

HASSE PRINCIPLE FOR  $G$ -QUADRATIC FORMSEVA BAYER–FLUCKIGER, NIVEDITA BHASKHAR,  
AND RAMAN PARIMALA

Received: August 19, 2012

Revised: February 14, 2013

Communicated by Ulf Rehmann

ABSTRACT.

INTRODUCTION.

Let  $k$  be a global field of characteristic  $\neq 2$ . The classical Hasse–Minkowski theorem states that if two quadratic forms become isomorphic over all the completions of  $k$ , then they are isomorphic over  $k$  as well. It is natural to ask whether this is true for  $G$ -quadratic forms, where  $G$  is a finite group. In the case of number fields the Hasse principle for  $G$ -quadratic forms does not hold in general, as shown by J. Morales [M 86]. The aim of the present paper is to study this question when  $k$  is a global field of positive characteristic. We give a sufficient criterion for the Hasse principle to hold (see th. 2.1.), and also give counter-examples. These counter-examples are of a different nature than those for number fields : indeed, if  $k$  is a global field of positive characteristic, then the Hasse principle does hold for  $G$ -quadratic forms on projective  $k[G]$ -modules (see cor. 2.3), and in particular if  $k[G]$  is semi-simple, then the Hasse principle is true for  $G$ -quadratic forms, contrarily to what happens in the case of number fields. On the other hand, there are counter-examples in the non semi-simple case, as shown in §3. Note that the Hasse principle holds in all generality for  $G$ -trace forms (cf. [BPS 13]).

The third named author is partially supported by National Science Foundation grant DMS-1001872.

## §1. DEFINITIONS, NOTATION AND BASIC FACTS

Let  $k$  be a field of characteristic  $\neq 2$ . All modules are supposed to be left modules.

*G*-quadratic spaces

Let  $G$  be a finite group, and let  $k[G]$  be the associated group ring. A  $G$ -quadratic space is a pair  $(V, q)$ , where  $V$  is a  $k[G]$ -module that is a finite dimensional  $k$ -vector space, and  $q : V \times V \rightarrow k$  is a non-degenerate symmetric bilinear form such that

$$q(gx, gy) = q(x, y)$$

for all  $x, y \in V$  and all  $g \in G$ .

Two  $G$ -quadratic spaces  $(V, q)$  and  $(V', q')$  are *isomorphic* if there exists an isomorphism of  $k[G]$ -modules  $f : V \rightarrow V'$  such that  $q'(f(x), f(y)) = q(x, y)$  for all  $x, y \in V$ . If this is the case, we write  $(V, q) \simeq_G (V', q')$ , or simply  $q \simeq_G q'$ .

*Hermitian forms*

Let  $R$  be a ring endowed with an involution  $r \mapsto \bar{r}$ . For any  $R$ -module  $M$ , we denote by  $M^*$  its dual  $\text{Hom}_R(M, R)$ . Then  $M^*$  has an  $R$ -module structure given by  $(rf)(x) = f(x)\bar{r}$  for all  $r \in R$ ,  $x \in M$  and  $f \in M^*$ . If  $M$  and  $N$  are two  $R$ -modules and if  $f : M \rightarrow N$  is a homomorphism of  $R$ -modules, then  $f$  induces a homomorphism  $f^* : N^* \rightarrow M^*$  defined by  $f^*(g) = gf$  for all  $g \in N^*$ , called the *adjoint* of  $f$ .

A *hermitian form* is a pair  $(M, h)$  where  $M$  is an  $R$ -module and  $h : M \times M \rightarrow R$  is biadditive, satisfying the following two conditions:

(1.1)  $h(rx, sy) = rh(x, y)\bar{s}$  and  $\overline{h(x, y)} = h(y, x)$  for all  $x, y \in M$  and all  $r, s \in R$ .

(1.2) The homomorphism  $h : M \rightarrow M^*$  given by  $y \mapsto h(\cdot, y)$  is an isomorphism.

Note that the existence of  $h$  implies that  $M$  is *self-dual*, i.e. isomorphic to its dual.

