J. Eur. Math. Soc. 20, 137–163

DOI 10.4171/JEMS/762

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

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

Received February 2, 2015

Abstract. We give necessary and sufficient conditions for the Hasse principle to hold for the embeddings of maximal tori into classical groups over global fields of characteristic not 2.

Keywords. Maximal tori, classical groups, oriented embeddings, local-global principles, Brauer–Manin obstruction

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 [PR10], [F12], [Lee14], [B14], [B15]), with special attention to the Hasse principle. The present paper gives necessary and sufficient conditions for the Hasse principle to hold.

The results can be summarized as follows. As in [PR10], 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 (§1). In §3, we define a group $Ш(E, \sigma)$ depending only on (E, σ). 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 $f : Ш(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}$ such that (E, σ) can be embedded in (A, τ) globally if and only if $f = 0$ (Theorem 4.6.1).

To illustrate our results, let us first recall one of the main theorems of [PR10], which is concerned with the Hasse principle in the case where E is a field. Assuming that E is a field and also a hypothesis on (A, τ) (some orthogonal involutions are excluded), the Hasse principle holds (see [PR10, Theorem A, p. 584] for details). In the present paper we introduce the notion of *oriented embedding* (§2), and obtain the following improvement of [PR10, Theorem A]:

E. Bayer-Fluckiger, T.-Y. Lee: EPFL-FSB-MATHGEOM-CSAG,
Station 8, 1015 Lausanne, Switzerland; e-mail: eva.bayer@epfl.ch, ting-yu.lee@epfl.ch

R. Parimala: Department of Mathematics & Computer Science, Emory University,
Atlanta, GA 30322, USA; e-mail: parimala@mathcs.emory.edu

Mathematics Subject Classification (2010): 11E57, 11E88, 20G30

Theorem A′. *Assume that E is a field, and that there exists an oriented embedding of (E, σ) into (A, τ) everywhere locally. Then there exists a global embedding of (E, σ) into (A, τ).*

In [PR10], it is shown that the Hasse principle does not hold in general (except in the symplectic case), and the paper [Lee14] establishes that the Brauer–Manin obstruction is the only one, building upon some results of Borovoi [Bo99]). On the other hand, [B14] gives a combinatorial criterion for the Hasse principle to hold in the case where A is a matrix algebra and the involution is of orthogonal type. Inspired by these points of view, in Sections 3 and 4 we construct an obstruction to the Hasse principle which in particular explains all these earlier results.

We define a group $Ш(E, \sigma)$ that encodes some of the ramification properties of the components of the étale algebra E with involution. A closely related group $Ш(E', \sigma)$ (see §5) is isomorphic to a Tate–Shafarevich group associated to the embedding functor defined in [Lee14]; see also [BLP15].

In §4, we describe some data associated to oriented local embeddings of (E, σ) into (A, τ), called *local embedding data*. Set $F = \{e \in E \mid \sigma(e) = e\}$. Denote by Ω_K the set of places of K, and let K_v be the completion of K at $v \in \Omega_K$. Then a local embedding datum consists of some elements of $(F \otimes K_v)^\times$ obtained from the embedding of (E, σ) into (A, τ) at v.

Using a local embedding datum, we define a group homomorphism $f : Ш(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}$, and we show that f does not depend of the choice of the local embedding datum. The main result of the paper is the following (see Theorem 4.6.1):

Theorem. *Assume that for all $v \in \Omega_K$ there exists an oriented embedding of (E, σ) into (A, τ) over K_v. Then (E, σ) can be embedded into (A, τ) if and only if $f = 0$.*

The paper is organized as follows. The first section recalls some preliminary results, most of which can be found in [PR10]. The second section concerns the notions of orientation and oriented embeddings. In that section, (A, τ) is supposed to be orthogonal, and A of even degree. We recall several notions and results concerning algebras with involution, in particular the discriminant algebra $\Delta(E)$ and the center $Z(A, \tau)$ of the Clifford algebra. An *orientation* is the choice of an isomorphism $\Delta(E) \to Z(A, \tau)$. In §2.5 we define the notion of *compatible orientations*, and we recall a result of Brusamarello, Chuard and Morales [BCM03] concerning Clifford algebras of orthogonal involutions that is used in §4. We then define *oriented embeddings* and their parameters (§2.6). Finally, in §2.7 and §2.8 we show that in some cases it is possible to change the orientation keeping the same parameters.

Sections 3 and 4 are the technical heart of the paper. In §3 we define the obstruction group $Ш(E, \sigma)$, and prove some of its properties that are then used in §4. In §4, we introduce the notion of *local embedding data*. Assuming the existence of an oriented local embedding of (E, σ) into (A, τ) for all $v \in \Omega_K$, we obtain elements $a^v \in (F \times K_v)^\times$ for all $v \in \Omega_K$. These are not unique, and most of §3 and §4 is aimed at understanding how far one can modify them. The Brauer–Manin homomorphism is defined in §4.4, and the Hasse principle theorem (Theorem 4.6.1) is proved in §4.6.

Section 5 contains some examples and applications. In particular, we show that the Hasse principle results of Prasad and Rapinchuk [PR10] (in particular, Theorem A) can be explained by the vanishing of the Tate–Shafarevich group. Moreover, the results of [Lee14] and [B14] are consequences of Theorem 4.6.1. We also show that the Tate–Shafarevich group vanishes if E is a CM étale algebra with involution, hence the Hasse principle holds (for oriented embeddings) in this case (Corollary 5.2.5); we also show by an example that the non-oriented Hasse principle does not always hold (§5.3). This answers a question of Jean-Pierre Serre. Note that [BLP16] gives necessary and sufficient conditions for an embedding to exist everywhere locally, and [BLP15] clarifies the relationship with the Brauer–Manin obstruction.

§1. Definitions, notation and basic facts

1.1. Embeddings of algebras with involution

Let L be a field with $\mathrm{char}(L) \neq 2$, 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 the latter 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 $F = \{e \in E \mid \sigma(e) = e\}$. Assume that $\dim_L(E) = n$, and that if $L = K$, then $\dim_K(F) = [(n+1)/2]$. Note that if $L \neq K$, then $\dim_K(F) = n$ [PR10, Proposition 2.1].

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 [PR10, 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''.

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 [PR10, 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 $\alpha \in A^\times$ such that for $\theta = \tau \circ \mathrm{Int}(\alpha)$ we have*

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

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

Proof. See [K69, §2.5] or [PR10, 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 [PR10], 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.

1.2. Invariants of central simple algebras with involution

If (A, τ) is of orthogonal type and n is even, we denote by $C(A, \tau)$ its *Clifford algebra* [KMRT98, Chap. II, (8.7)], and by $Z(A, \tau)$ the center of $C(A, \tau)$. 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* [KMRT98, Chap. II, (10.28)].

§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 algebra with an orthogonal involution, and that the degree of A is even. Set $\deg(A) = 2r$.

The existence of an embedding $(E, \sigma) \to (A, \tau)$ of algebras with involution implies that 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.

