Werk

Titel: Sur le genre de la forme trace

Autor: Perlis, R.; Erez, B.; MORALES, J.

PURL: https://resolver.sub.uni-goettingen.de/purl?320141322_0016|log21

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Séminaire de Théorie des Nombres de Bordeaux
Année 1987-1988 - Exposé n° 18 le 4 mars 1988

SUR LE GENRE DE LA FORME TRACE

par

B. EREZ, J. MORALES et R. PERLIS*

* Une partie du travail exposé ici a été effectué pendant que le premier auteur bénéficiait d'une bourse du F.N.R.S. Suisse et de l'hospitalité de l'U.E.R. de Mathématiques de l'Université de Bordeaux I.

RESUME : Nous donnons une description complète du genre de la forme quadratique entière obtenue en restreignant la forme trace d'une extension modérément ramifiée de $\mathbb{Q}$ à son anneau des entiers.

INTRODUCTION

La restriction de l'application $x \to \text{trace}_{K/\mathbb{Q}}(x^2)$ à l'anneau des entiers O_K d'un corps de nombres K fournit une forme quadratique entière notée q_K :

$$q_K : O_K \to \mathbb{Z}$$

$$q_K(x) = \text{trace}_{K/\mathbb{Q}}(x^2).$$

Le discriminant D_K de q_K est par définition même le discriminant absolu du corps K, son rang n est le degré de K sur $\mathbb{Q}$. Les autres invariants rationnels de q_K ont été l'objet de travaux récents qui ont donné des résultats inattendus : le plus frappant étant probablement que le calcul de l'invariant de Hasse-Witt de q_K permet le calcul de l'obstruction à un problème de plongement par une formule de Serre [16]. De plus on a calculé les invariants rationnels locaux dans un grand nombre de cas - voir par exemple [3], [5] et leurs bibliographies. On peut donc dire que la structure rationnelle de q_K est bien connue. Très peu est connu - par contre - sur la structure entière de q_K.

Dans la première partie de cet exposé nous rendons compte de la description complète de la structure entière locale de q_K, obtenue dans [7] pour une extension $K/\mathbb{Q}$ *modérément ramifiée*. La description est faite en termes des constantes de ramification (voir Théorèmes 1.3 et 1.12).

Dans la deuxième partie nous faisons quelques remarques sur les liens entre nos résultats et d'autres concernant en particulier la relation avec la fonction zêta de Dedekind et les symboles des restes quadratiques des discriminants.

DEFINITION 0.1.- Deux formes quadratiques entières q et q' sont dans le même *genre* si pour toute place p de $\mathbb{Q}$ - aussi $p = \infty$ - q et q' sont localement isométriques sur $\mathbb{Z}_p$:

$$\text{gen}(q) = \text{gen}(q') \iff \begin{cases} q \sim_{\mathbb{R}} q', \text{ et} \\ \text{pour tout premier } p \text{ de } \mathbb{Z} \\ q \sim_{\mathbb{Z}_p} q' \end{cases}$$

Une des conséquences de nos résultats est le

THEOREME 1.10. *Pour une extension modérément ramifiée* $K/\mathbb{Q}$ *le discriminant* D_K *et la classe rationnelle de* q_K *déterminent son genre.*

En guise de conclusion pour cette introduction signalons que notre intérêt dans les questions traitées ici a été stimulé par un travail de D. Maurer, qui a considéré dans [9] le cas d'une extension modérément ramifiée, galoisienne et non-ramifiée en 2 (voir aussi Remarque 2.2).

NOTATIONS. Nous dénotons par

$\oplus$ une somme orthogonale

$\langle e \rangle$ la forme quadratique ex^2

$\langle p \rangle V$ le produit tensoriel des formes $\langle p \rangle$ et V

O_L l'anneau des entiers d'un corps L

Pour un idéal premier P d'un corps de nombres K l'indexation K_P signifie localisation et complétion. Nous écrivons $q \sim_A q'$ s'il existe une isométrie entre les formes q et q' qui soit définie sur l'anneau A.

I. DESCRIPTION LOCALE

Il s'agit de décrire q_K à $\mathbb{Z}_p$-isométrie près, pour toute place p de $\mathbb{Q}$.