If  $G$  is a finite group, then the group algebra  $R = k[G]$  has a natural  $k$ -linear involution, characterized by the formula  $\bar{g} = g^{-1}$  for every  $g \in G$ . We have the following dictionary (see for instance [BPS 13, 2.1, Example])

- a)  $R$ -module  $M \iff k$ -module  $M$  with a  $k$ -linear action of  $G$ ;
- b)  $R$ -dual  $M^* \iff k$ -dual of  $M$ , with the contragredient (i.e. dual) action of  $G$ .
- c) hermitian space  $(M, h) \iff$  symmetric bilinear form on  $M$ , which is  $G$ -invariant and defines an isomorphism of  $M$  onto its  $k$ -dual.

Therefore a hermitian space over  $k[G]$  corresponds to a  $G$ -quadratic space, as defined above.

*Hermitian elements*

Let  $E$  be a ring with an involution  $\sigma : E \rightarrow E$  and put

$$E^0 = \{z \in E^\times \mid \sigma(z) = z\}.$$

If  $z \in E^0$ , the map  $h_z : E \times E \rightarrow E$  defined by  $h_z(x, y) = x.z.\sigma(y)$  is a hermitian space over  $E$ ; conversely, every hermitian space over  $E$  with underlying module  $E$  is isomorphic to  $h_z$  for some  $z \in E^0$ .

Define an equivalence relation on  $E^0$  by setting  $z \equiv z'$  if there exists  $e \in E^\times$  with  $z' = \sigma(e)ze$ ; this is equivalent to  $(E, h_z) \simeq (E, h_{z'})$ . Let  $H(E, \sigma)$  be the quotient of  $E^0$  by this equivalence relation. If  $z \in E^0$ , we denote by  $[z]$  its class in  $H(E, \sigma)$ .

#### *Classifying hermitian spaces via hermitian elements*

Let  $(M, h_0)$  be a hermitian space over  $R$ . Set  $E_M = \text{End}(M)$ . Let  $\tau : E_M \rightarrow E_M$  be the involution of  $E_M$  induced by  $h_0$ , i.e.

$$\tau(e) = h_0^{-1}e^*h_0, \quad \text{for } e \in E_M,$$

where  $e^*$  is the adjoint of  $e$ . If  $(M, h)$  is a hermitian space (with the same underlying module  $M$ ), we have  $\tau(h_0^{-1}h) = h_0^{-1}(h_0^{-1}h)^*h_0 = h_0^{-1}h^*(h_0^{-1})^*h_0 = h_0^{-1}h$ . Hence  $h_0^{-1}h$  is a hermitian element of  $(E_M, \tau)$ ; let  $[h_0^{-1}h]$  be its class in  $H(E_M, \tau)$ .

LEMMA 1.1. (see for instance [BPS 13, lemma 3.8.1]) *Sending a hermitian space  $(M, h)$  to the element  $[h_0^{-1}h]$  of  $H(E_M, \tau)$  induces a bijection between the set of isomorphism classes of hermitian spaces  $(M, h)$  and the set  $H(E_M, \tau)$ .*

#### *Components of algebras with involution*

Let  $A$  be a finite dimensional  $k$ -algebra, and let  $\iota : A \rightarrow A$  be a  $k$ -linear involution. Let  $R_A$  be the radical of  $A$ . Then  $A/R_A$  is a semi-simple  $k$ -algebra, hence we have a decomposition  $A/R_A = \prod_{i=1, \dots, r} M_{n_i}(D_i)$ , where  $D_1, \dots, D_r$  are division algebras. Let us denote by  $K_i$  the center of  $D_i$ , and let  $D_i^{\text{op}}$  be the opposite algebra of  $D_i$ .