2.1. Discriminant algebra

We have $E \simeq F[X]/(X^2 - d)$ for some $d \in F^\times$. 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 $(E, \sigma) \simeq (F[X]/(X^2 - d), \sigma')$ of algebras with involution. Let x be the image of X in E, and note that $\sigma(x) = -x$. Let $\Delta(E)$ be the discriminant algebra of E [KMRT98, Chap. 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 [KMRT98, 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 $\langle 2, 2d\rangle$. Further, we have $d = -\mathrm{N}_{E/F}(x)$ and hence $\mathrm{N}_{F/K}(d) = (-1)^r \mathrm{N}_{E/K}(x)$. Therefore $\det(T_{E/K}) = (-1)^r \mathrm{N}_{E/K}(x) \in K^\times/K^{\times 2}$, and this concludes the proof of the lemma. □

Let y be the image of Y in $\Delta(E)$. The elements x and y will be fixed in what follows. Let $\rho : \Delta(E) \to \Delta(E)$ be the automorphism of $\Delta(E)$ induced by σ. Note that $\rho(y) = (-1)^r$, and 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, denote by $\mathrm{Skew}(A, \theta)$ the set $\{a \in A \mid \theta(a) = -a\}$ of skew elements of A with respect to θ. Recall that $C(A, \theta)$ is the Clifford algebra of (A, θ), and $Z(A, \theta)$ is the center of $C(A, \theta)$. Recall that $Z(A, \theta)$ is a quadratic étale algebra over K. Denote by γ the non-trivial automorphism of $Z(A, \theta)$ over K.

The *generalized Pfaffian* [KMRT98, Chap. 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 $\pi_\theta(xa\theta(x)) = \mathrm{Nrd}_A(x)\pi_\theta(a)$ [KMRT98, 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*.

Assume that the étale algebra E can be embedded in the central simple algebra A, and fix such 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.

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

$$u : \Delta(E) \to Z(A, \theta), \qquad y \mapsto \pi_\theta(\epsilon(x)).$$

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

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

2.4. Similitudes

Let $\alpha \in A^\times$. Following [KMRT98, Definition (12.14), p. 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 α. We say that α is *proper* if

$$\mathrm{Nrd}(\alpha) = (\alpha\tau(\alpha))^r;$$

otherwise, α is *improper*. 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 one).

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

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

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

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 [KMRT98, Proposition (13.2), p. 173]. □

2.5. Compatible orientations

Recall that $\epsilon : E \to A$ is an embedding of algebras, $\theta : A \to A$ is an orthogonal involution such that $\epsilon : (E,\sigma) \to (A,\theta)$ is an embedding of algebras with involution, and we have fixed 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 an 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 $\alpha = \iota(x)$ 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 $(\iota x)\tau(\iota x) = \lambda$. 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 (a), we have $\alpha\tau\alpha = \iota(x\sigma(x)) = \iota(\lambda) = \lambda$. This implies that α is a similitude. Moreover, $\mathrm{Nrd}(\alpha) = \mathrm{N}_{E/K}(x) = \mathrm{N}_{F/K}(\lambda) = \lambda^r$. Hence α is proper, and by Lemma 2.4.1 this implies that $c(\alpha)$ is the identity. □

Let K_s be a separable closure of K, and set $A_s = A \otimes_K K_s$.

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 $\mathrm{Int}(\alpha) : (A_s, \theta) \to (A_s, \theta')$ of algebras with involution 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 $\epsilon : (E, \sigma) \to (A, \theta_a)$ of algebras with involution. Our next aim is to define an orientation of (A, θ_a) compatible with the orientation u of (A, θ).

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 $\alpha \in A_s^\times$ giving an isomorphism* $\mathrm{Int}(\alpha) : (A_s, \theta) \to (A_s, \theta_a)$ *of algebras with involution 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 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 $a \in F^\times$. 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 $C(A_s, \theta) \to C(A_s, \theta_a)$ of the Clifford algebras.

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 $(e_1, \dots, e_{2r})$ be an orthogonal basis for q. Since $Z(A, \theta) = K \oplus K(e_1 \dots e_{2r})$, we have $z = \mu(e_1 \dots e_{2r})$ for some $\mu \in K_s^\times$. We replace e_1 by $\mu^{-1}e_1$. Then $z = e_1 \dots e_{2r}$.

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. Consider the isometry $\epsilon(b) : (V, q) \to (V, q_a)$. It induces a map $c(\epsilon(b)) : C(V, q) \to C(V, q_a)$ which sends $e_1 \dots e_{2r}$ to $(\epsilon(b)e_1) \dots (\epsilon(b)e_{2r})$. Therefore $(\epsilon(b)e_1) \dots (\epsilon(b)e_{2r})^2 = q_a(\epsilon(b)e_1) \dots q_a(\epsilon(b)e_{2r}) = q(e_1) \dots q(e_{2r}) = (e_1 \dots e_{2r})^2 = d$. This implies that $\epsilon(b)(e_1) \dots \epsilon(b)(e_{2r}) = \pm z_a$ 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 $b' \in A_s$ be such that $b'\sigma(b') = a$. Then $c(\mathrm{Int}(\epsilon(b'))) = c(\mathrm{Int}(\epsilon(b)))$. We have an isomorphism $\mathrm{Int}(\epsilon(b^{-1}b')) : (A, \theta) \to (A, \theta)$ of algebras with involution 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 $c(\epsilon(b)) = c(\epsilon(b'))$, so $c(\epsilon(b))$ 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 $c(\mathrm{Int}(\epsilon(x))) = c(\epsilon(b)) = \phi_a$. 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 $a \in F^\times$, 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 the structure of a $\Delta(E)$-algebra.

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

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

Proof. This follows from [BCM03, Proposition 5.3]. □

2.6. Oriented embeddings

Recall that the existence of an embedding $(E,\sigma) \to (A,\tau)$ of algebras with involution is equivalent to 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:

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 said to be *oriented* 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.

Proposition 2.7.1. *Suppose that (A,τ) admits an improper similitude. Assume that there exists an embedding $(E,\sigma) \to (A,\tau)$ of algebras with involution. 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 $c(\gamma\alpha) \circ u_a = \nu$. Set $\beta = \gamma\alpha$. Then $(\mathrm{Int}(\beta) \circ \epsilon, a, \beta)$ are parameters of an oriented embedding, as claimed. □

Lemma 2.7.2. *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 $A \simeq M_r(H)$, 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 [T61, Theorem 3] if K is a local field, and [Sch85, 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 $B = M_{r'}(H)$. 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 the multiplier of a similitude of (B, τ'). Indeed, since $r' \leq 3$, we may apply the criterion of [PT04, Theorem 4]. Let $\gamma(B, \tau') \in \mathrm{Br}(K)$ be such that $\gamma_Z = C(B', \tau')$ in $\mathrm{Br}(Z)$ [PT04, Theorem 2]. Then by [PT04, 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 $\lambda.\gamma = 0$ in $H^3(K)/(K^{\times}.A)$ in both cases.

