

# GROUPE DE TRAVAIL D'ANALYSE ULTRAMÉTRIQUE

BRUNO KAHN

## **Sommes de Gauss attachées aux caractères quadratiques de petit conducteur**

*Groupe de travail d'analyse ultramétrique*, tome 13 (1985-1986), p. 55-66

[http://www.numdam.org/item?id=GAU\\_1985-1986\\_\\_13\\_\\_55\\_0](http://www.numdam.org/item?id=GAU_1985-1986__13__55_0)

© Groupe de travail d'analyse ultramétrique  
(Secrétariat mathématique, Paris), 1985-1986, tous droits réservés.

L'accès aux archives de la collection « Groupe de travail d'analyse ultramétrique » 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/>

SOMMES DE GAUSS ATTACHEES AUX CARACTERES QUADRATIQUES  
DE PETIT CONDUCTEUR

*Bruno Kahn*

Soit  $p$  un nombre premier et  $K$  une extension finie de  $\underline{\mathbb{Q}}_p$ . On s'intéresse aux constantes  $W(\rho)$  associées aux caractères quadratiques du groupe multiplicatif  $K^*$ , définies par exemple dans [Ta]. On sait que  $W(\rho)$  est une racine 4<sup>e</sup> de l'unité; d'autre part, il existe  $a \in K^*$ , bien déterminé modulo  $K^{*2}$ , tel que  $\rho(x) = (-1)^{(a,x)}$  pour tout  $x \in K^*$ , où  $(a,x) \in \underline{\mathbb{Z}}/2$  est le symbole de Hilbert de  $a$  et  $x$ . Notons  $\rho = \rho_a$ ; le problème que l'on considère est de trouver une formule "simple" exprimant  $W(\rho_a)$  en fonction de  $a$ .

Considérons  $a \in K^*/K^{*2}$  comme un élément de  $H^1(K, \underline{\mathbb{Z}}/2)$ , au moyen de la théorie de Kummer. On a la formule ([BK2], p.26-23):

$$(1) \quad W_K(\rho_a) = W_{\underline{\mathbb{Q}}_p}(\rho_{Na}) (-1)^{N_2(a)},$$

où  $N = N_{K/\underline{\mathbb{Q}}_p}$  et  $N_2: H^1(K, \underline{\mathbb{Z}}/2) \rightarrow H^2(\underline{\mathbb{Q}}_p, \underline{\mathbb{Z}}/2) \simeq \underline{\mathbb{Z}}/2$  est la composante en degré 2 du transfert multiplicatif ([BK1], I.2.4). Le problème peut donc se ramener à un calcul de  $N_2(a)$  (cf infra).

Supposons d'abord  $p \neq 2$ . On a alors:

<p><u>Théorème 1.</u> Supposons <math>p \neq 2</math>. Choisissons une uniformisante <math>\pi</math> de <math>K</math>; notons <math>K_0</math> la sous-extension non-ramifiée maximale de <math>K</math> et <math>P</math> le polynôme caractéristique de <math>\pi</math> sur <math>K_0</math>. Soit <math>\delta = P'(\pi)</math>, <math>e</math> l'indice de ramification et <math>f</math> le degré résiduel de <math>K/\underline{\mathbb{Q}}_p</math>. Alors, pour tout <math>a \in K^*</math>, on a:</p>
---

$$W(\rho_a) = i^{v(a)^2((q-1)/2)^2} (-1)^{(\delta, a) + v(a)\phi(a)},$$

où  $q = p^f$  est le cardinal du corps résiduel, et

$$\phi(a) = (\pi, pa) + f-1 + (ef + \frac{f(f-1)}{2}) \frac{p-1}{2}.$$

(Rappelons que si  $x, y \in K^*$ , on a  $(-1)^{(x, y)} \equiv [(-1)^{v(x)v(y)} \frac{x^{v(y)}}{y^{v(x)}}] \pmod{M_K}$ , où  $M_K$  est l'idéal de valuation de  $K$ .)

