Embeddings of maximal tori in classical groups and explicit Brauer–Manin obstruction

E. Bayer-Fluckiger, T-Y. Lee, R. Parimala

Introduction

Embeddings of maximal tori into classical groups over global fields of characteristic $\neq 2$ are the subject matter of several recent papers (see for instance Prasad and Rapinchuk [PR 10], [F 12], [Lee 14], [B 12], [B 13]), with special attention to the Hasse principle. In particular, it is shown in [Lee 14] that the Brauer–Manin obstruction is the only one.

The present paper gives necessary and sufficient conditions for the embedding of maximal tori in classical groups. As in [PR 10], the embedding problem will be described in terms of embeddings of étale algebras with involution into central simple algebras with involution. Let (E, σ) be an étale algebra with involution defined over a global field, satisfying certain dimension conditions (cf. §1). In §4, we define a group $Ш(E, \sigma)$ which plays an important role in the embedding problem.

Let (A, τ) be a central simple algebra with involution defined over the same global field, and assume that everywhere locally there exists an (oriented) embedding of (E, σ) in (A, τ). Then we define a map $f : Ш(E, \sigma) \to \mathbf{Z}/2\mathbf{Z}$ such that (E, σ) can be embedded in (A, τ) globally if and only if $f = 0$ (cf. Theorem 5.5.1.).

By [Lee 14] we know that the Brauer–Manin obstruction is the only one, hence we obtain an explicit description of this obstruction.

In addition to the Hasse principle, one also needs to know when an embedding exists over local fields. This is done in [Lee 14] in terms of Tits indices, and in §3 of the present paper (see also 6.3. and 8.2.) in terms of classical invariants. Finally, §9 contains some applications and examples. In particular, we recover Theorem A of Prasad and Rapinchuk (see [PR 10], Introduction, page 584).

The paper has two appendices. The first one outlines the relationship of the point of view and results of [Lee 14] and those of the present paper, and the second one contains a new proof of Theorem B of Prasad and Rapinchuk (see [PR 10], Introduction, page 586).

We thank Gopal Prasad for his interest in our results, and for encouraging us to include an alternative proof of Theorem B of [PR 10] in our paper.

§1. Definitions, notation and basic facts

1.1. Embeddings of algebras with involution

Let L be a field, and let A be a central simple algebra over L. Let τ be an involution of A, and let K be the fixed field of τ in L. Recall that τ is said to be of the *first kind* if $K = L$ and of the *second kind* if $K \neq L$; in this case, L is a quadratic extension of K. Let $\dim_L(A) = n^2$. Let E be a commutative étale algebra of rank n over L, and let $\sigma : E \to E$ be a K–linear involution. such that $\sigma|L = \tau|L$. Set $F = \{e \in E | \sigma(e) = e\}$. Assume that the following dimension condition holds :

$$\dim_K F = \begin{cases} n & \text{if } L \neq K\,; \\ [\frac{n+1}{2}] & \text{if } L = K. \end{cases}$$

An *embedding* of (E, σ) in (A, τ) is by definition an injective homomorphism $f : E \to A$ such that $\tau(f(e)) = f(\sigma(e))$ for all $e \in E$. It is well–known that embeddings of maximal tori into classical groups can be described in terms of embeddings of étale algebras with involution into central simple algebras with involution satisfying the above dimension hypothesis (see for instance [PR 10], Proposition 2.3).

We say that a separable field extension E'/L is a *factor* of E if $E = E' \times E''$ for some étale L–algebra E''. It is well–known that E can be embedded in the algebra A if and only if each of the factors of E splits A :

Proposition 1.1.1. *The étale algebra E can be embedded in the central simple algebra A if and only if for every factor E' of E, the algebra $A \otimes_L E'$ is a matrix algebra over E'.*

Proof. See for instance [PR 10], Proposition 2.6.

Let $\epsilon : E \to A$ be an L–embedding which may not respect the given involutions. The following properties are well–known :

Proposition 1.1.2. *There exists a τ–symmetric element $\alpha \in A^\times$ such that for*

$$\theta = \tau \circ \mathrm{Int}(\alpha)$$

we have

$$\epsilon(\sigma(e)) = \theta(\epsilon(e)) \text{ for all } e \in E,$$

in other words $\epsilon : (E, \sigma) \to (A, \theta)$ is an L—embedding of algebras with involution.

Proof. See [K 69], §2.5. or [PR 10], Proposition 3.1.

Note that θ and τ are of the same type (orthogonal, symplectic or unitary), since α is τ–symmetric.

For all $a \in F^\times$, let $\theta_a : A \to A$ be the involution given by $\theta_a = \theta \circ \mathrm{Int}(\epsilon(a))$. Note that $\epsilon : (E, \sigma) \to (A, \theta_a)$ is an embedding of algebras with involution.

Proposition 1.1.3. *The following conditions are equivalent :*

(a) *There exists an L–embedding $\iota : (E, \sigma) \to (A, \tau)$ of algebras with involution.*

(b) *There exists an $a \in F^\times$ such that $(A, \theta_a) \simeq (A, \tau)$ as algebras with involution.*

Proof. See [PR 10], Theorem 3.2.

If $\iota : (E, \sigma) \to (A, \tau)$ is an embedding of algebras with involution, and if $a \in F^\times$, $\alpha \in A^\times$ are such that $\mathrm{Int}(\alpha) : (A, \theta_a) \to (A, \tau)$ is an isomorphism of algebras with involution satisfying $\mathrm{Int}(\alpha) \circ \epsilon = \iota$, then (ι, a, α) are called *parameters* of the embedding.

Lemma 1.1.4. *Let $a, b \in F^\times$ and let $\alpha \in A^\times$. Then we have :*

(i) $\mathrm{Int}(\alpha) : (A, \theta_a) \to (A, \theta_b)$ *is an isomorphism of algebras with involution if and only if there exists $\lambda \in L^\times$ such that $\theta(\alpha)\epsilon(b)\alpha = \lambda\epsilon(a)$.*

(ii) *Moreover, we have $\mathrm{Int}(\alpha) \circ \epsilon = \epsilon$ if and only if there exists $y \in E^\times$ and $\lambda \in L^\times$ such that $\alpha = \epsilon(y)$ and $\mathrm{N}_{E/F}(y) = \lambda ab^{-1}$.*

Proof. The proof of (i) follows from a direct computation. Let us prove (ii). If $\mathrm{Int}(\alpha) \circ \epsilon = \epsilon$, then we have $\alpha\epsilon(x)\alpha^{-1} = \epsilon(x)$ for all $x \in E$. Since E is a maximal commutative subalgebra of A, this implies that $\alpha \in \epsilon(E)$. Let $\alpha = \epsilon(y)$ for some $y \in E$. Then we have $\theta(\epsilon(y))\epsilon(b)\epsilon(y) = \lambda\epsilon(a)$. This implies that $b\sigma(y)y = \lambda a$, hence $\mathrm{N}_{E/F}(y) = \lambda ab^{-1}$. The converse is clear.

In particular, there exists an isomorphism of algebras with involution $(A, \theta_a) \to (A, \theta_b)$ commuting with ϵ if and only if we have $ab^{-1} \in L^\times \mathrm{N}_{E/F}(E^\times)$.

Definition 1.1.5. We say that (E, σ) is *split* if there exists an idempotent $e \in E$ such that $e + \sigma(e) = 1$.

Equivalently, (E, σ) is split if $E \simeq E_1 \times E_2$ with $\sigma(E_1) = E_2$.

Definition 1.1.6. We say that (A, τ) is *hyperbolic* if there exists an idempotent $a \in A$ such that $a + \tau(a) = 1$.

Equivalently, (A, τ) is hyperbolic if $A \simeq M_r(D)$ for some division algebra D, and τ is induced by a hyperbolic hermitian form over D (cf. [KMRT 98], Chapter II, (6.7) and (6.8)).

Proposition 1.1.7. *Suppose that (E, σ) is split. Then the following are equivalent :*

(a) *The étale algebra with involution (E, σ) can be embedded in the central simple algebra with involution (A, τ).*

(b) *All the factors of E split A, and the involution (A, τ) is hyperbolic.*

Proof. Assume that (a) holds. Then by Proposition 1.1.1. all the factors of E split A. Let $\iota : (E, \sigma) \to (A, \tau)$ be an embedding, and let $e \in E$ be an idempotent such that $e+\sigma(e) = 1$. Set $a = \iota(e)$. Then $a \in A$ is an idempotent, and we have $a+\tau(a) = 1$, hence (A, τ) is hyperbolic. Conversely, assume that (b) holds. Since E can be embedded in A, by Proposition 1.1.2. there exists an involution $\theta : A \to A$ such that (E, σ) embeds into (A, θ). Hence (A, θ) is hyperbolic, and therefore $(A, \tau) \simeq (A, \theta)$. By Proposition 1.1.3. this implies that (E, σ) embeds into (A, τ), hence (a) holds.

1.2. Scaled trace forms

Let us keep the notation introduced in 1.1. In particular, (E, σ) is an étale algebra with involution. Let $a \in F^\times$, and let us consider the form

$$T_a : E \times E \to L$$

given by

$$T_a(x, y) = \mathrm{Tr}_{E/L}(ax\sigma(y)).$$

Then T_a is a quadratic form if $L = K$, and a hermitian form if L/K is a quadratic extension. For $a = 1$, we use the notation $T = T_1$.

Proposition 1.2.1. *Let $a \in F^\times$. Then we have*

$$\det(T_a) = \mathrm{N}_{E/L}(a)\det(T),$$

in $K^\times/K^{\times 2}$ if $L = K$, and in $K^\times/\mathrm{N}_{L/K}(L^\times)$ if L/K is a quadratic extension.

Proof. Let $E^\sharp$ be the L–vector space of σ-semilinear homomorphisms $f : E \to L$ (i.e. $f(\lambda x) = \sigma(\lambda)f(x)$ for all $x \in E$ and $\lambda \in L$). For any quadratic or hermitian form $b : E \times E \to L$, let us denote by $\mathrm{ad}(b) : E \to E^\sharp$ the L–linear map defined by $\mathrm{ad}(b)(x)(y) = b(x, y)$ for all $x, y \in E$. Let $(e_1, \ldots, e_n)$ be an L–basis of E, and let $(e_1^\sharp, \ldots, e_n^\sharp)$ be the dual basis. Then $\det(b)$ is the determinant of $\mathrm{ad}(b)$ in the bases $(e_1, \ldots, e_n)$ and $(e_1^\sharp, \ldots, e_n^\sharp)$.

Let $m_a : E \to E$ be the multiplication by a. By definition, we have $\mathrm{N}_{E/L}(a) = \det(m_a)$. Note that we have $\mathrm{ad}(T_a) = \mathrm{ad}(T) \circ m_a$. This implies that $\det(T_a) = \mathrm{N}_{E/L}(a)\det(T)$.

Corollary 1.2.2. *Let $a \in F^\times$. Then we have*

(a) *If $L = K$ and n is even, then* $\det(T_a) = \det(T)$.

(b) *If L is a quadratic extension of K, then* $\det(T_a) = \mathrm{N}_{F/K}(a)\det(T)$.

Proof. Let us assume that $L = K$. By Proposition 1.2.1. we have $\det(T_a) = \mathrm{N}_{E/K}(a)\det(T) \in K^\times/K^{\times 2}$. Since $a \in F^\times$, we have $\mathrm{N}_{E/K}(a) = \mathrm{N}_{F/K}(a)^2$, which is an element of $K^{\times 2}$, hence we have $\det(T_a) = \det(T) \in K^\times/K^{\times 2}$. This proves (a).

Suppose now that L is a quadratic extension of K. Then Proposition 1.2.1. implies that $\det(T_a) = \mathrm{N}_{E/L}(a)\det(T) \in K^\times/\mathrm{N}_{L/K}(L^\times)$. Since $a \in F^\times$, we have $\mathrm{N}_{E/L}(a) = \mathrm{N}_{F/K}(a)$, and this implies (b).

1.3. The discriminant of an étale algebra with involution

Recall that $T : E \times E \to L$ is defined by $T(x, y) = \mathrm{Tr}_{E/L}(x\sigma(y))$.

Definition 1.3.1. Set $\mathrm{disc}(E, \sigma) = \det(T)$, considered as an element of $K^\times/K^{\times 2}$ if $L = K$, and as an element of $K^\times/\mathrm{N}_{L/K}(L^\times)$ if L/K is a quadratic extension. This element is called the *discriminant* of the étale algebra with involution (E, σ).

Lemma 1.3.2. *Suppose that $L = K$, and that $n = 2r$. Then*

(i) $\mathrm{disc}(E, \sigma) = (-1)^r\mathrm{disc}(E)$.

(ii) *For all $a \in F^\times$ we have* $\mathrm{disc}(T_a) = \mathrm{disc}(E)$.

Proof. Let us denote by $T_{E/K} : E \times E \to K$, given by $(x, y) \mapsto \mathrm{Tr}_{E/K}(xy)$, the usual trace form. We have $\mathrm{rank}(E) = 2\mathrm{rank}(F) = 2r$. Writing $E = F(\sqrt{d})$ for some $d \in F^\times$, a computation shows that $\det(T) = (-1)^r\det(T_{E/K})$. By definition, we have $\mathrm{disc}(E) = \det(T_{E/K})$, hence $\mathrm{disc}(E, \sigma) = (-1)^r\mathrm{disc}(E)$.

Since $\mathrm{disc}(T) = (-1)^r\det(T)$, by (i) we have $\mathrm{disc}(T) = \mathrm{disc}(E)$. By Corollary 1.2.2. we have $\mathrm{disc}(T_a) = \mathrm{disc}(T)$, hence $\mathrm{disc}(T_a) = \mathrm{disc}(E)$.

1.4. An embedding criterion

Assume that $A = M_n(L)$ and that τ is an orthogonal or unitary involution. Then $\tau : A \to A$ is given by an n–dimensional form $b : V \times V \to L$, which is quadratic if $L = K$ and hermitian if $L \neq K$. We have an embedding criterion, in terms of the forms introduced in 1.2 :

Proposition 1.4.1. *There exists an embedding of algebras with involution $(E, \sigma) \to (A, \tau)$ if and only if there exists $a \in F^\times$ such that $b \simeq T_a$.*

Proof. If $L = K$, then this is well–known (see for instance [PR], 7.1.). The proof is similar in the case when $L \neq K$. However, we give a proof for the convenience of the reader.

Note that $A = \mathrm{End}(V)$. Since τ is induced by $b : V \times V \to L$, we have $b(ex, y) = b(x, \tau(e)y)$ for all $e \in \mathrm{End}(V)$ and all $x, y \in V$.

Suppose first that there exists $a \in F^\times$ such that $b \simeq T_a$. Let us identify V to E and b to T_a, and note that sending $e \in E$ to the multiplication by e gives rise to an embedding $E \to \mathrm{End}(E)$. Identifying b to T_a, we have, for all $e, x, y \in E$,

$$b(ex, y) = \mathrm{Tr}_{E/L}(aex\sigma(y)) = \mathrm{Tr}_{E/L}(ax\sigma(\sigma(e)y)) = b(x, \sigma(e)y).$$

Since this holds for all $x \in E$, and that $b(ex, y) = b(x, \tau(e)y)$ for all $x \in E$, we have $\sigma(e) = \tau(e)$ for all $e \in E$. Hence the natural embedding of E in $A \simeq \mathrm{End}(E)$ is an embedding of algebras with involution.

Suppose now that there exists an embedding of algebras with involution $\iota : (E, \sigma) \to (A, \tau)$. Then for all $e \in E$, we have

$$b(\iota(e)x, y) = b(x, \tau(\iota(e))y) = b(x, \iota(\sigma(e))y).$$

Let us show that there exists a hermitian form $h : V \times V \to E$ such that $b(x, y) = \mathrm{Tr}_{E/L}(h(x, y))$ for all $x, y \in V$. Let us fix $x, y \in V$, and let us consider the linear form $E \to L$ such that $e \mapsto f(e) = b(\iota(e)x, y)$. Since E is a separable L–algebra, there exists $e' \in E$ such that $\mathrm{Tr}_{E/L}(ee') = f(e)$ for all $e \in E$. Set $h(x, y) = e'$. Let us check that h is a hermitian form. It is easy to see that h is linear in the first variable, so it remains to check that $\sigma(h(x, y)) = h(y, x)$ for all $x, y \in V$. We have

$$\mathrm{Tr}_{E/L}(e\sigma(h(x, y))) = \sigma\ [\mathrm{Tr}_{E/L}(\sigma(e)h(x, y))] = \sigma[b(\iota(\sigma(e))x, y))] =$$

$$= \sigma[b(x, \iota(e)y)] = \sigma[\sigma[b(\iota(e)y, x)]] = b(\iota(e)y, x) = \mathrm{Tr}_{E/L}(eh(y, x)).$$

Since this holds for all $e \in E$, we have $h(y, x) = \sigma(h(x, y))$, as claimed. Therefore $h : V \times V \to E$ is a one dimensional hermitian form. Let us identify the 1–dimensional E–vector space V with E. Then there exists $a \in F^\times$ such that $h(x, y) = ax\sigma(y)$. Hence we have $b \simeq T_a$, and this completes the proof of the Proposition.

Note that if (A, θ) is the involution induced by T and if $a \in F^\times$, then T_a induces the involution (A, θ_a).

1.5. Invariants of central simple algebras with involution

If (A, τ) is of orthogonal type and n is even, we denote by $\mathrm{disc}(A, \tau)$ its *discriminant* (cf. [KMRT 98], Chap II. (7.2), and by $C(A, \tau)$ its *Clifford algebra* (cf. [KMRT 98], Chap II. (8.7)). We denote by $Z(A, \tau)$ the center

of the algebra $C(A,\tau)$. Then $Z(A,\tau)$ is a quadratic étale algebra over K. If (A,τ) is unitary, then we denote by $D(A,\tau)$ its *discriminant algebra* (cf. [KMRT 98], Chap II, (10.28)). The *signature* of (A,τ) is defined in [KMRT 98], Chap II. (11.10) and (11.25).

If moreover $A \simeq M_n(L)$, then τ is induced by a symmetric, skew–symmetric or hermitian form, according as τ is of orthogonal, symplectic or unitary type. In this case, we have some additional invariants, such as the Hasse invariant (in the orthogonal case), as well as the determinant (in the unitary case). In particular, if τ is unitary and induced by a hermitian form h over L/K, then we set $\det(A,\tau) = \det(h) \in K^\times/\mathrm{N}_{L/K}(L^\times)$. Let us write $L = K(\sqrt{\delta})$, and let us denote by $\mathrm{Br}(K)$ the Brauer group of K. Then we have $D(A,\tau) = (\mathrm{disc}(h),\delta) \in \mathrm{Br}(K)$, where $\mathrm{disc}(h) = (-1)^{n(n-1)/2}\det(h)$ (cf. [KMRT 98], Chap II. (10.35)). If τ is orthogonal and induced by a quadratic form q over K, then we denote by $w(q) \in \mathrm{Br}_2(K)$ its Hasse invariant.

Let $d \in F^\times$ be such that $E = F(\sqrt{d})$. The following result is due to Brusamarello, Chuard–Koulmann and Morales (cf. [BCM 03], Theorem 4.3.) :

Lemma 1.5.1. *Let (A,θ) be an orthogonal involution. Assume that n is even, and let $a \in F^\times$. Then we have $w(T_a) = w(T) + \mathrm{cor}_{F/K}(a,d)$.*

Lemma 1.5.2. *Let (A,θ) be a unitary involution, and let $a \in F^\times$. Then $D(A,\theta_a) = D(A,\theta) + \mathrm{cor}_{F/K}(a,d)$.*

Proof. By [KMRT 98], Chap. II, (10.36), we have $D(A,\theta_a) = D(A,\theta) + (\mathrm{N}_{F/K}(a), L/K)$. We have $(\mathrm{N}_{F/K}(a), L/K) = \mathrm{cor}_{F/K}(a, E/F) = \mathrm{cor}_{F/K}(a,d)$, hence the lemma is proved.

1.6. Some necessary embedding conditions

The existence of an embedding of algebras with involution $(E,\sigma) \to (A,\tau)$ implies the following relationship between the discriminants of E and (A,τ) :

Proposition 1.6.1. *Suppose that the degree of A is even, and that (A,τ) is of the orthogonal type. If there exists an embedding of algebras with involution $(E,\sigma) \to (A,\tau)$, then we have $\mathrm{disc}(E) = \mathrm{disc}(A,\tau) \in K^\times/K^{\times 2}$.*

Proof. Let M be the function field of the Severi–Brauer variety of the algebra A. Then we have $A \otimes_K M \simeq M_n(M)$, and the involution τ is induced by a quadratic form q over M. By Proposition 1.4.1. and Lemma 1.3.2. (ii) (see also [B 12], Lemma 1.4.1.) we have $\mathrm{disc}(E \otimes_K M) = \mathrm{disc}(q) \in M^\times/M^{\times 2}$. Since the natural map $K^\times/K^{\times 2} \to M^\times/M^{\times 2}$ is injective, we have $\mathrm{disc}(E) = \mathrm{disc}(A,\tau) \in K^\times/K^{\times 2}$.

Proposition 1.6.2. *Suppose that $A \simeq M_n(L)$, and that (A,τ) is of the unitary type. If there exists an embedding of algebras with involution $(E,\sigma) \to (A,\tau)$, then we have $\det(A,\tau)\mathrm{disc}(E,\sigma)^{-1} \in \mathrm{N}_{F/K}(F^\times)\mathrm{N}_{L/K}(L^\times)$.*

Proof. Since $A \simeq M_n(L)$, the involution τ is induced by a hermitian form h. By Proposition 1.4.1. there exists $a \in F^\times$ such that $h \simeq T_a$. By Corollary 1.2.2. (b) we have $\det(T_a) = \mathrm{N}_{F/K}(a)\det(T)$. Recall that $\mathrm{disc}(E,\sigma)$ is by definition equal to $\det(T) \in K^\times/\mathrm{N}_{L/K}(L^\times)$. We have $\det(A,\tau) = \det(h) = \det(T_a)$. This implies that $\det(A,\tau) = \mathrm{N}_{F/K}(a)\mathrm{disc}(E,\sigma) \in K^\times/\mathrm{N}_{L/K}(L^\times)$, hence we have $\det(A,\tau)\mathrm{disc}(E,\sigma)^{-1} \in \mathrm{N}_{F/K}(F^\times)\mathrm{N}_{L/K}(L^\times)$.

§2. Orientation

In order to treat the *non–split orthogonal* case, we need an additional tool, namely the notion of *orientation*. Assume that (A,τ) is an orthogonal involution, and that the degree of A is even. Let us set $\deg(A) = 2r$.

We have seen that the existence of an embedding of algebras with involution $(E,\sigma) \to (A,\tau)$ implies that $\mathrm{disc}(E) = \mathrm{disc}(A,\tau) \in K^\times/K^{\times 2}$ (see Proposition 1.6.1.). Therefore the discriminant algebra of E (see below) is isomorphic to the K–algebra $Z(A,\tau)$. However, such an isomorphism is not unique. This leads to the notions of *orientation*, and of *oriented embedding*, needed for the analysis of the Hasse principle (see 6.1.).

2.1. Discriminant algebra

We have $E \simeq F[X]/(X^2-d)$ for some $d \in F^\times$. Let us consider the F–linear involution $\sigma' : F[X]/(X^2-d) \to F[X]/(X^2-d)$ determined by $\sigma'(X) = -X$. Then we have an isomorphism of algebras with involution $(E,\sigma) \simeq (F[X]/(X^2-d),\sigma')$. Let x be the image of X in E, and note that we have $\sigma(x) = -x$. Let $\Delta(E)$ be the discriminant algebra of E (cf. [KMRT 98], Chapter V, §18, p. 290).

Lemma 2.1.1. *We have an isomorphism of K–algebras*

$$\Delta(E) \simeq K[Y]/(Y^2 - (-1)^r\mathrm{N}_{E/K}(x)).$$

Proof. Recall that $T_{E/K} : E \times E \to K$, defined by $T_{E/K}(e,f) = \mathrm{Tr}_{E/K}(ef)$, is the trace form of E. Then by [KMRT 98], Proposition (18.2) we have

$$\Delta(E) \simeq K[Y]/(Y^2 - \det(T_{E/K})).$$

Note that $\mathrm{Tr}_{E/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{E/F}$, and that the trace form $T_{E/F} : E \times E \to F$, defined by $T_{E/F}(e,f) = \mathrm{Tr}_{E/F}(ef)$, is isomorphic to $< 2, 2d >$. Further, we have $d = -\mathrm{N}_{E/F}(x)$ and hence $\mathrm{N}_{F/K}(d) = (-1)^r\mathrm{N}_{E/K}(x)$. Therefore we have $\det(T_{E/K}) = (-1)^r\mathrm{N}_{E/K}(x) \in K^\times/K^{\times 2}$, and this concludes the proof of the lemma.

Let us denote by y the image of Y in $\Delta(E)$. The elements x and y will be fixed in the sequel. Let $\rho : \Delta(E) \to \Delta(E)$ be the automorphism of $\Delta(E)$

induced by σ. Note that we have $\rho(y) = (-1)^r$, and that hence ρ is the identity if r is even and the non–trivial automorphism of the quadratic algebra $\Delta(E)$ if r is odd.

2.2. Generalized Pfaffian

For any central simple algebra A over K of degree $2r$ with an orthogonal involution θ, let us denote by $\mathrm{Skew}(A,\theta)$ the set $\{a \in A \mid \theta(a) = -a\}$ of skew elements of A with respect to the involution τ. Recall that $C(A,\theta)$ is the Clifford algebra of (A,θ), and that $Z(A,\theta)$ is the center of $C(A,\theta)$. Recall that $Z(A,\theta)$ is a quadratic étale algebra over K. Let us denote by γ the non–trivial automorphism of $Z(A,\theta)$ over K.

