THÉORIE DES NOMBRES
BESANÇON

Années 1992/93-1993/94

Formes hermitiennes sur des algèbres sur des anneaux locaux

L. FAINSILBER

Formes hermitiennes sur des algèbres sur des anneaux locaux

Laura Fainsilber

Université de Franche-Comté
Laboratoire de Mathématiques, U.R.A. 741
16 rte de Gray, 25030 Besançon cedex, France
laura@ grenet.fr

Introduction.

Le but de cet article est de généraliser des résultats obtenus par E. Bayer-Fluckiger et H. W. Lenstra ([BL], [BAY]) sur les formes quadratiques sur des extensions de corps de degré impair et sur les bases normales autoduales, à la situation des formes hermitiennes sur des anneaux locaux complets.

Pour un corps K, Springer a démontré (voir [SCH]) qu'une forme quadratique anisotrope sur K, est également anisotrope sur toute extension de K de degré impair. Un corollaire de ce théorème dit que si deux formes sur K deviennent isomorphes sur une extension de degré impair de K, alors elles sont isomorphes sur K. C'est ce corollaire que l'on généralise aux formes hermitiennes sur des algèbres sur les anneaux d'entiers des corps locaux complets. Le résultat s'applique en particulier pour montrer que deux systèmes de formes bilinéaires sur l'anneau d'entiers d'un corps local complet qui deviennent isomorphes sur une extension de degré impair, sont isomorphes, et que l'anneau d'entiers d'une extension de degré impair non-ramifiée de corps locaux complets a une base normale autoduale.

Remerciements.

Je remercie chaleureusement Eva Bayer-Fluckiger, sans qui ce travail n'aurait pas eu lieu.

1. Définitions, Groupe de Witt d'un anneau.

Soit A un anneau dans lequel 2 est inversible, et soit $^- : A \to A$ une involution; soit M un A-module à gauche, projectif, de type fini. Une **forme sesquilinéaire** $h : M \times M \to A$ est une application bi-additive, telle que, pour tous $a, b \in A$ et tous $m, n \in M$, on ait $h(am, bn) = a \cdot h(m, n) \cdot \overline{b}$. Une forme h est dite **hermitienne** si elle est sesquilinéaire, et si de plus $h(m, n) = \overline{h(n, m)}$ pour tous $m, n \in M$. On dit alors que (M, h) est un **module hermitien**. On pose $M^* = \mathrm{Hom}_A(M, A)$, muni de la structure de A-module à gauche donnée par $(a \cdot f)(m) = f(m) \cdot \overline{a}$ pour tous $a \in A$, $m \in M$, $f \in M^*$. Etant

donné un module hermitien (M,h), on considère l'**application adjointe** $H : M \to M^*$, $m \mapsto H_m$, où H_m est l'application linéaire $n \mapsto h(n,m)$. On dit que le module (M,h) est **unimodulaire** si l'application adjointe H est bijective.

Exemple : On considère les formes hermitiennes de rang 1, de la forme $(A, \langle a \rangle)$ pour $a \in A$ tel que $\overline{a} = a$: $\langle a \rangle (x,y) = xa\overline{y}$ pour tous $x, y \in A$. Une telle forme est unimodulaire si et seulement si l'élément a est inversible dans A.

Un **morphisme** de modules hermitiens de (M,h) dans (M',h') est un morphisme de A-modules $f : M \to M'$ tel que $h'(fm,fn) = h(m,n)$ pour tous les $m,n \in M$. La **somme directe** de deux modules hermitiens $(M,h) \oplus (N,g)$ est un module hermitien $(M \oplus N, h \oplus g)$, où $h \oplus g(m+n, m'+n') = h(m,m') + g(n,n')$, pour tous $m,m' \in M$, $n,n' \in N$.