Cet énoncé n'avait pas été dégagé dans [BK2]. Pour le démontrer, commençons par noter plus précisément  $(, )_K$  le symbole de Hilbert relatif à  $K$  (N.B.: j'adopterai ce procédé dans la suite quand nécessaire pour la clarté des formules, sans autre commentaire). Si  $L$  est une extension finie de  $K$ , rappelons la formule:

$$(x, y)_L = (x, N_{L/K}y)_K \text{ si } x \in K^*, y \in L^*.$$

D'autre part,  $\text{Cor}_{L/K} : {}_2\text{Br}(L) \rightarrow {}_2\text{Br}(K)$  n'est autre que l'identité quand on identifie ces groupes à  $\mathbb{Z}/2$ . Dans loc. cit., th 3, remplaçons l'extension  $E/K$  par  $K/\mathbb{Q}_p$  et prenons  $x = \langle\langle a \rangle\rangle$ ,  $\pi_K = \pi$ ,  $\pi_{\mathbb{Q}_p} = p$ ,  $\delta = P'(\pi)$ . La formule du théorème 3 devient alors:

$$(2) \quad \mathcal{N}_2(a) = (\delta, a)_K + v(a) [(p, cN_{K_0/\mathbb{Q}_p} \mu)_{\mathbb{Q}_p} + (\pi p^{-f}, a)_K],$$

avec  $c = c_1(K_0/\mathbb{Q}_p)$ .

(N.B. Il y a une faute d'impression dans la formule du théorème 3, où le premier  $\pi_E$  devrait être lu  $\pi_K$ ).

On a  $\mu = \text{Tr}_{K/K_0}(p/\delta\pi)$ . Mais:

$$\text{Lemme 1. } \text{Tr}_{K/K_0}(1/\delta\pi) = (-1)^{e+1} (N_{K/K_0} \pi)^{-1}.$$

Démonstration. D'après [CL], ch.3, p.65, lemme 2, on a  $\text{Tr}_{\mathbb{K}/\mathbb{K}_0}(\pi^i/\delta) =$

$$\begin{cases} 0 & \text{si } 0 \leq i \leq e-2 \\ 1 & \text{si } i = e-1 . \end{cases}$$

Ecrivons  $P(X) = (-1)^{eN\pi} + XQ(X)$ , où  $Q$  est unitaire de degré  $e-1$ . Alors  $\pi^{-1} = (-1)^{e+1} (N\pi)^{-1} Q(\pi)$ , d'où le lemme.

Par suite,  $N_{\mathbb{K}_0/\mathbb{Q}_p} \mu = (-1)^{(e+1)f} f_{\mathbb{K}_0/\mathbb{Q}_p} \pi^{-1}$  et la formule (2) devient:

$$\begin{aligned} (3) \quad N_2(a) &= (\delta, a)_{\mathbb{K}} + v(a) [ (p, (-1)^{(e+1)f} f_{\mathbb{K}_0/\mathbb{Q}_p} \pi \cdot c)_{\mathbb{Q}_p} + (\pi p^f, a)_{\mathbb{K}} ] \\ &= (\delta, a)_{\mathbb{K}} + v(a) [ (p, c(-1)^{ef} f_{\mathbb{K}_0/\mathbb{Q}_p} \pi)_{\mathbb{Q}_p} + (\pi p^f, a)_{\mathbb{K}} ] , \end{aligned}$$

puisque  $(p, p) = (p, -1)$ .

