Il existe un unique idempotent $e$ de $K_s \otimes_K L$ tel que $\chi(e) = 1$ et $\chi'(e) = 0$ si $\chi' \neq \chi$. Cet élément est un vecteur basique pour $K_s \otimes_K L$. En utilisant la formule $s\chi = \chi\phi(s)$, cf. n°1.3, on constate que $s(e) = \phi(s)^{-1}e$ pour tout $s \in G_K$. Le cocycle correspondant est donc $s \mapsto \phi(s)$, ce qui démontre le théorème.

*Variante*. Le calcul ci-dessus peut s'interpréter de la façon suivante: La $G$-algèbre galoisienne décomposée $K^{(G)} = K \times \cdots \times K$ a pour groupe d'automorphismes le groupe $G$ lui-même, vu comme groupe algébrique de dimension 0. L'homomorphisme $\phi_L : G_K \to G$ permet de tordre $K^{(G)}$, et l'algèbre obtenue est $L$. Cette torsion transforme la $G$-forme quadratique de $K^{(G)}$ en celle de $L$, ce qui équivaut à 1.5.3.

**1.6. Exemple—le cas de $A_4$.** Dans ce n°, $G$ est le groupe alterné $A_4$. On suppose, pour simplifier, que le corps $K$ est de caractéristique $\neq 3$ et contient les racines cubiques de l'unité.

L'algèbre $K[G]$ se décompose alors en

$$K[G] = K \times K \times K \times \mathbf{M}_3(K),$$

les différents facteurs correspondant aux représentations irréductibles de $G$: la représentation unité, les deux représentations de degré 1 à image d'ordre 3 et la représentation irréductible de degré 3. Dans cette décomposition, l'involution permute le second et le troisième facteur, et est de type orthogonal dans les deux autres. On en déduit

$$U_G = \mathbf{O}_1 \times \mathbf{G}_m \times \mathbf{O}_3,$$

où $\mathbf{O}_1 = \{\pm 1\}$ est le groupe orthogonal à une variable, $\mathbf{G}_m$ est le groupe multiplicatif, et $\mathbf{O}_3$ est le groupe orthogonal de la forme unité à 3 variables $\langle 1,1,1\rangle$. (De façon plus précise, $\mathbf{O}_3$ est le groupe orthogonal de la forme $X_1^2 + \cdots + X_4^2$ sur l'hyperplan $X_1 + \cdots + X_4 = 0$, le groupe $G = A_4$ agissant par permutation des coordonnées.)

Soit maintenant $L$ une $G$-algèbre galoisienne sur $K$, et soit $u(L) \in H^1(K, U_G)$ l'invariant correspondant, cf. n°1.5. Vu la décomposition de $U_G$ donnée ci-dessus, $u(L)$ s'identifie à un triplet $(u_1, u_2, u_3)$ de classes de cohomologie, avec $u_1 \in H^1(K, \mathbf{O}_1)$, $u_2 \in H^1(K, \mathbf{G}_m)$, $u_3 \in H^1(K, \mathbf{O}_3)$. D'après le th. 1.5.3, chacune de ces classes provient du cocycle donné par l'homomorphisme de $G_K$ dans le groupe correspondant, via $\phi_L$ et $G$. Comme l'image de $G$ dans $\mathbf{O}_1$ est triviale, on a $u_1 = 0$. On a $u_2 = 0$ puisque $H^1(K, \mathbf{G}_m) = 0$. Enfin, $u_3$ s'identifie à la classe de la forme quadratique $q_3(L)$ obtenue par *torsion* ([19], *loc. cit.*) de la forme unité $\langle 1,1,1\rangle$ grâce à $\phi_L : G_K \to G$ et à l'action de $G$ sur cette forme. D'où:

PROPOSITION 1.6.1. *Pour que $L$ ait une base normale autoduale, il faut et il suffit que la forme quadratique $q_3(L)$ soit isomorphe à la forme unité $\langle 1,1,1\rangle$.*

On peut expliciter $q_3(L)$ de la manière suivante: soit $E$ la sous-algèbre de $L$ fixée par le sous-groupe $A_3$ de $A_4$. C'est une algèbre étale de rang 4. Sa forme trace $q_E$ est *isomorphe à la somme directe de $q_3(L)$ et de la forme unité* $\langle 1\rangle$. Le critère 1.6.1 peut donc se reformuler en disant que *$L$ a une base normale autoduale si et seulement si $q_E$ est isomorphe à la forme unité* $\langle 1,1,1,1\rangle$ (la *nécessité* de cette condition résulte aussi de la prop. 1.4.2).

*Remarques.* 1) La proposition ci-dessus est en fait valable même si $K$ est de caractéristique 3, ou si $K$ ne contient pas les racines cubiques de l'unité. Cela se voit par un argument analogue, et cela sera démontré par une voie différente au n°8.1.

2) On peut appliquer ce genre de méthode à d'autres groupes (par exemple $A_5$, ou $A_6$), les classes de cohomologie obtenues s'interprétant en termes de formes quadratiques ou hermitiennes. Il est alors nécessaire de déterminer les relations qu'ont entre elles ces diverses formes, ce qui n'est pas toujours facile. Aussi suivrons-nous une méthode différente dans la partie II.

## 2. Réduction aux 2-groupes et critères en dimension 1.

**2.1. Réduction aux 2-groupes.** Soit $S$ un 2-sous-groupe de Sylow de $G$.

PROPOSITION 2.1.1. *Soit $L$ une $G$-algèbre galoisienne. Il existe une extension de degré impair $K'$ de $K$, et une $S$-algèbre galoisienne $M$ sur $K'$, telles que $K' \otimes_K L$ soit isomorphe (*comme $G$-algèbre galoisienne sur $K'$*) à l'algèbre induite* $\mathrm{Ind}_S^G M$, cf. n°1.3.2.

Soit $\phi_L : G_K \to G$ un homomorphisme définissant $L$, cf. n°1.3.1. Quitte à remplacer $\phi_L$ par un conjugué, on peut supposer que $\phi_L(G_K) \cap S$ est un 2-

sous-groupe de Sylow de $\phi_L(G_K)$. L'image réciproque de ce sous-groupe par $\phi_L$ est d'indice impair dans $G_K$; soit $K'$ l'extension de $K$ correspondante. Par construction, $[K' : K]$ est impair, et $\phi_L(G_{K'})$ est contenu dans $S$. La restriction de $\phi_L$ à $G_{K'}$ définit (cf. 1.3.1) une $S$-algèbre galoisienne $M$ sur $K'$, et il est clair que $\mathrm{Ind}_S^G M$ est isomorphe à $K' \otimes_K M$.

*Remarque*. Nous utiliserons fréquemment la prop. 2.1.1 par la suite. On notera que, pour l'énoncer, il est nécessaire de disposer de la notion générale de $G$-algèbre galoisienne: si l'on voulait se limiter aux *extensions* galoisiennes (i.e. au cas où $L$ est un corps), on ne pourrait utiliser, ni l'induction, ni l'extension des scalaires.

D'autre part, d'après [4], th. 4.1, on a le résultat suivant (qui signifie que les extensions de degré impair "n'ont pas d'importance"):

THÉORÈME 2.1.2. *Soit $K'$ une extension de degré impair de $K$. Si deux $G$-formes quadratiques sur $K$ deviennent isomorphes après extension du corps de base à $K'$, elles sont isomorphes sur $K$.*

En particulier:

COROLLAIRE 2.1.3. *Si une $G$-algèbre galoisienne acquiert une base normale autoduale après extension de degré impair de $K$, elle en a une sur $K$.*

Dans la suite, nous donnerons des critères permettant de comparer les $G$-formes quadratiques associées à deux $G$-algèbres galoisiennes. Grâce à 2.1.1 et 2.1.2 nous pourrons souvent nous ramener au cas où ces algèbres sont *induites* de $S$-algèbres galoisiennes.

**2.2. Critères en dimension 1.** *Images réciproques de classes de cohomologie*. Soit $L$ une $G$-algèbre galoisienne, et soit $\phi_L : G_K \to G$ l'homomorphisme correspondant (défini à conjugaison près, cf. n°1.3.1). Soit $n$ un entier $\geq 0$. Si $x$ est un élément du groupe de cohomologie $H^n(G, \mathbf{Z}/2\mathbf{Z})$, son image par l'homomorphisme

$$\phi_L^* : H^n(G, \mathbf{Z}/2\mathbf{Z}) \to H^n(G_K, \mathbf{Z}/2\mathbf{Z}) = H^n(K, \mathbf{Z}/2\mathbf{Z}) \qquad \text{(cf. n°1.1)}$$

sera notée $x_L$. Cette image ne dépend pas du choix de $\phi_L$ dans sa classe de conjugaison, cf. e.g. [18], chap. VII, prop. 3.

*Une condition nécessaire.*

PROPOSITION 2.2.1. *Soient $L$ et $L'$ deux $G$-algèbres galoisiennes, et soit $x$ un élément de $H^1(G, \mathbf{Z}/2\mathbf{Z}) = Hom(G, \mathbf{Z}/2\mathbf{Z})$. Si les $G$-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes, alors $x_L = x_{L'}$ dans $H^1(K, \mathbf{Z}/2\mathbf{Z})$.*

On peut supposer $x \neq 0$. Soit $H$ le noyau de $x$, vu comme homomorphisme de $G$ dans $\mathbf{Z}/2\mathbf{Z}$. On a $(G : H) = 2$. Soient d'autre part $\phi_L$ et $\phi_{L'}$ les homomorphismes de $G_K$ dans $G$ définissant $L$ et $L'$. On a par définition

$$x_L = x \circ \phi_L \quad \text{et} \quad x_{L'} = x \circ \phi_{L'}.$$

Soient $E = L^H$ et $E' = L'^H$ les sous-algèbres de $L$ et $L'$ fixées par $H$. Ce sont des algèbres quadratiques sur $K$, associées respectivement à $x_L$ et $x_{L'}$. D'après la prop. 1.4.1, les formes traces de $E$ et $E'$ sont isomorphes. Or la forme trace d'une algèbre quadratique détermine cette algèbre à isomorphisme près (si son discriminant est $d$, l'algèbre est isomorphe à $K[X]/(X^2 - d)$). On en conclut que $E$ et $E'$ sont isomorphes, d'où le fait que $x_L = x_{L'}$.

COROLLAIRE 2.2.2. *Si une $G$-algèbre galoisienne $L$ a une base normale autoduale, on a $x_L = 0$ pour tout $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$ (autrement dit, $\phi_L(G_K)$ est contenu dans tous les sous-groupes d'indice 2 de $G$).*

Cela résulte de la prop. 2.2.1, appliquée à $L$ et à une $G$-algèbre décomposée. (On pourrait aussi utiliser la prop. 1.4.2.)

*Réciproque*. La prop. 2.2.1 admet la réciproque suivante:

THÉORÈME 2.2.3. *Supposons que la 2-dimension cohomologique $\mathrm{cd}_2(G_K)$ du groupe profini $G_K$ soit $\leq 1$ (cf. [19], I.17). Soient $L$ et $L'$ deux $G$-algèbres galoisiennes. Les propriétés suivantes sont équivalentes:*

(a) *On a $x_L = x_{L'}$ pour tout $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$.*

(b) *Les $G$-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes.*

Le fait que (a) $\Rightarrow$ (b) sera démontré au n°2.4. L'implication (b) $\Rightarrow$ (a) résulte de la prop. 2.2.1.

*Remarques*. 1) Soit $H$ le sous-groupe de $G$ engendré par les carrés, autrement dit l'intersection des noyaux des homomorphismes de $G$ dans $\mathbf{Z}/2\mathbf{Z}$. La propriété (a) du th. 2.2.3 équivaut à:

(a') *Les $G/H$-algèbres galoisiennes $L^H$ et $L'^H$ sont isomorphes.*

2) L'hypothèse $\mathrm{cd}_2(G_K) \leq 1$ est satisfaite si $K$ est un corps fini, ou une extension de degré de transcendance 1 d'un corps algébriquement clos, cf. [19], Chap. II, §3.

*Applications*. Dans le cas où $L'$ est *décomposée*, le th. 2.2.3 donne:

PROPOSITION 2.2.4. *Soit $L$ une $G$-algèbre galoisienne. Si $\mathrm{cd}_2(G_K) \leq 1$ les deux propriétés suivantes sont équivalentes:*

(a) *On a $x_L = 0$ pour tout $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$.*

(b) *$L$ a une base normale autoduale.*

Lorsque $L$ est un *corps*, $\phi_L : G_K \to G$ est surjectif, et l'homomorphisme

$$\phi_L^* : H^1(G, \mathbf{Z}/2\mathbf{Z}) \to H^1(K, \mathbf{Z}/2\mathbf{Z})$$

est injectif. On en déduit:

PROPOSITION 2.2.5. *Soit $L$ une extension galoisienne de $K$ de groupe de Galois $G$. Supposons que $\mathrm{cd}_2(G_K)$ soit $\leq 1$. Pour que $L$ ait une base normale autoduale il faut et il suffit que $H^1(G, \mathbf{Z}/2\mathbf{Z}) = 0$, i.e. que $G$ n'ait pas de sous-groupe d'indice 2.*

### 2.3. Résultats auxiliaires.

PROPOSITION 2.3.1. *Il existe une extension algébrique $K'$ de $K$ ayant les propriétés suivantes:*

(1) *$K'$ est réunion filtrante d'extensions de degrés impairs de $K$;*

(2) *$K'$ est un corps parfait;*

(3) *$G_{K'}$ est un pro-2-groupe.*

Soit $S_2(G_K)$ un 2-sous-groupe de Sylow de $G_K$, cf. [19], I-4, et soit $K_2$ le sous-corps de $K_s$ fixé par $S_2(G_K)$. Le corps $K_2$ satisfait à (1) et (3). Sa clôture radicielle $K'$ satisfait à (1), (2) et (3).

*Remarques.* 1) En fait, $K'$ est déterminé *à isomorphisme près* par les conditions (1), (2) et (3).

2) Comme $G_{K'}$ est isomorphe à $S_2(G_K)$, la dimension cohomologique de $G_{K'}$ est égale à $\mathrm{cd}_2(G_K)$. Si $\mathrm{cd}_2(G_K) \leq 1$, le corps $K'$ est *de dimension* $\leq 1$ au sens de [19], II-8.

PROPOSITION 2.3.2. *Soit $A$ une algèbre à involution sur $K$ de dimension finie et soit $U$ le groupe unitaire correspondant. Soit $U^0$ la composante neutre de $U$. Alors:*

(i) *$U/U^0$ est un 2-groupe abélien élémentaire.*

(ii) *Si $\mathrm{cd}_2(G_K) \leq 1$, l'application $H^1(K, U) \to H^1(K, U/U^0)$ est injective.*

*Démonstration de (i).* L'énoncé étant géométrique, on peut supposer $K$ algébriquement clos. Soit $\mathfrak{r}$ le radical de $A$, soit $B = A/\mathfrak{r}$, et soit $U(B)$ le groupe unitaire de $B$. On vérifie (cf. par exemple [3],[4]) que $U(B)$ est isomorphe au quotient de $U$ par un sous-groupe unipotent connexe. En particulier, l'homomorphisme $U/U^0 \to U(B)/U(B)^0$ est un isomorphisme. Cela permet de remplacer $A$ par $B$, i.e. de supposer que $A$ est *semi-simple*. Le groupe $U$ se décompose alors en produit de groupes isomorphes à un groupe linéaire $\mathbf{GL}_n$, à un groupe symplectique $\mathbf{Sp}_{2n}$, où à un groupe orthogonal $\mathbf{O}_n$. Ces groupes sont connexes, à l'exception de $\mathbf{O}_n$: la composante neutre de $\mathbf{O}_n$ est $\mathbf{SO}_n$, et $\mathbf{O}_n/\mathbf{SO}_n$ est cyclique d'ordre 2. D'où (i).

*Démonstration de (ii).* Choisissons une extension $K'$ de $K$ ayant les propriétés (1), (2) et (3) de la prop. 2.3.1. D'après la remarque 2) ci-dessus, $K'$ est *de dimension* $\leq 1$. Considérons le diagramme commutatif

$$\begin{array}{ccc} H^1(K,U) & \xrightarrow{f} & H^1(K',U) \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g'} \\ H^1(K,U/U^0) & \xrightarrow{f_0} & H^1(K',U/U^0), \end{array}$$

où les flèches $f, f_0, g, g'$ sont définies de façon évidente.

LEMME 2.3.3. *L'application* $f : H^1(K,U) \to H^1(K',U)$ *est injective.*

Cela résulte du th. 2.1 de [4], qui est applicable du fait que $K'$ est réunion filtrante d'extensions de degrés impairs de $K$.

LEMME 2.3.4. *L'application* $g' : H^1(K',U) \to H^1(K',U/U^0)$ *est injective.*

Soit $\beta \in H^1(K',U)$, et soit $b$ un 1-cocycle représentant $\beta$. Soit $X_\beta = g'^{-1}(g'(\beta))$ la fibre de $g'$ contenant $\beta$. D'après la suite exacte de cohomologie (non abélienne), $X_\beta$ est quotient de $H^1(K', {}_bU^0)$, où ${}_bU^0$ est le groupe déduit de $U^0$ par torsion au moyen de $b$ ([19], chap. I, cor. 2 à la prop. 39). Or ${}_bU^0$ est un groupe linéare connexe. Comme $K'$ est un corps parfait de dimension $\leq 1$, on a $H^1(K', {}_bU^0) = 0$ d'après un théorème de Steinberg ([23], th. 1.9). L'ensemble $X_\beta$ est donc réduit à un seul élément; d'où l'injectivité de $g'$.

D'après les lemmes ci-dessus, $g' \circ f = f_0 \circ g$ est injectif. Il en est donc de même de $g$, ce qui démontre (ii).

*Démonstration du théorème 2.2.3.* L'hypothèse (a) équivaut à dire que, pour tout homomorphisme $\varepsilon$ de $G$ dans un 2-groupe abélien élémentaire, on a $\varepsilon \circ \phi_L = \varepsilon \circ \phi_{L'}$. Appliquons ceci à l'homomorphisme

$$\varepsilon : G \to U_G(K) \to (U_G/U_G^0)(K),$$

ce qui est licite vu la prop. 2.3.2 (i). On a donc $\varepsilon \circ \phi_L = \varepsilon \circ \phi_{L'}$. Ceci entraîne que les classes de cohomologie $u(L)$ et $u(L')$ de $H^1(K, U_G)$ ont même image dans $H^1(K, U_G/U_G^0)$. D'après la prop. 2.3.2 (ii), ces classes sont donc égales, et les $G$-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes, cf. prop. 1.5.1.

## 3. Critères en dimension 2 (corps de nombres).

**3.1. Le cas du corps R.** Comme $G_{\mathbf{R}} = \mathrm{Gal}(\mathbf{C}/\mathbf{R}) \cong \{\pm 1\}$, une $G$-algèbre galoisienne $L$ sur $\mathbf{R}$ correspond à un élément $\sigma(L)$ de $G$, défini à conjugaison près, tel que $\sigma(L)^2 = 1$. Deux $G$-algèbres galoisiennes sur $\mathbf{R}$ sont isomorphes si et seulement si les classes de conjugaison correspondantes sont les mêmes.

PROPOSITION 3.1.1. *Soient $L_1$ et $L_2$ deux $G$-algèbres galoisiennes sur* $\mathbf{R}$. *Les $G$-formes quadratiques associées à $L_1$ et $L_2$ sont isomorphes si et seulement si $L_1$ et $L_2$ sont isomorphes.*

La suffisance est triviale.

Supposons que les $G$-formes quadratiques associées à $L_1$ et à $L_2$ soient isomorphes. Soient $\sigma_1 = \sigma(L_1)$, $\sigma_2 = \sigma(L_2)$.

Soit $H$ un sous-groupe de $G$. L'algèbre étale $L_1^H$ se décompose en produit de corps $\mathbf{R}$ et $\mathbf{C}$. Les facteurs $\mathbf{R}$ correspondent aux points de $G/H$ fixés par $\sigma_1$, les facteurs $\mathbf{C}$ aux orbites de $\sigma_1$ dans le complémentaire. Il en résulte que la forme trace de $L_1^H$ est hyperbolique si et seulement si $H$ ne contient aucun conjugué de $\sigma_1$. De même, la forme trace de $L_2^H$ est hyperbolique si et seulement si $H$ ne contient aucun conjugué de $\sigma_2$.

Prenons $H = \{1\}$. On voit que la forme quadratique de $L_i$ est hyperbolique si et seulement si $\sigma_i \neq 1$. Donc $\sigma_1 = 1$ si et seulement si $\sigma_2 = 1$.

Supposons maintenant $\sigma_1 \neq 1$, et prenons $H = \{1, \sigma_1\}$. Alors la forme trace de $L_1^H$ n'est pas hyperbolique. D'après 1.2.4, les formes trace de $L_1^H$ et de $L_2^H$ sont isomorphes. Donc la forme trace de $L_2^H$ n'est pas hyperbolique non plus, ce qui entraîne que $H$ contient un conjugué de $\sigma_2$. On en déduit que $\sigma_2$ est, soit conjugué à $\sigma_1$, soit égal à 1. Mais nous avons déjà vu que si $\sigma_2 = 1$, alors $\sigma_1 = 1$. Nous avonc donc montré que $\sigma_1$ et $\sigma_2$ sont conjugués. Donc les $G$-algèbres galoisiennes $L_1$ et $L_2$ sont isomorphes.

COROLLAIRE 3.1.2. *Une $G$-algèbre galoisienne $L$ sur* $\mathbf{R}$ *a une base normale autoduale si et seulement si elle est décomposée.*

Cela résulte de la prop. 3.1.1, appliquée à $L$ et à une $G$-algèbre galoisienne décomposée.

**3.2. Le cas des corps de nombres; énoncé du théorème.** Supposons que $K$ soit une extension finie de $\mathbf{Q}$. Soit $L$ une $G$-algèbre galoisienne sur $K$. Pour toute place réelle $v$ de $K$, on obtient une $G$-algèbre galoisienne réelle $L_v$. Comme dans 3.1, on lui associe un élément $\sigma_v = \sigma(L_v)$ de $G$, défini à conjugaison près, tel que $\sigma_v^2 = 1$.

