ANNALES DE L'INSTITUT FOURIER

ANNE-MARIE BERGÉ
JACQUES MARTINET

Formes quadratiques et extensions en caractéristique 2

Annales de l'institut Fourier, tome 35, n° 2 (1985), p. 57-77
<http://www.numdam.org/item?id=AIF_1985__35_2_57_0>

© Annales de l'institut Fourier, 1985, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
35, 2 (1985), 57-77.

FORMES QUADRATIQUES ET EXTENSIONS EN CARACTÉRISTIQUE 2

par A.-M. BERGÉ et J. MARTINET

Introduction.

Soit K un corps, et soit E une K-algèbre étale, c'est-à-dire un produit fini d'extensions séparables finies de K (cf. [3], A V.28). Lorsque K n'est pas de caractéristique 2, la forme quadratique $x \mapsto \mathrm{Tr}_{E/K}(x^2)$ est non dégénérée. A une forme non dégénérée sont attachés classiquement trois invariants : le rang (ici, le degré n de E/K), le discriminant dans K^*/K^{*2} (ici, le discriminant de l'algèbre) et l'invariant de Hasse-Witt (cf. [7], p. 122), qui est un élément d'ordre 1 ou 2 du groupe de Brauer de K ; un procédé permettant le calcul de cet invariant pour la forme $x \mapsto \mathrm{Tr}_{E/K}(x^2)$ a été donné par Serre ([12]).

Lorsque K est de caractéristique 2, la forme ci-dessus est de rang 0, et il est naturel de lui chercher un substitut. Pour $k = 1, \ldots, n$, associons à tout élément x de E sa « k-ième trace » $T_k(x)$ définie à l'aide du polynôme caractéristique χ_x de x par la formule :

$$\chi_x(X) = X^n - T_1(x)X^{n-1} + T_2(x)X^{n-2} + \cdots + (-1)^n T_n(x).$$

Il est clair que T_2 est une forme quadratique sur E. On vérifie qu'elle est de rang maximum, i.e. n ou $n-1$ selon la parité de n (cf. § 2). En remplaçant l'algèbre E par l'algèbre $E \times K$ lorsque n est impair, on voit que l'on peut associer à E une forme quadratique non dégénérée (de rang n ou $n+1$); c'est cette forme que nous étudions dans cet article. (Voir aussi [8].)

Dans le § 1 et son appendice 1 bis, on étudie l'invariant de Arf d'un espace quadratique non dégénéré (V, Q) : c'est un élément de $K/\mathscr{P}(K)$ ($\mathscr{P}$

Mots-clés : Formes quadratiques - Discriminants - Équations algébriques - Polynômes.

désigne l'application d'Artin-Schreier $x \mapsto x^2 + x$), qui est l'analogue en caractéristique 2 du groupe K^*/K^{*2} en caractéristique $\neq 2$. On définit plus précisément, à l'aide de relèvements en caractéristique 0, un invariant de Arf dans K attaché à une base de V, qui coïncide modulo $\mathscr{P}(K)$ avec l'invariant de Arf de (V, Q).

Dans le § 2, on applique ces résultats au cas d'une algèbre E. En corrigeant l'invariant de Arf par un « signe additif », on définit le discriminant additif appartenant à $K/\mathscr{P}(K)$; il est additif vis-à-vis du produit direct des algèbres. De plus, on montre que l'extension quadratique séparable de K (ou K lui-même) définie à isomorphisme près par le discriminant additif est celle qui est associée à l'algèbre par la théorie de Galois au moyen d'un calcul de signature (comparer avec [3]. A V.151-152, exer. 23, où est également utilisé un relèvement en caractéristique zéro pour l'étude de la forme bilinéaire $(x,y) \mapsto \mathrm{Tr}(xy)$; voir aussi [2]; noter que la relation entre discriminant additif et invariant de Arf est conjecturée et démontrée dans un cas particulier dans [8]).

Dans le § 3, on détermine la classe d'isométrie de T_2 sur E ou sur $E \times K$. Le résultat est que cet espace quadratique est caractérisé par son invariant de Arf et sa dimension; on montre en particulier que son algèbre de Clifford est décomposée.

Enfin, dans le § 4, inspiré par l'article [11] de Serre, on utilise les résultats du § 3 pour réduire des équations, à la façon de Klein. Un résultat typique est le suivant : une extension de degré 5 peut être définie par un polynôme de la forme $X^5 + tX + t$ (dépendant donc d'un seul paramètre) si et seulement si son invariant de Arf est nul.

Postérieurement à l'envoi de cet article, nous avons appris l'existence d'un « preprint » de Wadsworth [15], dans lequel est également étudiée la relation entre invariant de Arf et discriminant additif qui fait l'objet du paragraphe 2. En particulier, la conjecture proposée par Revoy dans [8] y est aussi démontrée.

Par sa lecture attentive de notre manuscrit, le « referee » nous a permis de corriger un certain nombre d'erreurs; nous l'en remercions, et le remercions en outre de nous avoir permis d'attribuer à C.T.C. Wall le lemme 4.1.

Cet article reproduit à quelques changements mineurs près, avec l'accord des organisateurs, le texte d'un exposé fait le 3 juin 1983 au Séminaire de Théorie des Nombres de Bordeaux.

1. Relèvement en caractéristique 0.

Rappelons les définitions classiques, afin de fixer nos notations, qui diffèrent un peu des notations en usage sur un corps de caractéristique $\neq 2$.

Soit A un anneau commutatif unitaire, et soit M un A-module libre de rang fini n, muni d'une forme quadratique Q. La forme bilinéaire symétrique s_Q associée à Q

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

vérifie, pour tout $x \in M$, la relation $s_Q(x,x) = 2Q(x)$; elle est donc paire. Soit $(e_i)_{1 \leqslant i \leqslant n}$ une base de M sur A. Pour $x = \sum_i x_i e_i \in M$, on a :

$$Q(x) = \sum_i x_i^2 Q(e_i) + \sum_{i<j} x_i x_j s_Q(e_i, e_j).$$

Nous représentons la forme quadratique par la matrice triangulaire supérieure $C = (c_{ij})$ où c_{ij} vaut 0 pour $i > j$, $Q(e_i)$ pour $i = j$, et $s_Q(e_i, e_j)$ pour $i < j$. La matrice de s_Q dans cette base est donc $C + {}^tC$, et son déterminant s'appelle discriminant de Q dans la base (e_i). C'est un élément de A, inversible si et seulement si s_Q est non dégénérée, c'est-à-dire identifie M à son dual. On dit alors que la forme quadratique Q est non dégénérée. Nous allons montrer une propriété modulo 4 de ce discriminant. Pour cela, on utilise la matrice alternée $C - {}^tC$.

PROPOSITION 1.1. — *On suppose l'anneau* A *intègre, local, de caractéristique* 0 *et de caractéristique résiduelle* 2, *et la forme* Q *non dégénérée. Le rang* n *du* A*-module* M *est alors pair, et le « discriminant à signe »* $(-1)^{n/2} \det(C+{}^tC)$ *est congru modulo* 4A *au carré d'une unité. Plus précisément, on a :*

$$(-1)^{n/2} \det(C+{}^tC) = \det(C-{}^tC).(1+4a),$$

où l'élément a *de* A *ne dépend modulo* 2 *que de la réduction de* Q *modulo* 2.