Note that  $\iota(R_A) = R_A$ , hence  $\iota$  induces an involution  $\iota : A/R_A \rightarrow A/R_A$ . Therefore  $A/R_A$  decomposes into a product of involution invariant factors. These can be of two types : either an involution invariant matrix algebra  $M_{n_i}(D_i)$ , or a product  $M_{n_i}(D_i) \times M_{n_i}(D_i^{\text{op}})$ , with  $M_{n_i}(D_i)$  and  $M_{n_i}(D_i^{\text{op}})$  exchanged by the involution. We say that a factor is *unitary* if the restriction of the involution to its center is not the identity : in other words, either an involution invariant  $M_{n_i}(D_i)$  with  $\iota|_{K_i}$  not the identity, or a product  $M_{n_i}(D_i) \times M_{n_i}(D_i^{\text{op}})$ . Otherwise, the factor is said to be of the first kind. In this case, the component is of the form  $M_{n_i}(D_i)$  and the restriction of  $\iota$  to  $K_i$  is the identity. We say that the component is *orthogonal* if after base change to a separable closure  $\iota$  is given by the transposition, and *symplectic* otherwise. A component  $M_{n_i}(D_i)$  is said to be *split* if  $D_i$  is a commutative field.

#### *Completions*

If  $k$  is a global field and if  $v$  is a place of  $k$ , we denote by  $k_v$  the completion of  $k$  at  $v$ . For any  $k$ -algebra  $E$ , set  $E_v = E \otimes_k k_v$ . If  $K/k$  is a field extension of finite degree and if  $w$  is a place of  $K$  above  $v$ , then we use the notation  $w|v$ .

## §2. HASSE PRINCIPLE

In this section,  $k$  will be a global field of characteristic  $\neq 2$ . Let us denote by  $\Sigma_k$  the set of all places of  $k$ . The aim of this section is to give a sufficient criterion for the Hasse principle for  $G$ -quadratic forms to hold. All modules are left modules, and finite dimensional  $k$ -vector spaces.

**THEOREM 2.1.** *Let  $V$  be a  $k[G]$ -module, and let  $E = \text{End}(V)$ . Let  $R_E$  be the radical of  $E$ , and set  $\overline{E} = E/R_E$ . Suppose that all the orthogonal components of  $\overline{E}$  are split, and let  $(V, q), (V, q')$  be two  $G$ -forms. Then  $q \simeq_G q'$  over  $k$  if and only if  $q \simeq_G q'$  over all the completions of  $k$ .*

This is announced in [BP 13], and replaces th. 3.5 of [BP 11]. The proof of th. 2.1 relies on the following proposition

**PROPOSITION 2.2.** *Let  $E$  be a finite dimensional  $k$ -algebra endowed with a  $k$ -linear involution  $\sigma : E \rightarrow E$ . Let  $R_E$  be the radical of  $E$ , and set  $\overline{E} = E/R_E$ . Suppose that all the orthogonal components of  $\overline{E}$  are split. Then the canonical map  $H(E, \sigma) \rightarrow \prod_{v \in \Sigma_k} H(E_v, \sigma_v)$  is injective.*

**PROOF.** *The case of a simple algebra.* Suppose first that  $E$  is a simple  $k$ -algebra. Let  $K$  be the center of  $E$ , and let  $F$  be the fixed field of  $\sigma$  in  $K$ . Let  $\Sigma_F$  denote the set of all places of  $F$ . For all  $v \in \Sigma_k$ , set  $E_v = E \otimes_k k_v$ , and note that  $E_v = \prod_{w|v} E_w$ , therefore  $\prod_{v \in \Sigma_k} H(E_v, \sigma_v) = \prod_{w \in \Sigma_F} H(E_w, \sigma_w)$ . By definition,  $H(E, \sigma)$  is the set of isomorphism classes of one dimensional hermitian forms over  $E$ . Moreover, if  $\sigma$  is orthogonal, then the hypothesis implies that  $E$  is split, in other words we have  $E \simeq M_n(F)$ . Therefore the conditions of [R 11, th. 3.3.1] are fulfilled, hence the Hasse principle holds for hermitian forms over  $E$  with respect to  $\sigma$ . This implies that the canonical map  $H(E, \sigma) \rightarrow \prod_{v \in \Sigma_k} H(E_v, \sigma_v)$  is injective.

