Comment. Math. Helvetici **59** (1984) 651–676 0010–2571/84/040651–26$01.50 + 0.20/0

L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$

JEAN-PIERRE SERRE

à John C. Moore

Introduction

Soit E une extension finie séparable d'un corps commutatif K de caractéristique $\neq 2$. La forme quadratique $x \mapsto \mathrm{Tr}_{E/K}(x^2)$ attachée à cette extension a été souvent étudiée (cf. par exemple [2], [6], [10]). Il est naturel de s'intéresser à son *invariant de Witt*. Dans ce qui suit, je donne une formule reliant cet invariant à la *seconde classe de Stiefel–Whitney* de la représentation de permutation du groupe de Galois de E (cette classe peut aussi s'interpréter comme *l'obstruction* d'un certain "problème de plongement", cf. n° 3.1).

La formule en question fait l'objet du §2; sa démonstration utilise l'interprétation spinorielle de l'invariant de Witt et de la seconde classe de Stiefel–Whitney. Le §1 est consacré à des préliminaires; le §3 donne des exemples et des applications (notamment aux extensions ayant pour groupe de Galois le "Monstre" de Griess–Fischer); le §4 étend les résultats du §2 à la forme $x \mapsto \mathrm{Tr}_{E/K}(\alpha x^2)$, avec $\alpha \in E^*$. Les Appendices contiennent divers résultats auxiliaires.

§1. Notations

1.1. *Cohomologie galoisienne* mod 2 ([11], [12], [15])

Dans ce qui suit, K désigne un corps commutatif, K_s une clôture séparable de K, et Γ_K le groupe de Galois $\mathrm{Gal}(K_s/K)$. On suppose que la caractéristique de K est $\neq 2$ (le cas où $\mathrm{car}(K) = 2$ est traité dans [1]). Si G est un groupe profini, on note $H^m(G)$ les groupes de cohomologie $H^m(G, \mathbf{Z}/2\mathbf{Z})$; ce sont des espaces vectoriels sur le corps $\mathbf{F}_2$. Ceci s'applique en particulier à $G = \Gamma_K$; pour $m = 1, 2$, les groupes $H^m(\Gamma_K)$ ont une interprétation simple, fournie par la théorie de Kummer:

(i) $H^1(\Gamma_K) = \mathrm{Hom}(\Gamma_K, \mathbf{Z}/2\mathbf{Z})$ s'identifie au groupe K^*/K^{*2}; si a appartient à K^*/K^{*2} (ou à K^*), on note (a) l'élément correspondant de $H^1(\Gamma_K)$; c'est l'unique homomorphisme $\chi : \Gamma_K \to \mathbf{Z}/2\mathbf{Z}$ tel que $\gamma(\sqrt{a}) = (-1)^{\chi(\gamma)}\sqrt{a}$ pour tout $\gamma \in \Gamma_K$;

comme on écrit $H^1(\Gamma_K)$ additivement, on a $(xy)=(x)+(y)$ si $x, y \in K^*$;

(ii) $H^2(\Gamma_K)$ s'identifie à $\mathrm{Br}_2(K)$, noyau de la multiplication par 2 dans le groupe de Brauer $\mathrm{Br}(K)=H^2(\Gamma_K, K_s^*)$.

Si $(a_1), \ldots, (a_m)$ appartiennent à $H^1(\Gamma_K)$, on note $(a_1)\ldots(a_m)$ leur cup-produit dans $H^m(\Gamma_K)$. Lorsque $m=2$, $(a_1)(a_2)$ coïncide avec l'élément (a_1, a_2) de $\mathrm{Br}_2(K)=H^2(\Gamma_K)$ défini par l'algèbre de quaternions $\{i^2=a_1,\ j^2=a_2,\ ij=-ji\}$. On a $(a_1)(a_2)=0$ si et seulement si la forme $Z^2-a_1X^2-a_2Y^2$ représente 0.

1.2. *Formes quadratiques* ([4], [9], [11], [12], [18], [22])

Soit $Q=Q(X_1, \ldots, X_n)$ une forme quadratique non dégénérée de rang n sur K. Soit m un entier ≥ 0, et soit $w_m(Q) \in H^m(\Gamma_K)$ la m-ième classe de Stiefel-Whitney de Q, au sens de [4]. Rappelons que, si $Q \sim a_1X_1^2+\ldots+a_nX_n^2$, avec $a_i \in K^*$, on a

$$w_m(Q)=\sum_{i_1<\cdots<i_m}(a_{i_1})\cdots(a_{i_m}).$$

Si $d=d(Q) \in K^*/K^{*2}$ est le discriminant de Q, on a $w_1(Q)=(d)$. Quant à $w_2(Q)=\sum_{i<j}(a_i)(a_j)$, c'est *l'invariant de Witt* (appelé aussi "invariant de Hasse") de la forme Q; il peut s'interpréter en termes d'algèbres de Clifford, cf. [9], [18], [22].

1.3. *Extensions étales*

Soit E une K-algèbre commutative de rang fini $n \geq 1$. Nous supposerons que E est *étale* au sens de Bourbaki A. V. 28, i.e. est produit d'extensions finies séparables de K; le cas le plus important pour la suite (et auquel on pourrait se ramener si on le désirait) est celui où E est un *corps*.

Soit Φ l'ensemble des K-homomorphismes de E dans K_s. On a $\mathrm{Card}\,(\Phi)=n$. Le groupe Γ_K opère de façon évidente sur Φ, d'où un homomorphisme continu $e: \Gamma_K \to \mathfrak{S}_\Phi$, où $\mathfrak{S}_\Phi$ est le groupe des permutations de Φ. En identifiant Φ à $[1, n]$, on transforme e en un homomorphisme continu

$$e: \Gamma_K \to \mathfrak{S}_n,$$

défini à conjugaison près. D'après la théorie de Galois (Bourbaki, A. V. 73), E est déterminée à isomorphisme près par e, et l'on peut se donner e arbitrairement; dans le langage de [15], III, §1, l'algèbre E se déduit de l'algèbre déployée $K^n=K\times\cdots\times K$ par *torsion* au moyen du 1-cocycle

$$e: \Gamma_K \to \mathfrak{S}_n=\mathrm{Aut}\,(K^n).$$

On notera G_E le sous-groupe $e(\Gamma_K)$ de $\mathfrak{S}_n$. Lorsque $E = K[X]/(f)$, où f est un polynôme séparable de degré n, le groupe G_E est le "groupe de Galois de f", vu comme groupe de permutations des racines de f; il est transitif si et seulement si f est irréductible, i.e. si E est un corps.

1.4. *La forme Q_E*

Soit E comme ci-dessus. L'application $Q_E : E \to K$ définie par $Q_E(x) = \mathrm{Tr}_{E/K}(x^2)$ est une forme quadratique non dégénérée de rang n. Lorsque $E = K^n$, c'est la forme unité $X_1^2 + \cdots + X_n^2$. Dans le cas général, Q_E se déduit de cette forme par *torsion* (cf. [15], III-4, prop. 4) au moyen du 1-cocycle

$$e : \Gamma_K \to \mathfrak{S}_n \subset \mathbf{O}_n(K),$$

où $\mathbf{O}_n$ désigne le groupe orthogonal à n variables (relatif à la forme unité).

Le *discriminant* d_E de Q_E est (par définition) le discriminant de la K-algèbre E. L'élément correspondant $(d_E) = w_1(Q_E)$ du groupe $H^1(\Gamma_K) = \mathrm{Hom}(\Gamma_K, \mathbf{Z}/2\mathbf{Z})$ n'est autre que le composé

$$\Gamma_K \xrightarrow{e} \mathfrak{S}_n \xrightarrow{\varepsilon_n} \{\pm 1\} \simeq \mathbf{Z}/2\mathbf{Z},$$

où ε_n est la signature (cf. Bourbaki, A. V. 57, exemple 6).

L'*invariant de Witt* $w_2(Q_E)$ fait l'objet du §2 ci-après.

1.5. *Les groupes $H^m(\mathfrak{S}_n)$ pour $m = 1, 2$*

Ces groupes sont bien connus ([3], [13]):

$$H^1(\mathfrak{S}_n) = \begin{cases} 0 & \text{si} \quad n = 1 \\ \mathbf{Z}/2\mathbf{Z} & \text{si} \quad n \geqslant 2 \end{cases}$$

$$H^2(\mathfrak{S}_n) = \begin{cases} 0 & \text{si} \quad n = 1 \\ \mathbf{Z}/2\mathbf{Z} & \text{si} \quad n = 2,3 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} & \text{si} \quad n \geqslant 4. \end{cases}$$

L'élément non nul de $H^1(\mathfrak{S}_n)$, $n \geqslant 2$, est la signature

$$\varepsilon_n : \mathfrak{S}_n \to \{\pm 1\} \simeq \mathbf{Z}/2\mathbf{Z}.$$

Les éléments de $H^2(\mathfrak{S}_n)$ sont décrits dans [13] en termes d'extensions de $\mathfrak{S}_n$ par un groupe à deux éléments $\{1, \omega\}$. Nous aurons surtout besoin de l'élément

$s_n \in H^2(\mathfrak{S}_n)$ correspondant à l'extension

$$1 \to \{1, \omega\} \to \tilde{\mathfrak{S}}_n \to \mathfrak{S}_n \to 1$$

notée (II') dans [13], p. 355. On peut caractériser $\tilde{\mathfrak{S}}_n$ (et s_n) par la propriété suivante:

(C) *Tout élément de* $\tilde{\mathfrak{S}}_n$ *dont l'image dans* $\mathfrak{S}_n$ *est une transposition* (resp. *un produit de deux transpositions à supports disjoints*) *est d'ordre* 2 (resp. *d'ordre* 4).