Démonstration. — La matrice alternée $R = C - {}^tC$ est inversible, car elle est congrue modulo 2 à la matrice $S = C + {}^tC$; son ordre n est donc pair, et son déterminant est égal au carré d'une unité de A (cf.

l'appendice à ce paragraphe). Notons χ_P le polynôme caractéristique d'une matrice P d'ordre n à coefficients dans A :

$$\chi_P(X) = \det(XI_n - P) = X^n - T_1(P)X^{n-1} + T_2(P)X^{n-2} + \cdots + (-1)^n T_n(P) \in A[X].$$

De la relation $S = -R + 2C = -2R\left(\frac{1}{2}I_n - R^{-1}C\right)$, on tire

$$\det S = (-2)^n \det R \,.\, \chi_{R^{-1}C}(1/2),$$

d'où la congruence modulo 8A :

$$\det S \equiv \det R(1 - 2T_1(R^{-1}C) + 4T_2(R^{-1}C)).$$

Comme on a $I_n = R^{-1}C - R^{-1}\,{}^tC$, et que les matrices $R^{-1}C$ et $-R^{-1}\,{}^tC = {}^t(CR^{-1})$ ont même trace, l'élément $1 - 2T_1(R^{-1}C)$ vaut $1 - n$, $\wedge$ et prend, modulo 8, les valeurs suivantes : 1 si $n \equiv 0$, -1 si $n \equiv 2$, $1 + 4$ si $n \equiv 4$, et $-1 + 4$ si $n \equiv 6$ modulo 8. Définissons le « signe additif » $\varepsilon : \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ par :

$$(1.2) \qquad \begin{cases} \varepsilon_i = 0 & \text{si } i \equiv -1, 0, 1 \text{ ou } 2 \bmod 8 \\ \varepsilon_i = 1 & \text{si } i \equiv 3, 4, 5 \text{ ou } 6 \bmod 8; \end{cases}$$

on obtient ainsi la relation de (1.1) avec $a = T_2(R^{-1}C) + \varepsilon_n$, c.q.f.d.

Dans la suite du paragraphe, K désigne un corps de caractéristique 2, et A un anneau de valuation discrète de caractéristique 0 et de corps résiduel $A/2A = K$. On note $\hat{K}$ le corps des fractions de A, et $a \mapsto \bar{a}$ la surjection canonique de A sur K. Une extension séparable E/K de degré n se relève en la clôture intégrale B de A dans une extension non ramifiée $\hat{E}$ de $\hat{K}$ (cf. [10], ch. II). Le procédé s'étend aux algèbres étales par produit direct, B est alors la clôture intégrale de A dans un produit d'extensions non ramifiées de $\hat{K}$.

Exemple 1.3. — Soit E/K une algèbre quadratique étale, éventuellement décomposée en $K \times K$. L'algèbre $\hat{E}$ est isomorphe à un quotient $\hat{K}[X]/(X^2 - d)$, où l'élément d de A est inversible et congru à un carré modulo 4 (« congruence de Stickelberger »). A toute écriture $d = u^2(1 + 4a)$, $a \in A$, $u \in A^*$ (groupe des éléments inversibles de A), correspond un polynôme $X^2 + X + \bar{a}$ définissant l'algèbre E. L'élément u est défini modulo 2; si l'on pose $u = u'(1 + 2b)$, avec $b \in A$, on

obtient $d \equiv u'^2(1+4a+4b+4b^2)$ mod. 8, de sorte que l'élément $\bar{a}$ de K est changé en $\bar{a} + \mathscr{P}(\bar{b})$. (Noter que, si A est complet, $d \in A^*$ est un carré si et seulement si c'est un carré modulo 4 et si $\bar{a}$ est nul mod. $\mathscr{P}(K)$.)

Considérons maintenant un K-espace vectoriel V de dimension n muni d'une base $\mathscr{B} = (e_i)$ et d'une forme quadratique Q. On associe à Q et à $\mathscr{B}$ la matricetriangulaire $C = (\gamma_{ij})$ à coefficients dans K, que l'on relève en une matrice triangulaire $\hat{C} = (c_{ij})$ à coefficients dans A (i.e., $\overline{c_{ij}} = \gamma_{ij}$). La forme quadratique $\hat{Q}$ définie sur le A-module A^n muni de sa base canonique par la matrice $\hat{C}$ relève Q, en ce sens que, pour tout $(a_i) \in A^n$, on a $\overline{\hat{Q}((a_i))} = Q\left(\sum_i \bar{a}_i e_i\right)$. A la forme quadratique $\hat{Q}$, on associe la matrice symétrique $\hat{C} + {}^t\hat{C}$ et la matrice alternée $\hat{C} - {}^t\hat{C}$. On suppose dans la suite que la forme Q est non dégénérée; la forme $\hat{Q}$ est alors également non dégénérée sur A^n.

La proposition (1.1) permet d'associer à la forme quadratique Q et à la base $\mathscr{B}$ un élément bien déterminé $\bar{a}$ de K.

PROPOSITION 1.4. — *L'élément* $\bar{a}$ *est un représentant dans* K *de l'invariant de Arf de la forme quadratique* Q; *on le note* $\mathrm{Arf}_Q(\mathscr{B})$. (*L'invariant de Arf est l'élément de* $K/\mathscr{P}(K)$ *défini dans* [1], p. 154-155; voir aussi [6].)

Démonstration. — Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de V, et soient C et C' les matrices triangulaires associées à Q dans ces bases; P désignant la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$, C' est de la forme ${}^tPCP + T$, où T est une matrice alternée. Relevons P et C en $\hat{P}$ et $\hat{C}$, $\hat{C}$ étant triangulaire; la relation $\hat{C}' = {}^t\hat{P}\hat{C}\hat{P} + \hat{T}$ définit de façon unique une matrice triangulaire $\hat{C}'$ et une matrice alternée $\hat{T}$, relèvements de C' et T respectivement. Les congruences modulo 8 (cf. prop. (1.1)) :

$$(-1)^{n/2} \det(\hat{C}+{}^t\hat{C}) \equiv \det(\hat{C}-{}^t\hat{C}).(1+4a)$$

et

$$(-1)^{n/2} \det(\hat{C}'+{}^t\hat{C}') \equiv \det(\hat{C}'-{}^t\hat{C}').(1+4a'),$$

qui déterminent $\bar{a}$ et $\bar{a}'$ dans K, montrent que l'on a $\bar{a}' \equiv \bar{a} \bmod \mathscr{P}(K)$: en effet, $\det(\hat{C}-{}^t\hat{C})$, $\det(\hat{C}'-{}^t\hat{C}')$ et $\det(\hat{C}'+{}^t\hat{C}').[\det(\hat{C}+{}^t\hat{C})]^{-1}$ sont des carrés. Calculons $\bar{a}$ modulo $\mathscr{P}(K)$ en prenant pour $\mathscr{B} = (e_i)$ une base symplectique (au sens de [4], § 5, p. 81). Dans ce cas, la matrice C est

formée de $m = \frac{n}{2}$ blocs diagonaux de la forme

$$\begin{pmatrix} \gamma_1 & 1 \\ 0 & \gamma'_1 \end{pmatrix}, \ldots, \begin{pmatrix} \gamma_m & 1 \\ 0 & \gamma'_m \end{pmatrix},$$

et l'on peut la relever en une matrice $\hat{C}$ formée de m blocs diagonaux de la forme

$$\begin{pmatrix} c_1 & 1 \\ 0 & c'_1 \end{pmatrix}, \ldots, \begin{pmatrix} c_m & 1 \\ 0 & c'_m \end{pmatrix}.$$

On a alors $\det(\hat{C} - {}^t\hat{C}) = 1$, et

$$(-1)^m \det(\hat{C} + {}^t\hat{C}) = (1 - 4c_1c'_1) \ldots (1 - 4c_mc'_m)$$

est congru modulo 8 à $1 + 4(c_1c'_1 + \cdots + c_mc'_m)$, d'où

$$\bar{a} = \gamma_1\gamma'_1 + \cdots + \gamma_m\gamma'_m = Q(e_1)Q(e_2) + \cdots + Q(e_{n-1})Q(e_n).$$

On reconnaît l'expression classique de l'invariant de Arf dans une base symplectique ([6], p. 123; cf. aussi [1], p. 154), c.q.f.d.

Signalons que l'expression $T_2((C - {}^tC)^{-1}C) + \varepsilon_n$ d'un représentant de l'invariant de Arf de Q (qui résulte de la démonstration de (1.1)) a été donnée par Tits ([14], p. 37).

