THE HASSE PRINCIPLE FOR SIMILARITIES OF BILINEAR FORMS

by Anne Cortella

Introduction

Let k be a number field and V a finite-dimensional k-vector space . Two bilinear forms b and $b' : V \times V \longrightarrow k$ are *similar* if there exists $\lambda \in k^*$ such that b and $\lambda b'$ are isomorphic. T. Ono proved [O] that the Hasse principle holds for similarities of quadratic forms (another proof of this fact is given in [C1]). W.C. Waterhouse [W] proved that the Hasse principle also holds for isomorphisms of non-symmetric bilinear forms.

This article studies the problem for similarities of bilinear forms. We show that this Hasse principle is not true in general and give a description of the obstruction group associated with the problem. In part I, we define some invariants of bilinear forms, using a k-algebra introduced by E. Bayer-Fluckiger [Ba]. These invariants are pairs of matrix algebras over k, switched by an involution, and quadratic, alternating and hermitian forms over finite extensions of the base field.

When the only invariant of a form b is a hermitian form of rank one over an extension L/k of the basis field, the Hasse principle for being similar to b is equivalent to a local-global principle concerning the norms of L over an intermediate extension. In part II, we express the obstruction group of this norm problem, which we first translate into the language of cohomology of algebraic tori. Then, using a theorem of Tate, we show that the obstruction is a finite group and give an expression for this group in the case when L/k is a Galois extension. If L/k is not Galois, we give an expression for a subgroup of the obstruction group.

We evaluate this expression for extensions of small degree, and we see that the smallest order of the Galois group for which the obsruction can be non trivial is 8. Part III gives a counter-example to the Hasse principle for similarities of bilinear forms. This uses a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{H}_8$ due to J. Martinet [Ma].

I thank Eva Bayer-Fluckiger who has been my supervisor during this work, and Georges Gras for the interest he has shown.

I Invariants associated with a bilinear form

Two bilinear forms b and $b' : V \times V \longrightarrow k$ are isomorphic if and only if their non-degenerate parts are isomorphic. Moreover, if k is a number field, v a place of k and k_v the completion of

k at v, the non-degenerate part of $b \otimes k_v$ is the extension to k_v of the non-degenerate part of b. Hence, we restrict ourselves to non-degenerate bilinear forms.

I.1 The algebra with involution

To a bilinear form $b : V \times V \to k$, we associate the k-algebra

$$R = \{(e, f) \in \text{End } V \times \text{End } V \mid \forall (x, y) \in V \ , \ b(ex, y) = b(x, fy) \ \text{ and } \ b(x, ey) = b(fx, y)\}$$

following E. Bayer-Fluckiger in [Ba]. The algebra R only depends on the equivalence class of b (although two non-equivalent forms can have the same k-algebra). The algebra R has a natural involution * defined by $(e, f)^* = (f, e)$.

Recall that the norm-one group of the involution is

$$U(R) = \{(e, f) \in R \mid (e, f)^*(e, f) = 1\}.$$

It is easy to see that the automorphism group A_b of the form b is canonically isomorphic to $U(R)$.

Let B be the matrix of b with respect to a basis of V . Then we have

$$R = \{(E, F) \in \mathbf{M}_n(k) \times \mathbf{M}_n(k) \mid BE = F^t B \ \text{ and } \ E^t B = BF\}$$

$$= \{E \in \mathbf{M}_n(k) \mid EB^{-1}B^t = B^{-1}B^t E\}.$$

Let $M = B^{-1}B^t$. The involution of R can now be written : $E^* = (BEB^{-1})^t$. Moreover $M^* = M^{-1}$.

I.2 Decomposition of R

We now define matrix algebras over extension fields of k that characterise the algebra R .

Let J be the radical of R . Then $J^* = J$ and the involution * induces an involution, again denoted by *, on the semi-simple algebra R/J. This algebra has a decomposition into simple algebras :

$$R/J = R_1 \times ... \times R_r \times (R_{r+1} \times R_{r+1}^*) \times ... \times (R_s \times R_s^*)$$

where $R_i = \mathbf{M}_{n_i}(D_i)$, D_i is a division algebra over k , and $R_i^* = R_i$ for $i \leq r$.

Proposition : The divison algebras D_i are commutative fields.

Proof : The matrix M induces a $k[X]$-module structure on V, where the action of X is given by the endomorphism associated to M (again denoted by M). Then V is a finitely generated torsion $k[X]$-module (since it is finitely generated over k).

The module V is the direct sum of its indecomposable submodules. As $k[X]$ is a principal ideal domain, the indecomposable submodules are of the type $V_i = k[X]/P_i^{m_i}$ where P_i is an irreducible polynomial. Note that $M(V_i) \subset V_i$. We denote by M_i the restriction of M to V_i . Its minimal polynomial is $P_i^{m_i}$, and there exists a basis $(\varepsilon_{i,j})_{1 \leq j \leq n_i}$ in which the matrix of M_i

is the companion-matrix of $P_i^{m_i}$, defined as follows : let $P_i^{m_i} = X^{r_i} + a_{i,r_i-1}X^{r_i-1} + ... + a_{i,0}$; then

$$M_i(\varepsilon_{i,j}) = \varepsilon_{i,j+1} \text{ if } j \leq r_i - 1 \text{ , and } M(\varepsilon_{i,r_i}) = -\sum_{j=0}^{r_i-1} a_{i,j}\varepsilon_{i,j+1}.$$

Then M is bloc-diagonal with blocs M_i. Let us reorder the blocs such that M_1, ..., M_t are all distinct and that t is maximal with this property. Let n'_i be the multiplicity of the bloc M_i, and let M'_i be the bloc-diagonal matrix consisting in n'_i blocs all equal to M_i .

As R is the centralizer of M , we have

$$R/J = \prod_{i=1}^{t} R'_i/Rad\, R'_i$$

where R'_i is the centralizer of the matrix M'_i. Moreover, R'_i is the set of matrices of $n_i'^2$ blocs of size $r_i \times r_i$ (i.e. the size of M_i) that all commute with M_i :

$$R'_i = \mathrm{M}_{n'_i}(Z(M_i)) \text{ with } Z(M_i) = \{N \in \mathrm{M}_{r_i}(k) \,|\, M_iN = NM_i\}.$$

Let $A_i = k[X]/P_i^{m_i}$. Then $A_i \simeq \mathrm{End}_{A_i} A_i$, the set of k-endomorphisms of A_i that commute with the action of X, i.e. with the matrix M_i . Therefore we have :

$$A_i = \mathrm{End}_{A_i}\ A_i = \{N \in \mathrm{M}_{r_i}(k) \,|\, M_iN = NM_i\} = Z(M_i)$$

and $R'_i = \mathrm{M}_{n'_i}(A_i)$

Let L_i be the commutative field $k[X]/P_i$. We know that
$L_i = A_i/\mathrm{Rad}\ A_i$ and that $R'_i/\mathrm{Rad}\ R'_i = \mathrm{M}_{n'_i}(L_i)$.

Remark : Note that we have in fact proved that the division algebras D_i are extension fields $L_i = k(\alpha_i)$ of k, where α_i is a root of the irreducible polynomial P_i where $P_i^{m_i}$ is the minimal polynomial of M_i for a certain m_i (up to a change of indices).

I.3 The invariants of the form b

We now associate to the algebra R , and in particular to its simple factors, some invariants of the bilinear form b. As we shall see, these invariants are of different nature according as the simple factor is stable under the involution or not.

Recall that we have the decomposition :

$$R/J = R_1 \times ... \times R_r \times (R_{r+1} \times R_{r+1}^*) \times ... \times (R_s \times R_s^*)$$

where $R_i = \mathbf{M}_{n_i}(L_i)$, L_i is an extension field of k , and $R_i^* = R_i$ for $i \leq r$.

Let us first assume that $r + 1 \leq i \leq s$. Then the algebras R_i and R_i^* are switched by the involution. The invariant associated to the form b will then be the pair $R_i \times R_i^*$.

Now assume that $1 \leq i \leq r$. Then the algebra R_i is stable under the involution. The field L_i is the center of the algebra, and therefore is also preserved by the involution. The restriction of * to L_i is an involution of the field. We denote it by $^-$.

The map $N \mapsto \overline{N}^t$ is then another involution of R_i . The Skolem-Noether theorem implies that these two involutions are conjugate to each other. Hence there exists an $H_i \in R_i$ such that for all $N \in R_i$ we have $N^* = H_i \overline{N}^t H_i^{-1}$. Moreover, H_i satisfies $H_i = \pm \overline{H}_i^t$ [Sch, th. 7-4 p301].

When the involution of L_i is of the first kind (i.e. when $^- = Id_{L_i}$), then $H_i^{-1} = \pm H_i^t$. This is the matrix of a symmetric or antisymmetric bilinear form h_i over $W_i = L_i^{n_i}$.

When the involution of L_i is of the second kind (i.e. when $^- \neq Id_{L_i}$), then by the same theorem, we can take $H_i^{-1} = \overline{H}_i^t$. This is the matrix of a hermitian form h_i over $W_i = L_i^{n_i}$ for the involution $^-$.

The isomorphism classes of these quadratic, alternating or hermitian forms are invariants of the isomorphism class of b.

I.4 Restatement of the Hasse principle in a special case

The aim of this article is to study the special case where there is only one term in the decomposition of the algebra R/J into simple factors, and where the associated invariant is a one-dimensional hermitian form over an extension of k .

In the general case, the group GA_b of similarities of b is the group :

$$\begin{aligned} GA_b(k) &= \{e \in \mathrm{GL}(V) \mid \exists \lambda \in k\ ,\ \lambda \neq 0\ ,\ \forall (x,y) \in V\ ,\ b(ex,ey) = \lambda b(x,y)\} \\ &= \{e \in \mathrm{GL}(V) \mid \exists \lambda \in k\ ,\ \lambda \neq 0\ ,\ \forall (x,y) \in V\ ,\ b(ex,y) = b(x,\lambda e^{-1} y)\}\ . \\ &= \{(e,f) \in R \mid \exists \lambda \in k\ ,\ \lambda \neq 0\ ,\ ef = \lambda\ \mathrm{Id}\} \end{aligned}$$

Hence $GA_b(k) = GU(R) = \{r \in R \mid rr^* \in k^*\}$.