The *generalized Pfaffian* (cf. [KMRT 98], Chapter II, §8) of (A,θ) is a homogeneous polynomial map of degree r, denoted by

$$\pi_\theta : \mathrm{Skew}(A,\theta) \to Z(A,\theta)$$

such that for all $a \in \mathrm{Skew}(A,\theta)$, we have $\gamma(\pi_\theta(a)) = -\pi_\theta(a)$, and $\pi_\theta(a)^2 = (-1)^r \mathrm{Nrd}(a)$; for all $x \in A$ and $a \in \mathrm{Skew}(A,\theta)$, we have $(\pi_\theta(xa\theta(x)) = \mathrm{Nrd}_A(x)\pi_\theta(a)$ (cf. [KMRT 98], Proposition (8.24)).

2.3. Orientation

For any orthogonal involution (A,τ), an isomorphism of K–algebras

$$\Delta(E) \to Z(A,\tau)$$

will be called an *orientation*.

Let us assume that the étale algebra E can be embedded in the central simple algebra A, and let us fix an embedding $\epsilon : E \to A$. By Proposition 1.1.2. there exists an involution $\theta : A \to A$ of orthogonal type such that $\epsilon : (E,\sigma) \to (A,\theta)$ is an embedding of algebras with involution.

Let us fix such an involution (A,θ). We now define an orientation $u : \Delta(E) \to Z(A,\theta)$ that will be fixed in the sequel. Fix a generalized Pfaffian map $\pi_\theta : \mathrm{Skew}(A,\theta) \to Z(A,\theta)$ as above. Recall that $E \simeq F[X]/(X^2 - d)$, that $\Delta(E) \simeq K[Y]/(Y^2 - (-1)^r \mathrm{N}_{E/K}(x))$, and that we have fixed the images x of X in E and y of Y in $\Delta(E)$. Let

$$u : \Delta(E) \to Z(A,\theta)$$

be defined by

$$y \mapsto \pi_\theta(\epsilon(x)).$$

Lemma 2.3.1. *The map u is an isomorphism of K–algebras.*

Proof. We have $\gamma(\epsilon(x)) = -\epsilon(x)$. Further, $(\pi_\theta(\epsilon(x))^2 = (-1)^r \mathrm{Nrd}_A(\epsilon(x)) = (-1)^r \mathrm{N}_{E/K}(x) = y^2$. This implies that u is an isomorphism of K–algebras.

2.4. Similitudes

Let $\alpha \in A^\times$. Following [KMRT], Definition (12.14), page 158, we say that α is a *similitude* of (A, τ) if $\alpha\tau(\alpha) \in K^\times$. For a similitude $\alpha \in A^\times$, the scalar $\alpha\tau(\alpha)$ is called the *multiplier* of the similitude. We say that α is a *proper* similitude if $\mathrm{Nrd}(\alpha) = (\alpha\tau(\alpha))^r$; otherwise, α is called an *improper* similitude. Note that α is a similitude if and only if $\mathrm{Int}(\alpha) : (A, \tau) \to (A, \tau)$ is an isomorphism of algebras with involution. If A is split, then (A, τ) admits improper similitudes (indeed, any reflection is an improper similitude).

Any isomorphism of algebras with involution $\mathrm{Int}(\alpha) : (A, \tau) \to (A, \tau')$ induces an isomorphism of the Clifford algebras $C(A, \tau) \to C(A, \tau')$. Let us denote by

$$c(\alpha) : Z(A, \tau) \to Z(A, \tau')$$

the restriction of this isomorphism to the centers of the Clifford algebras. The following property will be important in the sequel.

Lemma 2.4.1. *Let (A, τ) be an orthogonal involution, and let $\alpha \in A^\times$ be a similitude. Then α is a proper similitude if and only if $c(\alpha)$ is the identity.*

Proof. See for instance [KMRT 98], Proposition (13.2), page 173.

2.5. Compatible orientations

Recall that $\epsilon : E \to A$ is an embedding of algebras, that $\theta : A \to A$ is an orthogonal involution such that $\epsilon : (E, \sigma) \to (A, \theta)$ is an embedding of algebras with involution, and that we are fixing an orientation $u : \Delta(E) \to Z(A, \theta)$. We now define a notion of *compatibility* of orientations.

Lemma 2.5.1. *Let (A, τ) be a central simple algebra with an orthogonal involution, and let $\iota : (E, \sigma) \to (A, \tau)$ be a embedding of algebras with involution. Let $\alpha \in A^\times$ be such that $\mathrm{Int}(\alpha) : (A, \tau) \to (A, \tau)$ is an automorphism of algebras with involution, and $\mathrm{Int}(\alpha) \circ \iota = \iota$. Then*

(a) *There exists $x \in E^\times$ such that $\alpha = \iota(x)$, and $\mathrm{N}_{E/F}(x) \in K^\times$.*

(b) *The map $c(\alpha)$ is the identity.*

Proof. Since $\mathrm{Int}(\alpha) \circ \iota = \iota$, the restriction of $\mathrm{Int}(\alpha)$ to $\iota(E)$ is the identity. Note that $\iota(E)$ is a maximal commutative subalgebra of A. Hence we have $\alpha = \iota(x)$ for some $x \in E^\times$. As $\mathrm{Int}(\alpha) : (A, \tau) \to (A, \tau)$ is an automorphism of algebras with involution, we have $\alpha\tau(\alpha) = \lambda$ for some $\lambda \in K^\times$. Hence we have $(\iota x)\tau(\iota x) = \lambda$. Since $\iota : (E, \sigma) \to (A, \tau)$ is an embedding of algebras with involution, we have $\iota(x\sigma(x)) = \lambda$. This completes the proof of (a).

Let us prove (b). By part (a), we have $\alpha\tau\alpha = \iota(x\sigma(x)) = \iota(\lambda) = \lambda$. This implies that α is a similitude. Moreover, we have $\mathrm{Nrd}(\alpha) = \mathrm{N}_{E/K}(x) = \mathrm{N}_{F/K}(\lambda) = \lambda^r$. Hence α is a proper similitude, and by lemma 1.7.1. this implies that $c(\alpha)$ is the identity.

Definition 2.5.2. Let $\theta' : A \to A$ be an orthogonal involution such that $\epsilon : (E, \sigma) \to (A, \theta')$ is an embedding of algebras with involution, and let $u' : \Delta(E) \to Z(A, \theta')$ be an orientation. We say that the orientations u and u' are *compatible* if for every isomorphism of algebras with involution $\mathrm{Int}(\alpha) : (A, \theta) \to (A, \theta')$ such that $\mathrm{Int}(\alpha) \circ \epsilon = \epsilon$, we have $u' = c(\alpha) \circ u$.

Recall that for all $a \in F^\times$, we define an involution $\theta_a : A \to A$ by $\theta_a = \theta \circ \mathrm{Int}(\epsilon(a))$. Note that the embedding $\epsilon : (E, \sigma) \to (A, \theta)$ induces an embedding of algebras with involution $\epsilon : (E, \sigma) \to (A, \theta_a)$. Our next aim is to define an orientation of (A, θ_a) compatible with the orientation u of (A, θ). Let K_s be a separable closure of K, and set $A_s = A \otimes_K K_s$.

Proposition 2.5.3. *Let $a \in F^\times$. Then there exists a unique isomorphism $\phi_a : Z(A, \theta) \to Z(A, \theta_a)$ such that for all $\alpha \in A_s^\times$ which gives an isomorphism of algebras with involution $\mathrm{Int}(\alpha) : (A_s, \theta) \to (A_s, \theta_a)$ with $\mathrm{Int}(\alpha) \circ \epsilon = \epsilon$, we have $c(\alpha) = \phi_a$.*

Proof. Let $d \in K^\times$ represent the square class of $\mathrm{disc}(A, \theta)$, and let us write $Z(A, \theta) = K \oplus Kz$ with $z^2 = d$. Note that d also represents the square class of $\mathrm{disc}(A, \theta_a)$, since $a \in F^\times$. Let us write $Z(A, \theta_a) = K \oplus Kz_a$ with $z_a^2 = d$.

Let $b \in (E \otimes_K K_s)^\times$ be such that $b\sigma(b) = a^{-1}$. Then $\mathrm{Int}(\epsilon(b)) : (A_s, \theta) \to (A_s, \theta_a)$ is an isomorphism of algebras with involution commuting with ϵ, and it induces an isomorphism of the Clifford algebras $C(A_s, \theta) \to C(A_s, \theta_a)$.

We have $A_s = M_{2r}(K_s)$, and $\theta : A_s \to A_s$ is induced by a quadratic form $q : V \times V \to K_s$. Let $(e_1, \ldots, e_{2r})$ be an orthogonal basis for q. Since $Z(A, \theta) = K \oplus K(e_1 \ldots e_{2r})$, we have $z = \mu(e_1 \ldots e_{2r})$ for some $\mu \in K_s^\times$. Let us replace e_1 by $\mu^{-1}e_1$. Then we have $z = e_1 \ldots e_{2r}$.

Set $q = \epsilon(b)^t q_a \epsilon(b)$. Since $a^{-1} = b\sigma(b)$ and a is θ–symmetric, the involution induced by q_a is θ_a. Let us consider the isometry $\epsilon(b) : (V, q) \to (V, q_a)$. Then $\epsilon(b)$ induces a map $c(\epsilon(b)) : C(V, q) \to C(V, q_a)$ which sends $e_1 \ldots e_{2r}$ to $(\epsilon(b)e_1) \ldots (\epsilon(b)e_{2r})$. Therefore we have $(\epsilon(b)e_1) \ldots (\epsilon(b)e_{2r})^2 = q_a(\epsilon(b)e_1) \ldots q_a(\epsilon(b)e_{2r}) = q(e_1) \ldots q(e_{2r}) = (e_1 \ldots e_{2r})^2 = d$. This implies that $\epsilon(b)(e_1) \ldots \epsilon(b)(e_{2r}) = \pm z_a$ and $c(\epsilon(b))(z) = \pm z_a$. Hence the restriction of the map $c(\epsilon(b))$ to $Z(A_s, \theta)$ is defined over K.

Set $\phi_a = c(\epsilon(b))$, and note that $\phi_a : Z(A, \theta) \to Z(A, \theta_a)$ is an isomorphism.

Let us show that ϕ_a is independent of the choice of b. Let $b' \in A_s$ such that $b'\sigma(b') = a$. Then we have $c(\mathrm{Int}(\epsilon(b'))) = c(\mathrm{Int}(\epsilon(b)))$. We have an isomorphism of algebras with involution $\mathrm{Int}(\epsilon(b^{-1}b')) : (A,\theta) \to (A,\theta)$ satisfying $\mathrm{Int}(\epsilon(b^{-1}b')) \circ \epsilon = \epsilon$. Hence by Lemma 2.4.1. the map

$$c(\mathrm{Int}(\epsilon(b^{-1}b'))) : Z(A,\theta) \to Z(A,\theta)$$

is the identity. Therefore $c(\epsilon(b)) = c(\epsilon(b'))$, hence $c(\epsilon(b))$ is independent of the choice of b.

Let $\alpha \in A_s^\times$ be such that $\mathrm{Int}(\alpha) : (A_s,\theta) \to (A_s,\theta_a)$ is an isomorphism of algebras with involution with $\mathrm{Int}(\alpha) \circ \epsilon = \epsilon$. Then by Lemma 2.4.1. there exists $x \in (E \otimes_K K_s)^\times$ such that $\alpha = \epsilon(x)$. This implies that $c(\mathrm{Int}(\epsilon(x))) = c(\epsilon(b)) = \phi_a$. Hence $c(\alpha) = \phi_a$, as required. This also shows the uniqueness of ϕ_a, and completes the proof of the proposition.

Recall that we have fixed an isomorphism $u : \Delta(E) \to Z(A,\theta)$. For all $a \in F^\times$, let us define an orientation by $u_a = \phi_a \circ u : \Delta(E) \to Z(A,\theta_a)$. Then u_a is compatible with u. Note that ϕ_1 is the identity, hence $u_1 = u$.

For all $a \in F^\times$, let us identify $\Delta(E)$ with $Z(A,\theta_a)$ via the orientation u_a. This endows the Clifford algebra $C(A,\theta_a)$ with a structure of $\Delta(E)$–algebra. We have the following

Lemma 2.5.4. *For all $a \in F^\times$ we have*

$$C(A,\theta_a) = C(A,\theta) + \mathrm{res}_{\Delta(E)/K}\mathrm{cor}_{F/K}(a,d)$$

in $\mathrm{Br}(\Delta(E))$.

Proof. This follows from [BCM 03], Proposition 5.3.

2.6. Oriented embeddings

Recall that the existence of an embedding of algebras with involution $(E,\sigma) \to (A,\tau)$ is equivalent with the existence of an element $a \in F^\times$ such that the algebras with involution (A,θ_a) and (A,τ) are isomorphic. We need the stronger notion of oriented embedding, defined as follows :

Definition 2.6.1. Let (A,τ) be an orthogonal involution, and let $\nu : \Delta(E) \to Z(A,\tau)$ be an orientation. An embedding $\iota : (E,\sigma) \to (A,\tau)$ is called an *oriented embedding* with respect to ν if there exist $a \in F^\times$ and $\alpha \in A^\times$ satisfying the following conditions :

(a) $\mathrm{Int}(\alpha) : (A,\theta_a) \to (A,\tau)$ is an isomorphism of algebras with involution such that $\mathrm{Int}(\alpha) \circ \epsilon = \iota$.

(b) The induced automorphism $c(\alpha) : Z(A, \theta_a) \to Z(A, \tau)$ satisfies

$$c(\alpha) \circ u_a = \nu.$$

We say that there exists an oriented embedding of algebras with involution with respect to ν if there exists (ι, a, α) as above. The elements (ι, a, α, ν) are called *parameters* of the oriented embedding.

2.7. Changing the orientation – improper similitudes

Let $\nu : \Delta(E) \to Z(A, \tau)$ be an orientation. We have

Proposition 2.7.1. *Suppose that (A, τ) admits an improper similitude. Assume that there exists an embedding of algebras with involution $(E, \sigma) \to (A, \tau)$. Then there exists an oriented embedding $(E, \sigma) \to (A, \tau)$ with respect to ν. Moreover, if (ι, a, α) are parameters of an embedding of (E, σ) in (A, τ), then there exist ι' and β such that (ι', a, β, ν) are parameters of an oriented embedding.*

Proof. If $c(\alpha) \circ u_a = \nu$, then $(\mathrm{Int}(\alpha) \circ \epsilon, a, \alpha)$ are parameters of an oriented embedding $(E, \sigma) \to (A, \tau)$. Suppose that $c(\alpha) \circ u_a \neq \nu$. Let $\gamma \in A^\times$ be an improper similitude. Then $c(\gamma)$ is not the identity, and hence we have $c(\gamma\alpha) \circ u_a = \nu$. Set $\beta = \gamma\alpha$. Then $(\mathrm{Int}(\beta) \circ \epsilon, a, \beta)$ are parameters of an oriented embedding, as claimed.

Lemma 2.7.2. *Let Suppose that K is a local field or the field of real numbers, and let (A, τ) be an orthogonal involution. Assume that if A is non–split, then $\mathrm{disc}(A, \tau) \neq 1 \in K^\times / K^{\times 2}$. Then (A, τ) admits improper similitudes.*

Proof. If A is split, then any reflection is an improper similitude. Suppose now that A is not split. Then we have $A \simeq M_r(H)$, where H is a quaternion division algebra. Let $Z = Z(A, \tau)$. Set $D = \mathrm{disc}(A, \tau)$, and note that $Z \simeq K(\sqrt{D})$. Then Z is a quadratic extension of K, since $D \notin K^{\times 2}$. Hence H is split by Z. The involution τ is induced by an r–dimensional hermitian form h over H. If $r > 3$, then the hermitian form h is isotropic (see [T 61], Theorem 3, if K is a local field, and [Sch 85], Theorem 10.3.7. if K is the field of real numbers). Therefore $h \simeq h' \oplus h''$, where h' and h'' are hermitian forms over H with $\dim(h') \leq 3$ and h'' hyperbolic. Let $r' = \dim(h')$, and let $B = M_{r'}(H)$. Let τ' be the involution of B induced by h', and note that $\mathrm{disc}(B, \tau') = \mathrm{disc}(A, \tau) = D$. Since H is split by Z, we have $H = (\lambda, D) \in \mathrm{Br}(K)$ for some $\lambda \in K^\times$.

We claim that λ is a multiplier of a similitude of (B, τ'). Indeed, since $r' \leq 3$, we may apply the criterion of [PT 04], Theorem 4. Let $\gamma(B, \tau') \in \mathrm{Br}(K)$ such that $\gamma_Z = C(B', \tau')$ in $\mathrm{Br}(Z)$ (cf. [PT 04], Theorem 2). Then by

[PT 04], Theorem 4, the element λ is the multiplier of a similitude of (B, τ') if and only if $\lambda.\gamma = 0$ in $H^3(K)/(K^\times.A)$. If K is a local field, then $H^3(K) = 0$, hence the condition is fulfilled. Assume that K is the field of real numbers. Then either $\gamma = 0$, or $\gamma = H$ in $\mathrm{Br}(K)$. Since A is non-split, we have $A = H$ in $\mathrm{Br}(K)$. Therefore we have $\lambda.\gamma = 0$ n $H^3(K)/(K^\times.A)$ in both cases.

Therefore by [PT 04], Theorem 4, the element λ is the multiplier of a similitude of (B, τ'), therefore also of the hermitian form h'. The hermitian form h'' is hyperbolic, therefore h'' has a similitude of multiplier λ. Thus the hermitian form h has a similitude of multiplier λ as well, and hence (A, τ) has a similitude of multiplier λ. By [PT 04], Theorem 1, using the fact that $A = H = (\lambda, D) \in \mathrm{Br}_2(K)$, we see that λ is the multiplier of an improper similitude.

Corollary 2.7.3. *Suppose that there exists an embedding of algebras with involution $(E, \sigma) \to (A, \tau)$, and that one of the following holds :*

(i) *A is split.*

(ii) *K is a local field, or the field of real numbers, and* $\mathrm{disc}(A, \tau) \neq 1$ *in $K^\times/K^{\times 2}$.*

Then there exists an oriented embedding $(E, \sigma) \to (A, \tau)$ with respect to ν. Moreover, if (ι, a, α) are parameters of an embedding of (E, σ) in (A, τ) and if then there exist ι' and β such that (ι', a, β, ν) are parameters of an oriented embedding.

Proof. In both cases, (A, τ) admits an improper similitude. If A is split, then any reflection in $\mathrm{U}(A, \tau)$ is an improper similitude. If K is local or the field of real numbers, then Lemma 2.7.2. implies that (A, τ) has an improper similitude. Hence the Corollary follows from Proposition 2.7.1.

2.8. Changing the orientation – r odd

Recall that $E \simeq F[X]/(X^2 - d)$, that $\Delta(E) \simeq K[Y]/(Y^2 - (-1)^r \mathrm{N}_{E/K}(x))$, and that we have fixed the images x of X in E and y of Y in $\Delta(E)$. Recall that $\rho : \Delta(E) \to \Delta(E)$ is the automorphism of $\Delta(E)$ induced by $\sigma : E \to E$, and that ρ is the identity if r is even, and the non–trivial automorphism of $\Delta(E)$ over K if r is odd.

Recall also that $u : \Delta(E) \to Z(A, \theta)$ is defined by $y \mapsto \pi_\theta(\epsilon(x))$.

Lemma 2.8.1. *Let* $\mathrm{Int}(\gamma) : (A, \theta) \to (A, \theta)$ *be an isomorphism of algebras with involution safisfying* $\mathrm{Int}(\gamma) \circ \epsilon \circ \sigma = \epsilon$. *Then we have $c(\gamma) \circ u \circ \rho = u$.*

Proof. It suffices to prove that this is true over a separable closure. Therefore we may assume that $A = M_{2r}(K)$ and that $\theta : A \to A$ is the transposition. We have $\gamma\theta(\gamma) = \gamma\gamma^t = \lambda$ for some $\lambda \in K^\times$. Recall that $\mathrm{Nrd}(\gamma) = \eta\lambda^r$, where

$\eta = 1$ if γ is a proper similitude, and $\eta = -1$ if γ is an improper similitude. We have $\epsilon(x) = \mathrm{Int}(\gamma) \circ \epsilon \circ \sigma(x) = \gamma\epsilon(\sigma(x))\gamma^{-1} = \lambda^{-1}\gamma\epsilon(\sigma(x))\gamma^t$.

On the other hand, we have $\pi_t(\lambda^{-1}\gamma(\epsilon(\sigma(x))\gamma^t) = \lambda^{-r}\mathrm{Nrd}(\gamma)\pi_t(\epsilon(\sigma(x)) = \eta\pi_t(-\epsilon(x)) = (-1)^r\eta\pi_t(\epsilon(x))$. Hence we have $(-1)^r\eta\pi_t(\epsilon(x)) = \pi_t(\epsilon(x))$, thus $\eta = (-1)^r$. This implies that γ is a proper similitude if r is even, and an improper similitude if r is odd. By Lemma 2.4.1. this implies that $c(\gamma)$ is the identity if r is even, and the non–trivial automorphism of $Z(A, \theta)$ if r is odd. Therefore we have $c(\gamma) \circ u \circ \rho(y) = u(y)$, and hence $c(\gamma) \circ u \circ \rho = u$.

Proposition 2.8.2. *Let $a, b \in F^\times$, and let $\mathrm{Int}(\alpha) : (A, \theta_a) \to (A, \tau)$ and $\mathrm{Int}(\beta) : (A, \theta_b) \to (A, \tau)$ be isomorphisms of algebras with involution such that $\mathrm{Int}(\alpha) \circ \epsilon \circ \sigma = \mathrm{Int}(\beta) \circ \epsilon$. Then we have $c(\alpha) \circ u_a \circ \rho = c(\beta) \circ u_b$.*

Proof. Let K_s be a separable closure of K, and let $\gamma_a, \gamma_b \in K_s^\times$ be such that $\mathrm{Int}(\gamma_a) : (A, \theta) \to (A, \theta_a)$ and $\mathrm{Int}(\gamma_b) : (A, \theta) \to (A, \theta_b)$ are isomorphisms of algebras with involution commuting with ϵ. Then we have $u_a = c(\gamma_a) \circ u$ and $u_b = c(\gamma_b) \circ u$. We have $\mathrm{Int}(\gamma_b^{-1}\beta^{-1}\alpha\gamma_a) \circ \epsilon \circ \sigma = \mathrm{Int}(\gamma_b^{-1}\beta^{-1}\alpha) \circ (\mathrm{Int}(\gamma_a)) \circ \epsilon \circ \sigma = \mathrm{Int}(\gamma_b^{-1}\beta^{-1}) \circ \mathrm{Int}(\alpha) \circ \epsilon \circ \sigma = \mathrm{Int}(\gamma_b^{-1}\beta^{-1}) \circ \mathrm{Int}(\beta) \circ \epsilon = \mathrm{Int}(\gamma_b^{-1}) \circ \epsilon = \epsilon$. By Lemma 2.8.1. this implies that $c(\gamma_b^{-1}\beta^{-1}\alpha\gamma_a) \circ u \circ \rho = u$, hence we have $c(\alpha) \circ u_a \circ \rho = c(\beta) \circ u_b$.

Let $\nu : \Delta(E) \to Z(A, \tau)$ be an orientation.

Corollary 2.8.3. *Suppose that r is odd, and that there exists an embedding of algebras with involution $(E, \sigma) \to (A, \tau)$. Then there exists an oriented embedding $(E, \sigma) \to (A, \tau)$ with respect to ν. Moreover, if (ι, a, α) are parameters of an embedding of (E, σ) in (A, τ), then there exist ι', b and β such that (ι', b, β, ν) are parameters of an oriented embedding.*

Proof. Let (ι, a, α) be parameters of an embedding of (E, σ) in (A, τ). If $c(\alpha) \circ u_a = \nu$, then (ι, a, α, ν) are parameters of an oriented embedding with respect to ν. Otherwise, we have $c(\alpha) \circ u_a \circ \rho = \nu$. Set $\iota' = \iota \circ \sigma$. Then there exist $b \in F^\times$ and $\beta \in A^\times$ such that $\iota' = \mathrm{Int}(\beta) \circ \epsilon$. By Proposition 2.8.2. we have $c(\beta) \circ u_b = c(\alpha) \circ u_a \circ \rho = \nu$, and hence (ι', b, β, ν) are parameters of an oriented embedding.

§3. Local conditions

The aim of this section is to give necessary and sufficient conditions for an embedding of (E, σ) in (A, τ) to exist when K is a local field of characteristic $\neq 2$ or the field of real numbers. This is done in [Lee14] in terms of Tits indices - however, the results of [Lee 14] are not used here. We assume that all the factors of E split A. Hence there exists an embedding of algebras $\epsilon : E \to A$, and an involution θ of A of the same type as τ such that $\epsilon : (E, \sigma) \to (A, \theta)$ is an embedding of algebras with involution (cf. Proposition 1.1.2).

Let $E = E_s \times E_n$ where E_s and E_n are étale K–algebras stable under σ with (E_s, σ) split and of maximal rank for this property. Let 2ρ be the rank of E_s.

3.1. Orthogonal involutions – the even dimensional case

Assume that (A, τ) is an orthogonal involution.

Proposition 3.1.1. *Assume that n is even, and that K is a local field. Then there exists an embedding of algebras with involution of (E, σ) into (A, τ) if and only if one of the following conditions holds :*

(i) *(E, σ) is split and (A, τ) is hyperbolic.*

(ii) *(E, σ) is not split, and* $\mathrm{disc}(A, \tau) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$.

Proof. (i) Suppose that (E, σ) is split. Then (E, σ) embeds into (A, τ) if and only if (A, τ) is hyperbolic (cf. Proposition 1.1.7.).