Remarque 1.5. — L'élément $\mathrm{Arf}_Q(\mathscr{B})$ de K est généralement modifié lorsque l'on effectue une permutation des vecteurs de $\mathscr{B}$. La remarque (1^{bis} 3) fournit cependant la relation $\mathrm{Arf}_Q(\mathscr{B}_2 \cup \mathscr{B}_1) = \mathrm{Arf}_Q(\mathscr{B}_1 \cup \mathscr{B}_2)$ pour toute partition de $\mathscr{B}$, qui sera utilisée dans la suite.

Remarque 1.6. — Examinons brièvement le cas des formes dégénérées. Pour un sous-espace non isotrope W de V, on appelle *invariant de Arf de* W, et l'on note Arf_W, l'invariant de Arf mod. $\mathscr{P}(K)$ de la restriction de Q à W. Soit V^0 le radical de V, i.e. l'orthogonal de V pour s_Q. La question se pose de savoir quelles sont les valeurs prises par l'invariant de Arf des divers supplémentaires de V^0. (Question analogue : quelles sont les valeurs prises par l'invariant de Clifford — cf. infra, § 3 — des divers supplémentaires de V^0 ?)

Si Q s'annule sur V^0 (i.e. si Q est non défective), les supplémentaires de V^0 dans V sont isométriques au quotient V/V^0, et ont donc tous

même invariant de Arf mod.$\mathscr{P}(K)$ (et aussi même invariant de Clifford). Il n'en est généralement pas de même si $Q(V^0)$ n'est pas réduit à 0. Plaçons-nous dans ce cas, et supposons V distinct de V^0. Choisissons un élément e_0 de V^0 avec $Q(e_0) \neq 0$, et un plan P_0 non isotrope dans V; notons V' la somme directe $P_0 \oplus Ke_0$. Soient P un plan non isotrope de V', $x \neq 0$ un élément de $P \cap P_0$, y un élément de P_0 avec $s_Q(x,y) = 1$, et z un élément de P tel que $s_Q(x,z) = 1$; quitte à ajouter à z un élément de Kx, on suppose z de la forme $\lambda e_0 + y$. Alors, modulo $\mathscr{P}(K)$, on a la relation $\mathrm{Arf}_P = \mathrm{Arf}_{P_0} + Q(\lambda x)Q(e_0)$. On en déduit que, lorsque Q prend la valeur 0 en dehors de V^0, les invariants de Arf des supplémentaires de V^0 dans V décrivent le groupe $K/\mathscr{P}(K)$ tout entier; cette condition est équivalente à la suivante : il existe un élément de K représenté par Q à la fois sur V^0 et en dehors de V^0. Il en est toujours ainsi lorsque K est un corps parfait.

Signalons enfin, lorsque K est une extension séparable finie d'un corps K', une formule de transitivité relative à Q et à la forme $Q' = \mathrm{Tr}_{K/K'} \circ Q$ sur V considéré comme K'-espace vectoriel : on a, modulo $\mathscr{P}(K')$,

$$\mathrm{Arf}_{Q'} \equiv \mathrm{Tr}_{K/K'}(\mathrm{Arf}_Q).$$

1^bis. Quelques calculs de pfaffiens.

Dans cet appendice au paragraphe 1, V désigne un espace vectoriel de dimension n sur un corps K, muni d'une forme bilinéaire alternée φ non dégénérée (de sorte que n est pair). Soit $\mathscr{S}$ une base symplectique de V. Si $\mathscr{B}$ est une base quelconque de V, et si P désigne la matrice de passage de $\mathscr{S}$ à $\mathscr{B}$, la matrice R de φ dans la base $\mathscr{B}$ a pour déterminant $\det R = (\det P)^2$; l'élément $\det P$ de K^*, qui ne dépend que de φ et de $\mathscr{B}$, est appelé pfaffien de φ dans $\mathscr{B}$, ou pfaffien de R, et noté $\mathrm{Pf}_\varphi(\mathscr{B})$ ou Pf(R) (cf. [4], § 5, p. 82).

Soient V_1 et V_2 deux sous-espaces supplémentaires de V, non isotropes (i.e. les restrictions φ_1 et φ_2 de φ à V_1 et V_2 sont non dégénérées) et « *presque orthogonaux* » dans le sens suivant : il existe un hyperplan H_1 de V_1 orthogonal à V_2, et un hyperplan H_2 de V_2 orthogonal à V_1. Si $\mathscr{B}_1$ est une base de V_1 et $\mathscr{B}_2$ une base de V_2, on a :

$$(1^{bis}\ 1) \qquad \mathrm{Pf}_\varphi(\mathscr{B}_1 \cup \mathscr{B}_2) = \mathrm{Pf}_{\varphi_1}(\mathscr{B}_1).\mathrm{Pf}_{\varphi_2}(\mathscr{B}_2).$$

Pour la démonstration de cette formule, la définition du pfaffien permet de se ramener au cas où V_1 et V_2 sont deux plans rapportés à des bases symplectiques $\mathscr{B}_i = (e_i, e_i')$ avec $e_i \in H_i$, $i = 1, 2$; le premier membre de $(1^{bis}\,1)$ est alors le pfaffien d'une matrice alternée (x_{ij}) d'ordre 4 avec $x_{12} = x_{34} = 1$ et $x_{13} = x_{14} = x_{23} = 0$, qui vaut 1 : d'une façon générale, un pfaffien d'ordre 4 est donné par la formule $\mathrm{Pf}((x_{ij})) = x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$, comme le montre par exemple la méthode de développement suivante.

Soit $C = (c_{ij})$ une matrice triangulaire supérieure, et soit R la matrice alternée $R = C - {}^tC$. Pour $i > j$, on pose $c_{ij} = c_{ji}$, et l'on note R_{ij} la matrice alternée d'ordre $n - 2$ obtenue en barrant, dans R, les lignes et les colonnes d'indices i et j. Alors on a :

$$(1^{bis}\,2) \qquad \mathrm{Pf}\,R = \sum_{j=1}^{n} (-1)^{i+j-1}\,\mathrm{Pf}(R_{ij})c_{ij}$$

(cf. [4], § 5, ex. 5, p. 86).

Soit enfin $s \in S_n$ une permutation de l'ensemble $\{1,2,\ldots,n\}$. Nous notons R^s la matrice alternée définie par les coefficients (au sens précédent) $c'_{ij} = c_{s(i)\,s(j)}$, $1 \leqslant i,\ j \leqslant n$. La formule $(1^{bis}\,2)$ montre que, sous l'effet de la transposition qui échange i et $i+1$, le pfaffien de R devient $\mathrm{Pf}(R^s) = -\mathrm{Pf}(R) + 2\mathrm{Pf}(R_{i,\,i+1})c_{i,\,i+1}$. En itérant $(n-1)$ fois, on voit que, sous l'effet de la permutation $s : \{1,2,\ldots,n\} \mapsto \{2,\ldots,n,1\}$, le pfaffien de R est inchangé. On en déduit immédiatement que, pour toute permutation s de la forme

$$(1,2,\ldots,p,p+1,\ldots,n) \mapsto (p+1,\ldots,n,1,\ldots,p),$$

avec $1 \leqslant p \leqslant n-1$,

on a :

$$(1^{bis}\,3) \qquad \mathrm{Pf}(R^s) = \mathrm{Pf}(R).$$

2. Discriminant additif d'une algèbre.

En caractéristique 2, la forme quadratique $x \mapsto T_1(x^2)$ est de rang 0. Pour cette raison, nous allons étudier la forme quadratique « seconde trace » $x \mapsto T_2(x)$ (cf. introduction). Pour alléger les notations, nous écrirons souvent Q au lieu de T_2. On note $d_Q(\mathscr{B})$ le discriminant de Q

dans la base $\mathscr{B}$ (i.e. le discriminant dans $\mathscr{B}$ de la forme bilinéaire s_Q associée à Q). Enfin, on note T la forme bilinéaire usuelle $(x,y) \mapsto T_1(xy)$. La proposition suivante est partiellement démontrée dans [8] :

PROPOSITION 2.1. — *Soit* K *un corps, et soit* E *une* K*-algèbre étale de degré* n.