*The case of a semi-simple algebra.* Suppose now that  $E$  is semi-simple. Then

$$E \simeq E_1 \times \dots \times E_r \times A \times A^{\text{op}},$$

where  $E_1, \dots, E_r$  are simple algebras which are stable under the involution  $\sigma$ , and where the restriction of  $\sigma$  to  $A \times A^{\text{op}}$  exchanges the two factors. Applying [BPS 13, lemmas 3.7.1 and 3.7.2] we are reduced to the case where  $E$  is a simple algebra, and we already know that the result is true in this case.

*General case.* We have  $\overline{E} = E/R_E$ . Then  $\overline{E}$  is semi-simple, and  $\sigma$  induces a  $k$ -linear involution  $\overline{\sigma} : \overline{E} \rightarrow \overline{E}$ . We have the following commutative diagram

$$\begin{array}{ccc} H(E, \sigma) & \xrightarrow{f} & \prod_{v \in \Sigma_k} H(E_v, \sigma) \\ \downarrow & & \downarrow \\ H(\overline{E}, \overline{\sigma}) & \xrightarrow{\overline{f}} & \prod_{v \in \Sigma_k} H(\overline{E}_v, \overline{\sigma}), \end{array}$$

where the vertical maps are induced by the projection  $E \rightarrow \overline{E}$ . By [BPS 13, lemma 3.7.3], these maps are bijective. As  $\overline{E}$  is semi-simple, the map  $\overline{f}$  is injective, hence  $f$  is also injective. This concludes the proof.

PROOF OF TH. 2.1. It is clear that if  $q \simeq_G q'$  over  $k$ , then  $q \simeq_G q'$  over all the completions of  $k$ . Let us prove the converse. Let  $(V, h)$  be the  $k[G]$ -hermitian space corresponding to  $(V, q)$ , and let  $\sigma : E \rightarrow E$  be the involution induced by  $(V, h)$  as in §1. Let  $(V, h')$  be the  $k[G]$ -hermitian space corresponding to  $(V, q')$ , and set  $u = h^{-1}h'$ . Then  $u \in E^0$ , and by lemma 1.1. the element  $[u] \in H(E, \sigma)$  determines the isomorphism class of  $(V, q')$ ; in other words, we have  $q \simeq_G q'$  if and only if  $[u] = [1]$  in  $H(E, \sigma)$ . Hence the theorem is a consequence of proposition 2.2.

COROLLARY 2.3 *Suppose that  $\text{char}(k) = p > 0$ , and let  $V$  be a projective  $k[G]$ -module.. Let  $(V, q), (V, q')$  be two  $G$ -forms. Then  $q \simeq_G q'$  over  $k$  if and only if  $q \simeq_G q'$  over all the completions of  $k$ .*