THÉORÈME 3.2.1. *Supposons que $H^1(G, \mathbf{Z}/2\mathbf{Z}) = H^2(G, \mathbf{Z}/2\mathbf{Z}) = 0$. Alors les propriétés suivantes sont équivalentes:*

(1) *$L$ a une base normale autoduale.*

(2) *$\sigma_v = 1$ pour toute place réelle $v$ de $K$*

Le fait que (1) entraîne (2) est vrai sans hypothèse sur $G$ d'après 3.1.2. Que (2) entraîne (1) sera démontré au n°3.4.

COROLLAIRE 3.2.2. *Supposons que $H^1(G, \mathbf{Z}/2\mathbf{Z}) = H^2(G, \mathbf{Z}/2\mathbf{Z}) = 0$. Alors toute $G$-algèbre galoisienne sur un corps de nombres totalement imaginaire a une base normale autoduale.*

*Remarque*. Les hypothèses de 3.2.1 signifient que le groupe dérivé de $G$ est d'indice impair, et que le multiplicateur de Schur de $G$ est d'ordre impair. Cette dernière hypothèse est vérifiée pour beaucoup de groupes simples, cf. [8].

*Question*. Le cor. 3.2.2 peut-il s'étendre à tous les corps dont la 2-dimension cohomologique est $\leq 2$? C'est le cas pour les corps de fonctions dúne variable sur un corps fini.

**3.3. Un résultat auxiliaire.** Rappelons que $U_G$ désigne le groupe unitaire associé à l'algèbre à involution $K[G]$ (cf. 1.5) et que l'on considère $G$ comme plongé dans $U_G(\mathbf{Q})$. Soit $U^0$ la composante neutre de $U_G$. On a vu que $U_G/U^0$ est de type $(2,\dots,2)$, cf. prop. 2.3.2. Comme $H^1(G,\mathbf{Z}/2\mathbf{Z}) = 0$, l'image de $G$ dans $U_G/U^0$ est triviale, autrement dit $G$ est contenu dans $U^0(\mathbf{Q})$. Soit $U^1$ le groupe dérivé de $U^0$. Alors $U^1$ est un groupe algébrique semi-simple connexe. On note $\tilde{U}^1$ le revêtement universel de $U^1$. Soit $G'$ le groupe dérivé de $G$. Le groupe $G'$ est contenu dans $U^1(\mathbf{Q})$.

THÉORÈME 3.3.1. *Le groupe $G'$ se relève en un sous-groupe de $\tilde{U}^1(\mathbf{Q})$.*

Pour démontrer de théorème, nous utiliserons le résultat suivant (cf. [5], 2.24, (ii)):

PROPOSITION 3.3.2. *Soit $R$ un groupe algébrique réductif connexe défini sur un corps $k$ de caractéristique 0. Soient $R'$ le groupe dérivé de $R$ et $\tilde{R}'$ le revêtement universel de $R'$. Soit $\pi$ la projection de $\tilde{R}'$ sur $R'$. Il existe alors un morphisme $c : R \times R \to \tilde{R}'$ et un seul, tel que*

$$\begin{cases} c(1,1) = 1; \\ \pi c(x,y) = xyx^{-1}y^{-1} \text{ pour tout couple de points } x, y \text{ de } R. \end{cases}$$

*En particulier, si $x, y \in R(k)$, le commutateur $xyx^{-1}y^{-1}$ est image d'un élément de $\tilde{R}'(k)$, à savoir $c(x,y)$.*

Revenons à la démonstration du théorème 3.3.1. Du fait que $G/G'$ est d'ordre impair, la suite spectrale des extensions de groupes dégénère en un isomorphisme

$$H^i(G,\mathbf{Z}/2\mathbf{Z}) \cong H^0(G/G', H^i(G',\mathbf{Z}/2\mathbf{Z})).$$

Les hypothèses $H^1(G,\mathbf{Z}/2\mathbf{Z}) = H^2(G,\mathbf{Z}/2\mathbf{Z}) = 0$ se traduisent donc par:

(3.3.3) Pour $i = 1, 2$ tout élément de $H^i(G',\mathbf{Z}/2\mathbf{Z})$ invariant par $G/G'$ est 0.

Comme $G'$ est engendré par des commutateurs, la prop. 3.3.2 appliquée à $R = U^0$ et $R' = U^1$, montre que $G'$ *est contenu dans l'image de* $\tilde{U}^1(\mathbf{Q})$. Soit $E$

l'image réciproque de $G'$ dans $\tilde{U}^1(\mathbf{Q})$. On a une suite exacte

$$1 \to C(\mathbf{Q}) \to E \to G' \to 1, \tag{3.3.4}$$

où $C(\mathbf{Q})$ est le groupe des points $\mathbf{Q}$-rationnels du noyau $C$ de $\tilde{U}^1 \to U^1$. Sur $\overline{\mathbf{Q}}$, le groupe $U^1$ est un produit de groupes isomorphes à $\mathbf{SL}_n$ ($n \geq 2$), $\mathbf{Sp}_{2n}$ ($n \geq 2$), ou $\mathbf{SO}_n$ ($n \geq 3$); il en résulte que $C$ est de type $(2, \ldots, 2)$; d'où le même résultat pour $C(\mathbf{Q})$.

Soit $e \in H^2(G', C(\mathbf{Q}))$ la classe de cohomologie correspondant à l'extension (3.3.4). Faisons agir $G$ sur $G'$ par conjugaison et sur $C(\mathbf{Q})$ par action triviale. On obtient ainsi une action de $G$ sur $H^2(G', C(\mathbf{Q}))$.

LEMME 3.3.5. *La classe e est invariante par G.*

Il faut prouver que, pour tout $s \in G$, il existe un automorphisme de $E$ qui est l'identité sur $C(\mathbf{Q})$ et qui donne par passage au quotient l'automorphisme $x \mapsto sxs^{-1}$ de $G'$. Remarquons pour cela que l'on a des homomorphismes de groupes algébriques

$$U^0 \to \mathrm{Aut}(U^1) \to \mathrm{Aut}(\tilde{U}^1).$$

Ceci provient de ce que $U^1$ est normal dans $U^0$, et que tout automorphisme de $U^1$ se relève de façon unique à son revêtement universel. Comme $G$ est contenu dans $U^0(\mathbf{Q})$, cela donne un homomorphisme $G \to \mathrm{Aut}_{\mathbf{Q}}(\tilde{U}^1)$. L'élément $s$ de $G$ donne ainsi un automorphisme $\tilde{s}$ de $\tilde{U}^1$. Cet automorphisme laisse $E$ stable, et donne par passage au quotient la conjugaison par $s$. Il reste à montrer que $\tilde{s}$ est l'identité sur $C(\mathbf{Q})$. Or, l'image de l'homomorphisme $U^0 \to \mathrm{Aut}(\tilde{U}^1)$ agit trivialement sur $C$ puisque $U^0$ est connexe.

Revenons à la démonstration du th. 3.3.1.

Décomposons $C(\mathbf{Q})$ en un produit de copies de $\mathbf{Z}/2\mathbf{Z}$. Ceci identifie la classe de cohomologie $e$ à une famille d'éléments de $H^2(G', \mathbf{Z}/2\mathbf{Z})$. Ces éléments sont invariants par l'action de $G$. Par 3.3.3, ils sont nuls. Donc $e = 0$, et $E$ est isomorphe à $C(\mathbf{Q}) \times G'$, ce qui donne un relèvement de $G'$ à $\tilde{U}^1(\mathbf{Q})$.

**3.4. Démonstration du théorème 3.2.1.** Les notations étant celles de 3.2.1, supposons que les $\sigma_v$ soient égaux à 1 pour toute place réelle $v$ de $K$. Il nous faut montrer que $L$ a une base normale autoduale. D'après le n°2.1, on peut supposer (quitte à faire une extension de degré impair) que $L$ provient d'un homomorphisme $\phi_L : G_K \to G$ dont l'image est un 2-groupe. Cette image est contenue dans le groupe dérivé $G'$ de $G$, puisque $(G : G')$ est impair. D'après 3.3.1, le groupe $G'$ se relève en un sous-groupe de $\tilde{U}^1(\mathbf{Q})$, lequel est contenu dans $\tilde{U}^1(K)$. En composant $G_K \to G'$ et $G' \to \tilde{U}^1(K)$, on obtient un homomorphisme $f_L : G_K \to \tilde{U}^1(K)$, qui définit une classe de cohomologie $\tilde{u}(L) \in H^1(K, \tilde{U}^1)$. Soit $\mathbf{\Sigma}$ l'ensemble des places réelles de $K$; pour tout $v \in \mathbf{\Sigma}$, soit $K_v = \mathbf{R}$ le complété

de $K$ en $v$. D'apres un théorème de Kneser ([12], [13]), applicable parce que $\tilde{U}^1$ est semi-simple et simplement connexe, l'application canonique

$$H^1(K, \tilde{U}^1) \longrightarrow \prod_{v \in \Sigma} H^1(K_v, \tilde{U}^1)$$

est injective. Or, pour tout $v \in \Sigma$, l'élément $\sigma_v$ de $G'$ est égal à 1, et son image dans $\tilde{U}^1(K)$ est aussi égale à 1. Il en résulte que la composante d'indice $v$ de $\tilde{u}(L)$ est 0. Ceci étant vrai pour tout $v$, on a $\tilde{u}(L) = 0$. Mais l'image de $\tilde{u}(L)$ par l'application composée

$$H^1(K, \tilde{U}^1) \longrightarrow H^1(K, U^1) \longrightarrow H^1(K, U^0) \longrightarrow H^1(K, U_G)$$

n'est autre que la classe $u(L)$ du n°1.5. On a donc $u(L) = 0$, d'où le théorème, d'après 1.5.2.

**3.5. Exemple: le cas du groupe alterné $A_n$.** On considère ici le cas où $G$ est le groupe alterné $A_n$, $n \geq 4$. On note $\tilde{A}_n = 2.A_n$ l'unique extension non scindée de $A_n$ par un groupe d'ordre 2, cf. e.g. [20], n°1.5.

Rappelons que $K$ est un corps de nombres. Comme ci-dessus, soit $\Sigma$ l'ensemble des places réelles de $K$. Soit $L$ une $A_n$-algèbre galoisienne sur $K$. Posons $H = A_{n-1}$, et soit $E = L^H$. Alors $E$ est une algèbre étale de rang $n$ et de discriminant un carré. (Inversement tout algèbre étale de rang $n$ et de discriminant un carré peut être obtenu ainsi, essentiellement de deux manières.)

THÉORÈME 3.5.1. *Les propriétés suivantes sont équivalentes:*

(1) *$L$ a une base normale autoduale.*

(2) *La forme trace $q_E$ de l'algèbre étale $E$ est la forme unité $\langle 1, \ldots, 1 \rangle$ de rang $n$.*

(3) *$\phi_L$ se relève en un homomorphisme continu $\tilde{\phi}_L : G_K \to \tilde{A}_n$, et l'on a $\sigma_v = 1$ pour tout $v \in \Sigma$.*

(4) *$\phi_L$ se relève en un homomorphisme continu $\tilde{\phi}_L : G_K \to \tilde{A}_n$, tel que la $\tilde{A}_n$-algèbre galoisienne correspondante ait une base normale autoduale.*

On a (1) $\Rightarrow$ (2), cf. prop. 1.4.1. Supposons (2); alors pour tout $v \in \Sigma$, la forme quadratique $q_E$ est positive et cela entraîne que $\sigma_v = 1$, cf. n°3.1. D'autre part, l'invariant de Hasse-Witt de $q_E$ est 0; par [20], th. 1 et 3.1, cela entraîne que $\phi_L$ se relève à $\tilde{A}_n$. D'où (3). Si (3) est vérifiée, choisissons un relèvement $\tilde{\phi}_L : G_K \to \tilde{A}_n$ de $\phi_L$ et soient $\tilde{\sigma}_v$ les classes correspondantes. Les $\tilde{\sigma}_v$ s'identifient à des éléments $\varepsilon_v$ du groupe $\{\pm 1\}$, noyau de $\tilde{A}_n \to A_n$. En utilisant le théorème d'approximation faible, on construit un caractère quadratique $\varepsilon : G_K \to \{\pm 1\}$ ayant pour signe $\varepsilon_v$ en tout $v$. Si l'on remplace $\tilde{\phi}_L$ par $\varepsilon \cdot \tilde{\phi}_L$, on obtient alors un relèvement où les nouveaux $\tilde{\sigma}_v$ sont triviaux. Notons $\tilde{L}$ la $\tilde{A}_n$-algèbre galoisienne

correspondant à ce nouveau relèvement. D'après un résultat classique de Schur, on a

$$H^1(\tilde{A}_n, \mathbf{Z}/2\mathbf{Z}) = H^2(\tilde{A}_n, \mathbf{Z}/2\mathbf{Z}) = 0.$$

On peut donc appliquer le th. 3.2.1 à $\tilde{L}$, et l'on en déduit que $\tilde{L}$ a une base normale autoduale. D'où l'implication (3) $\Rightarrow$ (4). Enfin (4) $\Rightarrow$ (1) résulte de 1.4.2.(ii).

## II. Groupes de Sylow élémentaires et quaternioniens.

### 4. Résultats auxiliaires sur les formes quadratiques.

**4.1. Notations.** On rappelle que toutes les formes quadratiques considérées sont supposées non dégénérées.

On note $\mathrm{W}_K$ *l'anneau de Witt* de $K$, et $\mathrm{GrW}_K$ *l'anneau de Grothendieck-Witt* de $K$, cf. [16], p. 33. On identifie $\mathrm{GrW}_K$ au sous-anneau de $\mathrm{W}_K \times \mathbf{Z}$ formé des couples $(q, n)$ ayant même image dans $\mathbf{Z}/2\mathbf{Z}$. On note $\mathrm{GrW}_K^+$ le sous-ensemble de $\mathrm{GrW}_K$ formé des classes de formes quadratiques sur $K$; un élément de $\mathrm{GrW}_K^+$ est dit *effectif*.

**4.2. Extensions de degré impair.** Soit $K'/K$ une extension finie de degré impair. Les applications naturelles $\mathrm{W}_K \to W_{K'}$ et $\mathrm{GrW}_K \to \mathrm{GrW}_{K'}$ sont alors injectives ([16], 2.5.4, p. 47). De façon plus précise, il existe des rétractions (*transferts de Scharlau*) $\mathrm{W}_{K'} \to \mathrm{W}_K$ qui sont $\mathrm{W}_K$-linéaires ([16], 2.5.6 et 2.5.8). Le même résultat est vrai pour l'anneau de Grothendieck-Witt. En effet, si $s$ : $\mathrm{W}_{K'} \to \mathrm{W}_K$ est un transfert de Scharlau, on en définit un sur $\mathrm{GrW}_{K'} \subset \mathrm{W}_{K'} \times \mathbf{Z}$ par $(q, n) \mapsto (s(q), n)$.

On utilisera les résultats suivants:

**4.2.1.** Soient $q_1$ et $q_2$ deux formes quadratiques sur $K$. Disons que $q_1$ *contient* $q_2$ *sur* $K$ s'il existe une forme quadratique $q_3$ sur $K$ telle que $q_1$ soit isomorphe à $q_2 \oplus q_3$.

Alors *si* $q_1$ *contient* $q_2$ *sur* $K'$, $q_1$ *contient* $q_2$ *sur* $K$ ([16], 2.5.4). En particulier, si $q_1$ et $q_2$ sont $K'$-isomorphes, elles sont $K$-isomorphes.

**4.2.2.** Soit $q \in \mathrm{GrW}_K$. *Si* $q$ *devient effectif sur* $K'$, *alors* $q$ *est effectif sur* $K$. (Si l'on convient d'identifier $\mathrm{GrW}_K$ à son image dans $\mathrm{GrW}_{K'}$, ceci s'écrit: $\mathrm{GrW}_K \cap \mathrm{GrW}_{K'}^+ = \mathrm{GrW}_K^+$.)

Cela résulte de 4.2.1, en écrivant $q = q_1 - q_2$, où les $q_i$ sont des éléments effectifs de $\mathrm{GrW}_K$.

**4.3. Equations tensorielles.** Soit $(f_{ij})$, $i,j \in I$, une matrice carrée dont les éléments sont des formes quadratiques $f_{ij}$ sur $K$. Pour tout $i \in I$, soit $a_i$ une forme quadratique.

On cherche des formes quadratiques $(q_i)$ telles que l'on ait:

$$(*) \qquad \bigoplus f_{ij} \otimes q_i \cong a_j \qquad \text{pour tout } j \in I,$$

le signe $\oplus$ indiquant une somme directe orthogonale (ou une somme dans l'anneau $\mathrm{GrW}_K$, cela revient au même).

Si de tels $f_{ij}$ existent, on dira que *le système* $(*)$ *est résoluble sur* $K$.

Nous ferons l'hypothèse

$$(H) \qquad \det(\mathrm{rang}(f_{ij})) \equiv 1 \pmod 2.$$

THÉORÈME 4.3.1. *Supposons (H). Alors:*

*(a) Si le système* $(*)$ *a une solution, cette solution est unique.*

*(b) Si* $(*)$ *a une solution sur* $K'$*, où* $K'$ *est une extension de degré impair de* $K$*, il a une solution sur* $K$.

*Démonstration de* (a). D'après un théorème de Pfister ([16], 2.6.5) un élément de $\mathrm{GrW}_K$ dont le rang est impair est non diviseur de zéro. D'après l'hypothèse (H), c'est le cas pour l'élément $\det(f_{ij})$ de $\mathrm{GrW}_K$. En appliquant un résultat standard d'algèbre linéaire ([6], A.III.91, prop. 3, ou A.III.102, prop. 14), on en déduit que le système $(*)$ a au plus une solution dans $\mathrm{GrW}_K$, ce qui démontre (a).

*Démonstration de* (b). Soit $(q'_i)$ une solution de $(*)$ dans $K'$. Choisissons une rétraction $\mathrm{GrW}_K$-linéaire $s : \mathrm{GrW}_{K'} \to \mathrm{GrW}_K$, cf. 4.2. Posons $q_i = s(q'_i)$. Alors $(q_i)$ est une solution de $(*)$ dans $\mathrm{GrW}_K$. Vu (a), appliqué à $K'$, on a $q_i = q'_i$ dans $\mathrm{GrW}_{K'}$, d'où $q_i \in \mathrm{GrW}_K \cap \mathrm{GrW}^+_{K'}$. Par 4.2.2, ceci entraîne $q_i \in \mathrm{GrW}^+_K$. Donc $(q_i)$ est une solution de $(*)$ sur $K$.

COROLLAIRE 4.3.2. *Soit* $K'$ *une extension de* $K$ *de degré impair. Soit* $f$ *une forme quadratique sur* $K$ *de rang impair. Soit* $a$ *une forme quadratique sur* $K$*. S'il existe une forme quadratique* $q$ *sur* $K'$ *telle que* $f \otimes q \cong a$*, il en existe une seule (à isomorphisme près), et elle est définissable sur* $K$.

**4.4. Formes de Pfister.** Si $a \in K^*$, on note $\langle a \rangle$ la forme quadratique $aX^2$ de rang 1. Si $a_1, \ldots, a_n \in K^*$, on note $\langle a_1, \ldots, a_n \rangle$ la somme directe orthogonale des $\langle a_i \rangle$.

Soit $r$ un entier $\geq 0$. Si $a_1, \ldots, a_r \in K^*$, on pose

$$\langle\langle a_1, \ldots, a_r \rangle\rangle = \langle 1, a_1 \rangle \otimes \cdots \otimes \langle 1, a_r \rangle.$$

Une forme $q$ de rang $2^r$ est appelée une *r-forme de Pfister* s'il existe $a_1, \ldots, a_r \in K^*$ tels que $q \cong \langle\langle a_1, \ldots, a_r \rangle\rangle$.

Comme ci-dessus, soit $K'$ une extension de degré impair de $K$.

PROPOSITION 4.4.1. *Soit $q$ une forme quadratique sur $K$ de rang $2^r$. Si $q$ est une $r$-forme de Pfister sur $K'$, c'est une $r$-forme de Pfister sur $K$.*

Si $q$ est isotrope sur $K$, elle l'est *a fortiori* sur $K'$. Or on sait qu'une forme de Pfister isotrope est hyperbolique ([16], 4.1.5). Mais 4.2.1 entraîne que, si $q$ est hyperbolique sur $K'$, elle l'est sur $K$. Or une forme hyperbolique de rang $2^r$ est évidement une forme de Pfister.

Reste le cas où $q$ est anisotrope. Si $n = 2^r$, soient $X = (X_1, \ldots, X_n)$ et $Y = (Y_1, \ldots, Y_n)$ des indéterminées indépendantes. On sait ([16], 4.4.4) que $q$ est une forme de Pfister si et seulement si $q(X)q(Y)$ est représenté par $q$ sur le corps $K(X, Y)$. Par hypothèse, $q(X)q(Y)$ est donc représenté par $q$ sur le corps $K'(X, Y)$. Comme $[K' : K]$ est impair, il en résulte par 4.2.1 que $q(X)q(Y)$ est représenté par $q$ sur $K(X, Y)$, d'où la proposition.

**4.5. Divisibilité des formes de Pfister.** Soient $m, n$ des entiers $\geq 0$ et soit $r = m + n$. Soit $q_1$ une $r$-forme de Pfister et soit $q_2$ une $n$-forme de Pfister. Nous dirons que $q_1$ est *divisible* par $q_2$ s'il existe une $m$-forme de Pfister $q_3$ telle que $q_1 \cong q_2 \otimes q_3$. Cela revient à dire que l'on peut choisir $a_1, \ldots, a_n, b_1, \ldots, b_m$ dans $K^*$ tels que

$$q_1 \cong \langle\langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle\rangle \quad \text{et} \quad q_2 \cong \langle\langle a_1, \ldots, a_n \rangle\rangle.$$

PROPOSITION 4.5.1. *Pour que $q_1$ soit divisible par $q_2$, il faut et il suffit que $q_1$ contienne $q_2$.*

La nécessité est évidente, et la suffisance résulte du lemme 1.4 d'Arason [1].

PROPOSITION 4.5.2. *Si $q_1$ est divisible par $q_2$ sur $K'$, $q_1$ est divisible par $q_2$ sur $K$.*

Cela résulte de la prop. 4.5.1, combinée avec 4.2.1.

**5. $G$-formes quadratiques: induction et restriction.** Le problème dans ce § est le suivant: si $S$ est un 2-sous-groupe de Sylow de $G$, et si $V$ et $V'$ sont deux $S$-formes quadratiques, à quelle condition les $G$-formes induites correspondantes sont-elles isomorphes? On donne une réponse à cette question dans le cas particulier où $S$ est *abélien élémentaire*.