(On peut reformuler (C) en disant que, pour $n \geqslant 2$, la restriction de s_n au sous-groupe $\{1, (12)\}$ de $\mathfrak{S}_n$ est 0, et que, pour $n \geqslant 4$, la restriction de s_n au sous-groupe $\{1, (12)(34)\}$ est $\neq 0$.)

A la présentation standard de $\mathfrak{S}_n$ par $n-1$ générateurs t_i (les transpositions $(i, i+1)$) soumis aux relations

$$t_i^2 = 1, \qquad (t_i t_{i+1})^3 = 1, \qquad t_i t_j = t_j t_i \quad \text{si} \quad |j-i| \geqslant 2,$$

correspond une présentation de $\tilde{\mathfrak{S}}_n$ par des générateurs $\tilde{t}_i$ et ω, avec les relations

$$\tilde{t}_i^2 = 1, \quad \omega^2 = 1, \quad \omega \tilde{t}_i = \tilde{t}_i \omega, \quad (\tilde{t}_i \tilde{t}_{i+1})^3 = 1, \quad \tilde{t}_i \tilde{t}_j = \omega \tilde{t}_j \tilde{t}_i \quad \text{si} \quad |j-i| \geqslant 2.$$

On a $s_n = 0$ si et seulement si $n \leqslant 3$. Pour $n = 2, 3$ l'unique élément non nul de $H^2(\mathfrak{S}_n)$ est le cup-carré $\varepsilon_n \cdot \varepsilon_n$ de la signature $\varepsilon_n \in H^1(\mathfrak{S}_n)$. Pour $n \geqslant 4$, $\varepsilon_n \cdot \varepsilon_n$ et s_n forment une base de $H^2(\mathfrak{S}_n)$; de plus, la restriction de s_n au groupe alterné $\mathfrak{A}_n$ est l'unique élément non nul de $H^2(\mathfrak{A}_n)$.

Une autre façon de définir s_n consiste à utiliser la représentation évidente $\mathfrak{S}_n \to \mathbf{O}_n(\mathbf{R})$. A cette représentation est associé un *fibré orthogonal* l_n sur l'*espace classifiant* $B\mathfrak{S}_n$ de $\mathfrak{S}_n$; si $m \geqslant 0$, la classe de Stiefel–Whitney $w_m(l_n)$ est un élément du groupe

$$H^m(B\mathfrak{S}_n, \mathbf{Z}/2\mathbf{Z}) = H^m(\mathfrak{S}_n).$$

Pour $m = 2$, *on a* $w_2(l_n) = s_n$: cela se vérifie en utilisant (C). Quant à $w_1(l_n)$, c'est bien sûr la signature ε_n.

§2. Le résultat principal

2.1. *Enoncé*

On reprend les notations des n^{os} 1.3 et 1.4:

E est une K-algèbre commutative étale de rang n,

$d_E \in K^*/K^{*2}$ est le discriminant de E,

Q_E est la forme quadratique $x \mapsto \mathrm{Tr}_{E/K}(x^2)$,

$e : \Gamma_K \to \mathfrak{S}_n$ est l'homomorphisme (défini à conjugaison près) qui correspond à E par la théorie de Galois.

Le groupe $H^2(\Gamma_K) = \mathrm{Br}_2(K)$ contient les deux éléments suivants:

(i) $w_2(Q_E)$, invariant de Witt de la forme quadratique Q_E;

(ii) e^*s_n, image réciproque par e de $s_n \in H^2(\mathfrak{S}_n)$, cf. n° 1.5.

(Comme e est défini à conjugaison près, e^*s_n est défini sans ambiguïté: cela résulte, par exemple, de [14], p. 124, prop. 3.)

Nous allons comparer ces éléments:

THÉORÈME 1. *On a*

$$w_2(Q_E) = e^*s_n + (2)(d_E). \tag{1}$$

La démonstration sera donnée au n° 2.6.

Remarques. 1) Le terme $(2)(d_E)$ est égal (cf. n° 1.1) à $(2, d_E)$, classe dans $\mathrm{Br}_2(K)$ de l'algèbre de quaternions $\{i^1 = 2, j^2 = d_E, ij = -ji\}$. Ce terme est nul si et seulement si d_E est de la forme $x^2 - 2y^2$ avec $x, y \in K$.

2) Comme $(d_E) = e^*\varepsilon_n$, on peut récrire (1) sous la forme équivalente:

$$w_2(Q_E) = e^*s_n + (2) \cdot e^*(\varepsilon_n), \tag{1'}$$

ou encore (cf. n° 1.5):

$$w_2(Q_E) = e^*w_2(l_n) + (2) \cdot e^*w_1(l_n). \tag{1''}$$

Question.[1] Y a-t-il une formule analogue à (1'') qui relie les $w_m(Q_E)$ aux $e^*w_m(l_n)$, i.e. aux classes de Stiefel–Whitney de la représentation de permutation de Γ_K associée à E?

Ainsi, pour $m = 3$, on a

$$w_3(Q_E) = e^*w_3(l_n); \tag{2}$$

cela se déduit du th. 1 et du fait que $w_3 = Sq^1w_2 + w_1 \cdot w_2$.

[1] Cette question vient d'être résolue affirmativement par B. Kahn ("Classes de Stiefel–Whitney de formes quadratiques et de représentations galoisiennes réelles", à paraître). En particulier, la formule (3) ci-après est valable sans restriction sur n.

(Note ajoutée en mai 1984.)

D'autre part, on peut vérifier que, pour $n \leq 7$, on a:

$$w_m(Q_E) = \begin{cases} e^* w_m(l_n) & \text{si } m \text{ est impair} \\ e^* w_m(l_n) + (2) \cdot e^* w_{m-1}(l_n) & \text{si } m \text{ est pair.} \end{cases} \tag{3}$$

[Indiquons brièvement comment on démontre (3) pour $n \leq 7$. Par un argument élémentaire de restriction, on peut supposer que Γ_K est un pro-2-groupe. D'autre part, en utilisant le fait que $(2)(2) = 0$ (cf. n° 2.2), on montre que, si (3) est vraie pour deux algèbres étales E_1 et E_2, elle est aussi vraie pour leur produit $E_1 \times E_2$. Cela permet de se ramener au cas où E est un corps de degré $n \leq 7$. Comme Γ_K est un 2-groupe, on a $n = 1$, 2 ou 4. Les cas $n = 1$ et $n = 2$ sont immédiats. Pour $n = 4$, on écrit E sous la forme $K(\sqrt{x}, \sqrt{y})$ avec $x \in K^*$ et $y \in K(\sqrt{x})^*$, et l'on détermine explicitement les classes de cohomologie $w_m(Q_E)$ et $e^* w_m(l_4)$; on trouve que ces classes sont nulles pour $m \geq 3$, ce qui démontre (3), compte tenu du th. 1.]

2.2. *Démonstration du théorème* 1 *pour* $n = 1, 2, 3$

Dans chacun de ces cas on a $s_n = 0$ (cf. n° 1.5) et la formule à démontrer s'écrit:

$$w_2(Q_E) = (2)(d_E) \qquad (n = 1, 2, 3). \tag{4}$$

Vérifions-la:

(i) $n = 1$

On a $w_2(Q_E) = 0$ et $(d_E) = (1) = 0$, d'où $(2)(d_E) = 0$.

(ii) $n = 2$

On a $Q_E(1) = n = 2$, d'où $Q_E \sim 2X_1^2 + \alpha X_2^2$, avec $\alpha \in K^*$. En comparant les discriminants, on voit que $(\alpha) = (2d_E)$, d'où

$$Q_E \sim 2X_1^2 + 2d_E X_2^2, \tag{5}$$

et $w_2(Q_E) = (2)(2d_E) = (2)(2) + (2)(d_E)$. Mais $(2)(2) = 0$ puisque la forme $Z^2 - 2X^2 - 2Y^2$ représente 0 (prendre $Z = 2$, $X = Y = 1$). On obtient donc bien $w_2(Q_E) = (2)(d_E)$.

(iii) $n = 3$

Montrons d'abord que l'on a:

$$Q_E \sim X_1^2 + 2X_2^2 + 2d_E X_3^2. \tag{6}$$

Distinguons deux cas:

(a) E se décompose en $E_1 \times E_2$, avec $\mathrm{rg}(E_1) = 1$, $\mathrm{rg}(E_2) = 2$.

On a alors $Q_E \sim Q_{E_1} \oplus Q_{E_2}$; la forme Q_{E_1} est isomorphe à la forme unité X_1^2; d'après (5) et le fait que $(d_E) = (d_{E_2})$, la forme Q_{E_2} est isomorphe à $2X_2^2 + 2d_E X_3^2$; on obtient bien (6).

(b) E est un corps.