(ii) Suppose that (E, σ) is not split. By Proposition 1.6.1. if (E, σ) can be embedded into (A, τ), then we have $\mathrm{disc}(A, \tau) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$. Conversely, assume that $\mathrm{disc}(A, \tau) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$.

Suppose first that A is split, in other words that $A \simeq M_n(K)$. Then τ is induced by an n–dimensional quadratic form q over K, and we have $\mathrm{disc}(q) = \mathrm{disc}(A, \tau) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$. By [B 12], Proposition 2.2.1. there exists $a \in F^\times$ such that $w(T_a) = w(q) \in \mathrm{Br}_2(K)$. We have $\mathrm{disc}(T_a) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$ (cf. [B 12], Lemma 1.3.2.) Therefore the quadratic forms q and T_a have the same dimension, discriminant and Hasse invariant, hence they are isomorphic. Thus (E, σ) embeds into (A, τ) (cf. Proposition 1.4.1.).

Suppose now that A is not split. Since K is a local field, we have $A = M_r(H)$ with H a quaternion division algebra. By Proposition 1.6.1. we have $\mathrm{disc}(A, \theta) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$. Therefore $\mathrm{disc}(A, \tau) = \mathrm{disc}(A, \theta)$. By [T 61], Theorem 3, this implies that $(A, \tau) \simeq (A, \theta)$. Therefore (E, σ) embeds into (A, τ). This completes the proof of the Proposition.

Proposition 3.1.2. *Suppose that $K = \mathbf{R}$ and that n is even. Then there exists an embedding of (E, σ) in (A, τ) if and only one of the following conditions hold :*

(i) *$A \simeq M_n(\mathbf{R})$, the involution τ is induced by the quadratic form q, and the signature of q is of the shape $(2r + \rho, 2s + \rho)$ for some non–negative integers r and s.*

(ii) *$A \simeq M_r(H)$, where H is a quaternion division algebra.*

Proof. If $A \simeq M_n(\mathbf{R})$, then the result follows from [B 12], Proposition 2.3.2. Assume that $A \simeq M_r(H)$. Then by [Sch 85], Theorem 10.3.7. we have $(A, \tau) \simeq (A, \theta)$. Therefore (E, σ) can be embedded in (A, τ).

3.2. Orthogonal involutions – the odd dimensional case

Assume that (A, τ) is an orthogonal involution, and that n is odd. Then we have $A \simeq M_n(K)$, and τ is induced by an n–dimensional quadratic form q. We have $E = E' \times K$, where E' is a rank $n-1$ étale K–algebra invariant by σ. If $n = 1$, then $E = K$ and σ is the identity. In this case, it is clear that there exists an embedding of (E, σ) into (A, τ). Suppose that $n \geq 3$, and let $F' = (E')^\sigma$ be the subalgebra of E' composed of the elements fixed by the restriction of σ to E'. We have the following :

Proposition 3.2.1. *Assume that n is odd and $n \geq 3$, and that K is a local field. Then there exists an embedding of (E, σ) in (A, τ) if and only if one of the following holds :*

(i) *(E', σ) is split, and $q \simeq q' \oplus q''$ with $\dim(q') = n-1$ and q' hyperbolic.*

(ii) *(E', σ) is not split.*

Proof. Suppose that (E, σ) embeds into (A, τ). Then by Proposition 1.4.1. there exists $a \in F^\times$ such that $q \simeq T_a$. We have $F = F' \times K$, and $a = (a', a'')$ with $a' \in (F')^\times$ and $a'' \in K^\times$. Note that we have $T_a \simeq T_{a'} \oplus T_{a''}$. Let $A' = M_{n-1}(K)$, and let τ' be the involution of A' induced by $T_{a'}$. Then (E', σ) embeds into (A', τ'). If (E', σ) is split, then by Proposition 3.1.1. (i), the quadratic form $T_{a'}$ is hyperbolic. Set $q' = T_{a'}$ and $q'' = T_{a''}$; then we have $q \simeq q' \oplus q''$ with $\dim(q') = n-1$ and q' hyperbolic, as claimed.

Conversely, suppose that if (E', σ) is split, then $q \simeq q' \oplus q''$ with $\dim(q') = n-1$ and q' hyperbolic, and let us prove that embeds (E, σ) into (A, τ). Let us show that we have $q \simeq T_{a'} \oplus T_{a''}$ with $a' \in (F')^\times$ and $a'' \in K^\times$. Suppose first that (E', σ) is split. Then we have $q \simeq q' \oplus q''$ with $\dim(q') = n-1$ and q' hyperbolic. Let $A' = M_{n-1}(K)$ and let τ' be the involution induced by q'. Then Proposition 3.1.1. (i) implies that (E', σ) embeds into (A', τ'). Therefore by Proposition 1.4.1. there exists $a' \in (F')^\times$ such that $q' \simeq T_{a'}$. Note that as $\dim(q'') = 1$, there exists $a'' \in K^\times$ such that $q'' \simeq T_{a''}$, hence the statement is proved in this case. Suppose now that (E', σ) is not split, and set $a'' = (-1)^{\frac{n-1}{2}} \det(q) \mathrm{disc}(E') \in K^\times / K^{\times 2}$. Since K is a local field, there exist quadratic forms q' and q'' with $q \simeq q' \oplus q''$, $\dim(q') = n-1$, $\dim(q'') = 1$, and $\det(q'') = a''$. This is clear if $n \geq 5$, since a non–degenerate quadratic form of dimension ≥ 5 over a local field represents all non–zero elements. Assume that $n = 3$. Then $a'' = -\det(q)\mathrm{disc}(E')$. Since (E', σ) is not split, we have $\mathrm{disc}(E') \notin K^{\times 2}$. The quadratic form $q \oplus < \det(q)\mathrm{disc}(E') >$ has dimension 4 and non–square discriminant, hence it is isotropic (see for instance [Sch 85], Theorem 6.4.2. page 217). Hence q represents $a'' = -\det(q)\mathrm{disc}(E')$, as claimed. This implies that $\mathrm{disc}(q') = \mathrm{disc}(E')$. Set $A' = M_{n-1}(K)$, and let τ' be the involution of A' induced by q'. Then Proposition 3.1.1. (ii) implies

that (E', σ) embeds into (A', τ'). By Proposition 1.4.1. we have $q' \simeq T_{a'}$ for some $a' \in (F')^\times$. Note that as $\dim(q'') = 1$, we have $q'' \simeq T_{a''}$.

Therefore in both cases we have $q \simeq T_{a'} \oplus T_{a''}$ with $a' \in (F')^\times$ and $a'' \in K^\times$. Set $a = (a', a'')$. Then $q \simeq q_a$, and by Proposition 1.4.1. there exists an embedding of (E, σ) in (A, τ). This completes the proof of the Proposition.

Proposition 3.2.2. *Suppose that $K = \mathbf{R}$ and that n is odd. Then there exists an embedding of (E, σ) in (A, τ) if and only if the signature of q is of the shape $(r + \rho, s + \rho)$ for some non–negative integers r and s.*

Proof. We have $E = E' \times \mathbf{R}$, where E' is a rank $n - 1$ étale $\mathbf{R}$–algebra invariant by σ. Let F' be the subalgebra of E' of the elements fixed by σ. Assume that there exists an embedding of (E, σ) in (A, τ). Then by Proposition 1.4.1. there exists $a \in F^\times$ such that $q \simeq T_a$. We have $F = F' \times \mathbf{R}$, and $a = (a', a'')$ with $a' \in (F')^\times$ and $a'' \in \mathbf{R}^\times$. Let $A' = M_{n-1}(K)$, and let τ' be the involution of A' induced by $T_{a'}$. Then by Proposition 1.4.1. there exists an embedding of (E', σ) in (A', τ'). By Proposition 3.1.2. this implies that the signature of $T_{a'}$ is of the shape $(2r' + \rho, 2s' + \rho)$ for some non–negative integers r' and s'. Therefore the signature of q is $(2r' + 1 + \rho, 2s' + \rho)$ or $(2r' + \rho, 2s' + 1 + \rho)$.

Conversely, assume that the signature of q is of the shape $(r + \rho, s + \rho)$ for some non–negative integers r and s. Then $r + s + 2\rho = n$, hence one of r or s is odd and the other is even. Let q' be a quadratic form of signature $(r-1+\rho, s+\rho)$ if r is odd, and $(r+\rho, s-1+\rho)$ if s is odd. Then the dimension of q' is even, and hence by Proposition 2.1.3. there exists an embedding of (E', σ) in (A', τ'), where $A' = M_{n-1}(K)$, and where τ' is the involution of A' induced by q'. Therefore by Proposition 1.4.1. there exists $a' \in (F')^\times$ such that $q' \simeq T_{a'}$. Set $a'' = 1$ if r is odd and $a'' = -1$ if s is odd, and let $a = (a', a'')$. Then q and T_a have the same signature, hence they are isomorphic. By Proposition 3.1.2.. this implies that there exists an embedding of (E, σ) in (A, τ).

3.3. The symplectic case

Assume that (A, τ) is a symplectic involution. If $A \simeq M_r(D)$ for some quaternion division algebra D, let h be a hermitian form with respect to the canonical involution of D which induces τ. The signature of h is defined as in [Sch 85], 10.1.8. (i). Let $E = E_s \times E_n$, where E_s and E_n are stable under σ such that (E_s, σ) is split and (E_n, σ) is non-split. Let 4ρ be the rank of E_s.

Theorem 3.3.1. *Suppose that K is a local field, or $K = \mathbf{R}$. Then (E, σ) can be embedded in (A, τ) if and only if one of the following holds :*

(i) *K is a local field, or A is split.*

(ii) *$K = \mathbf{R}$, A is non–split, and* $\mathrm{sign}(h)$ *is of the shape $(s+\rho, s'+\rho)$, where s and s' are non–negative integers.*

Proof.(i) If A is split, then the involutions are given by skew–symmetric matrices with coefficients in K. All non–degenerate skew–symmetric matrices of the same dimension are isomorphic. Hence the algebras with involution (A,τ) and (A,θ) are isomorphic, therefore (E,σ) can be embedded in (A,τ). Suppose that $A = M_r(D)$, where D is the unique quaternion division algebra over K, and that K is a local field. By [Sch 85], 10.1.7. the algebras with involution (A,τ) and (A,θ) are isomorphic. Therefore (E,σ) can be embedded in (A,τ).

(ii) Suppose that K is the field of real numbers and that $A = M_r(D)$, where D is the unique quaternion division algebra over K. Since all the factors of E split A, the étale algebra E is isomorphic to the direct product of r copies of $\mathbf{C}$. Hence we have $E_s = (\mathbf{C}\times\mathbf{C})^\rho$, and σ acts on each copy of $\mathbf{C}\times\mathbf{C}$ by exchanging the two factors, and we have $E_n = \mathbf{C}^{r-2\rho}$, and σ acts on each copy of $\mathbf{C}$ by complex conjugation. Set $F_s = E_s^\sigma$ and $F_n = E_n^\sigma$. Then we have $F_s \simeq \mathbf{C}^\rho$ and $F_n \simeq \mathbf{R}^{r-2\rho}$.

Let us consider the following hermitian forms with respect to the canonical involution of D : let h_1 be the 2ρ–dimensional hyperbolic form, and let h_2 be the $r-2\rho$–dimensional unit form. Let h_0 be the orthogonal sum of h_1 and h_2, and let $\theta : A \to A$ be the involution induced by h_0.

Let us denote by $x \mapsto \overline{x}$ the canonical involution of D, and let $\epsilon : E_s \times E_n \to A$ be the map defined by

$$\alpha(x_1, y_1, \ldots, x_\rho, y_\rho, z_1, \ldots, x_{r-2\rho}) = \mathrm{diag}(x_1, \overline{y}_1, \ldots, x_\rho, \overline{y}_\rho, z_1, \ldots, z_{r-2\rho}).$$

It is easy to check that ϵ is an embedding of algebras with involution $(E,\sigma) \to (A,\theta)$.

If $c_1, \ldots, c_{r-2\rho} \in \mathbf{R}$, let us denote by h_c the $r-2\rho$–dimensional diagonal hermitian form $< c_1, \ldots, c_{r-2\rho} >$. Let H_c be the orthogonal sum of the 2ρ–dimensional hyperbolic hermitian form with h_c. For $a = (b_1, \ldots, b_\rho) \times (c_1, \ldots, c_{r-2\rho}) \in {F_s}^\times \times {F_n}^\times$, we see that the involution $\theta_a : A \to A$ is induced by the hermitian form H_c. Note that the signature of H_c is equal to $(\rho+s, \rho+s')$, where s is the number of positive c_i's, and s' the number of negative c_i's. By Proposition 1.1.3. there exists an embedding of algebras with involution $(E,\sigma) \to (A,\tau)$ if and only if there exists $a \in F^\times$ such that $(A,\theta_a) \simeq (A,\tau)$. By [Sch 85], 10.1.7. and 10.1.8. (i), this is equivalent with the existence of $a \in F^\times$ such that $\mathrm{sign}(h_a) = \mathrm{sign}(h)$. Therefore there exists an

embedding of algebras with involution $(E,\sigma) \to (A,\tau)$ if and only if $\mathrm{sign}(h)$ is of the shape $(s+\rho, s'+\rho)$, where s and s' are non–negative integers.

3.4. The unitary case

Assume that L is a quadratic extension of K, and suppose that (A,τ) is an L/K unitary involution. Assume that $A = M_n(L)$, and that τ is induced by an n–dimensional hermitian form h over L/K (note that when K is a local field or $K = \mathbf{R}$, then this hypothesis is always fulfilled).

Proposition 3.4.1. *Suppose that K is a local field. Then there exists an embedding of algebras with involution of (E,σ) into (A,τ) if and only if one of the following conditions holds :*

(i) *(E,σ) is split and (A,τ) is hyperbolic.*

(ii) *(E,σ) is not split, and* $\det(A,\tau)\mathrm{disc}(E,\sigma)^{-1} \in \mathrm{N}_{F/K}(F^\times)\mathrm{N}_{L/K}(L^\times)$.

Proof. (i) follows from Proposition 1.1.7. Suppose that (E,σ) is not split, and that (E,σ) embeds into (A,τ). Then by Proposition 1.6.2. we have

$$\det(A,\tau)\mathrm{disc}(E,\sigma)^{-1} \in \mathrm{N}_{F/K}(F^\times)\mathrm{N}_{L/K}(L^\times).$$

Conversely, assume that $\det(A,\tau)\mathrm{disc}(E,\sigma)^{-1} \in \mathrm{N}_{F/K}(F^\times)\mathrm{N}_{L/K}(L^\times)$. Then there exists $a \in F^\times$ such that $\det(A,\tau) = \mathrm{N}_{F/K}(a)\mathrm{disc}(E,\sigma) \in K^\times/\mathrm{N}_{L/K}(L^\times)$. We have $\det(T_a) = \det(A,\tau)$, hence h and T_a have equal dimension and determinant. Since K is a local field, this implies that $T_a \simeq h$. By Proposition 1.4.1. there exists an embedding of (E,σ) into (A,τ). This completes the proof of the proposition.

Recall that $E = E_s \times E_n$ where E_s and E_n are étale K–algebras stable under σ with (E_s,σ) split and of maximal rank for this property, and that we denote by 2ρ the rank of E_s.

Proposition 3.4.2. *Suppose that $K = \mathbf{R}$. Then there exists an embedding of algebras with involution of (E,σ) into (A,τ) if and only if the signature of h is of the shape $(r+\rho, s+\rho)$ for some non–negative integers r and s.*

Proof. Indeed, since L/K is a quadratic field extension, we have $L = \mathbf{C}$. Therefore E is isomorphic to the direct product of n copies of $\mathbf{C}$. Let us denote by $\sigma_0 : \mathbf{C} \to \mathbf{C}$ the complex conjugation, and by $\sigma_1 : \mathbf{C}\times\mathbf{C} \to \mathbf{C}\times\mathbf{C}$ the map defined by $\sigma_1(a,b) = (\sigma_0(b), \sigma_0(a))$. Then we have $E_s = (\mathbf{C}\times\mathbf{C})^\rho$, and the restriction of $\sigma : E_s \to E_s$ to each copy of $\mathbf{C}\times\mathbf{C}$ is equal to σ_1 ; we have $E_n = \mathbf{C}^{n-2\rho}$, and the restriction of $\sigma : E_n \to E_n$ to each copy of $\mathbf{C}$ is equal to σ_0.

Set $F_s = E_s^\sigma$ and $F_n = E_n^\sigma$. Note that $F = F_s \times F_n$, and that $F_s = \mathbf{C}^\rho$ and $F_n = \mathbf{R}^{n-\rho}$. Let $a = (a_s, a_n) \in F_s^\times \times F_n^\times$. Then the restriction of T_a :

$E \times E \to K$ to E_s is hyperbolic with signature (ρ, ρ), and its restriction to E_n has signature (r_a, s_a), where r_a (respectively s_a) is the number of positive (respectively negative) coefficients of $a_n \in \mathbf{R}^{n-2\rho}$. Hence the signature of T_a is $(\rho+r_a, \rho+s_a)$. By Proposition 1.4.1. there exists an embedding of (E, σ) into (A, τ) if and only if $h \simeq T_a$ for some $a \in F^\times$. Hence (E, σ) can be embedded into (A, τ) if and only if the signature of h is of the shape $(\rho + r, \rho + s)$ for some non-negative integers r and s.

§4. The Tate–Shafarevich group

We keep the notation of the previous sections, and suppose that K is a global field. Recall that either $L = K$, or L is a quadratic extension of K. The aim of this section is to define a group that measures the failure of the Hasse principle.

Let us denote by Ω_K the set of places of K. For all $v \in \Omega_K$, we denote by K_v the completion of K at v. For all K–algebras B, set $B^v = B \otimes_K K_v$.

The commutative étale algebra E is by definition a product of separable field extensions of L. Let us write $E = E_1 \times \cdots \times E_m$, with $\sigma(E_i) = E_i$ for all $i = 1, \ldots, m$, and such that E_i is either a field stable by σ or a product of two fields exchanged by σ. Recall that $F = E^\sigma$.

Set $I = \{1, \ldots, m\}$. We have $F = F_1 \times \cdots \times F_m$, where F_i is the fixed field of σ in E_i for all $i \in I$. Note that either $E_i = F_i = K$, $E_i = F_i \times F_i$ or E_i is a quadratic field extension of F_i. For all $i \in I$, let $d_i \in F_i^\times$ such that $E_i = F_i(\sqrt{d_i})$ if E_i/F_i is a quadratic extension, and $d_i = 1$ otherwise. Set $d = (d_1, \ldots, d_m)$.

If $i \in I$ is such that E_i is a quadratic extension of F_i, let Σ_i be the set of places $v \in \Omega_K$ such that all the places of F_i over v split in E_i. If $E_i = F_i \times F_i$ or if $E_i = K$, set $\Sigma_i = \Omega_K$.

If $L \neq K$, let $\Sigma(L/K)$ be the set of places of K that split in L. If $L = K$, then we set $\Sigma(L/K) = \emptyset$.

Given an m-tuple $x = (x_1, ..., x_m) \in (\mathbf{Z}/2\mathbf{Z})^m$, set

$$I_0 = I_0(x) = \{i \mid x_i = 0\},$$

$$I_1 = I_1(x) = \{i \mid x_i = 1\}.$$

Note that (I_0, I_1) is a partition of I. Let S' be the set

$$S' = \{(x_1, ..., x_m) \in (\mathbf{Z}/2\mathbf{Z})^m \mid \Sigma(L/K) \cup (\bigcap_{i \in I_0} \Sigma_i) \cup (\bigcap_{j \in I_1} \Sigma_j) = \Omega_K\},$$

and set

$$S = S' \cup (0, ..., 0) \cup (1, ..., 1).$$

We define an equivalence relation on S by

$$(x_1, ..., x_m) \sim (x'_1, ..., x'_m) \text{ if } (x_1, ..., x_m) + (x'_1, ..., x'_m) = (1, ..., 1).$$

Let us denote by $Ш = Ш(E, \sigma)$ the set of equivalence classes of S under the above equivalence relation.

For all $x \in S$, we denote by x its class in Ш, and by $(I_0(x), I_1(x))$ the corresponding partition of I. Let us denote by P' the set of non–trivial partitions (I_0, I_1) of I such that $\Sigma(L/K) \cup (\underset{i \in I_0}{\cap} \Sigma_i) \cup (\underset{j \in I_1}{\cap} \Sigma_j) = \Omega_K$, and set $P = P' \cup \{(I, \emptyset)\} \cup \{\emptyset, I)\}$. Let us define an equivalence relation on P by $(I_0, I_1) \sim (I_1, I_0)$. Sending x to $(I_0(x), I_1(x))$ induces a bijection between Ш and the set of equivalence classes of P under this equivalence relation.

Componentwise addition gives a group structure on the set of equivalence classes of $(\mathbf{Z}/2\mathbf{Z})^m$. Let us denote this group by $(C_m, +)$. We have

Lemma 4.1.1. *The set* Ш *is a subgroup of* C_m.

Proof. It is clear that the class of $(0, \ldots, 0)$ is the neutral element, and that every element is its own opposite, so we only need to check that the sum of two elements of Ш is again in Ш. If J is a subset of I, set $\Omega(J) = \underset{i \in J}{\cap} \Sigma_i$. As we have seen above, the set Ш is in bijection with the set of equivalence classes of partitions $P/\sim$. Moreover, the transport of structure induces

$$(I_0, I_1) + (I'_0, I'_1) = ((I_0 \cap I'_0) \cup (I_1 \cap I'_1), (I_0 \cap I'_1) \cup (I_1 \cap I'_0)).$$

Let us show that this is an element of $P/\sim$. This is equivalent with proving that Ω_K is equal to

$$\Sigma(L/K) \cup [(\Omega(I_0 \cap I'_0)) \cap (\Omega(I_1 \cap I'_1))] \cup [(\Omega(I_0 \cap I'_1)) \cap (\Omega(I'_0 \cap I_1))],$$

and this follows from the equalities

$$\Sigma(L/K) \cup \Omega(I_0) \cup \Omega(I_1) = \Omega_K,$$

and

$$\Sigma(L/K) \cup \Omega(I'_0) \cup \Omega(I'_1) = \Omega_K,$$

which hold as (I_0, I_1) and (I'_0, I'_1) are in $P/\sim$.

The following propositions will be used in Sections 6 and 8 in order to give necessary and sufficient conditions for the Hasse principle to hold. Let us start with introducing some notation.

Set $\mathcal{C}_I = \{(i,j) \in I \times I \mid i \neq j \text{ and } \Sigma(L/K) \cup \Sigma_i \cup \Sigma_j \neq \Omega_K\}$. For any subset J of I, we say that $i, j \in J$ are *connected in* J if there exist $j_1, \ldots, j_k \in J$ with $j_1 = i$, $j_k = j$ and $(j_r, j_{r+1}) \in \mathcal{C}_I$ for all $r = 1, \ldots, k-1$.

Lemma 4.1.2. *Let $(i,j) \in \mathcal{C}_I$, and let $v \in \Omega_K$ such that $v \notin \Sigma(L/K) \cup \Sigma_i \cup \Sigma_j$. Let $a_r^u \in (F_r^u)^\times$ for all $r \in I$ and $u \in \Omega_K$. Then there exist $b_r^u \in (F_r^u)^\times$ such that*

- *$b_r^u = a_r^u$ whenever $u \neq v$ or $r \neq i, j$, and*
- *$\mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) \neq \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$, $\mathrm{cor}_{F_i^v/K_v}(b_j^v, d_j) \neq \mathrm{cor}_{F_i^v/K_v}(a_j^v, d_j)$.*

In particular, we have

$$\Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i),$$

$$\Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_j^v/K_v}(a_j^v, d_j) \neq \Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_j^v/K_v}(b_j^v, d_j).$$

Proof. Since $(i,j) \in \mathcal{C}_I$, we have $\Sigma(L/K) \cup \Sigma_i \cup \Sigma_j \neq \Omega_K$. Hence by Chebotarev's density theorem, the complement of the set $\Sigma(L/K) \cup \Sigma_i \cup \Sigma_j$ contains finite places. Let us choose a finite place v of K such that $v \notin \Sigma(L/K) \cup \Sigma_i \cup \Sigma_j$. As $v \notin \Sigma_i$, we have $E_i^v = E_i' \times M$, where M is a field stable by σ, and $M^\sigma \neq M$. Set $M_0 = M^\sigma$. Similarly, we have $E_j^v = E_j' \times N$, where N is a field stable by σ, and $N^\sigma \neq N$. Set $N_0 = N^\sigma$. Then M/M_0 and N/N_0 are quadratic extensions of local fields. Let $\gamma \in M_0$ such that $\gamma \notin \mathrm{N}_{M/M_0}(M)$, and let $\delta \in N_0$ such that $\delta \notin \mathrm{N}_{N/N_0}(N)$. Let us write $a_i^v = (\alpha_1, \alpha_2)$ with $\alpha_1 \in (E_i')^\sigma$, $\alpha_2 \in M_0$, and $a_j^v = (\beta_1, \beta_2)$ with $\beta_1 \in (E_j')^\sigma$, $\beta_2 \in N_0$.

Set $b_i^v = (\alpha_1, \alpha_2\gamma)$ and $b_j^v = (\beta_1, \beta_2\delta)$. If $r \in I$ is such that $r \neq i, j$, then set $b_r^v = a_r^v$. For all $u \neq v$, set $b_r^u = a_r^u$ for all $r \in I$. Then $b_r^u \in (F_r^u)^\times$ have the required properties for all $u \in \Omega_K$ and $r \in I$. This completes the proof of the Lemma.