Le résultat démontré ici sera utilisé de façon essentielle au §6.

**5.1. Notations.** On note $S$ un 2-sous-groupe de Sylow de $G$. On suppose que $S$ est *abélien élémentaire*, i.e. produit de groupes d'ordre 2. On pose

$$S' = \mathrm{Hom}(S, \{\pm 1\}).$$

C'est le *dual* de $S$.

Rappelons (n°1.2) qu'un *G-espace quadratique* est un espace vectoriel de dimension finie muni d'une action de $G$ et d'une forme quadratique invariante par $G$. Les $G$-espaces quadratiques et les $S$-espaces quadratiques sont liés par les foncteurs suivants:

$\mathrm{Res}_S^G$: "*restriction* de $G$ à $S$"; ce foncteur transforme un $G$-espace quadratique en un $S$-espace quadratique (on conserve l'espace quadratique et l'on restreint l'action du groupe à $S$);

$\mathrm{Ind}_S^G$: "*induction* de $S$ à $G$"; ce foncteur transforme un $S$-espace quadratique en un $G$-espace quadratique, cf. n°1.2.

**5.2. Structure des $S$-espaces quadratiques.** Soit $(V, q)$ un $S$-espace quadratique. Pour tout $x \in S'$, notons $V_x$ le sous-espace propre de $V$ de type $x$, i.e. l'ensemble des $v \in V$ tels que $sv = x(s)v$ pour tout $s \in S$. Comme la caractéristique du corps de base $K$ est différente de 2, $V$ est *somme directe* des $V_x$ et ceux-ci sont orthogonaux entre eux deux à deux. On peut donc écrire

$$V = \bigoplus_{x \in S'} V_x.$$

En fait, il est plus commode d'écrire cette décomposition autrement:

Introduisons la notation $1_x$ pour désigner le $S$-espace quadratique $K$ muni de la forme quadratique unité et de l'action de $S$ via $x$ (cet espace a donc une base formée d'un élément $e_x$ sur lequel $S$ opère par $se_x = x(s)e_x$ et la forme quadratique de $1_x$ prend la valeur 1 en $e_x$).

On a alors:

$$V = \bigoplus_{x \in S'} V_x \otimes 1_x \tag{1}$$

cette décomposition étant compatible avec la structure de $S$-module quadratique (on convient que $S$ opère trivialement sur $V_x$).

Inversement, si l'on se donne pour tout $x \in S'$ un espace quadratique non dégénéré $V_x$, et si l'on forme la somme directe

$$V = \bigoplus_{x \in S'} V_x \otimes 1_x,$$

on obtient ainsi un $S$-espace quadratique (précisons que, dans $V_x \otimes 1_x$, l'action de $S$ est triviale sur $V_x$). La catégorie des $S$-espaces quadratiques est ainsi équivalente à celle des *familles* $(V_x)$ *d'espaces quadratiques*, indexées par $x \in S'$.

**5.3. Enoncé du théorème principal.** Soit $N$ le normalisateur de $S$ dans $G$. Le groupe $N$ opère sur $S$ par conjugaison (comme l'action de $S$ est triviale, c'est en fait une action de $N/S$). Il opère donc aussi sur le dual $S'$ de $S$. Soit $\Omega$ l'ensemble quotient $S'/N$. Un élément $\omega$ de $\Omega$ est une *orbite* de $N$ dans $S'$.

Si $V$ est un $S$-espace quadratique, nous poserons

$$V_\omega = \bigoplus_{x\in\omega} V_x; \tag{2}$$

c'est un espace quadratique (on oublie l'action de $S$—ou plutôt on la remplace par l'action triviale).

THÉORÈME 5.3.1. *Soient $V^1$ et $V^2$ deux $S$-espaces quadratiques. Les propriétés suivantes sont équivalentes:*

(a) *Pour tout $\omega \in \Omega$, les espaces quadratiques $V^1_\omega$ et $V^2_\omega$ sont isomorphes.*

(b) *Les $G$-espaces quadratiques $W^1 = \mathrm{Ind}_S^G V^1$ et $W^2 = \mathrm{Ind}_S^G V^2$ sont isomorphes.*

(c) *Les $S$-espaces quadratiques $\mathrm{Res}_S^G W^1$ et $\mathrm{Res}_S^G W^2$ sont isomorphes.*

L'implication (a) $\Rightarrow$ (b) sera prouvée au n°5.4 ci-dessous. L'implication (b) $\Rightarrow$ (c) est triviale. L'implication (c) $\Rightarrow$ (a) sera prouvée au n°5.5.

**5.4. Démonstration de** (a) $\Rightarrow$ (b)**.** Soit $V$ un $S$-espace quadratique. Ecrivons-le sous la forme de 5.2.1:

$$V = \bigoplus_{x\in S'} V_x \otimes 1_x.$$

On a:

$$\mathrm{Ind}_S^G V = \bigoplus_{x\in S'} V_x \otimes \mathrm{Ind}_S^G 1_x. \tag{5.4.1}$$

Soit $\omega$ une orbite de $N$ dans $S'$. Il est clair que, si $x$ et $y$ sont deux éléments de $\omega$, les $G$-espaces quadratiques $\mathrm{Ind}_S^G 1_x$ et $\mathrm{Ind}_S^G 1_y$ sont isomorphes. Convenons de noter $I(\omega)$ l'un quelconque de ces $G$-espaces. La somme directe (pour $x \in \omega$) des $V_x \otimes \mathrm{Ind}_S^G 1_x$ est isomorphe à $V_\omega \otimes I(\omega)$, ce qui permet de récrire 5.4.1 sous la forme:

$$\mathrm{Ind}_S^G V = \bigoplus_{\omega\in\Omega} V_\omega \otimes I(\omega). \tag{5.4.2}$$

En appliquant ceci à $V = V^1$ et $V = V^2$, et en tenant compte de ce que $V^1_\omega$ est isomorphe à $V^2_\omega$ pour tout $\omega$, on obtient bien l'isomorphisme cherché de $\mathrm{Ind}_S^G V^1$ avec $\mathrm{Ind}_S^G V^2$.

*Remarque.* Il n'est pas difficile d'*expliciter* le $G$-espace quadratique $I(\omega)$. Soit $x \in \omega$, et choisissons un système de représentants $T$ de $G/S$. Le $G$-espace $I(\omega)$ a une base $(e_t)_{t\in T}$ jouissant des propriétés suivantes:

(i) c'est une base autoduale (i.e. chaque $e_t$ est de carré 1 et des $e_t$ distincts sont orthogonaux);

(ii) Si $g \in G$, et si $gt$ est de la forme $t's$, avec $s \in S$ et $t' \in T$, on a $g.e_t = x(s)e_{t'}$.

En particulier, $I(\omega)$ ne dépend pas de $K$, en un sens évident.

**5.5. Démonstration de** (c) $\Rightarrow$ (a). Conservons les notations ci-dessus, et posons

$$A(V) = \mathrm{Res}_S^G \mathrm{Ind}_S^G V. \tag{5.5.1}$$

Vu 5.4.2, on a:

$$A(V) = \bigoplus_{\omega \in \Omega} V_\omega \otimes \mathrm{Res}_S^G I(\omega). \tag{5.5.2}$$

Si $y \in S'$, comparons les $y$-composantes des deux membres de 5.5.2. Nous obtenons:

$$A(V)_y = \bigoplus_{\omega \in \Omega} V_\omega \otimes (\mathrm{Res}_S^G I(\omega))_y. \tag{5.5.3}$$

Soit $\omega'$ une orbite de $N$ dans $S'$. Choisissons $y \in \omega'$. Il est clair que les espaces quadratiques $A(V)_y$ et $(\mathrm{Res}_S^G I(\omega))_y$ ne dépendent pas du choix de $y$, à isomorphisme près. Convenons de les noter respectivement $A(V)_{\omega'}$ et $F_{\omega,\omega'}$. On a alors:

$$A(V)_{\omega'} = \bigoplus_{\omega \in \Omega} V_\omega \otimes F_{\omega,\omega'} \qquad \text{pour tout } \omega' \in \Omega. \tag{5.5.4}$$

Notons $r(\omega, \omega')$ la dimension de l'espace $F_{\omega,\omega'}$.

LEMME 5.5.5. *On a* $\det(r(\omega,\omega')) \equiv 1 \pmod 2$.

La démonstration sera donnée au n°5.6.

Admettons ce lemme. Notons $a(V)_{\omega'}$, $v_\omega$, $f_{\omega,\omega'}$ les éléments de l'anneau de Grothendieck-Witt $\mathrm{GrW}_K$ définis par les espaces quadratiques $A(V)_{\omega'}$, $V_\omega$ et $F_{\omega,\omega'}$. On a alors

$$\sum_{\omega \in \Omega} v_\omega \cdot f_{\omega,\omega'} = a(V)_{\omega'} \qquad \text{pour tout } \omega' \in \Omega. \tag{5.5.6}$$

Appliquons cette équation avec $V = V^1$ et avec $V = V^2$. Vu l'hypothèse (c), on a $a(V^1)_{\omega'} = a(V^2)_{\omega'}$ pour tout $\omega' \in \Omega$. On en conclut que

$$\sum_{\omega \in \Omega} (v_\omega^1 - v_\omega^2) \cdot f_{\omega,\omega'} = 0 \text{ dans } \mathrm{GrW}_K \text{ pour tout } \omega' \in \Omega.$$

D'après le lemme 5.5.5, le déterminant de la matrice $(f_{\omega,\omega'})$ est un élément de $\mathrm{GrW}_K$ de rang impair. Cet élément est donc non diviseur de zéro (cf. [16], 2.6.5); le système d'équations linéaires ci-dessus a donc pour seule solution la solution 0. On en déduit que $v^1_\omega = v^2_\omega$ pour tout $\omega \in \Omega$, ce qui démontre (a).

**5.6. Démonstration du lemme 5.5.5.** Par définition, $F_{\omega,\omega'}$ est la $y$-composante du $S$-module quadratique $\mathrm{Res}^G_S \mathrm{Ind}^G_S 1_x$, où $x$ est un élément de $\omega$. Or, la formule de décomposition de Mackey s'applique au foncteur $\mathrm{Res}^G_S \mathrm{Ind}^G_S$. On obtient ainsi:

$$\mathrm{Res}^G_S \mathrm{Ind}^G_S 1_x \cong \bigoplus_{g \in S\backslash G/S} \mathrm{Ind}^S_{S_g} 1_{x_g}, \tag{5.6.1}$$

où $S_g = S \cap g^{-1}Sg$, et où $x_g$ est le caractère de $S_g$ défini par $x_g(s) = x(gsg^{-1})$.

Définissons $\delta(g,x,y) \in \{0,1\}$ par:

$$\delta(g,x,y) = \begin{cases} 1 & \text{si la restriction de } y \text{ à } S_g \text{ est } x_g; \\ 0 & \text{sinon.} \end{cases} \tag{5.6.2}$$

On vérifie facilement que la dimension de la $y$-composante de $\mathrm{Ind}^S_{S_g} 1_x$ est égale à $\delta(g,x,y)$. On déduit de là une formule explicite pour la dimension $r(\omega,\omega')$ de $F_{\omega,\omega'}$:

$$r(\omega,\omega') = \sum_{g \in S\backslash G/S} \delta(g,x,y) \qquad \text{si } x \in \omega, y \in \omega'. \tag{5.6.3}$$

Cette formule montre entre autres choses que $r(\omega,\omega')$ ne dépend pas de $K$. On peut donc prendre $K = \mathbf{C}$. Dans ce cas, les éléments de $S'$ peuvent être vus comme des *caractères* de degré 1 de $S$, et $r(\omega,\omega')$ s'interprète comme le nombre de fois que $y$ intervient dans la restriction à $S$ de la représentation induite $\mathrm{Ind}^G_S(x)$.

On doit calculer $\det(r(\omega,\omega'))$ et montrer que c'est un entier *impair*. Soit $X$ l'espace vectoriel des fonctions complexes sur $S$ invariantes par $N$. Soit $\phi = \mathrm{Res}^G_S \mathrm{Ind}^G_S$, considéré comme endomorphisme de $X$. Nous allons calculer de deux façons différentes le déterminant de $\phi$.

(1) Pour tout $\omega \in \Omega$, posons $p_\omega = \sum_{s \in \omega} s$; c'est un caractère de degré $|\omega|$ de $S$ invariant par $N$. Il est clair que les $p_\omega$ $(\omega \in \Omega)$ forment une base de $X$. De plus, on a

$$\phi(p_\omega) = |\omega|\phi(s) = \sum_{\omega' \in \Omega} r(\omega,\omega')p_{\omega'};$$

cela résulte de la définition de $r(\omega,\omega')$. Or on a $|\omega| \equiv 1 \pmod 2$ pour tout $\omega$, puisque $\omega$ est une orbite du groupe $N/S$, qui est d'ordre impair. On voit ainsi que *la matrice donnant $\phi$ par rapport à la base $(p_\omega)$ est à coefficients entiers, et*

*est congrue* (mod 2) *à la matrice* $(r(\omega,\omega'))$. D'où:

$$\det_X(\phi) \equiv \det(r(\omega,\omega')) \pmod 2. \tag{5.6.4}$$

(2) Soit $\Sigma$ l'ensemble quotient de $S$ par l'action de $N$. Si $\sigma \in \Sigma$ (i.e. si $\sigma$ est une orbite de $N$ dans $S$), notons $q_\sigma$ la fonction sur $S$ qui est égale à 1 sur $\sigma$ et à 0 ailleurs. Les $q_\sigma$ ($\sigma \in \Sigma$) forment une base de $X$. Soient $\sigma, \sigma' \in \Sigma$; choisissons $s \in \sigma$ et $s' \in \sigma'$. Le coefficient de $q_\sigma$ dans $\phi(q_{\sigma'})$ est égal au nombre des $g \in G/S$ tels que $gs'g^{-1} \in \sigma$. Or, puisque $S$ est commutatif, deux éléments de $S$ sont conjugués dans $G$ si et seulement s'ils le sont dans $N$ (cf. [10], p. 419). Il en résulte que le coefficient ci-dessus est 0 si $\sigma \neq \sigma'$; et, si $\sigma = \sigma'$, il est égal à $|\sigma|(C_s : S)$, où $C_s$ est le centralisateur de $s$ dans $G$. Or ce nombre est impair, puisque $S$ est un 2-groupe de Sylow de $G$. On en conclut que *la matrice donnant* $\phi$ *par rapport à la base* $(q_\sigma)$ *est à coefficients entiers, et est congrue* (mod 2) *à la matrice unité*. On a donc

$$\det_X(\phi) \equiv 1 \pmod 2. \tag{5.6.5}$$

En combinant 5.6.4. et 5.6.5., on obtient le lemme 5.5.5.

*Remarque*. On a vu en cours de démonstration que $|\Omega| = |\Sigma|$. Autrement dit, *le nombre des orbites de N dans S' et dans S est le même*.

(Plus généralement, supposons qu'un groupe fini $\Phi$ opère sur un groupe fini $H$. Soit $\mathrm{Cl}(H)$ l'ensemble des classes de conjugaison de $G$, et soit $\mathrm{Irr}(H)$ l'ensemble des caractères irréductibles de $H$. Le groupe $\Phi$ opère sur $\mathrm{Cl}(H)$ et $\mathrm{Irr}(H)$ avec *le même nombre d'orbites*; de façon plus précise, les $\Phi$-ensembles $\mathrm{Cl}(H)$ et $\mathrm{Irr}(H)$ sont *faiblement isomorphes* au sens de [17], §13.1, exerc. 5.)

## 6. Le cas où les 2-sous-groupes de Sylow de $G$ sont abéliens élémentaires.

Dans ce §, $S$ est un 2-sous-groupe de Sylow de $G$. A partir du n°6.2, on suppose que $S$ est *abélien élémentaire*, et l'on note $S'$ son dual, cf. n°5.1.

Soit $m$ l'indice de $S$ dans $G$, et soit $2^r$ l'ordre de $S$. On a

$$|G| = 2^r m.$$

On note $L$ une $G$-algèbre galoisienne sur $K$. Sa forme trace est $q_L$.

### 6.1. La forme $q_L^1$.

THÉORÈME 6.1.1. (a) *Il existe une forme quadratique* $q_L^1$ *sur K, de rang* $2^r$, *telle que* $q_L \cong m \otimes q_L^1$ *(i.e.* $q_L$ *est isomorphe à la somme directe orthogonale de m copies de* $q_L^1$*). Cette forme est unique, à isomorphisme près.*

(b) *Si M est une S-algèbre galoisienne sur K, et si L est la G-algèbre induite* $\mathrm{Ind}_S^G M$, *on a* $q_L^1 \cong q_M$.

L'unicité de $q_L^1$ résulte de ce que $m$ est impair (cf. 4.3.2 ou [16], 2.6.5).

Si $L = \mathrm{Ind}_S^G M$, la forme $q_L$ est somme directe de $m$ copies de $q_M$. Cela montre que $q_L^1$ existe dans ce cas, et est isomorphe à $q_M$. D'où (b).

Dans le cas général, on sait (cf. 2.1.1) qu'il existe une extension $K'$ de $K$ de degré impair telle que $K' \otimes_K L$ soit isomorphe à $\mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne sur $K'$. Cela entraîne que $q_L$ est divisible par $m$ sur $K'$; d'après 4.3.2, $q_L$ est donc divisible par $m$ sur $K$, ce qui achève la démonstration de (a).

*Remarques.* (1) La forme $q_L^1$ représente $2^r$; en effet, cela devient vrai après une extension convenable de $K$ de degré impair en vertu de 2.1.1 et de (b). Cela est donc vrai sur $K$.

(2) Le discriminant de $q_L^1$ est égal à celui de $q_L$; il est égal à 1 si $S$ n'est pas cyclique.

*Exemples.* $r = 1$, $S$ cyclique d'ordre 2. On a alors $q_L^1 \cong \langle 2\rangle \otimes \langle 1, d\rangle = \langle 2, 2d\rangle$ où $d$ est un élément de $K^*$. (De façon plus précise, $d$ est le discriminant de $L$; c'est aussi le discriminant de la $K$-algèbre quadratique associée à l'unique homomorphisme surjectif $G \to \{\pm 1\}$.)

$r = 2$, $S$ cyclique d'ordre 4. On peut montrer que $q_L^1 \cong \langle 1, d, a, a\rangle$, où $d$ est le discriminant de $L$ et $a$ un élément de $K^*$.

$r = 2$, $S$ de type (2,2). D'après les deux remarques ci-dessus, $q_L^1$ est une forme de rang 4 qui représente 1, et dont le discriminant est égal à 1. C'est donc une 2-forme de Pfister $\langle\langle a, b\rangle\rangle = \langle 1, a, b, ab\rangle$, avec $a, b \in K^*$. (Pour une généralisation de ce fait, voir th. 6.2.1 ci-après.)

$r = 3$, $S$ quaternionien d'ordre 8. On verra au n°9.3 que $q_L^1$ est une 3-forme de Pfister de type $\langle\langle 1, 1, a\rangle\rangle$ avec $a \in K^*$.

$r = 3$, $S$ diédral d'ordre 8. On peut montrer que $q_L^1$ est une 3-forme de Pfister de type $\langle\langle 1, a, b\rangle\rangle$ avec $a, b \in K^*$.

*Complément.* Le théorème 6.1.1 (a) peut se généraliser de la façon suivante:

THÉORÈME 6.1.2. *Soit $H$ un sous-groupe d'ordre impair de $G$, et soit $E = L^H$ la sous-algèbre de $L$ fixée par $H$. On a*

$$q_E \cong m_H \otimes q_L^1, \quad \text{où} \quad m_H = m/|H| = 2^{-r}(G : H).$$

Grâce à 2.1.1, on peut supposer que $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne. Comme $H$ est d'ordre impair, $H$ agit librement sur $G/S$. Il en résulte que $H$ permute librement les facteurs de $L = M \times \cdots \times M$, et par suite $E = L^H$ est isomorphe au produit de $m_H$ copies de $M$. On en déduit:

$$q_E \cong m_H \otimes q_M \cong m_H \otimes q_L^1.$$

*Remarque.* Une autre façon d'énoncer 6.1.2 est de dire que $|H| \otimes q_E$ *est isomorphe* à $q_L$.

**6.2. Structure de $q_L^1$.** Rappelons qu'à partir de maintenant, et jusqu'à la fin de ce paragraphe, on suppose que $S$ est *abélien élémentaire* de type $(2, \dots, 2)$, i.e. produit de $r$ groupes cycliques d'ordre 2. On reprend les notations du n°5.1. En particulier $S'$ désigne le groupe $\mathrm{Hom}(S, \{\pm 1\})$ des caractères de $S$, et $N$ est le normalisateur de $S$ dans $G$. Le groupe $N$ opère de façon naturelle sur $S$ et $S'$.

THÉORÈME 6.2.1. *La forme $2^r q_L^1$ est une $r$-forme de Pfister.*

(Précisons que $2^r q_L^1$ désigne ici le produit de $q_L^1$ et de $\langle 2^r \rangle$. Le th. 6.2.1 équivaut donc à dire que $q_L^1$ est une $r$-forme de Pfister si $r$ est pair et que c'est 2 fois une $r$-forme de Pfister si $r$ est impair.)

Supposons d'abord que $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne. D'après le th. 6.1.1 (b) on a $q_L^1 \cong q_M$, et il faut donc montrer que $q_M$ est une $r$-forme de Pfister. Or, puisque $S$ est produit de $r$ groupes cycliques d'ordre 2, on peut écrire $M$ comme produit tensoriel de $r$ algèbres quadratiques $L_i$ $(i = 1, \dots, r)$. La forme $q_M$ est le produit tensoriel des formes $q_{L_i}$. Mais la forme trace d'une algèbre quadratique de discriminant $d$ est $\langle 2, 2d \rangle = \langle 2 \rangle \otimes \langle 1, d \rangle = \langle 2 \rangle \otimes \langle\langle d \rangle\rangle$. Si l'on note $d_i$ le discriminant de $L_i$, on a donc

$$q_M \cong \langle 2^r \rangle \otimes \langle\langle d_1 \rangle\rangle \otimes \cdots \otimes \langle\langle d_r \rangle\rangle \cong \langle 2^r \rangle \otimes \langle\langle d_1, \dots d_r \rangle\rangle. \tag{6.2.1}$$

Cela démontre le théorème dans le cas considéré.