PROOF. Since  $V$  is projective, there exists a  $k[G]$ -module  $W$  and  $n \in \mathbb{N}$  such that  $V \oplus W \simeq k[G]^n$ . The endomorphism ring of  $k[G]^n$  is  $M_n(k[G])$ , and as  $\text{char}(k) = p > 0$ , we have  $k[G] = F_p[G] \otimes_{F_p} k$ . Hence  $M_n(k[G])$  is isomorphic to  $M_n(F_p[G]) \otimes_{F_p} k$ . Let  $E = \text{End}(V)$ , let  $R_E$  be the radical of  $E$ , and let  $\overline{E} = E/R_E$ . Let us show that all the components of  $\overline{E}$  are split. Let  $e$  be the idempotent endomorphism of  $V \oplus W$  which is the identity of  $V$ . Set  $\Lambda = \text{End}(V \oplus W)$  and let  $R_\Lambda$  be the radical of  $\Lambda$ . Then  $e\Lambda e = \overline{E}$  and  $eR_\Lambda e = R_E$ . Set  $\overline{\Lambda} = \Lambda/R_\Lambda$ , and let  $\overline{e}$  be the image of  $e$  in  $\overline{\Lambda}$ . Set  $\overline{k[G]} = k[G]/\text{rad}(k[G])$ . Then we have  $\overline{E} \simeq \overline{e}\overline{\Lambda}\overline{e} \simeq \overline{e}M_n(\overline{k[G]})\overline{e}$ . This implies that  $\overline{E}$  is a component of the semi-simple algebra  $M_n(\overline{k[G]})$ . Let us show that all the components of  $M_n(\overline{k[G]})$  are split. As  $F_p$  is a finite field,  $F_p[G]/(\text{rad}(F_p[G]))$  is a product of matrix algebras over finite fields. Moreover, for any finite field  $F$  of characteristic  $p$ , the tensor product  $F \otimes_{F_p} k$  is a product of fields. This shows that  $(F_p[G]/(\text{rad}(F_p[G])) \otimes_{F_p} k$  is a product of matrix algebras over finite extensions of  $k$ ; in particular, it is semi-simple. The natural isomorphism  $F_p[G] \otimes_{F_p} k \rightarrow k[G]$  induces an isomorphism  $[F_p[G]/(\text{rad}(F_p[G])) \otimes_{F_p} k \rightarrow k[G]/(\text{rad}(F_p[G]).k[G])$ . Therefore  $\text{rad}(F_p[G].k[G])$  is the radical of  $k[G]$ , and we have an isomorphism  $[F_p[G]/(\text{rad}(F_p[G])) \otimes_{F_p} k \rightarrow k[G]/(\text{rad}(k[G]))$ . Hence all the components of  $k[G]/(\text{rad}(k[G]))$  are split. This implies that all the components of  $\overline{E}$  are split as well. Therefore the corollary follows from th. 2.1.

The following corollary is well-known (see for instance [R 11, 3.3.1 (b)]).

COROLLARY 2.4 *Suppose that  $\text{char}(k) = p > 0$ , and that the order of  $G$  is prime to  $p$ . Then two  $G$ -quadratic forms are isomorphic over  $k$  if and only if they become isomorphic over all the completions of  $k$ .*

PROOF. This follows immediately from cor. 2.3.

### §3. COUNTER-EXAMPLES TO THE HASSE PRINCIPLE

Let  $k$  be a field of characteristic  $p > 0$ , let  $C_p$  be the cyclic group of order  $p$ , and let  $G = C_p \times C_p \times C_p$ . In this section we give counter-examples to the Hasse principle for  $G \times G$ -quadratic forms over  $k$  in the case where  $k$  is a global field. We start with some constructions that are valid for any field of positive characteristic.

#### 3.1 A CONSTRUCTION

Let  $D$  be a division algebra over  $k$ . It is well-known that there exist indecomposable  $k[G]$ -modules such that their endomorphism ring modulo the radical is isomorphic to  $D$ . We recall here such a construction, brought to our attention by R. Guralnick, in order to use it in 3.2 in the case of quaternion algebras.

The algebra  $D$  can be generated by two elements (see for instance [J 64, Chapter VII, §12, th. 3, p. 182]). Let us choose  $i, j \in D$  be two such elements. Let us denote by  $D^{\text{op}}$  the opposite algebra of  $D$ , and let  $d$  be the degree of  $D$ . Then we have  $D \otimes_k D^{\text{op}} \simeq M_{d^2}(k)$ . Let us choose an isomorphism  $f : D \otimes_k D^{\text{op}} \simeq M_{d^2}(k)$ , and set  $a_1 = f(1 \otimes 1) = 1$ ,  $a_2 = f(i \otimes 1)$  and  $a_3 = f(j \otimes 1)$ .

Let  $g_1, g_2, g_3 \in G$  be three elements of order  $p$  such that the set  $\{g_1, g_2, g_3\}$  generates  $G$  and let us define a representation  $G \rightarrow \text{GL}_{2d^2}(k)$  by sending  $g_m$  to the matrix

$$\begin{pmatrix} I & a_m \\ 0 & I \end{pmatrix}$$

for all  $m = 1, 2, 3$ . Note that this is well-defined because  $\text{char}(k) = p$ . This endows  $k^{2d^2}$  with a structure of  $k[G]$ -module. Let us denote by  $N$  this  $k[G]$ -module, and let  $E_N$  be its endomorphism ring. Then

$$E_N = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \mid x \in D^{\text{op}} \subset M_{d^2}(k), y \in M_{d^2}(k) \right\},$$

and its radical is

$$R_N = \left\{ \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \mid y \in M_{d^2}(k) \right\},$$

hence  $E_N/R_N \simeq D^{\text{op}}$ .