Proposition 4.1.3. Let $i, j \in I$ be connected, and let $a_r^u \in (F_r^u)^\times$ for all $r \in I$ and $u \in \Omega_K$. Then there exist $b_r^u \in (F_r^u)^\times$ satisfying the following conditions

(i) $\Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i)$.

(ii) $\Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_j^v/K_v}(a_j^v, d_j) \neq \Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_j^v/K_v}(b_j^v, d_j)$.

(iii) If $r \neq i, j$, then we have $\Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_r^v/K_v}(a_r^v, d_r) = \Sigma_{v \in \Omega_K} \ \mathrm{cor}_{F_r^v/K_v}(b_r^v, d_r)$.

(iv) For all $v \in \Omega_K$, we have $\Sigma_{i \in I} \ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \Sigma_{i \in I} \ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$.

(v) If v is an infinite place of K, then $b_r^v = a_r^v$ for all $r \in I$.

Proof. Let $j_1, \ldots, j_k \in J$ with $j_1 = i$, $j_k = j$ and $(j_s, j_{s+1}) \in \mathcal{C}_I$ for all $s = 1, \ldots, k-1$. Starting with $a_r^u \in (F_r^u)^\times$, let us apply Lemma 4.1.2.

successively to each of the pairs (j_s, j_{s+1}), and let $b_r^u \in (F_r^u)^\times$ be the elements obtained at the end of the process.

Note that if $s \neq 1, k$, then we applied Lemma 4.1.2. twice. Hence we have

$$\mathrm{cor}_{F_{j_s}^v/K_v}(b_{j_s}^v, d_{j_s}) = \mathrm{cor}_{F_{j_s}^v/K_v}(a_{j_s}^v, d_{j_s})$$

for $s \neq 1, k$ and for all $v \in \Omega_K$.

On the other hand, if $s = 1$ or $s = k$, then we applied Lemma 4.1.2. only once. Note also that $j_1 = i$ and $j_k = j$. Therefore we have

$$\mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) \neq \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$$

for a certain $v \in \Omega_K$, and

$$\mathrm{cor}_{F_i^v/K_v}(b_i^u, d_i) = \mathrm{cor}_{F_i^v/K_v}(a_i^u, d_i)$$

for all $u \in \Omega_K$ with $u \neq v$. Similarly, we have

$$\mathrm{cor}_{F_j^w/K_w}(b_j^w, d_j) \neq \mathrm{cor}_{F_j^w/K_w}(a_j^w, d_j)$$

for a certain $w \in \Omega_K$, and

$$\mathrm{cor}_{F_j^u/K_u}(b_j^u, d_j) = \mathrm{cor}_{F_j^u/K_u}(a_j^u, d_j)$$

for all $u \in \Omega_K$ with $u \neq w$. Therefore we have

$$\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i),$$

$$\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_j^v/K_v}(a_j^v, d_j) \neq \Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_j^v/K_v}(b_j^v, d_j).$$

Note that $b_r^v = a_r^v$ for all $v \in \Omega_K$ if $r \neq i, j$, hence we have

$$\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_r^v/K_v}(a_r^v, d_r) = \Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_r^v/K_v}(b_r^v, d_r).$$

Moreover, all the applications of Lemma 4.1.2. concern a place $v \in \Omega_K$ and two distinct indices $(j_s, j_{s+1}) \in \mathcal{C}_I$. This implies that for all $v \in \Omega_K$, we have

$$\Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$$

All the changes were made at finite places, hence we have $b_r^v = a_r^v$ for all $r \in I$ if v is an infinite place. This completes the proof of the Proposition.

Proposition 4.1.4. *Let $a_i^v \in (F_i^v)^\times$ for all $v \in \Omega_K$, $i \in I$, such that :*
(i) *We have*

$$\Sigma_{v\in\Omega_K}\Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0.$$

(ii) *For all* $x \in Ш$*, we have*

$$\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0(x)}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0.$$

Then there exist $b_i^v \in F_i^v$ *for all* $v \in \Omega_K$*,* $i \in I$ *such that :*

(iii) *For all* $i \in I$*, we have*

$$\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0.$$

(iv) For all $v \in \Omega_K$, we have

$$\Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i).$$

(v) if v is an infinite place of K, then $b_i^v = a_i^v$.

Proof. For all $i \in I$, set $C_i = C_i(a) = \Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$. If $C_i = 0$ for all $i \in I$, we set $b_i^v = a_i^v$ for all $i \in I$ and $v \in \Omega_K$. If not, then we construct a connected graph with vertex set $\mathcal{V}$ and edge set $\mathcal{E}$ in order to make successive modifications.

Our aim is to construct a graph containing two elements $i_0, i_k \in I$ such that $C_{i_0} = C_{i_k} = 1$ and that i_0 and i_k are connected within the graph.

Let us now construct the desired graph with vertex set $\mathcal{V}$ and edge set $\mathcal{E}$. We start with the empty graph, and add edges and vertices as follows. Let us choose $i_0 \in I$ such that $C_{i_0} = 1$, and add $\{i_0\}$ to $\mathcal{V}$. Set $I_0 = \{i_0\}$ and $I_1 = I - I_0$. Note that $(I_0, I_1) \notin Ш$. Indeed, if $(I_0, I_1) \in Ш$, then by (ii) we have $\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0$. But $\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = C_{i_0}$, and $C_{i_0} = 1$, so this leads to a contradiction. Therefore by definition of Ш, we have

$$\Sigma(L/K) \cup (\bigcap_{i\in I_0} \Sigma_i) \cup (\bigcap_{j\in I_1} \Sigma_j) \neq \Omega_K.$$

Hence there exist $i_1 \in I_1$ and $v \in \Omega_K$ such that $v \notin \Sigma(L/K) \cup \Sigma_{i_0} \cup \Sigma_{i_1}$. In other words, we have $(i_0, i_1) \in \mathcal{C}_I$, hence i_0 and i_1 are connected. Add $\{i_1\}$ to $\mathcal{V}$, and add the edge connecting i_0 to i_1 to $\mathcal{E}$. If $C_{i_1} = 1$, we stop. If not, set $I_0 = \{i_0, i_1\}$ and $I_1 = I - I_0$. We again have $(I_0, I_1) \notin Ш$. Indeed, if $(I_0, I_1) \in Ш$, then by (ii) we have $\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0$. But $\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = C_{i_0} + C_{i_1}$, and $C_{i_0} = 1$, $C_{i_1} = 0$, so this is again a contradiction. Therefore by definition of Ш, we have

$$\Sigma(L/K) \cup (\bigcap_{i\in I_0} \Sigma_i) \cup (\bigcap_{j\in I_1} \Sigma_j) \neq \Omega_K.$$

Hence there exists $i_2 \in I_1$ and $v \in \Omega_K$ such that $v \notin \Sigma(L/K) \cup (\bigcap_{i\in I_0} \Sigma_i) \cup \Sigma_{i_2}$. This implies that at least one of $(i_0, i_2), (i_1, i_2)$ belong to $\mathcal{C}_I$. We now add i_2

to $\mathcal{V}$, and add to $\mathcal{E}$ all the edges connecting j to i_2 with $j \in \mathcal{V}$ such that $(j, i_2) \in \mathcal{C}_I$. Note that i_0 and i_2 are connected within the graph. We continue this way, adding vertices to $\mathcal{V}$ and edges to $\mathcal{E}$. Since I is finite, and since by (i) there exists $j \in I$ with $j \neq i_0$ and $C_j = 1$, the process will stop after a finite number of steps.

In other words, after a finite number of steps we find $i_k \in I$ such that $C_{i_k} = 1$, and such that the resulting graph with vertices $\mathcal{V}$ and edges $\mathcal{E}$ has the following property : there exists a loop–free path in $\mathcal{E}$ connecting i_0 to i_k such that for any two adjacent vertices $i, j \in \mathcal{V}$ we have $(i, j) \in \mathcal{C}_I$. In other words, i_0 and i_k are connected in $\mathcal{V}$. By Proposition 4.1.3. this implies that there exist $c_i^v \in F_i^v$ for all $v \in \Omega_K$, $i \in I$ such that for $(c) = (c_i^v)$ we have $C_{i_0}(c) = C_{i_k}(c) = 0$ and $C_i(c) = C_i(a)$ for all $i \neq i_0, i_k$. Therefore the number of $i \in I$ with $C_i(c) = 1$ is less than the number of $i \in I$ with $C_i(a) = 1$. Moreover, for all $v \in \Omega_K$, we have $\Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(c_i^v, d_i) = \Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$, and that if v is an infinite place, then $c_i^v = a_i^v$ for all $i \in I$. Continuing this way leads to the desired conclusion : we obtain $b_i^v \in F_i^v$ for all $v \in \Omega_K$, $i \in I$ such that for $(b) = (b_i^v)$ we have $C_i(b) = \Sigma_{v \in \Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0$, for all $i \in I$, and this implies (iii). Note that for all $v \in \Omega_K$, we have $\Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$. This implies that (iv) holds. Moreover, all the modifications were made at finite places, hence (v) holds.

Proposition 4.1.5. *Let $a_i^v \in (F_i^v)^\times$ for all $v \in \Omega_K$, $i \in I$, such that :*
(i) *We have*

$$\Sigma_{v \in \Omega_K} \Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0.$$

(ii) *For all $x \in Ш$, we have*

$$\Sigma_{v \in \Omega_K} \Sigma_{i \in I_0(x)}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0.$$

Then for all $i \in I$, there exist $b_i \in F_i^\times$ such that
(iii) *For all $v \in \Omega_K$, we have*

$$\Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(b_i, d_i) = \Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i).$$

Proof. By Proposition 4.1.4. conditions (i) and (ii) imply that for all $v \in \Omega_K$ and all $i \in I$, there exist $b_i^v \in (F_i^v)^\times$ such that for all $i \in I$, we have $\Sigma_{v \in \Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0$, and that for all $v \in \Omega_K$, we have

$$\Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \Sigma_{i \in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i).$$

Let $i \in I$. Since $\Sigma_{v \in \Omega_K}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0$, we have $\Sigma_{w \in \Omega_{F_i}}(b_i^w, d_i) = 0$. The Brauer–Hasse–Noether Theorem implies that there exists a quaternion

algebra Q_i over F_i such that for all $v \in \Omega_K$, we have $Q_i \simeq (b_i^v, d_i)$. Since Q_i^v splits over E_i^v for all $v \in \Omega_K$, the algebra Q_i splits over E_i. Therefore there exists $b_i \in (F_i)^\times$ such that $Q_i \simeq (b_i, d_i)$.

Then, for all $v \in \Omega_K$, we have

$$\Sigma_{i\in I}\ \mathrm{cor}_{F_i/K}(b_i, d_i) = \Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \Sigma_{i\in I}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i).$$

Therefore (iii) holds. This completes the proof of the proposition.

5. The Brauer–Manin map

Assume that K is a global field, and that (E^v, σ) can be embedded in (A^v, τ) for all $v \in \Omega_K$. This implies that there exists an embedding of algebras $\epsilon : E \to A$. By Proposition 1.1.2. there exists an involution $\theta : A \to A$ of the same type as τ such that ϵ induces an embedding of algebras with involution $(E, \sigma) \to (A, \theta)$. Let us fix such an involution θ. If $A \simeq M_n(K)$ and if τ is an orthogonal involution, then let us chose for θ the involution induced by the quadratic form $T : E \times E$, given by $T(x, y) = \mathrm{Tr}_{E/K}(x\sigma(y))$ for all $x, y \in E$. Note that this is possible by Proposition 1.4.1.

The aim of this section is to define a map $Ш(E, \sigma) \to \mathbf{Z}/2\mathbf{Z}$ the vanishing of which is a necessary and sufficient condition for the existence of an embedding of algebras with involution $(E, \sigma) \to (A, \tau)$. To define this map, we need the notion of *embedding data* (cf. 5.1.-5.3.). The Brauer–Manin map is defined in 5.4.

5.1. Local embedding data – even degree orthogonal case

Assume that (A, τ) is an orthogonal involution, with A of degree n. Assume that n is even, and set $n = 2r$. Let us fix an isomorphism of K–algebras $u : \Delta(E) \to Z(A, \theta)$, and recall (cf. 2.5.) that for all $a^v \in (F^v)^\times$ this induces a uniquely defined isomorphism of K_v–algebras $u_{a^v} : \Delta(E^v) \to Z(A, \theta_{a^v})$.

We are assuming that for all $v \in \Omega_K$, there exists an embedding of algebras with involution $(E^v, \sigma) \to (A^v, \tau)$. This implies that the K–algebras $\Delta(E)$ and $Z(A, \tau)$ are isomorphic. Let us fix an isomorphism of K–algebras

$$\nu : \Delta(E) \to Z(A, \tau).$$

Let us denote by $\mathcal{O}(E, A)$ the set of $(a) = (a^v)$, with $a^v \in (F^v)^\times$, such that for all $v \in \Omega_K$, there exists $\alpha^v \in (A^v)^\times$ with the properties :
(a) $\mathrm{Int}(\alpha) : (A^v, \theta_{a^v}) \to (A^v, \tau)$ is an isomorphism of K_v–algebras with involution.

(b) The induced automorphism $c(\alpha) : Z(A^v, \theta_{a^v}) \to Z(A^v, \tau)$ satisfies

$$c(\alpha) \circ u_{a^v} = \nu.$$

In other words, $(\mathrm{Int}(\alpha) \circ \epsilon, a^v, \alpha^v, \nu)$ are parameters of an oriented embedding.

Proposition 5.1.1. *Let $(a) = (a^v) \in \mathcal{O}(E, A)$. Then we have :*

(i) $\mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ *for almost all $v \in \Omega_K$, and*

$$\Sigma_{v\in\Omega_K} \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = 0.$$

(ii) *Let Ω' be the set of places $v \in \Omega_K$ such that $\Delta(E^v) \simeq K_v \times K_v$. Then we have $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ for almost all $v \in \Omega'$, and*

$$\Sigma_{v\in\Omega'}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = 0.$$

Proof. By Lemma 2.5.4. $C(A^v, \theta_{a^v}) = C(A^v, \theta) + \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d)$ in $\mathrm{Br}(\Delta(E^v)$ for all $v \in \Omega_K$. Since $(a^v) \in \mathcal{O}(E, A)$ we have $C(A^v, \theta_{a^v}) = C(A^v, \tau)$ for all $v \in \Omega_K$. Therefore we have

$$C(A^v, \tau) - C(A^v, \theta) = \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d),$$

hence (i) holds. If $\Delta(E^v) \simeq K_v \times K_v$, then $\mathrm{res}_{\Delta(E^v)/K_v}$ is injective, and this implies (ii).

Proposition 5.1.2. *Let $(a^v), (b^v) \in \mathcal{O}(E, A)$. Then, for all $v \in \Omega_K$*

(i) $\mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(b^v, d)$.

(i) *If moreover $\Delta(E^v) \simeq K_v \times K_v$, then $\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d)$.*

Proof. We have $C(A^v, \theta_{a^v}) = C(A^v, \theta) + \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d)$, and $C(A^v, \theta_{b^v}) = C(A^v, \theta) + \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(a^v, d)$ in $\mathrm{Br}(\Delta(E^v))$ (cf. Lemma 2.5.4.). Since $(a^v), (b^v) \in \mathcal{O}(E, A)$ we have $C(A^v, \theta_{a^v}) = C(A^v, \theta_{b^v})$, and this implies (i). If $\Delta(E^v) \simeq K_v \times K_v$, then $\mathrm{res}_{\Delta(E^v)/K_v}$ is injective, hence (ii).

A *local embedding datum* will be a set $(a) = (a^v) \in \mathcal{O}(E, A)$ such that

• If $v \in \Omega_K$ is such that $\Delta(E_v)$ is a quadratic extension of K_v, then there exist only finitely many $v \in \Omega_K$ such that $\mathrm{cor}_{F^v/K_v}(a^v, d) \neq 0$.

• We have

$$\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = 0.$$

We denote by $\mathcal{L}(E, A)$ the set of local embedding data.

Remark. Let $(a^v) \in \mathcal{L}(E, A)$. Then we have $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ for almost all $v \in \Omega_K$. Indeed, by hypothesis this is true if v is such that $\Delta(E_v)$ is a quadratic extension of K_v, and by Proposition 5.1.1. (ii) it also holds if v is such that $\Delta(E_v) \simeq K_v \times K_v$.

Recall that the notion of oriented embedding was defined in 2.6.

Proposition 5.1.3. *Assume that for all $v \in \Omega_K$, there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$ with respect to ν. Then there exists a local embedding datum $(a) = (a^v) \in \mathcal{L}(E, A)$ such that for all $v \in \Omega_K$ there exist ι_v and α^v such that $(\iota_v, a^v, \alpha^v, \nu)$ are parameters of an oriented embedding.*

Proof. Case 1. Assume that $\Delta(E^v)/K_v$ is a quadratic extension. Let $(b^v) \in \mathcal{O}(E, A)$. Then $C(A^v, \tau) = C(A^v, \theta) + \mathrm{res}_{\Delta(E^v)/K_v}\ \mathrm{cor}_{F^v/K_v}(b^v, d) = C(A^v, \theta)$ in $\mathrm{Br}(\Delta(E^v))$, since $\Delta(E^v)/K_v$ is a quadratic extension. Moreover, we have $\mathrm{disc}(A^v, \tau) = \mathrm{disc}(A^v, \theta_{b^v}) = \mathrm{disc}(A^v, \theta)$. Hence (A^v, θ) and (A^v, τ) are isomorphic. By Corollary 2.7.3. (ii) there exist ι_v and α^v such that $(\iota_v, 1, \alpha^v, \nu)$ are parameters of an oriented embedding.

Case 2. Assume now that we have $\Delta(E^v) \simeq K_v \times K_v$. Let $(\iota_v, a^v, \alpha^v, \nu)$ be parameters for an oriented embedding.

Let $(a) = (a^v)$, where for $v \in \Omega_K$ the element a^v is chosen as above, in each of the two cases. We claim that $(a) = (a^v) \in \mathcal{L}(E, A)$. Since $a^v = 1$ when $\Delta(E^v)/K_v$ is a quadratic extension, we have $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ for all such v. Let Ω' be the set of $v \in \Omega_K$ such that $\Delta(E^v) \simeq K_v \times K_v$. Then we have $\Sigma_{v \in \Omega_K}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = \Sigma_{v \in \Omega'}\ \mathrm{cor}_{F^v/K_v}(a^v, d)$, and by Proposition 5.1.1. (ii) this sum is zero. Therefore we have $(a) \in \mathcal{L}(E, A)$.

Proposition 5.1.4. *Let $(a) = (a^v), (b) = (b^v) \in \mathcal{L}(E, A)$. Then there exists $\lambda \in K^\times$ such that for all $v \in \Omega_K$ we have $\mathrm{cor}_{F^v/K_v}(\lambda b^v, d) = \mathrm{cor}_{F^v/K_v}(a^v, d)$.*

Proof. We have $\mathrm{res}_{\Delta(E^v)/K}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{res}_{\Delta(E^v)/K}\ \mathrm{cor}_{F^v/K_v}(b^v, d)$ for all $v \in \Omega_K$, and if $\Delta(E^v) \simeq K_v \times K_v$, then $\mathrm{cor}_{F^v/K_v}(b^v, d) = \mathrm{cor}_{F^v/K_v}(a^v, d)$ (cf. Proposition 5.1.2.).

Let $\Omega' = \{v \in \Omega_K \mid \mathrm{cor}_{F^v/K_v}(b^v, d) \neq \mathrm{cor}_{F^v/K_v}(a^v, d)\}$. The above argument shows that if $v \in \Omega'$, then $\Delta(E^v)$ is a quadratic extension of K_v. It follows from the definition of $\mathcal{L}(E, A)$ that there exist only finitely many $v \in \Omega_K$ such that $\mathrm{cor}_{F^v/K_v}(a^v, d) \neq 0$ or $\mathrm{cor}_{F^v/K_v}(b^v, d) \neq 0$, hence Ω' is a finite set.

Let $v \in \Omega'$. Then $\Delta(E^v)$ splits $\mathrm{cor}_{F^v/K_v}(b^v, d) - \mathrm{cor}_{F^v/K_v}(a^v, d)$. Recall that $\Delta(E^v) = K_v(\sqrt{D})$, where $D = (-1)^r \mathrm{N}_{E/K}(\sqrt{d}) = \mathrm{N}_{F/K}(d)$. Then we have $\mathrm{cor}_{F^v/K_v}(b^v, d) - \mathrm{cor}_{F^v/K_v}(a^v, d) = (\lambda^v, D)$ for some $\lambda^v \in K_v^\times$.

Since $(a), (b) \in \mathcal{L}(E, A)$, by definition we have $\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = \Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F^v/K_v}(b^v, d) = 0$. This implies that $\Sigma_{v\in\Omega_K}(\lambda^v, D) = 0$. Hence by the Brauer–Hasse–Noether theorem, there exists $\lambda \in K^\times$ such that $(\lambda, D) = (\lambda^v, D) \in \mathrm{Br}(K_v)$ for all $v \in \Omega'$, and λ has the required property.

5.2. Local embedding data – odd degree orthogonal case

In this section, we assume that $A \simeq M_n(K)$ and that τ is induced by an n–dimensional quadratic form q. We are primarily interested in the case where n is odd, but we also need to consider the case where n is even.

Let us assume that there exists an embedding of algebras with involution $(E^v, \sigma) \to (A^v, \tau)$ for all $v \in \Omega_K$. By Proposition 1.4.1. this implies that for all $v \in \Omega_K$ there exists $a^v \in (F^v)^\times$ such that $q \simeq T_{a^v}$. Let us write $a^v = (a^v_1, \ldots, a^v_m)$ with $a^v_i \in (F^v_i)^\times$. The set of $(a) = (a^v_i)$ with this property will be denoted by $\mathcal{L}'(E, A)$.

Proposition 5.2.1. *Let $(a) \in \mathcal{L}'(E, A)$, with $(a) = (a^v_i)$. Then the following properties hold :*

(i) $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ *for almost all $v \in \Omega_K$, and*

$$\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = 0.$$

(ii) *Let $(b) \in \mathcal{L}'(E, A)$, with $(b) = (b^v_i)$. Then for all $v \in \Omega_K$, we have*

$$\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d).$$

Proof. Let us first assume that n is even. Since $(a) \in \mathcal{L}'(E, A)$, we have $q \simeq T_{a^v}$, and hence $w(T_{a^v}) = w(q)$ for all $v \in \Omega_K$. By Lemma 1.5.1. we have $w(T_{a^v}) = w(T) + \mathrm{cor}_{F^v/K_v}(a^v, d)$. Hence for all $v \in \Omega_K$, we have $w(q) = w(T_{a^v}) = w(T) + \mathrm{cor}_{F^v/K_v}(a^v, d)$. Note that $\Sigma_{v\in\Omega_K} w(q) = \Sigma_{v\in\Omega_K} w(T) = 0$. Therefore we have $\Sigma_{v\in\Omega_K}\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$, and this proves (i).

Let us prove (ii). Since $(b) \in \mathcal{L}'(E, A)$, for all $v \in \Omega_K$ we have $w(T_{b^v}) = w(q)$. By Lemma 1.5.1. we have $w(T_{b^v}) = w(T) + \mathrm{cor}_{F^v/K_v}(b^v, d)$ for all $v \in \Omega_K$. Therefore, for all $v \in \Omega_K$, we have $w(T) + \mathrm{cor}_{F^v/K_v}(a^v, d) = w(q) = w(T) + \mathrm{cor}_{F^v/K_v}(b^v, d)$. Hence we have $\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d)$, and this implies (ii).

Suppose that n is odd, and set $A' = M_{n-1}(K)$. Then by [PR 10], Proposition 7.2. there exists a σ–invariant étale subalgebra E' of rank $n-1$ of E such that $E = E' \times K$, an $(n-1)$–dimensional quadratic form q' and a 1–dimensional quadratic form q'' over K such that $q \simeq q' \oplus q''$, and that the

étale algebra with involution (E', σ) can be embedded in the central simple algebra (A', τ') over K_v for all $v \in \Omega_K$, where $\tau' : A' \to A'$ is the involution induced by q'. Moreover, there exists an embedding of (E, σ) into (A, τ) if and only if there exists an embedding of (E', σ) into (A', τ'). Note that we have $\mathcal{L}'(E, A) = \mathcal{L}'(E', A') \times \mathcal{L}'(K, K)$. We may suppose that $E_m = K$. Then we have $d_m = 1$. Set $J = \{1, \ldots, m-1\}$, and note that for all $v \in \Omega_K$, we have $\Sigma_{i\in I}\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = \Sigma_{i\in J}\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$. Since $n-1$ is even, statements (i) and (ii) easily follow.

If n is odd, then we set $\mathcal{L}(E, A) = \mathcal{L}'(E, A)$, and an element $(a) \in \mathcal{L}(E, A)$ will be called *local embedding datum.*

If n is even, then the set of embedding data $\mathcal{L}(E, A)$ was defined in the previous section. The relationship between $\mathcal{L}(E, A)$ and $\mathcal{L}'(E, A)$ is as follows :

Proposition 5.2.2. *Assume that n is even. Then we have*

(i) $\mathcal{L}'(E, A) \subset \mathcal{L}(E, A)$.

(ii) *Let $(a) \in \mathcal{L}(E, A)$. Then there exists $\lambda \in K^\times$ such that $(\lambda a) \in \mathcal{L}'(E, A)$.*

Proof. Let $(a) \in \mathcal{L}'(E, A)$. Then $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ for almost all $v \in \Omega_K$, and $\Sigma_{v\in\Omega_K}\ \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ (cf. Proposition 5.2.1. (i)). Since $q \simeq T_{a^v}$ for all $v \in \Omega_K$, the algebras with involution (A^v, τ) and (A^v, θ_{a^v}) are isomorphic. Since A is split, Corollary 2.7.3. implies that for all $v \in \Omega_K$ there exist ι_v and α^v such that $(\iota_v, a^v, \alpha^v, \nu)$ are parameters of an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$. This implies that $(a) \in \mathcal{L}(E, A)$, hence (i) is proved.