Soit N un A-module projectif. On appelle **module hyperbolique** sur N le module hermitien $(N \oplus N^*, \mathbb{H}_N)$, où $\mathbb{H}_N((m,f),(n,g)) = g(m) + \overline{f(n)}$.

Remarques :

- Si le module N est libre et de dimension n sur A, $\mathbb{H}_N$ est donné par la matrice $\begin{pmatrix} 0 & 1_n \\ e & 0 \end{pmatrix}$, où e est la matrice de l'isomorphisme canonique $N \to N^{**}$.
- Dans le module hyperbolique $(N \oplus N^*, \mathbb{H}_N)$, le sous-module N est son propre orthogonal, car $N = N \oplus \{0\} \subset N \oplus N^*$ est tel que

$$\begin{aligned} N^{\perp} &= \{(n,f) \in N \oplus N^* / \mathbb{H}_N((m,0),(n,f)) = 0, \forall m \in N\} \\ &= N \, . \end{aligned}$$

- La forme $\mathbb{H}_N$ est unimodulaire; en effet, l'application adjointe

$$\begin{aligned} N \oplus N^* &\to (N \oplus N^*)^* \cong N^* \oplus N^{**} \cong N^* \oplus N \\ (m,f) &\mapsto \varphi : (n,g) \mapsto g(m) + \overline{f(n)} \end{aligned}$$

est bijective, d'inverse $\varphi \mapsto (\varphi(0,1_N), \overline{\varphi(\cdot,0)})$.

On note $G(A)$ le groupe de Grothendieck de l'ensemble des classes d'isomorphisme de modules hermitiens unimodulaires, muni de la somme directe. On définit le **groupe de Witt** $W(A)$ comme le quotient de $G(A)$ par le sous-groupe engendré par les formes hyperboliques. Deux modules hermitiens (M,h) et (M',h') sont donc équivalents dans $W(A)$ si et seulement s'il existe des modules hyperboliques (N,g) et (N',g') tels que $(M,h) \oplus (N,g) \cong (M',h') \oplus (N',g')$.

Lorsque A est commutatif, et $\overline{\ }$ est l'involution triviale, on retrouve la notion usuelle de groupe de Witt [SCH]. Dans ce cas, les formes hermitiennes sur A sont les formes bilinéaires, et on a une structure d'anneau sur $W(A)$, avec le produit tensoriel

$$(M, \langle a_1, \ldots, a_n \rangle) \otimes (N, \langle b_1, \ldots, b_m \rangle) = (M \otimes N, \langle a_1 \otimes b_1, \ldots, a_2 \otimes b_1, \ldots, a_n \otimes b_m \rangle) \, .$$

Si $\mathcal{O}$ est un anneau commutatif, et si A est une algèbre de type fini sur $\mathcal{O}$ munie d'une involution $\mathcal{O}$-linéaire, on a également une structure de $W(\mathcal{O})$-module sur $W(A)$ donnée par $(\mathcal{O}^n, \langle a_1, \ldots, a_n \rangle) \otimes (M,h) = (M^n, a_1 h \oplus a_2 h \oplus \cdots \oplus a_n h)$.

Cas particulier : l'anneau de Witt d'un anneau local.

Soit $\mathcal{O}$ un anneau commutatif local dans lequel 2 est inversible. On a les propriétés suivantes : ([SCH] I,6)

- Tout module projectif de type fini sur $\mathcal{O}$ est libre, et toute forme bilinéaire sur $\mathcal{O}$ est diagonalisable.
- Si (M,h) est un module bilinéaire unimodulaire de dimension paire $2n$ sur $\mathcal{O}$, les conditions suivantes sont équivalentes :

(i) $(M,h) \cong \mathbb{H}(N)$ pour un module projectif N de dimension n sur $\mathcal{O}$.

(ii) M contient un sous-module N totalement isotrope de dimension n.

