Local-global principles for embedding of fields with involution into simple algebras with involution

Autor(en): **Prasad, Gopal / Rapinchuk, Andrei S.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **85 (2010)**

PDF erstellt am: **20.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-130674

Comment. Math. Helv. 85 (2010), 583–645
DOI 10.4171/CMH/206

Commentarii Mathematici Helvetici

Local–global principles for embedding of fields with involution into simple algebras with involution

Gopal Prasad and Andrei S. Rapinchuk

Dedicated to Jean-Pierre Serre

Abstract. In this paper we prove local–global principles for the existence of an embedding $(E,\sigma) \hookrightarrow (A,\tau)$ of a given global field E endowed with an involutive automorphism σ into a simple algebra A given with an involution τ in all situations except where A is a matrix algebra of even degree over a quaternion division algebra and τ is orthogonal (Theorem A of the introduction). Rather surprisingly, in the latter case we have a result which in some sense is opposite to the local–global principle, viz. algebras with involution locally isomorphic to (A,τ) are distinguished by their maximal subfields invariant under the involution (Theorem B of the introduction). These results can be used in the study of classical groups over global fields. In particular, we use Theorem B to complete the analysis of weakly commensurable Zariski-dense S-arithmetic groups in all absolutely simple algebraic groups of type different from D_4 which was initiated in our paper [23]. More precisely, we prove that in a group of type D_n, n even > 4, two weakly commensurable Zariski-dense S-arithmetic subgroups are actually commensurable. As indicated in [23], this fact leads to results about length-commensurable and isospectral compact arithmetic hyperbolic manifolds of dimension $4n + 7$, with $n \geqslant 1$. The appendix contains a Galois-cohomological interpretation of our embedding theorems.

Mathematics Subject Classification (2010). 11E57, 14L35, 20G30, 22E40, 53C35.

Keywords. Local–global principles, central simple algebras, involutions, arithmetic groups, locally symmetric spaces.

1. Introduction

Let A be a central simple algebra of dimension n^2 over a field L, and let τ be an involution of A. Set $K = L^\tau$. We recall that τ is said to be of the *first* (resp., *second*) kind if the restriction $\tau|L$ is trivial (resp., nontrivial); involutions of the second kind are often called *unitary*. While dealing with central simple algebras with involution of the first kind, we will always assume that the center is a field of characteristic $\neq 2$. If τ is an involution of the first kind, then it is either of *symplectic* type (if $\dim_L A^\tau = n(n-1)/2$) or of *orthogonal* type (if $\dim_L A^\tau = n(n+1)/2$),

cf. [14], Proposition 2.6. Now, let E be an n-dimensional commutative étale L-algebra endowed with an automorphism σ of order two such that $\sigma|L = \tau|L$. In this paper, we will investigate the validity of the local–global principle for the existence of an L-embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ of algebras with involution (i.e., satisfying $\iota \circ \sigma = \tau \circ \iota$) in case K is a global field. More precisely, if K is a global field, we say that the local–global principle for embeddings holds (for a particular class of commutative étale algebras with involution (E,σ), or for a particular class of central simple algebras with involution (A,τ)) if the existence of $(L \otimes_K K_v)$-embeddings

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}) \quad \text{for all } v \in V^K$$

(here V^K denotes the set of all places of K) implies the existence of an L-embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ as above. We will only be interested in the commutative étale L-algebras E with involution σ such that

$$\dim_K E^\sigma = \begin{cases} n & \text{if } \sigma|L \neq \mathrm{id}_L, \\ \left[\frac{n+1}{2}\right] & \text{if } \sigma|L = \mathrm{id}_L, \end{cases} \tag{1}$$

as the τ-invariant maximal commutative étale subalgebras of A satisfying this condition (for $\sigma = \tau|E$) correspond to the maximal K-tori of the associated (special) unitary group $\mathrm{SU}(A,\tau)$ (cf. Proposition 2.3). So, (1) will be tacitly assumed to hold for all algebras (E,σ) considered in the paper (notice that (1) is satisfied automatically if either E is a field or $\sigma|L \neq \mathrm{id}_L$, cf. Proposition 2.1).

It turns out that the local–global principle holds unconditionally (i.e., without any additional restriction on (E,σ)) only if τ is a symplectic involution of A, and moreover, in this case, provided that there exists an embedding $E \hookrightarrow A$ as algebras without involutions, one needs to check the local conditions only for real v – cf. Theorem 5.1 and Corollary 5.3 for the precise statements. In most of the other cases, the local–global principle holds if E is a field extension of L (as opposed to a general commutative étale L-algebra). The following theorem combines the essential parts of Theorems 4.1, 6.1 and 7.3.

Theorem A. *Let L be global field. Let A be a central simple L-algebra of dimension n^2 with an involution τ, and let E/L be a* ***field extension*** *of degree n endowed with an involutive automorphism σ such that $\sigma|L = \tau|L$. Then the local–global principle for the existence of an embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ holds in each of the following situations:*

(i) *τ is an involution of the second kind;*

(ii) *$A = M_n(K)$, and τ is an orthogonal involution;*

(iii) *$A = M_m(D)$, where D is a quaternion division algebra, m is odd, and τ is an orthogonal involution.*

Assertion (i) of the above theorem for n odd was established earlier in our paper [21] (Proposition A.2 in Appendix A) where it was used to compute the metaplectic kernel for absolutely simple simply connected groups of outer type A_n. The other assertions of Theorem A were unknown prior to this work (however as this work progressed we became aware of the fact that the questions about existence of local–global principles for embeddings were raised in various contexts by different mathematicians). The results of §§ 4, 6 and 7 furnish local–global principles for embedding of commutative étale algebras with involution in more general situations. On the other hand, the examples constructed in §§ 4 and 7 show that the local–global principle may fail in general if E is not a field.