Let us prove (ii). Let S be the finite set of places of K at which q or T is not hyperbolic, or $(a^v, d) \neq 0$. Since $(a) \in \mathcal{L}(E, A)$, there exists $\lambda^v \in K_v^\times$ such that q and $\lambda^v T_{a^v}$ are isomorphic over K_v for all $v \in S$. There exists $\lambda \in K^\times$ such that $\lambda(\lambda^v)^{-1} \in (K_v)^{\times 2}$ for all $v \in S$. Then q and λT_{a^v} are isomorphic over K_v for all $v \in S$. For $v \notin S$, both q and T_{a^v} are hyperbolic over K_v, hence we have $q \simeq \lambda T_{a^v}$. Since $\lambda T_{a^v} = T_{\lambda a^v}$, we have $(\lambda a) \in \mathcal{L}'(E, A)$.

5.3. Local embedding data – the unitary case

Let us assume that (A, τ) is a unitary involution.

The set of $(a) = (a^v)$, with $a^v \in (F^v)^\times$, such that for all $v \in \Omega_K$ we have $(A_v, \tau) \simeq (A_v, \theta_{a^v})$, is called a *local embedding datum.* We denote by $\mathcal{L}(E, A)$ the set of local embedding data.

Proposition 5.3.1. *Let $(a) \in \mathcal{L}(E, A)$ be an embedding datum, with $(a) = (a_i^v)$. Then the following properties hold :*

(i) *We have*

$$\Sigma_{v\in\Omega_K}\mathrm{cor}_{F^v/K_v}(a^v,d)=0.$$

(ii) *Let $(b)\in\mathcal{L}(E,A)$ be an embedding datum, with $(b)=(b_i^v)$. Then for all $v\in\Omega_K$, we have*

$$\mathrm{cor}_{F^v/K_v}(a^v,d)=\mathrm{cor}_{F^v/K_v}(b^v,d).$$

Proof. Since $(a)\in\mathcal{L}(E,A)$, we have $(A^v,\theta_{a^v})\simeq(A^v,\tau)$ for all $v\in\Omega_K$. Hence for all $v\in\Omega_K$, we have $D(A^v,\theta_{a^v})=D(A^v,\tau)$. By Lemma 1.5.2. we have $D(A^v,\theta_{a^v})=D(A^v,\theta)+\mathrm{cor}_{F^v/K^v}(a^v,d)$ for all $v\in\Omega_K$. We have $\Sigma_{v\in\Omega_K}D(A^v,\tau)=\Sigma_{v\in\Omega_K}D(A^v,\theta)=0$, hence $\Sigma_{v\in\Omega_K}\mathrm{cor}_{F^v/K_v}(a^v,d)=0$. This proves (i).

Let us prove (ii). Let $v\in\Omega_K$. Since $(b)\in\mathcal{L}(E,A)$, by Lemma 1.5.2. we have $D(A^v,\theta)+\mathrm{cor}_{F^v/K^v}(a^v,d)=D(A^v,\theta_{a^v})=D(A^v,\tau)=D(A^v,\theta_{b^v})=D(A^v,\theta)+\mathrm{cor}_{F^v/K^v}(b^v,d)$. Hence we have $\mathrm{cor}_{F^v/K_v}(a^v,d)=\mathrm{cor}_{F^v/K_v}(b^v,d)$, as claimed.

5.4. The Brauer–Manin map

Let $(a)\in\mathcal{L}(E,A)$ be an embedding datum, with $(a)=(a_i^v)$. Let us consider the map

$$f_{(a)}:Ш(E,\sigma)\to\mathbf{Z}/2\mathbf{Z}$$

defined by

$$f_{(a)}(I_0,I_1)=\Sigma_{i\in I_0}\Sigma_{v\in\Omega_K}\mathrm{cor}_{F_i^v/K_v}(a_i^v,d_i).$$

Note that this is well–defined, since $\Sigma_{i\in I}\Sigma_{v\in\Omega_K}\mathrm{cor}_{F_i^v/K_v}(a_i^v,d_i)=0$. As we will see, this map is independent of the choice of (a). In other words, we have

Theorem 5.4.1. *Let $(a),(b)\in\mathcal{L}(E,A)$ be two local embedding data. Then we have $f_{(a)}=f_{(b)}$.*

Proof. Suppose that $(a),(b)\in\mathcal{L}(E,A)$ are such that $f_{(a)}\neq f_{(b)}$. Note that for all $\lambda\in K^\times$, we have $(\lambda b)\in\mathcal{L}(E,A)$, and $f_{(b)}=f_{(\lambda b)}$. Since there exists $\lambda\in K^\times$ such that for all $v\in\Omega_K$ we have $\Sigma_{i\in I}\mathrm{cor}_{F_i^v/K_v}(a_i^v,d_i)=\Sigma_{i\in I}\mathrm{cor}_{F_i^v/K_v}(\lambda b_i^v,d_i)$ (cf. Proposition 5.1.4. Proposition 5.2.1. (ii) and Proposition 5.3.1. (ii)), we may assume that for all $v\in\Omega_K$, we have

$$\Sigma_{i\in I}\mathrm{cor}_{F_i^v/K_v}(a_i^v,d_i)=\Sigma_{i\in I}\mathrm{cor}_{F_i^v/K_v}(b_i^v,d_i).$$

Let $(I_0, I_1) \in Ш(E, \sigma)$ be such that $f_{(a)}(I_0, I_1) \neq f_{(b)}(I_0, I_1)$. Then there exists $v \in \Omega_K$ such that $\Sigma_{i \in I_0} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \Sigma_{i \in I_0} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i)$. This implies that $v \notin \Sigma(L/K)$, and $v \notin \bigcap\limits_{i \in I_0} \Sigma_i$. Since $\Sigma_{i \in I} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = \Sigma_{i \in I} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i)$, there exists $j \in I_1$ such that

$$\mathrm{cor}_{F_j^v/K_v}(a_j^v, d_j) \neq \mathrm{cor}_{F_j^v/K_v}(b_j^v, d_j).$$

Therefore $v \notin \bigcap\limits_{i \in I_1} \Sigma_i$, and this contradicts $\Sigma(L/K) \cup \bigcap\limits_{i \in I_0} \Sigma_i \cup \bigcap\limits_{i \in I_1} \Sigma_i = \Omega_K$. Hence we have $f_{(a)} = f_{(b)}$ for all $(a), (b) \in \mathcal{L}(E, A)$.

Since $f_{(a)}$ is independent of (a), we obtain a map

$$f : Ш(E, \sigma) \to \mathbf{Z}/2\mathbf{Z}$$

defined by

$$f(I_0, I_1) = \Sigma_{i \in I_0} \Sigma_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$$

for any $(a) = (a_i^v) \in \mathcal{L}(E, A)$. Note that f is a group homomorphism.

Recall that we are fixing an embedding $\epsilon : E \to A$, and an involution $\theta : A \to A$ such that $\epsilon : (E, \sigma) \to (A, \tau)$ is an embedding of algebras with involution. If (A, θ) is orthogonal, then we also fix an orientation $u : \Delta(E) \to Z(A, \theta)$. Our next aim is to discuss the dependence of f on these choices. We first introduce some notation.

Recall that for all $a \in F^\times$, we set $\theta_a = \theta \circ \mathrm{Int}(\epsilon(a))$. Similarly, if $\tilde{\theta} : A \to A$ is an involution and if $\tilde{\epsilon} : (E, \sigma) \to (A, \theta)$ is an embedding of algebras with involution, then we set $\tilde{\theta}_a = \tilde{\theta} \circ \mathrm{Int}(\tilde{\epsilon}(a))$. Then $\tilde{\theta}_a : A \to A$ is an involution, and $\tilde{\epsilon} : (E, \sigma) \to (A, \tilde{\theta})$ is an embedding of algebras with involution.

Definition 5.4.2. Let $\tilde{\epsilon} : E \to A$ be an embedding, and let $\tilde{\theta} : A \to A$ be an involution such that $\tilde{\epsilon} : (E, \sigma) \to (A, \tilde{\theta})$ is an embedding of algebras with involution. Let $\tilde{u} : \Delta(E) \to Z(A, \tilde{\theta})$ be an orientation. We say that (ϵ, θ, u) and $(\tilde{\epsilon}, \tilde{\theta}, \tilde{u})$ are *compatible* if there exists $\alpha \in A^\times$ and $c \in F^\times$ such that the following two conditions are satisfied

(a) $\mathrm{Int}(\alpha) : (A, \tilde{\theta}) \to (A, \theta_c)$ is an isomorphism of algebras with involution such that $\mathrm{Int}(\alpha) \circ \tilde{\epsilon} = \epsilon$.

(b) The induced automorphism $c(\alpha) : Z(A, \tilde{\theta}) \to Z(A, \theta_c)$ satisfies

$$c(\alpha) \circ \tilde{u} = u_c.$$

Recall that if (A, τ) is orthogonal, then we are fixing an orientation $\nu : \Delta(E) \to Z(A, \tau)$.

Proposition 5.4.3. *Assume that* (ϵ, θ, u) *and* $(\tilde{\epsilon}, \tilde{\theta}, \tilde{u})$ *are compatible. Let* $\tilde{\mathcal{L}}(A, E)$ *be the set of local embedding data defined with respect to* $(\tilde{\epsilon}, \tilde{\theta}, \tilde{u})$*, and let* $(a) \in \tilde{\mathcal{L}}(A, E)$*. Let*

$$f'_{(a)} : Ш(E, \sigma) \to \mathbf{Z}/2\mathbf{Z}$$

be defined by

$$f'_{(a)}(I_0, I_1) = \Sigma_{i \in I_0} \Sigma_{v \in \Omega_K} \mathrm{cor}_{F_i^v / K_v}(a_i^v, d_i).$$

Then $f'_{(a)} = f$*.*

Proof. Let $\alpha \in A^\times$ and $c \in F^\times$ be such that $\mathrm{Int}(\alpha) : (A, \tilde{\theta}) \to (A, \theta_c)$ is an isomorphism of algebras with involution such that $\mathrm{Int}(\alpha) \circ \tilde{\epsilon} = \epsilon$, and that if θ is orthogonal, then we have $c(\alpha) \circ \tilde{u} = u_c$.

Let $(a) = (a^v) \in \tilde{\mathcal{L}}(A, E)$. We claim that $(ca) \in \mathcal{L}(E, A)$. A straightforward computation shows that $\mathrm{Int}(\alpha^{-1}) : (A, \theta_{ca^v}) \to (A, \tilde{\theta}_{a^v})$ is an isomorphism of algebras with involution for all $v \in \Omega_K$.

For all $v \in \Omega_K$, let $(\mathrm{Int}(\beta^v) \circ \tilde{\epsilon}, a^v, \beta^v, \nu)$ be parameters of an oriented embedding. Since $\tilde{\epsilon} = \mathrm{Int}(\alpha^{-1}) \circ \epsilon$ and $c(\alpha) \circ \tilde{u}_a = u_{ca}$, we see that $(\mathrm{Int}(\beta^v \alpha^{-1}) \circ \epsilon c a^v, \beta^v \alpha^{-1}, \nu)$ are parameters of an oriented embedding with respect to (ϵ, θ, u). Therefore we have $(ca) \in \mathcal{L}(E, A)$.

Let $c = (c_1, \ldots, c_m)$ with $c_i \in F_i^\times$. We have

$$f'_{(a)}(I_0, I_1) = \Sigma_{i \in I_0} \Sigma_{v \in \Omega_K} \mathrm{cor}_{F_i^v / K_v}(a_i^v, d_i) =$$

$$= \Sigma_{i \in I_0} \Sigma_{v \in \Omega_K} \mathrm{cor}_{F_i^v / K_v}(a_i^v, d_i) + \Sigma_{i \in I_0} \Sigma_{v \in \Omega_K} \mathrm{cor}_{F_i^v / K_v}(c_i, d_i) =$$

$$= \Sigma_{i \in I_0} \Sigma_{v \in \Omega_K} \mathrm{cor}_{F_i^v / K_v}(c_i a_i^v, d_i) = f(I_0, I_1),$$

since $(ca) \in \mathcal{L}(E, A)$.

Corollary 5.4.4. *Suppose that there exists an embedding of algebras with involution* $(E, \sigma) \to (A, \tau)$*. Then we have* $f = 0$*.*

Proof. Since there exists an embedding $(E, \sigma) \to (A, \tau)$, there exists $a \in F^\times$ such that $\tau \simeq \theta_a$. We have $a = (a_1, \ldots, a_m)$ with $a_i \in F_i^\times$. For all $v \in \Omega_K$, set $a_i^v = a_i$, and let $(a) = (a_i^v)$. By Theorem 5.4.1. it suffices to show that $f_{(a)} = 0$. Let $(I_0, I_1) \in Ш(E, \sigma)$. Then we have

$$f_{(a)}(I_0, I_1) = \Sigma_{v \in \Omega_K} \Sigma_{i \in I_0} \mathrm{cor}_{F_i^v / K_v}(a_i, d_i) = \Sigma_{v \in \Omega_K} \Sigma_{i \in I_0} \mathrm{cor}_{F_i / K}(a_i, d_i) = 0.$$

Therefore $f = f_{(a)} = 0$, as claimed.

5.5. Hasse principle

The main result of the paper is the following :

Theorem 5.5.1. *Let $\nu : \Delta(E) \to Z(A,\tau)$ be an orientation. Suppose that for all $v \in \Omega_K$ there exists an oriented embedding $(E^v,\sigma) \to (A^v,\tau)$ with respect to ν. Then there exists an embedding $(E,\sigma) \to (A,\tau)$ if and only if $f = 0$.*

This will be proved in Sections 6–8.

§6. Orthogonal involutions

Suppose that K is a global field, that (A,τ) is orthogonal, and that all the factors of E split A. The aim of this section is to give a criterion for the Hasse principle for the existence of an embedding of (E,σ) into (A,τ) : in other words, to prove Theorem 5.5.1. for orthogonal involutions. Moreover, based on the results of §2, we give necessary and sufficient conditions for such an embedding to exist everywhere locally.

6.1. The even degree case – Hasse principle

Suppose that $\deg(A) = n = 2r$. We fix an embedding $\epsilon : (E,\sigma) \to (A,\theta)$ and an isomorphism of K–algebras $u : \Delta(E) \to Z(A,\theta)$.

Let us assume that for all $v \in \Omega_K$, there exists an embedding of algebras with involution $(E^v,\sigma) \to (A^v,\tau)$. This implies that the K–algebras $\Delta(E)$ and $Z(A,\tau)$ are isomorphic. Let us fix an isomorphism of K–algebras $\nu : \Delta(E) \to Z(A,\tau)$.

The Brauer–Manin map $f : Ш(E,\sigma) \to \mathbf{Z}/2\mathbf{Z}$ was defined in 5.4.

Theorem 6.1.1. *Suppose that for all $v \in \Omega_K$ there exists an oriented embedding $(E^v,\sigma) \to (A^v,\tau)$ with respect to ν. Then there exists an embedding $(E,\sigma) \to (A,\tau)$ if and only if $f = 0$.*

Proof. By Corollary 5.4.4. we already know that the existence of a global embedding $(E,\sigma) \to (A,\tau)$ implies that $f = 0$. Let us prove the converse. Let $(a) = (a_i^v) \in \mathcal{L}(E,A)$, and let $(I_0,I_1) \in Ш$. Then by hypothesis we have $f(I_0,I_1) = f_{(a)}(I_0,I_1) = 0$, hence

$$\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v,d_i) = 0.$$

By Proposition 4.1.5. there exists $b \in F^\times$ such that

$$\mathrm{cor}_{F^v/K_v}(b,d) = \mathrm{cor}_{F^v/K_v}(a^v,d)$$

for all $v \in \Omega_K$. Applying Lemma 2.5.4. we see that $C(A^v,\theta_{a^v}) = C(A^v,\theta_b)$ in $\mathrm{Br}(\Delta(E^v))$ for all $v \in \Omega_K$. Since the embedding is oriented with respect to ν,

we have $C(A^v,\tau) = C(A^v,\theta_{a^v})$ in $\mathrm{Br}(\Delta(E^v))$ for all $v \in \Omega_K$. Therefore for all $v \in \Omega_K$, we have $C(A^v,\tau) = C(A^v,\theta_b)$ in $\mathrm{Br}(\Delta(E^v))$. Then by the Brauer–Hasse–Noether Theorem, we have $C(A,\tau) = C(A,\theta_b)$ in $\mathrm{Br}(\Delta(E))$, hence $C(A,\tau)$ and $C(A,\theta_b)$ are isomorphic over K. Note that $(A^v,\tau) \simeq (A^v,\theta_b)$ over K_v if v is a real place. Hence by [LT 99], Theorems A and B, we conclude that $(A,\tau) \simeq (A,\theta_b)$. By Proposition 1.1.3. there exists an embedding of (E,σ) into (A,τ).

Corollary 6.1.2. *Assume that for all $v \in \Omega_K$ there exists an embedding $(E^v,\sigma) \to (A^v,\tau)$. Suppose moreover that one of the following holds :*

(i) *A is split.*

(ii) *If $v \in \Omega_K$ is such that A^v is non-split, then $\mathrm{disc}(A^v,\tau) \neq 1$ in $K_v^\times/K_v^{\times 2}$.*

(iii) *$\deg(A) = 2r$ with r odd.*

Then there exists an embedding $(E,\sigma) \to (A,\tau)$ if and only if $f = 0$.

Proof. This follows from Theorem 6.1.1. together with Corollary 2.7.3. (in cases (i) and (ii)), and Corollary 2.8.3. (in case (iii)).

6.2. The odd degree case - Hasse principle

Suppose that $A = M_n(K)$, and that τ is induced by an n–dimensional quadratic form q. Recall that $f : Ш \to \mathbf{Z}/2\mathbf{Z}$ was defined in 4.4.

Theorem 6.2.1. *Suppose that n is odd, and that for all $v \in \Omega_K$ there exists an embedding of algebras with involution $(E^v,\sigma) \to (A^v,\tau)$. Then there exists an embedding $(E,\sigma) \to (A,\tau)$ if and only if $f = 0$.*

Proof. We already know that if there exists an embedding $(E,\sigma) \to (A,\tau)$, then we have $f = 0$ (cf. Corollary 5.4.3). Let us show that the converse also holds. Assume that we have $f = 0$.

If $n = 1$ then $E = A = K$, hence (E,σ) can be embedded into (A,τ). Let us assume that $n \geq 3$. Set $A' = M_{n-1}(K)$. Then by [PR 10], Proposition 7.2. there exists a σ–invariant étale subalgebra E' of rank $n-1$ of E such that $E = E' \times K$, an $(n-1)$–dimensional quadratic form q' and a 1–dimensional quadratic form q'' over K such that $q \simeq q' \oplus q''$, and that the étale algebra with involution (E',σ) can be embedded in the central simple algebra (A',τ') over K_v for all $v \in \Omega_K$, where $\tau' : A' \to A'$ is the involution induced by q'. Moreover, there exists an embedding of (E,σ) into (A,τ) if and only if there exists an embedding of (E',σ) into (A',τ'). Note that we have $\mathcal{L}(E,A) = \mathcal{L}'(E',A') \times \mathcal{L}(K,K)$. We may suppose that $E_m = K$. Then we have $d_m = 1$. Set $J = \{1,\ldots,m-1\}$.

Let $f' : Ш(E', \sigma) \to \mathbf{Z}/2\mathbf{Z}$ be the Brauer–Manin map associated to (E', σ) and (A', τ'). Let $(a) = (a_i^v) \in \mathcal{L}(E, A)$. Set $b_i^v = a_i^v$ if $i = 1, \ldots, m-1$. Then $(b) = (b_i^v)$ is an element of $\mathcal{L}'(E', A')$. By Proposition 5.2.2. (i) we have $\mathcal{L}'(E', A') \subset \mathcal{L}(E', A')$, hence $(b) \in \mathcal{L}(E', A')$.

For all $(J_0, J_1) \in Ш(E', A')$ we have $f'(J_0, J_1) = f'_{(b)}(J_0, J_1) = f_{(a)}(I_0, I_1)$, where $I_0 = J_0$ and $I_1 = J_1 \cup \{m\}$. Since $f_a = f = 0$ by hypothesis, this implies that $f' = 0$. By Corollary 6.1.2. (i) this implies that (E', σ) can be embedded into (A', τ'). Therefore (E, σ) can be embedded into (A, τ).

6.3. Orthogonal involutions – local conditions

An infinite place w of F is said to be *ramified in* E if w is a real place that extends to a complex place of E. For all $v \in \Omega_K$, let ρ_v be the number of places of F above v which are not ramified.

Definition 6.3.1. We say that the *signature conditions* hold if for every real prime v of K such that $A^v \simeq M_n(K_v)$, the signature of q at v is of the shape $(r_v + \rho_v, s_v + \rho_v)$ for some non–negative integers r_v and s_v such that r_v and s_v are even if n is even.

Definition 6.3.2. We say that the *hyperbolicity condition* is satisfied if for all $v \in \Omega_K$ such that the étale algebra with involution (E^v, σ) is split, the algebra with involution (A^v, τ) is hyperbolic.

Note that as (A^v, τ) is hyperbolic for all but a finite number of places $v \in \Omega$, we only need to check the hyperbolicity condition at finitely many places.

The following is a consequence of the results of §3, in particular Propositions 3.1.1. and 3.1.2. (see also [B 12], Proposition 2.4.1. and [B 13], Theorem 12.1.).

Proposition 6.3.3. *Suppose that n is even. The étale algebra with involution (E^v, σ) can be embedded in the algebra with involution (A^v, τ) for all $v \in \Omega_K$ if and only if the following conditions hold :*

(i) *We have* $\mathrm{disc}(A, \tau) = \mathrm{disc}(E) \in K^\times / K^{\times 2}$.

(ii) *The hyperbolicity condition is satisfied.*

(iii) *The signature conditions are satisfied.*

Assume now that n is odd. We have $E \simeq E' \times K$, where E' is an étale algebra of rank $n-1$ stable by σ. Note that if $n = 1$, then an embedding of (E, σ) into (A, τ) always exists, hence we may assume that $n \geq 3$. The following is a consequence of Propositions 3.2.1. and 3.2.2.

Proposition 6.3.4. *Suppose that n is odd and ≥ 3. The étale algebra with involution (E^v, σ) can be embedded in the algebra with involution (A^v, τ) for all $v \in \Omega_K$ if and only if the following conditions hold :*

(i) *For all $v \in \Omega_K$ such that $(E')^v, \sigma)$ is split, we have $q \simeq q' \oplus q''$, where q' is hyperbolic, and q'' is a 1–dimensional quadratic form over K_v.*

(ii) *The signature conditions are satisfied.*

§7. Symplectic involutions

Suppose that K is a global field, that all the factors of E split A, and that (A, τ) is a symplectic involution. Prasad and Rapinchuk proved that the Hasse principle holds in this case (cf. [PR 10], Theorem 5.1).

An infinite place w of F is said to be *ramified in E* if w is a real place that extends to a complex place of E. For all $v \in \Omega_K$, let ρ_v be the number of places of F above v which are not ramified.

Definition 7.1.1. We say that the *signature condition* holds if for every real prime v of K such that A^v is non–split, the signature of (A^v, τ) is of the shape $(r_v + \rho_v, s_v + \rho_v)$ for some non–negative integers r_v and s_v.

The following result is a consequence of the Hasse principle, and of Proposition 3.3.1.

Theorem 7.1.2. *The étale algebra with involution (E, σ) can be embedded in the central simple algebra with involution (A, τ) if and only if the signature condition holds.*

§8. Unitary involutions

Suppose that K is a global field, that all the factors of E split A, and that (A, τ) is a unitary involution.

8.1. Unitary involutions – Hasse principle

Suppose that (E^v, σ) can be embedded in (A^v, τ) for all $v \in \Omega_K$, and recall that $f : Ш(E, \sigma) \to \mathbf{Z}/2\mathbf{Z}$ is the Brauer–Manin map defined in 5.4.

Theorem 8.1.1. *Suppose that for all $v \in \Omega_K$ there exists an embedding of algebras with involution $(E^v, \sigma) \to (A^v, \tau)$. Then there exists an embedding of algebras with involution $(E, \sigma) \to (A, \tau)$ if and only if $f = 0$.*

Proof. If there exists a global embedding, then we have $f = 0$ (cf. Corollary 5.4.4.). Let us prove the converse. For all $v \in \Omega_K$ there exist $a^v \in (F^v)^\times$ such that $(A^v, \tau) = (A^v, \theta_{a^v})$, hence we have $\mathrm{D}(A^v, \tau) = \mathrm{D}(A^v, \theta_{a^v})$ in $\mathrm{Br}(K_v)$.

On the other hand, by Lemma 1.5.2. we have $\mathrm{D}(A^v, \theta_{a^v}) = \mathrm{D}(A^v, \theta) + \mathrm{cor}_{F^v/K_v}(a^v, d)$. Hence we have $\Sigma_{v\in\Omega_K}\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$. Let $(I_0, I_1) \in Ш$. Then by hypothesis we have $f_{(a)}(I_0, I_1) = 0$, therefore

$$\Sigma_{v\in\Omega_K}\Sigma_{i\in I_0}\ \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0.$$

By Proposition 4.1.5. there exists $b \in F^\times$ such that for all $v \in \Omega_K$, we have $\mathrm{cor}_{F^v/K_v}(b, d) = \mathrm{cor}_{F^v/K_v}(a^v, d)$, and that $b^v = a^v$ if v is a real place. On the other hand, we have $\mathrm{D}(A, \tau) = \mathrm{D}(A, \theta_b)$. Hence we have $(A, \tau) \simeq (A, \theta_b)$. By Proposition 1.1.3. there exists an embedding of (E, σ) into (A, τ).