Hence by [PT04, 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, so it has a similitude of multiplier λ. Thus h also has a similitude, and hence so does (A, τ). By [PT04, 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 $(E, \sigma) \to (A, \tau)$ of algebras with involution, 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), 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 the unitary group $U(A, \tau)$ 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 $E \simeq F[X]/(X^2 - d)$, $\Delta(E) \simeq K[Y]/(Y^2 - (-1)^r \mathrm{N}_{E/K}(x))$, and 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 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 satisfying $\mathrm{Int}(\gamma) \circ \epsilon \circ \sigma = \epsilon$. Then $c(\gamma) \circ u \circ \rho = u$.*

Proof. It suffices to prove that this is true over a separable closure. Therefore we may assume that $A = M_{2r}(K)$ and $\theta : A \to A$ 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, $\pi_t(\lambda^{-1}\gamma(\epsilon(\sigma(x))\gamma^t)) = \lambda^{-r}\mathrm{Nrd}(\gamma)\pi_t(\epsilon(\sigma(x)) = \eta\pi_t(-\epsilon(x)) = (-1)^r\eta\pi_t(\epsilon(x))$. Hence $(-1)^r\eta\pi_t(\epsilon(x)) = \pi_t(\epsilon(x))$, 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 $c(\gamma)\circ u\circ\rho(y) = u(y)$, 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 $c(\alpha)\circ u_a\circ\rho = c(\beta)\circ u_b$.*

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 $u_a = c(\gamma_a)\circ u$ 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 $c(\alpha)\circ u_a\circ\rho = c(\beta)\circ u_b$. □

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

Corollary 2.8.3. *Suppose that r is odd and there exists an embedding $(E,\sigma) \to (A,\tau)$ of algebras with involution. 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, $c(\alpha)\circ u_a\circ\rho = \nu$. 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, $c(\beta)\circ u_b = c(\alpha)\circ u_a\circ\rho = \nu$, and hence (ι', b, β, ν) are parameters of an oriented embedding. □

§3. 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 Ω_K be 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. Write $E = E_1 \times \cdots \times E_m$, with $\sigma(E_i) = E_i$ for all $i = 1,\ldots,m$, and with each E_i either a field stable by σ or a product of two fields exchanged by σ. Recall that $F = E^\sigma$.

Set $I = \{1, \dots, m\}$. 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 $d_i \in F_i^\times$ be such that $E_i = F_i(\sqrt{d_i})$ if E_i/F_i is a quadratic extension, and $d_i = 1$ otherwise. Set $d = (d_1, \dots, d_m)$.

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 $E_i = K$, set $\Sigma_i = \Omega_K$.

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

$$I_0 = I_0(x) = \{i \mid x_i = 0\}, \qquad I_1 = I_1(x) = \{i \mid x_i = 1\}.$$

Note that (I_0, I_1) is a partition of I. Let

$$\begin{aligned} S' &= \Big\{(x_1, \dots, x_m) \in (\mathbb{Z}/2\mathbb{Z})^m \;\Big|\; \Big(\bigcap_{i \in I_0} \Sigma_i\Big) \cup \Big(\bigcap_{j \in I_1} \Sigma_j\Big) = \Omega_K\Big\}, \\ S &= S' \cup \{(0, \dots, 0), (1, \dots, 1)\}. \end{aligned}$$

We define an equivalence relation on S by

$$(x_1, \dots, x_m) \sim (x_1', \dots, x_m') \quad \text{if} \quad (x_1, \dots, x_m) + (x_1', \dots, x_m') = (1, \dots, 1).$$

Let $\text{Ш} = \text{Ш}(E, \sigma)$ be the set of equivalence classes of this 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 P' be the set of non-trivial partitions (I_0, I_1) of I such that $(\bigcap_{i \in I_0} \Sigma_i) \cup (\bigcap_{j \in I_1} \Sigma_j) = \Omega_K$, and set $P = P' \cup \{(I, \emptyset), (\emptyset, I)\}$. 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 relation.

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

Lemma 3.1.1. *The set* Ш *is a subgroup of* C_m.

Proof. It is clear that the class of $(0, \dots, 0)$ 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. For $J \subset I$, set $\Omega(J) = \bigcap_{i \in J} \Sigma_i$. As we have seen above, Ш is in bijection with $P/{\sim}$. Moreover, the transport of structure induces

$$(I_0, I_1) + (I_0', I_1') = \big((I_0 \cap I_0') \cup (I_1 \cap I_1'), (I_0 \cap I_1') \cup (I_1 \cap I_0')\big).$$

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

$$[(\Omega(I_0 \cap I_0')) \cap (\Omega(I_1 \cap I_1'))] \cup [(\Omega(I_0 \cap I_1')) \cap (\Omega(I_0' \cap I_1))],$$

and this follows from the equalities $\Omega(I_0) \cup \Omega(I_1) = \Omega_K$ and $\Omega(I_0') \cup \Omega(I_1') = \Omega_K$, which hold as (I_0, I_1) and (I_0', I_1') are in $P/{\sim}$. □

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

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

Lemma 3.1.2. *Let $(i, j) \in \mathcal{C}_I$, and let $v \in \Omega_K$ be such that $v \notin \Sigma_i \cup \Sigma_j$. 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*
- *$\mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) \neq \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$ and $\mathrm{cor}_{F_i^v/K_v}(b_j^v, d_j) \neq \mathrm{cor}_{F_i^v/K_v}(a_j^v, d_j)$.*

In particular,

$$\sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i),$$
$$\sum_{v \in \Omega_K} \mathrm{cor}_{F_j^v/K_v}(a_j^v, d_j) \neq \sum_{v \in \Omega_K} \mathrm{cor}_{F_j^v/K_v}(b_j^v, d_j).$$

Proof. Since $(i, j) \in \mathcal{C}_I$, we have $\Sigma_i \cup \Sigma_j \neq \Omega_K$. Hence by Chebotarev's density theorem, the complement of the set $\Sigma_i \cup \Sigma_j$ contains finite places. Let us choose a finite place v of K such that $v \notin \Sigma_i \cup \Sigma_j$. 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, $E_j^v = E_j' \times N$, 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 $\gamma \in M_0$ be such that $\gamma \notin \mathrm{N}_{M/M_0}(M)$, and let $\delta \in N_0$ be such that $\delta \notin \mathrm{N}_{N/N_0}(N)$. 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 $r \in I$. □

Proposition 3.1.3. *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) $$\sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i),$$

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

(iii) $$\sum_{v \in \Omega_K} \mathrm{cor}_{F_r^v/K_v}(a_r^v, d_r) = \sum_{v \in \Omega_K} \mathrm{cor}_{F_r^v/K_v}(b_r^v, d_r) \quad \text{if } r \neq i, j,$$

(iv) $$\sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \quad \text{for all } v \in \Omega_K,$$