(iii) (M,h) est donné par une matrice de la forme $B = \begin{pmatrix} 0 & C \\ C^t & D \end{pmatrix}$, où 0, C, et D sont des matrices carrées d'ordre n, et C est inversible dans $\mathbf{M}_n(\mathcal{O})$.

(iv) (M,h) est donné par une matrice de la forme $B = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}$, où $E = \mathrm{Id}_n$.

(v) (M,h) est donné par une matrice de la forme $B = \begin{pmatrix} A & 0 \\ 0 & -A \end{pmatrix}$, où A est inversible dans $\mathbf{M}_n(\mathcal{O})$.

(vi) $(M,h) \cong \langle 1,\ldots,1,-1,\ldots,-1\rangle \cong \langle 1,-1,\ldots,1,-1\rangle$.

2. Injectivité de l'homomorphisme de restriction sur le groupe de Witt.

Soient K un corps local non-dyadique, $\mathcal{O}_K$ l'anneau des entiers de K, L une extension finie de K telle que l'extensions des corps résiduels soit séparable, $\mathcal{O}_L$ l'anneau d'entiers de L. Soit A_K une $\mathcal{O}_K$-algèbre de type fini, munie d'une involution $\mathcal{O}_K$-linéaire : $^-$.

On pose $A_L = A_K \otimes_{\mathcal{O}_K} \mathcal{O}_L$, et on munit A_L de l'involution $\mathcal{O}_L$-linéaire qui prolonge l'involution de A_K. Pour tout module hermitien (M,h) sur A_K, on pose $M_L = M \otimes_{\mathcal{O}_K} \mathcal{O}_L$ et $h_L : M_L \times M_L \to A_L$ est le prolongement de h à M_L. On a ainsi défini l'homomorphisme canonique de "restriction"

$$\begin{aligned} r^* : W(A_K) &\to W(A_L) \\ (M,h) &\mapsto (M_L, h_L)\,. \end{aligned}$$

Proposition 2.1 : Si L/K est une extension de degré impair, alors l'homomorphisme $r^* : W(A_K) \to W(A_L)$ est injectif.

Démonstration : Soit $s : \mathcal{O}_L \to \mathcal{O}_K$ un homomorphisme $\mathcal{O}_K$-linéaire non-trivial. On prolonge s en un homomorphisme A_K-linéaire $s_A : A_L \to A_K$, $a \otimes x \mapsto a \cdot s(x)$ pour tout $a \in A_K$ et tout $x \in \mathcal{O}_L$, et on obtient des homomorphismes de groupes

$$s_* : W(\mathcal{O}_L) \to W(\mathcal{O}_K) \qquad \text{et} \qquad \begin{aligned} s_* : W(A_L) &\to W(A_K) \\ (N,g) &\mapsto (N, s_A g) \end{aligned}$$

Lemme : Pour tous les modules hermitiens $(P,b) \in W(\mathcal{O}_L)$ et $(M,h) \in W(A_K)$, on a $s_*(b) \otimes h = s_*(b \otimes r^*(h))$ dans $W(A_K)$.

Démonstration du lemme : L'isométrie de A_K-modules $f : p \otimes (\lambda \otimes m) \mapsto \lambda p \otimes m$, $\forall p \in P$, $\lambda \in \mathcal{O}_L$, $m \in M$, associe $s_*(b) \otimes h$ à $s_*(b \otimes r^*(h))$. En effet, on a (réciprocité de Frobenius)

$$\begin{aligned} s_*(b \otimes r^*(h))[p \otimes (\lambda \otimes m), p' \otimes (\lambda \otimes m')] &= s(b(p,p') \cdot \lambda\lambda' h(m,m')) \\ &= s(\lambda\lambda' b(p,p'))h(m,m') \\ &= sb(\lambda p, \lambda' p')h(m,m') \\ &= s_*b \otimes h(\lambda p \otimes m, \lambda' p' \otimes m') \\ &= s_*b \otimes h\big(f(p \otimes (\lambda \otimes m)), f(p' \otimes (\lambda' \otimes m'))\big) \end{aligned}$$

□

Pour prouver que r^* est injectif, il suffit de trouver un homomorphisme $s : \mathcal{O}_L \to \mathcal{O}_K$ tel que $s_*(1) = 1 \in W(\mathcal{O}_K)$. En effet, en utilisant le lemme, on aura alors $s_*(r^*h) = h$ pour tout $h \in W(A_K)$, d'où l'injectivité de r^*.