The only case not covered by the above theorem is $A = M_m(D)$, where D is a quaternion division algebra, m is even, and τ is an orthogonal involution of A (then the corresponding algebraic group $\mathrm{SU}(A, \tau)$ is of type D_m). For us, this case was, in fact, the main motivation to investigate the local–global principle for embeddings since it is linked to a question left open in the original version of our paper [23]; this question has now been resolved using Theorem B of this paper. The main focus in [23] was to determine when the "weak commensurability" of arithmetic groups implies their commensurability. Since the relevant definitions are somewhat technical, we will postpone them until §9, and instead discuss here a closely related problem whether two forms over a number field K, of an absolutely simple simply connected algebraic group G, are K-isomorphic if they have the same K-isomorphism classes of maximal K-tori. It was shown in [23], Theorem 7.5, that the latter condition indeed forces the forms to be K-isomorphic if the type of G is different from A_n $(n > 1)$, D_n $(n \geq 4)$ or E_6. On the other hand, in §9 of [23] we developed a Galois-cohomological construction of nonisomorphic K-forms having the same K-isomorphism classes of maximal K-tori for each of the following types: A_n, $n > 1$, D_n with n odd > 1, and E_6. We will now explain how examples of this kind (for classical types) can be produced using Theorem A.

Suppose we are able to construct two central simple L-algebras A_1 and A_2 of dimension n^2 endowed with involutions τ_1 and τ_2 of the same kind and type such that

(a) (A_1, τ_1) is not isomorphic to (A_2, τ_2) or its opposite;

(b) for each $v \in V^K$, the algebra $(A_1 \otimes_K K_v, \tau_1 \otimes \mathrm{id}_{K_v})$ is isomorphic as a $(L \otimes_K K_v)$-algebra to either $(A_2 \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v})$ or its opposite.

Then the corresponding special unitary groups $G_i = \mathrm{SU}(A_i, \tau_i)$ are not isomorphic over K but are isomorphic over K_v for all $v \in V^K$. Furthermore, any maximal K-torus of G_1 corresponds to a maximal commutative étale τ_1-invariant subalgebra E_1 of A_1 satisfying (1). Condition (b) implies that for each $v \in V^K$, there is an embedding

$$(E_1 \otimes_K K_v, (\tau_1|E_1) \otimes \mathrm{id}_{K_v}) \hookrightarrow (A_2 \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v})$$

of algebras with involution. So, if the local–global principle for embeddings holds for $(E_1, \tau_1|E_1)$, there exists an embedding $(E_1, \tau_1|E_1) \hookrightarrow (A_2, \tau_2)$. Thus, under appropriate assumptions, we obtain that A_1 and A_2 have the same isomorphism classes of maximal commutative étale subalgebras, invariant under the involutions and satisfying (1), hence the groups G_1 and G_2 have the same isomorphism classes of maximal K-tori.

It is simplest to implement this construction by taking for A_1 and A_2 suitable *division* algebras with involutions of the second kind as then, by Theorem A (i), the local–global principle for embeddings holds for all maximal commutative étale subalgebras invariant under involutions. (This was actually done in Example 6.6 in [23] for n odd – the restriction on n was due to the fact that while working on [23] we did not know if the local–global principle for embeddings of fields holds for arbitrary n.) Along the same lines, one can construct, for each *odd* $m \geq 3$, a central simple K-algebra A of dimension n^2, with $n = 2m$, and two orthogonal involutions τ_1 and τ_2 such that $(A, \tau_1) \not\simeq (A, \tau_2)$ but $(A \otimes_K K_v, \tau_1 \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v})$ for all $v \in V^K$, and then use Theorem A (iii) to conclude that (A, τ_1) and (A, τ_2) have at least the same isomorphism classes of maximal subfields invariant under the involutions (existence of involutions which give the same isomorphism classes of *all* maximal commutative étale subalgebras, invariant under the involutions and satisfying (1), is more subtle and requires the Galois-cohomological constructions described in [23], §9). Theorem A, however, does not provide information that would allow one to construct similar examples if m is even. Rather surprisingly, it turned out that such examples simply do not exist in this case, so in effect algebras of dimension n^2, with $4|n$, endowed with orthogonal involutions *are differentiated* by the isomorphism classes of maximal commutative étale subalgebras invariant under the involutions and satisfying (1) (and even by the isomorphism classes of maximal invariant subfields).