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

Proof. Let $j_1, \dots, j_k \in J$ with $j_1 = i$, $j_k = j$ and $(j_s, j_{s+1}) \in \mathcal{C}_I$ for all $s = 1, \dots, k-1$. Starting with $a_r^u \in (F_r^u)^\times$, we apply Lemma 3.1.2 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 have applied Lemma 3.1.2 twice. Hence

$$\sum_{v \in \Omega_K} \mathrm{cor}_{F^v_{j_s}/K_v}(b^v_{j_s}, d_{j_s}) = \sum_{v \in \Omega_K} \mathrm{cor}_{F^v_{j_s}/K_v}(a^v_{j_s}, d_{j_s}) \quad \text{for } s \neq 1, k.$$

On the other hand, if $s = 1$ or $s = k$, then we have applied Lemma 3.1.2 only once. Note also that $j_1 = i$ and $j_k = j$. Therefore

$$\mathrm{cor}_{F^v_i/K_v}(b^v_i, d_i) \neq \mathrm{cor}_{F^v_i/K_v}(a^v_i, d_i) \quad \text{for a certain } v \in \Omega_K,$$
$$\mathrm{cor}_{F^v_i/K_v}(b^u_i, d_i) = \mathrm{cor}_{F^v_i/K_v}(a^u_i, d_i) \quad \text{for all } u \in \Omega_K \text{ with } u \neq v.$$

Similarly,

$$\mathrm{cor}_{F^w_j/K_w}(b^w_j, d_j) \neq \mathrm{cor}_{F^w_j/K_w}(a^w_j, d_j) \quad \text{for a certain } w \in \Omega_K,$$
$$\mathrm{cor}_{F^u_j/K_u}(b^u_j, d_j) = \mathrm{cor}_{F^u_j/K_u}(a^u_j, d_j) \quad \text{for all } u \in \Omega_K \text{ with } u \neq w.$$

Therefore

$$\sum_{v \in \Omega_K} \mathrm{cor}_{F^v_i/K_v}(a^v_i, d_i) \neq \sum_{v \in \Omega_K} \mathrm{cor}_{F^v_i/K_v}(b^v_i, d_i),$$
$$\sum_{v \in \Omega_K} \mathrm{cor}_{F^v_j/K_v}(a^v_j, d_j) \neq \sum_{v \in \Omega_K} \mathrm{cor}_{F^v_j/K_v}(b^v_j, d_j).$$

Note that for $r \neq i, j$ we have

$$\sum_{v \in \Omega_K} \mathrm{cor}_{F^v_r/K_v}(a^v_r, d_r) = \sum_{v \in \Omega_K} \mathrm{cor}_{F^v_r/K_v}(b^v_r, d_r).$$

Moreover, all the applications of Lemma 3.1.2 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

$$\sum_{i \in I} \mathrm{cor}_{F^v_i/K_v}(b^v_i, d_i) = \sum_{i \in I} \mathrm{cor}_{F^v_i/K_v}(a^v_i, d_i).$$

All the changes were made at finite places, hence $b^v_r = a^v_r$ for all $r \in I$ if v is an infinite place. This completes the proof of the proposition. □

Proposition 3.1.4. *Let $a^v_i \in (F^v_i)^\times$, for all $v \in \Omega_K$ and $i \in I$, be such that:*

(i) $$\sum_{v \in \Omega_K} \sum_{i \in I} \mathrm{cor}_{F^v_i/K_v}(a^v_i, d_i) = 0,$$

(ii) $$\sum_{v \in \Omega_K} \sum_{i \in I_0(x)} \mathrm{cor}_{F^v_i/K_v}(a^v_i, d_i) = 0 \quad \textit{for all } x \in \text{Ш}.$$

Then there exist $b^v_i \in F^v_i$ for all $v \in \Omega_K$ and $i \in I$ such that:

(iii) $$\sum_{v \in \Omega_K} \mathrm{cor}_{F^v_i/K_v}(b^v_i, d_i) = 0 \quad \textit{for all } i \in I,$$

(iv) $$\sum_{i \in I} \mathrm{cor}_{F^v_i/K_v}(b^v_i, d_i) = \sum_{i \in I} \mathrm{cor}_{F^v_i/K_v}(a^v_i, d_i) \quad \textit{for all } v \in \Omega_K,$$

(v) *if v is an infinite place of K, then $b^v_i = a^v_i$.*

Proof. For all $i \in I$, set $C_i = C_i(a) = \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$. 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 elements $i_0, i_k \in I$ such that $C_{i_0} = C_{i_k} = 1$ and i_0 and i_k are connected within the graph.

We start with the empty graph, and add edges and vertices as follows. 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 $\sum_{v \in \Omega_K} \sum_{i \in I_0} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0$. But on the other hand this sum equals $C_{i_0} = 1$, a contradiction. Therefore, by definition of Ш, we have

$$\Big(\bigcap_{i \in I_0} \Sigma_i\Big) \cup \Big(\bigcap_{j \in I_1} \Sigma_j\Big) \neq \Omega_K. \tag{$*$}$$

Hence there exist $i_1 \in I_1$ and $v \in \Omega_K$ such that $v \notin \Sigma_{i_0} \cup \Sigma_{i_1}$. 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 $\sum_{v \in \Omega_K} \sum_{i \in I_0} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0$. But this sum equals $C_{i_0} + C_{i_1}$, and $C_{i_0} = 1$, $C_{i_1} = 0$, so this is again a contradiction. Therefore, by definition of Ш, $(*)$ holds again. Hence there exist $i_2 \in I_1$ and $v \in \Omega_K$ such that $v \notin (\bigcap_{i \in I_0} \Sigma_i) \cup \Sigma_{i_2}$. This implies that at least one of (i_0, i_2), (i_1, i_2) belongs 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 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 3.1.3 this implies that there exist $c_i^v \in F_i^v$ for all $v \in \Omega_K$ and $i \in I$ 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 $\sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(c_i^v, d_i) = \sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$, and 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 $v \in \Omega_K$ and $i \in I$ such that for $(b) = (b_i^v)$ we have $C_i(b) = \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0$ for all $i \in I$, and this implies (iii). Note that for all $v \in \Omega_K$, we have $\sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i) = \sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$. This implies that (iv) holds. Moreover, all the modifications were made at finite places, hence (v) holds. □

Proposition 3.1.5. *Let $a_i^v \in (F_i^v)^\times$, for all $v \in \Omega_K$ and $i \in I$, be such that:*

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

(ii) $$\sum_{v \in \Omega_K} \sum_{i \in I_0(x)} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = 0 \quad \textit{for all } x \in Ш.$$

Then for all $i \in I$ there exist $b_i \in F_i^\times$ such that $(b_i, d_i)^v = (a_i^v, d_i)$ for all real places v and

$$\text{(iii)} \qquad \sum_{i \in I} \operatorname{cor}_{F_i^v/K_v}(b_i, d_i) = \sum_{i \in I} \operatorname{cor}_{F_i^v/K_v}(a_i^v, d_i) \quad \text{for all } v \in \Omega_K.$$

Proof. By Proposition 3.1.4 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 $\sum_{v \in \Omega_K} \operatorname{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0$ for all $i \in I$, $b_i^v = a_i^v$ if v is an infinite place of K, and,

$$\sum_{i \in I} \operatorname{cor}_{F_i^v/K_v}(b_i^v, d_i) = \sum_{i \in I} \operatorname{cor}_{F_i^v/K_v}(a_i^v, d_i) \quad \text{for all } v \in \Omega_K.$$