(i) *La forme bilinéaire* s_Q *est donnée par la formule :*

$$s_Q(x,y) = T_1(x)T_1(y) - T_1(xy).$$

(ii) *La forme* Q *est de rang* n *si la caractéristique de* K *ne divise pas* $n-1$, *et de rang* $n-1$ *sinon, et son discriminant dans une base* $\mathscr{B}$ *de* E *est lié au discriminant usuel* $d_{E/K}(\mathscr{B})$ *par la relation*

$$d_Q(\mathscr{B}) = (-1)^{n-1}(n-1)\, d_{E/K}(\mathscr{B}).$$

(iii) *Soit* F *l'hyperplan de* E, *noyau de la forme linéaire* T_1. *Alors* F *et* K *sont orthogonaux pour* Q *et* T_1, *et sont supplémentaires dans* E *si et seulement si la caractéristique de* K *ne divise pas* n.

(iv) *La restriction* Q_0 *de* Q *à* F *est de rang* $n-1$ *si la caractéristique de* K *ne divise pas* n, *et de rang* $n-2$ *sinon; les discriminants de* Q_0 *et de* T_F *dans une même base* $\mathscr{B}_0$ *sont liés par la relation*

$$d_{Q_0}(\mathscr{B}_0) = (-1)^{n-1}\, d_T(\mathscr{B}_0).$$

Démonstration. — Soient $\sigma_1, \ldots, \sigma_n$ les n K-homomorphismes de E dans une clôture séparable K_s de K. Alors,

$$T_1(x) = \sum_i \sigma_i(x) \text{ et } T_2(x) = \sum_{i<j} \sigma_i(x)\,\sigma_j(x)$$

donc

$$T_2(x+y) - T_2(x) - T_2(y) = \sum_{i \neq j} \sigma_i(x)\,\sigma_j(y) = T_1(x)T_1(y) - T_1(xy),$$

d'où (i).

L'assertion (iii) est évidente.

Les formes s_Q et T étant opposées sur F, et T étant non dégénérée sur E, les assertions (iv) résultent tout de suite de (iii).

L'égalité qui figure dans (ii) ne dépendant pas du choix de la base, on fait les calculs dans une base $\mathscr{B} = (e_1, \ldots, e_n)$ telle que $(e_2, \ldots, e_n)$ soit une base de F. Soient (a_{ij}) et (b_{ij}) les matrices des formes s_Q et T dans une telle base. Lorsque la caractéristique de K ne divise pas n, on prend $e_1 = 1$, d'où $a_{11} = n(n-1)$ et $b_{11} = n$; (ii) résulte alors de (iv) et de (iii). Sinon, quel que soit le choix de e_1, on a $a_{ij} + b_{ij} = 0$ si $i > 1$ ou si $j > 1$; comme le mineur de a_{11} est alors nul, le quotient des déterminants des matrices (a_{ij}) et (b_{ij}) est égal à $(-1)^n$, c.q.f.d.

Supposons maintenant K de caractéristique 2. Posons $E' = E$ si n est pair et $E' = E \times K$ si n est impair, et notons n' le degré de E'. La forme quadratique $Q' = T_2$ associée à l'algèbre E' est non dégénérée. A toute base $\mathscr{B} = (e_1, \ldots, e_n)$ de E/K correspond de façon naturelle une base $\mathscr{B}'$ de E' sur K : $\mathscr{B}' = \mathscr{B}$ si $E' = E$, et $\mathscr{B}' = ((e_1,0), \ldots, (e_n,0), (0,1))$ sinon. On relève, comme au § 1, l'algèbre E/K en une A-« algèbre étale » B (rappelons que A est un anneau de valuation discrète de corps résiduel K); la base $\mathscr{B}$ se relève en une base $\hat{\mathscr{B}}$ de B sur A, à laquelleest associée comme ci-dessus une base $\hat{\mathscr{B}}'$ de B'(B'=B ou B'=B×A) qui relève encore $\mathscr{B}'$. Enfin, la forme quadratique $\hat{Q}' = T_2$ associée à la A-algèbre B' relève Q'. Le discriminant à signe $(-1)^{n'/2} d_{Q'}(\hat{\mathscr{B}}')$ est, d'après (2.1, (ii)), lié au discriminant usuel $d_{B'/A}(\hat{\mathscr{B}}')$ (égal à $d_{B/A}(\hat{\mathscr{B}})$) par les relations

$$(-1)^{n'/2} d_{Q'}(\mathscr{B}') = (-1)^{n'/2}(1-n')\, d_{B'/A}(\hat{\mathscr{B}}') = (1+4\varepsilon_n)\, d_{B/A}(\hat{\mathscr{B}}) \bmod 8,$$

où $\varepsilon_{n'} = \varepsilon_n$ est défini dans (1.2).

Notons $\hat{R}'$ la matrice alternée associée au module quadratique $(B', \hat{Q}')$ dans la base $\hat{\mathscr{B}}'$, et a' un représentant dans A de l'invariant $\mathrm{Arf}(Q', \hat{\mathscr{B}}')$. La congruence (1.1) :

$$(-1)^{n'/2} d_{Q'}(\hat{\mathscr{B}}') \equiv \det \hat{R}'(1+4a') \bmod 8$$

s'écrit encore :

$$d_{B/A}(\hat{\mathscr{B}}) \equiv \det \hat{R}'(1+4(a'+\varepsilon_n)) \bmod 8. \tag{2.2}$$

On est conduit à poser la définition suivante :

DÉFINITION 2.3. — Soient E/K une algèbre étale et $\mathscr{B}$ une base de E sur K. On appelle *discriminant additif* de l'algèbre E/K dans la base $\mathscr{B}$ l'élément $d^+_{E/K}(\mathscr{B}) = \mathrm{Arf}_{Q'}(\mathscr{B}') + \varepsilon_{n'}$ de K. Son image dans $K/\mathscr{P}(K)$, qui ne dépend pas du choix de $\mathscr{B}$, est appelée *discriminant additif* de

l'algèbre, et notée $d^+_{E/K}$. L'élément $\mathrm{Arf}_Q(\mathscr{B}')$ de K est appelé *invariant de Arf de* E *dans la base* $\mathscr{B}$, et noté $\mathrm{Arf}_{E/K}(\mathscr{B})$. Son image modulo $\mathscr{P}(K)$ est appelée *invariant de Arf de l'algèbre* E/K, et est notée $\mathrm{Arf}_{E/K}$.

Remarque 2.4. — L'élément $\det \hat{R}' = (\mathrm{Pf}\,\hat{R}')^2$ qui figure dans (2.2) est le carré d'un élément inversible de A. Pour toute congruence $d_{B/A}(\hat{\mathscr{B}}) \equiv u^2(1+4v) \mod. 8$ $(u,v \in A)$, l'image $\bar{v}$ de v mod. 2 est un représentant dans K de $d^+_{E/K}$ (cf. (1.3)). On en déduit tout de suite la formule d'addition $d^+_{E_1 \times E_2/K} \equiv d^+_{E_1/K} + d^+_{E_2/K} \mod. \mathscr{P}(K)$. On a en fait un résultat plus précis :

PROPOSITION 2.5. — *Soient* E_1 *et* E_2 *deux algèbres étales, et soient* $\mathscr{B}_1$ *une base de* E_1 *et* $\mathscr{B}_2$ *une base de* E_2. *On a :*

$$d^+_{E_1 \times E_2/K}(\mathscr{B}_1 \times \{0\} \cup \{0\} \times \mathscr{B}_2) = d^+_{E_1/K}(\mathscr{B}_1) + d^+_{E_2/K}(\mathscr{B}_2).$$