Theorem B. (i) *Let A_1 and A_2 be two central simple K-algebras, of dimension n^2, $n \geq 3$, endowed with orthogonal involutions τ_1 and τ_2, respectively. If A_1 and A_2 have the same isomorphism classes of n-dimensional commutative étale subalgebras invariant under the involutions and satisfying* (1) *(i.e., for any n-dimensional τ_1-invariant commutative étale subalgebra E_1 of A_1 satisfying* (1)*, there exists an embedding $(E_1, \tau_1|E_1) \hookrightarrow (A_2, \tau_2)$, and vice versa), then*

$$(A_1 \otimes_K K_v, \tau_1 \otimes \mathrm{id}_{K_v}) \simeq (A_2 \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v}) \quad \textit{for all } v \in V^K,$$

and hence, in particular, $A_1 \simeq A_2$. If n is even, then the same conclusion holds if (A_1, τ_1) and (A_2, τ_2) just have the same isomorphism classes of maximal ***subfields*** *invariant under the involutions.*

(ii) *Let A be a central simple K-algebra with an orthogonal involution τ, of dimension n^2 with $4|n$. Let $\mathscr{I} = \mathscr{I}(A, \tau)$ be the set of orthogonal involutions η of*

A such that $(A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v, \eta \otimes \mathrm{id}_{K_v})$ for all $v \in V^K$. Then given $\eta \in \mathscr{I}$, one can find an η-invariant maximal field E_η in A so that if $v \in \mathscr{I}$ is such that there exists an embedding $(E_\eta, \eta|E_\eta) \hookrightarrow (A, v)$, then $(A, v) \simeq (A, \eta)$.

We notice that since $\mathscr{I}$ in general contains more than one isomorphism class (cf. [16] in conjunction with Proposition 3.3 below), the local–global principle does not hold even for embeddings of fields with involution when n is a multiple of four (cf. Remark 8.6).

Theorem B can be used to resolve the ambiguity left open in the original version of [23] for groups of type D_{2r}: we show in §9 that at least when $r > 2$, weak commensurability of two arithmetic subgroups of an absolutely simple group of this type implies their commensurability (see Theorem 9.1 below for the precise formulation). To describe some geometric consequences of this result, we will now recall the main geometric results of [23]. Given a connected absolutely simple real algebraic group G, let X be the symmetric space of $G(\mathbb{R})$ and Γ_1 and Γ_2 be two torsion-free lattices in the latter, at least one of which is arithmetic. Let $L(X/\Gamma_1)$ and $L(X/\Gamma_2)$ be the set of lengths of closed geodesics on X/Γ_1 and X/Γ_2 respectively. X/Γ_1 and X/Γ_2 are said to be *length-commensurable* if $\mathbb{Q} \cdot L(X/\Gamma_1) = \mathbb{Q} \cdot L(X/\Gamma_2)$. We have proved in [23] that if either X/Γ_1 and X/Γ_2 are length-commensurable, or they are compact and isospectral, and G is of type other than A_n $(n > 1)$, D_n $(n \geq 4)$ and E_6, then X/Γ_1 and X/Γ_2 are commensurable (i.e., they admit a common finite-sheeted cover). Theorem 9.1 of this paper allows us to draw the same conclusion if G is of type D_{2r} with $r > 2$, for example, if X is the hyperbolic space of dimension $4r - 1$, with $r > 2$. It has been shown in [23], §9, that if G is of type A_r, D_{2r+1}, $r > 1$, or E_6, then the above conclusion fails in general.

In the Appendix, we interpret the problem of the existence of an embedding $(E, \sigma) \hookrightarrow (A, \tau)$ in terms of Galois cohomology and also relate it to the problem of finding a rational point on a certain homogeneous space.

Notation. For a field K, $\overline{K}$ will denote an algebraic closure. If K is a global field, V^K will denote the set of all places of K, and V_r^K (resp., V_f^K) the set of real (resp., finite) places.

Acknowledgments. Both authors were partially supported by the NSF (grants DMS-0653512 and DMS-0502120), BSF (grant 2004083) and the Humboldt Foundation.

It is a pleasure to thank Jean-Louis Colliot-Thélène and Jean-Pierre Tignol for their comments. We thank the referee for suggestions that helped to improve the exposition.

2. On commutative étale algebras with involution

In §§2, 3, we collect, with partial proofs, some known results about étale algebras and their embeddings into central simple algebras. In these two sections, L will denote an arbitrary infinite field. Let E be a commutative étale L-algebra of dimension n. Then $E = \prod_{i=1}^{r} E_i$, where E_i/L is a separable field extension and $\sum_{i=1}^{r}[E_i : L] = n$. As usual, for $x = (x_1, \dots, x_r) \in E$, we set $N_{E/L}(x) = \prod_{i=1}^{r} N_{E_i/L}(x_i)$. Let σ be a ring automorphism of E of order two leaving L invariant.

Proposition 2.1. (1) *Assume that* $\sigma|L \neq \mathrm{id}_L$ *and set* $K = L^\sigma$. *Then* $\dim_K E^\sigma = n$ *and any* $x \in E$ *such that* $x\sigma(x) = 1$ *is of the form* $x = y\sigma(y)^{-1}$ *for some* $y \in E^\times$.

(2) *Let now* $\sigma|L = \mathrm{id}_L$, *and assume that* $\dim_L E^\sigma = \left[\frac{n+1}{2}\right]$. *If* $x \in E$ *satisfies* $x\sigma(x) = 1$, *then in each of the following cases:* (i) n *is even, or* (ii) n *is odd and* $N_{E/L}(x) = 1$, *we have* $x = y\sigma(y)^{-1}$ *for some* $y \in E^\times$.

Proof. (1) We have $E = E^\sigma \otimes_K L$ (cf. [1], AG 14.2), so $\dim_K E^\sigma = n$. Clearly, E is a direct product of σ-invariant subalgebras R of one of the following types: (a) R is a separable field extension of L, or (b) $R = R' \times R''$ with R', R'' separable field extensions of L interchanged by σ, and it is enough to prove the second assertion of (1) for each of these types of algebras. In case (a), the claim follows from the Hilbert's Theorem 90. In case (b), we have $x = (x', x'')$ with $x'\sigma(x'') = 1_{R'}$ and $x''\sigma(x') = 1_{R''}$. Set $y = (x', 1_{R''})$. Then $x = y\sigma(y)^{-1}$, as required.