Let $i \in I$. Since $\sum_{v \in \Omega_K} \operatorname{cor}_{F_i^v/K_v}(b_i^v, d_i) = 0$, we have $\sum_{w \in \Omega_{F_i}} (b_i^w, d_i) = 0$. The Brauer–Hasse–Noether theorem implies that there exists a quaternion algebra Q_i over F_i such that $Q_i^v \simeq (b_i^v, d_i)$ for all $v \in \Omega_K$. 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 $v \in \Omega_K$,

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

Therefore (iii) holds. □

§4. The Brauer–Manin map

Assume that K is a global field and (E^v, σ) can be embedded in (A^v, τ) for all $v \in \Omega_K$. This implies that there exists an embedding $\epsilon : E \to A$ of algebras. 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 $(E, \sigma) \to (A, \theta)$ of algebras with involution. We fix such an involution θ.

The aim of this section is to define a map $Ш(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}$ whose vanishing is necessary and sufficient for the existence of an embedding $(E, \sigma) \to (A, \tau)$ of algebras with involution. To define this map, we need the notion of *embedding data* (§§4.1–4.3). The Brauer–Manin map is defined in §4.4.

4.1. 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 $n = 2r$. Fix an isomorphism $u : \Delta(E) \to Z(A, \theta)$ of K-algebras, and recall (§2.5) that for all $a^v \in (F^v)^\times$ this induces a uniquely defined isomorphism $u_{a^v} : \Delta(E^v) \to Z(A, \theta_{a^v})$ of K_v-algebras.

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

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

Let $\mathcal{O}(E, A)$ be 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 4.1.1. *Let* $(a) = (a^v) \in \mathcal{O}(E, A)$. *Then:*

(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*

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

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

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

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

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

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). $\square$

Proposition 4.1.2. *Let* $(a^v), (b^v) \in \mathcal{O}(E, A)$. *Then, for all* $v \in \Omega_K$*:*

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

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

- Let Ω'' be the set of places $v \in \Omega_K$ such that $\Delta(E_v)$ is a quadratic extension of K_v. Then $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ for almost all $v \in \Omega''$.
- $\sum_{v \in \Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$.

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

Remark. Let $(a^v) \in \mathcal{L}(E, A)$. Then $\mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ for almost all $v \in \Omega_K$. Indeed, by hypothesis this is true if $\Delta(E_v)$ is a quadratic extension of K_v, and by Proposition 4.1.1(ii) it also holds if $\Delta(E_v) \simeq K_v \times K_v$.

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

Proposition 4.1.3. *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, $\mathrm{disc}(A^v, \tau) = \mathrm{disc}(A^v, \theta_{b^v}) = \mathrm{disc}(A^v, \theta)$. 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 $\Delta(E^v) \simeq K_v \times K_v$. Let $(\iota_v, a^v, \alpha^v, \nu)$ be parameters of 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 $\sum_{v\in\Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = \sum_{v\in\Omega'} \mathrm{cor}_{F^v/K_v}(a^v, d)$, and by Proposition 4.1.1(ii) this sum is zero. It follows that $(a) \in \mathcal{L}(E, A)$. □

Proposition 4.1.4. *Let $(a) = (a^v), (b) = (b^v) \in \mathcal{L}(E, A)$. Then there exists $\lambda \in K^\times$ such that $\mathrm{cor}_{F^v/K_v}(\lambda b^v, d) = \mathrm{cor}_{F^v/K_v}(a^v, d)$ for all $v \in \Omega_K$.*

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 $\mathrm{cor}_{F^v/K_v}(b^v, d) = \mathrm{cor}_{F^v/K_v}(a^v, d)$ (Proposition 4.1.2).

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 $\mathrm{cor}_{F^v/K_v}(b^v, d) - \mathrm{cor}_{F^v/K_v}(a^v, d) = (\lambda^v, D)$ for some $\lambda^v \in K_v^\times$. Since $(a), (b) \in \mathcal{L}(E, A)$, by definition we have $\sum_{v\in\Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = \sum_{v\in\Omega_K} \mathrm{cor}_{F^v/K_v}(b^v, d) = 0$. This implies that $\sum_{v\in\Omega_K}(\lambda^v, D) = 0$. 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. □

4.2. 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 of n even.

For all $a \in F^\times$, let $T_a : E \times E \to K$ be the quadratic form given by $T_a(x, y) = \mathrm{Tr}_{E/K}(ax\sigma(y))$. The Hasse invariant of a quadratic form Q will be denoted by $w(Q)$.

Assume that there exists an embedding $(E^v, \sigma) \to (A^v, \tau)$ of algebras with involution for all $v \in \Omega_K$. By [PR10, Proposition 7.1] this implies that for all $v \in \Omega_K$ there exists $a^v \in (F^v)^\times$ such that $q \simeq T_{a^v}$. Write $a^v = (a_1^v, \dots, a_m^v)$ with $a_i^v \in (F_i^v)^\times$. The set of $(a) = (a_i^v)$ with this property will be denoted by $\mathcal{L}'(E, A)$.

Proposition 4.2.1. *Let* $(a) \in \mathcal{L}'(E, A)$ *with* $(a) = (a_i^v)$. *Then:*

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

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

(ii) *Let* $(b) \in \mathcal{L}'(E, A)$ *with* $(b) = (b_i^v)$. *Then*

$$\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d) \quad \textit{for all } v \in \Omega_K.$$

Proof. 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 [BCM03, Theorem 4.3] we have $w(T_{a^v}) = w(T) + \mathrm{cor}_{F^v/K_v}(a^v, d)$. Hence $w(q) = w(T_{a^v}) = w(T) + \mathrm{cor}_{F^v/K_v}(a^v, d)$ for all $v \in \Omega_K$. Note that $\sum_{v \in \Omega_K} w(q) = \sum_{v \in \Omega_K} w(T) = 0$. Therefore $\sum_{v \in \Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$, and this proves (i).

For (ii), since $(b) \in \mathcal{L}'(E, A)$, for all $v \in \Omega_K$ we have $w(T_{b^v}) = w(q)$. By [BCM03, Theorem 4.3] we have $w(T_{b^v}) = w(T) + \mathrm{cor}_{F^v/K_v}(b^v, d)$ for all $v \in \Omega_K$. Therefore $w(T) + \mathrm{cor}_{F^v/K_v}(a^v, d) = w(q) = w(T) + \mathrm{cor}_{F^v/K_v}(b^v, d)$ for all $v \in \Omega_K$. Hence $\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d)$, and this implies (ii).