Le cas général se ramène au précédent par la méthode du §2. D'après la prop. 2.1.1, il existe une extension de degré impair $K'$ de $K$ et une $S$-algèbre galoisienne $M$ tels que $K' \otimes_K M = \mathrm{Ind}_S^G M$. Donc $2^r q_L^1$ est une $r$-forme de Pfister sur $K'$; d'après la prop. 4.4.1 c'est une $r$-forme de Pfister sur $K$.

*Remarque.* Il y a intérêt pour la suite à préciser la structure du $G$-espace quadratique $q_M$:

Notons $\phi_M$ l'homomorphisme de $G_K$ dans $S$ qui définit la $S$-algèbre galoisienne $M$. Si $x \in S'$, le composé $x \circ \phi_M$ est un homomorphisme de $G_K$ dans $\{\pm 1\}$, donc correspond à un élément $a_x$ de $K^*/K^{*2}$; l'application $x \mapsto a_x$ est un homomorphisme de $S'$ dans $K^*/K^{*2}$. Si l'on note $M_x$ la $x$-composante de $M$ (au sens du n°5.2), on vérifie facilement que $M_x$ est un espace quadratique de dimension 1, isomorphe à $\langle 2^r a_x \rangle$. Avec les notations du n°5.2, on peut donc écrire:

$$M \cong \bigoplus_{x \in S'} \langle 2^r a_x \rangle \otimes 1_x, \tag{6.2.2}$$

et en particulier

$$2^r q_M \cong \bigoplus_{x\in S'} \langle a_x\rangle. \tag{6.2.3}$$

Si $(x_1,\dots,x_r)$ est une base de $S'$ (vu comme espace vectoriel sur $\mathbf{F}_2$), l'algèbre $M$ est isomorphe au quotient de l'algèbre de polynômes $K[T_1,\dots,T_r]$ par l'idéal engendré par les $T_i^2 - a_{x_i}$. L'action de $S$ sur $M$ est donnée par

$$s(T_i) = x_i(s)T_i \qquad \text{pour } i = 1,\dots,r.$$

On a:

$$2^r q_M \cong \langle\langle a_{x_1},\dots,a_{x_r}\rangle\rangle. \tag{6.2.4}$$

**6.3. Décomposition de la forme $q_L^1$.** Nous nous proposons maintenant de *décomposer* la forme quadratique $q_L^1$ en somme orthogonale de formes quadratiques $q_L^1(\omega)$ indexées par les *orbites* $\omega$ de $N$ dans $S'$ (cf. n°5.3):

$$q_L^1 \cong \bigoplus_{\omega\in\Omega} q_L^1(\omega). \tag{6.3.1}$$

Cette décomposition jouira des deux propriétés suivantes:

(6.3.2) Elle est invariante par extension du corps de base.

(6.3.3) Si $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne, $q_L^1(\omega)$ est la forme quadratique donnée par la $\omega$-composante du $S$-espace quadratique $q_M$ (cf. 5.3.1). Avec les notations de la fin du n° précédent, cela signifie que l'on a:

$$2^r q_L^1(\omega) = \bigoplus_{x\in\omega} \langle a_x\rangle. \tag{6.3.3$'$}$$

(Cela revient à dire que, dans la décomposition de 6.2.3, on regroupe les termes appartenant à une même orbite $\omega$.)

THÉORÈME 6.3.4. *Il est possible, d'une façon et d'une seule, de définir des formes quadratiques $q_L^1(\omega)$ ayant les propriétés 6.3.2 et 6.3.3 ci-dessus.*

Si $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne, *l'unicité* de la décomposition résulte de 6.3.3. Le cas général se ramène à celui-ci par extension de degré impair du corps de base, cf. 2.1.1.

Reste à prouver *l'existence*. Nous allons utiliser les formes quadratiques $F_{\omega,\omega'}$ définies au n°5.5. Rappelons que ces formes sont invariantes par extension des

scalaires et que leurs rangs $r(\omega,\omega')$ sont tels que $\det(r(\omega,\omega')) \equiv 1 \pmod 2$, cf. 5.5.5.

On peut considérer $L$, muni de $q_L$, comme un $S$-espace quadratique. Pour tout $x \in S'$, notons $L_x$ le sous-espace propre correspondant, et si $\omega \in \Omega$, posons $L_\omega = \oplus_{x\in\omega} L_x$.

Notons $a_\omega$ la restriction de $q_L$ à $L_\omega$.

PROPOSITION 6.3.5. (1) *Il existe une famille et une seule d'éléments $q_\omega$ ($\omega \in \Omega$) de $GrW_K^+$ telle que*

$$\bigoplus_{\omega\in\Omega} q_\omega \otimes F_{\omega,\omega'} \cong a_{\omega'} \text{ pour tout } \omega' \in \Omega. \tag{6.3.6}$$

(2) *Les formes $q_L^1(\omega) = 2^r q_\omega$ satisfont aux propriétés (6.3.2) et (6.3.3) du th. 6.3.4.*

*Démonstration de* (1): D'après le théorème 4.3.1, il suffit de voir que le système d'équations ci-dessus est résoluble sur une extension de degré impair de $K$. Cela permet de supposer que $L$ est de la forme $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne. Avec les notations du §5, le $S$-espace quadratique $L$ est isomorphe à

$$A(V) = \mathrm{Res}_S^G \mathrm{Ind}_S^G V,$$

où $V = M$ vu comme $S$-espace quadratique.

D'après 5.5.6, on a

$$a_{\omega'} \cong \bigoplus_{\omega\in\Omega} V_\omega \otimes F_{\omega,\omega'},$$

où $V_\omega$ est la forme quadratique définie par la $\omega$-composante de $V$. Cela montre que les $V_\omega$ satisfont au système d'équations de la proposition, donc que ce système a une solution.

*Démonstration de* (2): La propriété (6.3.2) est évidente. Vérifions (6.3.3). Supposons donc que $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne. On doit montrer que

$$q_\omega \cong \bigoplus_{x\in\omega} \langle a_x \rangle.$$

Vu la définition des $q_\omega$, il suffit de voir que les formes

$$V_\omega = \bigoplus_{x\in\omega} \langle a_x \rangle$$

satisfont à la même équation que 6.3.6, i.e.

$$\bigoplus_{\omega\in\Omega} V_\omega \otimes F_{\omega,\omega'} \cong a_{\omega'} \qquad \text{pour tout } \omega' \in \Omega.$$

Or cela résulte de la définition de $F_{\omega,\omega'}$ et de la formule 5.5.4.

**6.4. Un critère.** On conserve les notations du n° précédent. En particulier, on note $q_L^1(\omega)$ les formes quadratiques du th. 6.3.4.

THÉORÈME 6.4.1. *Soient $L$, $L'$ deux $G$-algèbres galoisiennes. Il y a équivalence entre:*

(1) *Les $G$-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes.*

(2) $q_L^1(\omega) \cong q_{L'}^1(\omega)$ *pour tout* $\omega \in \Omega$.

Quitte à faire une extension de degré impair, on peut supposer qu'il existe des $S$-algèbres galoisiennes $M$ et $M'$ telles que $L = \mathrm{Ind}_S^G M$ et $L' = \mathrm{Ind}_S^G M'$. L'équivalence (1) $\Leftrightarrow$ (2) résulte alors du th. 5.3.1.

THÉORÈME 6.4.2. *Soit $L$ une $G$-algèbre galoisienne. Alors $L$ a une base normale autoduale si et seulement si, pour tout $\omega \in \Omega$, la forme quadratique $2^r q_L^1(\omega)$ est isomorphe à la forme unité $\langle 1, \ldots, 1\rangle$.*

En effet, pour une $G$-algèbre galoisienne décomposée cette forme quadratique est isomorphe à $\langle 1, \ldots, 1\rangle$. On conclut par le th. 6.4.1.

**6.5. Application: la forme trace de l'algèbre $L^H$.** Soit $H$ un sous-groupe de $G$, et soit $E = L^H$ la sous-algèbre de $L$ fixée par $H$. D'après le n°1.4, la forme $q_E$ ne dépend que de $H$, et de la $G$-forme quadratique $(L, q_L)$. Vu le th. 6.4.1, il est donc possible d'expliciter $q_E$ en fonction de $H$ et des $q_L^1(\omega)$. C'est ce que nous allons faire.

Soit $S\backslash G/H$ l'ensemble des doubles classes de $G$ modulo $S$ et $H$, et soit $T$ un ensemble de représentants de $S\backslash G/H$ dans $G$. Si $t \in T$, posons $S(t) = S \cap tHt^{-1}$, et notons $2^{r(t)}$ l'ordre du groupe $S(t)$. Pour tout $\omega \in \Omega$, choisissons $x_\omega \in \omega$, et notons $S_\omega$ le sous-groupe de $S$ noyau de $x_\omega$. Définissons une forme quadratique $Q_\omega$ par

$$Q_\omega = \bigoplus_{S(t)\subset S_\omega} \langle 2^{r(t)}\rangle, \tag{6.5.1}$$

où la sommation porte sur les $t \in T$ tels que $S(t) \subset S_\omega$ (i.e. tels que la restriction de $x_\omega$ à $S(t)$ égale à 1).

On vérifie facilement que l'on a:

$$\mathrm{rang}(Q_\omega) = \begin{cases} |T| = |S\backslash G/H| & \text{si } \omega = \{1\}, \\ |S_\omega\backslash G/H| - |S\backslash G/H| & \text{sinon.} \end{cases} \tag{6.5.2}$$

THÉORÈME 6.5.3. *On a* $q_E = \oplus_{\omega\in\Omega} Q_\omega \otimes q_L^1(\omega)$.

*Exemple.* Si $H$ est *d'ordre impair*, on a $S(t) = \{1\}$ pour tout $t \in T$. Il en résulte que $Q_\omega$ est isomorphe à $m_H = \langle 1, \dots, 1\rangle$, où $m_H = |T| = 2^{-r}(G : H)$. Le th. 6.5.3 donne alors

$$q_E = m_H \otimes \Big(\bigoplus_{\omega\in\Omega} q_L^1(\omega)\Big) = m_H \otimes q_L^1;$$

on retrouve la formule du th. 6.1.2.

*Démonstration du th. 6.5.3.* Quitte à remplacer $K$ par une extension de degré impair, on peut supposer que $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne. Faisons cette hypothèse.

LEMME 6.5.4. *L'algèbre $E = L^H$ est isomorphe au produit $\prod_{t\in T} M^{S(t)}$.*

On peut identifier $L$ à l'algèbre des fonctions $f : G \to M$ telles que

(i) $f(sx) = sf(x)$ si $s \in S$, $x \in G$, cf. n°1.3.2.

On a $f \in L^H$ si et seulement si:

(ii) $f(xh) = f(x)$ si $h \in H$ et $x \in G$.

Si $t \in T$ et $s \in S(t)$ il résulte de (i) et (ii) que l'on a:

$$sf(t) = f(st) = f(t.t^{-1}st) = f(t), \quad \text{puisque } t^{-1}st \in H.$$

On a donc $f(t) \in M^{S(t)}$, d'où un homomorphisme $L^H \to \prod_{t\in T} M^{S(t)}$, et l'on vérifie facilement que c'est un isomorphisme.

Posons $E(t) = M^{S(t)}$. Le lemme ci-dessus entraîne:

$$q_E \cong \bigoplus_{t\in T} q_{E(t)}. \tag{6.5.5}$$

Reprenons les notations du n°6.2: notons $\phi_M$ l'homomorphisme $G_K \to S$ définissant $M$, et, pour tout $x \in S'$, soit $a_x \in K^*/K^{*2}$ l'élément correspondant à $x\circ\phi_M : G_K \to S \to \{\pm 1\}$. Si $S_1$ est un sous-groupe de $S$ de rang $r_1$, la forme trace de $M^{S_1}$ est isomorphe à $\oplus_{x|S_1=1}\langle 2^{r-r_1}a_x\rangle$. En appliquant ceci aux sous-groupes $S(t)$ de $S$, et en utilisant (6.5.5), on en déduit:

$$q_E \cong \bigoplus_{t\in T}\ \bigoplus_{x|S(t)=1} \langle 2^{r-r(t)}a_x\rangle,$$

ou encore

$$q_E \cong \bigoplus_{x\in S'} Q_x \otimes \langle 2^r a_x\rangle, \text{ avec } Q_x = \bigoplus_{x|S(t)=1} \langle 2^{r(t)}\rangle.$$

Si $x \in \omega$, on a $Q_x = Q_{x_\omega} = Q_\omega$, cf. (6.5.1). La formule ci-dessus peut donc se récrire sous la forme

$$q_E \cong \bigoplus_{\omega\in\Omega} Q_\omega \otimes \Big(\bigoplus_{x\in\omega} \langle 2^r a_x\rangle\Big). \tag{6.5.6}$$

D'après (6.3.3'), on a $\oplus_{x\in\omega}\langle 2^r a_x\rangle = q_L^1(\omega)$. On en déduit la formule cherchée:

$$q_E \cong \bigoplus_{\omega\in\Omega} Q_\omega \otimes q_L^1(\omega).$$

*Remarque*. Dans la définition de $Q_\omega$ on peut remplacer $\langle 2^{r(t)}\rangle$ par $\langle 1\rangle$ si $r(t)$ est pair, et par $\langle 2\rangle$ si $r(t)$ est impair. Il en résulte que $Q_\omega$ est de la forme $\langle 1,\dots,1,2,\dots,2\rangle$. Si le nombre des "2" est pair, on peut tout les remplacer par des "1", vu la formule $\langle 2,2\rangle = \langle 1,1\rangle$; on obtient alors la forme unité $\langle 1,\dots,1\rangle$. De même, si le nombre des "2" est impair, on obtient $\langle 1,\dots,1,2\rangle$. D'où la description suivante de $Q_\omega$:

On a:

(6.5.7) $Q_\omega \cong \langle 1,\dots,1\rangle$ si le nombre des $t \in T$ tels que $r(t)$ soit impair et $S(t) \subset \operatorname{Ker} x_\omega$ est pair ;

$Q_\omega \cong \langle 1,\dots,1,2\rangle$ sinon.

En particulier:

COROLLAIRE 6.5.8. *Si 2 est un carré dans K, on a*

$$q_E = \bigoplus_{\omega\in\Omega} m_\omega \otimes q_L^1(\omega), \quad \textit{avec } m_\omega = \operatorname{rang}(Q_\omega), \text{ cf. (6.5.2).}$$

**6.6. Le cas d'une action transitive.** Nous avons vu au n°5.6 que le nombre d'orbites de $N$ sur $S$ et sur $S'$ est le même. En particulier, les propriétés suivantes sont équivalentes:

(i) $N$ opère transitivement sur $S-\{1\}$;

(ii) $N$ opère transitivement sur $S'-\{1\}$.

Ces propriétés sont aussi équivalentes à la suivante (cf. [10], p. 418, Hilfsatz 2.5):

(iii) Les éléments d'ordre 2 de $G$ sont conjugués entre eux.

THÉORÈME 6.6.1. *Supposons* (i) *vérifiée. Soient L et L' deux G-algèbres galoisiennes. Il y a équivalence entre:*

(1) *Les G-formes quadratiques* $(L, q_L)$ *est* $(L', q_{L'})$ *sont isomorphes.*

(2) *Les r-formes de Pfister* $2^r q_L^1$ *et* $2^r q_{L'}^1$ *sont isomorphes.*

(3) *Les formes quadratiques* $q_L$ *et* $q_{L'}$ *sont isomorphes.*

Il est clair que l'on a (1) $\Rightarrow$ (3) $\Rightarrow$ (2). Il suffit donc de montrer que (2) $\Rightarrow$ (1). Or $\Omega$ a deux éléments (si $r \geq 1$), à savoir $\omega_1 = \{1\}$ et $\omega_2 = S' - \{1\}$. Il est clair que

$$q_L^1(\omega_1) \cong \langle 2^r \rangle \cong q_{L'}^1(\omega_1).$$

Comme $q_L^1(\omega_1) \oplus q_L^1(\omega_2) \cong q_L^1$ , et $q_{L'}^1(\omega_1) \oplus q_{L'}^1(\omega_2) \cong q_{L'}^1$, cela entraîne que $q_L^1(\omega_2) \cong q_{L'}^1(\omega_2)$, et l'on applique le th. 6.4.2.

*Remarque*. L'intérêt du th. 6.6.1 est qu'il ramène la question de l'isomorphisme des $G$-formes quadratiques associées à deux algèbres galoisiennes à celle de l'isomorphisme des formes de Pfister correspondantes. Lorsque $r \leq 4$, ceci peut se traduire en termes cohomologiques, cf. §§ 7,8.

THÉORÈME 6.6.2. *Supposons* (i) *vérifiée. Il y a équivalence entre:*

(1) *L a une base normale autoduale.*

(2) *La r-forme de Pfister* $2^r q_L^1$ *est isomorphe à* $\langle\langle 1, \ldots, 1\rangle\rangle$.

(3) $q_L^1$ *est isomorphe à la forme unité de rang* $2^r$.

(4) $q_L$ *est isomorphe à la forme unité de rang* $n = m.2^r$.

L'équivalence (2) $\Leftrightarrow$ (3) résulte de ce que $\langle 2, 2\rangle \cong \langle 1, 1\rangle$. Le reste est une conséquence du th. 6.6.1.

*Application: la forme trace de* $L^H$. Revenons aux notations du n°6.5: $H$ est un sous-groupe de $G$, $E = L^H$, et $T$ est un système de représentants de $S\backslash G/H$. La description de $q_E$ donnée par le th. 6.5.3 se simplifie notablement (du fait qu'il n'y a que deux orbites $\omega$ à considérer, cf. ci-dessus). Si l'on convient de noter $q$ la $r$-forme de Pfister $2^r q_L^1$, on a:

THÉORÈME 6.6.3. *Soit e le nombre des* $t \in T$ *tels que* $r - r(t)$ *soit impair. Il existe des entiers* $u, v \geq 0$ *(avec* $v = 0$ *si* $r = 0$*) tels que:*

$$u + v = |S\backslash G/H| \quad \text{et} \quad u + 2^r v = (G : H).$$

*On a:*

$$q_E \cong u \otimes \langle 1\rangle \oplus \begin{cases} v \otimes q & \text{si } e \text{ est pair} \\ ((v-1) \oplus \langle 2\rangle) \otimes q & \text{si } e \text{ est impair.} \end{cases}$$

Cela se déduit sans difficultés du th. 6.5.3, compte tenu de ce que

$$q_L^1(\omega) \cong \langle 2^r \rangle \quad \text{si } \omega = \{1\},$$

et

$$q_L^1(\omega) \oplus \langle 2^r \rangle \cong \langle 2^r \rangle \otimes q \quad \text{si } \omega = S' - \{1\}.$$

*Exemples.* 1) Prenons $G = \mathbf{PSL}_2(\mathbf{F}_{11})$ et $H$ isomorphe au groupe alterné $A_5$, de sorte que $(G : H) = 11$. On a $r = 2$. Les orbites de $S$ sur $G/H$ sont d'ordres 1,2,2,2,4. D'où $|S\backslash G/H| = 5$, et les $r(t)$ sont égaux à 2,1,1,1 et 0. On a $u = 3$, $v = 2$, $e = 3$, d'où

$$q_E \cong \langle 1, 1, 1 \rangle \oplus \langle 1, 2 \rangle \otimes q.$$

Si $q \cong \langle\langle a, b \rangle\rangle$, cela donne:

$$q_E \cong \langle 1, 1, 1, 1, 2, a, 2a, b, 2b, ab, 2ab \rangle.$$

2) Prenons $G = \mathbf{SL}_2(\mathbf{F}_8)$, et choisissons pour $H$ un sous-groupe de Borel de $G$, de sorte que $(G : H) = 9$. On a $r = 3$. Les orbites de $S$ sur $G/H$ sont d'ordres 1 et 8. D'où $|S\backslash G/H| = 2$ et les $r(t)$ sont égaux à 3 et 0. On a $u = 1$, $v = 1$, $e = 1$, d'où

$$q_E \cong \langle 1 \rangle \oplus \langle 2 \rangle \otimes q.$$

Si $q \cong \langle\langle a, b, c \rangle\rangle$, cela donne:

$$q_E \cong \langle 1, 2, 2a, 2b, 2c, 2ab, 2bc, 2ac, 2abc \rangle.$$

3) Prenons $G = \mathbf{PSL}_2(\mathbf{F}_{13})$, $H$ = sous-groupe de Borel de $G$. On a $(G : H) = 14$, $|S\backslash G/H| = 5$, $r(t) = 0, 0, 1, 1, 1$, $u = 2$, $v = 3$, $e = 1$, d'où

$$q_E \cong \langle 1, 1 \rangle \oplus \langle 1, 1, 2 \rangle \otimes q.$$

Si $q \cong \langle\langle a, b \rangle\rangle$, cela donne:

$$q_E \cong \langle 1, 1, 1, 1, 2, a, a, 2a, b, b, 2b, ab, ab, 2ab \rangle.$$

**7. Invariants cohomologiques.** On a vu dans les §§ précédents que l'existence de bases normales autoduales est liée à la structure de certaines *formes quadratiques* attachées à l'algèbre galoisienne considérée. Or, en basse dimension,

l'équivalence de deux formes quadratiques (par exemple de deux formes de Pfister) peut se lire sur leurs *invariants cohomologiques*. Le but de ce § est de préciser comment se calculent ces invariants.

**7.1. Rappels sur la cohomologie des groupes finis.** Soient $G$ un groupe fini, $p$ un nombre premier, $S$ un $p$-sous-groupe de Sylow de $G$ et $N$ le normalisateur de $S$ dans $G$. On dit que $N$ *contrôle la fusion de* $S$ si la propriété suivante est satisfaite:

(F) *Quels que soient le sous-groupe* $S_1$ *de* $S$ *et l'élément* $g \in G$ *tels que* $gS_1g^{-1} \subset S$, *il existe* $n \in N$ *tel que* $nxn^{-1} = gxg^{-1}$ *pour tout* $x \in S_1$ (d'où, en particulier, $nS_1n^{-1} = gS_1g^{-1}$).

Soit $A$ un $G$-module; si $i \geq 1$, notons $H^i(G,A)_p$ la composante $p$-primaire du groupe de cohomologie $H^i(G,A)$. On sait (cf. e.g. [7], chap. XII, §10) que l'application de restriction

$$\text{Res} : H^i(G,A)_p \to H^i(S,A)_p$$

est *injective*, et que son image est contenue dans le sous-espace $H^i(S,A)_p^N$ de $H^i(S,A)_p$ formé des éléments fixés par l'action de $N/S$. De plus:

PROPOSITION 7.1.1. *Faisons les deux hypothèses suivantes:*

(a) *Le normalisateur* $N$ *de* $S$ *contrôle la fusion de* $S$.