(2) Here E is a direct product of σ-invariant subalgebras R of the following three types: (a) R is a separable field extension of L and $\sigma|R \neq \mathrm{id}_R$; (b) same R but $\sigma|R = \mathrm{id}_R$; (c) $R = R' \times R''$ where R', R'' are separable field extensions of L interchanged by σ. In cases (a) and (c), we have $\dim_L R^\sigma = (1/2)\dim_L R$, and the same argument as in (1) shows that any $x \in R$ satisfying $x\sigma(x) = 1$ is of the form $x = y\sigma(y)^{-1}$ for some $y \in R^\times$, in particular, $N_{R/L}(x) = 1$. The assumption $\dim_L E^\sigma = \left[\frac{n+1}{2}\right]$ implies that if n is even, then E does not have components of type (b), and our assertion follows. If n is odd, then there is only one component of type (b), and this component is 1-dimensional, i.e., $E = E' \times E''$ where E' is a direct product of components of types (a) and (c), and $E'' = L$. Writing $x = (x', x'')$, we observe that $N_{E/L}(x) = 1$ implies that $x'' = 1$, and our assertion again follows. □

Proposition 2.2. *We assume that* L *is not of characteristic* 2. *Let* E *be a commutative étale* L*-algebra with an involution* σ *such that* $\sigma|L = \mathrm{id}_L$, *with* $n := \dim_L E$ *even. Set* $F = E^\sigma$ *and assume that* $\dim_L F = n/2$. *Then there exists* $d \in F^\times$ *such that*

$$(E, \sigma) \simeq (F[x]/(x^2 - d), \theta),$$

where θ *is defined by* $x \mapsto -x$.

Proof. We have seen in the proof of Proposition 2.1 (2) that E is a direct product of σ-invariant subalgebras R of type (a) or (c) introduced therein, and it is enough to prove our claim for algebras of each of those types. If R is of type (a), then the assertion is well known. So, let $R = R' \times R''$ where R' and R'' are separable extensions of L such that $\sigma(R') = R''$. Then $F = R^\sigma$ coincides with $\{(a, \sigma(a)) | a \in R'\}$, using which it is easy to see that the map $F[x] \to E$, $x \mapsto (1, -1)$, yields an isomorphism

$$(F[x]/(x^2 - 1), \theta) \simeq (E, \sigma),$$

so we can take $d = 1$. □

Now, let A be a central simple L-algebra with an involution τ, $\dim_L A = n^2$. Set $K = L^\tau$, and let $H = \mathrm{U}(A, \tau)$ and $G = \mathrm{SU}(A, \tau)$ be the corresponding algebraic K-groups. Given an n-dimensional τ-invariant (maximal) commutative étale L-subalgebra E of A, we consider the associated maximal K-torus $\mathrm{R}_{E/K}(\mathrm{GL}_1) \subset \mathrm{R}_{L/K}(\mathrm{GL}_{1,A})$, and then define the corresponding K-tori

$$S = (\mathrm{R}_{E/K}(\mathrm{GL}_1) \cap H)^\circ \quad \text{and} \quad T = (\mathrm{R}_{E/K}(\mathrm{GL}_1) \cap G)^\circ$$

in H and G, respectively.

Proposition 2.3. *S is a maximal torus in H (resp., T is a maximal torus in G) if and only if* (1) *holds (for $\sigma = \tau|_E$). Any maximal K-torus in H (resp., G) corresponds to an n-dimensional τ-invariant commutative étale L-subalgebra E of A for which* (1) *holds.*

Proof. The involution τ induces an automorphism of $\mathrm{R}_{E/K}(\mathrm{GL}_1)$, and we then get a homomorphism

$$\varphi\colon \mathrm{R}_{E/K}(\mathrm{GL}_1) \longrightarrow S, \quad x \longmapsto \tau(y)y^{-1}.$$

Clearly, $\ker \varphi = \mathrm{R}_{E^\tau/K}(\mathrm{GL}_1)$, yielding the bound

$$\dim S \geqslant \dim_K E - \dim_K E^\tau = \dim_K E_{-1},$$

where E_{-1} is the (-1)-eigenspace of τ in E. On the other hand, the Cayley–Dickson parametrization $s \mapsto (1 - s)(1 + s)^{-1}$ gives an injective rational map of S into the affine space corresponding to E_{-1}, providing the opposite bound. Therefore,

$$\dim S = \dim_K E - \dim_K E^\tau = \dim_K E_{-1} \tag{2}$$

in all cases. If $\tau|L \neq \mathrm{id}_L$, then, on the one hand, $\dim_K E^\tau = n$ (Proposition 2.1 (1)), hence $\dim S = n$, and on the other hand, $\mathrm{rk}\, H = n$. So, S is a maximal torus of H. Furthermore, $\dim T \geqslant n - 1$ and $\mathrm{rk}\, G = n - 1$, so T is a maximal torus

of G. Now, suppose $\tau|L = \mathrm{id}_L$. Then $G = H^\circ$ and $S = T$. If n is even, then for both orthogonal and symplectic involutions we have $\mathrm{rk}\, G = n/2$, and in view of (2), the fact that $\dim S = n/2$ is equivalent to $\dim_K E^\tau = n/2$, i.e., to (1). In n is odd, then the involution is necessarily orthogonal and $\mathrm{rk}\, G = (n-1)/2$. Then again from (2) we obtain that $\dim S = (n-1)/2$ is equivalent to the assertion that $\dim_K E^\tau = (n+1)/2$, which is again (1).