Suppose now that n is odd, and set $A' = M_{n-1}(K)$. Then by [PR10, Proposition 7.2] there exists a σ-invariant étale subalgebra E' of E of rank $n-1$ with $E = E' \times K$, an $(n-1)$-dimensional quadratic form q' and a 1-dimensional quadratic form q'' over K such that $q \simeq q' \oplus q''$ and 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 $\mathcal{L}'(E, A) = \mathcal{L}'(E', A') \times \mathcal{L}'(K, K)$. We may suppose that $E_m = K$. Then $d_m = 1$. Set $J = \{1, \dots, m-1\}$, and note that $\sum_{i \in I} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = \sum_{i \in J} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i)$ for all $v \in \Omega_K$. 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 a *local embedding datum*. If n is even, then $\mathcal{L}(E, A)$ was defined in the previous section. The relationship between $\mathcal{L}(E, A)$ and $\mathcal{L}'(E, A)$ is as follows:

Proposition 4.2.2. *Assume that n is even. Then:*

(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 $\sum_{v\in\Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$ (Proposition 4.2.1(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.

For (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 $q \simeq \lambda T_{a^v}$. Since $\lambda T_{a^v} = T_{\lambda a^v}$, we have $(\lambda a) \in \mathcal{L}'(E, A)$. ◻

4.3. Local embedding data—the unitary case

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

Proposition 4.3.1. *Let $(a) \in \mathcal{L}(E, A)$ be an embedding datum with $(a) = (a_i^v)$. Then:*

(i) $\sum_{v\in\Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$.
(ii) *Let $(b) \in \mathcal{L}(E, A)$ be an embedding datum with $(b) = (b_i^v)$. Then*

$$\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d) \quad \text{for all } v \in \Omega_K.$$

We need the following lemma:

Lemma 4.3.2. *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 [KMRT98, Chap. II, (10.36)], $D(A, \theta_a) = D(A, \theta) + (\mathrm{N}_{F/K}(a), L/K)$. Since $(\mathrm{N}_{F/K}(a), L/K) = \mathrm{cor}_{F/K}(a, E/F) = \mathrm{cor}_{F/K}(a, d)$, the lemma is proved. ◻

Proof of Proposition 4.3.1. 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 $D(A^v, \theta_{a^v}) = D(A^v, \tau)$ for all $v \in \Omega_K$. By Lemma 4.3.2, $D(A^v, \theta_{a^v}) = D(A^v, \theta) + \mathrm{cor}_{F^v/K^v}(a^v, d)$ for all $v \in \Omega_K$. We have $\sum_{v\in\Omega_K} D(A^v, \tau) = \sum_{v\in\Omega_K} D(A^v, \theta) = 0$, hence $\sum_{v\in\Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$. This proves (i).

For (ii), let $v \in \Omega_K$. Since $(b) \in \mathcal{L}(E, A)$, from Lemma 4.3.2 we deduce that $D(A^v, \theta) + \mathrm{cor}_{F^v/K^v}(a^v, d) = D(A^v, \theta_{a^v}) = D(A^v, \tau) = D(A^v, \theta_{b^v}) = D(A^v, \theta) + \mathrm{cor}_{F^v/K^v}(b^v, d)$. Hence $\mathrm{cor}_{F^v/K_v}(a^v, d) = \mathrm{cor}_{F^v/K_v}(b^v, d)$, as claimed. ◻

4.4. The Brauer–Manin map

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

$$f_{(a)} : \text{Ш}(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}, \qquad f_{(a)}(I_0, I_1) = \sum_{i\in I_0} \sum_{v\in\Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i).$$

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

Theorem 4.4.1. *Let $(a), (b) \in \mathcal{L}(E, A)$ be two local embedding data. Then $f_{(a)} = f_{(b)}$.*

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 $\sum_{i\in I}\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = \sum_{i\in I}\mathrm{cor}_{F_i^v/K_v}(\lambda b_i^v, d_i)$ (Propositions 4.1.4, 4.2.1(ii) and 4.3.1(ii)), we may assume that for all $v \in \Omega_K$,

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

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 $\sum_{i\in I_0}\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \neq \sum_{i\in I_0}\mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i)$. This implies that $v \notin \bigcap_{i\in I_0}\Sigma_i$. Since $\sum_{i\in I}\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) = \sum_{i\in I}\mathrm{cor}_{F_i^v/K_v}(b_i^v, d_i)$, 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 $v \notin \bigcap_{i\in I_1}\Sigma_i$, and this contradicts $\bigcup_{i\in I_0}\Sigma_i \cup \bigcap_{i\in I_1}\Sigma_i = \Omega_K$. 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

$$f : Ш(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}, \qquad f(I_0, I_1) = \sum_{i\in I_0}\sum_{v\in\Omega_K}\mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i),$$

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

Recall that we have fixed 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 4.4.2. 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 exist $\alpha \in A^\times$ and $c \in F^\times$ such that:

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

Proposition 4.4.3. *Assume that* (ϵ, θ, u) *and* $(\tilde{\epsilon}, \tilde{\theta}, \tilde{u})$ *are compatible. Define* $\tilde{\mathcal{L}}(A, E)$ *to be the set of local embedding data with respect to* $(\tilde{\epsilon}, \tilde{\theta}, \tilde{u})$*, and let* $(a) \in \tilde{\mathcal{L}}(A, E)$*. Let*

$$f'_{(a)} : Ш(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}, \qquad f'_{(a)}(I_0, I_1) = \sum_{i \in I_0} \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i).$$

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 satisfying $\mathrm{Int}(\alpha) \circ \tilde{\epsilon} = \epsilon$, and if θ is orthogonal, then $c(\alpha) \circ \tilde{u} = u_c$.

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 $(\mathrm{Int}(\beta^v) \circ \tilde{\epsilon}, a^v, \beta^v, \tilde{u})$ 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 $(\mathrm{Int}(\beta^v \alpha^{-1}) \circ \epsilon ca^v, \beta^v \alpha^{-1}, u)$ are parameters of an oriented embedding with respect to (ϵ, θ, u). Therefore $(ca) \in \mathcal{L}(E, A)$.

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

$$\begin{aligned} f'_{(a)}(I_0, I_1) &= \sum_{i \in I_0} \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) \\ &= \sum_{i \in I_0} \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(a_i^v, d_i) + \sum_{i \in I_0} \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(c_i, d_i) \\ &= \sum_{i \in I_0} \sum_{v \in \Omega_K} \mathrm{cor}_{F_i^v/K_v}(c_i a_i^v, d_i) = f(I_0, I_1), \end{aligned}$$

since $(ca) \in \mathcal{L}(E, A)$. □

Corollary 4.4.4. *Suppose that there exists an embedding* $(E, \sigma) \to (A, \tau)$ *of algebras with involution. Then* $f = 0$*.*

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 4.4.1 it suffices to show that $f_{(a)} = 0$. Let $(I_0, I_1) \in Ш(E, \sigma)$. Then

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

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

4.5. Oriented embeddings

Definition 4.5.1. We say that there exists an *oriented embedding* $(E^v, \sigma) \to (A^v, \tau)$ for all $v \in \Omega_K$ if:

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

(ii) If moreover (A, τ) is of orthogonal type with A non-split, $\deg(A) = 2r$ with r even, $\mathrm{disc}(A^v, \tau) = 1$ in $K_v^\times / K_v^{\times 2}$ for all $v \in \Omega_K$ such that A^v is non-split, then there exists an orientation $\nu : \Delta(E) \to Z(A, \tau)$ such that for all $v \in \Omega_K$ there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$ with respect to ν.