(b) *L'action de* $G$ *sur le* $G$*-module* $A$ *est triviale.*

*Alors l'application de restriction* Res : $H^i(G,A)_p \to H^i(S,A)_p$ *applique isomorphiquement* $H^i(G,A)_p$ *sur le sous-espace* $H^i(S,A)_p^N$ *de* $H^i(S,A)_p$ *formé des éléments fixés par* $N$.

Cela résulte de la caractérisation des éléments "stables" de $H^i(S,A)_p$ donnée dans [7], chap. XII, §10. En effet, l'image de Res est formée des éléments stables, et les hypothèses (a) et (b) entraînent que tout élément invariant par $N$ est stable.

*Remarques.* 1) Il est bien connu (Burnside) que l'hypothèse "$N$ contrôle la fusion de $S$" est satisfaite lorsque $S$ est abélien. (En effet, avec les notations de (F), on remarque que $S$ et $g^{-1}Sg$ sont des $p$-groupes de Sylow du centralisateur $C$ de $S_1$ dans $G$. En appliquant le théorème de Sylow à $C$, on en déduit qu'il existe $c \in C$ tel que $cSc^{-1}$ soit égal à $g^{-1}Sg$. L'élément $n = gc$ convient.). De même, cette hypothèse est aussi satisfaite lorsque $p = 2$ et que $S$ est un groupe quaternionien d'ordre 8. Elle ne l'est pas toujours lorsque $S$ est un groupe diédral (exemple: $G = A_6$, $S = D_4$).

2) On peut dans certains cas supprimer l'hypothèse (b), par exemple lorsque $S$ a la "propriété d'intersection triviale": $S \cap gSg^{-1} = \{1\}$ pour tout $g \in G - N$.

**7.2. Construction de la classe fondamentale: le cas de $S$.** A partir de maintenant on ne s'intéresse qu'à la cohomologie (mod 2). Si $\Gamma$ est un groupe fini (ou profini) quelconque, on écrit $H^i(\Gamma)$ à la place de $H^i(\Gamma, \mathbf{Z}/2\mathbf{Z})$, et l'on note $H^\bullet(\Gamma)$ l'algèbre de cohomologie $\oplus_{i\geq 0} H^i(\Gamma)$.

Soit $S$ un groupe abélien élémentaire d'ordre $2^r$, $r \geq 1$. On a

$$H^1(S) = \mathrm{Hom}(S, \mathbf{Z}/2\mathbf{Z});$$

c'est un $\mathbf{F}_2$-espace vectoriel de dimension $r$, et $H^\bullet(S)$ s'identifie à *l'algèbre symétriqu* de cet espace. En particulier, $H^\bullet(S)$ est isomorphe à une *algèbre de polynômes* $\mathbf{F}_2[X_1, \ldots, X_r]$ en $r$ générateurs.

PROPOSITION 7.2.1. *Il existe un élément $z$ de $H^r(S)$ ayant la propriété suivante:*

$(*)$ *La restriction de $z$ à tout sous-groupe d'ordre 2 de $S$ est $\neq 0$.*

Cela revient à dire qu'il existe un polynôme homogène $Z(X_1, \ldots, X_r)$, de degré $r$, à coefficients dans $\mathbf{F}_2$, tel que l'on ait:

$(**)$ $Z(x_1, \ldots, x_r) = 1$ *pour tout* $(x_1, \ldots, x_r) \in (\mathbf{F}_2)^r - \{0\}$.

*Exemples.* Pour $r = 1$, $Z = X_1$; pour $r = 2$, $Z = X_1^2 + X_1X_2 + X_2^2$; pour $r = 3$, $Z = X_1^3 + X_2^3 + X_3^3 + X_1^2X_2 + X_1^2X_3 + X_2^2X_3 + X_1X_2X_3$.

Voici deux constructions possibles d'un tel polynôme $Z$:

(7.2.1.a) On prend pour $z$ la *forme norme* d'une extension $\mathbf{F}_{2^r}/\mathbf{F}_2$ de degré $r$.

(7.2.1.b) Pour tout partie non vide $I$ de $\{1, \ldots, r\}$, notons $X_I$ le monôme $\prod_{i\in I} X_i$, et posons $Z_I = X_I . X_{i(I)}^{r-|I|}$, où $i(I)$ est le plus petit élément de $I$. Soit $Z = \sum_{I\neq\emptyset} Z_I$. Le polynôme $Z$ convient. En effet, $Z_I$ et $X_I$ prennent les mêmes valeurs sur $(\mathbf{F}_2)^r$. Si $(x_1, \ldots, x_r)$ est un élément non nul de $(\mathbf{F})_2)^r$, on a donc $Z(x_1, \ldots, x_r) = \sum_{I\neq\emptyset} \prod_{j\in I} x_j = (1 + x_1) \ldots (1 + x_r) - 1 = 1$, puisque l'un des facteurs $(1 + x_j)$ est égal à 2, c'est-à-dire à 0.

*Remarque.* On vérifie facilement que l'élément $z$ de la prop. 7.2.1 est *unique* si $r \leq 2$. Il n'en est plus ainsi pour $r \geq 3$. Pour préciser ceci, introduisons l'idéal homogène $J$ de $H^\bullet(S)$ engendré par les éléments $x^2y + xy^2$, où $x$ et $y$ parcourent $H^1(S)$.

PROPOSITION 7.2.2. *Si $z$ et $z'$ sont deux éléments de $H^\bullet(S)$ satisfaisant à la propriété $(*)$ de* 7.2.1, *on a $z \equiv z'$* (mod $J$).

Cela résulte de la proposition suivante:

PROPOSITION 7.2.3. *Soit $t \in H^i(S)$, $i > 0$. Pour que $t$ appartienne à l'idéal $J$ il faut et il suffit que la restriction de $t$ à tous les sous-groupes d'ordre 2 de $S$ soit 0.*

Lorsqu'on traduit cet énoncé en termes de polynômes homogènes, on voit qu'il résulte du lemme élémentaire suivant (dont la démonstration est laissée au lecteur):

LEMME 7.2.4. *Soit $k$ un corps fini à $q$ éléments. L'idéal homogène des polynômes en $X_1, \ldots, X_r$ qui s'annulent sur le sous-ensemble $\mathbf{P}_{r-1}(k)$ de l'espace projectif $\mathbf{P}_{r-1}$ est engendré par les $X_i^q X_j - X_i X_j^q$, pour $i < j$.*

**7.3. Construction de la classe fondamentale: le cas de $G$.** On revient maintenant aux hypothèses du n°6.2:

$S$ est un 2-sous-groupe de Sylow de $G$ et *l'on suppose que $S$ est abélien élémentaire d'ordre $2^r$, $r > 0$.* Comme aux n$^{os}$ précédents, on note $N$ le normalisateur de $S$ dans $G$. Nous allons voir que la prop. 7.2.1 reste valable pour $G$. Plus précisément:

THÉORÈME 7.3.1. *Il existe un élément $z$ de $H^r(G)$ ayant la propriété suivante:*

(∗) *La restriction de $z$ à tout sous-groupe d'ordre 2 de $G$ est $\neq 0$.*

Soit $z_S \in H^r(S)$ un élément ayant la propriété de la prop. 7.2.1. Le groupe $W = N/S$ opère sur $S$, donc aussi sur $H^r(S)$; si $w \in W$, notons $w(z_S)$ le transformé de $z_S$ par $w$. Posons

$$\bar{z} = \sum_{w \in W} w(z_S).$$

Il est clair que l'élément $\bar{z}$ de $H^r(S)$ est invariant par $W$. D'après la prop. 7.1.1 c'est donc la restriction d'un élément $z$ de $H^r(G)$. Cet élément est unique. Il répond à la question. En effet, soit $S_1$ un sous-groupe d'ordre 2 de $G$; on doit vérifier que la restriction de $z$ à $S_1$ est $\neq 0$. Quitte à conjuguer $S_1$, on peut supposer que $S_1$ est contenu dans $S$. La restriction de $z$ à $S_1$ est alors égale à celle de $\bar{z}$, c'est-à-dire à la somme de celles des $w(z_S)$. Mais chaque $w(z_S)$ a pour restriction à $S_1$ l'unique élément non nul de $H^r(S_1)$; comme le nombre des $w$ est impair, la somme en question est bien $\neq 0$. (*Variante*: définir $z$ comme $\mathrm{Cor}_S^G(z_S)$.)

**7.4. Rappels de cohomologie galoisienne.** Il s'agit de notations standard, que nous rappelons pour la commodité du lecteur (cf. [1], [14], [18], [19]).

**7.4.1. Cohomologie** (mod 2)**.** On pose:

$$H^n(K) = H^n(G_K, \mathbf{Z}/2\mathbf{Z}), \text{ où } G_K = \mathrm{Gal}(K_s/K).$$

On a $H^1(K) = K^*/K^{*2}$ (théorie de Kummer); si $a \in K^*$, on note $(a)$ son image dans $H^1(K)$; on a $(ab) = (a) + (b)$ et $(a) = 0$ si et seulement si $a$ est un carré.

Le groupe $H^2(K)$ peut être identifié à $\mathrm{Br}_2(K)$, noyau de la multiplication par 2 dans le groupe de Brauer $\mathrm{Br}(K)$. Si $a, b \in K^*$, le cup-produit $(a)(b) \in H^2(K)$ correspond à la classe de l'algèbre de quaternions $(a, b)$. On a $(a)(b) = 0$ si et seulement si cette algèbre est décomposée, i.e. si $b$ est une norme de l'extension $K(\sqrt{a})/K$. En particulier:

$$(-a)(a) = 0 \quad \text{pour tout } a \in K^*;$$

ce que l'on peut aussi écrire:

$$(-1)x = x^2 \text{ pour tout } x \in H^1(K). \tag{7.4.1.1}$$

**7.4.2. Invariants des formes quadratiques: les classes de Stiefel-Whitney.** Soit $q = \langle a_1, \ldots, a_n \rangle$ une forme quadratique, et soit $k$ un entier $\geq 0$. Posons:

$$w_k(q) = \sum_{i_1 < \cdots < i_k} (a_{i_1}) \ldots (a_{i_k}) \quad \text{dans } H^k(K).$$

La classe de cohomologie $w_k(q)$ ne dépend que de $q$ et de $k$, mais pas de la décomposition de $q$ choisie. C'est la *k-ème classe de Stiefel-Whitney de q*.

Pour $k = 1$, on a $w_1(q) = (d)$, où $d$ est le *discriminant* de $q$, vu comme élément de $K^*/K^{*2}$. Pour $k = 2$, $w_2(q)$ est *l'invariant de Hasse-Witt* de $q$.

**7.4.3. L'invariant d'Arason d'une forme de Pfister.** Soit $q = \langle\langle a_1, \ldots, a_r \rangle\rangle$ une $r$-forme de Pfister (cf. n°4.4). Posons:

$$e(q) = (-a_1) \ldots (-a_r) \quad \text{dans } H^r(K).$$

D'après un théorème d'Arason ([1], §1), $e(q)$ ne dépend que de $q$. Si $q'$ est une autre $r$-forme de Pfister, on a

$$e(q) = e(q') \Longleftrightarrow q \cong q'$$

pourvu que $r \leq 4$, cf. [2], p. 652; les conjectures de Milnor [14] entraîneraient que ceci reste vrai pour tout $r$.

**7.5. L'invariant d'une $G$-algèbre galoisienne.** Les hypothèses sur $G$ et $S$ sont celles des n$^{os}$ 6.2 et 7.3. Soit $L$ une $G$-algèbre galoisienne, définie par un homomorphisme

$$\phi_L : G_K \to G.$$

Si $z \in H^n(G)$, on note $z_L$ la classe de cohomologie $\phi_L^*(z) \in H^n(K)$, cf. n°2.2.

LEMME 7.5.1. *Si la restriction de z à tous les sous-groupes d'ordre 2 de G est nulle, on a* $z_L = 0$.

(Autrement dit, $z$ est *négligeable*, au sens de [21], §7.)

Si $K'$ est une extension de degré impair de $K$, l'application $H^n(K) \to H^n(K')$ est injective. Or on peut choisir $K'$ de telle sorte que, sur $K'$, l'algèbre $L$ soit induite d'une $S$-algèbre galoisienne, cf. 2.1.1. Cela permet de réduire la question au cas où $G = S$. Mais, dans ce cas, la prop. 7.2.3 montre que $z$ appartient à l'idéal homogène $J$ engendré par les $x^2y + xy^2$, avec $x, y \in H^1(G)$. Il suffit donc de prouver que l'on a

$$(x^2y + xy^2)_L = 0 \text{ dans } H^3(K).$$

Or cela résulte de la relation 7.4.1.1:

$$(x^2y + xy^2)_L = (-1)x_Ly_L + x_L(-1)y_L = 2.(-1)x_Ly_L = 0.$$

Soit maintenant $z$ un élément de $H^r(G)$ ayant la propriété $(*)$ du th. 7.3.1: la restriction de $z$ à tout sous-groupe d'ordre 2 de $G$ est $\neq 0$. Il résulte du lemme ci-dessus que *l'élément* $z_L$ *de* $H^r(K)$ *ne dépend pas du choix de* $z$. C'est un *invariant* de la $G$-algèbre galoisienne $L$. Nous allons voir que cet invariant est étroitement lié à la $r$-forme de Pfister $2^r q_L^1$ du n°6.2:

THÉORÈME 7.5.2. *L'invariant d'Arason* $e(2^r q_L^1)$ *de la r-forme de Pfister* $2^r q_L^1$ *est égal à* $z_L + (-1)\dots(-1)$.

(Rappelons, cf. 7.4.3, que cet invariant appartient à $H^r(K)$.)

Commençons par démontrer ce théorème *dans le cas particulier où* $G = S$, auquel cas $q_L^1 = q_L$. Soit $(x_1, \dots, x_r)$ une base du groupe $S' = H^1(S)$. Chacun des $(x_i)_L$ peut être identifié à un élément $a_{x_i}$ de $K^*/K^{*2}$, et l'on a

$$2^r q_L \cong \langle\langle a_{x_1}, \dots, a_{x_r} \rangle\rangle, \text{ cf. (6.2.4).}$$

On a donc:

$$e(2^r q_L) = (-a_{x_1})\dots(-a_{x_r}) = \prod_{i=1}^{i=r} ((-1) + (x_i)_L).$$

Pour toute partie non vide $I$ de $\{1, \dots, r\}$, posons $x_I = \prod_{i \in I} x_i$. Notons $u$ l'élément $(-1)$ de $H^1(K)$. La formule ci-dessus s'écrit:

$$e(2^r q_L) = u^r + \sum_{I \neq \emptyset} u^{r-|I|} x_I.$$

Pour tout $I \neq \emptyset$, soit $i = i(I)$ le plus petit élément de $I$. D'après la formule (7.4.1.1), on a $u^k xy = x^{k+1}y$ pour tout $x, y \in H^1(K)$ et $k \geq 0$. En particulier:

$$u^{r-|I|}(x_I)_L = ((x_i)_L)^{r-|I|}(x_I)_L.$$

D'où:

$$\begin{aligned} e(2^r q_L) &= u^r + \sum_{I \neq \emptyset} ((x_i)_L)^{r-|I|}(x_I)_L \\ &= u^r + Z((x_1)_L, \ldots, (x_r)_L), \end{aligned}$$

où $Z$ est le polynôme construit dans (7.2.1.b). Comme on peut prendre pour $z$ la classe $Z(x_1, \ldots, x_r)$, on a

$$z_L = Z((x_1)_L, \ldots, (x_r)_L),$$

ce qui démontre la formule voulue dans le cas particulier considéré.

Le *cas général* se déduit de celui que nous venons de traiter. En effet, il suffit de vérifier la formule

$$e(2^r q_L^1) = u^r + z_L$$

après une extension de degré impair du corps de base. Cela permet de supposer (cf. 2.1.1) que $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne, et l'on a alors $q_L^1 \cong q_M$, cf. th. 6.1.1.(b). On est ainsi ramené au cas où $G = S$.

COROLLAIRE 7.5.3. *Pour que* $q_L$ (resp. $q_L^1$, resp. $2^r q_L^1$) *soit isomorphe à la forme unité de rang* $|G|$ (resp. *de rang* $2^r$), *il faut que l'on ait* $z_L = 0$ *et cela suffit si* $r \leq 4$.

L'invariant d'Arason de la $r$-forme de Pfister $\langle\langle 1, \ldots, 1\rangle\rangle$ est $(-1)\ldots(-1)$. Cela montre que $2^r q_L^1 \cong \langle\langle 1, \ldots, 1\rangle\rangle \Rightarrow z_L = 0$, et la réciproque est vraie si $r \leq 4$, cf. 7.4.3. On a d'autre part les équivalences:

$$q_L \cong \langle 1, \ldots, 1\rangle \Leftrightarrow q_L^1 \cong \langle 1, \ldots, 1\rangle \Leftrightarrow 2^r q_L^1 \cong \langle\langle 1, \ldots, 1\rangle\rangle.$$

(La première équivalence provient de ce que $q_L \cong m \otimes q_L^1$, avec $m$ impair, cf. th. 6.1.1.(a); la seconde est évidente si $r$ est pair, et, si $r$ est impair, elle résulte de $\langle 2, 2\rangle \cong \langle 1, 1\rangle$.)

THÉORÈME 7.5.4. *Supposons que* $r \leq 4$ *et que le normalisateur de* $S$ *opère transitivement sur* $S - \{1\}$. *Soient* $L$ *et* $L'$ *deux* $G$*-algèbres galoisiennes sur* $K$. *Il y a équivalence entre les propriétés suivantes:*

(a) *Les* $G$*-formes quadratiques* $(L, q_L)$ *et* $(L', q_{L'})$ *sont isomorphes.*

(b) *On a* $z_L = z_{L'}$ *dans* $H^r(K)$.

Cela résulte du th. 7.5.2, combiné avec le th. 6.5.1.

Le cas particulier où $L'$ est décomposée donne:

THÉORÈME 7.5.5. *Supposons que $r \leq 4$ et que le normalisateur de $S$ opère transitivement sur $S-\{1\}$. Soit $L$ une $G$-algèbre galoisienne sur $K$. Pour que $L$ ait une base normale autoduale il faut et il suffit que $z_L = 0$.*

*Remarques.* 1) L'hypothèse $r \leq 4$ pourrait être supprimée si les conjectures de Milnor [14] étaient démontrées.

2) Lorsque le normalisateur de $S$ opère transitivement sur $S-\{1\}$, on peut montrer que, si $x \in H^n(G)$, $n \geq 1$, on a, soit $x_L = 0$, soit $n \geq r$ et $x_L = u^{n-r} z_L$, avec $u = (-1)$. (La démonstration utilise les lemmes 7.5.1 et 7.2.4.) En particulier, les deux propriétés suivantes sont équivalentes:

(i) $z_L = 0$;

(ii) $x_L = 0$ pour toute classe de cohomologie $x$ de $G$ de degré $> 0$.

**7.6. Les classes de Stiefel-Whitney des formes $2^r q_L^1(\omega)$.** Les notations et hypothèses sont les mêmes que ci-dessus.

On a défini au n°6.3 une décomposition de $q_L^1$ en somme orthogonale de formes quadratiques $q_L^1(\omega)$, correspondant aux *orbites* $\omega$ de $N$ dans $S'$. Nous allons voir comment l'on peut calculer les *classes de Stiefel-Whitney* de ces formes.

Il est commode pour cela de définir $q_L^1(\alpha)$ pour toute partie $\alpha$ de $S'$ stable par $N$ au moyen de la formule

$$q_L^1(\alpha) = \bigoplus_{\omega \subset \alpha} q_L^1(\omega),$$

où la somme porte sur les orbites $\omega$ contenues dans $\alpha$.

Si $\beta$ est une partie de $S' = H^1(S)$, notons $w_\beta$ l'élément de $H^\bullet(S)$ produit des éléments de $\beta$ (vus comme éléments de $H^1(S)$); on a $\deg(w_\beta) = |\beta|$. Pour toute partie $\alpha$ de $S'$ et tout $k \geq 0$, définissons un élément $w(k, \alpha)$ de $H^k(S)$ par la formule:

$$w(k, \alpha) = \sum w_\beta,$$

où $\beta$ parcourt les parties à $k$ éléments de $\alpha$.

Supposons maintenant que $\alpha$ soit *stable par l'action de $N$*. Il est clair que $w(k, \alpha)$ est alors invariant par $N$; d'après la prop. 7.1.1, on peut *l'identifier à un élément de $H^k(G)$*.

PROPOSITION 7.6.1. *Soit $L$ une $G$-algèbre galoisienne sur $K$, soit $\alpha$ une partie de $S'$ stable par $N$ et soit $k$ un entier $\geq 0$. La $k$-ième classe de Stiefel-Whitney de la forme $2^r q_L^1(\alpha)$ est donnée par la formule:*

$$w_k(2^r q_L^1(\alpha)) = w(k, \alpha)_L.$$

La démonstration est analogue à celle du th. 7.5.2. On se ramène par une extension des scalaires de degré impair au cas où $L$ est la $G$-algèbre induite d'une $S$-algèbre galoisienne $M$. La formule (6.3.3′) montre que l'on a

$$2^r q_L^1(\alpha) \cong \bigoplus_{x\in\alpha} \langle a_x \rangle,$$

les notations étant celles du n°6.3. La formule à démontrer résulte alors de la définition de $w(k,\alpha)$ donnée ci-dessus.

*Remarque.* On passe des classes de Stiefel-Whitney de $2^r q_L^1(\alpha)$ à celles de $q_L^1(\alpha)$ grâce à la formule suivante (facile à vérifier en utilisant le fait que (2)(2) = 0):

$$w_k(2q) = \begin{cases} w_k(q) + (2).w_{k-1}(q) & \text{si } k \equiv \operatorname{rang}(q) \pmod 2 \\ w_k(q) & \text{sinon.} \end{cases}$$

**8. Exemples.** Ces exemples concernent le cas où un 2-sous-groupe de Sylow $S$ de $G$ est *abélien élémentaire*, cf. §§ 6,7. Les notations sont celles de ces §§; en particulier, l'ordre de $S$ est noté $2^r$ et son normalisateur est noté $N$.