Pour la place archimédienne rappelons seulement la

PROPOSITION 1.1. [3,I.5.2]. *La signature de* q_K *est égale au nombre* r_1 *de plongements réels de* K :

$$\mathrm{sign}(q_K) = r_1. \qquad \square$$

Ici la signature est le nombre de + 1 moins le nombre de - 1 dans une diagonalisation de la forme sur $\mathbb{Z}_\infty = \mathbb{R}$.

Pour p un nombre premier donné on notera

$$e_i = e_i(p),\ f_i = f_i(p) \text{ et } g = g(p).$$

les constantes de ramification définies comme d'habitude par les égalités

$$pO_K = P_1^{e_1} \ldots P_g^{e_g} \quad \text{et} \quad f_i = [O_K/P_i : \mathbb{Z}/p],$$

où $P_1, \ldots, P_g$ est une numérotation donnée des g différents premiers de O_K divisant p. Rappelons que $K/\mathbb{Q}$ est ***modérément ramifiée*** si et seulement si pour tout premier p, p ne divise aucun des $e_i(p)$. On sait ([15, Chap. III], [8, Chap. 25 p. 436]) que pour une telle extension l'ordre en p du discriminant D_K de q_K vaut

$$\text{ord}_p(O_K) = f_1(e_1-1)+\ldots+f_g(e_g-1) = n-s \tag{1.2}$$

où $n = \sum_i e_i f_i$ est le degré de K sur $\mathbb{Q}$ et où nous avons posé

$$s = s(p) = \sum_i f_i(p)$$

Avec ces notations nous sommes prêts à énoncer notre résultat de base.

THEOREME 1.3. *Soit* $K/\mathbb{Q}$ *une extension modérément ramifiée. Alors pour tout nombre premier* p, *la forme entière* q_K *obtenue en restreignant la forme trace* $\text{trace}_{K/\mathbb{Q}}(x^2)$ *à l'anneau des entiers de* K, *admet la décomposition suivante sur* $\mathbb{Z}_p$,

$$q_K \sim_{\mathbb{Z}_p} U \oplus \langle p \rangle V$$

avec a) $U \sim_{\mathbb{Z}_p} \langle e_1 \rangle q_{F_1} \oplus \ldots \oplus \langle e_g \rangle q_{F_g}$

où q_{F_i} *est la forme trace sur les entiers de la sous-extension* $F_i/\mathbb{Q}_p$ *non-ramifiée maximale de* $K_{P_i}/\mathbb{Q}_p$. U *est* $\mathbb{Z}_p$*-unimodulaire et son discriminant modulo les carrés d'unités de* $\mathbb{Z}_p$ *vaut*

$$\text{dis}(U) = (\Pi e_i^{f_i})\varepsilon^{s-g} \tag{1.4}$$

où ε *est une unité non-carré de* $\mathbb{Z}_p$, *égale à 5 si* $p=2$.

b) V *est* $\mathbb{Z}_p$*-unimodulaire de rang* $n-s$ *et si* $p=2$ *alors* V *est paire.*

I.1 Démonstration du théorème 1.3.

Il est bien connu que pour un premier donné p la forme q_K est la somme orthogonale des formes trace des localisés K_{P_i} en les premiers P_i de K divisant p ([15, II.3.Cor. 2][9]) ; pour la démonstration il suffit donc de considérer la forme trace dans une extension locale. Fixons un premier p et un diviseur premier $P=P_i$ de p dans K. Notons $F=F_i$ la sous-extension non-ramifiée maximale contenue dans $K_P/\mathbb{Q}_p$. On a alors l'équation de *transfert*

$$q_{K_P/\mathbb{Q}_p} = \text{trace}_{\mathbb{Q}_p}^{F} (q_{K_P/F})_p \tag{1.5}$$

qui nous permet de découper naturellement la démonstration en deux parties faciles.

LEMME 1.6. *Avec les notations ci-dessus. Pour la forme trace de* K_P/F *restreinte aux entiers de* K_P *on a la décomposition*

$$q_{K_P/F} \sim_{O_F} \langle e\rangle \oplus \langle p\rangle V \tag{1.7}$$

ou V *est* O_F*-unimodulaire et* $e=e_i(p)$. *De plus si* p=2, *alors* V *est paire, c'est-à-dire que pour tout* $\alpha\in O_{K_P}$ *on a* $V(\alpha)\equiv 0 \bmod 2$.