Par ailleurs, pour  $b \in \mathbb{Q}_p^*$ , les formules pour  $W(\rho_b)$  données en [BK2], p.26-23 peuvent se résumer en:

$$W(\rho_b) = i^{v(b)^2} ((p-1)/2)^2 (-1)^{v(b)} (p, b) .$$

En prenant  $b = N_{\mathbb{K}/\mathbb{Q}_p} a$ , on trouve donc:

$$\begin{aligned} (4) \quad W(\rho_{Na}) &= i^{f^2 v(a)^2} ((p-1)/2)^2 (-1)^{fv(a)} (p, Na)_{\mathbb{Q}_p} \\ &= i^{v(a)^2} ((q-1)/2)^2 (-1)^{v(a)} (p^f, a)_{\mathbb{K}} . \end{aligned}$$

En combinant (3) et (4) au moyen de (1), il vient:

$$W(\rho_a) = i^{v(a)^2} ((q-1)/2)^2 (-1)^{v(a)} \psi(a) , \text{ avec:}$$

$$\begin{aligned} \psi(a) &= v(a) (p^f, a)_{\mathbb{K}} + (\delta, a)_{\mathbb{K}} + v(a) [ (p, c(-1)^{ef} N\pi)_{\mathbb{Q}_p} + (\pi p^f, a)_{\mathbb{K}} ] \\ &= (\delta, a)_{\mathbb{K}} + v(a) [ (\pi, pa)_{\mathbb{K}} + (p, c(-1)^{ef})_{\mathbb{Q}_p} ] . \end{aligned}$$

Mais  $(p, -1) \equiv \frac{p-1}{2} \pmod{2}$  ; de plus on a  $c = (-1)^{f(f-1)/2} d$  , où  $d$  est le discriminant de  $K_0/\underline{\mathbb{Q}}_p$  ; comme cette extension est non-ramifiée, on a  $(p, d) \equiv f-1 \pmod{2}$ . D'où le théorème 1.

Passons maintenant au cas  $p = 2$  . Vu l'identité:

$$(5) \quad W(\rho_{ab}) = W(\rho_a)W(\rho_b)(-1)^{(a,b)} ,$$

([Ta], p.126, cor.2), toute formule pour  $W(\rho_a)$  fournit immédiatement une formule pour  $(a,b)$  . Comme les symboles de Hilbert "sauvages" sont difficiles à calculer, on voit qu'une formule "simple" pour  $W(\rho_a)$  est à peu près hors de portée en général pour  $p = 2$  . On peut cependant espérer:

- une formule dans l'esprit de [He] en général;
- des formules raisonnables dans certains cas particuliers.

C'est cette dernière question que je vais traiter ici. Soit  $a, b \in \mathbb{O}_K$  , l'anneau des entiers de  $K$  ; on a la formule:

$$(6) \quad (1+2a, 1+2b) \equiv \text{Tr}_{K/\underline{\mathbb{Q}}_2} ab \pmod{2} .$$

En effet, rappelons l'identité  $(x, 1-x) = 0$  pour  $x \neq 0, 1$  . En l'utilisant deux fois, on peut écrire:

$$\begin{aligned} (1+2a, 1+2b) &= (-2b(1+2a), 1+2b) \\ &= (-2b(1+2a), [1+2b(1+2a)](1+2b)^{-1}) \\ &= (-2b(1+2a), 1+4ab(1+2b)) . \end{aligned}$$

Mais pour tout  $(x, y) \in K^* \times \mathbb{O}_K$  , on a ([CL], ch.15, prop.6):

$$(6\text{bis}) \quad (x, 1+4y) = v(x) \text{Tr}_{k/\underline{\mathbb{F}}_2} \bar{y} ,$$

où  $k$  est le corps résiduel de  $K$  et  $\bar{y}$  est la projection de  $y$  sur  $k$  .  
Par suite:

$$(1+2a, 1+2b) = v(2b) \text{Tr}_{k/\mathbb{F}_2} \overline{ab} .$$

Si  $v(b) > 0$ , on a  $(1+2a, 1+2b) = 0$  et  $\text{Tr}_{K/\mathbb{Q}_2} ab \equiv 0 \pmod{2}$ . Supposons  $v(b) = 0$ ; alors  $v(2b) = e$  (indice de ramification), donc

$$(1+2a, 1+2b) = e \text{Tr}_{k/\mathbb{F}_2} \overline{ab} \equiv \text{Tr}_{K/\mathbb{Q}_2} ab \pmod{2} .$$