Using the well-known description of the possibilities for $(A \otimes_K \bar{K}, \tau \otimes \mathrm{id}_{\bar{K}})$, one easily produces a maximal torus T_0 of G which generates a $\bar{K}$-subalgebra of dimension n if $\sigma|L = \mathrm{id}_L$, and of dimension $2n$ otherwise, and in the latter case this subalgebra is an algebra over $L \otimes_K \bar{K}$. Then in view of the conjugacy of maximal tori ([1], 11.3), we see that the same is true for any maximal torus. Now, if T is a maximal K-torus of G, then the Zariski-density of $T(K)$ in T ([1], 8.14) implies that the K-subalgebra E of A generated by $T(K)$ (which is automatically étale and τ-invariant) is an n-dimensional L-algebra. Since T is maximal, (1) holds for E by the first part of the proof. The argument for maximal tori in H is similar. □

The connection between the subalgebras satisfying (1) and the maximal tori of the corresponding unitary group can be used to prove the following.

Proposition 2.4. *Let A be a central simple algebra over a global field L, of dimension n^2, with an involution τ, and let $G = \mathrm{SU}(A, \tau)$. Suppose that we are given a finite set V of places of $K = L^\tau$, and for each $v \in V$, an n-dimensional $(\tau \otimes \mathrm{id}_{K_v})$-invariant commutative étale $(L \otimes_K K_v)$-subalgebra $E(v)$ of $A \otimes_K K_v$ satisfying* (1) *of* §1. *Then there exists an n-dimensional τ-invariant commutative étale L-subalgebra E of A satisfying* (1) *of* §1 *such that*

$$E(v) = g_v^{-1}(E \otimes_K K_v)g_v \quad \text{with } g_v \in G(K_v),$$

in particular, $(E(v), (\tau \otimes \mathrm{id}_{K_v})|E(v)) \simeq (E \otimes_K K_v, (\tau|E) \otimes \mathrm{id}_{K_v})$ as $L \otimes_K K_v$-algebras with involutions, for all $v \in V$.

Proof. Corresponding to $E(v)$, there is a maximal K_v-torus $T(v)$ of G. Using weak approximation in the variety of maximal tori of G (cf. [20], Corollary 3 in §7.2), we can find a maximal K-torus T of G such that for all $v \in V$, $T(v) = g_v^{-1}Tg_v$ for some $g_v \in G(K_v)$. By Proposition 2.3, T corresponds to an n-dimensional τ-invariant commutative étale L-subalgebra E of A, which is as required (notice that since $g_v \in G(K_v)$, the K_v-algebra isomorphism $a \mapsto g_v a g_v^{-1}$, $E(v) \to E \otimes_K K_v$, respects involutions). □

Next, we will recall the definition of a class of maximal tori in a given semi-simple group which will play an important role in §9 (cf. also [22], [23]). Let G be a connected semi-simple group defined over a field F. Fix a maximal F-torus T of G, and let $\Phi = \Phi(G, T)$ denote the corresponding root system. Furthermore,

let F_T be the minimal splitting field of T (over F). Then the action of the Galois group $\mathrm{Gal}(F_T/F)$ on the character group $X(T)$ of T induces an injective group homomorphism $\theta_T\colon \mathrm{Gal}(F_T/F) \to \mathrm{Aut}(\Phi)$. In the sequel, we will identify the Weyl group $W(\Phi)$ of the root system Φ with the Weyl group $W(G,T)$. We say that T is *generic* (over F) if $\theta_T(\mathrm{Gal}(F_T/F)) \supset W(G,T)$.

Proposition 2.5. *Let (A,τ) be a central simple L-algebra with involution, of dimension n^2, with $n > 2$. Set $K = L^\tau$, and let $G = \mathrm{SU}(A,\tau)$ be the corresponding algebraic K-group. Furthermore, let E be an n-dimensional τ-invariant commutative étale L-subalgebra of A that satisfies* (1) *of* §1, *and let T be the corresponding maximal K-torus of G. Assume that T is generic over K.*

- *If either τ is of the first kind and n is even, or τ is of the second kind, then E is a field extension of L.*
- *If τ is of the first kind and n is odd, then $E = E' \times K$ where E' is a field extension of $K = L$.*

Proof. Since the Weyl group acts on $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ (nontrivially and) irreducibly, the assumption that T is generic over K implies that T does not contain proper K-subtori and is K-anisotropic. Assume that τ is of the first kind. If E is not as described in the statement of the proposition, then (cf. the proof of Proposition 2.1) there is a nontrivial decomposition $E = E_1 \times E_2$ such that $E_2 \neq K$ and E_1 is either a τ-stable field extension of K such that $\tau|E_1$ is nontrivial, or is of the form $E_1 = E' \times E''$ and τ interchanges E' and E''. But in the first case T has a proper K-subtorus corresponding to E_1, and in the second case a 1-dimensional K-split subtorus coming from the subalgebra $K \times K \subset E' \times E''$, which is impossible.