On s'intéressera particulièrement au cas où $N$ agit *transitivement* sur $S-\{1\}$, i.e. où les éléments d'ordre 2 de $G$ sont conjugués entre eux. Ce cas sera appelé par la suite "le cas de fusion maximale."

**8.1. $r = 2$ et fusion maximale.** On suppose que $S$ est de type $(2,2)$ et que $N$ permute transitivement les trois éléments d'ordre 2 de $S$.

*Exemple.* $G = \mathbf{PSL}_2(\mathbf{F}_q)$, avec $q \equiv \pm 3 \pmod 8$; pour $q = 3$, cela donne $G = A_4$, et pour $q = 5$, $G = A_5$.

Si $(x,y)$ est une base de $H^1(S)$, le groupe $H^2(S)$ a un seul élément non nul invariant par $N$, à savoir $z_S = x^2 + y^2 + xy$. On en conclut que le groupe $H^2(G)$ est de dimension 1 sur $\mathbf{F}_2$, et a pour unique élément non nul un élément $z$ dont la restriction à $S$ est $z_S$ (cf. 7.1.1). Si $C$ est un groupe d'ordre 2, notons $\tilde{G}$ l'extension centrale de $G$ par $C$ correspondant à $z$; on a une suite exacte:

$$1 \to C \to \tilde{G} \to G \to 1.$$

Soit $\tilde{S}$ l'image réciproque de $S$ dans $\tilde{G}$; l'image réciproque dans $\tilde{S}$ d'un élément d'ordre 2 de $S$ est d'ordre 4. Ceci montre que $\tilde{S}$ est isomorphe au *groupe quaternionien* d'ordre 8.

(Lorsque $G = A_4$ ou $A_5$, $\tilde{G}$ est le groupe $\tilde{A}_4$ ou $\tilde{A}_5$; lorsque $G = \mathbf{PSL}_2(\mathbf{F}_q)$, $q \equiv \pm 3 \pmod 8$, $\tilde{G}$ est le groupe $\mathbf{SL}_2(\mathbf{F}_q)$.)

Soit $L$ une $G$-algèbre galoisienne sur $K$, définie par un homomorphisme $\phi_L : G_K \to G$.

THÉORÈME 8.1.1. *Les propriétés suivantes sont équivalentes:*

(1) *La $G$-algèbre $L$ a une base normale autoduale.*

(2) *L'homomorphisme $\phi_L$ se relève en un homomorphisme de $G_K$ dans $\tilde{G}$.*

L'obstruction à relever $\phi_L$ est l'élément $\phi_L^*(z) = z_L$ de $H^2(K)$. La propriété (2) équivaut donc à:

(2′) $z_L = 0$.

L'équivalence de (1) et de (2′) n'est autre que le th. 7.5.5 pour $r = 2$.

*Remarques.* 1) Lorsque $L$ est un *corps* (donc une extension galoisienne de $K$ de groupe de Galois $G$), la propriété (2) signifie que le "problème de plongement" associé à $L$ et à $\tilde{G} \to G$ est résoluble, autrement dit qu'il existe une extension galoisienne de $K$ de groupe de Galois $\tilde{G}$ contenant $L$.

2) Supposons que $G = A_n$, avec $n = 4$ ou 5. La sous-algèbre $E$ de $L$ fixée par $A_{n-1}$ est une algèbre étale de rang $n$ et de discriminant unité. D'après [20], prop. 1, la propriété (2) du th. 8.1.1 est équivalente à:

(3) *La forme $q_E$ est isomorphe à la forme unité $\langle 1, \ldots, 1 \rangle$ de rang $n$.*

(Noter que (1) $\Rightarrow$ (3) est vrai pour tout $n$, cf. 1.4.2. Nous ignorons ce qu'il en est de l'implication réciproque (3) $\Rightarrow$ (1).)

Dans le cas général, tout relèvement $\psi : G_K \to \tilde{G}$ de $\phi_L$ définit une $\tilde{G}$-algèbre galoisienne $\tilde{L}_\psi$ telle que la sous-algèbre $(\tilde{L}_\psi)^C$ fixée par $C$ soit isomorphe à $L$. On peut se demander si $\tilde{L}_\psi$ a elle-même une base normale autoduale. Il n'en est rien en général. Toutefois:

THÉORÈME 8.1.2. *Supposons que $L$ jouisse des propriétés* (1) *et* (2) *du th. 8.1.1. Il existe alors un relèvement $\psi : G_K \to \tilde{G}$ de $\phi_L$ tel que la $\tilde{G}$-algèbre galoisienne $\tilde{L}_\psi$ ait une base normale autoduale.*

Soit $\psi_0$ un relèvement quelconque de $\phi_L$. On verra au n°9.6 (cor. 9.6.2) qu'il existe un caractère quadratique $\sigma : G_K \to C$ tel que l'algèbre $\tilde{L}_\psi$ associée à $\psi = \psi_0 \cdot \sigma$ ait une base normale autoduale. Comme $\psi$ est un relèvement de $\phi_L$, le théorème en résulte.

*Remarque.* Si $K$ contient des éléments qui ne sont pas sommes de 4 carrés, on peut montrer qu'il existe des relèvements $\psi$ de $\phi_L$ tels que $\tilde{L}_\psi$ *n'ait pas de base normale autoduale.*

**8.2. $r = 3$ et fusion maximale.** On suppose que $S$ est de type (2,2,2) et que $N$ permute transitivement les 7 éléments d'ordre 2 de $S$. L'image de $N$ dans $\mathrm{Aut}(S)$ est alors, soit cyclique d'ordre 7, soit non abélienne d'ordre 21.

*Exemples.* $G = \mathbf{SL}_2(\mathbf{F}_8)$; $G = J_1$, premier groupe de Janko; $G = {}^2G_2(\mathbf{F}_q)$, groupe de Ree sur le corps $\mathbf{F}_q$, où $q$ est une puissance impaire de 3.

On peut choisir une base $(u, v, w)$ de $H^1(S)$ telle que l'automorphisme d'ordre 7

$$n : u \mapsto v, \quad v \mapsto w, \quad w \mapsto u + v,$$

soit induit par un élément de $N$. Un calcul simple montre qu'il existe un polynôme homogène cubique non nul $z(u, v, w)$ et un seul qui est invariant par $n$, à savoir:

$$z = u^3 + v^3 + w^3 + uv^2 + uw^2 + v^2w + uvw.$$

On peut identifier $z$ à un élément de $H^3(S)$; on obtient ainsi l'élément $z_S$ du n°7.3. Cet élément est invariant par l'action de $N$, donc définit un élément de $H^3(G)$, que l'on note encore $z$.

On a $H^3(G) = \{0, z\}$.

Le th. 7.5.5, appliqué avec $r = 3$, donne:

THÉORÈME 8.2.1. *Soit $L$ une $G$-algèbre galoisienne sur $K$. Pour que $L$ ait une base normale autoduale il faut et il suffit que $z_L = 0$* (autrement dit que l'homomorphisme $H^3(G) \to H^3(K)$ défini par $L$ soit nul).

*Exemple*. Prenons pour groupe $G$ le groupe de Janko $J_1$ et pour corps $K$ le corps $\mathbf{Q}(T)$, i.e. le corps des fonctions sur la droite projective $\mathbf{P}_1$. D'après [9] (voir aussi [22], n$^{os}$ 7.4.5 et 8.2.2), il existe une extension galoisienne $L$ de $K$, de groupe de Galois $G$, ayant les propriétés suivantes:

(a) $L/K$ est ramifiée en deux points de $\mathbf{P}_1$ conjugués sur $\mathbf{Q}(\sqrt{5})$, la ramification en ces points étant d'ordre 5;

(b) $L/K$ est ramifiée en un point rationnel de $\mathbf{P}_1$, la ramification en ce point étant d'ordre 2;

(c) $L/K$ est non ramifiée en dehors des trois points ci-dessus.

On peut calculer l'invariant $z_L \in H^3(K)$ correspondant à l'extension $L/K$. Le résultat est le suivant:

(8.2.2) *On a* $z_L = (-1)(-1)(-1)$ *dans* $H^3(K)$.

(Indiquons le principe du calcul. On montre d'abord que les *résidus* $\delta_v(z_L)$ de $z_L$ (au sens de [1], §4) sont nuls en toute place $v$ de $K$ où la ramification de $L/K$ est impaire. Comme toutes les places sauf une sont de ce type, on conclut au moyen de la formule des résidus ([1], Satz 4.17) que tous les $\delta_v(z_L)$ sont 0. Cela entraîne (*loc. cit.*) que $z_L$ est "constant," i.e. appartient au sous-groupe $H^3(\mathbf{Q})$ de $H^3(K)$. Mais $H^3(\mathbf{Q})$ n'a que deux éléments: 0 et $(-1)(-1)(-1)$. Il faut voir que $z_L = 0$ est impossible. Cela se fait en spécialisant la variable $T$ en un point réel, et en observant que l'extension de corps obtenue n'est pas réelle (cf. [22], n°8.4.3) et sa forme trace n'est donc pas isomorphe à la forme unité.)

On déduit de (8.2.2) que, si $L$ est une $J_1$-algèbre galoisienne obtenue par spécialisation à partir de l'extension ci-dessus, *$L$ possède une base normale autoduale si et seulement si $-1$ est somme de 4 carrés.*

*Remarques.* 1) Le fait que l'invariant $z_L$ de $L$ soit $(-1)(-1)(-1)$ est équivalent à chacune des deux propriétés suivantes:

(a) La forme $q_L$ est hyperbolique.

(b) Si $s$ est un élément d'ordre 2 de $G$, $L$ possède une base normale "$s$-autoduale": il existe $x \in L$ tel que $\mathrm{Tr}(x.g(x)) = 0$ (resp. 1) si $g \neq s$ (resp. $g = s$).

2) On a des résultats analogues pour le groupe $G = \mathbf{SL}_2(\mathbf{F}_8)$ en prenant pour extension $L/\mathbf{Q}(T)$ une extension ramifiée en trois points avec ramification d'ordre 9, cf. [22], 7.4.4 et 8.2.2.

3) Nous ignorons s'il existe des extensions galoisiennes de $\mathbf{Q}$ à groupe de Galois $J_1$ qui soient *totalement réelles* (et possèdent donc une base normale autoduale, d'après le th. 3.2.1).

**8.3. Quelques exemples de fusion non maximale.** Lorsque la fusion n'est pas maximale, le critère d'existence d'une base normale autoduale donnée au n°6.4 fait intervenir les formes quadratiques $q_L^1(\omega)$ associées aux orbites $\omega$ de $N$ dans $S' = H^1(S)$. Les classes de Stiefel-Whitney de ces formes peuvent être calculées par la méthode du n°7.6; lorsque les rangs de ces formes sont assez petits, cela conduit à des critères cohomologiques, comme on va le voir.

**8.3.1. Aucune fusion.** On suppose que $N$ opère trivialement sur $S$, autrement dit que $S$ est contenu dans le centre de $N$. On a alors $H^1(G) = H^1(S)$: tout homomorphisme de $S$ dans un groupe à 2 éléments se prolonge à $G$. Il en résulte qu'il existe une rétraction $r : G \to S$. Le noyau $H$ de $r$ est un sous-groupe normal de $G$ d'ordre impair, et $G$ est *produit semi-direct* de $S$ par $H$. Si $L$ est une $G$-algèbre galoisienne sur $K$ définie par un homomorphisme $\phi_L : G_K \to G$, alors *$L$ a une base normale autoduale si et seulement si l'image de $\phi_L$ est contenue dans $H$*, autrement dit *si et seulement si l'on a $x_L = 0$ pour tout $x \in H^1(G)$*; en effet, cette condition est nécessaire d'après 2.2.2, et elle est suffisante d'après [4], puisqu'elle entraîne $\phi_L(G_K) \subset H$.

**8.3.2. $r = 3$ et fusion d'ordre 3.** On suppose que $S$ est de type (2,2,2) et que l'image de $N/S$ dans $\mathrm{Aut}(S)$ est cyclique d'ordre 3. Cela signifie que l'on peut décomposer le $N$-module $S$ en somme directe $S = S_1 \times S_2$, où $S_1$ est d'ordre 2 et $S_2$ d'ordre 4, l'action de $N$ sur $S_2$ étant non triviale. Les groupes de cohomologie $H^1(G)$ et $H^2(G)$ sont faciles à déterminer:

$H^1(G)$ est de dimension 1; son élément non nul $x$ a pour image dans $H^1(S)$ l'homomorphisme $S \to \mathbf{Z}/2\mathbf{Z}$ de noyau $S_2$;

$H^2(G)$ est de dimension 2; il a pour base $\{x^2, y\}$ où $y$ induit sur $S_2$ la classe de cohomologie correspondant à l'extension quaternionique de $S_2$ (cf. n°8.1).

On constate alors que $L$ *a une base normale autoduale si et seulement si* $x_L = 0$ *et* $y_L = 0$, autrement dit si les homomorphismes $H^1(G) \to H^1(K)$ et $H^2(G) \to H^2(K)$ définis par $L$ sont nuls.

**8.3.3.** $r = 4$ **et fusion d'ordre 3, avec** $H^1(G) = 0$**.** On suppose que $S$ est de type (2,2,2,2) et peut se décomposer (comme $N$-module) en $S_1 \times S_2$, où les $S_i$ sont de type (2,2); on suppose de plus que l'image de $N$ dans Aut($S$) est d'ordre 3, et opère non trivialement sur chacun des $S_i$. On a alors

$$H^1(G) = 0 \text{ et } \dim H^2(G) = 4.$$

Le groupe $S'$ a 16 éléments. Il se décompose en six orbites sous l'action de $N$: l'orbite triviale $\{1\}$, et cinq orbites d'ordre 3. Chacune des orbites $\omega$ d'ordre 3 conduit à une forme ternaire $q^1_L(\omega)$; on vérifie facilement que ces formes sont de déterminant unité et que l'on a

$$w_2(q^1_L) = (x_\omega)_L,$$

où $x_\omega$ est un certain élément de $H^2(G)$ (cela se voit en utilisant le n°7.6). De plus, les cinq classes de cohomologie $x_\omega$ *engendrent* $H^2(G)$, et leur somme est 0. Or on sait qu'une forme ternaire est déterminée par ses invariants $w_1$ et $w_2$. On déduit de là que $L$ *admet une base normale autoduale si et seulement si l'on a* $x_L = 0$ *pour tout* $x \in H^2(G)$.

**8.3.4.** $r = 4$ **et fusion d'ordre 9.** On suppose que $S$ a une décomposition $S = S_1 \times S_2$ comme au n°8.3.3, mais que l'image de $N$ dans Aut($S$) est de type (3,3). (Exemple: $G = A_5 \times A_5$.) On a alors:

$$H^1(G) = 0 \text{ et } \dim H^2(G) = 2.$$

Les 16 éléments de $S'$ se répartissent en quatre orbites: l'orbite triviale $\{1\}$, deux orbites d'ordre 3 et une orbite d'ordre 9. Cela conduit à deux formes $q$, $q'$ de rang 3 et à une forme $q''$ de rang 9. On montre que $q''$ est isomorphe à $q \otimes q'$, de sorte qu'il suffit de considérer $q$ et $q'$. On obtient ainsi un critère analogue au précédent: $L$ *admet une base normale autoduale si et seulement si l'on a* $x_L = 0$ *pour tout* $x \in H^2(G)$.

**8.3.5.** $r = 4$ **et fusion d'ordre 5.** On suppose que $S$ est de type (2,2,2,2) et que l'image de $N$ dans Aut($S$) est d'ordre 5. On a alors:

$$H^1(G) = 0 \text{ et } \dim H^2(G) = 2.$$

Les 16 éléments de $S'$ se répartissent en quatre orbites: $\{1\}$, et trois orbites d'ordre 5. D'où trois formes quadratiques de rang 5: $q$, $q'$ et $q''$. En utilisant le n°7.6, on montre que les invariants $w_1$ de ces formes sont triviaux, et que l'on a

$$w_2(q) = x_L,\ w_2(q') = x'_L \text{ et } w_2(q'') = x''_L,$$

où $x, x', x''$ sont les trois éléments non nuls de $H^2(G)$. Pour que $L$ ait une base normale autoduale, il est donc *nécessaire* que $x_L = x'_L = x''_L = 0$. Si cette condition est satisfaite, on peut montrer que $q, q'$ et $q''$ sont de la forme

$$q = \langle 1, a, a, a, a\rangle,\ q' = \langle 1, a', a', a', a'\rangle,\ q'' = \langle 1, a'', a'', a'', a''\rangle,$$

avec $a, a', a'' \in K^*$ et $aa'a'' = 1$. De plus, les images de $a, a', a''$ dans le groupe $S_4(K) = K^*/(\text{sommes de 4 carrés})$, cf. n°9.2, déterminent $q, q'$ et $q''$ sans ambiguïté. La question de l'existence d'une base normale autoduale est alors ramenée à la suivante:

Est-ce que $a, a', a''$ sont sommes de 4 carrés dans $K$?

Ceci peut se traduire en termes cohomologiques. En effet, un élément $a$ de $K^*$ est somme de 4 carrés si et seulement si $(-1)(-1)(a) = 0$ dans $H^3(K)$ (cela résulte d'un théorème d'Arason et Merkurjev-Suslin dont on trouvera une généralisation dans [2]). Ceci conduit à associer à $L$ certaine *invariants dans* $H^3(K)$; il serait intéressant de les expliciter.

**9. Le cas où les 2-sous-groupes de Sylow de $G$ sont quaternioniens.** Dans ce §, on suppose qu'un 2-sous-groupe de Sylow $S$ de $G$ est isomorphe au *groupe des quaternions* d'ordre 8.

Exemple de tel groupe: $G = \mathbf{SL}_2(\mathbf{F}_q)$, avec $q \equiv \pm 3 \pmod 8$.

**9.1. Préliminaires.** Soit

$$1 \to \{1, \varepsilon\} \to \Gamma \to \Gamma_0 \to 1 \tag{9.1.1}$$

une suite exacte de groupes finis, où $\varepsilon$ est un élément central d'ordre 2 de $\Gamma$. Les éléments $e_+ = (1+\varepsilon)/2$ et $e_- = (1-\varepsilon)/2$ sont des idempotents centraux de l'algèbre $K[\Gamma]$.

Si $(V, q)$ est une $\Gamma$-forme quadratique, on pose

$$V_+ = e_+V,\ V_- = e_-V,$$

et l'on note $q_+$ (resp. $q_-$) la restriction de $q$ à $V_+$ (resp. à $V_-$). On a

$$V = V_+ \oplus V_-,$$

et $(V_+, q_+)$ est une $\Gamma_0$-forme quadratique. Si $D_\Gamma$ est le quotient de $K[\Gamma]$ par l'idéal engendré par $e_+$, alors $V_-$ est un $D_\Gamma$-module, et l'on a

$$q_-(hx, y) = q_-(x, h^* y) \quad (x, y \in V_-,\ h \in D_\Gamma), \tag{9.1.2}$$

où $h \mapsto h^*$ est l'involution de $D_\Gamma$ déduite par passage au quotient de celle de $K[\Gamma]$, cf. n°1.1.

**9.2. $S$-algèbres galoisiennes.** Comme $S$ est quaternionien d'ordre 8, on a une suite exacte de type (9.1.1):

$$1 \to \{1, \varepsilon\} \to S \to S_0 \to 1, \tag{9.2.1}$$

où $\varepsilon$ est l'élément d'ordre 2 de $S$, et $S_0$ est abélien élémentaire de type (2,2). L'algèbre à involution $D_S$ associée à $S$ comme ci-dessus est *l'algèbre des quaternions de Hamilton*, de base $\{1, i, j, k\}$ avec les relations usuelles: $i^2 = -1$, $j^2 = -1$, $k = ij = -ji$. On notera

$$\mathrm{Nrd} : D_S \to K$$

la *norme réduite* de cette algèbre. On a:

$$\mathrm{Nrd}(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2.$$

La forme quadratique Nrd est isomorphe à $\langle 1, 1, 1, 1\rangle = \langle\langle 1, 1\rangle\rangle$, cf. n°4.4.

Comme Nrd est multiplicative, $\mathrm{Nrd}(D_S^*)$ est un sous-groupe de $K^*$. On posera:

$$S_4(K) = K^*/\mathrm{Nrd}(D_S^*) = K^*/(\text{sommes de 4 carrés}). \tag{9.2.2}$$

Le groupe $S$ agit sur $D_S$ par multiplication à gauche; dans cette action, $\varepsilon$ opère par $x \mapsto -x$, et la forme quadratique Nrd est invariante. Si $a \in K^*$, le couple $(D_S, a.\mathrm{Nrd})$ est une $S$-forme quadratique.

LEMME 9.2.3. *Soient $a, b \in K^*$. Il y a équivalence entre:*

(i) *Les formes quadratiques $a$.Nrd et $b$.Nrd sont équivalentes.*

(ii) *Les $S$-formes quadratiques $(D_S, a.\mathrm{Nrd})$ et $(D_S, b.\mathrm{Nrd})$ sont isomorphes.*

(iii) *Les images de $a$ et $b$ dans $S_4(K)$ (cf. 9.2.2 ci-dessus) coïncident (autrement dit $ab$ est somme de 4 carrés).*

L'équivalence de (i) et (iii) résulte de la multiplicativité de Nrd (c'est une propriété générale des formes de Pfister). L'implication (ii) $\Rightarrow$ (i) est triviale. Enfin, (iii) $\Rightarrow$ (i), car si $b = \mathrm{Nrd}(z).a$, avec $z \in D_S^*$, la multiplication à droite par $z$ est un isomorphisme du $S$-espace quadratique $(D_S, a.\mathrm{Nrd})$ sur le $S$-espace quadratique $(D_S, b.\mathrm{Nrd})$.

Soit maintenant $M$ une *$S$-algèbre galoisienne*, et soit $q_M$ sa forme trace. Soit $M_0$ la sous-algèbre de $M$ fixée par $\{1, \varepsilon\}$. Avec les notations du n°9.1, on a $M_0 = M_+$ et $q_{M_0} = \frac{1}{2}(q_M)_+$.

LEMME 9.2.4. *Les formes quadratiques $q_{M_0}$ et $(q_M)_+$ sont isomorphes à la forme unité $\langle 1, 1, 1, 1\rangle$.*

La $S_0$-algèbre galoisienne $M_0$ est définie par un homomorphisme

$$\phi_{M_0} : G_K \to S_0$$

qui est relevable en $\phi_M : G_K \to S$ par construction. D'après un théorème de Witt [24] (voir aussi 8.1, ainsi que [20], n°3.2) cela entraîne que sa forme trace $q_{M_0}$ est isomorphe à $\langle 1, 1, 1, 1\rangle$. Comme 2 est somme de 4 carrés, il en est de même de $(q_M)_+ = 2.q_{M_0}$.