If k is a number field, we denote by Σ the set of places of k, and by k_v the completion of k at the place v.

Recall that for b bilinear over k (resp. k_v), $H^1(k, GA_b)$ (resp. $H^1(k_v, GA_b)$) is the pointed set of similarity classes over k (resp. k_v) of bilinear forms isomorphic to b over a separable closure k^{sep} of k (resp. k_v^{sep} of k_v), with distinguished element the class of b (cf [Se1, X]). Moreover, if there is a place v such that the two forms b and b' are isomorphic over k_v^{sep} , they are also isomorphic over k^{sep}. Indeed, the manifold of isomorphisms from b to b' is smooth; such a manifold has points over k^{sep}. (cf [Ro]).

The restriction $H^1(k, GA_b) \longrightarrow H^1(k_v, GA_b)$ maps the similarity class of b' over k to its class over k_v. We see that all bilinear forms from $V \times V$ to k similar to b over every k_v are similar to b over k if and only if the kernel of the natural morphism

$$H^1(k, GU(R)) \longrightarrow \prod_{v \in \Sigma} H^1(k_v, GU(R))$$

is trivial.

Let us see what this means in the simplest case : suppose from now on that R is a k-algebra which is an extension field $R = L$ of k (i.e. $r = s = 1$ and $n_1 = 1$). Then $L = k(\alpha)$ with α a root of the minimal polynomial of the irreducible matrix $M = B^{-1}B^t$. The involution on L is the k-involution defined by $\overline{\alpha} = \alpha^{-1}$.

If this involution is trivial, then $M^{-1} = M$, hence $M^2 - Id = 0$. As there is no subspace invariant by M, this implies that $M = \pm Id$ and $L = k$. Hence $GU(L) = k^*$. By Hilbert's theorem 90 we have $H^1(k, GA_b) = H^1(k,\mathbb{G}_m) = 0$. Thus every bilinear form isomorphic to b over k^{sep} is similar to b over k.

If now the involution $^-$ is not trivial, then L is a genuine extension of k , of even degree, and $L = k[X]/P$ where P is an irreducible polynomial of the type :

$$P = \sum_{i=0}^{n} a_i X^i, \text{ with for all } i \ : a_{n-i} = \varepsilon a_i \ , \ \varepsilon = \pm 1$$

(because the inverses of the roots of P are again roots of P). In other words P is symmetric or skew-symmetric. However, a skew-symmetric polynomial of even degree is always divisible by $1 - X^2$, hence cannot be irreducible. Therefore P is symmetric.

We see that

$$GU(L) = \{z \in L \,|\, z\overline{z} \in k^*\}$$

is the set of k-similarities of the hermitian form $< 1 >$ over L. Hence $H^1(k, GA_b)$ is the set of k-similarity classes of one-dimensional hermitian forms over L. Note that a hermitian form $< a >$ over L is k-similar to $< 1 >$ if and only if there exist $z \in L^*$ and $\lambda \in k^*$ such that $a = \lambda N_{L/K}(z)$.

Recall that the subfield of L fixed by the involution is $K = k[\alpha + \alpha^{-1}]$

We obtain the following restatement of the Hasse principle :

Proposition : *Let k be a number field, and b be a bilinear form over k. Suppose that the k-algebra associated to b is a commutative field L and that the involution is not trivial. Let K be the fixed field of the involution.*

For every place v of k, let K_v be the étale algebra $\prod_{w|v} K_w$, product of the completions of K for the places w of K lying over v, and $L_v = \prod_{w'|v} L_{w'}$.

Then, every bilinear form over V similar to b over all the completions k_v of k is similar to b over k if and only if every element a of K that can be written $a = \lambda_v N_{L_v/K_v}(z_v)$, with $z_v \in L_v^*$ and $\lambda_v \in k_v^*$, is in $k^* N_{L/K}(L^*)$.

II Reformulation of the Hasse principle in terms of cohomology of algebraic tori

Let L/k be a finite extension of number fields and let K/k be a subextension. We denote by Σ the set of places of k. Set :

$$\mathcal{L} = \{a \in K^* \mid \forall v \in \Sigma \ , \ \exists z_v \in L_v^* \text{ et } \exists \lambda_v \in k_v^* \mid a = \lambda_v N_{L_v/K_v}(z_v) \ \}$$
$$\mathcal{G} = k^* N_{L/K}(L^*)$$

where $K_v = \prod_{w|v} K_w$, and $L_v = \prod_{w'|v} L_{w'}$.

Let $Ш(k, K, L) = \mathcal{L}/\mathcal{G}$. If L/K is quadratic, then by the proposition I.4, the Hasse principle is equivalent to the vanishing of the group $Ш(k, K, L)$.

II.1 A Tate-Schafarevich obstruction for algebraic tori

For a finite separable extension k'/k, we denote by $T_{k'} = \mathbf{R}_{k'/k}\mathbb{G}_m$ the algebraic torus over k which is the Weil restriction from k' to k of the mutiplicative algebraic group $\mathbb{G}_m$. The group of k-points of $T_{k'}$ is then $T_{k'}(k) \simeq k'^*$. In particular $T_k = \mathbb{G}_m$.

Let us consider the homomorphism of k-algebraic groups :

$$f : \begin{cases} \mathbb{G}_m \times T_L & \longrightarrow & T_K \\ (x, y) & \longmapsto & xN_{T_L/T_K}y \end{cases}$$

which is surjective and has connected kernel. The kernel of f is then another k-torus, which we denote by T' .

We have the short exact sequence of tori :

$$(1) \qquad 1 \longrightarrow T' \longrightarrow \mathbb{G}_m \times T_L \longrightarrow T_K \longrightarrow 1.$$

This sequence induces the long exact sequence of cohomology :

$$0 \to H^0(k, T') \to H^0(k,\mathbb{G}_m \times T_L) \xrightarrow{f_0} H^0(k, T_K) \to H^1(k, T') \to H^1(k,\mathbb{G}_m \times T_L) .$$

Recall that $H^i(k, T_{k'}) = H^i(k, \mathbf{R}_{k'/k}\mathbb{G}_m) = H^i(k',\mathbb{G}_m)$. Hence we have :

$$\begin{array}{l} H^0(k, T_K) = K^* \\ H^0(k,\mathbb{G}_m \times T_L) = H^0(k,\mathbb{G}_m) \times H^0(k, T_L) = k^* \times L^* \\ H^1(k,\mathbb{G}_m \times T_L) = H^1(k,\mathbb{G}_m) \times H^1(L,\mathbb{G}_m) = 0 \text{ by Hilbert's theorem 90.} \end{array}$$

Moreover $f_0 : k^* \times L^* \longrightarrow K^*$ is defined by $f_0(\lambda, z) = \lambda N_{L/K}(z)$, therefore $\mathcal{G} = \operatorname{Im} f_0$. The last exact sequence implies :

$$k^* \times L^* \longrightarrow K^* \longrightarrow H^1(k, T') \longrightarrow 0$$

$$K^*/\mathcal{G} = \operatorname{coker} f_0 = H^1(k, T') .$$

For a place v of k , (1) is again an exact sequence of k_v-tori, and we can take its cohomology exact sequence over k_v. We get, as for k, that

$$K_v^*/\mathcal{L}_v = \operatorname{coker} f_0^v = H^1(k_v, T')$$

where $\mathcal{L}_v = k_v^* N_{L_v/K_v}(L_v^*)$.

The fact that $Ш(k, K, L) = \ker(K^*/\mathcal{G} \longrightarrow \prod_{v\in\Sigma} K_v^*/\mathcal{L}_v)$ (this natural morphism being the restriction on each component) then implies :

Theorem : *The obstruction group* $Ш(k, K, L)$ *for the Hasse principle is the Tate-Schafarevich group of the torus* T' :

$$Ш(k, K, L) = Ш(k, T') = \ker(\, H^1(k, T') \longrightarrow \prod_{v\in\Sigma} H^1(k_v, T')\,).$$

II.2 Consequences of Tate's theorem

If T is a k-torus, M/k a Galois extension containing L that splits the torus T, $G = \mathrm{Gal}(M/k)$ and G_v the decomposition group of M/k at the place v. Denote by $X(T) = \mathrm{Hom}(T, \mathbb{G}_m)$ the group of characters of the torus T . The action of G on $X(T)$ is given by :

$$({}^s f)(t) = s.\, f(s^{-1}(t))\,.$$

Theorem (Tate): (proof see for instance [PR, cor. to prop 6-9 p301 and th 6-10 p302 with i=1] *The group* $Ш(k,T)$ *is a finite group, dual to*

$$\ker(\, H^2(G, X(T)) \longrightarrow \prod_{v\in\Sigma} H^2(G_v, X(T))\,).$$

We now apply this theorem to the torus T'. Let M/k be a Galois extension that splits the torus T', $G = \mathrm{Gal}(M/k)$, J the set of k-embeddings from L to M, I those from K to M. Then we have :

$$\begin{array}{llll} J = G/\Gamma_1 & \text{where} & \Gamma_1 & = \mathrm{Gal}(M/L) \\ I = G/\Gamma_2 & \text{where} & \Gamma_2 & = \mathrm{Gal}(M/K). \end{array}$$

The action of G over J and I is the left translation.