8.2. Unitary involutions – local conditions

An infinite place w of F is said to be *ramified in* E if w is a real place that extends to a complex place of E. For all $v \in \Omega_K$, let ρ_v be the number of places of F above v which are not ramified.

Definition 8.2.1. We say that the *signature condition* holds if for every real prime v of K, the signature of (A^v, τ) is of the shape $(r_v + \rho_v, s_v + \rho_v)$ for some non–negative integers r_v and s_v.

Definition 8.2.2. We say that the *hyperbolicity condition* is satisfied if for all $v \in \Omega_K$ such that the étale algebra with involution (E^v, σ) is split, the algebra with involution (A^v, τ) is hyperbolic.

The following is a consequence of Propositions 3.4.1. and 3.4.2.

Proposition 8.2.3. *The étale algebra with involution (E^v, σ) can be embedded in the algebra with involution (A^v, τ) for all $v \in \Omega_K$ if and only if the following conditions hold :*

(i) *For all $v \in \Omega_K$, we have*

$$\det(A^v, \tau)\mathrm{disc}(E^v, \sigma)^{-1} \in \mathrm{N}_{F^v/K_v}((F^v)^\times)\mathrm{N}_{L^v/K_v}((L^v)^\times).$$

(iii) *The signature condition is satisfied.*

(iii) *The hyperbolicity condition is satisfied.*

9. Applications and examples

The aim of this section is to describe some special cases in which the Hasse principle for the embedding problem holds, and to give some examples. We keep the notation of the previous sections. In particular, K is a global field, (E, σ) is an étale algebra with involution, and (A, τ) is a central simple algebra with involution.

9.1. The group $Ш(E', \sigma)$

Let us write $E = E_1 \times \cdots \times E_{m_1} \times E_{m_1+1} \times \cdots \times E_m$, where E_i/F_i is a quadratic extension for all $i = 1, \ldots, m_1$ and $E_i = F_i \times F_i$ or $E_i = K$ if $i = m_1+1, \ldots, m$. Recall that $I = \{1, \ldots, m\}$, and set $I(\text{split}) = \{m_1+1, \ldots, m\}$, $I' = I(\text{nonsplit}) = \{1, \ldots, m_1\}$. If I' is empty, then we set $Ш(E', \sigma) = 0$.

Let $\pi : Ш(E, \sigma) \to Ш(E', \sigma)$ be the map that sends the class of (I_0, I_1) to the class of $(I_0 \cap I', I_1 \cap I')$. Then π is surjective, and $\mathrm{Ker}(\pi)$ is the subgroup of $Ш(E, \sigma)$ consisting of the classes of partitions (I_0, I_1) such that $I_0 \subset I(\text{split})$ or $I_1 \subset I(\text{split})$.

Let $f : Ш(E, \sigma) \to \mathbf{Z}/2\mathbf{Z}$ be the Brauer–Manin map (cf. §5.4.). Note that $\mathrm{Ker}(\pi) \subset \mathrm{Ker}(f)$, since if $i \in I(\text{split})$, then $d_i = 1$. Hence f induces a map $\overline{f} : Ш(E', \sigma) \to \mathbf{Z}/2\mathbf{Z}$ such that $f = \overline{f} \circ \pi$.

Proposition 9.1.1. *We have $f = 0$ if and only if $\overline{f} = 0$.*

Proof. This follows immediately from the definitions.

9.2. Sufficient conditions

Assume that for all $v \in \Omega_K$ there exists an embedding $(E^v, \sigma) \to (A^v, \tau)$, and let $\nu : \Delta(E) \to Z(A, \tau)$ be an orientation. The results of Sections 6–8 imply the following :

Theorem 9.2.1. *Suppose that the following conditions hold :*

(i) *For all $v \in \Omega_K$, there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$ with respect to ν.*

(ii) *$Ш(E', \sigma)$ is trivial.*

Then there exists an embedding $(E, \sigma) \to (A, \tau)$.

Proof. This follows from Theorems 6.1.1. 6.2.1. 7.1. 8.1.1. and Proposition 9.1.1.

Note that the existence of an *oriented* embedding is only necessary if (A, τ) is orthogonal, A is non-split and $\deg(A) = 2r$ with r even (cf. Corollary 6.1.2.). Note also that this implies Theorem A of Prasad and Rapinchuk (cf. [PR 10], page 584) – indeed, if E is a field extension of L, then $Ш(E, \sigma)$ $(= Ш(E', \sigma)$ in this case) is obviously trivial. Theorem 9.2.1. also has the following application :

Corollary 9.2.2. *Suppose that the following conditions hold :*

(i) *For all $v \in \Omega_K$, there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$ with respect to ν.*

(ii) *There exists $i_0 \in I$ such that for all $i \in I$, we have*

$$\Sigma(L/K) \cup \Sigma_{i_0} \cup \Sigma_i \neq \Omega_K.$$

Then there exists an embedding $(E, \sigma) \to (A, \tau)$.

This generalizes the Hasse principle results of [PR 10], [Lee 12] and [B 12]. The Corollary is a consequence of Theorem 9.2.1. and the following Lemma :

Lemma 9.2.3. *Assume that there exists* $i_0 \in I$ *such that for all* $i \in I$*, we have* $\Sigma(L/L) \cup \Sigma_{i_0} \cup \Sigma_i \neq \Omega_K$*. Then the group* $Ш(E, \sigma)$ *is trivial. Therefore* $Ш(E', \sigma)$ *is trivial.*

Proof. Suppose that the group $Ш(E, \sigma)$ is not trivial, and let (I_0, I_1) be a partition of I representing a non–trivial element of $Ш(E, \sigma)$. Then we have

$$\Sigma(L/K) \cup (\bigcap_{i \in I_0} \Sigma_i) \cup (\bigcap_{j \in I_1} \Sigma_j) = \Omega_K.$$

Assume that $i_0 \in I_0$. Then we have $\Sigma(L/K) \cup \Sigma_{i_0} \cup (\bigcap_{j \in I_1} \Sigma_j) = \Omega_K$, hence for all $j \in I_1$, we have $\Sigma(L/K) \cup \Sigma_{i_0} \cup \Sigma_j = \Omega_K$, contradicting the hypothesis.

Corollary 9.2.4. *Suppose that the following conditions hold :*

(i) *For all* $v \in \Omega_K$*, there exists an oriented embedding* $(E^v, \sigma) \to (A^v, \tau)$ *with respect to* ν*.*

(ii) *There exists a real place* $u \in \Omega_K$ *such that* $u \notin \Sigma_i$ *for all* $i \in I$*.*

Then there exists an embedding $(E, \sigma) \to (A, \tau)$*.*

Proof. By (ii), condition (ii) of Corollary 9.2.2. holds, hence there exists an embedding $(E, \sigma) \to (A, \tau)$.

Assume now that $K = \mathbf{Q}$. Recall that (E, σ) is a CM étale algebra if E is a product of CM fields, and if σ is the complex conjugation. Then we have

Corollary 9.2.5. *Suppose* $K = \mathbf{Q}$*, and that* (E, σ) *is a CM étale algebra. Assume that for all* $v \in \Omega_K$*, there exists an oriented embedding* $(E^v, \sigma) \to (A^v, \tau)$*. Then there exists an embedding* $(E, \sigma) \to (A, \tau)$*.*

Proof. This follows from Corollary 9.2.4. since condition (ii) holds for CM étale algebras.

9.3. An example

As we have seen in Corollary 9.2.5. above, the local–global principle holds for oriented embeddings when (E, σ) is a CM étale algebra with involution. The aim of this section is to show that this is not the case for not necessarily orientated local embeddings. More precisely, there exist CM étale algebras with involution (E, σ) and (non–split) central simple algebras with orthogonal involution (A, τ) such that (E, σ) embeds into (A, τ) everywhere locally, but not globally.

Let v_1, v_2, v_3 and v_4 be four distinct places of K. Let $a \in K^\times$ be such that $a \notin K_{v_i}^{\times 2}$ for $i = 1, \ldots, 4$, and let $b \in K^\times$ such that $b \notin K^{\times 2}$ and that $b \in K_{v_i}^{\times 2}$ for $i = 1, \ldots, 4$. Let $E_1 = K(\sqrt{a})$, and let $\sigma_1 : E_1 \to E_1$ be the K–linear involution such that $\sigma_1(\sqrt{a}) = -\sqrt{a}$. Set $E_2 = K(\sqrt{b})$, let $\sigma_2 : E_2 \to E_2$ be the K–linear involution such that $\sigma_2(\sqrt{b}) = -\sqrt{b}$. Set $E = E_1 \otimes E_2$ and $\sigma = \sigma_1 \otimes \sigma_2$. Then (E, σ) is a rank 4 étale K–algebra with involution, and $F = E^\sigma = K(\sqrt{ab})$.

Let H_1 be the quaternion skew field over K ramified exactly at v_1 and v_2, and H_2 the quaternion skew field over K ramified exactly at v_3 and v_4. Let $\tau_i : H_i \to H_i$ be the canonical involution for $i = 1, 2$, and set $(A, \tau) = (H_1, \tau_1) \otimes (H_2, \tau_2)$. Since τ_1 and τ_2 are both symplectic involutions, their tensor product τ is an orthogonal involution. We have $H_1 \otimes H_2 \simeq M_2(H)$, where H is a quaternion skew field over K.

Proposition 9.3.1. *For all $v \in \Omega_K$, there exists an embedding of algebras with involution $(E^v, \sigma) \to (A^v, \tau)$.*

Proof. Since E_1 splits H_1 and H_2 locally everywhere, it splits H locally everywhere too, and hence E embeds in H as a maximal subfield globally. Let τ_0 be the canonical involution of H. Since τ_0 restricts to the non–trivial automorphism on any maximal subfield, it follows that there exists an embedding of algebras with involution of (E_1, σ_1) into (H, τ_0).

Let $w \in \Omega_K$. By hypothesis, either H_1 or H_2 is split over K_w. Hence either $(H_1^w, \tau_1) \simeq (M_2(K_w), \sigma_0)$ or $(H_2^w, \tau_2) \simeq (M_2(K_w), \sigma_0)$, where σ_0 denotes the symplectic involution of $M_2(K_w)$. Therefore we have

$$(M_2(H^w), \tau) \simeq (H_1^w \otimes H_2^w, \tau_1 \otimes \tau_2) \simeq (M_2(K_w), \sigma_0) \otimes (H^w, \tau_0).$$

The algebra with involution (E_1^w, σ_1) can be embedded into (H^w, τ_0), and the algebra with involution (E_2^w, σ_2) can be embedded into $(M_2(K_w), \sigma_0)$. Hence (E^w, σ) embeds into $(M_2(H^w), \tau)$.

Proposition 9.3.2. *There is no global embedding $(E, \sigma) \to (A, \tau)$.*

Proof. Let us denote by H_i^0 the skew elements of H_1, for $i = 1, 2$. Then every skew element of $H_1 \otimes H_2$ belongs to the direct sum $H_1^0 \oplus H_2^0$. Moreover, if a skew element is square central, then it has to be in H_1^0 or in H_2^0. Assume by contradiction that there exists an embedding of algebras with involution $f : (E, \sigma) \to (A, \tau)$. Note that $f(\sqrt{b})$ is a square central skew element. Therefore it has to belong to H_1^0 or to H_2^0. But this contradicts the fact that $E_2 = K(\sqrt{b})$ does not split H_1 nor H_2.

In the above example, we can take $K = \mathbf{Q}$ and can choose a and b such that E is a CM étale algebra. This provides the desired counter–example to the Hasse principle.

Appendix A

Embedding functor, Tate–Shafarevich group and orientation

The purpose of this appendix is to recall some of the results of [Lee 14], and to outline the relationship of these results with those of the present paper.

§A1. The embedding functor

Let K be a field of characteristic $\neq 2$, let K_s be a separable closure of K, and let $\Gamma_K = \mathrm{Gal}(K_s/K)$. Let G be a reductive group over K. Let T be a torus and let Ψ be a root datum attached to T (see [SGA 3], Exp. XXI, 1.1.1.). For a maximal torus T' in G, we let $\Phi(G,T')$ be the root datum of G with respect to T'. If $\Phi(G,T')_{K_s}$ and Ψ_{K_s} are isomorphic, then we say that G and Ψ have the same type.

Assume that G and Ψ have the same type. Let $\underline{\mathrm{Isom}}(\Psi, \Phi(G,T'))$ be the scheme of isomorphisms between the root data Ψ and $\Phi(G,T')$. Define

$$\underline{\mathrm{Isomext}}(\Psi, \Phi(G,T')) = \underline{\mathrm{Isom}}(\Psi, \Phi(G,T'))/\mathrm{W}(\Psi),$$

where $\mathrm{W}(\Psi)$ is the Weyl group of Ψ. The scheme $\underline{\mathrm{Isomext}}(\Psi, \Phi(G,T'))$ is independent of the choice of the maximal torus T', and we denote it by $\underline{\mathrm{Isomext}}(\Psi, G)$. An *orientation* is by definition an element of $\underline{\mathrm{Isomext}}(\Psi, G)(K)$.

The *embedding functor* $E(G,\Psi)$ is defined as follows : for any K-algebra C, let $E(G,\Psi)(C)$ be the set of embeddings $f : T_C \to G_C$ such that f is both a closed immersion and a group homomorphism which induces an isomorphism $f^\Psi : \Psi_C \xrightarrow{\sim} \Phi(G_C, f(T_C))$ such that $f^\Psi(\alpha) = \alpha \circ f^{-1}|_{f(T_{C'})}$ for all the C'-roots α in $\Psi_{C'}$ for each C-algebra C' (see [Lee 14], 1.1.) Given an orientation $\nu \in \underline{\mathrm{Isomext}}(\Psi, G)(K)$, we define the *oriented embedding functor* as follows (cf. [Lee 14], 1.2.) : for any K-algebra C, set

$$E(G,\Psi,\nu)(C) = \left\{ f : T_C \hookrightarrow G_C \;\middle|\; \begin{array}{l} f \in E(G,\Psi)(C), \text{ and the image of } f^\Psi \\ \text{in } \underline{\mathrm{Isomext}}(\Psi, G)(C) \text{ is } \nu. \end{array} \right\}.$$

The oriented embedding functor is a homogeneous space under the adjoint action of G. For each root datum Ψ, we can associate a simply connected root datum $\mathrm{sc}(\Psi)$ to it (cf. [SGA3], Exp. XXI, 6.5.5 (iii)]). Let $\mathrm{sc}(T)$ be the torus associated to $\mathrm{sc}(\Psi)$.

§A2. Algebras with involution and the embedding functor

Let L be a field of characteristic $\neq 2$, and let A be a central simple algebra over L with involution τ. Let E be an étale algebra over L with involution σ, and suppose that $L^\sigma = K$. Given (A,τ) and (E,σ), we always assume that

$$\dim_L(E) = \deg_K(A) \text{ and } \tau|_L = \sigma|_L.$$

The unitary groups $\mathrm{U}(A,\tau)$ and $\mathrm{U}(E,\sigma)$ are defined as follows. For any commutative K-algebra C, set

$$\mathrm{U}(A,\tau)(C) = \{x \in A \otimes_K C |\ x\tau(x) = 1\},$$

and

$$\mathrm{U}(E,\sigma)(C) = \{x \in E \otimes_K C |\ x\sigma(x) = 1\}.$$

Let $G = \mathrm{U}(A,\tau)^\circ$ be the connected component of $\mathrm{U}(A,\tau)$ containing the neutral element, and let $T = \mathrm{U}(E,\sigma)^\circ$ be the connected component of $\mathrm{U}(E,\sigma)$ containing the neutral element.

Set $F = E^\sigma$. Let us suppose furthermore that

$$\dim_K(F) = \begin{cases} \lceil \frac{\dim_L(E)}{2} \rceil, & \text{if } \tau \text{ is of the first kind;} \\ \dim_L(E), & \text{if } \tau \text{ is of the second kind.} \end{cases}$$

Then one can associate a root datum Ψ to the torus T such that G is of type Ψ (see [Lee 14], 1.3.). Moreover, except for A of degree 2 with τ orthogonal, there exists a K-embedding from (E,σ) to (A,τ) if and only if there exists an orientation ν such that $E(G,\Psi,\nu)(K)$ is nonempty (see [Lee 14], Theorem 1.15. and Proposition 1.17.).

§A3. Orientations in terms of algebras

Let (E,σ) and (A,τ) be as above. Assume moreover that (A,τ) is orthogonal, and that the degree of A is even. Recall that $\Delta(E)$ is the discriminant of the étale algebra E, and that $Z(A,\tau)$ is the center of the Clifford algebra of (A,τ). In 1.8. an orientation is defined as the choice of an isomorphism $\Delta(E) \to Z(A,\tau)$. This is equivalent to the definition of A 1. More precisely, we have

Proposition A.3.1. *We have an isomorphism*

$$\underline{\mathrm{Isom}}(\Delta(E), Z(A,\tau)) \simeq \underline{\mathrm{Isomext}}(\Psi, G).$$

Proof. Let E_τ be a maximal τ-invariant étale subalgebra of A. Let $T_\tau = \mathrm{U}(E_\tau,\tau)^\circ$; then T_τ is a maximal torus of G. Let $\Phi(G,T_\tau)$ be the root datum of G with respect to T_τ. Then we have a natural map $\alpha : \underline{\mathrm{Isom}}((E,\sigma),(E_\tau,\tau)) \to \underline{\mathrm{Isom}}(\Psi,\Phi(G,T_\tau))$. Using the identification of $\underline{\mathrm{Aut}}(E,\sigma)$ and $\underline{\mathrm{Aut}}(\Psi)$, we see that α is equivariant under the action of $\underline{\mathrm{Aut}}(E,\sigma)$. Let Γ_0 be the subgroup of $\underline{\mathrm{Aut}}(E,\sigma)$ corresponding to the Weyl group of Ψ under this identification. Let us consider the following commutative diagram :

$$\begin{array}{ccc} \underline{\mathrm{Isom}}((E,\sigma),(E_\tau,\tau)) & \longrightarrow & \underline{\mathrm{Isom}}(\Psi,\Phi(G,T_\tau)) \\ \downarrow & & \downarrow \\ \underline{\mathrm{Isom}}((E,\sigma),(E_\tau,\tau))/\Gamma_0 & \longrightarrow & \underline{\mathrm{Isom}}(\Psi,\Phi(G,T_\tau))/\mathrm{W}(\Psi). \end{array}$$

Recall that $\underline{\mathrm{Isom}}(\Psi,\Phi(G,T_\tau))/\mathrm{W}(\Psi) = \underline{\mathrm{Isomext}}(\Psi,\Phi(G,T_\tau))$, and note that we have $\underline{\mathrm{Isom}}((E,\sigma),(E_\tau,\tau))/\Gamma_0 \simeq \underline{\mathrm{Isom}}(\Delta(E),\Delta(E_\tau))$.

If we pick another maximal étale subalgebra E'_τ of A invariant by τ, then the method used for $\underline{\mathrm{Isomext}}(\Psi,\Psi_\tau)$ in [Lee 14] 1.2.1. shows that we have a canonical isomorphism between $\underline{\mathrm{Isom}}(\Delta(E),\Delta(E'_\tau))$ and $\underline{\mathrm{Isom}}(\Delta(E),\Delta(E_\tau))$.

Let us fix an isomorphism $\Delta(E_\tau) \to Z(A,\tau)$ as in 1.8. This gives an isomorphism $\underline{\mathrm{Isom}}(\Delta(E),\Delta(E_\tau)) \to \underline{\mathrm{Isom}}(\Delta(E),Z(A,\tau))$. Hence, we have

$$\underline{\mathrm{Isom}}(\Delta(E),Z(A,\tau)) \simeq \underline{\mathrm{Isomext}}(\Psi,\Phi(G,T_\tau)) = \underline{\mathrm{Isomext}}(\Psi,G),$$

as claimed.

§A4. Tate–Shafarevich group

Assume now that K is a global field. Then, using Borovoi's results (cf. [Bo 99]), it is shown in [Lee 14] that the Brauer-Manin obstruction is the only obstruction to the local-global principle for $E(G,\Psi,u)$ and the obstruction lies in the Tate–Shafarevich group $Ш^2(K,\mathrm{sc}(T))$ (cf.[Lee 14], Proposition 2.8). Note that $Ш^2(K,\mathrm{sc}(T))$ is isomorphic to $Ш^1(K,\mathrm{sc}(\hat{T}))^*$ by Poitou-Tate duality (cf. [NSW 08], Chap. VIII, Thm. 8.6.9).

In the following, we determine the group $Ш^1(K,\mathrm{sc}(\hat{T}))$ explicitly, and show that it is isomorphic to the group $Ш(E',\sigma)$ defined in §9 :

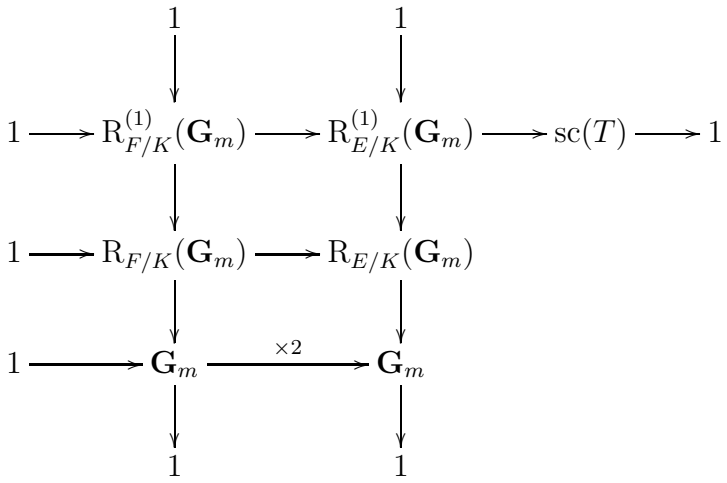
Proposition A.4.1. *The groups* $Ш^1(K,\mathrm{sc}(\hat{T}))$ *and* $Ш(E',\sigma)$ *are isomorphic.*

The proof of this proposition is different according as $L = K$ or $L \neq K$. Let us start by introducing some notation that will be used in both proofs. For any finite separable field extension N/N' and any discrete Γ_N–module M, set $\mathrm{I}_{N/N'}(M) = \mathrm{Ind}_{\Gamma_N}^{\Gamma_{N'}}(M)$. Note that $\mathrm{I}_{N/N'}(\mathbf{Z})$ is the character group of $\mathrm{R}_{N/N'}(\mathbf{G}_m)$. Let $\hat{\mathrm{S}}_{N/N'}$ be the character group of the norm-one torus $\mathrm{R}^{(1)}_{N/N'}(\mathbf{G}_m)$.

Proof of Proposition A.4.1. when $L = K$

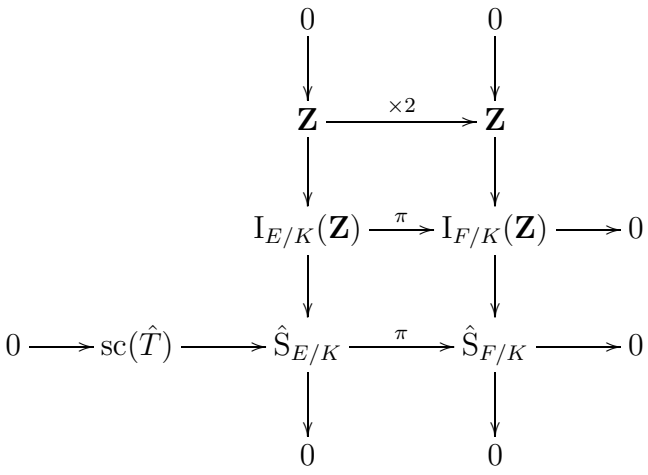
Let us consider the following diagram :

(1)



where the first row (cf. [Lee 14], Lemma 3.16.) and the columns are exact. Then consider the corresponding diagram of character groups :

(2)



Note that we have $\mathrm{I}_{E/K}(\mathbf{Z}) = \overset{m}{\underset{i=1}{\oplus}} \mathrm{I}_{E_i/K}(\mathbf{Z})$ and $\mathrm{I}_{F/K}(\mathbf{Z}) = \overset{m}{\underset{i=1}{\oplus}} \mathrm{I}_{F_i/K}(\mathbf{Z})$. The module $\mathrm{I}_{E_i/K}(\mathbf{Z})$ can also be written as $\mathrm{I}_{F_i/K}(\mathrm{I}_{E_i/F_i}(\mathbf{Z}))$. Let d be the degree map from $\mathrm{I}_{E_i/F_i}(\mathbf{Z}) \simeq \mathbf{Z} \oplus \mathbf{Z}$ to $\mathbf{Z}$, which sends (x, y) to $x + y$. Then on each $\mathrm{I}_{F_i/K}(\mathrm{I}_{E_i/F_i}(\mathbf{Z}))$, the map π is the map induced by the degree map from $\mathrm{I}_{E_i/F_i}(\mathbf{Z})$ to $\mathbf{Z}$.