Comme $\mathcal{O}_L$ et $\mathcal{O}_K$ sont des anneaux locaux et que l'extension résiduelle est séparable, on peut écrire $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, avec $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$ (voir [LNG], Cht.III,1, p59). On considère l'homomorphisme $\mathcal{O}_K$-linéaire $s : \mathcal{O}_L \to \mathcal{O}_K$, $s(1) = 1$, $s(\alpha^i) = 0$ pour $i = 1, \ldots, n-1$. La matrice de la forme $s_*(\langle 1 \rangle)$ pour la base $1, \alpha, \ldots, \alpha^{n-1}$ est

$$M = \big(s(\alpha^i\alpha^j)\big) = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & -a_n \\ \vdots & \vdots & \cdot & * \\ 0 & -a_n & * & * \end{pmatrix}.$$

La forme $s_*(\langle 1 \rangle)$ représente 1, et a un sous-module totalement isotrope engendré par $\alpha, \alpha^2, \ldots, \alpha^{(n-1)/2}$. Donc $s_*(\langle 1 \rangle) \cong \langle 1 \rangle \oplus \mathbb{H}_{\frac{n-1}{2}} \sim \langle 1 \rangle$ dans $W(\mathcal{O}_K)$. □

Corollaire 2.2 : Supposons de plus que K est complet. Si L/K est une extension de degré impair et si (M,h) et (M',h') sont deux modules hermitiens unimodulaires sur A_K, tels que (M_L, h_L) et (M'_L, h'_L) sont isomorphes sur A_L, alors (M,h) et (M',h) sont isomorphes sur A_K.

Démonstration : On sait par la proposition que les classes de Witt de (M,h) et de (M',h) dans $W(A_K)$ sont égales. Donc il existe deux modules hyperboliques (N,g) et (N',g') sur A_K, tels que $(M,h) \oplus (N,g) \cong (M',h') \oplus (N',g')$. Or $M_L \cong M'_L$ implique que $M \cong M'$, et alors, par le théorème de Krull-Schmidt-Azumaya (voir [CR], Introduction, 6B), on a $N \cong N'$. Deux formes hyperboliques sur des modules isomorphes, sont isomorphes, et on peut appliquer le théorème de simplification [QSS], qui donne $(M,h) \cong (M',h')$. □

3. Systèmes de formes.

Soient A un anneau dans lequel 2 est inversible, M et N deux A-module projectif de type fini, I un ensemble fini, n le nombre d'éléments de I.

On appelle système de formes $S = (M, \{h_i\}_{i\in I})$ un module muni de formes bilinéaires, $h_i : M \times M \to A$. Un morphisme de systèmes $f : S \to S' = (M', \{h'_i\}_{i\in I})$ est un morphisme de M dans M' tel que $h'_i(f(m), f(n)) = h_i(m, n)$ pour tous m, n dans M et $i \in I$.

On appelle carquois de n flèches de M dans N un triplet $\mathcal{M} = (M, N, \{(s_i)\}_{i\in I})$, où les s_i sont des homomorphismes de M dans N. Un homomorphisme de carquois $(M, N, \{s_i\}) \to (M', N', \{s'_i\})$ est une paire d'homomorphismes (h_1, h_2), $h_1 : M \to M'$ et $h_2 : N \to N'$ tels que $s'_i \circ h_1 = h_2 \circ s_i$ pour tout $i \in I$. Pour un anneau $B \supset A$, on définit de façon naturelle l'extension des scalaires $\mathcal{M} \otimes_A B = (M \otimes_A B, N \otimes_A B, \{(t_i)\}_{i\in I})$, où les t_i sont les prolongements B-linéaires des s_i.