Let $H = \mathrm{Gal}(L/K)\,(\simeq \mathbb{Z}/2\mathbb{Z})$. Then Γ_1 is normal in Γ_2 and $\Gamma_2/\Gamma_1 \simeq H$. This corresponds to the tower of fields:

$$G \left(\begin{array}{ll} \Gamma_2 & \left(\begin{array}{l} M \\ |\ \Gamma_1 \\ L \\ |\ H \\ K \\ | \\ k \end{array} \right. \end{array} \right.$$

With these notations, the character groups of the tori are (cf [Bo, ch III 8]) :

$$\begin{array}{lllllll} X(\mathbb{G}_m) & = & \mathbb{Z} & & & & (\text{ with trivial action of } G\ ) \\ X(T_K) & = & X(\mathbf{R}_{K/k}\mathbb{G}_m) & = & \mathbb{Z}^I & = & \mathbb{Z}[G/\Gamma_2] \\ X(T_L) & = & X(\mathbf{R}_{L/k}\mathbb{G}_m) & = & \mathbb{Z}^J & = & \mathbb{Z}[G/\Gamma_1]. \end{array}$$

The exact sequence (1) gives by transposition :

(2) $\qquad 0 \longrightarrow \mathbb{Z}[G/\Gamma_2] \longrightarrow \mathbb{Z}[G/\Gamma_1] \times \mathbb{Z} \longrightarrow X(T') \longrightarrow 0$

The first homomorphism of this sequence is given by

$$\text{(i)}\quad \begin{array}{ccc} \mathbb{Z}[G/\Gamma_2] & \hookrightarrow & \mathbb{Z}[G/\Gamma_1] \\ \overline{g} & \mapsto & \sum\limits_{s\in\Gamma_2/\Gamma_1} \overline{gs} \end{array} \qquad \text{and} \qquad \text{(ii)}\quad \begin{array}{ccc} \mathbb{Z}[G/\Gamma_2] & \to & \mathbb{Z} \\ \sum\limits_{\overline{g}\in G/\Gamma_2} n_{\overline{g}}\overline{g} & \mapsto & \sum\limits_{\overline{g}\in G/\Gamma_2} n_{\overline{g}} \end{array}$$

(obtained by transposing the norm $T_L \stackrel{N}{\to} T_K$ and the injection $\mathbb{G}_m \hookrightarrow T_K$).

We use the cohomology exact sequence of (2) to determine the group $Ш(k,T')$ that we have identified with its dual.

II.3 The Galois case

If L/k is Galois, we can take $M = L$ and we have $\Gamma_1 = 1$ et $\Gamma_2 = H$. Set $X = X(T')$.
The sequence (2) becomes (2') :

$$(2') \qquad 0 \longrightarrow \mathbb{Z}[G/H] \longrightarrow \mathbb{Z}[G]\times\mathbb{Z} \longrightarrow X \longrightarrow 0.$$

It follows that :

$$H^2(G,\mathbb{Z}[G/H]) \to H^2(G,\mathbb{Z}[G])\times H^2(G,\mathbb{Z}) \to H^2(G,X) \to H^3(G,\mathbb{Z}[G/H]).$$

For each place v of k, we have a similar exact sequence. The restriction morphisms from G to G_v commute with the morphisms of these sequences and give rise to the commutative diagram $(\mathcal{D})$:

$$\begin{array}{ccccccc} H^2(G,\mathbb{Z}[G/H]) & \to & H^2(G,\mathbb{Z}[G])\times H^2(G,\mathbb{Z}) & \to & H^2(G,X) & \to & H^3(G,\mathbb{Z}[G/H]) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \prod\limits_{v\in\Sigma} H^2(G_v,\mathbb{Z}[G/H]) & \to & \prod\limits_{v\in\Sigma} (H^2(G_v,\mathbb{Z}[G])\times H^2(G_v,\mathbb{Z})\,) & \to & \prod\limits_{v\in\Sigma} H^2(G_v,X) & \to & \prod\limits_{v\in\Sigma} H^3(G_v,\mathbb{Z}[G/H]). \end{array}$$

To simplify this diagram, we first observe that $\mathbb{Z}[G]$ is a free G-group and hence has trivial cohomology.

As a G-group, $\mathbb{Z}[G/H] = \mathrm{Ind}_H^G \mathbb{Z}$,where H acts trivially over $\mathbb{Z}$. From Shapiro's lemma [Br, prop. 6-2 p 73] , it follows that for all $r \geq 1$ we have inverse isomorphisms :

$$H^r(G,\mathbb{Z}[G/H]) \underset{cor\circ i}{\overset{j\circ res}{\rightleftarrows}} H^r(H,\mathbb{Z})$$

where $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[G/H]$ is the inclusion and $j : \mathbb{Z}[G/H] \to \mathbb{Z}$ is the morphism given by (ii).

As a G_v-group, $\mathbb{Z}[G/H] = \bigoplus\limits_{i=1}^{r_v} \mathbb{Z}[K_i^v/H] \simeq \bigoplus\limits_{i=1}^{r_v} \mathbb{Z}[G_v/H_i^v] = \bigoplus\limits_{i=1}^{r_v} \mathrm{Ind}_{H_i^v}^{G_v} \mathbb{Z}$;

there $K_i^v = G_v\, x_i^v\, H$ runs through the double classes of $G_v \backslash G / H$, $H_i^v = G_v \bigcap x_i^v\, H\, (x_i^v)^{-1}$ and the isomorphism in the middle is on each term the right translation by $(x_i^v)^{-1}$.

Shapiro's lemma then gives isomorphisms :

$$H^r(G_v, \mathbb{Z}[G/H]) \simeq \bigoplus_{i=1}^{r_v} H^r(H_i^v, \mathbb{Z})\,.$$

For $r = 3$, the facts that H and the H_i^v's are cyclic and act trivially on $\mathbb{Z}$ imply that $H^3(H, \mathbb{Z}) = H^1(H, \mathbb{Z}) = \mathrm{Hom}(H, \mathbb{Z}) = 0$.

The commutative diagram $(\mathcal{D})$ becomes :

$$\begin{array}{cccccccc} & H^2(H,\mathbb{Z}) & \stackrel{\varphi_0}{\to} & H^2(G,\mathbb{Z}) & \stackrel{\varphi_1}{\to} & H^2(G,X) & \to & 0 \\ (\mathcal{D}') & \downarrow\ \alpha_0 & & \downarrow\ \alpha_1 & & \downarrow\ \alpha_2 & & \\ & \prod\limits_{v\in\Sigma} (\bigoplus\limits_{i=1}^{r_v} H^2(H_i^v,\mathbb{Z})) & \stackrel{\psi_0}{\to} & \prod\limits_{v\in\Sigma} H^2(G_v,\mathbb{Z})) & \stackrel{\psi_1}{\to} & \prod\limits_{v\in\Sigma} H^2(G_v,X) & \to & 0 \end{array}$$

In this diagram, each morphism can be described in terms of the natural morphisms of restriction, corestriction and conjugation : we know from $(\mathcal{D})$ that α_1 and α_2 are, on each component, the restriction from G to G_v .

The morphism α_0 on each non-zero component is the bijection given by conjugation by $(x_i^v)^{-1}$ from H to H_i^v. Indeed, the cohomological functor (in A) $H^r(H, A) \longrightarrow \bigoplus\limits_{i=1}^{r_v} H^r(H_i^v, A_i^v)$ with $A_i^v = x_i^v A \subset \mathrm{Ind}_H^G A$, obtained by composition of the following functors

$$H^r(H,A) \stackrel{coro\,i}{\longrightarrow} H^r(G, \mathrm{Ind}_H^G A) \stackrel{res}{\longrightarrow} H^r(G_v, \mathrm{Ind}_H^G A) \stackrel{Shapiro}{\longrightarrow} \bigoplus_{i=1}^{r_v} H^r(H_i^v, A_i^v)$$

is exactly the functor given by the compatible morphisms : conjugation by $(x_i^v)^{-1} : H_i^v \to H$ and translation by $x_i^v : A \to A_i^v$ as it can easily be seen in degree zero.

By the same argument, the horizontal morphism φ_0 is the corestriction from H to G, and $\psi_{0,v}$ is the sum of corestrictions from H_i^v to G_v.

Hence we have proved :

Theorem :

$$Ш(k, T') \;=\; \alpha_1^{-1}(\mathrm{Im}\,\psi_0)/\mathrm{Im}\,\varphi_0\,.$$

We can also use the diagram to express $Ш(k, T')$ as a quotient of a subgroup of $\prod\limits_{v\in\Sigma} (\bigoplus\limits_{i=1}^{r_v} H^2(H_i^v, \mathbb{Z}))$. To do that, one just has to notice that α_0 is injective : it is bijective on each non-zero component and there is at least one non-zero H_i^v (for $G_v = H$ and $x_i^v = 1$).

We also need the fact that α_1 is injective : the exact sequence of cohomology of

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and the fact that $\hat{H}^i(G,\mathbb{Q}) = 0$ imply $\hat{H}^i(G,\mathbb{Z}) = \hat{H}^{i-1}(G,\mathbb{Q}/\mathbb{Z})$ for all $i \in \mathbb{Z}$ (this equality concerns Tate's modified cohomology groups). Hence

$$\alpha_1 = res \ : \ \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \longrightarrow \prod_{v\in\Sigma} \mathrm{Hom}(G_v,\mathbb{Q}/\mathbb{Z})$$

which is injective (because G is covered by the G_v's).

Thus $Ш(k,T') \simeq \psi_0^{-1}(\mathrm{Im}\,\alpha_1)/(\ker\psi_0 + \mathrm{Im}\,\alpha_0)$.

This gives rise to a first explicit description of $Ш(k,T')$. The group H is cyclic, and $H^2(H,\mathbb{Z}) = \hat{H}^0(H,\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. The same is true for each non-zero H_i^v : $H^2(H_i^v,\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. We deduce that :

Proposition : $Ш(k,T')$ *is a finite product of cyclic groups of order* 2.

To compute our obstruction group in concrete cases, we will use another description that can be found by using once again duality.

First notice that G has finitely many subgroups. Hence $\{G_v \ , \ v \in \Sigma\} = \{G_1,...,G_l\}$ for certain subgroups G_i of G. Let $v_i \in \Sigma$ be such that $G_i = G_{v_i}$ for $i = 1,...l$. Set $\Omega = \{v_1,...,v_l\}$. When we replace "$v \in \Sigma$" by "$v \in \Omega$" everywhere in $(\mathcal{D}')$, we get a new commutative diagram which discribes the obstruction group exactly as before.