4.6. Hasse principle

The main result of the paper is the following:

Theorem 4.6.1. *Suppose that for all $v \in \Omega_K$ there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$. Then there exists an embedding $(E, \sigma) \to (A, \tau)$ if and only if $f = 0$.*

By Corollary 4.4.4 we already know that the existence of a global embedding $(E, \sigma) \to (A, \tau)$ implies that $f = 0$, hence it suffices to prove the converse.

Proof of Theorem 4.6.1 in the even degree orthogonal case. Suppose that $\deg(A) = n = 2r$. We fix an embedding $\epsilon : (E, \sigma) \to (A, \theta)$ and an isomorphism $u : \Delta(E) \to Z(A, \theta)$ of K-algebras. Since for all $v \in \Omega_K$, there exists an embedding $(E^v, \sigma) \to (A^v, \tau)$ of algebras with involution, the K-algebras $\Delta(E)$ and $Z(A, \tau)$ are isomorphic. Fix such an isomorphism $\nu : \Delta(E) \to Z(A, \tau)$. By Corollaries 2.7.3 and 2.8.3 we may assume that there exists an oriented embedding with respect to ν for all $v \in \Omega_K$. 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

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

By Proposition 3.1.5 there exists $b \in F^\times$ such that

$$\mathrm{cor}_{F^v/K_v}(b, d) = \mathrm{cor}_{F^v/K_v}(a^v, d) \quad \text{for all } v \in \Omega_K.$$

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 $C(A^v, \tau) = C(A^v, \theta_b)$ in $\mathrm{Br}(\Delta(E^v))$ for all $v \in \Omega_K$. Then by the Brauer–Hasse–Noether theorem, $C(A, \tau) = C(A, \theta_b)$ 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 [LT99, 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). □

Proof of Theorem 4.6.1 in the odd degree orthogonal case. If $n = 1$ then $E = A = K$, hence (E, σ) can be embedded into (A, τ). Assume that $n \geq 3$. Set $A' = M_{n-1}(K)$. Then by [PR10, Proposition 7.2] there exists a σ-invariant étale subalgebra E' of E of rank $n-1$ with $E = E' \times K$, an $(n-1)$-dimensional quadratic form q' and a 1-dimensional quadratic form q'' over K such that $q \simeq q' \oplus q''$, and the étale algebra (E', σ) with involution 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 $\mathcal{L}(E, A) = \mathcal{L}'(E', A') \times \mathcal{L}(K, K)$. We may suppose that $E_m = K$. Then $d_m = 1$. Set $J = \{1, \ldots, m-1\}$.

Let $f' : Ш(E', \sigma) \to \mathbb{Z}/2\mathbb{Z}$ 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 4.2.2(i) we have $\mathcal{L}'(E', A') \subset \mathcal{L}(E', A')$, hence $(b) \in \mathcal{L}(E', A')$.

For all $(J_0, J_1) \in Ш(E', \sigma)$ 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 the even degree orthogonal case proved above, this implies that (E', σ) can be embedded into (A', τ'). Therefore (E, σ) can be embedded into (A, τ). □

Proof of Theorem 4.6.1 in the unitary case. Let $(a) = (a_i^v) \in \mathcal{L}(E, A)$. Then by Proposition 4.3.1 we have $\sum_{v \in \Omega_K} \mathrm{cor}_{F^v/K_v}(a^v, d) = 0$. Let $(I_0, I_1) \in \text{Ш}$. By hypothesis we have $f_{(a)}(I_0, I_1) = 0$, therefore

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

By Proposition 3.1.5 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 $v \in \Omega_K$, and $b^v = a^v$ if v is a real place. Since $(A^v, \tau) = (A^v, \theta_{a^v})$ for all $v \in \Omega_K$, we have $D(A, \tau) = D(A, \theta_b)$. Hence $(A, \tau) \simeq (A, \theta_b)$. By Proposition 1.1.3 there exists an embedding of (E, σ) into (A, τ). □

§5. 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.

5.1. The group $\text{Ш}(E', \sigma)$

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 $i = m_1 + 1, \ldots, m$. Set $E' = E_1 \times \cdots \times E_{m_1}$. Recall that $I = \{1, \ldots, m\}$, and set $I(\text{split}) = \{m_1 + 1, \ldots, m\}$, $I' = I(\text{non-split}) = \{1, \ldots, m_1\}$. If I' is empty, then we set $\text{Ш}(E', \sigma) = 0$.

Let $\pi : \text{Ш}(E, \sigma) \to \text{Ш}(E', \sigma)$ 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 $\text{Ш}(E, \sigma)$ 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 $f : \text{Ш}(E, \sigma) \to \mathbb{Z}/2\mathbb{Z}$ be the Brauer–Manin map (§4.4). 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 $\bar{f} : \text{Ш}(E', \sigma) \to \mathbb{Z}/2\mathbb{Z}$ such that $f = \bar{f} \circ \pi$.

Proposition 5.1.1. *We have $f = 0$ if and only if $\bar{f} = 0$.*

Proof. This follows immediately from the definitions. □

5.2. Sufficient conditions

We keep the notation of the previous sections. In particular, K is a global field of characteristic $\neq 2$.

Theorem 5.2.1. *Suppose that:*

(i) *For all $v \in \Omega_K$, there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$.*
(ii) *$\text{Ш}(E', \sigma)$ is trivial.*

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

Proof. This follows from Theorem 4.6.1 and Proposition 5.1.1. □

Theorem 5.2.1 implies that the Hasse principle is always true for oriented embeddings if E' is a field—indeed, if E' is a field extension of L, then $\text{Ш}(E', \sigma)$ is obviously trivial. In particular, this implies Theorem A of Prasad and Rapinchuk [PR10, p. 584], where E is a field.

Corollary 5.2.2. *Suppose that:*

(i) *For all $v \in \Omega_K$, there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$.*
(ii) *There exists $i_0 \in I$ such that $\Sigma_{i_0} \cup \Sigma_i \neq \Omega_K$ for all $i \in I$.*

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

This generalizes the Hasse principle results of [PR10], [Lee14] and [B14]. The corollary is a consequence of Theorem 5.2.1 and the following lemma:

Lemma 5.2.3. *Assume that there exists $i_0 \in I$ such that $\Sigma_{i_0} \cup \Sigma_i \neq \Omega_K$ for all $i \in I$. Then the group $\text{Ш}(E, \sigma)$ is trivial. Therefore $\text{Ш}(E', \sigma)$ is trivial.*

Proof. Suppose that $\text{Ш}(E, \sigma)$ is not trivial, and let (I_0, I_1) be a partition of I representing a non-trivial element of $\text{Ш}(E, \sigma)$. Then

$$\Big(\bigcap_{i \in I_0} \Sigma_i\Big) \cup \Big(\bigcap_{j \in I_1} \Sigma_j\Big) = \Omega_K.$$

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

Corollary 5.2.4. *Suppose that:*

(i) *For all $v \in \Omega_K$, there exists an oriented embedding $(E^v, \sigma) \to (A^v, \tau)$.*
(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 5.2.2 holds, hence there exists an embedding $(E, \sigma) \to (A, \tau)$. □

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

Corollary 5.2.5. *Suppose $K = \mathbb{Q}$ and (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 5.2.4 since (ii) holds for CM étale algebras. □

5.3. An example

As we have seen in Corollary 5.2.5 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 oriented local embeddings. More precisely, there exist CM étale algebras (E, σ) with involution and (non-split) central simple algebras (A, τ) with orthogonal involution such that (E, σ) embeds into (A, τ) everywhere locally, but not globally. Moreover, we can choose (A, τ) to be positive definite.