Démonstration. Comme e est une unité par l'hypothèse de ramification modérée et que $\text{trace}_{K_P/F}(1.1) = e = [K_P : F]$, on a certainement une décomposition

$$q_{K_P/F} \sim_{O_F} \langle e\rangle \oplus V''.$$

avec $V'' = \ker(\text{trace}_{K_P/F}) \cap O_{K_P}$, voir e.g. [10, I.3.1 p.5].

Pour montrer que V'' est divisible par p on utilise le fait que pour l'extension totalement et modérément ramifiée K_P/F on a $O_{K_P} = O_F[\Pi]$, où Π est une uniformisante racine d'un polynôme de la forme X^e-p (voir [15,I.6] [8, Ch. 16 p. 248]). Ainsi ([3,III 4.2.]) $\text{trace}_{K_P/F}(\Pi^j)=0$ pour $0<j\leqslant e-1$ et $\{\Pi,\ldots,\Pi^{e-1}\}$

est une base de V". Comme

$$\text{trace}_{K_p/F}(\Pi^i\Pi^j) = \begin{cases} 0 & \text{si } i+j \neq e \\ pe & \text{si } i+j = e \end{cases}$$

on en déduit que modulo p la matrice de $q_{K_p/F}$ dans la base

$\{1,\Pi,\ldots,\Pi^{e-1}\}$ a la forme diag $(e,0,\ldots,0)$: donc $V'' \equiv 0 \bmod p$ et $V'' = \langle p \rangle V$ pour une forme V. V est alors unimodulaire par le calcul du discriminant du point (1.2).

Soit maintenant $p = 2$. Nous affirmons que V est paire, i.e. que pour tout α dans $\ker(\text{trace}_{K_p/F}) \cap O_{K_p}$ on a $V(\alpha) \equiv 0 \bmod 2$.

On dénote par $\alpha = \alpha_1,\ldots,\alpha_e$ les conjugués de α dans une clôture normale N de $K_{P/F}$ et par Π' une uniformisante de N. En écrivant $\alpha = \sum a_j\Pi^j$ $j = 0,\ldots,e-1$ et en utilisant $\text{trace}_{K_p/F}(\Pi^j) = 0$ pour $j \neq 0$ on voit que $\text{trace}_{K_p/F}(\alpha) = 0$

entraîne que $a_0 = 0$, i.e. $\alpha \equiv 0 \bmod \Pi'$.

Ainsi $\alpha_i \equiv 0 \bmod \Pi'$ pour $i = 1,\ldots,e$.

Or

$$V(\alpha) = \frac{1}{2}\,\text{trace}_{K_p/F}(\alpha^2) = -\sum_{i<j}\alpha_i\alpha_j \equiv 0 \bmod 2 \text{ car } 2\mathbb{Z}_2 = (\Pi') \cap \mathbb{Z}_2,$$

et le lemme est démontré. □

La deuxième étape dans la démonstration du Théorème concerne la description de la forme q_F dans l'extension *cyclique* $F/\mathbb{Q}_p$ ([15, III.6]).

Rappelons la

PROPOSITION 1.8.-[3,I.3.4] *Soit* F/L *une extension galoisienne de corps. Alors le discriminant de* F/L *est un carré dans* $L\setminus\{0\}$ *si et seulement si le 2-sous-groupe de Sylow de* Gal(F/L) *est non-cyclique ou trivial.* □

LEMME 1.9. *On a une* $\mathbb{Q}_p$*-isométrie*

$$q_F \sim_{\mathbb{Q}_p} \langle 1,\ldots,1,2,2\varepsilon^{f-1}\rangle$$

où pour $p \neq 2$ ε *engendre* $\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}$ *et pour* $p = 2$ $\varepsilon = 5$.

Démonstration. Il suffit de calculer le discriminant et l'invariant de Hasse-Witt. D'après la Proposition 1.8 le discriminant D_F de q_F modulo les carrés de $\mathbb{Q}_p^*$ est

$$D_F = \begin{cases} \varepsilon^{f-1} & \text{si } p \neq 2 \\ 5^{f-1} & \text{si } p = 2 \end{cases}$$