The commutative square needed to describe the group Ш can be written as follows :

$$(\mathcal{C}) \qquad \begin{array}{ccc} \mathrm{Hom}(H,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi_0} & \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \\ \downarrow \alpha_0 & & \downarrow \alpha_1 \\ \prod\limits_{v\in\Omega} \big(\bigoplus\limits_{i=1}^{r_v} \mathrm{Hom}(H_i^v,\mathbb{Q}/\mathbb{Z}) \big) & \xrightarrow{\psi_0} & \prod\limits_{v\in\Omega} \mathrm{Hom}(G_v,\mathbb{Q}/\mathbb{Z}) \end{array}$$

Since the Pontriyagin dual of the finite group $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ is the greatest abelian quotient $G^{ab} = G/[G,G]$ of G (and the same for G_v , H_i^v et H), the dual diagram of $(\mathcal{C})$ is the commutative square :

$$(\mathcal{C}') \qquad \begin{array}{ccc} H & \xleftarrow{\mu} & G^{ab} \\ \uparrow \gamma & & \uparrow \delta \\ \prod\limits_{v\in\Omega} \big(\bigoplus\limits_{i=1}^{r_v} H_i^v \big) & \xleftarrow{\eta} & \prod\limits_{v\in\Omega} G_v^{ab} \end{array}$$

Each morphism involved in this diagram is the dual of the corresponding morphism in $(\mathcal{C}')$, so that : μ is the tranfert $ver_H^G : G^{ab} \to H$; $\eta_v = \sum\limits_{i=1}^{r_v} ver_{H_i^v}^{G_v} : G_v^{ab} \to \bigoplus\limits_{i=1}^{r_v} H_i^v$; δ_v is the

morphism $G_v^{ab} \to G^{ab}$ induced by the injection $G_v \to G$; and $\gamma_i^v : H_i^v \to H$ is the conjugation by $(x_i^v)^{-1}$.

The dual expression of the previous theorem is :

Theorem :

$$Ш(k, T') = \ker \mu / \delta\,(\ker \eta).$$

II.4 The general case

We keep the notations of paragraph 2.

The exact sequence (2) now gives rise to the commutative diagram :

$$\begin{array}{ccccccc}
H^2(G, \mathbb{Z}[G/\Gamma_2]) & \stackrel{\varphi_0}{\to} & H^2(G, \mathbb{Z}[G/\Gamma_1]) & \times & H^2(G, \mathbb{Z}) & \stackrel{\varphi_1}{\to} & \\
\downarrow \alpha_0 & & & & \downarrow \alpha_1 & & \\
\prod_{v\in\Sigma} H^2(G_v, \mathbb{Z}[G/\Gamma_2]) & \stackrel{\psi_0}{\to} & \prod_{v\in\Sigma} (H^2(G_v, \mathbb{Z}[G/\Gamma_1]) & \times & H^2(G_v, \mathbb{Z})) & \stackrel{\psi_1}{\to} &
\end{array}$$

$$\begin{array}{ccccc}
\stackrel{\varphi_1}{\to} & H^2(G, X) & \stackrel{\varphi_2}{\to} & H^3(G, \mathbb{Z}[G/\Gamma_2]) \\
& \downarrow \alpha_2 & & \downarrow \alpha_3 \\
\stackrel{\psi_1}{\to} & \prod_{v\in\Sigma} H^2(G_v, X) & \stackrel{\psi_2}{\to} & \prod_{v\in\Sigma} H^3(G_v, \mathbb{Z}[G/\Gamma_2])
\end{array}$$

But $Ч(k, T') = \alpha_1^{-1}(\text{Im } \psi_0)/\text{Im } \varphi_0$ is now just a subgroup of $Ш(k, T')$. It is the first obstruction group to the Hasse principle.

These two groups are again isomorphic as soon as α_3 is injective, and in particular when Γ_2 is cyclic : if we decompose, for any place v of k, G into its double classes $K_i^v = G_v x_i^v \Gamma_2$ $(i = 1, ..., r_v)$ of $G_v \backslash G / \Gamma_2$ and write $\Gamma_{2,i}^v = G_v \bigcap x_i^v \Gamma_2 (x_i^v)^{-1}$, it follows from Shapiro's lemma that α_3 can be seen as a morphism :

$$H^3(\Gamma_2, \mathbb{Z}) \longrightarrow \prod_{v\in\Sigma} (\bigoplus_{i=1}^{r_v} H^3(\Gamma_{2,i}^v, \mathbb{Z})) .$$

These groups of cohomology are trivial when Γ_2 is cyclic. The morphism α_3 is again injective if there is a place v such that G_v is large enough to contain a conjugate of Γ_2 , because the morphism from $H^3(\Gamma_2, \mathbb{Z})$ to $H^3(\Gamma_{2,i}^v, \mathbb{Z})$ is then an isomorphism (conjugation by x_i^v).

The commutative diagram used to define $Ч(k, T')$ can be split into two independant squares

$$
\begin{array}{ccc}
H^2(G,\mathbb{Z}[G/\Gamma_2]) & \stackrel{\phi}{\longrightarrow} & H^2(G,\mathbb{Z}[G/\Gamma_1]) \\
\downarrow \alpha_0 & & \downarrow \beta_0 \\
\prod\limits_{v\in\Sigma} H^2(G_v,\mathbb{Z}[G/\Gamma_2]) & \stackrel{\sigma}{\longrightarrow} & \prod\limits_{v\in\Sigma} H^2(G_v,\mathbb{Z}[G/\Gamma_1])
\end{array}
\qquad (\mathcal{C}_0)
$$

$$
\begin{array}{ccc}
H^2(G,\mathbb{Z}[G/\Gamma_2]) & \stackrel{\theta}{\longrightarrow} & H^2(G,\mathbb{Z}) \\
\downarrow \alpha_0 & & \downarrow \beta_1 \\
\prod\limits_{v\in\Sigma} H^2(G_v,\mathbb{Z}[G/\Gamma_2]) & \stackrel{\rho}{\longrightarrow} & \prod\limits_{v\in\Sigma} H^2(G_v,\mathbb{Z})
\end{array}
\qquad (\mathcal{C}_1)
$$

Thus

$$Ч(k,T') = Ч_0(k,T') \times Ч_1(k,T')$$

where $\quad Ч_0(k,T') = \beta_0^{-1}(\text{Im } \sigma)/\text{Im } \phi \quad$ and $\quad Ч_1(k,T') = \beta_1^{-1}(\text{Im } \rho)/\text{Im } \theta$

Study of $Ч_0(k,T')$

Let T_0 be the k-torus kernel of the norm homomorphism from T_L to T_K. We obtain the exact sequence

$$1 \to T_0 \to T_L \to T_K \to 1$$

The torus T_0 is in fact the Weil restriction from K to k of the kernel T_0' of the norm from $\mathbf{R}_{L/K}\mathbb{G}_m$ to $\mathbb{G}_m$. Hence we have :

$$\begin{array}{lcl} H^1(k,T_0) & = & H^1(K,T_0')\ , \text{ and for a place } v \text{ of } k \text{ we have} \\ H^1(k_v,T_0) & = & \prod\limits_{w|v} H^1(K_w,T_0'). \end{array}$$

So we have $\prod\limits_{v\in\Sigma} H^1(k_v,T_0) = \prod\limits_{w\in\Sigma_K} H^1(K_w,T_0')$ and $Ш(k,T_0) = Ш(K,T_0')$.

We can show as in II.1 that $Ш(K,T_0')$ is the group of elements of K which are norms from L_v locally everywhere, modulo the norms from L. But L/K is Galois with cyclic group H, and Hasse's theorem for norms then implies that $Ш(K,T_0') = 0$.

On the other hand, if we want to describe $Ш(k, T_0)$ with the help of a commutative diagram of cohomology groups, then we use the exact sequence of characters of (3) :

$$0 \to X(T_K) \to X(T_L) \to X(T_0) \to 0$$

from which we deduce :

$$\begin{array}{ccccccc} H^2(G, X(T_K)) & \xrightarrow{\phi} & H^2(G, X(T_L)) & \to & H^2(G, X(T_0)) & \to & H^3(G, X(T_K)) \\ \downarrow \alpha_0 & & \downarrow \beta_0 & & \downarrow \beta_2 & & \downarrow \alpha_3 \\ \prod_v H^2(G_v, X(T_K)) & \xrightarrow{\sigma} & \prod_v H^2(G_v, X(T_L)) & \to & \prod_v H^2(G_v, X(T_0)) & \to & \prod_v H^3(G_v, X(T_K)) \end{array}$$

The first part of this diagram is exactly the square $(\mathcal{C}_0)$.
We see that $\beta_0^{-1}(\text{Im } \sigma)/\text{Im } \phi = Ч_0(k, T')$ is a subgroup of $\ker \beta_2 = Ш(k, T_0)$, which we saw was trivial. We can conclude :

Proposition : $Ч_0(k, T') = 0$.

Study of $Ч_1(k, T')$

Recall that we have defined $Ш(k, K, M)$ in the beginning of II.

We denote by T_1 the k-torus, kernel of the morphism $\mathbb{G}_m \times T_M \to T_K$ defined by $(x, y) \mapsto x.N_{T_M/T_K} y$.