Let now τ be of the second kind. Then $E \simeq L \otimes_K F$ where $F = E^\tau$. Given a K-subalgebra F' of F of dimension n', corresponding to it there is a K-subtorus of T of dimension $n' - 1$. As T does not contain proper K-subtori, we conclude that F does not contain any proper K-subalgebra of dimension > 1. Since by our assumption, $n > 2$, we see that F must be a field extension of K. To prove that E is a field, we need to show that L and F are linearly disjoint over K. If L and F are not linearly disjoint over K, E contains a subalgebra of the form $L \otimes_K L$ (with the involution acting on the first factor). Corresponding to this subalgebra, we have a K-torus $S \subset H := \mathrm{U}(A,\tau)$ which is K-isomorphic to $\mathrm{R}_{L/K}(\mathrm{GL}_1)$. Since $H/G \simeq \mathrm{R}^{(1)}_{L/K}(\mathrm{GL}_1)$ is K-anisotropic, the 1-dimensional K-split subtorus of S is contained in G, hence in T, a contradiction. □

We will now formulate, for the convenience of future reference, two propositions about embeddings of commutative étale algebras into central simple algebras. The first proposition is a particular case of Proposition 4.3 in [6].

Proposition 2.6. *Let A be a central simple algebra of dimension n^2 over a field L, and let E be an n-dimensional commutative étale L-algebra. If $E = \prod_{j=1}^{\ell} E_j$, where E_j is a (separable) field extension of L, then E admits an L-embedding into A if and only if each E_j splits A, or, equivalently, $A \otimes_L E$ is a direct product of matrix algebras over field extensions of L.*

Proposition 2.7. *Let A be a central simple algebra of dimension n^2 over a* ***global*** *field L, and E be an n-dimensional commutative étale L-algebra. Then an L-embedding $\varepsilon\colon E \hookrightarrow A$ exists if and only if for every $w \in V^L$ there exists an L_w-embedding $\varepsilon_w\colon E \otimes_L L_w \hookrightarrow A \otimes_L L_w$.*

This follows from Proposition 2.6 and the fact that for a global field F, the map $\mathrm{Br}(F) \to \bigoplus_{w \in V^F} \mathrm{Br}(F_w)$ is injective (cf. [19], §18.4).

3. Embeddings of commutative étale algebras with involution into central simple algebras with involution

In this section, L is an arbitrary field, A is a central simple L-algebra of dimension n^2, and τ an involution on A. Let E be an n-dimensional commutative étale L-algebra with an involutive automorphism σ such that $\sigma|L = \tau|L$ and condition (1) of the introduction holds. Let $F = E^{\sigma}$. Let $\varepsilon\colon E \hookrightarrow A$ be an L-embedding which may not respect the given involutions.

Proposition 3.1 (cf. [13], §2.5). *There exists a τ-symmetric $g \in A^{\times}$ such that for*

$$\theta = \tau \circ \mathrm{Int}\, g = \mathrm{Int}\, g^{-1} \circ \tau,$$

we have

$$\varepsilon(\sigma(x)) = \theta(\varepsilon(x)) \quad \textit{for all} \quad x \in E, \tag{3}$$

i.e., $\varepsilon : (E, \sigma) \hookrightarrow (A, \theta)$ is an L-embedding of algebras with involution.

Proof. Since $\tau \circ \varepsilon \circ \sigma$ is an L-embedding of E into A, according to the "Skolem–Noether Theorem" for commutative étale subalgebras of dimension n (see [12], Hilfssatz 3.5, or [13], p. 37)[1] there exists $g \in A^{\times}$ such that

$$\varepsilon(x) = g^{-1}(\tau \circ \varepsilon \circ \sigma)(x)g \quad \text{for all } x \in E.$$

[1] We would like to point out the fact, apparently missing in the literature, that this form of the Skolem–Noether Theorem immediately follows from "Hilbert's Theorem 90". More precisely, let A be a central simple L-algebra of dimension n^2, and let E be a commutative étale L-algebra of dimension n. Let us show that given two L-embeddings $\iota_i : E \hookrightarrow A$ for $i = 1, 2$, there exists $g \in A^{\times}$ such that $\iota_2(x) = g^{-1}\iota_1(x)g$ for all $x \in E$. We will use ι_i to also denote its natural extension $E \otimes_L L_{\mathrm{sep}} \hookrightarrow A \otimes_L L_{\mathrm{sep}}$, where L_{sep} is a separable closure of L. There exists $a \in E \otimes_L L_{\mathrm{sep}}$ whose characteristic polynomial $p(t)$ has n distinct roots, and then $E \otimes_L L_{\mathrm{sep}} = L_{\mathrm{sep}}[a]$. The matrices $\iota_1(a), \iota_2(a) \in A \otimes_L L_{\mathrm{sep}} = M_n(L_{\mathrm{sep}})$ have $p(t)$ as their common

Substituting $\sigma(x)$ for x, we obtain

$$\varepsilon(\sigma(x)) = g^{-1}\tau(\varepsilon(x))g. \tag{4}$$

Now

$$\varepsilon(x) = g^{-1}(\tau\circ\varepsilon\circ\sigma)(x)g = g^{-1}\tau\left(g^{-1}\tau(\varepsilon(x))g\right)g = (g^{-1}\tau(g))\varepsilon(x)(\tau(g)^{-1}g),$$

for all $x \in E$. Since $\varepsilon(E)$ is its own centralizer in A, we see that

$$g^{-1}\tau(g) = \varepsilon(a) \quad \text{for some } a \in E.$$

Furthermore,

$$\varepsilon(\sigma(a)) = g^{-1}\tau(\varepsilon(a))g = g^{-1}\tau(g^{-1}\tau(g))g = \tau(g)^{-1}g = \varepsilon(a^{-1}).$$