On a effectivement $\varepsilon = 5$ pour $p = 2$ car F étant galoisien sur $\mathbb{Q}_2$ contient la racine carrée du discriminant $\sqrt{D_F} = \det(\sigma_i(x_j))$, où on note $\mathrm{Gal}(F/\mathbb{Q}_2) = \{\sigma_1,\ldots,\sigma_f\}$ et $\{x_1,\ldots,x_f\}$ une $\mathbb{Q}_2$-base de F. D'où $\varepsilon=5$ vu que $\mathbb{Q}_2(\sqrt{5})$ est l'unique extension quadratique non-ramifiée de $\mathbb{Q}_2$.
Pour les invariants de Hasse $h_p(q_F)$ rappelons que si $p \neq 2$ alors $h_p(q_F) = 1$ par [3,II.3.2] et que $h_2(q_F) = (2,D_F)_2$, où $(,)_2$ dénote le symbole de Hilbert en 2 (d'après [4, p.49] et [8, p. 502]). On en déduit le lemme car $(2,2)_2 = 1$. Les Lemmes 1.7 et 1.9 impliquent le Théorème 1.3 par les propriétés élémentaires du transfert. □

I.2. LE GENRE

La décomposition de Jordan canonique obtenue dans le Théorème 1.4 permet de déduire le théorème suivant.

THEOREME 1.10. *Soit* K (*resp.* K') *une extension modérément ramifiée de* $\mathbb{Q}$ *et* q_K (*resp.* $q_{K'}$) *la forme trace restreinte aux entiers de* K (*resp.* K'). *Alors sont équivalents :*

a) $q_K \sim_{\mathbb{Q}} q_{K'}$, *et les discriminants* D_K *et* $D_{K'}$, *sont égaux (dans* $\mathbb{Z}$*)*

b) $\mathrm{gen}(q_K) = \mathrm{gen}(q_{K'})$.

Démonstration. L'implication b) ⇒ a) est bien connue.

a) ⇒ b). Il suffit de vérifier que dans les décompositions de Jordan

$$q_K \sim U \oplus \langle p \rangle V$$

$$q_{K'} \sim U' \oplus \langle p \rangle V'$$

du Théorème 1.3, U(resp.V) est isométrique à U'(resp.V').

Les discriminants et les degrés de $K/\mathbb{Q}$ et $K'/\mathbb{Q}$ étant égaux par hypothèse on a certainement $s = \operatorname{rang} U = \operatorname{rang} U' = s'$ d'après (1.2).

Pour p=2 le lemme qui suit précise le Théorème 1.3 et montre que le degré et le discriminant déterminent complètement q_K sur $\mathbb{Z}_2$, par la classification des formes 2-adiques (voir [11, 93:16] et [9, lemma 1+2]).

LEMME 1.11. *Sur* $\mathbb{Z}_2$ *on a*

$$q_K \sim_{\mathbb{Z}_2} U \oplus 2(H \oplus \ldots \oplus H)$$

où U *est impaire et* H *est la forme binaire de matrice* $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Le lemme suit de 1)-3) ci-dessous.

1) V est paire par le Théorème 1.3 et si U n'était pas impaire en réduisant modulo 2 on obtiendrait que l'application trace de l'extension résiduelle en 2 est dégénérée, ce qui contredit l'hypothèse que $K/\mathbb{Q}$ est modérément ramifiée.

2) Sur $\mathbb{Z}_2$ une forme paire est une somme orthogonale de formes binaires isométriques soit à $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ soit à H [2, Chap. 8, Lemma 4.1] [11. 93:15].

3) Pour toute unité u de $\mathbb{Z}_2$ on a

$$\langle u \rangle \oplus 2 \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \sim_{\mathbb{Z}_2} \langle 5u \rangle \oplus 2 \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right).$$

Observer que la forme $ux^2 + 2(2y^2+2yz+2z^2)$ représente $5u$ avec $x=1$ car la norme dans l'extension non-ramifiée $\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2$ est surjective sur les unités et est égale à y^2+yz+z^2.