As we did previously, we can write the following commutative diagram whose first part is exactly $(\mathcal{C}_1)$:

$$\begin{array}{ccccccc} H^2(G, \mathbb{Z}[G/\Gamma_2]) & \xrightarrow{\theta} & H^2(G, \mathbb{Z}) & \to & H^2(G, X(T_1)) & \to & H^3(G, \mathbb{Z}[G/\Gamma_2]) \\ \downarrow \alpha_0 & & \downarrow \beta_1 & & \downarrow \beta_3 & & \downarrow \alpha_3 \\ \prod_{v\in\Sigma} H^2(G_v, \mathbb{Z}[G/\Gamma_2]) & \xrightarrow{\rho} & \prod_{v\in\Sigma} (H^2(G_v, \mathbb{Z}) & \to & \prod_{v\in\Sigma} H^2(G_v, X(T_1)) & \to & \prod_{v\in\Sigma} H^3(G_v, \mathbb{Z}[G/\Gamma_2]) \end{array}$$

$Ч(k, T_1) = \beta_1^{-1}(\text{Im } \rho)/\text{Im } \theta = Ч_1(k, T')$ is then a subgroup of $Ш(k, T_1) = \ker \beta_3$
This subgroup is the whole group as soon as α_3 is injective, which means :

Proposition : *If α_3 is injective,*

$$Ш(k, T') = Ч_1(k, T') = Ш(k, T_1) .$$

As above, we use Shapiro's lemma to describe the cohomology groups. We get :

$$\begin{aligned}\mathbb{Z}[G/\Gamma_2] &= \mathrm{Ind}_{\Gamma_2}^{G}\,\mathbb{Z} \qquad \text{seen as } G\text{-modules ;}\\ \mathbb{Z}[G/\Gamma_2] &= \bigoplus_{i=1}^{r_v} \mathrm{Ind}_{\Gamma_{2,i}^v}^{G_v}\,\mathbb{Z} \quad \text{seen as } G_v\text{-modules.}\end{aligned}$$

And the commutative diagram needed to describe $Ч_1$ can be written (after the same remarks as in the Galois case) :

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_2,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\theta} & \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \\ \downarrow \alpha_0 & & \downarrow \beta_1 \\ \prod_{v\in\Omega}\big(\bigoplus_{i=1}^{r_v} \mathrm{Hom}((\Gamma_{2,i}^v,\mathbb{Q}/\mathbb{Z})\,)\big) & \xrightarrow{\rho} & \prod_{v\in\Omega} \mathrm{Hom}(G_v,\mathbb{Q}/\mathbb{Z}) \end{array}$$

The dual diagram is :

$$\begin{array}{ccc} \Gamma_2^{ab} & \xleftarrow{\mu_1} & G^{ab} \\ \uparrow \gamma_1 & & \uparrow \delta_1 \\ \prod_{v\in\Omega}\big(\bigoplus_{i=1}^{r_v} (\Gamma_{2,i}^v)^{ab}\,\big) & \xleftarrow{\eta_1} & \prod_{v\in\Omega} G_v^{ab} \end{array}$$

These morphisms are again defined via transfers, injections and compositions of conjugations and injections.

We get $Ч_1(k,T') \simeq \ker \mu_1/\delta_1(\ker \eta_1)$.

Computations are more difficult that in the case when M/K is quadratic, especially when Γ_2 is not abelian. The simplest cases are once again those where Γ_2 is cyclic, and we then get a whole obstruction to the Hasse principle.

II.5 Use of the cyclic subgroups of G

If v is a place of k unramified in M then G_v is a cyclic subgroup of G . Conversely, a cyclic subgroup of G is of the form G_v for infinitely many places v (Frobenius-Tchebotarev). This proves that :

$$Ш(k,T') \subset Ш_c(k,T) = \ker[\, H^2(G,X(T')) \longrightarrow \prod_{C\in\mathcal{C}(G)} (H^2(C,X(T'))\,]$$

where $\mathcal{C}(G)$ is the set of cyclic subgroups of G.

This group $Ш_c(k,T')$ no longer depends on the extension L/k but only on the group G, and it turns the former arithmetic problem into an algebraic problem.

The group $Ш_c(k,T')$ can be computed exactly as $Ш(k,T')$; one just has to replace in all the results the products over the places of k by products over $\mathcal{C}$.

Since $Ш(k,T') \subset Ш_c(k,T')$, the triviality of $Ш_c(k,T')$ implies the triviality of $Ш(k,T')$. More precisely, if M/k is ramified then there exits a finite extension k'/k, linearly independent of M and such that Mk'/k' becomes unramified but with the same Galois group G . Then $Ш_c(k,T') = Ш_c(k',T') = Ш(k',T')$.

Searching for a counter-example to the Hasse principle for similarities of bilinear forms is then equivalent to searching for an extension $L/K/k$ such that $Ш_c(k,T') \neq 0$.

Remark : If G itself is cyclic, $Ш$ and $Ш_c$ are of course trivial.

II.6 Some computations in the Galois case

All extensions L/k considered here are Galois.

Recall that the expression of the transfer from G to H is the following (cf [Se1, prop. 7 p 129]) : let θ be a section from $H\backslash G$ to G . Let $s \in G$ and $t \in H\backslash G$. Let $x_{t,s}$ be defined by $\theta(t).s = x_{t,s}\theta(ts)$; then the transfer $ver_H^G : G^{ab} \to H^{ab}$ is defined by $s \mapsto \prod_t x_{t,s}$ modulo the commutators.

In particular, we have $ver_G^G = Id$.

We use this description to compute $Ш(k,K,L)$ in some cases of small degree.

a) *For $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*

Let $G = \{1, a, b, ab\}$, and let $H =< a >$, $H' =< b >$, $H'' =< ab >$ be the three subgroups of G.

Then θ : $\begin{array}{ccc} G/H & \to & G \\ 1 = \overline{a} & \mapsto & 1 \\ \overline{b} = \overline{ab} & \mapsto & b \end{array}$ is a homomorphism of commutative groups .

$ver_H^G(\overline{s}) = x_{1,\overline{s}} \,.\, x_{\overline{b},\overline{s}} = s.\theta(\overline{s})^{-1}.bs.\theta(\overline{bs})^{-1} = b.\theta(\overline{b})^{-1} = 1.$

We obtain $\ker(\mu : G^{ab} \to H) = G^{ab}$.

For $C = H'$ (or H''), $G = C.1.H$ and $H_1^C = H \bigcap H' = 1.$;

Hence $\ker \eta = H' \times H''$ and $\delta(\ker \eta) = G$

Conclusion : $Ш(k,K,L) = 1$

b) *For $G = H \times G'$ with G' abelian*

In this case $\theta : G/H \to G$ is again a group morphism.

$ver_H^G(s) = \prod_{t \in G'} \theta(\overline{t}).\, s \,.\, \theta(\overline{st})^{-1} = \prod_{t \in G'} s \,.\theta(\overline{s})^{-1}.\, t \,.\, \theta(\overline{t})^{-1} = \prod_{t \in G'} s \,.\theta(\overline{s})^{-1} = (s \,.\theta(\overline{s})^{-1})^{\sharp G'}$

If $s = h.t$, $h \in H$, $t \in G'$, $ver_H^G(s) = h^{-\sharp G'}$

We deduce that ker $(ver_H^G) = G$ if $\sharp G'$ is even and $= G'$ otherwise.

• If $\sharp G'$ is even :
If C is a cyclic subgroup of G', then $C \bigcap H = 1$; so $C \subset \ker \eta$.
Let h' be an element of G' of order two ; let h be the nontrivial element of H ; then hh' is again an element of order two of of G and $< hh' > \bigcap H = 1$ which implies that $< hh' > \subset \ker \eta$, and since $< h' > \subset \ker \eta$, we get $h \in \delta(\ker \eta)$. Hence $\delta(\ker \eta) = H \times G' = G$ and $Ш(k, K, L) = 1$

• If $\sharp G'$ is odd :
For any cyclic subgroup C of G' , $C \bigcap H = 1$, so $ker\ \eta$ contains all cyclic subgroups of G', and its image by δ contains G'.
Hence $Ш(k, K, L) = 1$

c) *For $G = S_3$*

Let write $G = \{1, s, s^2, t, ts, ts^2\}$, where t is of order two, s of order three, $tst = s^{-1}$ and $H =< t >$.

The transfer from $C =< s >$ to H is trivial because it is a homomorphism from a group of order three to a group of order two.
If $C =< ts >$, then $C \backslash G / H = \{1, s\}$ and $H_1^C = 1$, $H_s^C =< ts^2 > \bigcap < ts >= 1$ so $C \subset \ker \eta$.
It follows that $\ker \eta \supset < s > \times < ts >$ and since s and ts span G, $\delta(\ker \eta) = G$.
Conclusion : $Ш(k, K, L) = 1$.

d) *For the quaternion group $I\!H_8$*

$G =< t, s >$ with $s^2 = t^2$, $s^4 = 1$, $tst^{-1} = s^{-1}$.
The only subgroup of order two $H =< s^2 >=< t^2 >$ in G is normal, so :
$G^{ab} = G/H =< \overline{s} > \times < \overline{t} > \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$$\begin{array}{rccc} \theta\ : & G/H & \to & G \\ & \overline{s}^2 = \overline{t}^2 = 1 & \mapsto & 1 \\ & \overline{s}^3 = \overline{s} & \mapsto & s \\ & \overline{t}^3 = \overline{t} & \mapsto & t \\ & \overline{ts} = \overline{st} & \mapsto & st \end{array} \quad \text{can be defined by :}$$

$$\left\{ \begin{array}{lcll} x_{\overline{t},s} & = & \theta(\overline{t}).s.\theta(\overline{ts})^{-1} & = & ts(ts)^{-1} = 1 \\ x_{\overline{s},s} & = & \theta(\overline{s}).s.\theta(\overline{ss})^{-1} & = & 1 \\ x_{\overline{ts},s} & = & \theta(\overline{ts}).s.\theta(\overline{tss})^{-1} & = & stst^{-1} = ss^{-1} = 1 \\ x_{1,s} & = & \theta(1).s.\theta(\overline{s})^{-1} & = & 1 \end{array} \right.$$

We get $ver_H^G(\overline{s}) = 1$. In the same manner $ver_H^G(\overline{t}) = 1$, so the transfer from G_{ab} to H is trivial.

If C is a cyclic subgroup of G
$\star$ if $C = H$ then the transfer is the identity ;
$\star$ if C is cyclic of order four, then $C \bigcap H = H$.
We need to compute the transfer from $C = \mathbb{Z}/4\mathbb{Z} =< s >$ to $H = \mathbb{Z}/2\mathbb{Z} =< s^2 >$.
The corresponding set of representatives θ is obtained by the morphism of groups $C/H \to C$ defined by $\theta(1) = 1$ and $\theta(\overline{s}) = s$.

We have $ver_H^C(s) = \theta(\overline{s}).s.\theta(\overline{s}^2).\theta(1).s.\theta(\overline{s})^{-1} = s^2$.