Démonstration. — On remarque d'abord que $d^+_{K \times K/K}$ prend la valeur 0 sur la base canonique. La remarque (1.5) permet donc de se ramener au cas où les deux algèbres sont de degrés pairs, et $\geqslant 2$. On relève en caractéristique 0 la K-algèbre produit des algèbres E_1 et E_2 par le produit $B = B_1 \times B_2$ de relèvements de chacune d'elles, et l'on relève $\mathscr{B}_1$ et $\mathscr{B}_2$ en des bases $\hat{\mathscr{B}}_1$ et $\hat{\mathscr{B}}_2$, de sorte que $\hat{\mathscr{B}} = \hat{\mathscr{B}}_1 \times \{0\} \cup \{0\} \times \hat{\mathscr{B}}_2$ est une base de B. Pour montrer (2.5), il suffit de prouver les formules de multiplication pour les déterminants figurant dans la congruence (2.2). La formule $d_{B/A}(\hat{\mathscr{B}}) = d_{B_1/A}(\hat{\mathscr{B}}_1)\, d_{B_2/A}(\hat{\mathscr{B}}_2)$ est bien connue. La formule $\det \hat{R} = \det \hat{R}_1 \det \hat{R}_2$, où $\hat{R}$, $\hat{R}_1$ et $\hat{R}_2$ désignent les matrices alternées associées aux modules quadratiques (B,T_2), (B_1,T_2) et (B_2,T_2) dans les bases $\hat{\mathscr{B}}$, $\hat{\mathscr{B}}_1$ et $\hat{\mathscr{B}}_2$, résulte de (1 bis 1). En effet, soit $\hat{K}$ le corps des fractions de A, et soient $\hat{E}_1$ et $\hat{E}_2$ les K-algèbres $\hat{K} \otimes_A B_1$ et $\hat{K} \otimes_A B_2$; alors, $\hat{E} = \hat{K} \otimes_A B$ s'identifie à $\hat{E}_1 \times \hat{E}_2$. Notons φ la forme bilinéaire alternée sur $\hat{E}$ qui a $\hat{R}$ pour matrice dans la base $\mathscr{B}$, et soit ψ la forme bilinéaire associée à la forme quadratique T_2 de E. Par définition de $\hat{R}$, on a, pour $x_1 \in E_1$ et $x_2 \in E_2$:

$$\varphi((x_1,0),(0,x_2)) = \psi((x_1,0),(0,x_2)) = \mathrm{Tr}_{E_1/K}(x_1)\,\mathrm{Tr}_{E_2/K}(x_2).$$

Les sous-espaces $E_1 \times \{0\}$ et $\{0\} \times E_2$ de E sont donc presque orthogonaux pour φ au sens de (1^{bis} 1), c.q.f.d.

Rappelons maintenant comment on associe à l'algèbre E/K une extension quadratique $\tilde{E}$ de K (ou $\tilde{E}=K$). On choisit une clôture séparable K_s de K. Le groupe de Galois G_K de K_s/K opère sur l'ensemble H des n K-homomorphismes de E dans K_s par $(s,\sigma)\mapsto s\circ\sigma$ pour tout $s\in G_K$ et tout $\sigma\in H$. On prend pour $\tilde{E}$ la sous-extension de K_s/K fixée par les éléments s de G_K qui induisent sur H une permutation paire (ils forment un sous-groupe ouvert de G_K). En caractéristique $\neq 2$, $\tilde{E}$ est définie par le discriminant de E/K dans K^*/K^{*2}. Le discriminant additif joue un rôle analogue en caractéristique 2 :

THÉORÈME 2.6. — *L'extension* $\tilde{E}/K$ *est l'extension quadratique de* K *définie par l'élément* $d^+_{E/K}$ *de* $K/\mathscr{P}(K)$.

Démonstration. — La formule d'addition (2.5) permet de se limiter au cas où E est une extension de K, isomorphe à un quotient $K[X]/(p)$, p étant un polynôme unitaire irréductible. On suit alors la méthode indiquée par Bourbaki ([3], A V.151, Ex. 23; cf. aussi [2]). On décompose p dans une extension galoisienne finie N de K contenant E en un produit $p=\prod_i (X-\gamma_i)$; on relève K, E et N en des anneaux $A\subset B\subset C$ de caractéristique 0, et p en un polynôme $\hat{p}\in A[X]$, qui se décompose dans C[X] sous la forme $\hat{p}=\prod_i (X-c_i)$, de discriminant $d_{\hat{p}}=\prod_{i<j}(c_j-c_i)^2$. Tenant compte du fait que p est un polynôme séparable, on voit que $u=\prod_{i<j}(c_i+c_j)$ est un élément inversible de A; alors, $\bar{v}=\sum_{i<j}\gamma_i\gamma_j/(\gamma_i+\gamma_j)^2=\mathscr{P}(\delta)$, où $\delta=\sum_{i<j}\gamma_i/(\gamma_i+\gamma_j)$ est changé en $1+\delta$ par une transposition de deux indices. On a donc $\tilde{E}=K(\delta)$, c.q.f.d.

DÉFINITION 2.7. — *L'élément* $\sum_{i<j}\gamma_i\gamma_j/(\gamma_i+\gamma_j)^2$ *de* K *introduit dans la démonstration du théorème* (2.6) *est appelé discriminant additif de* p, *et noté* d^+_p; *l'élément* $d^+_p+\varepsilon_n$ *de* K *est appelé invariant de Arf de* p, *et noté* Arf_p.

On peut également définir le résultant additif de deux polynômes séparables et premiers entre eux p et q : on décompose p et q dans une

clôture algébrique de K, soit $p = \prod_{i=1}^{m} (X-\gamma_i)$ et soit $q = \prod_{j=1}^{n} (X-\delta_j)$, et l'on pose $r^+(p,q) = \sum_{i,j} \gamma_i/(\gamma_i+\delta_j)$. C'est un élément de K, et l'on a les deux formules $r^+(q,p) = r^+(p,q)+mn$ et $d^+_{pq} = d^+_p + d^+_q + \mathscr{P}(r^+(p,q))$.

Exemple 2.8. — Soit n un entier $\geqslant 2$, et soient a et $b \in K$, $a \neq 0$ si n est pair et $b \neq 0$ si n est impair. Soit p le polynôme $X^n + aX + b$ de K[X]. Le discriminant du polynôme $P = X^n + TX + U \in \mathbf{Z}[T,U][X]$ est :

$$d_P = (-1)^{(n-1)(n-2)/2}(n-1)^{n-1}T^n + (-1)^{n(n-1)/2}n^nU^{n-1}.$$

On voit facilement que, pour $n \geqslant 4$, d_P est, modulo 8, de la forme $a_n^2(1+4\varepsilon_n)$. Donc, Arf_p est nul pour $n \geqslant 4$. Pour $n = 2$ (resp. 3), on a $\mathrm{Arf}_p = ba^{-2}$ (resp. $\mathrm{Arf}_p = a^3b^{-2}$) mod. $\mathscr{P}(K)$.

3. Invariants de la forme T_2.

Dans ce paragraphe, K désigne un corps de caractéristique 2. Nous rappelons quelques généralités sur les K-espaces quadratiques (cf. [9]).

Soit V un K-espace vectoriel de dimension n muni d'une forme quadratique Q non dégénérée ($n=2m$ est donc pair). On lui associe, outre l'invariant de Arf

$$\mathrm{Arf}_Q \text{ (ou } \mathrm{Arf}_V) \in K/\mathscr{P}(K),$$

l'invariant « de Clifford » (ou « de Hasse-Witt »)

$$\mathrm{Clif}_Q \text{ (ou } \mathrm{Clif}_V) \in \mathrm{Br}(K)$$

qui est la classe dans le groupe de Brauer de K de l'algèbre de Clifford de Q.