Lemme 3.1 : Soient K un corps complet, L/K une extension galoisienne finie, et soient $\mathcal{M} = (M, N, \{(s_i)\}_{i\in I})$ et $\mathcal{M}' = (M', N', \{(s'_i)\}_{i\in I})$ deux carquois sur l'anneau des entiers $\mathcal{O}_K$. Alors $\mathcal{M}_L = \mathcal{M} \otimes_{\mathcal{O}_K} \mathcal{O}_L$ est isomorphe à $\mathcal{M}'_L = \mathcal{M}' \otimes_{\mathcal{O}_K} \mathcal{O}_L$ sur $\mathcal{O}_L$ si et seulement si $\mathcal{M}$ est isomorphe à $\mathcal{M}'$ sur $\mathcal{O}_K$

Démonstration : Soit (φ, ψ) un isomorphisme de $\mathcal{M}_L$ sur $\mathcal{M}'_L$; alors φ et ψ sont $\mathcal{O}_L$-linéaires et commutent avec les prolongements $\mathcal{O}_L$-linéaires s_{iL} et s'_{iL} des s_i et s'_i. On peut également considérer $\mathcal{M}_L$ et $\mathcal{M}'_L$ comme des carquois sur $\mathcal{O}_K$: M_L, N_L, M'_L, N'_L sont des $\mathcal{O}_K$-modules libres isomorphes à M^n, N^n, M'^n, N'^n respectivement, où $n = [L : K]$, et les s_{iL} et s'_{iL} sont $\mathcal{O}_K$-linéaires. L'isomorphisme $\mathcal{O}_L$-linéaire (φ, ψ) est a fortiori un isomorphisme $\mathcal{O}_K$-linéaire de $\mathcal{M}_L$ sur $\mathcal{M}'_L$ vus comme carquois sur $\mathcal{O}_K$, et isomorphes à $\mathcal{M}^n$ et $\mathcal{M}'^n$ respectivement. On voit donc, grâce au théorème de Krull-Schmidt-Azumaya [CR], que les composantes $\mathcal{M}$ et $\mathcal{M}'$ sont isomorphes sur $\mathcal{O}_K$. □

Il y a une notion de dualité pour la catégorie des carquois sur un anneau, avec

$$(M, N, \{s_i\})^* = (N^*, M^*, \{s_i^*\}),$$

où $s_i : N^* \to M^*$, et on a une catégorie hermitienne au sens de [QSS], [QSSS]. On peut ainsi définir des formes hermitiennes (unimodulaires) sur un carquois dont les flèches sont des isomorphismes : on prend $\gamma : \mathcal{M} \to \mathcal{M}^*$ de la forme $\gamma = (h, h^*)$, pour un isomorphisme $h : M \to N^*$.

Lemme 3.2 : Les classes d'isomorphisme de systèmes de formes unimodulaires sur un A-module M sont en bijection avec les classes d'isomorphisme de formes hermitiennes sur des carquois de flèches de M dans M^* (voir [QSSS], [BKW]).

Démonstration : A un système de formes $(M, \{h_i\})$, on associe le carquois (M, M^*, h_i) muni de la forme $\gamma = (\mathrm{Id}_M, \mathrm{Id}_{M^*})$. La bijection réciproque est donnée par

$$((M, M^*, \{s_i\}), (h, h^*)) \mapsto (M, \{h^* s_i\}).$$

□

Théorème 3.3 : Soient K un corps local complet non-dyadique, L une extension de K de degré impair d'extension résiduelle séparable, et soient $\mathcal{O}_K$ et $\mathcal{O}_L$ leurs anneaux d'entiers. Si S et S' sont deux systèmes de formes tels que les systèmes S_L et S'_L obtenus par extensions des scalaires, sont isomorphes sur $\mathcal{O}_L$, alors S et S' sont isomorphes sur $\mathcal{O}_K$.