Set $\Gamma = \Gamma_K$. We derive the following long exact sequence from diagram (2) :

$$0 \to \mathrm{sc}(\hat{T})^{\Gamma} \to (\hat{S}_{E/K})^{\Gamma} \xrightarrow{\pi} (\hat{S}_{F/K})^{\Gamma} \to H^1(K, \mathrm{sc}(\hat{T})) \to H^1(K, \hat{S}_{E/K}).$$

Thus we have the exact sequence

$$0 \to (\hat{S}_{F/K})^{\Gamma}/\pi((\hat{S}_{E/K})^{\Gamma}) \xrightarrow{\delta} H^1(K, \mathrm{sc}(\hat{T})) \to H^1(K, \hat{S}_{E/K})$$

Note that $\mathrm{H}^2(K, \mathrm{R}^{(1)}_{E/K}(\mathbf{G}_m))$ injects into $\mathrm{H}^2(K, \mathrm{R}_{E/K}(\mathbf{G}_m))$ by Hilbert's Theorem 90. By the Brauer-Hasse-Noether Theorem, $Ш^2(K, \mathrm{R}_{E/K}(\mathbf{G}_m))$ vanishes, hence so does $Ш^2(K, \mathrm{R}^{(1)}_{E/K}(\mathbf{G}_m))$. By Poitou-Tate duality, we have

$$Ш^1(K, \hat{\mathrm{S}}_{E/K}) \simeq Ш^2(K, \mathrm{R}^{(1)}_{E/K}(\mathbf{G}_m)))^* = 0.$$

Therefore, $Ш^1(K, \mathrm{sc}(\hat{T}))$ is in the image of $(\hat{S}_{F/K})^{\Gamma}/\pi((\hat{S}_{E/K})^{\Gamma})$.

Since the $F_i's$ are field extensions of K, we have $\mathrm{I}_{F_i/K}(\mathbf{Z})^{\Gamma} \simeq \mathbf{Z}$. Thus, we have $\mathrm{I}_{F/K}(\mathbf{Z})^{\Gamma} \simeq \overset{m}{\underset{i}{\oplus}} \mathrm{I}_{F_i/K}(\mathbf{Z})^{\Gamma} \simeq \mathbf{Z}^m$, and $(\hat{\mathrm{S}}_{F/K})^{\Gamma} \simeq \mathbf{Z}^m/(1, ..., 1)$.

If $E_i = F_i \times F_i$, then π sends $\mathrm{I}_{E_i/K}(\mathbf{Z})^{\Gamma} \simeq \mathrm{I}_{F_i/K}(\mathbf{Z})^{\Gamma} \times \mathrm{I}_{F_i/K}(\mathbf{Z})^{\Gamma}$ surjectively onto $\mathrm{I}_{F_i/K}(\mathbf{Z})^{\Gamma} \simeq \mathbf{Z}$. If $E_i = K$, then $\mathrm{I}_{E_i/K}(\mathbf{Z}) \simeq \mathbf{Z} \simeq \mathrm{I}_{F_i/K}(\mathbf{Z})$. If E_i is a quadratic field extension of F_i, the map π sends $\mathrm{I}_{E_i/K}(\mathbf{Z})^{\Gamma} \simeq \mathbf{Z}$ to $\mathrm{I}_{F_i/K}(\mathbf{Z})^{\Gamma} \simeq \mathbf{Z}$ by multiplication by 2. Recall that $m = m_1 + m_2$, where m_1 is the number of indices i such that E_i is a quadratic field extension of F_i, and m_2 the number of indices i such that either $E_i = F_i \times F_i$ or $E_i = K$. Then we have

$$(\hat{S}_{F/K})^{\Gamma}/\pi((\hat{S}_{E/K})^{\Gamma}) \simeq (\mathbf{Z}/2\mathbf{Z})^{m_1}/(1, ..., 1).$$

We claim that $\delta : (\hat{S}_{F/K})^{\Gamma}/\pi((\hat{S}_{E/K})^{\Gamma}) \to H^1(K, \mathrm{sc}(\hat{T}))$ sends bijectively $Ш(E', \sigma)$ to $Ш^1(K, \mathrm{sc}(\hat{T}))$.

Let $(I_0, I_1) \in Ш(E', \sigma)$, let a be the corresponding element in

$$(\hat{S}_{F/K})^{\Gamma}/\pi((\hat{S}_{E/K})^{\Gamma})$$

and let x be the image of a in $\mathrm{H}^1(K, \mathrm{sc}(\hat{T}))$. We claim that x is in $Ш^1(K, \mathrm{sc}(\hat{T}))$. It suffices to prove that for any $v \in \Omega_K$, we have $a^v = 0$.

For a place $v \in \underset{i \in \mathrm{I}_1}{\cap} \Sigma_i$, we have that E_i^v splits over F_i^v for all $i \in \mathrm{I}_1$. Hence, π maps $\mathrm{I}_{E_i^v/K_v}(\mathbf{Z})^{\Gamma_v} \simeq \mathrm{I}_{F_i^v/K_v}(\mathbf{Z})^{\Gamma_v} \oplus \mathrm{I}_{F_i^v/K_v}(\mathbf{Z})^{\Gamma_v}$ onto $\mathrm{I}_{F_i^v/K_v}(\mathbf{Z})^{\Gamma_v}$ for each $i \in \mathrm{I}_1$, so $(\hat{S}_{F/K})^{\Gamma_v}/\pi((\hat{S}_{E/K})^{\Gamma_v}) = 0$ for each $i \in \mathrm{I}_1$ and $a_i^v = 0$. On the other hand, for each $i \in \mathrm{I}_0$, $a_i = 0$ by definition. Therefore, we have $a^v = 0$.

For a place $v \in \underset{i \in \mathrm{I}_0}{\cap} \Sigma_i$, we replace $(a_1, ..., a_{m_1})$ by $(a_1, ..., a_{m_1}) + (1, ..., 1)$. Note that $(a_1, ..., a_{m_1}) + (1, ..., 1)$ and $(a_1, ..., a_{m_1})$ represent the same class a in $(\hat{S}_{F/K})^{\Gamma}/\pi((\hat{S}_{E/K})^{\Gamma})$. By the same argument as above, we have $a_v = 0$.

Since $(\underset{i\in \mathrm{I}_0}{\cap}\Sigma_i)\cup(\underset{j\in \mathrm{I}_1}{\cap}\Sigma_j)=\Omega_K$, we have $a^v=0$ for all $v\in\Omega_K$, which proves that x is in $Ш^1(K,\mathrm{sc}(\hat{T}))$.

This proves that δ induces a map $Ш(E',\sigma)\to Ш^1(K,\mathrm{sc}(\hat{T}))$. We already know that this map is injective. Let us prove that it is also surjective.

Let $0\neq x\in Ш^1(K,\mathrm{sc}(\hat{T}))$. Let $a\in(\hat{S}_{F/K})^\Gamma/\pi((\hat{S}_{E/K})^\Gamma)$ be the preimage of x, let a^v be the localization of a at the place v, and let $(a_1,...,a_{m_1})$ be a lift of a in $(\mathbf{Z}/2\mathbf{Z})^{m_1}$. Let (I_0,I_1) be the corresponding partition. Now we claim that $(\underset{i\in \mathrm{I}_0}{\cap}\Sigma_i)\cup(\underset{j\in \mathrm{I}_1}{\cap}\Sigma_j)=\Omega_K$. Suppose that $(\underset{i\in \mathrm{I}_0}{\cap}\Sigma_i)\cup(\underset{j\in \mathrm{I}_1}{\cap}\Sigma_j)\neq\Omega_K$, and let $v\in\Omega_K\backslash(\underset{i\in \mathrm{I}_0}{\cap}\Sigma_i)\cup(\underset{j\in \mathrm{I}_1}{\cap}\Sigma_j)$. Therefore there exist $i_0\in \mathrm{I}_0$ and $i_1\in \mathrm{I}_1$ such that $E^v_{i_0}$ is not split over $F^v_{i_0}$ and $E^v_{i_1}$ is not split over $F^v_{i_1}$. Let $F^v_i=\prod_{j=1}^{n_i}L_{i,j}$, where the $L_{i,j}$'s are field extensions of K_v. Let $E^v_i=\prod_{j=1}^{n_i}M_{i,j}$, where $M_{i,j}$ is a quadratic étale algebra over $L_{i,j}$. Set $\Gamma_v=\Gamma_{K_v}$. Then we have

$$\mathrm{I}_{F^v_i/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E^v_i/K_v}(\mathbf{Z})^{\Gamma_v})=\overset{n_i}{\underset{j=1}{\oplus}}\mathrm{I}_{L_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{M_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}).$$

If $M_{i,j}$ is split over $L_{i,j}$, then

$$\mathrm{I}_{M_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}=\mathrm{I}_{L_{i,j}\times L_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}=\mathrm{I}_{L_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}\oplus\mathrm{I}_{L_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v},$$

so the map π sends $\mathrm{I}_{M_{i,j}/k_v}(\mathbf{Z})^{\Gamma_v}$ surjectively to $\mathrm{I}_{L_{i,j}/k_v}(\mathbf{Z})^{\Gamma_v}$. On the other hand, if $M_{i,j}$ is a field extension over $L_{i,j}$, then π maps $\mathrm{I}_{M_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}\simeq\mathbf{Z}$ to $2\mathbf{Z}\subseteq\mathbf{Z}\simeq\mathrm{I}_{L_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}$ and we have

$$\mathrm{I}_{L_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{M_{i,j}/K_v}(\mathbf{Z})^{\Gamma_v})\simeq\mathbf{Z}/2\mathbf{Z}.$$

For $a_i\in\mathrm{I}_{F_i/K}(\mathbf{Z})^\Gamma/\pi(\mathrm{I}_{E_i/K}(\mathbf{Z})^\Gamma)\simeq\mathbf{Z}/2\mathbf{Z}$, the localization map sends a_i diagonally into to $\mathrm{I}_{F^v_i/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E^v_i/K_v}(\mathbf{Z})^{\Gamma_v})\simeq\underset{\substack{j,\ where M_{i,j}\\ is\ non-split}}{\bigoplus}\mathbf{Z}/2\mathbf{Z}$. Let a^v_i be the image of a_i in $\mathrm{I}_{F^v_i/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E^v_i/K_v}(\mathbf{Z})^{\Gamma_v})$. By our choice of v, we have $\mathrm{I}_{F^v_{i_0}/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E^v_{i_0}/K_v}(\mathbf{Z})^{\Gamma_v})$ (resp. $\mathrm{I}_{F^v_{i_1}/K_v}(\mathbf{Z})^{\Gamma_v}/\mathrm{I}_{E^v_{i_1}/K_v}(\mathbf{Z})^{\Gamma_v}$) non-trivial. In particular, $a^v_{i_1}$ is non-zero as a_{i_1} is non-zero. Note that

$$\underset{i}{\oplus}(\hat{\mathrm{S}}_{F^v_i/K_v})^{\Gamma_v}/\pi((\hat{\mathrm{S}}_{E^v_i/K_v})^{\Gamma_v})=\frac{\underset{i}{\oplus}\mathrm{I}_{F^v_i/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E^v_i/K_v}(\mathbf{Z})^{\Gamma_v})}{(\overline{1},...,\overline{1})},$$

where $\overline{1}$ denotes the image of the diagonal element of $\mathrm{I}_{F^v_i/K_v}(\mathbf{Z})^{\Gamma_v}$ in

$$\mathrm{I}_{F^v_i/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E^v_i/K_v}(\mathbf{Z})^{\Gamma_v}).$$

Since $a^v = 0$, either $a_i^v = 0 \in \mathrm{I}_{F_i^v/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E_i^v/K_v}(\mathbf{Z})^{\Gamma_v})$ for all i, or $a_i^v = \overline{1} \in \mathrm{I}_{F_i^v/K_v}(\mathbf{Z})^{\Gamma_v}/\pi(\mathrm{I}_{E_i^v/K_v}(\mathbf{Z})^{\Gamma_v})$ for all i. In particular, this implies that $a_{i_0}^v$ and $a_{i_1}^v$ are both 0 or both 1, which is a contradiction. Therefore we have $(\underset{i\in \mathrm{I}_0}{\cap} \Sigma_i) \cup (\underset{j\in \mathrm{I}_1}{\cap} \Sigma_j) = \Omega_K$ and $(I_0, I_1) \in Ш(E', \sigma)$. This completes the proof of the Proposition.

Proof of Proposition A 4.1. when $L \neq K$.

In this case, the torus $\mathrm{sc}(T)$ fits in the following exact sequence :

$$1 \longrightarrow \mathrm{sc}(T) \longrightarrow \mathrm{R}_{F/K}(\mathrm{R}^{(1)}_{E/F}(\mathbf{G}_m)) \longrightarrow \mathrm{R}^{(1)}_{L/K}(\mathbf{G}_m) \longrightarrow 1 \tag{3}$$

We take the dual sequence of exact sequence (3) :

$$0 \longrightarrow \hat{\mathrm{S}}_{L/K} \xrightarrow{\iota} \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F}) \xrightarrow{p} \mathrm{sc}(\hat{T}) \longrightarrow 0\ , \tag{4}$$

from which we derive the long exact sequence

(5)

$$\ldots \longrightarrow \mathrm{H}^1(K, \hat{\mathrm{S}}_{E/K}) \xrightarrow{\iota^1} \mathrm{H}^1(K, \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F})) \xrightarrow{p^1} \mathrm{H}^1(K, \mathrm{sc}(\hat{T})) \longrightarrow \mathrm{H}^2(K, \hat{\mathrm{S}}_{E/K})\ .$$

By Poitou-Tate duality, we have $Ш^2(K, \hat{\mathrm{S}}_{E/K}) \simeq Ш^1(K, \mathrm{R}^{(1)}_{E/K}(\mathbf{G}_m))^*$. We claim that $Ш^2(K, \hat{\mathrm{S}}_{E/K}) \simeq Ш^1(K, \mathrm{R}^{(1)}_{E/K}(\mathbf{G}_m))^* = 0$. To see this, we consider the following exact sequence :

$$1 \longrightarrow \mathrm{R}^{(1)}_{L/K}(\mathbf{G}_m) \longrightarrow \mathrm{R}_{L/K}(\mathbf{G}_m) \longrightarrow \mathbf{G}_m \longrightarrow 1\ ,$$

By Hilbert Theorem 90, we have $\mathrm{H}^1(K, \mathrm{R}^{(1)}_{L/K}(\mathbf{G}_m)) = K^\times/\mathrm{N}_{L/K}(L^\times)$, where $\mathrm{N}_{L/K}$ is the norm map from L to K. Since the norms of the quadratic extension L over K satisfy the local-global principle, we have $Ш^1(K, \mathrm{R}^{(1)}_{L/K}(\mathbf{G}_m)) = 0$. Hence $Ш^2(K, \hat{\mathrm{S}}_{L/K}) = 0$. Therefore the Tate–Shafarevich group $Ш^1(K, \mathrm{sc}(\hat{T}))$ lies in the image of $\mathrm{H}^1(K, \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F}))$.

Let us consider the following exact sequence :

$$1 \longrightarrow \mathbf{G}_m \longrightarrow \mathrm{R}_{L/K}(\mathbf{G}_m) \xrightarrow{\pi} \mathrm{R}^{(1)}_{L/K}(\mathbf{G}_m) \longrightarrow 1\ , \tag{6}$$

where $\pi(x) = x/\sigma(x)$. Considering the dual sequence, we get

$$0 \longrightarrow \hat{\mathrm{S}}_{L/K} \longrightarrow \mathrm{I}_{L/K}(\mathbf{Z}) \xrightarrow{d} \mathbf{Z} \longrightarrow 0\ , \tag{7}$$

where d is the degree map which maps $(a,b) \in \mathbf{Z} \oplus \mathbf{Z} \simeq \mathrm{I}_{L/K}(\mathbf{Z})$ to $a+b$. Taking the long exact sequence of (7), we have

$$(8) \qquad \mathrm{I}_{L/K}(\mathbf{Z})^{\Gamma} \xrightarrow{d} \mathbf{Z} \longrightarrow \mathrm{H}^1(K, \hat{\mathrm{S}}_{L/K}) \longrightarrow \mathrm{H}^1(K, \mathrm{I}_{L/K}(\mathbf{Z})) = 0 \, .$$

Since L is a quadratic field extension of K, we have

$$\mathrm{H}^1(K, \hat{\mathrm{S}}_{L/K}) \simeq \mathbf{Z}/d(\mathrm{I}_{L/K}(\mathbf{Z})^{\Gamma}) = \mathbf{Z}/2\mathbf{Z}.$$

Similarly, we have

$$\mathrm{H}^1(K, \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F})) = \mathrm{H}^1(F, \hat{\mathrm{S}}_{E/F}) = \prod_{i=1}^{m} \mathrm{H}^1(F_i, \hat{\mathrm{S}}_{E_i/F_i})$$

If $E_i = F_i \times F_i$, then $\mathrm{H}^1(F_i, \hat{\mathrm{S}}_{E_i/F_i}) = 0$ since d is surjective. If E_i is a quadratic extension of F_i, then $\mathrm{H}^1(F_i, \hat{\mathrm{S}}_{E_i/F_i}) = \mathbf{Z}/2\mathbf{Z}$. Recall that $m = m_1 + m_2$ where m_1 is the number of indices i such that E_i is a quadratic extension of F_i, and m_2 the number of indices i such that $E_i = F_i \times F_i$. Then we have $\mathrm{H}^1(K, \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F})) \simeq (\mathbf{Z}/2\mathbf{Z})^{m_1}$.

The map $\iota^1 : \mathrm{H}^1(K, \hat{\mathrm{S}}_{L/K}) \to \mathrm{H}^1(K, \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F}))$ maps $\mathbf{Z}/2\mathbf{Z}$ diagonally into $(\mathbf{Z}/2\mathbf{Z})^{m_1}$. Therefore, we have

$$Ш^1(k, \mathrm{sc}(\hat{T})) \subseteq \mathrm{Im}(p^1) \simeq (\mathbf{Z}/2\mathbf{Z})^{m_1}/(1, ..., 1).$$

Let us show that p^1 maps $Ш(E', \sigma)$ bijectively to $Ш(K, \mathrm{sc}(\hat{T}))$.

Let $(I_0, I_1) \in Ш(E', \sigma)$, and let a in $\mathrm{H}^1(K, \mathrm{I}_{F/K}(\hat{\mathrm{S}}_{E/F}))$ be the corresponding element. We want to show that $p^1(a) \in Ш^1(K, \mathrm{sc}(\hat{T}))$. Let $v \in \Omega_K$. If $v \in \Sigma(L/K)$ or $v \in \bigcap\limits_{j \in \mathrm{I}_1} \Sigma_j$, then $a^v = 0$. Hence, it suffices to prove that for $v \in \Omega_K \setminus (\Sigma(L/K) \cup (\bigcap\limits_{i \in \mathrm{I}_1} \Sigma_i))$, we have $a^v = \iota^1_v(1) = \iota^1(1)_v$. Since $\Sigma(L/K) \cup (\bigcap\limits_{i \in \mathrm{I}_0} \Sigma_i) \cup (\bigcap\limits_{j \in \mathrm{I}_1} \Sigma_j) = \Omega_K$, we have $v \in (\bigcap\limits_{i \in \mathrm{I}_0} \Sigma_i)$. Consequently, for all $i \in \mathrm{I}_0$, we have $\mathrm{H}^1(F_i, \hat{\mathrm{S}}_{E_i^v/F_i^v}) = 0$ and the projection of $\iota^1_v(1)$ to these components are trivial. For $i \in \mathrm{I}_1$, we have that a_i and the $i-th$ coordinate of $\iota^1(1)$ are both 1, so their images in $\mathrm{H}^1(F_i^v, \hat{\mathrm{S}}_{E_i^v/F_i^v})$ are equal. This proves that $a^v = \iota^1_v(1)$, hence $p^1(a^v) = 0$.

We next show that the restriction of p^1 to $Ш(E', \sigma)$ is surjective onto $Ш^1(K, \mathrm{sc}(\hat{T}))$.

Let $a = (a_1, ..., a_{m_1}) \in (\mathbf{Z}/2\mathbf{Z})^{m_1} \simeq \mathrm{H}^1(K, \mathrm{I}_{E^\sigma/k}(\hat{\mathrm{S}}_{E/F}))$ and let (I_0, I_1) be the associated partition. If $a = 0$ or $a = (1, ..., 1)$, then a is in the image of ι^1 and $p^1(a) = 0 \in Ш^1(K, \mathrm{sc}(\hat{T}))$. Hence, we may assume that I_0 and I_1 are non-empty. We claim that

$0 \neq p^1(a) \in Ш^1(K, \mathrm{sc}(\hat{T}))$ if and only if I_0 and I_1 are non-empty and

$$\Sigma(L/K) \cup (\bigcap_{i\in \mathrm{I}_0} \Sigma_i) \cup (\bigcap_{j\in \mathrm{I}_1} \Sigma_j) = \Omega_K.$$

Suppose that $0 \neq p^1(a) \in Ш^1(K, \mathrm{sc}(\hat{T}))$. Let $v \in \Omega_K \setminus (\Sigma(L/K) \cup (\bigcap_{i\in \mathrm{I}_0} \Sigma_i))$. Since $v \notin \Sigma(L/K)$, we have $\mathrm{H}^1(L^v, \hat{\mathrm{S}}_{L^v/K_v}) = \mathbf{Z}/2\mathbf{Z}$. Let a^v denote the localization of a at v. Since $p^1(a) \in Ш^1(K, \mathrm{sc}(\hat{T}))$, we have a^v in the image of ι_v^1, so either $a^v = 0$ or $a^v = \iota_v^1(1)$. It suffices to show that $v \in \bigcap_{i\in \mathrm{I}_1} \Sigma_i$. Consider the i-th component of $(\mathbf{Z}/2\mathbf{Z})^{m_1}$, which corresponds to $\mathrm{H}^1(K, \mathrm{I}_{F_i/K}(\hat{\mathrm{S}}_{E_i/F_i})) = \mathrm{H}^1(F_i, \hat{\mathrm{S}}_{E_i/F_i})$. If E_i splits over F_i at a place $v \in \Omega_K$, then by the exact sequence (8), the map d is surjective and $\mathrm{H}^1(F_i^v, \hat{\mathrm{S}}_{E_i^v/F_i^v}) = 0$, which means that the i-th component vanishes at place v. Since $v \notin \bigcap_{i\in \mathrm{I}_0} \Sigma_i$, there exists $i \in \mathrm{I}_0$ such that E_i^v is not split over F_i^v. Let $F_i^v = \prod_{j=1}^{n_i} L_{i,j}$, where $L_{i,j}$'s are field extensions of K_v. Let $E_i^v = \prod_{j=1}^{n_i} M_{i,j}$, where $M_{i,j}$ is a quadratic étale algebra over $L_{i,j}$. Then

$$\mathrm{H}^1(F_i^v, \hat{\mathrm{S}}_{E_i^v/F_i^v}) = \prod_j \mathrm{H}^1(L_{i,j}, \hat{\mathrm{S}}_{M_{i,j}/L_{i,j}}).$$

By the choice of i, there is j such that $M_{i,j}$ is not split over $L_{i,j}$, and hence $\mathrm{H}^1(L_{i,j}, \hat{\mathrm{S}}_{M_{i,j}/L_{i,j}}) \neq 0$. Then the projection of $\iota_v^1(1)$ to $\mathrm{H}^1(L_{i,j}, \hat{\mathrm{S}}_{M_{i,j}/L_{i,j}})$ is 1. On the other hand, the projection of a^v to the same component is 0 since $i \in \mathrm{I}_0$. Therefore, $a^v = 0$ which means that $\mathrm{H}^1(F_i^v, \hat{\mathrm{S}}_{E_i^v/F_i^v}) = 0$ for all $i \in \mathrm{I}_1$, hence $v \in \bigcap_{i\in \mathrm{I}_1} \Sigma_i$. This proves that $a \in Ш(E', \sigma)$.

Appendix B

Orthogonal involutions and maximal subfields

Let K be a global field of characteristic $\neq 2$, and let Ω_K be the set of places of K. The purpose of this appendix is to give a new proof of Theorem B of Prasad and Rapinchuk (see [PR 10], Introduction, page 586) using some of the results of the present paper, in particular the local embedding conditions of §3. Theorem B has two parts. The proof of the first part will be presented in the first section of this appendix, and the proof of the second one in the second section. The application to maximal subfields determining orthogonal involutions of degree divisible by 4 is given in §B3.

We thank Gopal Prasad for encouraging us to include our proofs of these results in our paper.

§B1. First part of Theorem B

We start by recalling the dimension condition :

Definition B.1.1. Let E be an n–dimensional commutative étale K–algebra, and let $\sigma : E \to E$ be a K–linear involution. Let $F = E^{\sigma}$. We say that (E, σ) satisfies the *dimension condition* if $\dim_K(F) = [\frac{n+1}{2}]$.

The following result was proved by Prasad and Rapinchuk (cf. [PR 10], Theorem B (i), Introduction, page 586 ; see also [PR 10], Theorem 9.4.) :

Theorem B.1. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with orthogonal involutions with* $\deg(A_1) = \deg(A_2) = n$, *with $n \geq 3$. Suppose that the A_i's have the same isomorphism classes of n–dimensional commutative étale algebras invariant under the involutions satisfying the dimension condition. Then for all $v \in \Omega_K$, we have $(A^v, \tau_1) \simeq (A^v, \tau_2)$.*

Definition B.1.2. Let (A, τ) be an orthogonal involution, with $\deg(A) = n$. Let $v \in \Omega_K$ and let E be a τ–invariant rank n étale subalgebra of A^v satisfying the dimension condition. An n–dimensional τ–invariant subalgebra $\tilde{E}$ of A is called a *lifting* of E if $(\tilde{E}, \tau) \simeq (E, \tau)$ over K_v.

Lemma B.1.3. *Let (A, τ) be an orthogonal involution, with* $\deg(A) = n$. *Let $v \in \Omega_K$ and let E be an n–dimensional τ–invariant étale subalgebra of A^v satisfying the dimension condition. Then E has a lifting in A.*

Proof. See for instance [PR 10] , Proposition 2.4.

Lemma B.1.4. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with orthogonal involutions with* $\deg(A_1) = \deg(A_2) = n$. *Suppose that the A_i's have a common n–dimensional commutative étale subalgebra invariant under the involutions satisfying the dimension condition. Then we have* $\mathrm{disc}(A_1, \tau_1) = \mathrm{disc}(A_2, \tau_2)$.