Therefore, $a\sigma(a) = 1$, so according to Proposition 2.1, $a = b\sigma(b)^{-1}$ for some $b \in E^\times$ (one needs to observe that if $\sigma|L = \mathrm{id}_L$ and n is odd, $N_{E/L}(a) = \mathrm{Nrd}_{A/L}(g^{-1}\tau(g)) = 1$). Set $h = g\varepsilon(b)$. Then we have

$$\varepsilon(\sigma(x)) = \varepsilon(b)^{-1}\varepsilon(\sigma(x))\varepsilon(b) = h^{-1}\tau(\varepsilon(x))h \quad \text{for } x \in E$$

and, in addition,

$$\tau(h) = \tau(\varepsilon(b))\tau(g) = g\varepsilon(\sigma(b))g^{-1}\tau(g) = g\varepsilon(\sigma(b)a) = g\varepsilon(b) = h.$$

So, we could have assumed from the very beginning that g in (4) is τ-symmetric. Then

$$\theta := \mathrm{Int}\, g^{-1}\circ\tau = \tau\circ\mathrm{Int}\, g$$

is an involution, and it follows from (4) that (3) holds. □

Fix an involution $\theta = \tau\circ\mathrm{Int}\, g$, where $\tau(g) = g$, satisfying (3).

Theorem 3.2. *The following conditions are equivalent:*

(i) *There exists an L-embedding $\iota\colon (E,\sigma) \to (A,\tau)$ of algebras with involution.*

(ii) *There exists an $a \in F^\times$ such that $(A,\theta_a) \simeq (A,\tau)$ as algebras with involution, where for $x \in F^\times$, we set $\theta_x = \theta\circ\mathrm{Int}\,\varepsilon(x) = \tau\circ\mathrm{Int}(g\varepsilon(x))$.*

characteristic polynomial, and are therefore conjugate to each other. It follows that there exists $h \in (A\otimes_L L_{\mathrm{sep}})^\times$ such that $\iota_2(x) = h^{-1}\iota_1(x)h$ for all $x \in E\otimes_L L_{\mathrm{sep}}$. Then for any $\theta \in \mathrm{Gal}(L_{\mathrm{sep}}/L)$, the element $h\theta(h)^{-1}$ centralizes $\iota_1(E)$, and hence there exists $\xi_\theta \in (E\otimes_L L_{\mathrm{sep}})^\times$ such that $\iota_1(\xi_\theta) = h\theta(h)^{-1}$. Then the family $\xi = \{\xi_\theta\}$ is a Galois 1-cocyle with values in $T(L_{\mathrm{sep}}) = (E\otimes_L L_{\mathrm{sep}})^\times$, where $T = \mathrm{R}_{E/L}(\mathrm{GL}_1)$ in the standard notations. Since $H^1(L,T) = \{1\}$ ("Hilbert's Theorem 90"), there exists $t \in (E\otimes_L L_{\mathrm{sep}})^\times$ such that $\xi_\theta = t\theta(t)^{-1}$ for all $\theta \in \mathrm{Gal}(L_{\mathrm{sep}}/L)$. Set $g = \iota_1(t)^{-1}h \in (A\otimes_L L_{\mathrm{sep}})^\times$. Then $\theta(g) = g$ for every θ, implying that $g \in A^\times$. At the same time, $\iota_2(x) = g^{-1}\iota_1(x)g$ for all $x \in E$, as required.

(iii) $g\varepsilon(b) = \tau(h)h$ *for some* $b \in F^\times$ *and* $h \in A^\times$.

Proof. (i) $\Longrightarrow$ (ii) Using the Skolem–Noether Theorem, we see that there exists $s \in A^\times$, such that $\iota = \operatorname{Int} s \circ \varepsilon$. By our assumption, $\iota \circ \sigma = \tau \circ \iota$ on E, and by our construction of θ, we have $\varepsilon \circ \sigma = \theta \circ \varepsilon$ on E. Let $\psi = \operatorname{Int} s$. Then

$$\psi \circ \theta \circ \varepsilon = \psi \circ \varepsilon \circ \sigma = \tau \circ \psi \circ \varepsilon \text{ on } E.$$

So, there exists $b \in E^\times$ such that

$$\tau \circ \psi = \psi \circ \theta \circ \operatorname{Int} \varepsilon(b), \tag{5}$$

i.e.,

$$\tau \circ \psi = \psi \circ \theta_b. \tag{6}$$

From

$$\mathrm{id}_A = (\psi^{-1} \circ \tau \circ \psi)^2 = (\theta \circ \operatorname{Int} \varepsilon(b))^2 = \operatorname{Int} \varepsilon(\sigma(b)^{-1}b),$$

it follows that $t := \sigma(b)^{-1}b \in L$, and clearly $\sigma(t) = t^{-1}$. If $\sigma|L = \mathrm{id}_L$, then $t = \pm 1$. However, if $t = -1$, then θ_b is an involution of type different from that of θ and τ (cf. [14], Proposition 2.7(3)), and (6) would be impossible. So, $t = 1$ and $b \in F^\times$, as desired. If $\sigma|L \neq \mathrm{id}_L$, then $N_{L/K}(t) = 1$, and therefore by Hilbert's Theorem 90, we can write

$$t = \sigma(b)^{-1}b = \sigma(c)c^{-1} \text{ for some } c \in L^\times.$$

Then $\sigma(bc) = bc$ and $\theta_b = \theta_{bc}$. Take $a = bc$.