Démonstration : On considère les formes hermitiennes sur des carquois correspondant aux systèmes S, S', S_L et S'_L. On sait grâce au lemme 3.1 que l'on peut prendre le même carquois $\mathcal{M}$ pour S et S'.

D'autre part, pour un anneau E muni d'une involution $\sim$, l'ensemble des formes hermitiennes de rang 1 sur E à isomorphisme près, est donné par

$$\mathrm{H}(\sim, E^\times) = \{f \in E^\times : \tilde{f} = f\}/\approx$$

où $f \approx g$ s'il existe un $h \in E^\times$ tel que $f = \tilde{h}gh$.

On prend ici $E = \mathrm{End}(\mathcal{M})$, l'anneau des endomorphismes de carquois de $\mathcal{M}$; on choisit une forme hermitienne η sur $\mathcal{M}$, et on munit E de l'involution $\tilde{f} = \eta^{-1} f^* \eta$. L'ensemble $\mathrm{H}(\sim, E^\times)$ des formes hermitiennes de rang 1 sur $\mathrm{End}(\mathcal{M})$ est alors en bijection avec l'ensemble des formes hermitiennes sur $\mathcal{M}$: à une forme $h : \mathcal{M} \to \mathcal{M}^*$, on associe $\eta^{-1}h \in \mathrm{End}(\mathcal{M})^\times$. Deux formes isomorphes correspondent à deux éléments équivalents dans $\mathrm{H}(\sim, E^\times)$.

On peut alors appliquer le corollaire 2.2 aux formes hermitiennes de rang 1 sur l'algèbre E : si des formes s et s' correspondant aux systèmes S et S' sont telles que leurs extensions s_L et s'_L sont isomorphes sur E_L, elles sont isomorphes sur E, et S et S' sont donc isomorphes sur $\mathcal{O}_K$. □

4. Formes équivariantes.

Soit A un anneau dans lequel 2 est inversible, et soit G un groupe fini; on note $A[G]$ l'anneau de groupe. Soit M un A-module muni d'une opération à gauche par G qui est un module projectif de type fini en tant que $A[G]$-module. On appelle G-forme, ou forme G-équivariante, une forme hermitienne $h : M \times M \to A$ telle que, pour tout $g \in G$ et tous $m, n \in M$, on ait $h(gm, gn) = h(m, n)$. Un morphisme de G-formes f de $h : M \times M \to A$ dans $h' : M' \times M' \to A$ est un morphisme de formes hermitiennes qui commute à l'opération de G, i.e. un morphisme de modules $f : M \to M'$ tel que, pour tout $g \in G$ et tous $m, n \in M$, $h'(f(m), f(n)) = h(m, n)$ et $f(gm) = g \cdot f(m)$.

Théorème 4.1 : Soient K un corps local complet non-dyadique, L une extension de K de degré impair et d'extension résiduelle séparable, et soient $\mathcal{O}_K$ et $\mathcal{O}_L$ leurs anneaux d'entiers. Si deux G-formes unimodulaires sur $\mathcal{O}_K$ deviennent isomorphes sur $\mathcal{O}_L$, alors elles sont isomorphes sur $\mathcal{O}_K$.

Démonstration : Il y a une équivalence de catégories entre la catégorie des G-formes sur un anneau A et la catégorie des formes hermitiennes sur l'algèbre $A[G]$ munie de

l'involution A-linéaire induite par $\overline{g} = g^{-1}$ pour $g \in G$. En effet, l'application de transfert $Tf : A[G] \to A : 1 \mapsto 1,\ g \mapsto 0$ induit une correspondance qui à la forme hermitienne $\sum_{g\in G} h_g(m,n)g$ sur $A[G]$ associe la G-forme $h_1(m,n)$ sur A. La réciproque de cette correspondance est donnée par $b(m,n) \mapsto \sum_{g\in G} b(gm,n)g^{-1}$. La correspondance est bijective, transforme les morphisme de formes hermitiennes en morphisme de G-formes, et les formes unimodulaires en formes unimodulaires.