Hence $\ker(\, ver_H^C\,) = H$

Conclusion : $Ш_c(k, K, L) = G/H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not trivial.

e) *For the dihedral group $G = \mathbb{D}_8$ and H normal*

$G =< t, s >$ with $t^2 = 1$, $s^4 = 1$, $tst^{-1} = s^{-1}$.
The normal subgroups of G are $< s >$ and $< s^2 >$, so $H =< s^2 >$ and :
$G^{ab} = G/ < s^2 > = < \overline{t} > \times < \overline{s} > \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

The map θ has exactly the same description as for $G = \mathbb{H}_8$.
We again get $ver_H^G(\overline{s}) = 1$, but we have to compute $ver_H^G(\overline{t})$:

$$\begin{cases} x_{\overline{t},t} &= \theta(\overline{t}).t.\theta(\overline{t^2})^{-1} &= t^2 = 1 \\ x_{\overline{s},t} &= \theta(\overline{s}).t.\theta(\overline{st})^{-1} &= st.(st)^{-1} = 1 \\ x_{\overline{st},t} &= \theta(\overline{st}).t.\theta(\overline{stt})^{-1} &= stts^{-1} = 1 \\ x_{1,t} &= \theta(1).t.\theta(\overline{t})^{-1} &= 1 \end{cases}$$

Therefore the transfer from G^{ab} to H is trivial.

If C is a cyclic subgroup of G
$\star$ if $C = H$ then the tranfer is the identity ;
$\star$ if $C =< t >$ (or an other subgroup of order two different from H) :
$C \bigcap H = 1$ and H is normal so $C \subset \ker \eta$
$\star$ if $C =< s >$ we already computed that $\ker ver_H^C = H$

Conclusion : $\ker \eta$ is the product of the subgroups of order two of G and we get $Ш(k, K, L) = 1$.

III Construction of a counter-example

The following construction is based on an idea of J-P. Serre [Se3] . In the first paragraph, we state the results concerning a counter-example to the problem of norms, and we prove these results in the next three paragraphs. We then give a counter-example to the problem of bilinear forms in the fifth paragraph.

As suggested by the previous results, we use a Galois extension of $\mathbb{Q}$ of Galois group $\mathbb{H}_8$, the group of quaternions of order 8, such that the decomposition groups are all cyclic.

Such an extension exists ; we use the example produced by Martinet in [Ma]. We then denote from now on :

$k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{5}, \sqrt{41})$ et $L = K(\sqrt{M})$ with $M = \frac{5+\sqrt{5}}{2}.\frac{41+\sqrt{41}\sqrt{5}}{2}$.

III.1 Local-global principle for norms

The aim of this section is to prove :

Proposition : *There is an element a in K which can be written $a = \lambda_v N_{L_v/K_v}(z_v)$, $\lambda_v \in k_v^*$ and $z_v \in L_v^*$ for any place v in k but is not of the form $\lambda N_{L/K}(z)$, $\lambda \in k^*$, $z \in L^*$.*

In order to produce a counter-example for the Hasse principle for similarities of bilinear forms, we need the additional property :

Lemma 1 *There is a primitive element α in L/k with a "symmetric" irreducible polynomial.*

The proof of the proposition is based on the following two lemmas :

Lemma 2 : *If $\lambda_v N_{L_v/K_v}(z_v) = 1$, $\lambda_v \in k_v^*$, $z_v \in L_v^*$, then $(\lambda_v, 5)_v = 1$* (cf Serre [Se3]).

Lemma3 : *There is an element a in K such that $(a, M)_{\mathfrak{p}_3} = (a, M)_{\mathfrak{q}_3} = -1$ and $(a, M)_w = 1$ everywhere else, where $\mathfrak{p}_3$ and $\mathfrak{q}_3$ are the two ideals over $< 3 >$ in K, and $(x, y)_w$ is the quaternion algebra over K_w associated with x and y.*

An element a that realizes lemma 3 also realizes the proposition : it has the right form over each K_v and the fact that it does not have the right form over K is a consequence of lemma 2.

We prove lemma 3 by taking the element $a = 3.\frac{1+\sqrt{5}}{2}$.

III.2 Proof of Lemma 1

We see that $\sqrt{M}$ is a primitive element of $L/\mathbb{Q}$. Now, a primitive element $\alpha \in L \setminus K$ has a symmetric irreducible polynomial over $\mathbb{Q}$ if and only if α^{-1} is a conjugate of α over K (in which case $K = \mathbb{Q}[\alpha + \alpha^{-1}]$) .

We look for α of the form $x + y\sqrt{M}$, $y \neq 0$, $x, y \in K$. Its irreducible polynomial over K is $P_K(X) = X^2 + aX + 1$ if and only if $(x + y\sqrt{M})^2 + a(x + y\sqrt{M}) + 1 = 0$.

This is equivalent to

$$\begin{cases} 2xy + ay = 0 \\ x^2 + My^2 + ax + 1 = 0 \end{cases} \quad \text{and to} \quad \begin{cases} 2x = -a \\ My^2 = \frac{a^2}{4} - 1 \end{cases}$$

Let $b = \frac{M+1}{2}$ and $2c = \frac{M-1}{2}$;
then $M = b^2 - 4c^2$ and $M(\frac{1}{2c})^2 = \frac{1}{4}(\frac{b}{c})^2 - 1$, which implies that $\alpha = \frac{M+1}{M-1} + \frac{2\sqrt{M}}{M-1}$ has the desired property.

Its irreducible polynomial over K is $P_K(X) = X^2 + 2\frac{M+1}{M-1}X + 1$.

The irreducible polynomial of M over $\mathbb{Q}$ is :

$P_M(X) = X^4 - 5 \cdot 41\, X^3 + 2^2 \cdot 5 \cdot 17 \cdot 41\, X^2 - 3^2 \cdot 5^2 \cdot 41^2\, X + 3^4 \cdot 5^2 \cdot 41^2$

And by replacing M by the expression $M = (\alpha - 1)^2/(\alpha + 1)^2$, in $P_M(M) = 0$, we obtain the irreducible polynomial of α over $\mathbb{Q}$:

$$P = \frac{1}{189971}(189971X^8 + 1607507X^7 + 5858953X^6 + 12008589X^5 + 15134360X^4$$

$$+12008589X^3 + 5858953X^2 + 1607507X + 189971)$$

III.3 Proof of the proposition assuming lemmas 2 and 3

Let $k_1 = \mathbb{Q}(\sqrt{5})$, $k_2 = (\sqrt{41})$ and $k_3 = (\sqrt{5.41})$ be the three quadratic subfields of $K/\mathbb{Q}$.

The prime ideal $< 3 >$ of $\mathbb{Q}$ is inert in k_1 (because $\left(\frac{3}{5}\right) = -1$) and the prime ideal spanned by 3 in k_1 splits in K/k_1 into $\mathfrak{p}_3 =< 3, \sqrt{5} + \sqrt{41} >$ and $\mathfrak{q}_3 =< 3, \sqrt{5} - \sqrt{41} >$
($< x_1, ...x_n >$ denotes the ideal spanned by the x_i's).

The completion of K at the place $\mathfrak{p}_3$ is $K_{\mathfrak{p}_3} \simeq \mathbb{Q}_3(\sqrt{5})$; here the uniformizer is 3 , and $\sqrt{5} + \sqrt{41} = 3^2 x$ with x an integer (because $\mathfrak{p}_3^2 =< \frac{\sqrt{5}+\sqrt{41}}{2} >$).

So $\sqrt{41} = 9x - \sqrt{5}$; $9x^2 - 2x\sqrt{5} - 4 = 0$ and $2x\sqrt{5} \equiv -4 (\text{mod } 3)$
$x \equiv -\sqrt{5} \equiv (1 + \sqrt{5})^2 (\text{mod } 3)$; x is a square in $K_{\mathfrak{p}_3}$.

It follows that $M = (\frac{1}{2})^2(5 + \sqrt{5})(\sqrt{41})(\sqrt{5} + \sqrt{41}) = (\frac{9x}{4})(5 + \sqrt{5})(\sqrt{41})$ with $(\frac{9x}{4})$ a square and $(5 + \sqrt{5})(\sqrt{41}) \equiv 1 + \sqrt{5} (\text{mod } 3)$ which is not a square in the residue field $\mathbb{F}_3(\sqrt{5})$ of $K_{\mathfrak{p}_3}$.

We deduce that M is a non trivial unit in $K^*_{\mathfrak{p}_3}/K^{*\,2}_{\mathfrak{p}_3}$.

Now do the same in the completion $K_{\mathfrak{q}_3}$ of K at the place $\mathfrak{q}_3$) ; $K_{\mathfrak{q}_3} \simeq \mathbb{Q}_3(\sqrt{5})$; here the uniformizer is 3 , and $\sqrt{41} = \sqrt{5} + 3y$; so $M \equiv -1 + \sqrt{5} (\text{mod } 3)$ which is not a square of $\mathbb{F}_3(\sqrt{5})$.

Hence M is once again a non trivial unit of $K^*_{\mathfrak{q}_3}/K^{*\,2}_{\mathfrak{q}_3}$.

Now suppose a satisfies lemma 3. Let us show that a also satisfies the proposition.

We first examine the places v of $\mathbb{Q}$ different from the prime ideal $< 3 >$. If $w|v$ in K , $(a, M)_w = 1$ so that a is a norm of $K_w(\sqrt{M})$.
But $K_v = K \otimes \mathbb{Q}_v = \prod_{w|v} K_w$ and $L_v = L \otimes \mathbb{Q}_v = \prod_{w'|v} K_{w'}$;
For every $w'|w|v$, $a \in N_{L_{w'}/K_w}(L_{w'})^*$ implies then $a \in N_{L_v/K_v}(L_v)^*$.

Now for the place $v =< 3 >$, $K_3 = K_{\mathfrak{p}_3} \times K_{\mathfrak{q}_3}$; $3 \in \mathbb{Q}_3$ has the property :
$(3, M)_{\mathfrak{p}_3} = -1 = (3, M)_{\mathfrak{q}_3}$. So $(3a, M)_{\mathfrak{p}_3} = (3a, M)_{\mathfrak{q}_3} = 1$. We conclude as in the previous case that $3a \in N_{L_3/K_3}(L_3)^*$.

So $a = 3N_{L_3/K_3}(z_3)$ with $3 \in \mathbb{Q}_3$ and $z_3 \in L_3^*$

We have proved thet a has the desired form for any place v.

If we had $a = \lambda NL/K(z)$ with $\lambda \in k^*$ and $z \in L^*$, then we would get $\prod_v (\lambda, 5)_v = 1$. By lemma 2, the symbol $\prod_v (\lambda_v, 5)_v$ is independent of the choice of the decompositions $a = \lambda_v N_{L/K}(z_v)$; but $\prod_v (\lambda_v, 5)_v = (3, 5)_3 = -1$ which implies that a does not have the desired global form.