3.2. THE CASE OF A QUATERNION ALGEBRA

Let  $H$  be a quaternion algebra over  $k$ . Then by 3.1, we get a  $k[G]$ -module  $N = N_H$  with endomorphism ring  $E_N$  such that  $E_N/R_N \simeq H^{\text{op}}$ , where  $R_N$  is the radical of  $E_N$ . We now construct a  $G$ -quadratic form  $q$  over  $N$  in such a way that the involution it induces on  $E_N/R_N \simeq H^{\text{op}}$  is the canonical involution.

Let  $i, j \in H$  such that  $i^2, j^2 \in k^\times$  and that  $ij = -ji$ . Let  $\tau : H \rightarrow H$  be the orthogonal involution of  $H$  obtained by composing the canonical involution of  $H$  with  $\text{Int}(ij)$ . Let  $\sigma : H^{\text{op}} \rightarrow H^{\text{op}}$  be the canonical involution of  $H^{\text{op}}$ . Let us consider the tensor product of algebras with involution

$$(H, \tau) \otimes (H^{\text{op}}, \sigma) = (M_4(k), \rho).$$

Then  $\rho$  is a symplectic involution of  $M_4(k)$  satisfying  $\rho(a_m) = a_m$  for all  $m = 1, 2, 3$ , since  $\tau(i) = (ij)(-i)(ij)^{-1} = i$ ,  $\tau(j) = (ij)(-j)(ij)^{-1} = j$ . Let  $\alpha \in M_4(k)$  be a skew-symmetric matrix such that for all  $x \in M_4(k)$ , we have  $\rho(x) = \alpha^{-1}x^T\alpha$ , where  $x^T$  denotes the transpose of  $x$ . Set  $A = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$ .

Then  $A^T = A$ . Let  $q : N \times N \rightarrow k$  be the symmetric bilinear form defined by  $A$  :

$$q(v, w) = v^T A w$$

for all  $v, w \in N$ . Let  $\gamma : M_8(k) \rightarrow M_8(k)$  be the involution adjoint to  $q$ , that is

$$\gamma(X) = A^{-1}X^T A$$

for all  $X \in M_8(k)$ , i.e.  $q(fv, w) = q(v, \gamma(f)w)$  for all  $f \in M_8(k)$  and all  $v, w \in N$ . The involution  $\gamma$  restricts to an involution of  $E_N$ , as for all  $x, y \in M_4(k)$ , we have

$$\gamma \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} = \begin{pmatrix} \alpha^{-1}x^T\alpha & -\alpha^{-1}y^T\alpha \\ 0 & \alpha^{-1}x^T\alpha \end{pmatrix}.$$

It also sends  $R_N$  to itself, and induces an involution  $\bar{\gamma}$  on  $H^{\text{op}} \simeq E_N/R_N$  that coincides with the canonical involution of  $H^{\text{op}}$ .

We claim that  $q : N \times N \rightarrow k$  is a  $G$ -quadratic form. To check this, it suffices to show that  $q(g_m v, g_m w) = q(v, w)$  for all  $v, w \in N$  and for all  $m = 1, 2, 3$ . Since  $\rho(a_m) = a_m$  for all  $m = 1, 2, 3$ , we have

$$\gamma \begin{pmatrix} I & a_m \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & a_m \\ 0 & I \end{pmatrix}^{-1}$$

and hence

$$q(g_m v, g_m w) = q(v, \gamma(g_m)g_m w) = q(v, w)$$

for all  $m = 1, 2, 3$  and all  $v, w \in N$ . Thus  $q$  is a  $G$ -quadratic form, and by construction, the involution of  $E_N$  induced by  $q$  is the restriction of  $\gamma$  to  $E_N$ .