Proof. Let E be an n–dimensional τ_1–invariant subalgebra of A_1 satisfying the dimension condition such that (E, τ_1) embeds into (A_2, τ_2). By Proposition 1.6.1. we have $\mathrm{disc}(A_1, \tau_1) = \mathrm{disc}(E) = \mathrm{disc}(A_2, \tau_2)$.

Proposition B.1.5. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with orthogonal involutions with* $\deg(A_1) = \deg(A_2) = n$, *with $n \geq 3$. Suppose that the A_i's have the same isomorphism classes of n–dimensional commutative étale algebras invariant under the involutions satisfying the dimension condition. Then we have the following*

(i) $\mathrm{disc}(A_1, \tau_1) = \mathrm{disc}(A_2, \tau_2)$.

(ii) *The algebras A_1 and A_2 are isomorphic.*

(iii) *Let $v \in \Omega_K$ be such that A_1^v and A_2^v are split, and let q_1 and q_2 be quadratic forms inducing the involutions τ_1 and τ_2. Then the Witt indices of q_1 and q_2 are equal.*

Proof. (i) This follows from Lemma B.1.4.

(ii) If n is odd, then A_1 and A_2 are both split, hence they are isomorphic. Let us assume that n is even, and set $n = 2r$. Let $v \in \Omega_K$. Then for $i = 1, 2$, either A_i^v is split or it is isomorphic to $M_r(D)$, where D is the unique quaternion division algebra over K_v. Hence it suffices to prove that for all $v \in \Omega$, the algebra A_1^v splits if and only if A_2^v splits.

Let $v \in \Omega_K$ be a place such that $A_1^v \simeq M_r(D)$. Let τ_1 be induced by a hermitian form h_1 over D. Suppose that A_2^v splits, and that τ_2 is induced by a quadratic form q_2 over K_v. We claim that q_2 is isotropic.

Assume first that v is a finite place. For $n \geq 5$ all quadratic forms are isotropic (cf. [Sch 85], 6.4.2.). For $n = 4$, if q_2 is anisotropic, then the determinant of q_2 is trivial. Since $\mathrm{disc}(A_1, \tau_1) = \mathrm{disc}(A_2, \tau_2) = 1$, the 2–dimensional hermitian form h_1 over D is hyperbolic (cf. [T 61], Theorem 3.). Then there exists an n–dimensional τ_1–invariant étale subalgebra E_1 of A_1^v satisfying the dimension condition such that (E_1, τ_1) is split. Let E be a lifting of E_1 in A_1. Then (E, τ_1) can be embedded into (A_2, τ_2). Since $(E^v, \tau_1) \simeq (E_1^v, \tau_1)$ is split, by Proposition 3.1.1. this implies that (A_2^v, τ_2) is hyperbolic, which contradicts the assumption that q_2 is anisotropic. Therefore q_2 is isotropic.

Suppose now that v is a real place. Let $k = [\frac{r}{2}]$, and let $E_1 = \mathbf{C}^k \times \mathbf{C}^k \times \mathbf{C}^{r-2k}$, and let $\sigma : E_1 \to E_1$ be the involution which exchanges the two copies of $\mathbf{C}^k$, and acts on $\mathbf{C}^{r-2k}$ as the complex conjugation. Then (E_1, σ) can be embedded into (A_1^v, τ_1) (cf. Proposition 3.1.2.), hence we can assume that the restriction of τ_1 to E_1 is σ. Let E be a lifting of E_1 in A_1. Since (E, τ_1) can be embedded into (A_2, τ_2), by Proposition 3.1.2. the signature of q_2 is of the form $(2k+2s, 2k+2s')$ for some non–negative integers s, s'. Note that $k \geq 1$, since $n \geq 3$. Hence q_2 is isotropic.

Let $v \in \Omega_K$, and let us write $q_2 \simeq q_0 \oplus q$, with q_0 hyperbolic and q anisotropic. Let $\dim(q_0) = 2m$; since q_2 is isotropic, we have $m \geq 1$. Then there exists a τ_2–invariant commutative étale subalgebra $E_2 = K_v^m \times K_v^m \times E'$ of A_2^v satisfying the dimension condition such that τ_2 permutes the two copies of K_v^m. Let E be a lift of E_2. Since (E, τ_2) can be embedded into (A_1, τ_1), we see that K_v splits A_1^v, which is a contradiction.

Therefore for all $v \in \Omega_K$, the algebra A_1^v splits if and only if A_2^v splits. This implies that A_1 and A_2 are isomorphic. If v is a place such that A_1^v and

A_2^v are split, the above argument also shows that the Witt indices of q_1 and q_2 are equal, and this proves (iii).

Proposition B.1.6. *Let A be a central simple K–algebra of degree n, and let $\tau_1 : A \to A$ and $\tau_2 : A \to A$ be two orthogonal involutions. Assume that we have*

(i) $\mathrm{disc}(A, \tau_1) = \mathrm{disc}(A, \tau_2)$.

(ii) *Let $v \in \Omega_K$ be such that A^v is split, and let q_1 and q_2 be quadratic forms inducing the involutions τ_1 and τ_2. Then the Witt indices of q_1 and q_2 are equal.*

Then for all $v \in \Omega_K$, the algebras with involution (A^v, τ_1) and (A^v, τ_2) are isomorphic.

Proof. If $v \in \Omega_K$ is a real place such that A^v splits, then having the same Witt index implies that q_1 and q_2 have the same signature, hence they are isomorphic. Therefore we have $(A^v, \tau_1) \simeq (A^v, \tau_2)$. For a real place v such that A^v is not split, we have $(A^v, \tau_1) \simeq (A^v, \tau_2)$ (cf. [Sch 85], 10.3.7). Therefore for all real places $v \in \Omega_K$, we have $(A^v, \tau_1) \simeq (A^v, \tau_2)$.

Let $v \in \Omega_K$ be a finite place. Assume first that A^v is non-split. By (i) we have $\mathrm{disc}(A^v, \tau_1) = \mathrm{disc}(A, \tau_2)$, and this implies that $(A^v, \tau_1) \simeq (A^v, \tau_2)$ (cf. [T 61], Theorem 3.).

Assume now that v is a finite place such that A^v is split. Since q_1 and q_2 have the same Witt index, it remains to prove that their anisotropic parts are similar. Let n_0 be the dimension of the anisotropic parts of q_1 and q_2. We are reduced to the case where $n_0 \leq 4$, and the quadratic forms q_1 and q_2 are anisotropic of dimension n_0. If $n_0 = 4$, then there is only one isomorphism class of anisotropic forms, hence $q_1 \simeq q_2$. Recall that we have $\det(q_1) = \det(q_2)$. Two anisotropic forms of dimension ≤ 3 having the same determinant are similar. Therefore q_1 and q_2 are similar, hence $(A^v, \tau_1) \simeq (A^v, \tau_2)$. This completes the proof of the Proposition.

Proof of Theorem B.1. By Proposition B.1.5. we can assume that $A_1 = A_2 = A$, and that conditions (i) and (ii) of Proposition B.1.6. are fulfilled. Hence Proposition B.1.6. implies the Theorem.

If n is even, having the same invariant *subfields* is enough. In order to prove this, we need a few lemmas :

Lemma B.1.7. *Let k be a local field, let $r \geq 1$ be an integer, and let $\delta \in k^\times/k^{\times 2}$. Assume that one of the following holds*

(i) *$\delta \neq 1$ in $k^\times/k^{\times 2}$.*

(ii) *r is even, and $\delta = 1$ in $k^\times/k^{\times 2}$.*

Then we have the following :

(iii) *There exists a degree r field extension M of k and $x \in M^\times$ such that $x \notin M^{\times 2}$ and that $\mathrm{N}_{M/k}(x) = \delta \in k^\times/k^{\times 2}$.*

(iv) *There exists a tower of field extensions $N/M/k$ with $[M : k] = r$ and $[N : M] = 2$ such that the discriminant of N is δ.*

Proof. Let us prove (iii). Assume first that (i) holds. Suppose that δ is a unit, and let M be the unique unramified extension of k of degree r. Let x be a unit of M such that $\mathrm{N}_{M/k}(x) = \delta$. Then $x \notin M^{\times 2}$.

Suppose that $\delta = \pi$, where π is a uniformizer of K. Let $f(X) = X^r + (-1)^r\pi$, and let $M = k[X]/(f)$. Let x be the image of X in M. Then we have $\mathrm{N}_{M/k}(x) = \pi$, and $x \notin M^{\times 2}$.

Assume that (ii) holds, and let $r = 2m$. Let M/k be unramified of degree $2m$. Let π be a uniformizer of k. Then π is also a uniformizer of M, hence $\pi \notin M^{\times 2}$. We have $\mathrm{N}_{M/K}(\pi) = \pi^{2m}$, hence $\mathrm{N}_{M/K}(\pi) \in k^{\times 2}$. Set $x = \pi$.

Therefore (iii) is proved. Let us prove (iv). With M and x as in (iii), let us set $N = M(\sqrt{x})$. Then N and M have the required properties, hence (iv) is proved.

Lemma B.1.8. *Let (A, τ) be an orthogonal involution, with $\deg(A) = 2r$ with $r \geq 2$. Let S be a finite subset of Ω_K and for all $v \in S$, let $E(v)$ be an n–dimensional τ–invariant étale subalgebra of A^v satisfying the dimension condition. Then the algebras $E(v)$ for $v \in S$ have a common lifting in A which is a degree $2r$ field extension of K.*

Proof. Assume first that r is even, or $\mathrm{disc}(A, \tau) \neq 1 \in K^\times/K^{\times 2}$. Let $\delta = \mathrm{disc}(A, \tau) \in K^\times/K^{\times 2}$. Let $w \in \Omega_K$ be a finite place such that $w \notin S$, and that if $\delta \neq 1 \in K^\times/K^{\times 2}$, then $\delta \notin K_w^{\times 2}$. Let N and M be as in Lemma B.1.7. (iv) and let $\sigma : N \to N$ be the K_w–linear involution with fixed field M. Note that since $\mathrm{disc}(N) = \delta$ and (N, σ) is not split, Proposition 3.1.1. (ii) implies that (N, σ) can be embedded into (A^w, τ). By [PR 10], Proposition 2.4. there exists an étale subalgebra E of A which is a common lifting of N and $E(v)$, for all $v \in S$. Since N is a field, E is a field as well.

Suppose now that r is odd and that $\mathrm{disc}(A, \tau) = 1 \in K^\times/K^{\times 2}$. Then by hypothesis we have $r \geq 3$; let us write $r = m + 3$. Let v_1 and v_2 be two distinct finite places of K such that $v_1, v_2 \notin S$, that A^{v_1} and A^{v_2} are split, and that (A^{v_2}, τ) is hyperbolic.

Let π be a uniformizer at v_1, and let μ be an unit such that $\mu \notin K_{v_1}^{\times 2}$. Then K_{v_1} has exactly four square classes, and they are represented by 1, μ,

π and $\mu\pi$. Set $E_1 = K_{v_1}(\sqrt{\mu})$, $E_2 = K_{v_1}(\sqrt{\pi})$, and $E_3 = K_{v_1}(\sqrt{\mu}\pi)$. Let $\sigma_i : E_i \to E_i$ be the non-trivial automorphism of E_i/K_{v_1} for all $i = 1, 2, 3$. If $m > 0$, let $E_4 = K_{v_1}^m \times K_{v_1}^m$, and let $\sigma_4 : E_4 \to E_4$ be the involution which exchanges the two copies of K_{v_1}. Set $E(v_1) = E_1 \times E_2 \times E_3 \times E_4$, and let $\sigma(v_1) : E(v_1) \to E(v_1)$ be the involution which is equal to σ_i on E_i. Then $(E(v_1), \sigma(v_1))$ is a non–split rank $2r$ étale algebra of discriminant 1 satisfying the dimension condition. Hence $(E(v_1), \sigma(v_1))$ can be embedded into (A, τ) by Proposition 3.1.1. (ii). Let us denote by $(E(v_1), \tau)$ the image of $(E(v_1), \sigma(v_1))$ in (A^{v_1}, τ).

Let L be the unramified extension of degree r of K_{v_2}. Since r is odd, we have $\mathrm{disc}(L) = 1 \in K_{v_2}^\times / K_{v_2}^{\times 2}$. Let $E(v_2) = L \times L$, and let $\sigma(v_2) : E(v_2) \to E(v_2)$ be the involution exchanging the two copies of L. Then $(E(v_2), \sigma(v_2))$ is a split rank $2r$ étale algebra with involution satisfying the dimension condition. Since A^{v_2} is split and (A^{v_2}, τ) is hyperbolic, $(E(v_2), \sigma(v_2))$ can be embedded into (A^{v_2}, τ) by Proposition 3.1.1. (i). Let us denote by $(E(v_2), \tau)$ the image of $(E(v_2), \sigma(v_2))$ in (A^{v_2}, τ).

Let (E, τ) be a common lifting of $(E(v_1), \tau)$, $(E(v_2), \tau)$ and of $(E(v), \tau)$ for $v \in S$; such a lifting exists by [PR 10], Proposition 2.4. Let F be the subalgebra of τ–symmetric elements of E. Then F is a field, since F^{v_2} is a field. Moreover, (E, τ) is not split, since $(E(v_1), \tau)$ is not split. Therefore E is a degree $2r$ field extension of K. This completes the proof of the proposition.

We have the following strengthening of Proposition B.1.5. :

Proposition B.1.9. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with orthogonal involutions with $\deg(A_1) = \deg(A_2) = 2r$ with $r \geq 2$. Suppose that the A_i's have the same isomorphism classes of $2r$–dimensional subfields invariant under the involutions satisfying the dimension condition. Then*

(i) $\mathrm{disc}(A_1, \tau_1) = \mathrm{disc}(A_2, \tau_2)$.

(ii) *The algebras A_1 and A_2 are isomorphic.*

(iii) *Let $v \in \Omega_K$ be such that A_1^v and A_2^v are split, and let q_1 and q_2 be quadratic forms inducing the involutions τ_1 and τ_2. Then the Witt indices of q_1 and q_2 are equal.*

Proof. (i) follows from Lemma B.1.4. The proofs of (ii) and (iii) follow the pattern of the proof of Proposition B.1.5. with the following modifications. By Lemma B.1.8. the algebras E_1 and E_2 appearing in the proof of Proposition B.1.5. have liftings that are subfields of A_1 respectively A_2. Since we are assuming that A_i's have the same isomorphism classes of $2r$–dimensional subfields invariant under the involutions satisfying the dimension condition,

the arguments of the proof of Proposition B.1.5. apply and we get the desired conclusion.

Therefore we obtain the following :

Theorem B.1'. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with orthogonal involutions with $\deg(A_1) = \deg(A_2) = 2r$, with $r \geq 2$. Suppose that the A_i's have the same isomorphism classes of maximal subfields invariant under the involutions satisfying the dimension condition. Then for all $v \in \Omega_K$, we have $(A^v, \tau_1) \simeq (A^v, \tau_2)$.*

Proof. By Proposition B.1.9. we may assume that $A_1 = A_2 = A$, and that conditions (i) and (ii) of Proposition B.1.6. are fulfilled. Hence Proposition B.1.6. implies the Theorem.

§B2. Second part of Theorem B

We now prove the second part of Theorem B of Prasad and Rapinchuk (cf. [PR 10], Introduction, page 586, and Theorem 8.1.). Let A be a central simple K–algebra, let $\tau : A \to A$ be an orthogonal involution of degree $4m$.

Let $\mathcal{J} = \mathcal{J}(A, \tau)$ be the set of orthogonal involutions $\eta : A \to A$ such that $(A^v, \eta) \simeq (A^v, \tau)$ for all $v \in \Omega_K$. Let Ω' be the set of places $v \in \Omega_K$ such that A^v is not split and that $Z(A^v, \tau) = K_v \times K_v$.

Theorem B.2. *We have the following :*

(i) *Let $\eta \in \mathcal{J}$. Then there exists an η–invariant maximal subfield E_η of A satisfying the dimension condition such that (E_η^v, η) is split for all $v \in \Omega'$.*

(ii) *Let $\eta \in \mathcal{J}$, and let E_η be an η–invariant subalgebra of A of rank $4m$ such that (E_η^v, η) is split for all $v \in \Omega'$. Let $\gamma \in \mathcal{J}$. If (E_η, η) embeds into (A, γ), then the algebras with involution (A, η) and (A, γ) are isomorphic.*

Proof. (i) Let $v \in \Omega'$. Then we have $A \simeq M_{2m}(D(v))$, where $D(v)$ is the unique quaternion division algebra over K_v. By hypothesis, we have $\mathrm{disc}(A, \eta) = 1 \in K^\times / K^{\times 2}$. By [T 61], Theorem 3. this implies that (A, η) is hyperbolic. Let $L(v)$ be a quadratic extension of K_v splitting $D(v)$ and set $E(v) = L(v)^m \times L(v)^m$. Let us endow $E(v)$ with the involution $\sigma(v) : E(v) \to E(v)$ which exchanges the two copies of $L(v)$. By Propositions 3.1.1. and 3.1.2. there exists an embedding of algebras with involution $(E(v), \sigma(v)) \to (A^v, \eta)$. By Lemma B.1.8. there exists a η–invariant subfield E_η of A such that $(E_\eta^v, \eta) \simeq (E(v), \sigma(v))$ for all $v \in \Omega'$.

(ii) Let E_η be an η–invariant étale subalgebra of A satisfying the dimension condition such that (E_η, η) is split over K_v for all $v \in \Omega'$. Let F_η be the subalgebra of η–symmetric elements of E_η, and let $d \in F_\eta^\times$ such that

$E_\eta = F_\eta(\sqrt{d})$. Let $\gamma \in \mathcal{J}$, and assume that there exists an embedding of algebras with involution $(E_\eta, \eta) \to (A, \gamma)$. By Proposition 1.1.3. there exists $a \in F_\eta^\times$ such that $(A, \eta_a) \simeq (A, \gamma)$. We claim that $(A, \eta_a) \simeq (A, \eta)$.

Let Ω_1 be the set of places of K such that A^v is non-split and that $Z(A^v, \tau)$ is a field. Let Ω_2 be the set of places of K such that A^v is split. Note that we have $\Omega_K = \Omega' \cup \Omega_1 \cup \Omega_2$. We have compatible orientations $u : \Delta(E_\eta) \to Z(A, \eta)$ and $u_a : \Delta(E_\eta) \to Z(A, \eta_a)$. We regard $C(A, \eta_a)$ and $C(A, \eta)$ as $\Delta(E_\eta)$–algebras via u_a and u. By Proposition 2.5.4. we have $C(A, \eta_a) = C(A, \eta) + \mathrm{res}_{\Delta(E_\eta)/K}\mathrm{cor}_{F_\eta/K}(a, d)$ in $\mathrm{Br}(\Delta(E_\eta))$.

Let $v \in \Omega'$. Then (E_η^v, η) is split by hypothesis, hence we have $d \in (F_\eta^v)^{\times 2}$. Therefore $\mathrm{cor}_{F_\eta^v/K}(a, d) = 0$, and hence we have $C(A^v, \eta_a) = C(A^v, \eta)$ in $\mathrm{Br}(\Delta(E_\eta^v))$.

Let $v \in \Omega_1$. Then $Z(A^v, \eta)$ is a field, hence $\Delta(E_\eta^v)$ is also a field. Thus $\mathrm{res}_{\Delta(E_\eta^v)/K}\mathrm{cor}_{F_\eta^v/K}(a, d) = 0$, hence we have $C(A^v, \eta_a) = C(A^v, \eta)$ in $\mathrm{Br}(\Delta(E_\eta^v))$.

Let $v \in \Omega_2$. Then A^v is split, and hence (A^v, η) admits improper similitudes. Hence there exists an isomorphism of algebras with involution $\mathrm{Int}(\alpha) : (A^v, \eta_a) \to (A^v, \eta)$ such that $u = c(\alpha) \circ u_a$. Therefore $C(A^v, \eta_a)$ is isomorphic to $C(A^v, \eta)$ as $\Delta(E_\eta^v)$–algebras.

Hence we have $C(A^v, \eta_a) = C(A^v, \eta)$ in $\mathrm{Br}(\Delta(E_\eta^v))$ for all $v \in \Omega_K$. By the Hasse–Brauer–Noether theorem, this implies that $C(A, \eta_a) = C(A, \eta)$ in $\mathrm{Br}(\Delta(E_\eta))$. Note that $\mathrm{disc}(A, \eta_a) = \mathrm{disc}(A, \eta)$, and that (A^v, η_a) and (A^v, η) are isomorphic for all real places v of K. By [LT 99], Theorems A and B this implies that $(A, \eta_a) \simeq (A, \eta)$. Since $(A, \eta_a) \simeq (A, \gamma)$, we obtain $(A, \eta) \simeq (A, \gamma)$.

§B3. Application

The results of §B1 and §B2 have the following application (see [PR 10], Introduction, page 586, last line before the statement of Theorem B) :

Theorem B.3. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with orthogonal involutions with $\deg(A_1) = \deg(A_2) = 4m$. Assume that the A_i's have the same isomorphism classes of maximal subfields invariant under the involutions satisfying the dimension condition. Then we have $(A, \tau_1) \simeq (A, \tau_2)$.*

Proof. By Theorem B.1.' we have $(A_1^v, \tau_1) \simeq (A_2^v, \tau_2)$ for all $v \in \Omega_K$. Let $\mathcal{J} = \mathcal{J}(A, \tau_1)$ be the set of orthogonal involutions $\eta : A \to A$ such that $(A^v, \eta) \simeq (A_2^v, \tau_1)$ for all $v \in \Omega_K$. Then we have $\tau_2 \in \mathcal{J}$. By Theorem B.2. (i) there exists a τ_1–invariant maximal subfield E_{τ_1} of A satisfying the dimension condition and such that $(E_{\tau_1}^v, \tau_1)$ is split over K_v for all $v \in \Omega'$ (where Ω' is the

set of places $v \in \Omega_K$ such that A^v is not split and $Z(A^v, \tau_1) = K_v \times K_v$. Since (A, τ_1) and (A, τ_2) have the same isomorphism classes of maximal subfields invariant by the involutions and satisfying the dimension condition, (E_{τ_1}, τ_1) embeds into (A, τ_2). Therefore by Theorem B.2. (ii) we have $(A, \tau_1) \simeq (A, \tau_2)$.

Bibliography

[B 12] E. Bayer–Fluckiger, Embeddings of maximal tori in orthogonal groups, *Ann. Inst. Fourier* (to appear).

[B 13] E. Bayer–Fluckiger, Isometries of quadratic spaces, *J. Eur. Math. Soc.* (to appear).

[Bo 91] A. Borel, *Linear algebraic groups*, Second enlarged edition, Graduate texts in mathematics **126**, Springer-Verlag, New York, 1991.

[Bo 99] M. Borovoi, A cohomological obstruction to the Hasse principle for homogeneous spaces, *Math. Ann.* **314** (1999), 491-504.

[BCM 03] R. Brusamarello, P. Chuard–Koulmann and J. Morales, Orthogonal groups containing a given maximal torus, *J. Algebra* **266** (2003), 87–101.

[SGA3] M. Demazure and A. Grothendieck, *Schémas en Groupes (SGA 3)* tome III, Documents Mathématiques **8**, SMF, 2011 (second edition, revised and completed by Ph. Gille and P. Polo).

[F 12] A. Fiori, Special points on orthogonal symmetric spaces, *J. Algebra*, **372** (2012), 397-419.

[G 12] S. Garibaldi, Outer automorphisms of algebraic groups and determining groups by their maximal tori, *Michigan Math. J.* **61** (2012), 227–237.

[GR 12] S. Garibaldi and A. Rapinchuk, Weakly commensurable S–arithmetic subgroups in almost simple algebraic groups of types B and C, *Algebra Number Theory* **7** (2013), 1147-1178.

[K 69] M. Kneser, *Lectures on Galois cohomology of classical groups*, Tata Institute of Fundamental Research Lectures on Mathematics **47**, TIFR Bombay (1969).

[KMRT 98] M. Knus, A. Merkurjev, M. Rost and J–P. Tignol, *The Book of Involutions*, AMS Colloquium Publications **44**, 1998.

[Lee 14] T-Y. Lee, Embedding functors and their arithmetic properties, *Comment. Math. Helv.*, **89** (2014), 671–717.

[LT 99] D. W. Lewis, J-P. Tignol, Classification theorems for central simple algebras with involution. With an appendix by R. Parimala. *Manuscripta Math.* **100** (1999), 259-276.

[MT 95] A. Merkurjev, J-P. Tignol, Multiples of similitudes and the Brauer group of homogeneous varieties, *J. reine angew. Math.* **461** (1995), 13-47.

[NSW 08] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Grundlehren der mathematischen Wissenschaften **323**, Springer, 2008

[PR 10] G. Prasad and A.S. Rapinchuk, Local–global principles for embedding of fields with involution into simple algebras with involution, *Comment. Math. Helv.* **85** (2010), 583–645.

[PT 04], R. Preeti and J-P. Tignol, Multipliers of improper similitudes, *Doc. Math* **9** (2004), 183-204

[Sch 85] W. Scharlau, *Quadratic and hermitian forms*, Grundlehren der Mathematischen Wissenschaften **270**, Springer-Verlag, Berlin, 1985.

[SGA 3] M. Demazure, A. Grothendieck, *Schémas en groupes*, Documents Mathématiques **7, 8**, SMF, 2011.

[T 61] T. Tsukamoto, On the local theory of quaternionic anti-hermitian forms, *J. Math. Soc. Japan* **13** (1961), 387400.

Eva Bayer–Fluckiger and Ting-Yu Lee
EPFL-FSB-MATHGEOM-CSAG
Station 8
1015 Lausanne, Switzerland

eva.bayer@epfl.ch
ting-yu.lee@epfl.ch

Raman Parimala
Department of Mathematics & Computer Science
Emory University
Atlanta, GA 30322, USA.

parimala@mathcs.emory.edu