Pour  $u \in 1+20_K$ , posons  $W'(\rho_u) = W(\rho_u) i^{-\text{Tr}((u-1)/2)}$ . D'après (5) et (6), on a:

$$W'(\rho_{uv}) = W'(\rho_u) W'(\rho_v) \text{ pour } u, v \in 1+20_K .$$

Faisant  $u = v$ , on trouve  $W'(\rho_u)^2 = 1$ ; par non-dégénérescence du symbole de Hilbert, il existe donc  $x_K \in K^*$  (déterminé modulo  $K^* U_{e+1}^{(1)}$ ) tel que, pour tout  $u \in 1+20_K$ , on ait:

$$(7) \quad W(\rho_u) = i^{\text{Tr}((u-1)/2)} (-1)^{(x_K, u)} .$$

Je me propose de donner une méthode de calcul de  $x_K$ ; elle consiste à se ramener par dévissage à une extension relative de degré 2, où l'on donnera une valeur explicite d'un  $x_K$  "relatif". En analysant de près le dévissage, on peut peut-être obtenir une formule pour  $x_K$  en général, mais je n'y suis pas parvenu. Voici toutefois une conséquence du calcul ci-dessous:

<p>Théorème 2. Si <math>K/\mathbb{Q}_2</math> est modérée, on a <math>x_K = 1</math>, i.e.:</p> $W(\rho_{1+2a}) = i^{\text{Tra}^2} \text{ pour } a \in 0_K .$
---

Ceci améliore le cor. à la prop. 11 de [BK2], où l'on supposait seulement  $K$  non-ramifié sur  $\mathbb{Q}_2$ .

(1) Je note  $U_i = \{x \in K | v(x-1) \geq i\}$ .

Le transfert multiplicatif.

Soit  $F$  un corps de caractéristique  $\neq 2$ , et  $E$  une extension finie, séparable de  $F$ . Dans [BK1], I.2.4, on a défini une application  $N_2: H^1(E, \underline{\mathbb{Z}}/2) \rightarrow H^2(F, \underline{\mathbb{Z}}/2)$ ; via la théorie de Kummer, on peut regarder  $N_2$  comme une application de  $E^*/E^{*2}$  dans  ${}_2\text{Br}(F)$  (sous-groupe de 2-torsion du groupe de Brauer de  $F$ ). Notons le premier groupe multiplicativement et le second additivement; alors  $N_2$  a les propriétés formelles suivantes (loc. cit.):

$$(8) \quad N_2(xy) = N_2(x) + N_2(y) + \text{Cor}_{E/F}(x, y)_E + (N_{E/F}x, N_{E/F}y)_F$$

pour  $x, y \in E^*$ ;

si  $D/E$  est une autre extension finie et séparable, on a (avec des notations évidentes):

$$(8 \text{ bis}) \quad N_2^{D/F}(x) = \text{Cor}_{E/F} N_2^{D/E}(x) + N_2^{E/F}(N_{D/E}x) \quad \text{pour } x \in D^* .$$

Notons  $c(E/F) = (-1)^{n(n-1)/2} d$  le "discriminant à signe" de l'extension  $E/F$ , où  $n = [E:F]$  et  $d$  est le discriminant ordinaire.