On applique alors le corollaire 2.2 aux formes hermitiennes sur l'algèbre $\mathcal{O}_K[G]$: deux formes hermitiennes unimodulaires sur $\mathcal{O}_K[G]$ qui deviennent isomorphes sur $\mathcal{O}_L[G]$, sont isomorphes sur $\mathcal{O}_K[G]$; les G-formes correspondantes sont donc isomorphes sur $\mathcal{O}_K$. □

5. Bases normales autoduales.

Soient K un corps local complet non-dyadique, L une extension galoisienne de K de degré impair et d'extension résiduelle séparable, et soit G le groupe de Galois de l'extension.

La forme trace $\mathrm{Tr} : \mathcal{O}_L \times \mathcal{O}_L \to \mathcal{O}_K : (m,n) \mapsto \mathrm{Tr}_{L/K}(mn)$ est une G-forme unimodulaire sur le $\mathcal{O}_K$-module $\mathcal{O}_L$.

Définition : Une base de $\mathcal{O}_L$ sur $\mathcal{O}_K$ est dite **normale** si elle est de la forme $\{ga\}_{g\in G}$ pour un élément $a \in \mathcal{O}_L$, autrement dit si $\{a\}$ forme une base de $\mathcal{O}_L$ sur $\mathcal{O}_K[G]$. Une base $\{a_1, \ldots, a_n\}$ de $\mathcal{O}_L$ sur $\mathcal{O}_K$ est dite **autoduale** si, pour $1 \le i,j \le n$, $\mathrm{Tr}(a_i, a_j) = \delta_{ij}$, autrement dit si la forme trace est isomorphe à la forme unité sur le $\mathcal{O}_K$-module $\mathcal{O}_L$.

On remarque que $a \in \mathcal{O}_L$ engendre une base normale autoduale sur $\mathcal{O}_K$ si et seulement si $\{a\}$ est une base orthonormale de $\mathcal{O}_L$ sur $\mathcal{O}_K[G]$.

Théorème 5.1 : Si L et K sont des extensions finies de $\mathbb{Q}_p$, et si l'extension L/K est non-ramifiée, alors $\mathcal{O}_L$ a une base normale autoduale sur $\mathcal{O}_K$.

Démonstration : Par le théorème de Noether (applicable même si L/K est modérément ramifiée) (voir [NOE]), $\mathcal{O}_L$ a une base normale sur $\mathcal{O}_K$, engendrée par un élément $a \in \mathcal{O}_L$. On a donc des isomorphismes de $\mathcal{O}_K$-modules $\mathcal{O}_L \simeq \bigoplus_{g\in G} g(a)\mathcal{O}_K \simeq \mathcal{O}_K[G]$, dont on déduit un isomorphisme de O_L-modules $\mathcal{O}_L \otimes \mathcal{O}_L \simeq \mathcal{O}_L \otimes \mathcal{O}_K[G] \simeq \mathcal{O}_L[G]$, où les produits tensoriels sont pris sur $\mathcal{O}_K$, et où G agit sur le second facteur : $g(y \otimes x) = y \otimes g(x)$ et $g(\sum_{\gamma\in G} x_\gamma \gamma) = \sum_{\gamma\in G} x_\gamma g\gamma$ pour $g \in G$, x, y et $x_\gamma \in \mathcal{O}_L$. On va donner un isomorphisme qui associe la G-forme trace à la G-forme unité.