Pour a, $b \in K$, notons $P_{a,b}$ le plan $K \times K$ muni de la forme quadratique $(x,y) \mapsto ax^2 + xy + by^2$; l'invariant de Arf de $P_{a,b}$ est représenté par ab, et l'invariant de Clifford $(a,b) \in \mathrm{Br}\, K$ par l'algèbre de quaternions $H_{a,b}$ définie par les générateurs i et j et les relations $i^2 = a$, $j^2 = b$, et $ij + ji = 1$. L'espace quadratique V est isométrique à une

somme directe orthogonale

$$V \cong P_{a_1,b_1} \perp \ldots \perp P_{a_m,b_m}, \tag{3.1}$$

et l'on a :

$$\mathrm{Arf}_V = a_1b_1 + \cdots + a_mb_m \mod \mathscr{P}(K), \tag{3.2}$$

et

$$\mathrm{Clif}_V = (a_1,b_1) + \cdots + (a_m,b_m). \tag{3.3}$$

Lorsque $n = 2$, on a $\mathrm{Clif}_V = 0$ si et seulement si Q représente 1 (et alors V est isométrique à un plan $P_{1,b}$), et $\mathrm{Arf}_V = 0$ si et seulement si Q représente 0 (i.e. V est un plan hyperbolique; alors Clif_V est également nul et V est isométrique à $P_{1,0}$ ainsi qu'à $P_{0,0}$). Notons également l'isométrie :

$$P_{1,b} \perp P_{1,c} \cong P_{1,0} \perp P_{1,b+c}. \tag{3.4}$$

Soit maintenant E une K-algèbre étale de dimension n que l'on munit de la forme quadratique $Q = T_2$. On note m la partie entière de $n/2$ et a un représentant dans K de $\mathrm{Arf}_{E/K}$. Quitte à remplacer E par $E \times K$, ce qui ne change pas a mod. $\mathscr{P}(K)$, on peut supposer n pair, et donc Q non dégénérée.

THÉORÈME 3.5. — *Soit* K *un corps de caractéristique* 2, *et soit* E *une* K*-algèbre étale de dimension paire* $n = 2m$. *Alors* E *est somme directe orthogonale de* $m - 1$ *plans hyperboliques et d'un plan isométrique à* $P_{1,a}$. *En particulier, l'invariant de Clifford de* E *est nul.*

Démonstration. — Soit $E = P_1 \perp \ldots \perp P_m$ une décomposition de E en somme directe orthogonale de plans, et, pour tout i, soit x_i un élément de P_i pour lequel $Q(x_i)$ est différent de 0. L'identité $T_j(x^2) = [T_j(x)]^2$ appliquée avec $j = 1$ ou $j = 2$ montre que les m vecteurs $x_1^2, \ldots, x_m^2$ sont deux-à-deux orthogonaux. En outre, ces vecteurs sont indépendants : soit en effet $\sum_j \lambda_j x_j^2 = 0$ une relation de dépendance sur K entre ces vecteurs; pour tout i, soit $e_i \in P_i$ tel que $s_Q(e_i, x_i) = 1$; alors $s_Q(e_i^2, x_j^2)$ est égal à 0 si $i \neq j$ et à 1 si $i = j$ (pour tous x, $y \in E$ on a $s_Q(x^2,y^2) = (s_Q(x,y))^2$), d'où $\lambda_i = 0$. Il existe donc une décomposition de E en somme directe orthogonale de plans $E = P'_1 \perp \ldots \perp P'_m$ avec $x_1^2 \in P'_1, \ldots, x_m^2 \in P'_m$. Comme Q prend la

valeur 1 sur les vecteurs $(Q(x_i))^{-1}x_i^2$, la formule (3.4) permet de conclure.

De façon générale, l'homomorphisme d'anneaux $x \mapsto x^2$ conserve le rang sur K des systèmes de vecteurs de E.

Dans la suite, on note F l'hyperplan $F = \operatorname{Ker} T_1$, noyau de la trace de E sur K.

COROLLAIRE 3.6. — *Si n est impair,* F *est somme directe orthogonale de $m-1$ plans hyperboliques et d'un plan isométrique à $P_{1,a}$.*

Démonstration. — Dans l'algèbre $E' = E \times K$, soit P le plan engendré par les vecteurs (1,0) et (0,1). On voit tout de suite que P est un plan hyperbolique et que son supplémentaire orthogonal est le sous-espace $F \times \{0\}$ de E', isométrique au sous-espace F de E. Le corollaire (3.6) se déduit du théorème (3.5) appliqué à l'algèbre E', en utilisant le théorème de simplification de Witt (cf. [5], 1.4.1 ou [4], § 4, n° 3).

Remarque 3.7. — Revenons au cas où E est de dimension $m = 2m$ paire. Soit V un sous-espace vectoriel de E non isotrope de dimension $2p > 0$, et soit V' le sous-espace de engendré par les carrés des éléments de V. Soit b un représentant dans K de l'invariant de Arf de V. La méthode utilisée pour démontrer le théorème (3.5) montre que V' est somme directe de $p-1$ plans hyperboliques et d'un plan isométrique à $P_{1,b}$ (noter que b est congru à b^2 mod. $\mathscr{P}(K)$). Prenons pour V un supplémentaire de K dans F; alors, V' est également supplémentaire de K dans F, et son supplémentaire orthogonal V'^0 est un plan contenant K. Si n est divisible par 4, la forme Q s'annule sur K (elle est de défaut nul sur F), le plan V'^0 est hyperbolique, et V et V' ont donc même invariant de Arf que E (cependant, l'invariant de Clifford de V peut ne pas être nul). Si n est congru à 2 modulo 4, la forme Q est de défaut 1 sur F, et l'invariant de Arf de V peut prendre n'importe quelle valeur modulo $\mathscr{P}(K)$ dès que n est > 2 : c'est une conséquence de la remarque (1.6) en observant que Q prend la valeur 1 à la fois sur K et en dehors de K.

4. Réduction des équations.

On considère dans ce paragraphe un corps K de caractéristique 2, et l'on cherche à décrire l'ensemble des extensions séparables de K de degré

n donné, et, éventuellement d'invariant de Arf donné, à l'aide de polynômes dépendant de peu de paramètres. Dans la suite, E désigne une extension séparable de K de degré fini n et F l'hyperplan de E noyau de la trace.

Si $n = 2$, on peut choisir les polynômes de la forme $X^2 + X + t$, t étant défini modulo $\mathscr{P}(K)$. Dans la suite, on suppose que n est $\geqslant 3$.

Les corps finis posent des problèmes particuliers de dénombrement. Pour les résoudre, nous utiliserons le lemme suivant, dont la démonstration ne sera qu'esquissée :

LEMME 4.1 (Wall). — *Soit* K *un corps fini de caractéristique* 2 *possédant* q *éléments, et soit* V *un* K*-espace vectoriel de dimension finie* t, *muni d'une forme quadratique* Q *de rang maximum* ($2s$, *si l'on pose* $t=2s$ *ou* $t=2s+1$, s *entier*). *Soit* V^0 *le radical de* V.

(i) *Si* t *est pair, le nombre d'éléments* x *de* V *tels que* $Q(x) = 0$ (*resp. tels que* $Q(x)$ *ait une valeur donnée non nulle*) *est* $a_t = q^{2s-1} + (q^s - q^{s-1})$ (*resp.* $b_t = q^{2s-1} - q^{s-1}$) *si l'invariant de Arf de* V *est nul, et* $a'_t = q^{2s-1} - (q^s - q^{s-1})$ (*resp.* $b'_t = q^{2s-1} + q^{s-1}$) *sinon.*

(ii) *Si* t *est impair, et si* $Q(V^0) = \{0\}$, *ce nombre est* qa_t (*resp.* qb_{t-1}) *si l'invariant de Arf de* V/V^0 *est nul, et* qa'_t (*resp.* qb'_t) *sinon.*

(iii) *Si* t *est impair et si* $Q(V^0) \neq \{0\}$, *ce nombre est* q^{2s}.

Démonstration. — On observe que le nombre de solutions à l'équation $Q(x) = a$ pour $a \in K^*$ est indépendant de a. On démontre alors (i) par récurrence sur t à partir du cas facile $t = 2$, en écrivant V comme somme orthogonale d'un plan et d'un espace hyperbolique.