Let v_1, v_2 and v_3 be three distinct places of K. Let $a \in K^\times$ be such that $a \notin K_{v_i}^{\times 2}$ for $i = 1, 2, 3$, and let $b \in K^\times$ be such that $b \notin K_{v_2}^{\times 2}$ and $b \in K_{v_i}^{\times 2}$ for $i = 1$ and $i = 3$. 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 $E_2 = K(\sqrt{b})$ and 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_2 and v_3. 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 5.3.1. *For all $v \in \Omega_K$, there exists an embedding $(E^v, \sigma) \to (A^v, \tau)$ of algebras with involution.*

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, there exists an embedding $(E_1, \sigma_1) \to (H, \tau_0)$ of algebras with involution.

Let $w \in \Omega_K$ be such that $w \neq v_2$. 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

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

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 $(M_2(H^w), \tau)$.

At v_2, both H_1 and H_2 are non-split, and E_1, E_2 are quadratic field extensions of K_{v_2}. Hence E_1 embeds into H_1, and E_2 embeds in H_2. Therefore $(E_1^{v_2}, \sigma_1)$ embeds into $(H_1^{v_2}, \tau_1)$, $(E_2^{v_2}, \sigma_2)$ embeds into $(H_2^{v_2}, \tau_2)$, and hence (E^{v_2}, σ) embeds into (A^{v_2}, τ). □

Proposition 5.3.2. *There is no global embedding $(E, \sigma) \to (A, \tau)$.*

Proof. 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 $H_1^0 \oplus H_2^0$. Moreover, if a skew element is square central, then it has to be in H_1^0 or in H_2^0. Assume for contradiction that there exists an embedding $f : (E, \sigma) \to (A, \tau)$ of algebras with involution. 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 or H_2. □

In the above example, we can take $K = \mathbb{Q}$, and let v_1 and v_3 be two distinct finite places and v_2 the infinite place of $\mathbb{Q}$. Choose a and b as above. Since a and b are negative at the real place v_2, the algebra E is a CM étale algebra. Note that H_1 and H_2 are both non-split at v_2. The involution on $H_1 \otimes H_2$ is the involution on $M_4(\mathbb{R})$ adjoint to the norm form of the non-split quaternion algebra, which is definite. This provides the desired counter-example to the Hasse principle.

Acknowledgments. The third author is partially supported by National Science Foundation grant DMS-1401319.

References

[B14] Bayer-Fluckiger, E.: Embeddings of maximal tori in orthogonal groups. Ann. Inst. Fourier (Grenoble) **64**, 113–125 (2014) Zbl 1318.11054 MR 3330542

[B15] Bayer-Fluckiger, E.: Isometries of quadratic spaces. J. Eur. Math. Soc. **17**, 1629–1656 (2015) Zbl 1326.11008 MR 3361725

[BLP15] Bayer-Fluckiger, E., Lee, T.-Y., Parimala, R.: Embedding functor for classical groups and Brauer–Manin obstruction. Pacific J. Math. **279**, 87–100 (2015) Zbl 1364.20037 MR 3437771

[BLP16] Bayer-Fluckiger, E., Lee, T.-Y., Parimala, R.: Embeddings of maximal tori in classical groups over local and global fields. Izvestiya Math. **80**, 647–664 (2016) Zbl 1368.11032 MR 3535356

[Bo99] Borovoi, M.: A cohomological obstruction to the Hasse principle for homogeneous spaces. Math. Ann. **314**, 491–504 (1999) Zbl 0966.14017 MR 1704546

[BCM03] Brusamarello, R., Chuard-Koulmann, P., Morales, J.: Orthogonal groups containing a given maximal torus. J. Algebra **266**, 87–101 (2003) Zbl 1079.11023 MR 1994530

[F12] Fiori, A.: Special points on orthogonal symmetric spaces. J. Algebra **372**, 397–419 (2012) Zbl 1316.11027 MR 2990017

[G12] Garibaldi, S.: Outer automorphisms of algebraic groups and determining groups by their maximal tori. Michigan Math. J. **61**, 227–237 (2012) Zbl 1277.20057 MR 2944477

[GR12] Garibaldi, S., Rapinchuk, A.: Weakly commensurable S-arithmetic subgroups in almost simple algebraic groups of types B and C. Algebra Number Theory **7**, 1147–1178 (2013) Zbl 1285.20045 MR 3101075

[K69] Kneser, M.: Lectures on Galois Cohomology of Classical Groups. Tata Inst. Fund. Res. Lectures Math. 47, TIFR, Bombay (1969) Zbl 0246.14008 MR 0340440

[KMRT98] Knus, M., Merkurjev, A., Rost, M., Tignol, J.-P.: The Book of Involutions. Amer. Math. Soc. Colloq. Publ. 44, Amer. Math. Soc. (1998) Zbl 0955.16001 MR 1632779

[Lee14] Lee, T.-Y.: Embedding functors and their arithmetic properties. Comment. Math. Helv. **89**, 671–717 (2014) Zbl 1321.11043 MR 3260846

[LT99] Lewis, D. W., Tignol, J.-P., Classification theorems for central simple algebras with involution (with an appendix by R. Parimala). Manuscripta Math. **100**, 259–276 (1999) Zbl 0953.11011 MR 1725355

[MT95] Merkurjev, A., Tignol, J.-P.: Multiples of similitudes and the Brauer group of homogeneous varieties. J. Reine Angew. Math. **461**, 13–47 (1995) Zbl 0819.16015 MR 1324207

[PR10] Prasad, G., Rapinchuk, A. S.: Local-global principles for embedding of fields with involution into simple algebras with involution. Comment. Math. Helv. **85**, 583–645 (2010) Zbl 1223.11047 MR 2653693

[PT04] Preeti, R., Tignol, J.-P.: Multipliers of improper similitudes. Doc. Math. **9**, 183–204 (2004) Zbl 1160.11321 MR 2117412

[Sch85] Scharlau, W.: Quadratic and Hermitian Forms. Grundlehren Math. Wiss. 270, Springer, Berlin (1985) Zbl 0584.10010 MR 0770063

[T61] Tsukamoto, T.: On the local theory of quaternionic anti-hermitian forms. J. Math. Soc. Japan **13**, 387–400 (1961) MR 0136662