On sait que pour $p \neq 2$ les formes $\mathbb{Z}_p$-unimodulaires sont classées par leur rang et leur discriminant [2, p. 116] [11, IV § 2 (1.5)]. Pour la démonstration du Théorème 1.10 il ne nous reste donc qu'à montrer que pour $p \neq 2$, $q_k \sim_{\mathbb{Q}_p} q_{K'}$ entraîne $U \sim_{\mathbb{Z}_p} U'$. Ceci se voit en utilisant d'une part le "residue class homomorphism" $\psi^0 : W(\mathbb{Q}_p) \to W(\mathbb{F}_p)$ définit sur les anneaux de Witt comme dans [2, Chap. 4 § 3] [10, Chap. 5] ou [14] par $\psi^0(\langle p^i u\rangle) = 0$ ou $\overline{u}$ suivant que $i \equiv 1 \bmod 2$ ou $i \equiv 0 \bmod 2$, et d'autre part le fait que pour $p \neq 2$ deux formes $\mathbb{Z}_p$-unimodulaires sont $\mathbb{Z}_p$-isométriques seulement si leurs réductions modulo p le sont : une forme sur $\mathbb{F}_p$ est encore déterminée par son rang et son discriminant et de plus la réduction modulo p induit un isomorphisme $U_p/U_p^2 \simeq \mathbb{F}_p^*/\mathbb{F}_p^{*2}$ ($U_p = \mathbb{Z}_p$-unités), (cfr. loc. cit.) □

Pour énoncer le théorème suivant nous aurons besoin du nombre

$$t = \begin{cases} t(p) = \#\{i \mid e_i \equiv \varepsilon \bmod U_p^2 \text{ et } f_i \text{ impair}\} & \text{si } p \neq 2 \\ t(2) = \#\{i \mid e_i \equiv 3 \text{ ou } 5 \bmod 8 \text{ et } f_i \text{ impair}\} & \text{si } p = 2 \end{cases}$$

Rappelons que $g = g(p)$ est le nombre de premiers de O_K qui divisent p.

THEOREME 1.12.- *Avec les hypothèses du Théorème 1.10. On a* $gen(q_k) = gen(q_{K'})$ *si et seulement si les conditions suivantes sont satisfaites :*

(dis) $D_K = D_{K'}$,

(∞) $sign(q_K) = sign(q_{K'})$ *et* $[K:\mathbb{Q}] = [K':\mathbb{Q}]$

(p) *pour tout premier impair* p *divisant les discriminants on a* $t+g \equiv t'+g' \bmod 2$.

DEMONSTRATION. La nécessité des conditions suit des propriétés du genre ([11, § 102]) et de l'expression pour le discriminant en (1.4). La suffisance est une conséquence des points suivants.

a) La condition (∞) décrit les formes sur $\mathbb{R}$,

b) (dis) entraîne avec (∞) que $s = s'$ pour tout p,

c) comme nous l'avons remarqué le Lemme 1.11 montre que le degré et le discriminant déterminent complètement la $\mathbb{Z}_2$-classe d'isométrie de q_K,

d) Si $p \neq 2,\infty$ ne divise pas D_K, la classe de $\mathbb{Z}_p$-isométrie de q_K ne dépend que de $dis(q_k) = \varepsilon^{n-s}$ et $rang\ (q_K) = n$ car pour un tel p q_K est $\mathbb{Z}_p$-unimodulaire.

e) Si $p \neq 2,\infty$ divise D_K alors les conditions (dis) et (p) permettent de conclure grâce à (1.4).

□

II - QUELQUES CONSEQUENCES ET REMARQUES

II.1.- Relation avec la fonction zêta de K

Dans [12] Perlis a montré -en utilisant la formule de Serre [16]- que deux corps ayant la même fonction zêta de Dedekind ont des formes trace rationnellement équivalentes. En conjonction avec le Théorème 1.10 ceci donne le

COROLLAIRE 2.1. *La fonction zêta d'un corps* K *modérément ramifié sur* $\mathbb{Q}$ *détermine le genre de* q_K.

□

II.2. Extensions galoisiennes de degré impair

II.2.1. Soient $K/\mathbb{Q}$ et $K'/\mathbb{Q}$ deux extensions galoisiennes modérément ramifiées, de même discriminant absolu et même degré impair.

REMARQUE 2.2. Par (1.2) $\mathbf{ord_p(dis(q_K)) = n - n/e(p)}$ (pour tout i, $e_i = e$) donc pour tout premier p les indices de ramification e(p) (resp. e'(p)) de p dans K(resp. K') sont égaux : $\mathbf{e(p) = e'(p)}$. Aussi la condition (ii) du théorème de Maurer dans [9] est redondante et pour tout p on a $\mathbf{t(p) = t'(p)}$. Par conséquent dans le Théorème 1.12 la condition (p) devient : $\mathbf{g \equiv g' \bmod 2}$ pour tout $p \neq 2$ divisant les discriminants.