Les assertions (ii) et (iii) sont des conséquences faciles de l'assertion (i).

PROPOSITION 4.2. — *Soit* E *une extension séparable de* K *de degré* $n \geqslant 3$. *Si* $n = 4$, *on suppose que* K *n'est pas le corps à deux éléments. Alors, l'extension* E/K *possède un élément primitif qui est racine d'un polynôme de la forme* $X^n + X^{n-2} + a_3X^{n-3} + \cdots + a_n$.

Démonstration. — Nous allons montrer que la quadrique Q définie sur K par l'équation $T_2(X) = 1$ possède dans $F = \operatorname{Ker} T_1$ un élément x qui engendre E. D'après (3.6) et (3.7), il existe un sous-espace F′ de F de codimension 0 ou 1 dans F et de dimension $\geqslant 2$ sur lequel la forme

T_2 est non dégénérée et représente 1. La quadrique Q′ de F′ définie par l'équation $T_2(X) = 1$ est alors non singulière. En particulier, si K est infini, l'ensemble des points de Q′ dans K, qui n'est pas vide, ne peut pas être contenu dans une réunion finie de sous-espaces stricts de F′. Or, l'ensemble des éléments x de E qui n'engendrent pas E sur K est une réunion finie de sous-espaces de E dont la dimension est majorée par le plus grand diviseur strict d de n. Si n n'est pas égal à 4, on a $d < \dim F'$; si $n = 4$, les sous-extensions quadratiques de E/K coupent F′ suivant des droites (car $F' \cap K = \{0\}$). La proposition est donc démontrée si K est infini.

Supposons maintenant K fini avec q éléments. Les sous-extensions de E autres que E sont en bijection avec les diviseurs stricts de n (E/K est cyclique); le nombre d'éléments imprimitifs de E/K est donc majoré par $S_n = \sum_{a=1}^{d} q^a = (q^{d+1}-q)/(q-1)$. Si n est pair $(n=2m)$, le nombre de solutions de l'équation $T_2(x) = 1$ dans F est minoré par $q^{2m-2} - q^{m-1}$, et S_n est majoré par $(q^{m+1}-q)/(q-1)$. Pour $m \geqslant 4$, on a :

$$(q^{m+1}-q) - (q-1)(q^{2m-2}-q^{m-1}) \geqslant (q^{m-3}-1)(q^{m+1}-q) > 0.$$

Pour $m = 3$, le nombre d'éléments imprimitifs est $q^3 + q^2 - q < q^4 - q^2$, ce qui suffit d'après le lemme 4.1, (ii). Pour $m = 2$, la sous-extension quadratique coupe la conique d'équation $T_2(x) = 1$ dans F en au plus deux points. L'existence d'un élément primitif est donc assurée dès que $q > 2$, mais le cas $q = 2$, $n = 4$ est une exception, les polynômes $X^4 + X^2 + aX + b$ étant tous réductibles sur F_2. Pour n impair, on conclut facilement si $n \geqslant 5$ en utilisant l'inégalité $d \leqslant n - 4$, et si $n = 3$ en observant que tout élément x de E non dans K est primitif, c.q.f.d.

Remarque 4.3. — La proposition 4.2 montre que les extensions cubiques d'un corps K de caractéristique 2 sont paramétrées par la famille de polynômes $X^3 + X + t$, d'invariants de Arf t^{-2} et de discriminant additif $1 + t^{-2}$ modulo $\mathscr{P}(K)$. Ce résultat complète le résultat suivant démontré par Serre ([12]) en étudiant la forme quadratique $Tr_{E/K}(x^2)$: toute extension cubique d'un corps de caractéristique $\neq 2$ et 3 peut être définie par un polynôme de la forme $X^3 - 3X + t$.

La proposition suivante permet de caractériser les extensions de degré n définies par un polynôme dépourvu de termes en X^{n-1} et en X^{n-2}.

PROPOSITION 4.4. — *Si le degré n de* E/K *est* $\geqslant 5$, *ou si l'invariant de Arf de* E/K *est nul (et* $n \geqslant 3$), *l'extension* E/K *peut être définie par un polynôme de la forme* $X^n + a_3X^{n-3} + \cdots + a_n$.

Démonstration. — Si $n = 3$, l'hypothèse signifie que l'extension quadratique associée à E/K s'obtient par adjonction à K des racines cubiques de l'unité; c'est là une condition nécessaire et suffisante pour que l'on puisse mettre E sous la forme $K(t^{1/3})$. Si $n = 4$, comme l'invariant de Arf de E/K est nul modulo $\mathscr{P}(K)$, on peut, d'après la remarque (3.7), trouver un plan F′ supplémentaire de K dans F qui soit un plan hyperbolique. Soit alors x un élément de F′ tel que $T_2(x) = 0$; x n'est pas dans K, car $F' \cap K = \{0\}$, et n'engendre pas non plus une extension quadratique de K (sinon, $T_2(x)$ serait non nul). Donc, $E = K(x)$, et $T_1(x) = T_2(x) = 0$. Supposons maintenant $n \geqslant 5$. La remarque 3.7 montre qu'il existe un sous-espace F′ de F tel que T_2 soit non dégénérée et représente 0 dans F′. Si K est infini, ou si n est impair, on conclut comme dans la démonstration de la proposition 4.2. Supposons maintenant K fini avec q éléments, et n pair ($n=2m$). Le nombre d'éléments imprimitifs est majoré par $S_n = (q^{m+1}-q)/(q-1)$ si $n \geqslant 8$, et est égal à $S_6 = q^3 + q^2 - q$ si $n = 6$, alors que le nombre de solutions dans F à l'équation $T_2(x) = 0$ est minoré par $q^{2m-2} - q^m$. L'inégalité $S_n < q^{2m-2} - q^m$ est vérifiée pour $n > 6$ et pour $n = 6$, $q > 2$; si $n = 6$ et $q = 2$, on constate que le polynôme $X^6 + X + 1$ convient, c.q.f.d.

Remarque 4.5. — La nullité de l'invariant de Arf est une condition nécessaire lorsque $n = 3$ ou 4 (cf. exemple 2.8). Par ailleurs, les polynômes de la forme $X^n + aX + b$ avec $a \neq 0$ et $b \neq 0$ se transforment en polynômes de la forme $X^n + tX + t$ par la substitution $X \mapsto ba^{-1}X$. Le coefficient b est non nul si le polynôme est irréductible, et, lorsque n est pair, le coefficient a est non nul lorsque le polynôme est séparable. Par conséquent, on voit que les extensions de degré 4 d'invariant de Arf nul peuvent être décrites par la famille des polynômes de la forme $X^4 + tX + t$, dépendant d'un paramètre. Si K est parfait, comme b est alors une puissance quatrième, on peut utiliser les polynômes $X^4 + tX + 1$.

On va voir qu'il est possible de faire une réduction analogue pour les polynômes de degré 5.

PROPOSITION 4.6. — *Soit* E/K *une extension de degré* 5, *et soit* $\alpha \in K$, *un représentant arbitraire de son invariant de Arf. Alors, il existe un élément*

x de E, *qui engendre* E *sur* K, *et dont le polynôme minimal est de la forme* $X^5 + \alpha(X^3+X^2) + \lambda X + \mu$.