Lemme 2. Pour tout  $x \in F^*$ , on a:

$$(8 \text{ ter}) \quad N_2(x) = (x, c(E/F)) .$$

Démonstration. C'est une application du principe de dévissage utilisé dans [BK1], et que l'on utilisera de nouveau plus loin. Si  $[E:F] = 2$ , la formule (8 ter) résulte de loc. cit., prop. I.2.5.d et du fait que  $(x, x) = (x, -1)$ . Si  $D/E$  et  $E/F$  sont des extensions successives, on a  $c(D/F) = c(E/F)^{[D:E]} N_{E/F} c(D/E)$ ; on en déduit que le second membre de (8 ter) a une propriété de transitivité analogue à (8 bis), donc que (8 ter) est vrai pour une extension formée d'extensions quadratiques successives. Enfin, supposons  $E/F$  quelconque; soit  $E$  la clôture galoisienne de  $E/F$ , et  $K \subset E$  une sous-extension correspondant à un 2-sous-groupe de Sylow de  $\text{Gal}(E/F)$ . Il suffit de prouver (8 ter) après extension des scalaires de  $F$  à  $K$ : en effet,  $[K:F]$  est impair, donc  $\text{Res}_{K/F}: {}_2\text{Br}(F) \rightarrow {}_2\text{Br}(K)$

est injective. Mais  $E \otimes_F K$  est produit fini d'extensions  $K_i$  de  $K$  qui sont formées d'extensions quadratiques successives; comme  $\text{Res}_{K/F} N_{2, \lambda}^{E/F}(x) = \prod_i N_{2, \lambda}^{K_i/K}(x)$  et que  $c(E/F) \equiv \prod_i c(K_i/K) \pmod{K^{*2}}$ , cela termine la démonstration.

Cas d'un corps local.

Soit  $K$  un corps complet pour une valuation discrète  $v$ ; on suppose que  $K$  est de caractéristique zéro et que son corps résiduel  $k$  est de caractéristique 2 et parfait. Notons  $O_K$  l'anneau de valuation de  $v$ ; alors (6) et (6 bis) se généralisent en:

$$(6') \quad (1+2a, 1+2b) = e\tau(ab) \quad \text{pour } a, b \in O_K;$$

$$(6' \text{ bis}) \quad (x, 1+4y) = v(x)\tau(y) \quad \text{pour } (x, y) \in K^* \times O_K,$$

où  $e = e_K = v(2)$  est l'indice de ramification absolu et  $\tau$  est le composé des projections  $O_K \rightarrow k$  et  $k \rightarrow k/P(k)$  (où  $P(x) = x^2 + x$ ), le groupe  $k/P(k)$  étant canoniquement identifié à  ${}_2\text{Br}(K)$  au moyen de [CL], ch.12, p.194, th.2 et ch.10, p.163, §3a).

Soit  $L$  une extension quadratique de  $K$ , de discriminant  $d$ .

Proposition 1. Pour tout  $a \in O_L$ , on a:

$$N_2(1+2a) = \begin{cases} e_K \tau_K(N_{L/K} a) & \text{si } L/K \text{ est non-ramifiée;} \\ (1 + \text{Tra}, d) + e_K \tau_K(Na) & \text{si } L/K \text{ est totalement ramifiée.} \end{cases}$$

Pour démontrer ceci, on a besoin du

Lemme 3. Supposons  $\text{Tr } a \equiv 1 \pmod{M_K}$ . Alors  $L/K$  est non-ramifiée, et  $(1+4Na)d \in K^{*2}$ .  
(On note  $M_K$  l'idéal de valuation de  $K$ .)



Démonstration. L'image résiduelle de  $a$  dans  $\mathfrak{l}$  (corps résiduel de  $L$ ) satisfait à une équation d'Artin-Schreier, donc  $\mathfrak{l}/k$  est quadratique, ce qui prouve que  $L/K$  est non-ramifiée. De plus, l'extension  $L$  est engendrée par  $a$ ; la classe de carrés  $d$  est donc représentée par  $(\text{Tr } a)^2 - 4Na$ . En utilisant le fait que  $(\text{Tr } a)^2 \equiv 1 \pmod{4}$ , on trouve:

$$((\text{Tr } a)^2 - 4Na)(1 + 4Na) \equiv (\text{Tr } a)^2 - 4Na + 4Na \pmod{16},$$

d'où  $d(1 + 4Na) \in K^{*2}$ , CQFD.