PROPOSITION 9.2.5. *Il existe $a \in K^*$ tel que $q_M$ soit isomorphe à la 3-forme de Pfister $\langle\langle 1, 1, a\rangle\rangle$, et l'image de $a$ dans $S_4(K)$ est un invariant de la $S$-forme quadratique $(M, q_M)$.*

Soit $M = M_+ \oplus M_-$ la décomposition de $M$ donnée par 9.1. L'espace quadratique $M_-$ est un module libre de rang 1 sur l'algèbre de quaternions $D_S$. Soit $x$ une base de ce module et soit $a = q_M(x)$. D'après (9.1.2), on a:

$$q_M(hx) = q_M(hx, hx) = q_M(x, h^*hx) = \mathrm{Nrd}(h).q_M(x) = a.\mathrm{Nrd}(h) \quad (h \in D_S),$$

ce qui montre que $(q_M)_-$ est isomorphe à $a.\mathrm{Nrd} = \langle a, a, a, a\rangle$, et que $a \neq 0$. D'autre part, le lemme 9.2.4 montre que $(q_M)_+ \simeq \langle 1, 1, 1, 1\rangle$. D'où

$$q_M \cong \langle 1, 1, 1, 1\rangle \oplus \langle a, a, a, a\rangle = \langle\langle 1, 1, a\rangle\rangle,$$

ce qui démontre la première partie de la proposition. Le fait que l'image de $a$ dans $S_4(K)$ soit un invariant de $q_M$ est bien connu (et résulte de 9.2.3).

On notera $a(M)$ *l'image de $a$ dans $S_4(K)$*. D'après la prop. 9.2.5, c'est un *invariant* de la $S$-forme quadratique $(M, q_M)$. Plus précisément, il résulte de la démonstration ci-dessus, combinée avec 9.2.3, que $a(M)$ *caractérise* la composante $(M_-, (q_M)_-)$ de $(M, q_M)$. Autrement dit:

PROPOSITION 9.2.6. *Soient $M$ et $M'$ deux $S$-algèbres galoisiennes. Il y a équivalence entre:*

(i) *Les formes quadratiques $(q_M)_-$ et $(q_{M'})_-$ sont équivalentes.*

(ii) *Les $S$-formes quadratiques $(M_-, (q_M)_-)$ et $(M', (q_{M'})_-)$ sont isomorphes.*

(iii) *On a $a(M) = a(M')$ dans $S_4(K)$.*

*Interprétation unitaire de l'invariant $a(M)$.* L'algèbre $K[S]$ du groupe $S$ se décompose en

$$K(S) = K \times K \times K \times K \times D_S,$$

où les quatre premiers facteurs correspondent aux caractères quadratiques de $S$. On en déduit:

$$U_S = \{\pm 1\} \times \{\pm 1\} \times \{\pm 1\} \times \{\pm 1\} \times U(D_S),$$

où $U_S$ est le groupe unitaire de l'algèbre à involution $K[S]$, et $U(D_S)$ celui de $D_S$. L'ensemble de cohomologie $H^1(K, U(D_S))$ s'identifie à $K^*/\mathrm{Nrd}(D_S^*) = S_4(K)$, cf. [19], p. III-24. On obtient ainsi une projection

$$\pi : H^1(K, U_S) \to S_4(K).$$

Si $M$ est une $S$-algèbre galoisienne, et $u(M)$ l'élément correspondant de $H^1(K, U_S)$, cf. n°1.5, *l'image de $u_M$ par $\pi$ n'est autre que l'invariant $a(M)$ défini ci-dessus.*

*Remarque.* Le groupe $S_4(K) = K^*/\mathrm{Nrd}(D_S^*)$ admet une autre interprétation cohomologique: si l'on associe à un élément $a$ de $K^*$ la classe de cohomologie

$$(a)^3 = (a)(a)(a) = (-1)(-1)(a) \quad \text{de } H^3(K), \tag{9.2.7}$$

on obtient un *plongement* de $S_4(K)$ dans $H^3(K)$, cf. 8.3.5. Cela permet *d'identifier $S_4(K)$ au sous-groupe de $H^3(K)$ formé des éléments qui sont multiples de $(-1)(-1) \in H^2(K)$.*

**9.3. La forme trace d'une $G$-algèbre galoisienne.** Posons $m = |G|/8$; c'est un entier impair.

Soit $L$ une $G$-algèbre galoisienne sur $K$. On a vu au n°6.1 qu'il existe une forme quadratique $q_L^1$ de rang $|S| = 8$ telle que $q_L \cong m \otimes q_L^1$, et que cette forme est unique, à isomorphisme près.

THÉORÈME 9.3.1. *Il existe $a \in K^*$ tel que $q_L^1$ soit isomorphe à la 3-forme de Pfister $\langle\langle 1, 1, a\rangle\rangle$.*

Si $L$ est de la forme $\mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne, on a $q_L^1 \simeq q_M$ d'après 6.1.1 et $q_M \simeq \langle\langle 1, 1, a\rangle\rangle$ avec $a \in K^*$ d'après 9.2.5. D'où l'existence de $a$ dans ce cas.

Le cas général se ramène au précédent en faisant une extension de degré impair de $K$, cf. 2.1.1. Après une telle extension, $q_L^1$ devient une 3-forme de Pfister divisible par $\langle\langle 1, 1\rangle\rangle$ (au sens du n°4.5); d'après 4.4.1 et 4.5.2 ces propriétés sont vraies sur $K$.

*Remarque.* Ici encore, l'image $a(L)$ de $a$ dans $S_4(K)$ est un invariant de $q_L^1$ (et *a fortiori* de $L$). Cet invariant détermine la structure de $q_L$:

$$q_L \simeq m \otimes \langle\langle 1, 1, a\rangle\rangle \simeq 4m \otimes \langle 1, a\rangle \simeq \langle 1, \ldots, 1\rangle \otimes \langle 1, a\rangle. \tag{9.3.2}$$

Nous allons voir que, lorsqu'il y a "fusion" dans $S$, $a(L)$ détermine même la $G$-forme quadratique $(L, q_L)$ à isomorphisme près.

**9.4. Critère d'isomorphisme pour les $G$-formes quadratiques $(L, q_L)$.** Soit $N$ le normalisateur de $S$ dans $G$. Faisons l'hypothèse suivante:

**9.4.1.** *Le groupe N permute transitivement les trois sous-groupes cycliques d'ordre 4 de S.*

Cette hypothèse équivaut à:

**9.4.2.** *Le groupe N permute transitivement les éléments d'ordre 4 de S.*

Elle équivaut aussi à:

**9.4.3.** *Les éléments d'ordre 4 de G sont conjugués entre eux.*

(Les implications 9.4.1 $\Leftrightarrow$ 9.4.2 $\Rightarrow$ 9.4.3 sont immédiates. L'implication 9.4.3 $\Rightarrow$ 9.4.2 provient de ce que $N$ *contrôle la fusion de* $S$ au sens du n°7.1—ce qui se vérifie par un argument analogue à celui utilisé pour les groupes de Sylow abéliens.)

THÉORÈME 9.4.4. *Supposons 9.4.1 vraie. Soient L et L′ deux G-algèbres galoisiennes sur K. Les propriétés suivantes sont équivalentes:*

(1) *Les formes quadratiques $q_L$ et $q_{L'}$ sont isomorphes.*

(2) *Les G-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes.*

(3) *On a $a(L) = a(L')$ dans $S_4(K)$.*

D'où, en prenant $L'$ décomposée:

COROLLAIRE 9.4.5. *Supposons 9.4.1 vraie. Pour que L ait une base normale autoduale, il faut et il suffit que $a(L) = 1$ dans $S_4(K)$.*

*Démonstration du th. 9.4.4.* L'équivalence de (1) et (3) résulte de (9.3.1) et (9.3.2). L'implication (2) $\Rightarrow$ (1) est claire. Il reste à montrer que (3) $\Rightarrow$ (2).

Supposons donc que l'on ait $a(L) = a(L')$. Quitte à faire une extension de degré impair de $K$, on peut aussi supposer (cf. n°2.1) que $L = \mathrm{Ind}_S^G M$ et $L' = \mathrm{Ind}_S^G M'$, où $M$ et $M'$ sont deux $S$-algèbres galoisiennes; on a $a(M) = a(M')$.

Il nous faut prouver que les $G$-formes quadratiques $\mathrm{Ind}_S^G(M, q_M)$ et $\mathrm{Ind}_S^G(M', q_{M'})$ sont isomorphes. Vu la transitivité de l'opération d'induction, il suffit de montrer qu'il en est ainsi pour les $N$-formes quadratiques

$$\mathrm{Ind}_S^N(M, q_M) \quad \text{et} \quad \mathrm{Ind}_S^N(M', q_{M'}).$$

En d'autres termes, *on est ramené au cas où* $N = G$. L'élément $\varepsilon$ appartient alors au centre de $G$. Si l'on pose $G_0 = G/\{1, \varepsilon\}$, on a une suite exacte du type (9.1.1):

$$1 \to \{1, \varepsilon\} \to G \to G_0 \to 1,$$

et $G_0$ a pour 2-sous-groupe de Sylow le groupe $S_0 = S/\{1, \varepsilon\}$. D'après le n°9.1, la $G$-forme quadratique $(L, q_L) = \mathrm{Ind}_S^G(M, q_M)$ se décompose en:

$$(L, q_L) = (L_+, (q_L)_+) \oplus (L_-, (q_L)_-). \tag{9.4.6}$$

La composante $(L_-, (q_L)_-)$ est isomorphe à $\mathrm{Ind}_S^G(M_-, (q_M)_-)$; or on a vu au n°9.2 que la $S$-forme quadratique $(M_-, (q_M)_-)$ est déterminée à isomorphisme près par l'invariant $a(M)$. Comme $a(M) = a(M')$, on déduit de là:

(9.4.7) *Les $G$-formes quadratiques $(L_-, (q_L)_-)$ et $(L'_-, (q_{L'})_-)$ sont isomorphes.*

D'autre part $L_+$ est une $G_0$-algèbre galoisienne, et, si $x \in L_+$, on a $q_L(x) = 2.q_{L_+}(x)$. Ainsi, à un facteur 2 près, $(L_+, (q_L)_+)$ n'est autre que la $G_0$-forme quadratique associée à la $G_0$-algèbre galoisienne $L_+$. Comme l'homomorphisme $\phi_{L_+} : G_K \to G_0$ définissant cette algèbre se relève en $\phi_L : G_K \to G$, il résulte du th. 8.1.1 que $(L_+, q_{L_+})$ *est isomorphe à la $G_0$-forme quadratique unité* (noter que 9.4.1 entraîne que les éléments d'ordre 2 de $S_0$ sont conjugués dans $G_0$-c'est ce qui permet d'appliquer le th. 8.1). Le même argument s'applique à $L'$. On en déduit:

(9.4.8) *Les $G$-formes quadratiques $(L_+, (q_L)_+)$ et $(L'_+, (q_{L'})_+)$ sont isomorphes.*

En combinant 9.4.7 et 9.4.8, on voit que les $G$-formes quadratiques $(L, q_L)$ et $(L', q_{L'})$ sont isomorphes, ce qui achève la démonstration.

*Remarque*. Lorsque la condition 9.4.1 n'est pas vérifiée (i.e. lorsqu'il n'y a pas de fusion dans $S$), le groupe $G$ est 2-*nilpotent* ([10], p. 432, Satz 4.9): il existe un sous-groupe normal $H$ de $G$, d'ordre $m = |G|/8$, tel que $G$ soit *produit semi-*

*direct de $S$ et de $H$*. Si $L$ est une $G$-algèbre galoisienne sur $K$, on peut montrer que *$L$ possède une base normale autoduale si et seulement si les deux conditions suivantes sont satisfaites*:

(i) $x_L = 0$ *pour tout* $x \in H^1(G)$.

(ii) $a(L) = 1$ *dans* $S_4(K)$.

La condition (i) signifie que $\phi_L(G_K)$ est contenu dans le sous-groupe $H.\{1,\varepsilon\}$ de $G$. Si elle est satisfaite, le composé de $\phi_L$ et de la projection $H.\{1,\varepsilon\} \to \{1,\varepsilon\}$ est un caractère quadratique de $G$, donc correspond à un élément $(a)$ de $H^1(K)$; l'image de $a$ dans $S_4(K)$ est l'invariant $a(L)$ de $L$; la condition (ii) équivaut à dire que $a$ est somme de 4 carrés dans $K$.

**9.5. Application: la forme trace de l'algèbre $L^H$.** Les notations sont les mêmes qu'au n° précédent. En particulier, *on suppose que la condition* 9.4.1 ("fusion totale") *est satisfaite.*

Soit $L$ une $G$-algèbre galoisienne et soit $a$ un représentant de $a(L)$ dans $K^*$. Si $C = \{1,\varepsilon\}$ est le centre de $S$, soit $M_a = K[X]/(X^2 - a)$ la $C$-algèbre galoisienne définie par $a$.

PROPOSITION 9.5.1. *Soit* $L' = \mathrm{Ind}_C^G M_a$. *Les $G$-formes quadratiques* $(L, q_L)$ *et* $(L', q_{L'})$ *sont isomorphes.*

Vu le th. 9.4.4, il suffit de vérifier que les formes quadratiques $q_L$ et $q_{L'}$ sont isomorphes, ce qui est immédiat: toutes deux sont isomorphes à $4m \otimes \langle 1, a\rangle = m \otimes \langle\langle 1, 1, a\rangle\rangle$, cf. (9.3.2).

Soit maintenant $H$ un sous-groupe de $G$, et soit $E = L^H$.

THÉORÈME 9.5.2. *Il existe des entiers* $u, v \geq 0$ *tels que*

$$u + 4v = |C\backslash G/H| \quad \text{et} \quad u + 8v = (G : H),$$

*et l'on a*

$$q_E = u \otimes \langle 1\rangle \oplus v \otimes \langle\langle 1, 1, a\rangle\rangle.$$

D'après 1.4.1 et 9.5.1 on peut supposer que $L = \mathrm{Ind}_C^G M_a$. Dans ce cas, un raisonnement analogue à celui du lemme 8.5.4 montre que $E$ est isomorphe au produit de $x$ copies de $K$ et de $y$ copies de $M_a$, avec:

$$\begin{aligned} x &= \text{nombre d'éléments de } G/H \text{ fixés par } C, \\ 2y &= (G : H) - x. \end{aligned}$$

Il est facile de voir que $y$ est divisible par 4. On a alors:

$$\begin{aligned} q_E &= x \otimes \langle 1\rangle \oplus (y/4) \otimes \langle 1,1,1,1\rangle \otimes \langle 2, 2a\rangle \\ &= x \otimes \langle 1\rangle \oplus (y/4) \otimes \langle\langle 1,1,a\rangle\rangle, \end{aligned}$$

ce qui démontre le théorème, avec $u = x$, $v = y/4$.

**9.6. Comportement de l'invariant $a(L)$ par torsion quadratique.** Supposons que le sous-groupe $C = \{1, \varepsilon\}$ de $S$ soit contenu dans le *centre* de $G$, autrement dit que $\varepsilon$ soit le seul élément d'ordre 2 de $G$. Posons comme ci-dessus $G_0 = G/C$, de sorte que l'on a la suite exacte

$$1 \to C \to G \to G_0 \to 1.$$

Soit $L$ une $G$-algèbre galoisienne sur $K$, et soit $\phi_L : G_K \to G$ un homomorphisme définissant $L$. Soit d'autre part $\sigma : G_K \to C$ un caractère quadratique de $G_K$, et soit $(z_\sigma)$ l'élément correspondant de $H^1(K)$. Le produit

$$\phi_L.\sigma : s \mapsto \phi_L(s)\sigma(s)$$

est un homomorphisme de $G_K$ dans $G$, donc définit une $G$-algèbre galoisienne $L_\sigma$ ("tordue" de $L$ par $\sigma$).

PROPOSITION 9.6.1. *Les invariants $a(L)$ et $a(L_\sigma)$ sont liés par la formule:*

$$a(L_\sigma) = z_\sigma a(L) \quad \text{dans } S_4(K).$$

COROLLAIRE 9.6.2. *Supposons 9.4.1 vraie. Il est alors possible de choisir $\sigma$ de telle sorte que la $G$-algèbre galoisienne $L_\sigma$ ait une base normale autoduale.*

Si $a$ est un représentant de $a(L)$, on choisit $\sigma$ de telle sorte que $(z_\sigma) = (a)$ dans $H^1(K)$. Le produit $z_\sigma a(L)$ est alors égal à 1 dans $S_4(K)$, ce qui montre que $a(L_\sigma) = 1$ et entraîne que $L_\sigma$ a une base normale autoduale d'après 9.4.5.

*Démonstration de la prop. 9.6.1.* Soit $L = L_+ \oplus L_-$ la décomposition de $L$ définie aux n$^{os}$ précédents. Soit $a \in K^*$ un représentant de $a(L)$.

LEMME 9.6.3. *On a $q_{L_+} \cong \langle 1, \ldots, 1\rangle$ et $q_{L_-} \cong \langle a, \ldots, a\rangle = m \otimes a$.*Nrd.

Vu 2.1.1, il suffit de vérifier ceci lorsque $L = \mathrm{Ind}_S^G M$, où $M$ est une $S$-algèbre galoisienne, auquel cas cela résulte de la décomposition de $q_M$ donnée au n°9.2.

Soit alors $K_\sigma = K \oplus Ku_\sigma$, avec $u_\sigma^2 = z_\sigma$, l'algèbre quadratique définie par le caractère $\sigma$. Le produit tensoriel $K_\sigma \otimes L$ se décompose en:

$$K_\sigma \otimes L = L_+ \ \oplus \ Ku_\sigma \otimes L_+ \ \oplus \ L_- \ \oplus \ Ku_\sigma \otimes L_-,$$

et l'on vérifie facilement que l'on a

$$L_\sigma \cong L_+ \oplus Ku_\sigma \otimes L_-.$$

Or, si $x \in L_-$, on a $\mathrm{Tr}((u_\sigma \otimes x)^2) = z_\sigma \mathrm{Tr}(x^2)$. Il en résulte que *la forme quadratique $q_{(L_\sigma)_-}$ est égale au produit de $q_{L_-}$ par $z_\sigma$*. Si $b$ est un représentant de $a(L_\sigma)$, cela montre, vu le lemme 9.6.3, que l'on a

$$m \otimes z_\sigma a.\mathrm{Nrd} \simeq m \otimes b.\mathrm{Nrd},$$

d'où $z_\sigma a.\mathrm{Nrd} \simeq b.\mathrm{Nrd}$ puisque $m$ est impair, ce qui entraîne

$$b = z_\sigma a \text{ dans } S_4(K), \text{cqfd.}$$

## III. Compléments.

**10. Deux contre-exemples.** Soit $L$ une $G$-algèbre galoisienne sur $K$. Considérons les deux propriétés suivantes:

(i) *$L$ a une base normale autoduale.*

(ii) *Pour tout $n > 0$ et tout $x \in H^n(G)$, on a $x_L = 0$ dans $H^n(K)$,* cf. n°2.2.

Dans divers cas particuliers (par exemple ceux de 2.2.4, 3.1.2, 3.2.1, 8.1.1, 8.2.1, 8.3.1, ...), on peut démontrer que (i) et (ii) sont équivalentes. Il est naturel de se demander si c'est là un fait général. Nous allons voir qu'il n'en est rien: *aucune des deux implications* (i) $\Rightarrow$ (ii) *et* (ii) $\Rightarrow$ (i) *n'est vraie* (même si $G$ est d'ordre 8).

**10.1. Un exemple où** (ii) **n'entraîne pas** (i). Prenons $G$ *quaternionien d'ordre* 8. Soit $C = \{1, \varepsilon\}$ le centre de $G$. Soit $z \in K^*$ et soit $\sigma : G_K \to C$ le caractère quadratique de $G_K$ associé à $K(\sqrt{z})$.

Notons $\phi : G_K \to G$ le composé $G_K \xrightarrow{\sigma} C \to G$, et soit $L$ la $G$-algèbre galoisienne correspondante. On a

$$L = \mathrm{Ind}_C^G M, \text{ où } M = K[T]/(T^2 - z).$$

LEMME 10.1.1. *On peut choisir $K$ et $z$ de telle sorte que:*

(10.1.2) $$H^n(K) = 0 \text{ pour tout } n > 3.$$

(10.1.3) *$z$ n'est pas somme de 4 carrés dans $K$.*

Soit $k$ un corps de nombres totalement imaginaire sur lequel l'algèbre de quaternions usuelle $(-1, -1)$ n'est pas décomposée, par exemple $k = \mathbf{Q}(\sqrt{-7})$.

Si $K = k((T))$, on a $\mathrm{cd}(G_K) = \mathrm{cd}(G_k) + 1 = 3$, ce qui montre que (10.1.2) est vraie. D'autre part, si l'on prend $z = T$, on vérifie facilement que $z$ n'est pas somme de 4 carrés dans $K$.

PROPOSITION 10.1.4. *Si $(K, z)$ satisfait aux conditions du lemme 10.1.1, l'algèbre $L$ n'a pas de base normale autoduale, et l'on a $x_L = 0$ pour tout $x \in H^n(G)$, $n > 0$.*

(En d'autres termes, on a (ii), mais pas (i).)

L'algèbre $L$ est obtenue à partir de l'algèbre décomposée $K^{(G)}$ par *torsion* au moyen du caractère quadratique $\sigma$, cf. n°9.5. D'après la prop. 9.5.1 son invariant $a(L)$ est égal à l'image de $z$ dans $S_4(K)$; vu l'hypothèse (10.1.3) cet invariant est non trivial; cela entraîne que $L$ n'a pas de base normale autoduale, cf. n°9.2.

Montrons que l'on a $x_L = 0$ pour tout $x \in H^n(G)$, $n > 0$. D'après (10.1.2), on peut se borner à $n = 1, 2$ ou 3. Or, pour ces valeurs de $n$, *l'homomorphisme de restriction $H^n(G) \to H^n(C)$ est égal à* 0. (Cela se vérifie, soit en explicitant la suite spectrale de la projection $G \to G/C$, soit en utilisant la détermination de $H^n(G)$ donnée dans [7], p. 253–254.) Comme $\phi$ se factorise par $C$, il en résulte bien que l'homomorphisme

$$\phi^* : H^n(G) \to H^n(C) \to H^n(K) \qquad (n = 1, 2, 3)$$

est nul.