## 3.3. TWO QUATERNION ALGEBRAS

Let  $H_1$  and  $H_2$  be two quaternion algebras over  $k$ . By the construction of 3.2, we obtain two indecomposable  $k[G]$ -modules  $N_1$  and  $N_2$ . Set  $E_1 = E_{N_1}$  and  $E_2 = E_{N_2}$ . Let  $R_i$  be the radical of  $E_i$  for  $i = 1, 2$ , and set  $\overline{E}_i = E_i/R_i$ . We also obtain  $G$ -quadratic spaces  $q_i : N_i \times N_i \rightarrow k$  inducing involutions  $\gamma_i : E_i \rightarrow E_i$  such that the involutions  $\overline{\gamma}_i : \overline{E}_i \rightarrow \overline{E}_i$  coincide with the canonical involution of  $H_i^{\text{op}}$ , for all  $i = 1, 2$ .

Let us consider the tensor product  $(N, q) = (N_1, q_1) \otimes_k (N_2, q_2)$ . Then  $(N, q)$  is a  $G \times G$ -quadratic space. Set  $E = \text{End}_{k[G \times G]}(N_1 \otimes N_2)$ . Then  $E \simeq E_1 \otimes E_2$ . Let  $I$  be the ideal of  $E$  generated by  $R_1$  and  $R_2$ . Then there is a natural isomorphism  $f : E_1 \otimes E_2 \rightarrow E$  with  $f(I) = R_E$ , where  $R_E$  is the radical of  $E$ . Set  $\overline{E} = E/R_E$ . Then  $\overline{E} \simeq \overline{E}_1 \otimes \overline{E}_2 \simeq H_1^{\text{op}} \otimes H_2^{\text{op}}$ .

Set  $\gamma = \gamma_1 \otimes \gamma_2$ . Then  $\gamma : E \rightarrow E$  is the involution induced by the  $G \times G$ -quadratic space  $(N, q)$ . We obtain an involution  $\overline{\gamma} : \overline{E} \rightarrow \overline{E}$ , and  $\overline{\gamma} = \overline{\gamma}_1 \otimes \overline{\gamma}_2$ . Let us recall that  $\overline{E}_i = H_i^{\text{op}}$  for  $i = 1, 2$ , and that  $\overline{\gamma}_i$  is the canonical involution of  $H_i^{\text{op}}$ . Hence  $\overline{\gamma} : \overline{E} \rightarrow \overline{E}$  is an orthogonal involution.

## 3.4. A COUNTER-EXAMPLE TO THE HASSE PRINCIPLE

Suppose now that  $k$  is a global field of characteristic  $p$ , with  $p > 2$ , and suppose that  $H_i$  is ramified at exactly two places  $v_i, v'_i$  of  $k$ , such that  $v_1, v'_1, v_2, v'_2$  are all distinct. We have  $H_1^{\text{op}} \otimes H_2^{\text{op}} \simeq M_2(Q)$  where  $Q$  is a quaternion division algebra over  $k$ , and  $Q$  is ramified exactly at the places  $v_1, v'_1, v_2, v'_2$  of  $k$ . Recall that the involution  $\overline{\gamma} : M_2(Q) \rightarrow M_2(Q)$  is the tensor product of the canonical involutions of  $H_i^{\text{op}}$ . In particular,  $\overline{\gamma}$  is of orthogonal type. Note that at all  $v \in \Sigma_k$ , one of the algebras  $H_1^{\text{op}}$  or  $H_2^{\text{op}}$  is split. This implies that at all  $v \in \Sigma_k$ , the involution  $\overline{\gamma}$  is hyperbolic.

Let  $\delta : Q \rightarrow Q$  be an orthogonal involution of the division algebra  $Q$ . Then  $\overline{\gamma}$  is induced by some hermitian space  $h : Q^2 \times Q^2 \rightarrow Q$  with respect to the involution  $\delta$ . As for all  $v \in \Sigma_k$ , the involution  $\overline{\gamma}$  is hyperbolic at  $v$ , the hermitian form  $h$  is also hyperbolic at  $v$ . By lemma 1.1 the set of isomorphism classes of hermitian spaces on  $Q^2$  is in bijection with the set  $H(\overline{E}, \overline{\gamma})$ , the hermitian space  $(Q^2, h)$  corresponding to the element  $[1] \in H(\overline{E}, \overline{\gamma})$ .