COROLLAIRE 2.3.- *Sous les hypothèses de ce paragraphe, comme* $\mathbf{g(p) \equiv g'(p) \equiv 1 \bmod 2}$ *on a toujours* $\mathbf{gen(q_K) = gen(q_{K'})}$.

□

REMARQUE 2.4. Le corollaire suit aussi directement du Théorème 1.10 car pour une extension galoisienne K/ℚ de degré impair $q_K \sim_{\mathbb{Q}} \langle 1,\ldots,1 \rangle$.

Observons aussi que dans le corollaire l'on ne suppose pas que Gal(K/ℚ) soit isomorphe à Gal(K'/ℚ).

Soit maintenant K de groupe de Galois fixé. Le corollaire suggère que l'on puisse trouver une forme "abstraite" décrivant le genre de q_K. Dans cette direction va un travail de M.J. Taylor qui compare q_K comme forme G-équivariante à un module de Swan généralisé (voir [17]).

II.2.2. Riehm a étudié les paires de formes (L,M) où

1) M est une somme de carrés : $x_1^2 + \ldots + x_n^2$ et

2) L est ***presque-unimodulaire***, i.e. L est $\mathbb{Z}_q$-unimodulaire pour tous les premiers q différents d'un premier p donné et $L \sim_{\mathbb{Z}_p} U \oplus \langle p \rangle V$

avec U et V $\mathbb{Z}_p$-unimodulaires.
Il a étudié en détail le cas où rang V = 2. Or d'une part le Théorème 1.3 dit que q_k pour une extension modérément ramifiée K/ℚ est une forme presque unimodulaire généralisée et d'autre part il est montré dans [6] que pour une telle extension K/ℚ abélienne de degré impair q_k est contenue dans une somme de carrés. Il serait intéressant d'étendre les résultats de [13] en vue de ces remarques.

II.3. Invariants de Hasse-Witt

Rappelons que nous avons utilisé la formule suivante dans la preuve du Lemme 1.9,

$$h_2(q_K) = (2,D_K)_2 = (-1)^{s+t}.$$

Pour $p \neq 2$ $q_K \sim U \oplus \langle p \rangle V$ donne avec $m = \text{rang } V$

$$h_p(q_K) = ((-1)^{(m(m-1)/2}d(V)^{m-1},p)_p (d(U),p^m d(V))_p$$

ou encore

$$h_p(q_K) = \begin{cases} (d(V),p) & \text{si } m \equiv 0\ [4] \\ (-d(V),p) & \text{si } m \equiv 2\ [4] \\ (d(U),p) & \text{si } m \equiv 1\ [4] \\ (-d(U),p) & \text{si } m \equiv 3\ [4] \end{cases}$$

(U et V sont unimodulaires).

II.4. Symboles des restes quadratiques des discriminants

Ici nous montrons comment on peut retrouver les résultats de [1] à partir de $q_{K/\mathbb{Q}_p} = \langle e \rangle q_F \oplus \langle p \rangle V$ (situation du Théorème 1.3). Il s'agit de calculer les symboles de Kronecker (D_K/p) sous l'hypothèse que $e = e(p) \equiv 1 \bmod 2$. Rappelons que pour $d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ et en posant $k = \mathbb{Q}(\sqrt{d})$, on définit (d/p) par

$$(d/p) = \begin{cases} +1 & \text{si } d = 1 \text{ ou si } p \text{ se décompose dans } k \\ 0 & \text{si } p \text{ se ramifie dans } k \\ -1 & \text{si } d \neq 1 \text{ et si } p \text{ est inerte dans } k \end{cases}$$

L'hypothèse $e \equiv 1 \bmod 2$ assure que $(D_K/p) \neq 0$, et aussi que $m = n-f = \text{rang } V$ est pair. D'où par II.3 $\quad h_p(q_{K/\mathbb{Q}_p}) = (\pm d(V), p)$.

Par [3, II.6.5] $e \equiv 1 \bmod 2$ entraîne $h_p(q_{K/\mathbb{Q}_p}) = 1$.

D'où pour les symboles de Hilbert en p :
$(p, D_k) = (p,p)^m \, (p, d(U))(p, d(V)) =$

$$= (-1)^{f-1} \, (p/e)^f \, (\pm 1, p)(-1)^{(p-1/2)\cdot(e-1/2)\cdot f}$$

en utilisant $d(U) = e^f \varepsilon^{f-1}$, $(\varepsilon, p)_p = -1$ et la réciprocité quadratique.