Notons ce corps K'; c'est une extension cubique de K. Soit $E' = K' \otimes_K E$ l'algèbre déduite de E par extension des scalaires à K'; il est clair que E' possède un facteur isomorphe à K', donc est du type (a) ci-dessus. Il en résulte que (6) devient vraie sur K'. Comme $[K' : K]$ est *impair*, (6) est donc vraie sur K, en vertu d'un théorème de Springer [17].

Une fois (6) prouvée, la formule (4) se démontre comme dans le cas $n = 2$.

Remarques. 1) Supposons $n = 3$, et $\mathrm{car}(K) \neq 3$. La restriction de Q_E aux éléments de trace 0 est non dégénérée; si l'on note cette forme Q'_E, on a $Q_E \sim 3X_1^2 \oplus Q'_E$, d'où, en utilisant (6):

$$Q'_E \sim 6X_2^2 + 2d_E X_3^2. \tag{7}$$

On en conclut qu'il existe $x \in E$ tel que $\mathrm{Tr}_{E/K}(x) = 0$ et $\mathrm{Tr}_{E/K}(x^2) = 6$. Un tel x satisfait à une équation de la forme

$$x^3 - 3x + t = 0, \quad \text{avec} \quad t \in K. \tag{8}$$

On voit ainsi que toute extension cubique de K peut être obtenue par une équation du type (8), si $\mathrm{car}(K) \neq 3$. (Ce résultat peut aussi se démontrer par un argument direct, et l'on en déduit alors (7) et (6).)

2) Les formules (5) et (6) sont des cas particuliers de formules valables pour tout n, cf. Appendices I et II.

2.3. *Rappels sur $\mathfrak{A}_n$ et le groupe des spineurs*

A partir de maintenant, et jusqu'à la fin du §2, on suppose $n \geq 4$. On note a_n l'élément non nul de $H^2(\mathfrak{A}_n)$, et $\tilde{\mathfrak{A}}_n$ l'extension centrale correspondante:

$$1 \to \{\pm 1\} \to \tilde{\mathfrak{A}}_n \to \mathfrak{A}_n \to 1. \tag{9}$$

(Il est commode pour la suite d'employer une notation multiplicative, i.e. d'écrire $\{\pm 1\}$ à la place de $\mathbf{Z}/2\mathbf{Z}$.)

On sait (cf. [3], [13]) que cette extension peut se construire à l'aide du groupe des spineurs $\mathbf{Spin}_n(K)$. Rappelons comment on procède:

On identifie $\mathfrak{A}_n$ à un sous-groupe de $\mathbf{SO}_n(K)$ grâce au plongement standard de $\mathfrak{S}_n$ dans $\mathbf{O}_n(K)$, et l'on utilise la suite exacte de groupes algébriques:

$$1 \to \{\pm 1\} \to \mathbf{Spin}_n \to \mathbf{SO}_n \to 1. \tag{10}$$

Par passage aux points rationnels, on obtient une suite exacte:

$$1 \to \{\pm\} \to \mathbf{Spin}_n(K) \to \mathbf{SO}_n(K). \tag{11}$$

LEMME 1. *Le groupe $\mathfrak{A}_n$ est contenu dans l'image de l'homomorphisme*

$$\mathbf{Spin}_n(K) \to \mathbf{SO}_n(K),$$

et son image réciproque dans $\mathbf{Spin}_n(K)$ est isomorphe à $\tilde{\mathfrak{A}}_n$.

Autrement dit, on a un diagramme commutatif:

$$\begin{array}{ccccc} 1 \to \{\pm 1\} & \to & \tilde{\mathfrak{A}}_n & \to & \mathfrak{A}_n \\ \| & & \downarrow & & \downarrow \\ 1 \to \{\pm 1\} & \to & \mathbf{Spin}_n(K) & \to & \mathbf{SO}_n(K). \end{array}$$

Démonstration. Soit (e_i), $1 \leq i \leq n$, la base canonique de l'espace $V = K^n$, muni de la forme quadratique standard Q:

$$Q(e_i) = 1, \qquad Q(e_i, e_j) = 0 \quad \text{si} \quad i \neq j.$$

Soit C l'algèbre de Clifford du couple (V, Q), autrement dit l'algèbre engendrée par les e_i soumis aux relations

$$e_i^2 = 1, \qquad e_i e_j = -e_j e_i \quad \text{si} \quad i \neq j.$$

Le groupe $\mathbf{Spin}_n(K)$ s'identifie à un sous-groupe de C^*, le "groupe de Clifford réduit" au sens de Bourbaki, *Alg.* IX, §9, n° 5 (ensemble des $x \in C^*$ de degré pair tels que $xVx^{-1} = V$ et que $x \cdot x' = 1$, où $x \mapsto x'$ désigne l'anti-involution de C qui est l'identité sur V); l'homomorphisme $\mathbf{Spin}_n(K) \to \mathbf{SO}_n(K)$ associe à un tel élément x la rotation $v \mapsto xvx^{-1}$ de V.

Soient $\{i, j, k, l\}$ des indices tels que $i \neq j$ et $k \neq l$. On a

$$Q(e_i - e_j) = Q(e_k - e_l) = 2.$$

Si l'on pose

$$x = \tfrac{1}{2}(e_i - e_j)(e_k - e_l),$$

on vérifie tout de suite que x appartient au groupe de Clifford réduit, i.e. à $\mathbf{Spin}_n(K)$; de plus, son image dans $\mathbf{SO}_n(K)$ est égale à $(ij)(kl)$, produit des transpositions (ij) et (kl). Comme $\mathfrak{A}_n$ est engendré par de tels produits, cela montre bien que $\mathfrak{A}_n$ est contenu dans l'image de $\mathbf{Spin}_n(K)$. Il reste à voir que l'image réciproque de $\mathfrak{A}_n$ dans $\mathbf{Spin}_n(K)$ est une extension non triviale de $\mathfrak{A}_n$. Or, si l'on choisit $\{i, j, k, l\}$ distincts (ce qui est possible puisque $n \geqslant 4$), les éléments $e_i - e_j$ et $e_k - e_l$ sont orthogonaux, donc anticommutent dans C, et l'on en déduit:

$$x^2 = -\tfrac{1}{4}(e_i - e_j)^2(e_k - e_l)^2 = -\tfrac{1}{4} \cdot 2 \cdot 2 \cdot = -1.$$

Il en résulte que x *est d'ordre* 4 dans $\mathbf{Spin}_n(K)$, ce qui démontre la non trivialité de l'extension considérée.

Remarque. Le fait que $\mathfrak{A}_n$ soit contenu dans l'image de $\mathbf{Spin}_n(K)$ peut aussi se déduire de ce que $\mathfrak{A}_n$ est *engendré par des carrés*, donc a une image triviale par la norme spinorielle $\mathbf{SO}_n(K) \to K^*/K^{*2}$.

2.4. *Démonstration du théorème* 1 *dans le cas alterné*

Revenons à la situation du th. 1, et supposons que $e : \Gamma_K \to \mathfrak{S}_n$ applique Γ_K dans $\mathfrak{A}_n$, ou ce qui revient au même que $(d_E) = 0$. La formule à démontrer s'écrit alors:

$$w_2(Q_E) = e^* a_n, \tag{12}$$

où e est maintenant considéré comme un homomorphisme de Γ_K dans $\mathfrak{A}_n$.

La forme Q_E se déduit de la forme unité $Q(X) = X_1^2 + \cdots + X_n^2$ par torsion galoisienne au moyen du 1-cocycle $e : \Gamma_K \to \mathfrak{A}_n \subset \mathbf{SO}_n(K)$. Soit $\bar{e}$ la classe de e dans l'ensemble de cohomologie

$$H^1(K, \mathbf{SO}_n) = H^1(\Gamma_K, \mathbf{SO}_n(K_s)).$$

(Il s'agit ici de cohomologie non abélienne, cf. par exemple, [15], chap. I, §5 et chap. III, §1.)

Soit d'autre part

$$\delta : H^1(K, \mathbf{SO}_n) \to H^2(K, \{\pm 1\}) \simeq H^2(\Gamma_K)$$

l'opérateur cobord associé à la suite exacte

$$1 \to \{\pm 1\} \to \mathbf{Spin}_n \to \mathbf{SO}_n \to 1, \tag{10}$$

cf. [15], p. I-69. D'après Springer ([18], formule (4.6)), on a

$$w_2(Q_E) = \delta(\bar{e}). \tag{13}$$

On obtient un 2-cocycle $d(\alpha, \beta)$ appartenant à la classe $\delta(\bar{e})$ par la construction suivante:

Pour tout $\sigma \in \mathfrak{A}_n$, on choisit un représentant σ' de σ dans $\tilde{\mathfrak{A}}_n \subset \mathbf{Spin}_n(K)$, cf. lemme 1. Si $\alpha \in \Gamma_K$, l'élément $x_\alpha = e(\alpha)'$ de $\mathbf{Spin}_n(K_s)$ a pour image $e(\alpha)$ dans $\mathbf{SO}_n(K)$; si l'on pose

$$d(\alpha, \beta) = x_\alpha \alpha(x_\beta) x_{\alpha\beta}^{-1} \qquad (\alpha, \beta \in \Gamma_K), \tag{14}$$

on obtient un 2-cocycle sur Γ_K, à valeurs dans $\{\pm 1\}$, dont la classe de cohomologie est $\delta(\bar{e})$, cf. [18], *loc. cit.* Comme les x_α sont rationnels sur K, la formule (14) se simplifie en

$$d(\alpha, \beta) = x_\alpha x_\beta x_{\alpha\beta}^{-1}. \tag{15}$$

Le 2-cocycle d est donc simplement l'image réciproque par e du *système de facteurs* de l'extension $\tilde{\mathfrak{A}}_n \to \mathfrak{A}_n$ (relativement aux représentants choisis). On a donc:

$$\delta(\bar{e}) = e^* a_n, \tag{16}$$

ce qui démontre (12), compte tenu de (13).