(N.B. Dans [BK2], on a besoin du même résultat pour démontrer la prop. 11, mais il y est prouvé incorrectement; on peut utiliser le lemme ci-dessus pour "réparer" cette preuve.)

Montrons maintenant la prop. 1. D'après [BK1], lemme II.2.1, on a:

$$N_2(1+2a) = (2, d) + (2+2\text{Tr } a, -dN(1+2a)),$$

le deuxième terme étant interprété comme zéro si  $\text{Tr}(1+2a) = 0$ .

Ecrivons  $N(1+2a) = 1 + 2\text{Tr } a + 4Na = (1+2\text{Tr } a)(1+4Na/(1+2\text{Tr } a))$   
 $\equiv (1+2\text{Tr } a)(1+4Na) \pmod{K^{*2}}$ . On en déduit:

$$N_2(1+2a) = (2, d) + (2+2\text{Tr } a, -1-2\text{Tr } a) + (2+2\text{Tr } a, d(1+4Na)).$$

Dans le membre de droite, le deuxième terme est nul vu l'identité  $(x, 1-x) = 0$ . Supposons  $\text{Tr } a \equiv 1 \pmod{M_K}$ . D'après le lemme 3,  $L/K$  est non-ramifiée et  $d(1+4Na) \in K^{*2}$ ; par suite:

$$N_2(1+2a) = (2, d) = (2, 1+4Na) = e_K \tau_K(Na).$$

Supposons  $\text{Tr } a \not\equiv 1 \pmod{M_K}$ . Alors on peut écrire:

$$N_2(1+2a) = (2, d) + (2+2\text{Tr } a, d) + (2+2\text{Tr } a, 1+4Na) \\ = (1+\text{Tr } a, d) + v(2+2\text{Tr } a) \tau_K(Na).$$

Comme  $\text{Tr } a \not\equiv 1 \pmod{M_K}$ ,  $v(2+2\text{Tr } a) = e_K$ . Si de plus  $L/K$  est non-ramifiée,

$d$  possède un représentant dans  $1+4\mathcal{O}_K$  ; comme  $1+\text{Tra}$  est une unité, la formule (6' bis) montre que  $(1+\text{Tra}, d) = 0$  ; ceci termine la démonstration.

Corollaire. Soit  $L/K$  une extension modérée. Alors, pour tout  $a \in \mathcal{O}_L$ , on a :

$$N_2(1+2a) = e_{K^T/K}(T_2(a)) ,$$

où  $T_2(a)$  est la "trace quadratique" de  $a$ , i.e. le  $(n-2)^e$  coefficient de son polynôme caractéristique ( $n = [L:K]$ ).

Ceci généralise la prop. 11 de [BK2], qui est le cas particulier où  $L$  et  $K$  sont absolument non-ramifiés. On procède exactement de la même manière qu'au lemme 2 : si  $L/K$  est quadratique, elle est non-ramifiée, donc l'énoncé se réduit à la prop. 1. En utilisant (8 bis) et son analogue pour  $T_2$ , on vérifie que l'égalité "passe" aux extensions composées d'extensions quadratiques successives et on termine en remarquant que la clôture galoisienne d'une extension modérée est modérée et que si  $M/K$  est modérée,  $e_M \equiv e_K \pmod{2}$ .

Le théorème 2 se déduit alors du corollaire ci-dessus exactement comme dans [BK2] le corollaire à la prop. 11 se déduit de celle-ci.

Passons maintenant au cas où l'extension quadratique  $L/K$  est ramifiée. Notons  $D$  la différentielle de l'extension, et  $t = v_L(D)$ .

Lemme 4.  $t$  est égal soit à  $2e_K+1$ , soit à un entier pair  $< 2e_K+1$ .