*Remarque*. L'hypothèse (10.1.2) pourrait être remplacée par l'hypothèse plus faible suivante:

(10.1.5) L'élément $(z)^4 = (-1)(-1)(-1)(z)$ de $H^4(K)$ est nul.

D'après [2], (10.1.5) équivaut à:

(10.1.6) $z$ est somme de 8 carrés dans $K$.

**10.2. Un exemple où** (i) **n'entraîne pas** (ii). Prenons $G$ *cyclique d'ordre* 8, de générateur $s$. Soit $\varepsilon = s^4$ l'élément d'ordre 2 de $G$.

Comme au n°10.1, soit $z \in K^*$, soit $\sigma : G_K \to \{1, \varepsilon\}$ le caractère quadratique correspondant, et soit $\phi$ le composé

$$G_K \xrightarrow{\sigma} \{1, \varepsilon\} \to G.$$

Soit $L$ la $G$-algèbre galoisienne définie par $\phi$. Ici encore, on a:

$$L = \mathrm{Ind}_C^G M, \text{ avec } C = \{1, \varepsilon\} \text{ et } M = K[T]/(T^2 - z).$$

LEMME 10.2.1. *On peut choisir $(K, z)$ de telle sorte que:*

(10.2.2) *$z$ n'est pas somme de 2 carrés dans $K$.*

(10.2.3) *$z$ est somme de 2 carrés dans $K(\sqrt{2})$.*

On peut prendre par exemple $K = \mathbf{Q}$ et $z = 3$: il est bien connu que (10.2.2) est vrai, et (10.2.3) résulte de ce que $3 = 1 + (\sqrt{2})^2$.

PROPOSITION 10.2.4. *Si $(K, z)$ satisfait aux conditions du lemme 10.2.1, l'algèbre $L$ a une base normale autoduale, et, si $x$ est l'unique élément non nul de $H^2(G)$, on a $x_L \neq 0$ dans $H^2(K)$.*

(On a (i), mais pas (ii).)

L'élément $x$ correspond à l'extension de $G$ par un groupe d'ordre 2 qui est cyclique d'ordre 16. La restriction $x_C$ de $x$ à $C$ est l'unique élément $\neq 0$ de $H^2(C)$, c'est-à-dire le carré de l'élément non nul de $H^1(C)$. On a donc:

$$x_L = \phi^*(x) = \sigma^*(x_C) = (z)(z) = (-1)(z) \text{ dans } H^2(K),$$

d'où $x_L \neq 0$ d'après (10.2.2).

Il reste à montrer que $L$ a une base normale autoduale. Cela peut se faire par voie cohomologique, en explicitant $H^1(K, U_G)$. Nous allons procéder différemment, et *construire* un vecteur basique de $L$.

Choisissons pour cela une décomposition de $z$ comme somme de deux carrés dans $K(\sqrt{2})$:

$$z = (a + b\sqrt{2})^2 + (c + d\sqrt{2})^2, \text{ avec } a, b, c, d \in K,$$

i.e.

(10.2.5) $$z = a^2 + c^2 + 2b^2 + 2d^2 \quad \text{et} \quad ab + cd = 0.$$

Soit $M = K[T]/(T^2 - z)$ comme ci-dessus. D'après (10.2.2), $z$ n'est pas un carré dans $K$; on a donc $M \simeq K(\sqrt{z})$. Notons $x \mapsto x'$ l'involution canonique de $K(\sqrt{z})$. Par construction, on a $L = \mathrm{Ind}_C^G K(\sqrt{z})$. Cela permet d'écrire $L$ sous la forme

$$L = K(\sqrt{z}) \times K(\sqrt{z}) \times K(\sqrt{z}) \times K(\sqrt{z}),$$

l'action du générateur $s$ de $G$ étant donnée par

$$(x_1, x_2, x_3, x_4) \mapsto (x_2, x_3, x_4, x_1');$$

ainsi, $\varepsilon = s^4$ agit par $(x_1, x_2, x_3, x_4) \mapsto (x_1', x_2', x_3', x_4')$.

Soit $e$ l'élément de $L$ défini par:

$$e = (1,0,0,0) + (\sqrt{z})^{-1}(a, b+d, c, d-b).$$

On a $e^2 = (1,0,0,0) + 2(\sqrt{z})^{-1}(a,0,0,0) + z^{-1}(a^2, b^2+2bd+d^2, c^2, b^2-2bd+d^2)$, d'où

$$\begin{aligned}\mathrm{Tr}_{L/K}(e^2) &= \mathrm{Tr}_{M/K}(1 + 2a(\sqrt{z})^{-1} + z^{-1}(a^2+b^2+2bd+d^2+c^2+b^2-2bd+d^2)) \\ &= 2(1 + z^{-1}(a^2+c^2+2b^2+2d^2)) = 4, \text{ d'après (10.2.5).}\end{aligned}$$

De même:

$$\begin{aligned}\mathrm{Tr}_{L/K}(e.s(e)) &= \mathrm{Tr}_{M/K}(z^{-1}(a(b+d)+(b+d)c+c(d-b)+(d-b)(-a))) \\ &= 2z^{-1}(ab+ad+bc+cd+cd-bc-ad+ab) \\ &= 4z^{-1}(ab+cd) = 0, \text{ d'après (10.2.5).}\end{aligned}$$

Des calculs analogues montrent que l'on a aussi

$$\mathrm{Tr}_{L/K}(e.s^i(e)) = 0 \text{ pour } i = 2, \ldots, 7.$$

Il résulte de ces formules que $e/2$ *est un vecteur basique de* $L$, ce qui achève la démonstration.

*Remarque*. On peut montrer que la condition (10.2.3) est *nécessaire et suffisante* pour que $L$ ait une base normale autoduale.

## 11. Torsion des tenseurs quadratiques.

**11.1. Tenseurs.** Soit $V$ un $K$-espace vectoriel de dimension finie, et soit $V^*$ son dual. Si $a$ et $b$ sont des entiers $\geq 0$, on note $T_b^a(V)$ le produit tensoriel de $(\otimes^a V)$ et de $(\otimes^b V^*)$, cf. [6], p. III.63.

Un élément $t$ de $T_b^a(V)$ est appelé un *tenseur de type* $(a,b)$. On dit que $t$ est *quadratique* si $a+b=2$, i.e. si:

$a = 2, b = 0$ : $t$ est un élément de $\otimes^2 V$;
$a = 1, b = 1$ : $t$ est un élément de $V \otimes V^* = \mathrm{End}\, V$;
$a = 0, b = 2$ : $t$ est une forme bilinéaire sur $V$.

**11.2. Torsion.** Soit $t = (t_i)_{i\in I}$ une famille de tenseurs sur $V$ de types $(a_i, b_i)$, et soit $G$ un groupe fini opérant linéairement sur $V$, et fixant chacun des $t_i$. Soit $L$ une $G$-algèbre galoisienne sur $K$, correspondant à $\phi_L : G_K \to G$. On peut *tordre* $(V,t)$ au moyen de $\phi_L$, cf. [19], chap. III, §1. On obtient ainsi un autre

couple $(V',t')$, que l'on notera $(V,t)_L$. Rappelons ([19], *loc. cit.*) que $(V',t')$ est caractérisé, à isomorphisme près, par la propriété suivante:

(11.2.1) Il existe un $K_s$-isomorphisme $\psi : (V,t)_{/K_s} \to (V',t')_{/K_s}$ tel que ${}^s\psi = \psi \circ \phi_L(s)_V$ pour tout $s \in G_K$.

(Dans cette formule, ${}^s\psi$ désigne le conjugué de $\psi$ par $s$, et $\phi_L(s)_v$ est l'automorphisme de $V$ défini par l'élément $\phi_L(s)$ de $G$.)

Nous allons voir que, lorsque les $t_i$ sont quadratiques, la torsion par $L$ *ne dépend que de la G-forme quadratique* $(L,q_L)$, et pas de la structure d'algèbre de $L$. De façon plus précise:

THÉORÈME 11.2.2. *Supposons que tous les $t_i$ soient quadratiques. Soient $L$ et $L'$ deux $G$-algèbres galoisiennes sur $K$ telles que les $G$-formes quadratiques $(L,q_L)$ et $(L',q_{L'})$ soient isomorphes. Alors $(V,t)_L$ est isomorphe à $(V,t)_{L'}$.*

Le cas particulier où $L'$ est décomposé donne:

COROLLAIRE 11.2.3. *Si $L$ a une base normale autoduale, on a $(V,t)_L \simeq (V,t)$.*

(Autrement dit, la torsion par $L$ n'a aucun effet sur les tenseurs quadratiques.)

*Démonstration du th. 11.2.2.* Soit $A = A(V,t)$ le groupe algébrique des automorphismes de $(V,t)$. C'est un sous-groupe fermé du groupe linéaire $\mathbf{GL}_V$. Par hypothèse, on a un homomorphisme de groupes

$$G \to A(K) \to \mathrm{Aut}(V),$$

d'où, par linéarité, un homomorphisme d'algèbres $K[G] \to \mathrm{End}(V)$. Par restriction aux éléments unitaires, cela donne un morphisme de groupes algébriques $\varepsilon : U_G \to \mathbf{GL}_V$.

LEMME 11.2.4. *L'image de $\varepsilon$ est contenue dans le sous-groupe $A = A(V,t)$ de $\mathbf{GL}_V$.*

Montrons que $\varepsilon(U_G(K))$ est contenu dans $A(K)$; ce résultat (appliqué aux extensions de $K$) suffira à démontrer 11.2.4.

Soit $u = \sum u_g g$, avec $u_g \in K$, un élément de $U_G(K)$. Il nous faut prouver que $u(t_i) = t_i$ pour tout $i \in I$. Distinguons trois cas suivant le type de $t_i$:

(1) $t_i$ est de type (1,1), i.e. $t_i$ s'identifie à un endomorphisme de $V$. L'hypothèse que $t_i$ est fixé par $G$ signifie que $t_i g_V = g_V t_i$ pour tout $g \in G$. Il en résulte par linéarité que $u$ commute à $t_i$, c'est-à-dire que $u$ fixe $t_i$.

(2) $t_i$ est de type (0,2), i.e. $t_i$ s'identifie à une forme bilinéaire $V \times V \to K$. Par hypothèse, on a $t_i(gx,gz) = t_i(x,z)$ si $g \in G$ et $x,z \in V$. Comme $u^* = \sum u_g g^{-1}$, on en déduit $t_i(ux,z) = t_i(x,u^*z)$ et en appliquant ceci à $z = uy$, avec $y \in V$, on trouve

$$t_i(ux,uy) = t_i(x,u^*uy) = t_i(x,y) \qquad (x,y \in V),$$

ce qui montre bien que $u$ fixe $t_i$. (Une autre façon de procéder consiste à utiliser la construction donnée dans [3], n°1.1, et à en déduire que $A$ est le *groupe unitaire* d'une algèbre à involution associée à $(V,t)$.)

(3) $t_i$ est de type (2,0). La vérification est analogue à celle du cas (2): on trouve que $(u \otimes u)(t_i) = (uu^* \otimes 1)(t_i) = t_i$.

Revenons maintenant à la démonstration du th. 11.2.2. Soient $\phi = \phi_L$ et $\phi' = \phi_{L'}$ des homomorphismes de $G_K$ dans $G$ définissant respectivement $L$ et $L'$. Le couple $(V,t)_L$ se déduit de $(V,t)$ par torsion au moyen de la classe de cohomologie $c(L) \in H^1(K,A)$ définie par le cocycle $G_K \xrightarrow{\phi} G \to A(K)$, cf. [19], *loc. cit.* De même, $(V,t)_{L'}$ se déduit de $(V,t)$ par torsion au moyen de $c(L') \in H^1(K,A)$. Vu le lemme ci-dessus, $c(L)$ et $c(L')$ sont les images des classes $u(L)$ et $u(L')$ de $H^1(K,U_G)$ (cf. n°1.5) par l'application $H^1(K,U_G) \to H^1(K,A)$. L'hypothèse $(L,q_L) \simeq (L',q_{L'})$ équivaut à dire que $u(L) = u(L')$, cf. prop. 1.5.1. On a donc $c(L) = c(L')$, et cela entraîne que $(V,t)_L$ est isomorphe à $(V,t)_{L'}$ d'après ce qui a été dit plus haut.

*Remarque.* (1) Le th. 11.2.2 admet la réciproque suivante: *si $L$ et $L'$ sont telles que $(V,t)_L = (V,t)_{L'}$ pour tout $(V,t)$, avec $t$ quadratique, alors les $G$-formes quadratiques $(L,q_L)$ et $(L',q_{L'})$ sont isomorphes.*

Cela se voit en prenant pour $V$ l'espace vectoriel $K^{(G)}$ muni des tenseurs de type (1,1) donnés par les multiplications à gauche par les éléments de $G$, et du tenseur de type (0,2) donné par la forme quadratique unité (l'action de $G$ sur $V$ se faisant par les multiplications à droite).

(2) Le th. 11.2.2 est spécial aux tenseurs quadratiques:

(a) Dans le cas des tenseurs *linéaires* (i.e. de type $(1,0)$ ou $(0,1)$), il résulte du "th. 90" que $(V,t)_L$ est isomorphe à $(V,t)$ quel que soit $L$: *il n'y a pas de torsion.*

(b) Au contraire, si l'on considère des tenseurs quadratiques et cubiques il existe des choix de $(V,t)$ tels que $(V,t)_{L'}$ *n'est isomorphe à* $(V,t)_L$ *que si* $L'$ *est isomorphe à* $L$ (comme $G$-algèbre galoisienne).

Cela se voit en prenant $V = K^{(G)}$ comme ci-dessus, muni des tenseurs de type $(1,1)$ donnés par les multiplications à gauche par les éléments de $G$, et du tenseur de type $(1,2)$ exprimant la loi de multiplication de l'algèbre $K^{(G)}$.

**11.3. Description explicite de la torsion des tenseurs quadratiques.** Conservons les notations et hypothèses ci-dessus. On vient de voir que, si les $t_i$ sont quadratiques, $(V,t)_L$ ne dépend que de la $G$-forme quadratique $(L,q_L)$. Il est naturel de chercher une expression *explicite* de $(V,t)_L$ mettant en évidence ce fait. Nous allons donner une telle expression, en nous bornant pour simplifier *au cas où tous les $t_i$ sont de type* (0,2) *i.e. sont des formes bilinéaires.*

De façon plus générale, soit $(P,q)$ un $G$-espace quadratique (cf. n°1.2), et supposons que le $K[G]$-module $P$ soit *projectif* (ce qui est le cas si $K$ est de

caractéristique 0, par exemple). Nous allons définir le "tordu" $(V_P, t_P)$ de $(V,t)$ par $(P,q)$:

Par définition, on a $V_P = \mathrm{Hom}_G(P,V)$. La $i$-ème composante $t_{i,P}$ de $t_P$ est définie par:

$$t_{i,P}(f_1,f_2) = \mathrm{Tr}_P(f_{1i}^* F_2) \qquad (f_1,f_2 \in V_P), \tag{11.3.1}$$

où $F_2 \in \mathrm{Hom}(P,V)$ est tel que $f_2 = \sum_{g\in G} g_V F_2 g_V^{-1}$, et $f_{1i}^* \in \mathrm{Hom}(V,P)$ est l'adjoint de $f_1$ par rapport à $q$ et $t_i$, autrement dit est caractérisé par la formule

$$t_i(f_1(x),y) = q(x,f_{1i}^*(y)) \qquad \text{pour } x,y \in V.$$

(Noter que $F_2$ existe du fait que $P$ est $K[G]$-projectif.)

On vérifie que le membre de droite de (11.3.1) ne dépend pas du choix de $F_2$ (car on ne peut modifier $F_2$ qu'en lui ajoutant des combinaisons linéaires des $g_V F g_V^{-1} - F$, avec $g \in G$ et $F \in \mathrm{Hom}(P,V)$).

La construction ci-dessus s'applique en particulier à $(P,q) = (L,q_L)$.

THÉORÈME 11.3.2. *Le couple $(V_P,t_P)$ obtenu par torsion de $(V,t)$ au moyen de $(P,q) = (L,q_L)$ est isomorphe à $(V,t)_L$.*

(On obtient bien ainsi une description de $(V,t)_L$ ne faisant intervenir que la $G$-forme quadratique associée à $L$.)

*Démonstration.* (a) Supposons d'abord que $L$ soit décomposée, et soit $e = (1,0,\ldots,0)$ le vecteur basique de $L$ associé au choix d'un élément $\chi$ de $X(L)$, cf. n°1.4. Le vecteur $e$ définit un isomorphisme

$$\theta_e : V_P \to V$$

par $f \mapsto f(e)$. *Cet isomorphisme transforme $t_{i,P}$ en $t_i$.* En effet, avec les notations de (11.3.1), on peut prendre pour $F_2$ l'homomorphisme de $P$ dans $V$ qui applique $e$ sur $f_2(e)$ et $ge$ sur 0 si $g \neq 1$; on en déduit que $f_{1i}^* F_2$ applique $e$ sur $f_{1i}^* f_2(e)$ et $ge$ sur 0 pour $g \neq 1$; d'où:

$$\begin{aligned} t_{i,P}(f_1,f_2) &= \mathrm{Tr}_P(f_{1i}^* F_2) = q(e,f_{1i}^* f_2(e)) = t_i(f_1(e),f_2(e)) \\ &= t_i(\theta_e(f_1),\theta_e(f_2)). \end{aligned}$$

Il en résulte que *$\theta_e$ est un isomorphisme de $(V_P,t_P)$ sur $(V,t)$.*

(b) Dans le cas général, on applique ce qui précède au corps $K_s$. Le choix d'un élément $\chi$ de $X(L)$ définit comme ci-dessus un isomorphisme

$$\theta_e : (V_P,t_P)_{/K_s} \to (V,t)_{/K_s}.$$

Si $s\chi = \chi\phi(s)$ (cf. 1.3), on a $s(e) = \phi(s)^{-1}e$, cf. démonstration du th. 1.5.3. On en déduit:

$$^s(\theta_e) = \theta_{s(e)} = \phi(s)_V^{-1}\theta_e.$$

Si l'on pose $\psi = \theta_e^{-1}$, on a donc $^s\psi = \psi \circ \phi(s)_V$ pour tout $s \in G_K$, et d'après (11.2.1) cela montre bien que $(V_P, t_P)$ est isomorphe à $(V, t)_L$.

UNIVERSITÉ DE FRANCHE-COMTÉ, FACULTÉ DES SCIENCES, MATHÉMATIQUES, U.R.A. 741 (CNRS), 16, ROUTE DE GRAY, 25030 BESANÇON, FRANCE

COLLÈGE DE FRANCE, 75231 PARIS CEDEX 05, FRANCE

## RÉFÉRENCES

[1] J. Arason, Cohomologische Invarianten quadratischer Formen, *J. Algebra*, **36** (1975), 448–491.
[2] J. Arason, R. Elman et B. Jacob, Fields of cohomological 2-dimension three, *Math. Ann.*, **274** (1986), 649–657.
[3] E. Bayer-Fluckiger, Principe de Hasse faible pour les systèmes de formes quadratiques, *J. reine angew. Math.*, **378** (1987), 53–59.
[4] E. Bayer-Fluckiger et H.W. Lenstra, Jr., Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.*, **112** (1990), 359–373.
[5] A. Borel et J. Tits, Compléments à l'article "Groupes réductifs," *Inst. Hautes Études Sci. Publ.*, **41** (1972), 253–276.
[6] N. Bourbaki, *Algèbre*, nouvelle éd., Hermann, Paris, 1970, Chapitres 1 à 3.
[7] H. Cartan et S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, 1956.
[8] R.L. Griess, Schur multipliers of the known finite simple groups II, *Santa Cruz Conf. on Finite Groups, Proc. Sympos. Pure Math.*, vol. **37**, American Mathematical Society, Providence, 1980, pp. 273–282.
[9] G. Hoyden-Siedersleben, Realisierung der Jankogruppen $J_1$ und $J_2$ als Galoisgruppen über **Q**, *J. Algebra*, **97** (1985), 14–22.
[10] B. Huppert, *Endliche Gruppen I, Grundlehren Math. Wiss.*, vol. **137**, Springer-Verlag, New York, 1967.
[11] W. Jacob et M. Rost, Degree four cohomological invariants for quadratic forms, *Invent. Math.*, **96** (1989), 551–570.
[12] M. Kneser, Galois-Kohomologie halbeinfacher algebraischer Gruppen über $p$-adischen Körpern, *Math. Z.*, **88** (1965), 40–47; **89** (1965), 250–272.
[13] ———, *Lectures on Galois cohomology of classical groups*, Tata Inst. Fund. Res. Lectures on Math. and Phys., vol. **47**, Tata Institute of Fundamental Research, Bombay, 1969.
[14] J. Milnor, Algebraic $K$-theory and quadratic forms, *Invent. Math.*, **9** (1970), 318–344.
[15] A. Pfister, Quadratische Formen in beliebigen Körpern, *Invent. Math.*, **1** (1966), 116–132.
[16] W. Scharlau, *Quadratic and Hermitian Forms*, *Grundlehren Math. Wiss.*, vol. **270**, Springer-Verlag, New York, 1985.
[17] J-P. Serre, *Représentations Linéaires des Groupes Finis*, Hermann, Paris, 1967.
[18] ———, *Corps Locaux*, Hermann, Paris, 1968.
[19] ———, *Cohomologie Galoisienne*, 4ème éd., *Lecture Notes in Math.*, vol **5**, Springer-Verlag, New York, 1973.
[20] ———, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment. Math. Helv.*, **59** (1984), 651–676.
[21] ———, Résumé des cours au Collège de France 1990/1991, *Annuaire du Collège de France*, 1991, 111–121.

[22] ———, *Topics in Galois Theory* (notes written by Henri Darmon), Jones and Bartlett Publ., Boston, 1992.

[23] R. Steinberg, Regular elements of semisimple algebraic groups, *Inst. Hautes Études Sci. Publ. Math.*, **25** (1965), 49–80.

[24] E. Witt, Konstruktion von galoisschen Körpern der Charakteristik $p$ zu vorgegebener Gruppe der Ordnung $p^f$, *J. reine angew. Math.*, **174** (1936), 237–245.