Nous affirmons que :

$$(2.5) \qquad (D_K/p) = (p, D_k)_p = (-1)^{f-1}(p/e)^f$$

Cette affirmation est le lemme qui est à la base du théorème de [1]. (voir [1, Lemme 4 et Théorème 1].
Pour montrer (2.5) observons que la première égalité suit directement des définitions, que si n est impair alors $m \equiv 0$ ou $2 \bmod 4$ suivant que $e \equiv 1$ ou $3 \bmod 4$ et que si n est pair alors $(e-1)f \equiv 0 \bmod 4$, donc toujours $(\pm 1, p)\ (-1)^{(p-1/2)(e-1/2)\cdot f} = 1$ en utilisant $(-1, p) = (-1)^{p-1/2}$.

II.5. Parité des nombres de décomposition

Il est amusant de remarquer que si dans deux extensions modérément ramifiées $K/\mathbb{Q}$ et $K'/\mathbb{Q}$ on a $g(p) \equiv g'(p) \bmod 2$ pour presque tous les premiers impairs alors on a la même condition pour tous les premiers. Ceci peut se voir directement via le théorème de Tchébotarev.

BIBLIOGRAPHIE

[1] **P. BARRUCAND, F. LAUBIE.-** *"Sur les symboles des restes quadratiques des discriminants"*. Acta Arith. XLVIII (1987) 81-88.

[2] **J.W.S. CASSELS.-** *"Rational Quadratic Forms"*. LMS Monographs 13, Academic Press, London 1978.

[3] **P.E. CONNER, R. PERLIS.-** *"A Survey of Trace Forms of Algebraic Number Fields"*, World Scientific Publishing, Singapore, 1984.

[4] **P.E. CONNER, N. YUI.-** *"The additive characters of the* Witt ring of an algebraic number field". Preprint, MSRI 12608-85, Berkeley, 1985.

[5] **M. EPKENHANS.-** *"Spurformen über Lokalen Körpern"*, Schriftenreihe des Math. Inst. der Univ. Münster, 2. Serie Heft 44, 1987.

[6] **B. EREZ.-** *"Structure Galoisienne et Forme Trace dans les Corps de Nombres"*. Thèse, Genève, 1987.

[7] **B. EREZ, J. MORALES, R. PERLIS.-** *On the genus of the trace form"*, soumis pour publication

[8] **H. HASSE.-** *"Number Theory"*, Grundlehren der math. Wissenschaften, Bd. 229, Springer Verlag, Heidelberg, 1980.

[9] **D. MAURER.-** *"The trace form of an algebraic number field"*. J. Number Th. 5 (1973), 379-384.

[10] **J. MILNOR, D. HUSEMOLLER.-** *"Symmetric Bilinear Forms"*. Ergebnisse der Mathematik, Bd. 73, Springer-Verlag, Heidelberg, 1973.

[11] **O.T. O'MEARA.-** *"Introduction to Quadratic Forms"*. Grundlehren der math. Wissenschaften, Bd. 117, Springer-Verlag, Berlin, 1963

[12] **R. PERLIS.-** *"On the analytic determination of the trace form"*, Canad. Math. Bull. 28 (4) 1985, 422-430.

[13] **C. RIEHM.-** *"Jordan splittings of almost unimodular integral quadratic forms"*. J. Number Th. 12 (1980) 395-420.

[14] **W. SCHARLAU.-** *"Quadratic and Hermitian Forms"*. Grundlehren der Math. Wissenschaften Bd. 270, Springer-Verlag, Berlin, 1985.

[15] **J.-P. SERRE.-** *"Corps locaux"*. Hermann, Paris, 1968.

[16] **J.-P. SERRE.-** *"L'invariant de Witt de la forme* $\mathrm{Tr}(X^2)$", Comm. Math. Helv. 59 (1984) 651.

[17] **M.-J. TAYLOR.-** *"On the trace form in Galois extensions of odd degree"*, Preprint, 1988.

B. EREZ
Section de Mathématiques
Université de Genève
CP 240
2-4, rue du Lièvre
CH - 1211 GENEVE 24
SUISSE

J. MORALES
R. PERLIS
Mathematics Departement
Louisiana State University
Baton Rouge,
LOUISIANA 70803
U.S.A.