Démonstration. Soit  $\pi$  une uniformisante de  $L$ , de polynôme caractéristique  $P = X^2 - TX + N$ . Comme  $\mathcal{O}_L = \mathcal{O}_K[\pi]$ ,  $D$  est engendré par  $P'(\pi) = 2\pi - T$ . Mais  $v_L(2\pi) = 2e_K+1$  et  $v_L(T)$  est un entier pair, d'où le lemme.

Proposition 2. Il existe  $\delta \in L^*$  tel que, pour tout  $a \in \mathcal{O}_L$ , on ait :

$$N_2(1+2a) = \text{Cor}_{L/K}(\delta, 1+2a) + e_K T(Na) .$$

Si  $\pi$  est une uniformisante de  $L$  telle que  $T = \text{Tr}\pi \neq 0$ , on peut choisir  $\delta = \pi/T - 1/2$ . Si  $t = 2e_K+1$ , on peut choisir pour  $\delta$  tout élément de  $L^*$  de trace 0.

Remarque. Si  $t < 2e_K + 1$ , on a  $t = v_L(T)$ , donc en particulier  $T \neq 0$ .

Démonstration. Supposons d'abord  $T \neq 0$ , et soit  $\delta$  comme dans l'énoncé. Ecrivons  $a = a_1 + \pi a_2$ , où  $a_1, a_2 \in K$ . Comme  $v_L(a_1)$  est pair et  $v_L(\pi a_2)$  impair, on a  $v_L(a) = \inf(v_L(a_1), v_L(\pi a_2))$ ; par conséquent,  $a_1$  et  $a_2 \in O_K$ . Posons  $\lambda = (1 + \text{Tra})^{-1}$ ; alors on a l'égalité:

$$\lambda(1+2a) - 2a_2 T \lambda \delta = 1 .$$

Par suite,  $(\lambda(1+2a), -2a_2 T \lambda \delta) = 0$ , c'est-à-dire:

$$(1+2a, \delta) = (\lambda, -2a_2 T \lambda)_L + (\lambda, \delta) + (\lambda, 1+2a) + (-2a_2 T, 1+2a) .$$

On a  $\text{Cor}_{L/K}(\lambda, -2a_2 T \lambda)_L = 2(\lambda, -2a_2 T \lambda)_K = 0$ , et  $\text{Cor}(\lambda, \delta) = (\lambda, N\delta) = (1 + \text{Tra}, -d)$ . De plus,

$$\text{Cor}(\lambda, 1+2a) = (\lambda, N(1+2a)) = (1 + \text{Tra}, (1+2\text{Tra})(1+4Na)) = (1 + \text{Tra}, -1) ,$$

puisque  $(1 + \text{Tra}, -1 - 2\text{Tra}) = (1 + \text{Tra}, 1 + 4Na) = 0$ .

Enfin,  $\text{Cor}(-2a_2 T, 1+2a) = (-2a_2 T, N(1+2a))$ . Mais:

|| Lemme 5. On a  $N(1+2a) \equiv 1 + 2a_2 T \pmod{K^{*2}}$ .

$$\begin{aligned} \text{En effet, on a } N(1+2a) &= 1 + 2\text{Tra} + 4Na = 1 + 4a_1 + 2a_2 T + 4N(a_1 + \pi a_2) \\ &\equiv 1 + 4a_1 + 2a_2 T + 4a_1^2 \pmod{4M_K} \\ &\equiv (1 + 2a_1)^2 (1 + 2a_2 T / (1 + 2a_1)^2) \pmod{4M_K} \\ &\equiv (1 + 2a_1)^2 (1 + 2a_2 T) \pmod{4M_K} \\ &\equiv 1 + a_2 T \pmod{K^{*2}} . \end{aligned}$$