2.5. *Un résultat auxiliaire*

Soient E_1 et E_2 deux algèbres étales, et soit $E_3 = E_1 \times E_2$ leur produit.

LEMME 2. *Si la formule* (1) *du th.* 1 *est vraie pour deux des trois algèbres* E_1, E_2, E_3, *elle est vraie pour la troisième.*

Soit n_i le rang de E_i, et soit e_i l'homomorphisme de Γ_K dans $\mathfrak{S}_{n_i}$ associé à E_i

$(i = 1, 2, 3)$. On a $n_3 = n_1 + n_2$, et l'homomorphisme $e_3 : \Gamma_K \to \mathfrak{S}_{n_3}$ se factorise en:

$$\Gamma_K \xrightarrow{(e_1, e_2)} \mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2} \xrightarrow{j} \mathfrak{S}_{n_3},$$

où j est l'injection naturelle de $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}$ dans $\mathfrak{S}_{n_3} = \mathfrak{S}_{n_1+n_2}$.

Posons:

$$w(E_i) = w_2(Q_{E_i}) \quad \text{et} \quad w'(E_i) = e_i^* s_{n_i} + (2)(d_{E_i}),$$

de sorte que (1) équivaut à $w(E_i) = w'(E_i)$.

Comme $Q_{E_3} \sim Q_{E_1} \oplus Q_{E_2}$, on a $(d_{E_3}) = (d_{E_1}) + (d_{E_2})$ et

$$w(E_3) = w(E_1) + w(E_2) + (d_{E_1})(d_{E_2}). \tag{17}$$

D'autre part, l'image de s_{n_3} par l'homomorphisme de restriction

$$j^* : H^2(\mathfrak{S}_{n_3}) \to H^2(\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2})$$

est donnée par la formule

$$j^* s_{n_3} = p_1^* s_{n_1} + p_2^* s_{n_2} + p_1^* \varepsilon_{n_1} \cdot p_2^* \varepsilon_{n_2},$$

où p_i désigne la projection de $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}$ sur son i-ème facteur (cela se voit, par exemple, en appliquant à l'espace classifiant $B(\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2})$ la formule donnant la classe de Stiefel–Whitney d'une somme directe).

On déduit de là:

$$\begin{aligned} e_3^* s_{n_3} &= (e_1, e_2)^* j^* s_{n_3} = (e_1, e_2)^* [p_1^* s_{n_1} + p_2^* s_{n_2} + p_1^* \varepsilon_{n_1} \cdot p_2^* \varepsilon_{n_2}] \\ &= e_1^* s_{n_1} + e_2^* s_{n_2} + e_1^* \varepsilon_{n_1} \cdot e_2^* \varepsilon_{n_2} = e_1^* s_{n_1} + e_2^* s_{n_2} + (d_{E_1})(d_{E_2}). \end{aligned}$$

En ajoutant $(2)(d_{E_3}) = (2)(d_{E_1}) + (2)(d_{E_2})$ aux deux membres, on obtient

$$w'(E_3) = w'(E_1) + w'(E_2) + (d_{E_1})(d_{E_2}). \tag{18}$$

En comparant (17) et (18) on voit que, si $w(E_i) = w'(E_i)$ pour deux des trois indices $\{1, 2, 3\}$, la même formule vaut pour le troisième indice. Le lemme en résulte.

2.6. *Fin de la démonstration du théorème* 1

Soit $E_2 = K[X]/(X^2 - d_E)$; c'est une K-algèbre étale de rang 2 ayant même discriminant que l'algèbre E donnée. La formule (1) est vraie pour E_2, cf. n° 2.2; elle est vraie pour $E \times E_2$ puisque le discriminant de $E \times E_2$ est 1, cf. n° 2.4; d'après le lemme 2, elle est donc vraie pour E, cqfd.

Remarques. 1) D'un point de vue "galoisien", la construction précédente revient à utiliser le plongement évident de $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$.

2) Le détour par le groupe alterné n'est pas indispensable. On peut faire des calculs analogues à ceux du n° 2.4 pour le groupe $\mathfrak{S}_n$ tout entier, à condition d'élargir le groupe $\mathbf{Spin}_n$ en un groupe $\tilde{\mathbf{O}}_n$ "deux fois plus grand", se projetant sur $\mathbf{O}_n$. Le groupe $\tilde{\mathfrak{S}}_n$ se réalise alors comme un sous-groupe de $\tilde{\mathbf{O}}_n(K_s)$ formé de points *rationnels sur* $K(\sqrt{2})$, mais pas sur K (sauf si 2 est un carré). La formule (14) ne se réduit plus à (15), mais à:

$$d(\alpha, \beta) = (x_\alpha x_\beta x_{\alpha\beta}^{-1})(\alpha(x_\beta)x_\beta^{-1}); \tag{15'}$$

le terme $(x_\alpha x_\beta x_{\alpha\beta}^{-1})$ donne $e^* s_n$ et le terme $(\alpha(x_\beta)x_\beta^{-1})$ donne $(2)(d_E)$.

§3. Applications

3.1. *Le problème de plongement associé à* $e^* s_n$

Soit E_g la sous-extension de K_s engendrée par les corps $\varphi(E)$, où φ parcourt l'ensemble Φ des K-homomorphismes de E dans K_s, cf. n° 1.3. C'est une extension galoisienne de K de groupe de Galois $G_E \subset \mathfrak{S}_n$.

Notons x_E l'image de s_n par $\mathrm{Res}: H^2(\mathfrak{S}_n) \to H^2(G_E)$, et notons $\tilde{G}_E$ l'extension centrale correspondante; le groupe $\tilde{G}_E$ s'identifie à l'image réciproque de G_E dans $\tilde{\mathfrak{S}}_n$, cf. n° 1.5. Si π désigne la projection $\Gamma_K \to G_E$, on a

$$e^* s_n = \pi^* x_E \quad \text{dans} \quad H^2(\Gamma_K) = \mathrm{Br}_2(K). \tag{19}$$

En d'autres termes, $e^* s_n$ est l'obstruction au *problème de plongement* associé à l'extension $\tilde{G}_E \to G_E$. Les deux propriétés suivantes sont équivalentes:

3.1.1. $e^* s_n = 0$.

3.1.2. *L'homomorphisme* $\pi: \Gamma_K \to G_E$ *se relève en un homomorphisme continu* $\tilde{\pi}: \Gamma_K \to \tilde{G}_E$.

Lorsque $x_E \neq 0$, i.e. lorsque $\tilde{G}_E$ est une extension non triviale de G_E, tout

homomorphisme $\tilde{\pi}$ satisfaisant à 3.1.2 est surjectif. Cela permet de reformuler 3.1.2 de la manière suivante:

3.1.3. *Il existe une sous-extension galoisienne $\tilde{E}_g$ de K_s contenant E_g, et un isomorphisme $\tilde{G}_E \simeq \mathrm{Gal}(\tilde{E}_g/K)$ tels que le diagramme*

$$\begin{array}{ccc} \tilde{G}_E & \simeq & \mathrm{Gal}(\tilde{E}_g/K) \\ \downarrow & & \downarrow \\ G_E & \simeq & \mathrm{Gal}(E_g/K) \end{array}$$

soit commutatif.

Le th. 1 ramène le calcul de e^*s_n à celui de l'invariant de Witt de la forme Q_E. Il permet, dans certains cas, de décider si les propriétés 3.1.1, 3.1.2 et 3.1.3 sont vraies ou non. Nous allons en voir quelques exemples.

3.2. *Extensions de degré 4 ou 5*

PROPOSITION 1. *Supposons $n = 4$ ou 5. Pour que $e^*s_n = 0$, il faut et il suffit que Q_E soit isomorphe*:

à la forme $X_1^2 + X_2^2 + 2X_3^2 + 2d_E X_4^2$ *si* $n = 4$,

à la forme $X_1^2 + X_2^2 + X_3^2 + 2X_4^2 + 2d_E X_5^2$ *si* $n = 5$.

Supposons d'abord $n = 4$. Si $Q_E \sim X_1^2 + X_2^2 + 2X_3^2 + 2d_E X_4^2$, on a $w_2(Q_E) = (2)(2d_E) = (2)(2) + (2)(d_E) = (2)(d_E)$ et le théorème 1 montre que $e^*s_n = 0$. Réciproquement, supposons que $e^*s_n = 0$, i.e. que $w_2(Q_E) = (2)(d_E)$. D'après la prop. 4 de l'App. I, on peut écrire Q_E sous la forme $X_1^2 + g(X_2, X_3, X_4)$, où g est une forme ternaire. On a $d(g) = d_E$ et $w_2(g) = w_2(Q_E) = (2)(d_E)$. Il en résulte que g a même discriminant et même invariant de Witt que $X_2^2 + 2X_3^2 + 2d_E X_4^2$. D'après [22], Satz 11, cela entraîne $g \sim X_2^2 + 2X_3^2 + 2d_E X_4^2$, d'où le résultat cherché.