Démonstration. — On sait (prop. 4.4) que E est engendrée sur K par un élément x racine d'un polynôme f de la forme $X^5 + cX^2 + dX + e$. Posons $m = c^2d + e^2$. On voit tout de suite que m est non nul sous la simple hypothèse que f soit séparable (du reste, les calculs qui suivent montrent que m est la racinecarrée du discriminant de f). Supposons d'abord c non nul, et définissons quatre éléments e_1, e_2, e_3, e_4 de $F = \operatorname{Ker} T_1$ de la façon suivante :

$$e_1=x,\ e_2=c^{-1}x^2,\ e_3=c^{-2}(cx^3+ex+c^2),\ e_4=m^{-1}c^3e_3x.$$

Notons P (resp. P′) le sous-espace de E engendré par e_1 et e_2 (resp. e_3 et e_4). Il est facile de vérifier que P et P′ sont des plans, que $F = \operatorname{Ker} T_1$ est somme directe orthogonale de P et de P′, et que l'on a $s_{T_2}(e_1,e_2) = s_{T_2}(e_3,e_4) =$ (i.e., P et P′ sont définis par des bases symplectiques pour s_{T_2}); il est également facile de calculer la valeur de T_2 sur les e_i : on trouve $T_2(e_1) = T_2(e_2) = 0$, $T_2(e_3) = 1$, et $T_2(e_4) = m^{-2}ec^5$. Il en résulte que P est un plan hyperbolique, et que l'invariant de Arf de E mod. $\mathscr{P}(K)$ est égal à celui de P′, lequel est représenté par $m^{-2}ec^5$. Un calcul un peu pénible montre que T_2 et T_3 prennent la même valeur sur chacun des éléments e_1^3, $e_1^2e_2$, e_1e_2 et e_2^3, à savoir 0, 1, 1 et $m^{-2}ec^5$ respectivement (il est utile d'observer que l'on a $T_3(y) = T_1(y^3)$ pour tout $y \in \operatorname{Ker} T_1$). Posons, pour tout $\lambda \in K$, $x_\lambda = \lambda e_1 + e_2$. Il est clair que l'on a :

$$T_1(x_\lambda) = 0 \text{ et } T_2(x_\lambda) = T_3(x_\lambda) = T_1(x_\lambda^3) = m^{-2}ec^5 + \mathscr{P}(\lambda).$$

On obtient le résultat cherché lorsque c n'est pas nul en choisissant λ de façon à avoir $m^{-2}c^5 + \mathscr{P}(\lambda) = \alpha$. Le cas où c est nul se ramène facilement au précédent : on a $T_1(x^i) = 0$ pour $i \not\equiv 0 \bmod 5$ et $T_1(x^5) = e \neq 0$, d'où $T_1(x+x^2) = T_2(x+x^2) = 0$ et $T_3(x+x^2) = T_1((x+x^2)^3) = T_1(x^5) = e \neq 0$, et il suffit de remplacer x par $x + x^2$, c.q.f.d.

Nous sommes maintenant en mesure de prouver un théorème de réduction pour les extensions de degré 5 dont l'invariant de Arf est nul :

THÉORÈME 4.7. — *Soit* E/K *une extension de degré* 5. *Les conditions suivantes sont équivalentes :*

(i) *L'invariant de Arf de* E/K *est nul mod.* $\mathscr{P}(K)$ (*i.e. le discriminant additif de* E/K *est égal à* 1 *mod.* $\mathscr{P}(K)$).

(ii) *Il existe un élément* x *de* E *dont le polynôme minimal est de la forme* $X^5 + tX + t$.

Démonstration. — L'implication (ii) $\Rightarrow$ (i) résulte de l'exemple 2.8. Réciproquement, si (i) est vérifiée, la proposition 4.6 montre que l'on peut choisir un élément primitif x de E/K dont le polynôme minimal est de la forme $X^5 + dX + e$. Si $d \neq 0$, le procédé de la remarque 4.5 permet de conclure. Si $d = 0$, soit $y = (x+e)/(x+1)$; on a $x = (y+e)/(y+1)$, et y est racine du polynôme

$$X^5 + ((e^4+e)/(e+1))X + (e^5+e)/(e+1);$$

comme $X^5 + e$ est irréductible, $e^4 + e$ est non nul, c.q.f.d.

Remarque 4.8. — Lorsque K est parfait, comme $K^4 = K$, on peut définir les extensions E/K de degré 5 à l'aide de polynômes de la forme $X^5 + X + t$.

Pour terminer, voici quelques calculs d'invariants de Arf de polynômes : on rappelle qu'invariant de Arf et discriminant additif diffèrent de 1 pour $n \equiv 3, 4, 5$ ou 6 mod. 8, et coïncident pour $n \equiv -1, 0,$ ou 2 mod. 8 (n désigne le degré du polynôme). On note m la racine carrée du discriminant. (Les résultats sont modulo $\mathscr{P}$K).)

$n = 3$, $p(X) = X^3 + aX^2 + bX + c$:

$$m = ab + c, \quad \mathrm{Arf}_p \equiv m^{-2}(a^3c + a^2b^2 + b^3)$$

$n = 4$, $p(X) = X^4 + aX^3 + bX^2 + cX + d$:

$$m = a^2d + abc + c^2, \quad \mathrm{Arf}_p \equiv m^{-2}(b^3c^2 + a^3c^3 + a^2b^3d + a^2b^2c^2)$$

$n = 5$, $p(X) = X^5 + bX^3 + cX^2 + dX + e$:

$$m = e^2 + bce + c^2d,$$
$$\mathrm{Arf}_p \equiv m^{-2}(b^5e^2 + b^3(c^2d^2 + de^2) + b^2c^2e^2 + bc^3de + c^5e)$$

$n = 6$, $p(X) = X^6 + dX^2 + eX + f$

$$m = e^3, \quad \mathrm{Arf}_p \equiv e^{-2}fd.$$

On voit que l'invariant de Arf du polynôme pour $n = 5$ est celui du plan

P' introduit dans la démonstration de la proposition 4.6, et que, pour $n = 6$, la possibilité de réduire le polynôme en supprimant les termes en X^5, X^4 et X^3 n'est pas liée à la valeur de l'invariant de Arf mod. $\mathscr{P}(K)$.

Les calculs pour $n = 4$ et $n = 5$ ont été faits en utilisant les calculs de discriminants de [13].

BIBLIOGRAPHIE

[1] C. ARF, Untersuchungen über quadratische Formen in Körpern der Characteristik 2 (Teil I), *J. reine angew. Math.*, 183 (1941), 148-167.

[2] E. R. BERLEKAMP, An Analog to the Discriminant over Fields of Characteristic Two, *J. Algebra*, 38 (1976), 315-317.

[3] N. BOURBAKI, *Algèbre*, Ch. 4 à 7, Masson, Paris, 1981.

[4] N. BOURBAKI, *Algèbre*, Ch. IX, Hermann, Paris, 1959.

[5] C. CHEVALLEY, *The algebraic theory of spinors*, Columbia University Press, New-York, 1954.

[6] M. KNESER, Bestimmung des Zentrums der Cliffordschen Algebren einer quadratischen Form über einem Körper der Characteristik 2, *J. reine angew. Math.*, 193 (1964), 123-125.

[7] T. Y. LAM, *The algebraic theory of quadratic forms*, Benjamin, Reading (Mass.), 1973.

[8] Ph. REVOY, Remarques sur la forme trace, *Linear Mult. Algebra*, 10 (1981), 223-233.

[9] C.-H. SAH, Symmetric Bilinear Forms and Quadratic Forms, *J. Algebra*, 20 (1972), 144-160.

[10] J.-P. SERRE, *Corps locaux*, 2e éd., Hermann, Paris, 1968.

[11] J.-P. SERRE, *Extensions icosaédriques*, Séminaire de théorie des nombres, exposé 19 (7 p.), Bordeaux, 1979-1980.

[12] J.-P. SERRE, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helvet.*, à paraître.

[13] T. SASAKI, Y. KANADA, S. WATANABE, Calculations of Discriminants of High Degree Equations, *Tokyo J. Math.*, 4 (1981), 493-499.

[14] J. TITS, Formes quadratiques, groupes orthogonaux et algèbres de Clifford. *Invent. Math.*, 5 (1968), 19-41.

[15] A. R. WADSWORTH, Discriminants in Characteristic two, *Linear Mult. Algebra*, à paraître.

Manuscrit reçu le 30 janvier 1984.

A.-M. BERGÉ & J. MARTINET,
Laboratoire Associé au C.N.R.S. 040226
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux I
351, cours de la Libération
F-33405 Talence Cedex (France).