III.4 Proof of lemma 2

If 5 is a square in k_v , this is clear.

Otherwise, v is such that $k_{1,v}$ is a field.

Thus $K_v = K_w \times K_{w'}$ and $L_v = L_w \times L_{w'}$ where w and w' are the places over v and $K_w = K_{w'} = k_{1,v}$.
$L_w \supset k_{1,v} \supset k_v$ is a cyclic extension of order 4.

We suppose that $z_w \in L_w^*$ is such that $\lambda_v^{-1} = N_{K_w/K_{0,w}}(z_w)$. We can use the following property :

Lemma 4 : *Let $E_4 \supset E_2 \supset E_1$ be a cyclic extension of degree 4 of local fields. The homomorphism induced by the inclusion $E_1^*/N_{E_2/E_1}E_2^* \longrightarrow E_2^*/N_{E_4/E_2}E_4^*$ is an isomorphism.*

Using the class field isomorphism, lemma 4 follows from the fact that if C is a cyclic group and C' a subgroup of C , then the transfert $C \longrightarrow C'$ is surjective.

We apply lemma 4 to $L_w \supset k_{1,v} \supset \mathbb{Q}_v$ and consider the element λ_v .
The image of this element in $E_v^*/N_{K_w/E_v}K_w^*$ is 1 , so its image in $Q_v^*/N_{E_v/Q_v}E_v$ is also 1, which means that $(\lambda_v, 5)_v = 1$.

III.5 Proof of lemma 3

We study the local conditions on a in order to have $(a, M)_{\mathfrak{p}_3} = (a, M)_{\mathfrak{q}_3} = -1$ and $(a, M)_w = 1$ everywhere else.

At places at infinity, M is totally positive, so it gives no condition on a.

At places over 3, we have seen that M is a non trivial unit of $K_{\mathfrak{p}_3}^*/K_{\mathfrak{p}_3}^{*\,2}$ (the same holds at $\mathfrak{q}_3$) ; so $(a, M)_{\mathfrak{p}_3 \, or \, \mathfrak{q}_3}$ is -1 if and only if a is not a unit of $K_{\mathfrak{p}_3}^*/K_{\mathfrak{p}_3}^{*\,2}$ (or $\mathfrak{q}_3$).

Let now look at the places dividing M. We have the equality $M = \frac{1+\sqrt{5}}{2}.\sqrt{5}.\sqrt{41}.\frac{\sqrt{5}+\sqrt{41}}{2}$.
Here $\frac{1+\sqrt{5}}{2}$ is a unit ;

$< \sqrt{5} >= \mathfrak{p}_5\mathfrak{q}_5$ where $\mathfrak{p}_5 =< \sqrt{5}, 1 + \sqrt{41} >$ and $\mathfrak{q}_5 =< \sqrt{5}, 1 - \sqrt{41} >$ are the two ideals lying over $< 5 >$ in K ;

$< \sqrt{41} >= \mathfrak{p}_{41}\mathfrak{q}_{41}$ where $\mathfrak{p}_{41} =< \sqrt{41}, 13 + \sqrt{5} >$ and $\mathfrak{q}_{41} =< \sqrt{41}, 13 - \sqrt{5} >$ are the two ideals lying over $< 41 >$ in K ;

and $< \frac{\sqrt{5}+\sqrt{41}}{2} >= \mathfrak{p}_3^2$.

We now have to look over 5 and 41 .

At $\mathfrak{p}_5$

The uniformizer is $\sqrt{5}$ and $\sqrt{41} \equiv -1 (\text{mod } \sqrt{5})$ is a square in $K^*_{\mathfrak{p}_5}$ because -1 is a square in the residue field $\mathbb{F}_5$.

$M = (\frac{1}{2})^2.\sqrt{41}.\sqrt{5}.(1+\sqrt{5}).(-1+\sqrt{5}+t\sqrt{5})$

We have $(1+\sqrt{5})(-1+\sqrt{5}+t\sqrt{5}) \equiv -1 (\text{mod } \sqrt{5})$ and hence it is a square in $K^*_{\mathfrak{p}_5}$.

We get $M = x^2\sqrt{5}$.

We know that $(\sqrt{5}, \sqrt{5})_{\mathfrak{p}_5} = (\sqrt{5}, -1)_{\mathfrak{p}_5} = 1$, because -1 is a square ; so

$$(a, M)_{\mathfrak{p}_5} = 1 \Longleftrightarrow (a, \sqrt{5})_{\mathfrak{p}_5} = 1 \Longleftrightarrow (a = 1 \text{ or } \sqrt{5} \text{ in } K^*_{\mathfrak{p}_5}/{K^*_{\mathfrak{p}_5}}^2)$$

At $\mathfrak{q}_5$

The uniformizer is again $\sqrt{5}$, and $\sqrt{41} \equiv 1 (\text{mod } \sqrt{5})$ is a square in $K^*_{\mathfrak{q}_5}$

$M = (\frac{1}{2})^2.\sqrt{41}.\sqrt{5}.(1+\sqrt{5}).(1+\sqrt{5}+t\sqrt{5})$

with $(1+\sqrt{5})(1+\sqrt{5}+t\sqrt{5}) \equiv 1 (\text{mod } \sqrt{5})$, so it is a square in $K^*_{\mathfrak{q}_5}$.

As in the previous case

$$(a, M)_{\mathfrak{q}_5} = 1 \Longleftrightarrow (a, \sqrt{5})_{\mathfrak{q}_5} = 1 \Longleftrightarrow (a = 1 \text{ or } \sqrt{5} \text{ in } K^*_{\mathfrak{q}_5}/{K^*_{\mathfrak{q}_5}}^2)$$

At $\mathfrak{p}_{41}$

The uniformizer is $\sqrt{41}$, and $\sqrt{5} \equiv -13 (\text{mod } \sqrt{41})$

$M = (\frac{1}{2})^2.\sqrt{41}.(5+\sqrt{5}).(\sqrt{5}+\sqrt{41})$

with $(5+\sqrt{5}).(\sqrt{5}+\sqrt{41}) \equiv 22 (\text{mod } \sqrt{41})$

And we can compute $\left(\dfrac{22}{41}\right) = -1$

So 22 is not a square in $\mathbb{F}_{41}$ and $M = y\sqrt{41}$ in $K^*_{\mathfrak{p}_{41}}/{K^*_{\mathfrak{p}_{41}}}^2$ with y a nonsquare unit.

That -1 is not a square in $\mathbb{F}_{41}$ implies $(\sqrt{41}, \sqrt{41})_{\mathfrak{p}_{41}} = (\sqrt{41}, -1)_{\mathfrak{p}_{41}} = 1$ and :

$$(a, M)_{\mathfrak{p}_{41}} = 1 \Longleftrightarrow (a, y\sqrt{41})_{\mathfrak{p}_{41}} = 1 \Longleftrightarrow (a = 1 \text{ or } y\sqrt{41} \text{ in } K^*_{\mathfrak{p}_{41}}/{K^*_{\mathfrak{p}_{41}}}^2)$$

At $\mathfrak{q}_{41}$

The uniformizer is $\sqrt{41}$, and $\sqrt{5} \equiv 13 (\text{mod } \sqrt{41})$

$(5+\sqrt{5}).(\sqrt{5}+\sqrt{41}) \equiv -12 (\text{mod } \sqrt{41})$

We know that $\left(\dfrac{-12}{41}\right) = -1$

We again have $M = y\sqrt{41}$ in $K^*_{\mathfrak{q}_{41}}/{K^*_{\mathfrak{q}_{41}}}^2$ with y a nonsquare unit and

$$(a,M)_{\mathfrak{q}_{41}}=1 \Longleftrightarrow (a,y\sqrt{41})_{\mathfrak{q}_{41}}=1 \Longleftrightarrow (a=1 \text{ or } y\sqrt{41} \text{ in } K^*_{\mathfrak{q}_{41}}/{K^*_{\mathfrak{q}_{41}}}^2)$$

At the remaining places, it is enough that a be a unit because M is one.

Claim : $a = 3.\frac{1+\sqrt{5}}{2}$ *has the desired properties.*

Proof :

$\star$ a is 3 times a unit in $K^*_{\mathfrak{p}_3}$ or $K^*_{\mathfrak{q}_3}$

$\star$ Neither 3 nor $\frac{1+\sqrt{5}}{2}$ are squares in $K^*_{\mathfrak{p}_5}$ and $K^*_{\mathfrak{q}_5}$ as $\left(\frac{3}{5}\right)=-1$ and $\frac{1+\sqrt{5}}{2}\equiv 3$ in $\mathbb{F}_5$, so a is a square.

$\star$ The same holds in $K^*_{\mathfrak{p}_{41}}$ since $\left(\frac{3}{41}\right)=-1$ and $\frac{1+\sqrt{5}}{2}\equiv -6(\text{mod } \sqrt{41})$ with $\left(\frac{-6}{41}\right)=-1$, so a is a square.

$\star$ It is also true in $K^*_{\mathfrak{q}_{41}}$ because $\left(\frac{3}{41}\right)=-1$ and $\frac{1+\sqrt{5}}{2}\equiv 7(\text{mod } \sqrt{41})$ with $\left(\frac{7}{41}\right)=-1$, so a is a square.

$\star$ Everywhere else, a is a unit.

This concludes the proof.

III.6 The counter-example for bilinear forms

We need to find two bilinear forms b and β that give respectively by I.2 the hermitian forms $< 1 >$ and $< a >$ over L . We look for the matrices (b_{ij}) and (β_{ij}) of these forms in the basis $(1, \alpha, \alpha^2, ..., \alpha^7)$ of L/k .

We find such matrices by using Riehm's definitions [W] of invariants of bilinear forms ; we easily see from the definition of these invariants that the two bilinear forms we find are similar over $\mathbb{Q}$ if and only if the two hermitian forms we began with are similar (and the same is true over $\mathbb{Q}_v$) . We can check that these two bilinear forms yield the algebra $R = L$ with the involution $^-$.