Let  $(Q^2, h')$  be a hermitian space which becomes isomorphic to  $(Q^2, h)$  over  $Q_v$  for all  $v \in \Sigma_k$ , but is not isomorphic to  $(Q^2, h)$  over  $Q$  (this is possible by [Sch 85, 10.4.6]). Let  $u \in \overline{E}^0$  such that  $[u] \in H(\overline{E}, \overline{\gamma})$  corresponds to  $(Q^2, h')$  by the bijection of lemma 1.1. Then  $[u] \neq [1] \in H(\overline{E}, \overline{\gamma})$ , and the images of  $[u]$  and  $[1]$  coincide in  $\prod_{v \in \Sigma_k} H(\overline{E}_v, \overline{\gamma})$ .

Recall that  $H(E, \gamma)$  is in bijection with the isomorphism classes of  $(G \times G)$ -quadratic forms over  $N$ , the element  $[1] \in H(E, \gamma)$  corresponding to the isomorphism class of  $(N, q)$ . Let  $\pi : E \rightarrow \overline{E}$  be the projection, and let  $\tilde{u} \in E^0$  be

such that  $\pi(\tilde{u}) = u$  (cf. lemma 1.1). Let  $(N, q')$  be a  $(G \times G)$ -quadratic form corresponding to  $\tilde{u}$ . The diagram

$$\begin{array}{ccc} H(E, \gamma) & \xrightarrow{f} & \prod_{v \in \Sigma_k} H(E_v, \gamma) \\ \downarrow & & \downarrow \\ H(\overline{E}, \overline{\gamma}) & \xrightarrow{\overline{f}} & \prod_{v \in \Sigma_k} H(\overline{E}_v, \overline{\gamma}), \end{array}$$

is commutative, and the vertical maps are bijective by [BPS 13, lemma 3.7.3]. Hence  $(N, q)$  and  $(N, q')$  are become isomorphic over all the completions of  $k$ , but are not isomorphic over  $k$ .

## BIBLIOGRAPHY

- [BP 11] E. Bayer–Fluckiger, R. Parimala, Galois algebras, Hasse principle and induction–restriction methods, *Documenta Math.* 16 (2011), 677–707.
- [BP 13] E. Bayer–Fluckiger, R. Parimala, Correction to : Galois algebras, Hasse principle and induction–restriction methods, *Documenta Math.* 16 (2011), 677–707 (to appear).
- [BPS 13] E. Bayer–Fluckiger, R. Parimala and J-P. Serre, Hasse principle for  $G$ -trace forms, *Izvestia Math.* (2013), to appear.
- [J 64] N. Jacobson, *Structure of rings*, AMS Colloquium Series XXXVII (1964).
- [KMRT 98] M. Knus, A. Merkurjev, M. Rost & J-P. Tignol, *The Book of Involutions*, AMS Colloquium Publications 44, 1998.
- [M 86] J. Morales, Integral bilinear forms with a group action, *J. Algebra* 98 (1986), 470 - 484.
- [R 11] C.R. Riehm, *Introduction to Orthogonal, Symplectic and Unitary Representations of Finite Groups*, Fields Institute Monographies 28, AMS, 2011.
- [Sch 85] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss, Springer–Verlag (1985).

Eva Bayer–Fluckiger  
École Polytechnique Fédérale  
de Lausanne  
EPFL/FSB/MATHGEOM/CSAG  
Station 8  
1015 Lausanne, Switzerland  
eva.bayer@epfl.ch

Nivedita Bhaskhar  
Department of Mathematics  
& Computer Science  
Emory University  
Atlanta, GA 30322, USA.  
nbhaskh@emory.edu

Raman Parimala  
Department of Mathematics  
& Computer Science  
Emory University  
Atlanta, GA 30322, USA.  
parimala@mathcs.emory.edu