Par conséquent,  $(-2a_2 T, N(1+2a)) = (-2a_2 T, 1 + 2a_2 T) = 0$ . En définitive, on trouve:

$$\text{Cor}(1+2a, \delta) = (1 + \text{Tra}, d) .$$

Supposons maintenant  $t = 2e_K + 1$ . Si  $\alpha \in K^*$ , on a

$$\text{Cor}(1+2a, \alpha) = (N(1+2a, \alpha)) = (1+2\text{Tra}+4Na, \alpha) = v(\alpha)\tau(Na + \text{Tra}/2),$$

car  $\text{Tra} \in 2O_K$ . Mais  $Na \equiv (\text{Tra}/2)^2 \pmod{M_K}$  (écrire  $a = a_0 + b$ , avec  $a_0 \in O_K$ ,  $b \in M_L$ ; on a  $\text{Tr}b \in 2M_K$ ); par conséquent  $\tau(Na + \text{Tra}/2) = 0$  et  $\text{Cor}(1+2a, \alpha) = 0$ .

Soit  $\pi$  une uniformisante de  $L$ ; quitte à remplacer  $\pi$  par  $\pi + 2$ , on peut supposer  $\text{Tr}\pi = T \neq 0$ ; alors on peut choisir  $\delta = \pi/T - 1/2$  dans la prop.2. On a  $\text{Tr}\delta = 0$ ; si  $\delta'$  est un autre élément de trace nulle, il existe  $\alpha \in K^*$  tel que  $\delta' = \alpha\delta$ . Par conséquent,  $\text{Cor}(1+2a, \delta') = \text{Cor}(1+2a, \delta)$ , ce qui termine de démontrer la prop. 2.

Corollaire. Soit  $L/K$  une extension finie quelconque. Il existe  $\delta = \delta_{L/K}$  tel que, pour tout  $a \in O_L$ , on ait:

$$N_2(1+2a) = \text{Cor}_{L/K}(\delta, 1+2a) + e_K \tau_K(T_2(a)).$$

De plus,  $\delta_{L/K}$  a les propriétés formelles suivantes:

i) Si  $M/L$  et  $L/K$  sont deux extensions successives,  $\delta_{M/K} = \delta_{M/L} \delta_{L/K}$ .

ii) Soit  $E/K$  une extension finie, et  $E \otimes_K L = \prod L_i$ . Alors

$$1 \otimes \delta_{L/K} \equiv \prod \delta_{L_i/E} \pmod{(E \otimes L)^{*2}}.$$

Démonstration. De nouveau, on déduit ceci du cas quadratique de la même manière que pour le lemme 2 et le corollaire à la prop.1; les détails sont laissés au lecteur.

Soit  $K$  une extension finie de  $\underline{Q}_p$ . Dans le cor. à la prop.2, remplaçons  $L$  par  $K$  et  $K$  par  $\underline{Q}_p$ ; la formule (1) montre alors que dans (7), on peut prendre  $x_K = \delta_{K/\underline{Q}_p}$ . De plus, le principe de dévissage, accompagné des propriétés i) et ii) ci-dessus et des propositions 1 et 2, donne un algorithme de calcul de  $x_K$ .

Références

[BK1] B.Kahn Classes de Stiefel-Whitney de formes quadratiques et de représentations galoisiennes réelles, Invent. Math. 78, 223-256 (1984).

[BK2] B.Kahn Le groupe des classes modulo 2, d'après Conner et Perlis, Sém. th. nombres Bordeaux, exp. n° 26 (1984-1985).

[He] G.Henniart Sur les lois de réciprocité explicites, I, J. de Crelle 329, 177-203 (1981).

[CL] J-P.Serre Corps locaux, Hermann, Paris, 1968.

[Ta] J.Tate Local constants, in Algebraic number fields (A.Fröhlich, éd.) 89-131, Academic Press, New-York, 1977.

Bruno Kahn

UNIVERSITE PARIS VII

U.A. 212 - MATHEMATIQUES

2, Place Jussieu

75221 - PARIS CEDEX 05