Hence they give the desired counter-example.

A survey of Riehm's method

There is a one-to-one correspondance between bilinear forms over k and $(-X)$-hermitian forms from $N \times N \to E$, where $A = k[X, 1/X]$ is endowed with the involution $X^J = 1/X$, F is its fraction field, $E = F/A$, and N runs through the finitely generated A-modules.

This correspondence is given as follows :

Let $b : V \times V \to k$ be a nondegenerate bilinear form ; B the corresponding linear map from V to its dual V^* ; N the A-module isomorphic to V over k and where the action of X is given by the endomorphism $B^{-1}B^t$; and let $N^* = \text{Hom }_A(N, E)$ be its dual.

Let $T : E \to k$ be the k-linear map which sends an element of E written under the form q/f, where f is a polynomial in X of degree $2d$ satisfying $f^J = f(1/X) = X^{-2}f$ and q is a polynomial of degree $\leq 2d$, to the constant term $T(q/f)$ of q .
We denote by $T_* : N^* \to V^*$ the k-linear map defined by $T_*(\phi) = T \circ \phi$. This map is bijective, and we associate to b the $(-X)$-hermitian form $C : N \to N^*$ defined by $B = TC$.

Such a $(-X)$-hermitian form is completely determined by the corresponding forms over the primaryfactors of N.

Moreover, if the irreducible polynomial P satisfies $P^J A = PA$ and J is non trivial over A/PA , and if we denote

$$N_P(r) = \{m \in N \mid P^r m = 0\}$$

$$V_P(r) = N_P(r)/[N_P(r-1) + PN_P(r+1)]\,,$$

then the form on N_P determines a family of $(-X)$-hermitian forms on $V_P(r)$ with values in $P^{-r}A/P^{-r+1}A$. So if we choose basis elements w_r of $P^{-r}A/P^{-r+1}A$ over $L = A/PA$, the coordinate forms are $(-Xx_r)$-hermitian forms with values in L, where x_r satisfies $w_r^J = x_r w_r$.

We change w_r to a new basis $y_r w_r$ with $y_r^J y_r^{-1} = (-Xx_r)^{-1}$, and the coordinate forms become hermitian forms : $V_P(r) \times V_P(r) \to L$.

Determination of b and β

We use Riehm's method for the hermitian forms $< 1 >$ and $< a >$ on the vector space $N = V_P(1) = L = A/PA$ where P is the irreducible polynomial of α .

We first must choose the right basis on $P^{-1}A/A$ over L.
$P^{-1} = (1/P)$ is a basis. We have $(1/P)^J = (1/P^J)$ with $P^J = X^{-8}P$.
$P' = X^{-4}P$ is a new basis satisfying $P'^J = X^4 P^J = X^{-4}P = P'$.
Then $x = 1$ and $y = X - 1$ satisfy $y^J = (-X)y$.

From now on, we use the basis $P'' = (X-1)X^4P^{-1}$ of $P^{-1}A/A$ over $L = A/PA$.

Now, the $(-X)$-hermitian forms h and h_a inducing $< 1 >$ and $< a >$ are defined by :

$$\begin{cases} h(Q \bmod P, S \bmod P) & = & \dfrac{QS^J(X-1)X^4}{P} & \bmod A \\ \\ h_a(Q \bmod P, S \bmod P) & = & \dfrac{UQS^J(X-1)X^4}{P} & \bmod A \end{cases}$$

where U is the polynomial defined modulo P such that $a = U(\alpha)$.

The bilinear forms b and β over L are defined by :

$$\begin{cases} b(Q(\alpha),S(\alpha)) &= T\left(\dfrac{QS^J(X-1)X^4}{P} \bmod A\right) \\ \\ \beta(Q(\alpha),S(\alpha)) &= T\left(\dfrac{UQS^J(X-1)X^4}{P} \bmod A\right) \end{cases}$$

Since P is of degree 8 and $P^J = X^{-8}P$, we need to find the constant terms of polynomials of the classes of $QS^J(X-1)X^4 \bmod P$ and $UQS^J(X-1)X^4 \bmod P$. We do that in the basis $(1, X, X^2, ...X^7)$ of A/PA over $\mathbb{Q}$ by using PARI system. We get :

$a = U(\alpha)$ with :

$$U(X) = \frac{94795529}{820}X^7 + \frac{2231284717}{2460}X^6 + \frac{614344038}{205}X^5 + \frac{16195852}{3}X^4 + \frac{70364504}{123}X^3 + \frac{8764206073}{2460}X^2 + \frac{989524041}{820}X + \frac{105449371}{615}$$

and the matrices of b and β in the basis $(1, \alpha, ..., \alpha^7)$ of L over k are :

$$\begin{pmatrix} 0 & 0 & 0 & -1 & b_5 & b_6 & b_7 & b_8 \\ 0 & 0 & 0 & 0 & -1 & b_5 & b_6 & b_7 \\ 0 & 0 & 0 & 0 & 0 & -1 & b_5 & b_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & b_5 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ b_5 & -1 & 0 & 0 & 0 & 0 & 0 & \\ b_6 & b_5 & -1 & 0 & 0 & 0 & 0 & 0 \\ b_7 & b_6 & b_5 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \beta_8 \\ \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 \\ \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 \\ \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 \\ \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 \\ \beta_6 & \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 \\ \beta_7 & \beta_6 & \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 \end{pmatrix}$$

with

$$\begin{cases} b_5 = 1797478/189971 \\ b_6 = -1776427306983/36088980841 \\ b_7 = 1288348045247800216/6855859779345611 \\ b_8 = -769037454741294091886545/1302414538142065067281 \end{cases}$$

$$\begin{cases} \beta_1 = 83397269/2460 \\ \beta_2 = -258550531/2460 \\ \beta_3 = 11208289/60 \\ \beta_4 = -706184071/2460 \\ \beta_5 = 194229083166919/467328660 \\ \beta_6 = -51909390322689686191/88778892868860 \\ \beta_7 = 13663658396321170597347199/16865415057190203060 \\ \beta_8 = -3565006060789271260797393731/320393976382948006551126 0 \end{cases}$$

References

[Ba] E. BAYER-FLUCKIGER : *Principe de Hasse pour les systèmes de formes quadratiques*. J.reine angew.Math **378** (1987) pp 55-59.

[Bo] A. BOREL : *Linear algebraic groups*. Graduate texts in math. **126**. Springer.

[Br] K.S. BROWN : *Cohomology of groups*. Graduate texts in math. **87**. Springer.

[C1] A. CORTELLA : *Le principe de Hasse pour les similitudes de formes quadratiques et hermitiennes*. Publi. Math. de Besançon - théorie des nombres 1993.

[C2] A. CORTELLA : *Un contre-exemple au principe de Hasse pour les similitudes de formes bilinéaires*. C.R. Acad. Sci. Paris, **t.317**, Série I, (1993) pp 707-710.

[Di] J. DIEUDONNE : *Sur les multiplicateurs de similitude*. Oeuvres, pp 408 - 418.

[DP1] YU.A. DRAKOKHRUST - V.P. PLATONOV : *On the Hasse principle for algebraic number fields*. Soviet.Math.Dokl. **31** (1985) pp 349-353.

[DP2] YU.A. DRAKOKHRUST - V.P. PLATONOV : *On the Hasse norm principle for primary extensions of algebraic number fields*. Soviet.Math.Dokl. **32** (1985) pp 789-792.

[DP3] YU.A. DRAKOKHRUST - V.P. PLATONOV : *The Hasse norm principle for algebraic number fields*. Math.USSR.Izvestiya **29** (1987) pp 299-322.

[G] G. GRAS : *Interprétation et calcul d'un groupe de défaut d'un principe de Hasse*. (with complementary results by A. CORTELLA). To appear in Math. Nachrichten.

[H] J.E. HUMPHREYS : *Linear algebraic groups*. Graduate texts in math. **21**. Springer.

[K] M. KNESER : *Lectures on Galois cohomology of classical groups*. (Bombay 1969).

[Ma] J. MARTINET : *Modules sur l'algèbre du groupe quaternionien*. Ann.Scient. E.N.S. **t.4** (1971) pp 399-408.

[Mi] J.S. MILNE : *Arithmetic duality theorems*. Perspectives in math. Academic Press Inc. (Orlando, Florida 1986).

[OE] J. OESTERLE : *Nombres de Tamagawa et groupes unipotents en car. p.* Invent. math. **78** (1984) pp 13-88.

[OM] O.T. O'MEARA : *Introduction to quadratic forms.* Grundlehren der Math. Wissenschaften **117** (1963) Springer.

[O] T. ONO : *Arithmetic of orthogonal groups* J.Math.Soc.Japan **7** (1955) pp 79-91.

[PR] V.P. PLATONOV- A.S. RAPINCHUCK : *Algebraic groups and number theory.* Moscow Nakaua Main Editorial Board for Physical and Math. Literature (1990) ; english version in Academic press 1993.

[Ri] C. RIEHM : *The equivalence of bilinear forms.* J.Algebra **31** (1974) pp 45-66.

[Ro] M. ROSENLICHT : *Some basic theorems on algebraic groups.* Amer. J. Math. **78** (1956) pp 401-443.

[Sa] J-J. SANSUC : *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres.* J.reine.angew.Math. **327** (1981) pp 12-80.

[Sch] W. SCHARLAU : *Quadratic and hermitian forms.* Grundlehren der Math. Wissenschaften **270** (1985).

[Se1] J-P. SERRE : *Corps locaux.* Hermann.(Paris 1962).

[Se2] J-P. SERRE : *Cohomologie Galoisienne.* Lecture Notes Math. **5**. Springer.

[Se3] J-P. SERRE : Letters to E.Bayer (February 1993).

[T] J. TATE : *The cohomology groups of tori in finite Galois extensions of number fields.* Nagoya Math. J.**27** (1966) pp 709-719.

[W] W.C. WATERHOUSE : *A non symmetric Hasse-Minkovski theorem.* Amer.J.Math. **99** (1977) pp 755-759.

Anne Cortella
Laboratoire de mathématiques
URA 741
Université de Franche-Comté
16 route de Gray
F- 25030 Besançon cedex
cortella@math.univ-fcomte.fr