On considère

$$\begin{aligned} \varphi : \mathcal{O}_L &\to \mathcal{O}_L[G] \\ x &\mapsto \sum_{g\in G} g(x)g^{-1} . \end{aligned}$$

L'application φ est O_K-linéaire et G-équivariante (voir [CP] p. 229). Pour $x, x' \in \mathcal{O}_L$, la $\mathcal{O}_L$-composante de $\varphi(x)\overline{\varphi(x')}$ (autrement dit l'image de (x,x') par la G-forme sur $\mathcal{O}_L$ correspondant à la forme $\langle 1 \rangle$ sur $\mathcal{O}_L[G]$) est $\sum_{g\in G} g(x)g(x')gg^{-1} = \sum_{g\in G} g(xx') = Tr(xx')$.

Lorsque l'on prend $\phi = \mathrm{Id} \otimes \varphi : \mathcal{O}_L \otimes \mathcal{O}_L \to \mathcal{O}_L[G]$, on obtient un homomorphisme G-équivariant de $\mathcal{O}_L$-modules, qui associe à la G-forme unité la G-forme prolongeant la forme trace après extension des scalaires. Or, si l'extension L/K est non-ramifiée, ϕ est un isomorphisme; en effet, étant donnée une base $\{x_i\}$ de $\mathcal{O}_L \otimes \mathcal{O}_L$ sur $\mathcal{O}_L$, les images des éléments de base dans le $\mathcal{O}_L$-module $\mathcal{O}_L[G]$ sont les $\sum_{g \in G} g(x_i)g^{-1}$, et la matrice de ϕ est la matrice des $\{g(x_i)\}_{g \in G}$, dont le déterminant est le discriminant de l'extension de corps, inversible si et seulement si L est non-ramifiée sur K.

Ainsi, l'algèbre galoisienne $\mathcal{O}_L[G]$ sur $\mathcal{O}_L$ possède une base normale autoduale. La G-forme unité et la G-forme trace sur le $\mathcal{O}_L$-module $\mathcal{O}_L[G]$, sont donc isomorphes, et on peut appliquer the théorème 4.1 pour conclure que la G-forme unité et la G-forme trace sur le $\mathcal{O}_K$-module $\mathcal{O}_L$, sont isomorphes, et que $\mathcal{O}_L$ a une base normale autoduale sur $\mathcal{O}_K$. □

Bibliographie.

[BAY] E. Bayer-Fluckiger, Self-dual normal bases, *Indag. Math.*, **51** (1989), 379–383.

[BL] E. Bayer-Fluckiger, H. W. Lenstra Jr, Forms in odd-degree extensions and self-dual normal bases, *Amer. J. Math.* **112** (1990), 359–373.

[BKW] E. Bayer-Fluckiger, C. Kearton and S. M. J. Wilson, Hermitian forms in additive categories, *J. Algebra* **123**, No. 2 (1989), 336–350.

[CP] P. E. Conner, R. Perlis *A survey of trace forms of algebraic number fields*, World Scientific, Singapore, (1984).

[CR] C. W. Curtis, I. Reiner, *Methods of representation theory, with applications to finite groups and orders*, vol 1, Wiley (1981).

[LNG] S. Lang, *Algebraic Number Theory*, Addison-Wesley (1970).

[NOE] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, *Crelle* **167** (1932), 147–152.

[QSS] H.-G. Quebbemann, W. Scharlau and M. Schulte, Quadratic and hermitian forms in additive and abelian categories, *J. Algebra* **59** (1979), 264–289.

[QSSS] H.-G. Quebbemann, R. Scharlau, W. Scharlau and M. Schulte, Quadratische Formen in additiven Kategorien, *Bull. Soc. Math. France*, Mémoire **48** (1976), 93–101.

[SCH] W. Scharlau, *Quadratic and hermitian forms*, Grundlehren der Math. Wiss. **270**, Springer Verlag (1985).

[SER] J.-P. Serre, *Corps locaux*, Hermann, Paris (1968).