Le même argument s'applique à $n = 5$, compte tenu de ce que

$$Q_E \sim X_1^2 + X_2^2 + g(X_3, X_4, X_5)$$

d'après la prop. 4 de l'App. I. (On peut aussi ramener le cas $n = 5$ au cas $n = 4$ par une extension convenable de degré impair du corps de base.)

EXEMPLE. Supposons que E soit une *extension biquadratique* de K, autrement dit un corps de degré 4, composé de trois extensions quadratiques $K(\sqrt{x})$,

$K(\sqrt{y})$ et $K(\sqrt{z})$ avec $xyz = 1$. Le groupe G_E est un groupe abélien élémentaire de type $(2, 2)$, et l'on vérifie facilement que $\tilde{G}_E$ est isomorphe au groupe H des quaternions. Si l'on prend $\{1, \sqrt{x}, \sqrt{y}, \sqrt{z}\}$ pour base de E, on voit que la forme Q_E est isomorphe à $T^2 + xX^2 + yY^2 + zZ^2$, et l'on a $d_E = 1$. En appliquant la prop. 1, on en déduit que e^*s_n *est nul* (i.e. que E peut être plongée dans une extension galoisienne $\tilde{E}$ de groupe de Galois H) *si et seulement si les formes* $xX^2 + yY^2 + zZ^2$ *et* $X^2 + Y^2 + Z^2$ *sont isomorphes* (noter en effet que $2Y^2 + 2Z^2$ est isomorphe à $Y^2 + Z^2$). On retrouve ainsi un résultat de Witt [21].

Remarque. Witt démontre davantage. Il donne un procédé permettant de *construire* $\tilde{E}$ à partir d'un isomorphisme de la forme $X^2 + Y^2 + Z^2$ sur la forme $xX^2 + yY^2 + zZ^2$. Il serait intéressant d'étendre sa construction à d'autres cas. (Signalons une faute d'impression dans [21], *Satz*, p. 244: le terme $r(p_{11}\xi_1 + p_{22}\xi_2 + p_{33}\xi_3)$ doit être remplacé par $r(1 + p_{11}\xi_1 + p_{22}\xi_2 + p_{33}\xi_3)$.)

Extensions icosaédriques du type de Klein

PROPOSITION 2. *Supposons que* $n = 5$, $d_E = 1$, *et que* 5 *soit un carré dans* K^*. *Les propriétés suivantes sont alors équivalentes*:

(a) $e^*s_n = (-1)(-1)$;
(b) $Q_E \sim X_1^2 + X_2^2 + X_3^2 - X_4^2 - X_5^2$;
(c) *Il existe* $x \in E$, $x \neq 0$, *tel que* $\mathrm{Tr}_{E/K}(x) = \mathrm{Tr}_{E/K}(x^2) = 0$;
(d) *L'extension* E_g/K *peut être construite par le procédé de Klein* (cf. [16]).

D'après le th. 1, (a) équivaut à $w_2(Q_E) = (-1)(-1)$. Notons Q'_E la forme quadratique de rang 4 obtenue en restreignant Q_E aux éléments $x \in E$ tels que $\mathrm{Tr}_{E/K}(x) = 0$. On a:

$$Q_E \sim 5X_1^2 \oplus Q'_E \sim X_1^2 \oplus Q'_E, \tag{20}$$

puisque 5 est un carré dans K^*. Cela permet de récrire (a), (b) et (c) en termes de Q'_E:

(a') $w_2(Q'_E) = (-1)(-1)$;
(b') $Q'_E \sim X_2^2 + X_3^2 - X_4^2 - X_5^2$;
(c') Q'_E représente 0.

D'autre part, la prop. 4 de l'App. I montre que

$$Q_E \sim X_1^2 + X_2^2 + g(X_3, X_4, X_5), \tag{21}$$

où g est une forme ternaire de discriminant 1. En comparant (20) et (21) on obtient:

$$Q'_E \sim X_2^2 + g(X_3, X_4, X_5), \tag{22}$$

et (a'), (b'), (c') se récrivent à leur tour:

(a'') $w_2(g) = (-1)(-1)$;
(b'') $g \sim X_3^2 - X_4^2 - X_5^2$;
(c'') g représente 0.

L'équivalence de ces propriétés est maintenant immédiate (cf. par exemple [22], Satz 11). Le fait que (a) et (c) soient équivalents à (d) est démontré dans [16].

3.3. *Extensions définies par une équation* $X^n + aX + b = 0$

Supposons que $E \simeq K[X]/(X^n + aX + b)$, avec $n \geqslant 2$, $a, b \in K$, le discriminant d du polynôme $X^n + aX + b$ étant $\neq 0$. On peut alors déterminer Q_E, $w_2(Q_E)$ et $e^* s_n$ en termes du couple (n, d), cf. App. II. On trouve (cor. à la prop. 7):

$$\begin{aligned} e^* s_n &= (-2)(d) + (-1)(-1) = (-2)(-d) \quad \text{si} \quad n = 4,5, \\ &= (3)(-d) + (-1)(-1) \quad \text{si} \quad \mathrm{car}(K) \neq 3 \quad \text{et} \quad n = 6,7, \\ &= (-1)(d) \quad \text{si} \quad n = 8,9, \\ &= (5)(-d) \quad \text{si} \quad \mathrm{car}(K) \neq 5 \quad \text{et} \quad n = 10,11, \\ &\ldots \\ &= 0 \quad \text{si} \quad n = 18,19,50,51,98,\ldots \end{aligned}$$

EXEMPLES. a) Supposons que $n = 7$ et $d = 1$, de sorte que G_E est un sous-groupe de $\mathfrak{A}_7$. On a $e^* s_7 = (-3)(-1)$. Il en résulte que le problème de plongement est résoluble si et seulement si -3 *est somme de* 2 *carrés* dans K.

Exemple numérique: $a = -154$, $b = 99$, et $[K: \mathbf{Q}] = 2$. Le groupe G_E est alors un groupe simple d'ordre 168, isomorphe à $\mathbf{PSL}_2(\mathbf{F}_7)$, cf. [5]; le groupe $\tilde{G}_E$ est isomorphe à $\mathbf{SL}_2(\mathbf{F}_7)$. On en conclut que, pour que E_g/K se plonge dans une extension galoisienne à groupe de Galois $\mathbf{SL}_2(\mathbf{F}_7)$, il faut et il suffit que K soit *imaginaire* et que 3 soit inerte ou ramifié dans $K/\mathbf{Q}$: en effet, on sait que ces conditions équivalent à dire que $(-3)(-1) = 0$ dans $\mathrm{Br}_2(K)$.

b) Supposons que $n = 18$ et $G_E = \mathfrak{S}_n$. Comme $e^* s_n = 0$, le problème de plongement a une solution: il existe une extension quadratique de E_g dont le groupe de Galois sur K est $\tilde{\mathfrak{S}}_n$. (Comment construire effectivement une telle extension?)

Pour d'autres exemples du même genre, voir [20].

3.4. *Exemples où* $K = \mathbf{Q}$ *et* $e^* s_n = 0$

Supposons que $K = \mathbf{Q}$, et définissons des entiers $r_1, r_2 \geqslant 0$ par la relation habituelle:

$$\mathbf{R} \otimes E \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}. \tag{23}$$

On a $r_1 + 2r_2 = n$. La *signature* de la forme Q_E est $(r_1 + r_2, r_2)$. Notons Q_{r_1,r_2} la forme quadratique à coefficients ± 1 ayant cette signature:

$$Q_{r_1,r_2} \sim X_1^2 + \cdots + X_{r_1+r_2}^2 - (X_{r_1+r_2+1}^2 + \cdots + X_n^2). \tag{24}$$

Nous allons comparer Q_E et Q_{r_1,r_2}:

PROPOSITION 3. *Les deux propriétés suivantes sont équivalentes*:

(a) $d_E = 1$ *et* $e^* s_n = 0$;
(b) $r_2 \equiv 0 \pmod 4$ *et* $Q_E \sim Q_{r_1,r_2}$.

Le discriminant de Q_{r_1,r_2} est $(-1)^{r_2}$, et son invariant de Witt est 0 (sur $\mathbf{Q}$, ou sur $\mathbf{R}$) si et seulement si $r_2 \equiv 0, 1 \pmod 4$. Si (b) est vérifié, on a donc $d_E = 1$ et $w_2(Q_E) = 0$, d'où $e^* s_n = 0$, ce qui prouve (a). Inversement, si (a) est vrai, r_2 est pair. De plus, Q_E est $\mathbf{R}$-isomorphe à Q_{r_1,r_2}, donc a même invariant de Witt sur $\mathbf{R}$; comme cet invariant est 0 (vu les hypothèses faites), cela montre que $r_2 \equiv 0 \pmod 4$. Il en résulte que les formes Q_E et Q_{r_1,r_2} ont même discriminant, même invariant de Witt, et même signature. Elles sont donc isomorphes, ce qui achève de prouver (b).

Exemples d'extensions satisfaisant à (a) *et* (b)

1) La propriété (a) est notamment vérifiée *lorsque le groupe* G_E *est tel que* $H^1(G_E) = H^2(G_E) = 0$. C'est le cas, par exemple, lorsque G est un groupe simple non abélien dont le multiplicateur de Schur est d'ordre impair. On trouvera la liste de ces groupes dans [7]; parmi les 26 groupes sporadiques, il y en a 17 qui conviennent: M_{11}, $M_{23}, \ldots$, et parmi eux le groupe de Griess–Fischer F_1. Comme Thompson a construit des extension de $\mathbf{Q}$ à groupe de Galois F_1 (cf. [19]), on peut leur appliquer la prop. 3: *la forme* Q_E *correspondante est isomorphe à la forme standard* Q_{r_1,r_2}. Signalons à ce sujet la question suivante: peut-on choisir E *totalement réelle* (i.e. $r_2 = 0$) telle que $G_E \simeq F_1$? (Noter que la méthode de Thompson fournit uniquement des extensions imaginaires.)

2) La propriété (a) est également vérifiée (sur un corps de base K quelconque) lorsque E est un corps, extension galoisienne de K, et que le groupe de Galois $G_E \simeq \mathrm{Gal}(E/K)$ est tel que *les deux premières classes de Stiefel–Whitney de sa représentation régulière sont nulles.* Les groupes finis satisfaisant à cette condition ont été déterminés par B. Kahn [8]. Il en est ainsi par exemple de:

a) tout groupe ayant un 2-groupe de Sylow non métacyclique,

b) tout groupe simple non abélien et non isomorphe à $\mathbf{PSL}_2(\mathbf{F}_q)$, $q \equiv \pm 3 \pmod 8$.

On peut donc appliquer la prop. 3 à toute extension galoisienne de $\mathbf{Q}$ ayant pour groupe de Galois l'un de ces groupes.

§4. Une généralisation: la forme $\mathrm{Tr}(\alpha x^2)$

4.1. *Enoncé du résultat*

Soit α un élément inversible de l'algèbre étale E. Si $x \in E$, posons

$$Q_{E,\alpha}(x) = \mathrm{Tr}_{E/K}(\alpha x^2).$$

On obtient ainsi une forme quadratique $Q_{E,\alpha}$, qui est non dégénérée de rang $n = \mathrm{rg}(E)$; pour $\alpha = 1$, on retrouve Q_E. On peut se poser les mêmes questions pour $Q_{E,\alpha}$ que pour Q_E. Les résultats sont tout à fait semblables, comme on va le voir.

Tout d'abord, si $\varphi_1, \ldots, \varphi_n$ sont les différents homomorphismes de E dans K_s, et si $\pm\beta_1, \ldots, \pm\beta_n$ sont les racines carrées de $\varphi_1(\alpha), \ldots, \varphi_n(\alpha)$, le groupe Γ_K opère sur les $\pm\beta_i$ par *permutations et changements de signes.* Cela conduit à introduire, à la place du groupe $\mathfrak{S}_n$ du n° 1.3, le groupe

$$\mathfrak{S}'_n = \{\pm 1\}^n \cdot \mathfrak{S}_n,$$

d'ordre $2^n n!$, produit semi-direct de $\{\pm 1\}^n$ et de $\mathfrak{S}_n$ (ce dernier opérant sur $\{\pm 1\}^n$ de façon évidente). Une autre façon de définir $\mathfrak{S}'_n$ est de dire que c'est le groupe de Weyl d'un système de racines de type B_n ou C_n, cf. Bourbaki LIE. VI.

L'action de Γ_K sur les φ_i et les $\pm\beta_i$ définit un homomorphisme

$$e_\alpha : \Gamma_K \to \mathfrak{S}'_n,$$

qui caractérise le couple (E, α), à la multiplication près de α par un carré. Ici encore, $\mathfrak{S}'_n$ s'identifie à un sous-groupe du groupe orthogonal $\mathbf{O}_n(K)$, et la forme

$Q_{E,\alpha}$ se déduit de la forme standard $\sum X_i^2$ par *torsion* au moyen du 1-cocycle

$$e_\alpha : \Gamma_K \to \mathfrak{S}'_n \subset \mathbf{O}_n(K).$$

Le *discriminant* de $Q_{E,\alpha}$ est donné par:

$$d(Q_{E,\alpha}) = d_E \cdot N\alpha,$$

où $N\alpha = N_{E/K}(\alpha)$ est la norme de α; cela se vérifie, soit par un calcul direct, soit en explicitant l'homomorphisme $\det : \mathfrak{S}'_n \to \{\pm 1\}$.

En ce qui concerne *l'invariant de Witt* de $Q_{E,\alpha}$, on procède comme pour Q_E. On définit d'abord un élément canonique s'_n de $H^2(\mathfrak{S}'_n)$ par la méthode de la fin du n° 1.5, i.e.

$$s'_n = w_2(l'_n),$$

où l'_n est le fibré orthogonal sur $B\mathfrak{S}'_n$ associé à la représentation évidente $\mathfrak{S}'_n \to \mathbf{O}_n(\mathbf{R})$. L'extension centrale $\tilde{\mathfrak{S}}'_n$ correspondant à s'_n est décrite par générateurs et relations dans [3], p. 619 (prendre $\gamma = \lambda = \mu = -1$). L'analogue du théorème 1 est:

THÉORÈME 1'. *On a*

$$w_2(Q_{E,\alpha}) = e_\alpha^* s'_n + (2)(d_E). \tag{25}$$

Noter que, dans le terme $(2)(d_E)$, c'est bien d_E qui intervient, et non $d(Q_{E,\alpha})$.

4.2. *Démonstration du théorème* 1'

On peut procéder de diverses manières. J'en indique deux, sans entrer dans les détails:

Première démonstration

Elle consiste à se ramener au th. 1, grâce à l'algèbre de rang $2n$:

$$E' = E[X]/(X^2 - \alpha).$$

Notons E'_0 l'ensemble des $x \in E'$ tels que $\mathrm{Tr}_{E'/E}(x) = 0$. L'espace vectoriel E' est somme directe de E et de E'_0. De plus, ces sous-espaces sont orthogonaux pour la forme $Q_{E'}$, et la restriction de $Q_{E'}$ à E (resp. E'_0) est $2Q_E$ (resp. $2Q_{E,\alpha}$). On a

donc:

$$Q_{E'} \sim 2Q_E \oplus 2Q_{E,\alpha}. \tag{26}$$

En appliquant le th. 1 à E et E', on obtient les valeurs de $w_2(Q_{E'})$ et $w_2(2Q_E)$, d'où, grâce à (26), la valeur de $w_2(Q_{E,\alpha})$. La formule (25) s'en déduit par un calcul sans difficulté (remarquer que la représentation $\Gamma_K \to \mathfrak{S}_{2n} \subset \mathbf{O}_{2n}(\mathbf{R})$ associée à E' est somme directe de $\Gamma_K \to \mathfrak{S}_n \subset \mathbf{O}_n(\mathbf{R})$ et $\Gamma_K \to \mathfrak{S}'_n \subset \mathbf{O}_n(\mathbf{R})$).

Seconde démonstration

Elle imite la démonstration du th. 1. On traite d'abord le cas où l'image de Γ_K dans $\mathfrak{S}'_n$ est contenue dans le sous-groupe $\mathfrak{A}'_n$ entendré par $\mathfrak{A}_n$ et par les éléments $(\varepsilon_i) \in \{\pm 1\}^n$ tels que $\prod \varepsilon_i = 1$ (cela revient à supposer $(d_E) = (N\alpha) = 0$). Notons a'_n la restriction de s'_n à $\mathfrak{A}'_n$, et soit $\tilde{\mathfrak{A}}'_n$ l'extension centrale correspondante. Comme au n° 2.3, on a un diagramme commutatif:

$$\begin{array}{ccccc} 1 \to \{\pm 1\} \to & & \tilde{\mathfrak{A}}'_n & \to & \mathfrak{A}'_n \\ \| & & \downarrow & & \downarrow \\ 1 \to \{\pm 1\} \to & \mathbf{Spin}_n(K) & & \to & \mathbf{SO}_n(K). \end{array}$$

La démonstration du n° 2.4 s'applique alors sans changement, et montre que $w_2(Q_{E,\alpha}) = e_\alpha^* a'_n$, d'où le th. 1' dans le cas considéré.

Le cas général se ramène au précédent par un procédé analogue à celui du n° 2.6. On utilise les couples (E_1, α_1) et (E_2, α_2) suivants:

$$E_1 = K, \qquad \alpha_1 = N\alpha$$
$$E_2 = K[X]/(X^2 - d_E), \qquad \alpha_2 = 1.$$

Le th. 1' se vérifie immédiatement pour ces couples, ainsi que pour leur produit $(E_1 \times E_2, (\alpha_1, \alpha_2))$. D'autre part, le produit

$$(E \times E_1 \times E_2, (\alpha, \alpha_1, \alpha_2))$$

est du type ci-dessus (i.e. correspond à un homomorphisme de Γ_K dans $\mathfrak{A}'_{n+3}$). On peut donc lui appliquer le th. 1'. On passe de là à (E, α) par un lemme analogue au lemme 2 du n° 2.5.

Appendice I. Une décomposition de Q_E

Ecrivons le rang n de E sous forme dyadique:

$$n = 2^{m_1} + \cdots + 2^{m_h}, \quad \text{avec} \quad 0 \leq m_1 < m_2 < \cdots < m_h.$$

PROPOSITION 4. (a) *Si* $\sum m_i$ *est pair, on a*

$$Q_E \sim X_1^2 + \cdots + X_h^2 + g(X_{h+1}, \ldots, X_n),$$

où g *est une forme quadratique de rang* $n-h$ *et de discriminant* d_E.

(b) *Si* $\sum m_i$ *est impair, on a*

$$Q_E \sim 2X_1^2 + X_2^2 + \cdots + X_h^2 + g(X_{h+1}, \ldots, X_n),$$

où g *est une forme quadratique de rang* $n-h$ *et de discriminant* $2d_E$.

EXEMPLES. Si $n=3$, on a $m_1=0$, $m_2=1$, $h=2$, et g est une forme à 1 variable de discriminant $2d_E$; on retrouve le fait que Q_E est isomorphe à $2X_1^2 + X_2^2 + 2d_E X_3^2$, cf. n° 2.2.

Si $n=5$, on a $m_1=0$, $m_2=2$, $h=2$, et l'on voit que

$$Q_E \sim X_1^2 + X_2^2 + g(X_3, X_4, X_5),$$

où g est une forme à 3 variables de discriminant d_E. Il en résulte ([22], Satz 11) que Q_E est bien déterminé par ses deux invariants d_E et $w_2(Q_E)$.

LEMME 3. *Il existe une extension finie* K' *de* K, *de degré impair, telle que la* K'*-algèbre* $E' = K' \otimes_K E$ *se décompose en produit d'algèbres* E'_i $(1 \leq i \leq h)$ *de rangs* 2^{m_i}.

Soit $G_E = e(\Gamma_K)$ le groupe de Galois de E, considéré comme sous-groupe de $\mathfrak{S}_n$ (n° 1.3). Soit P un 2-sous-groupe de Sylow de G_E, et soit K' l'extension de K correspondant à P. Le degré de K' sur K est égal à $(G_E : P)$, qui est impair. Comme $e(\Gamma_{K'}) = P$, les orbites de $e(\Gamma_{K'})$ dans $[1, n]$ ont pour ordres des puissances de 2. Il en résulte une décomposition de E' en produit

$$E' = \prod E'_j \qquad (1 \leq j \leq k),$$

où le rang n_j de chaque E'_j est une puissance de 2. Choisissons une telle décomposition avec le moins de facteurs possible, i.e. avec k minimum. Les n_j

sont alors distincts: en effet, si l'on avait $n_j = n_l$ pour $j \neq l$, on pourrait regrouper E'_j et E'_l, et remplacer k par $k-1$. Comme $n = \sum n_j$, ceci entraîne que les n_j sont égaux aux 2^{m_i}, à l'ordre près; d'où le lemme.

LEMME 4. *Soient φ et ψ des formes quadratiques sur K. Soit K' une extension finie de K de degré impair, et soit g' une forme quadratique sur K' telle que $\varphi \sim \psi \oplus g'$ sur K'. Il existe alors une forme quadratique g sur K telle que $\varphi \sim \psi \oplus g$.*

Soit k le rang de ψ. Pour qu'il existe g avec $\varphi \sim \psi \oplus g$, il faut et il suffit que l'indice sur K de la forme $\varphi \oplus (-\psi)$ soit $\geqslant k$ (cf. [22]). Or, d'après un théorème de Springer [17], cet indice est le même sur K et sur K'. D'où le résultat.

LEMME 5. *La forme quadratique $2^{m_1}X_1^2 + \cdots + 2^{m_h}X_h^2$ est isomorphe:*

à la forme $X_1^2 + \cdots + X_h^2$ si $\sum m_i$ est pair,

à la forme $2X_1^2 + X_2^2 + \cdots + X_h^2$ si $\sum m_i$ est impair.

On peut évidemment remplacer le coefficient 2^{m_i} par 1 si m_i est pair, et par 2 si m_i est impair. Cela montre que la forme considérée est isomorphe à:

$$2(X_1^2 + \cdots + X_r^2) + X_{r+1}^2 + \cdots + X_h^2,$$

où r est le nombre des indices i tels que m_i soit impair. Le lemme en résulte, compte tenu de ce que $2X^2 + 2Y^2 \sim X^2 + Y^2$.

Démonstration de la prop. 4

Vu les lemmes 3 et 4, on peut supposer que E se décompose en produit:

$$E = \prod E_i, \quad \text{avec} \quad \operatorname{rg}(E_i) = 2^{m_i}, \qquad 1 \leqslant i \leqslant h.$$

On a $Q_E \sim Q_{E_1} \oplus \cdots \oplus Q_{E_h}$. Comme $Q_{E_i}(1) = \operatorname{Tr}_{E_i/K}(1) = 2^{m_i}$, la forme Q_{E_i} se décompose en:

$$Q_{E_i} \sim 2^{m_i}X^2 \oplus g_i, \quad \text{avec} \quad \operatorname{rg}(g_i) = 2^{m_i} - 1.$$

On en déduit une décomposition de Q_E:

$$Q_E \sim 2^{m_1}X_1^2 + \cdots + 2^{m_h}X_h^2 + g(X_{h+1}, \ldots, X_n),$$

et l'on conclut en appliquant le lemme 5.

Appendice II. Détermination de Q_E lorsque E est définie par une équation de la forme $X^n + aX + b = 0$

Soient a et b deux éléments de K, et soit n un entier ≥ 2. Posons

$$f(X) = X^n + aX + b.$$

Le discriminant d de f est donné par la formule:

$$d = (-1)^{n(n-1)/2} n^n b^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} a^n. \tag{27}$$

Supposons $d \neq 0$. L'algèbre $E = K[X]/(X^n + aX + b)$ est alors étale, et $(d_E) = (d)$. Nous allons voir que l'on peut expliciter la forme quadratique Q_E en fonction seulement de n et de d (cf. prop. 5 et 6 ci-dessous). Ce résultat m'a été signalé par P. E. Conner, pour n impair (le cas n pair est d'ailleurs plus facile); on trouvera dans la thèse de N. Vila [20] des résultats analogues pour certaines équations du type $X^n + aX^2 + bX + c = 0$.

Il est commode de séparer les cas suivant la parité de n:

PROPOSITION 5. *Supposons n pair. On a alors*:

$$Q_E \sim X_1X_2 + X_3X_4 + \cdots + X_{n-1}X_n \quad \textit{si} \quad \text{car}\,(K) \textit{ divise } n, \tag{28}$$

et

$$Q_E \sim nX_1^2 - (-1)^{n/2} n\, dX_2^2 + X_3X_4 + \cdots + X_{n-1}X_n \quad \textit{sinon.} \tag{29}$$

Soit x l'image de X dans E. Les x^i $(0 \leq i \leq n-1)$ forment une base de E. D'après les formules de Newton, on a

$$\text{Tr}_{E/K}(1) = n \quad \text{et} \quad \text{Tr}_{E/K}(x^i) = 0 \quad \text{pour} \quad 1 \leq i \leq n-2. \tag{30}$$

Si la caractéristique de K divise n, le sous-espace de E engendré par $1, x, \ldots, x^{(n-2)/2}$ est totalement isotrope de dimension $n/2$; la forme Q_E est donc hyperbolique, d'où (28).

Supposons maintenant que car (K) ne divise pas n, et décomposons E en somme orthogonale

$$E = K \cdot 1 \oplus E',$$

où E' est l'hyperplan des éléments de trace 0. On en déduit $Q_E \sim nX_1^2 \oplus Q'_E$, où Q'_E est la restriction de Q_E à E'. D'après (30) les vecteurs $x, x^2, \ldots, x^{(n-2)/2}$

engendrent un sous-espace totalement isotrope de E' de dimension $(n-2)/2$. On a donc

$$Q'_E \sim cX_2^2 + X_3X_4 + \cdots + X_{n-1}X_n, \quad \text{avec} \quad c \in K^*.$$

Comme $d = d(Q_E) = nd(Q'_e) = nc(-1)^{(n-2)/2}$ (dans K^*/K^{*2}), on a

$$c = -(-1)^{n/2}nd,$$

d'où (29).

PROPOSITION 6. *Supposons n impair. On a alors*

$$Q_E \sim X_1^2 + X_2X_3 + X_4X_5 + \cdots + X_{n-1}X_n \quad \textit{si} \quad \text{car}(K) \textit{ divise } n-1, \tag{31}$$

et

$$Q_E \sim X_1^2 + (n-1)X_2^2 + (-1)^{(n-3)/2}(n-1)\,dX_3^2 + X_4X_5 + \cdots + X_{n-1}X_n \quad \textit{sinon.} \tag{32}$$

On définit comme ci-dessus les x^i, l'hyperplan E' et la forme Q'_E. Si car (K) divise $n-1$, on a $n=1$ dans K, d'où $Q_E \sim X_1^2 \oplus Q'_E$. De plus, les vecteurs x, $x^2, \ldots, x^{(n-1)/2}$ engendrent un sous-espace totalement isotrope de E' de dimension $(n-1)/2$: cela se voit en utilisant les formules (30) ainsi que le fait que $\mathrm{Tr}_{E/K}(x^{n-1}) = (1-n)a = 0$. La forme Q'_E est donc hyperbolique, d'où (31).

Supposons maintenant que car (K) ne divise pas $n-1$, et que $a \neq 0$. Soit V le sous-espace de E engendré par les vecteurs

$$e_1 = 1 + a^{-1}x^{n-1} \quad \text{et} \quad e_2 = a^{-1}x^{n-1}.$$

En utilisant les formules

$$\mathrm{Tr}_{E/K}(x^{n-1}) = (1-n)a \quad \text{et} \quad \mathrm{Tr}_{E/K}(x^{2n-2}) = (n-1)a^2,$$

on voit que

$$\mathrm{Tr}_{E/K}(e_1e_1) = 1, \qquad \mathrm{Tr}_{E/K}(e_1e_2) = 0 \quad \text{et} \quad \mathrm{Tr}_{E/K}(e_2e_2) = n-1.$$

On en déduit:

$$Q_E \sim X_1^2 + (n-1)X_2^2 \oplus Q''_E,$$

où Q''_E est la restriction de Q_E à l'orthogonal E'' de V dans E.

Les vecteurs x^i, avec $(n+1)/2 \leq i \leq n-2$, engendrent un sous-espace totalement isotrope de E'' de dimension $(n-3)/2$. On a donc:

$$Q''_E \sim cX_3^2 + X_4X_5 + \cdots + X_{n-1}X_n, \quad \text{avec} \quad c \in K^*.$$

Comme $d = d(Q_E) = (n-1)d(Q''_E) = (n-1)c(-1)^{(n-3)/2}$, on a

$$c = (n-1)d(-1)^{(n-3)/2} \qquad (\text{dans } K^*/K^{*2}),$$

d'où (32).

Reste le cas où $a = 0$ et où car (K) ne divise pas $n-1$. La formule (27) montre alors que car (K) ne divise pas n (sinon d serait 0), et que $d = (-1)^{(n-1)/2}n$ dans K^*/K^{*2}. On a donc $Q_E \sim nX_1^2 \oplus Q'_E$. Comme les vecteurs x, $x^2, \ldots, x^{(n-1)/2}$ engendrent un sous-espace totalement isotrope de E' de dimension $(n-1)/2$, la forme Q'_E est hyperbolique. D'où:

$$Q_E \sim nX_1^2 + X_2X_3 + X_4X_5 + \cdots + X_{n-1}X_n.$$

Pour prouver (32), il suffit donc de montrer que les deux formes

$$X_1^2 + (n-1)X_2^2 + (-1)^{(n-3)/2}(n-1)\,dX_3^2 \quad \text{et} \quad nX_1^2 + X_2X_3$$

sont équivalentes. Or, dans la première de ces formes, on peut remplacer d par $(-1)^{(n-1)/2}n$, ce qui donne $X_1^2 + (n-1)X_2^2 - n(n-1)X_3^2$; on obtient ainsi une forme ternaire de discriminant $-n$, qui représente 0 (prendre $X_1 = n-1$, $X_2 = X_3 = 1$); elle est donc bien équivalente à $nX_1^2 + X_2X_3$, cqfd.

Calcul de l'invariant de Witt de Q_E

On pose $m = [n/4]$, de sorte que $n = 4m$, $4m+1$, $4m+2$ ou $4m+3$.

PROPOSITION 7. *Si $n = 4m$ ou $4m+1$, on a:*

$$w_2(Q_E) = \begin{cases} 0 & \text{si car } (K) \text{ divise } m \\ (-4m)(d) + m(-1)(-1) & \text{sinon.} \end{cases}$$

Si $n = 4m+2$ ou $4m+3$, on a:

$$w_2(Q_E) = \begin{cases} 0 & \text{si car } (K) \text{ divise } 2m+1 \\ (4m+2)(-d) + m(-1)(-1) & \text{sinon.} \end{cases}$$

Traitons par exemple le cas $n = 4m+1$ (les autres cas sont analogues). Si car (K) divise m, la prop. 6 montre que

$$Q_E \sim X_1^2 + \cdots + X_{2m+1}^2 - (X_{2m+2}^2 + \cdots + X_{4m+1}^2).$$

On en déduit:

$$w_2(Q_E) = m(-1)(-1) = 0,$$

car $(-1)(-1) = 0$ dans tout corps de caractéristique $\neq 0$.

Si car (K) ne divise pas m, on a, d'après (32):

$$Q_E \sim X_1^2 + \cdots + X_{2m}^2 - (X_{2m+1}^2 + \cdots + X_{4m-1}^2) + 4mX_{4m}^2 - 4mdX_{4m+1}^2,$$

d'où

$$w_2(Q_E) = (-1)(-1) + m(-1)(-1) + (-1)(4m) + (-1)(-4md) + (4m)(-4md).$$

En développant, et en utilisant la formule connue $(x)(-x) = 0$, on obtient bien

$$w_2(Q_E) = (-4m)(d) + m(-1)(-1).$$

COROLLAIRE. *Si* $n = 4m$ *ou* $4m+1$, *on a*:

$$e^* s_n = \begin{cases} 0 & \text{si car } (K) \text{ divise } m \\ (-2m)(d) + m(-1)(-1) & \text{sinon.} \end{cases}$$

Si $n = 4m+2$ *ou* $4m+3$, *on a*:

$$e^* s_n = \begin{cases} 0 & \text{si car } (K) \text{ divise } 2m+1 \\ (2m+1)(-d) + m(-1)(-1) & \text{sinon.} \end{cases}$$

On applique la formule $e^* s_n = w_2(Q_E) + (2)(d)$, en tenant compte de ce que $(2)(-1) = 0$ [noter que, d'après (27), on a $d = \pm 1$ si $n = 4m$ ou $4m+1$ (resp. $4m+2$ ou $4m+3$), et car (K) divise m (resp. $2m+1$)].

BIBLIOGRAPHIE

[1] A.-M. Bergé et J. Martinet, *Formes quadratiques et extensions en caractéristique* 2, à paraître.

[2] P. E. Conner et R. Perlis, *A Survey of Trace Forms of Algebraic Number Fields*, World Scient. Publ., Singapore, 1984.

[3] J. W. DAVIES et A. O. MORRIS, *The Schur Multiplier of the Generalized Symmetric Group*, J. London Math. Soc. (2), *8* (1974), 615–620.
[4] A. DELZANT, *Définition des classes de Stiefel–Whitney d'un module quadratique sur un corps de caractéristique différente de* 2, C. R. Acad. Sci. Paris, *255* (1962), 1366–1368.
[5] J. FISCHER et J. MCKAY, *Polynomials with* PSL(2, 7) *as Galois Group*, J. Number Theory, *11* (1979), 69–75.
[6] V. P. GALLAGHER, *Local Trace Forms*, Linear and Multilinear Algebra, 7 (1979), 167–174.
[7] R. L. GRIESS, *Schur Multipliers of the Known Finite Simple Groups* II, Santa Cruz Conf. on Finite Groups, Proc. Symp. Pure Maths. A.M.S., *37* (1980), 279–282.
[8] B. KAHN, *La deuxième classe de Stiefel–Whitney d'une représentation régulière*, I, II. C.R. Acad. Sci. Paris, série I, *297* (1983), 313–316 et 573–576.
[9] T. Y. LAM, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin Publ., Reading, Mass., 1965.
[10] D. MAURER, *Invariants of the Trace Form of a Number Field*, Linear and Multilinear Algebra, 6 (1978/79), 33–36.
[11] J. MILNOR, *Algebraic K-Theory and Quadratic Forms*, Invent. Math. *9* (1970), 318–344.
[12] W. SCHARLAU, *Quadratischen Formen und Galois-Cohomologie*, Invent. Math., *4* (1967), 238–264.
[13] I. SCHUR, *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, J. Crelle, *139* (1911), 155–250 (= *Ges. Abh.* I, 346–441).
[14] J.-P. SERRE, *Corps Locaux*, 3 ème édition, Hermann, Paris, 1968.
[15] J.-P. SERRE, *Cohomologie Galoisienne*, 4 ème édit., Lect. Notes in Math., *5* (1973), Springer-Verlag, Heidelberg.
[16] J.-P. SERRE, *Extensions Icosaédriques*, Sém. Théorie des Nombres, Bordeaux, 1979/80, exposé 19.
[17] T. A. SPRINGER, *Sur les formes quadratiques d'indice zéro*, C.R. Acad. Sci. Paris, *244* (1952), 1517–1519.
[18] T. A. SPRINGER, *On the Equivalence of Quadratic Forms*, Proc. Neder. Acad. Sci., *62* (1959), 241–253.
[19] J. THOMPSON, *Some Finite Groups which appear as* Gal L/K, *where* $K \subseteq \mathbf{Q}(\mu_n)$, J. of Algebra, *89* (1984), 437–499.
[20] N. VILA, *Sobre la realitzacio de les extensions centrals del grup alternat com a grup de Galois sobre el cos dels racionals*, Thèse, Univ. Auton. Barcelone, 1983.
[21] E. WITT, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung* p^f, J. Crelle, *174* (1936), 237–245.
[22] E. WITT, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Crelle, *176* (1937), 31–44.

Collège de France,
75231 Paris Cedex 05

Reçu le 30 mai 1984