(ii) $\Longrightarrow$ (iii) Let $\varphi\colon (A, \theta_a) \to (A, \tau)$ be an isomorphism of L-algebras with involution. Then $\varphi = \operatorname{Int} h$ for some $h \in A^\times$. Equation (4) implies that

$$\varepsilon(a) = \varepsilon(\sigma(a)) = g^{-1}\tau(\varepsilon(a))g,$$

so

$$\tau(g\varepsilon(a)) = \tau(\varepsilon(a))\tau(g) = \tau(\varepsilon(a))g = g\varepsilon(a),$$

i.e., $g\varepsilon(a)$ is τ-symmetric. Using the equality $\varphi \circ \theta_a = \tau \circ \varphi$ we obtain that

$$\operatorname{Int} h \circ \theta_a = \operatorname{Int} h \circ \tau \circ \operatorname{Int}(g\varepsilon(a)) = \tau \circ \operatorname{Int}(\tau(h)^{-1}g\varepsilon(a)) = \tau \circ \operatorname{Int} h.$$

Therefore, $(g\varepsilon(a))^{-1}\tau(h)h \in L^\times$, i.e., $\tau(h)h = \lambda g\varepsilon(a)$ for some $\lambda \in L^\times$. Since $g\varepsilon(a)$ is τ-symmetric, λ must lie in $K^\times$. Let $b = a\lambda \in F^\times$. Then $g\varepsilon(b) = \tau(h)h$.

(iii) $\Longrightarrow$ (i) Suppose $g\varepsilon(b) = \tau(h)h$ for some $b \in F^\times$ and $h \in A^\times$. Set $\varphi = \operatorname{Int} h$. Then

$$\varphi \circ \theta_b = \operatorname{Int} h \circ \tau \circ \operatorname{Int}(g\varepsilon(b)) = \tau \circ \operatorname{Int}(\tau(h)^{-1}g\varepsilon(b)) = \tau \circ \operatorname{Int} h = \tau \circ \varphi.$$

It follows that for $\iota = \varphi \circ \varepsilon$ we have

$$\iota \circ \sigma = \varphi \circ \varepsilon \circ \sigma = \varphi \circ \theta \circ \varepsilon = \varphi \circ \theta_b \circ \varepsilon = \tau \circ \varphi \circ \varepsilon = \tau \circ \iota,$$

as required. □

We conclude this section with the following well-known fact.

Proposition 3.3. *Let $A = M_m(D)$, where D is a central division algebra over L endowed with an involution $a \mapsto \bar{a}$, and define an involution $x \mapsto x^*$ of A by $(x_{ij}) \mapsto (\overline{x_{ji}})$. Let ϵ be either $+1$ or -1. For $i = 1, 2$, let $Q_i \in A^\times$ be such that $Q_i^* = \epsilon Q_i$, and define involutions τ_i by $\tau_i(x) = Q_i^{-1} x^* Q_i$. Then $(A, \tau_1) \simeq (A, \tau_2)$ as L-algebras with involution if and only if there exist $z \in A^\times$ and $\lambda \in K^\times$ (where $K = L^\tau$) such that $Q_2 = \lambda z^* Q_1 z$.*

Proof. Any L-algebra automorphism $\varphi\colon A \to A$ is inner, i.e., it is of the form $x \mapsto z^{-1}xz$ for some $z \in A^\times$. Furthermore, a direct computation shows that the condition $\tau_2(\varphi(x)) = \varphi(\tau_1(x))$, for all $x \in A$, is equivalent to the fact that $\lambda := (z^*)^{-1} Q_2 z^{-1} Q_1^{-1}$ belongs to $Z(A) = L$. Then $Q_2 = \lambda z^* Q_1 z$, and applying * we obtain that actually $\lambda \in K$. □

We notice that the matrix equation relating Q_1 and Q_2 says that the associated (skew)-hermitian forms are *similar,* i.e., an appropriate scalar multiple of one is equivalent to the other.

4. Algebras with an involution of the second kind

In this section, we will establish a local–global principle for embedding of fields with an involutive automorphism into simple algebras with an involution of the second kind, which is assertion (i) of Theorem A (of the introduction). A partial result (with some extra conditions) in this direction was obtained earlier in our paper [21], Proposition A.2, and the argument below is a modification of the argument given therein. What has not been previously observed is that the local–global principle *fails* for general commutative étale algebras (see Example 4.6 below).

Theorem 4.1. *Let A be a central simple algebra over a global field L, of dimension n^2, with an involution τ of the second kind, $K = L^\tau$, and let E/L be a field extension of degree n provided with an involutive automorphism σ such that $\tau|L = \sigma|L$. Suppose that for each $v \in V^K$ there exists an $(L \otimes_K K_v)$-embedding*

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$$

of algebras with involutions. Then there exists an L-embedding

$$\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$$

of algebras with involutions.

Proof. First, we observe that the existence of ι_v for all $v \in V^K$ implies the existence of an L_w-embedding $\varepsilon_w : E \otimes_L L_w \hookrightarrow A \otimes_L L_w$, for all $w \in V^L$. Indeed, fix a w and let $v \in V^K$ be such that $w|v$. If $L \otimes_K K_v$ is a field, then it coincides with L_w, and then $\varepsilon_w = \iota_v$ is the required embedding. On the other hand, if $L \otimes_K K_v$ is not a field, then v has two extension to L, one of which is w and the other will be denoted w'. We have

$$L \otimes_K K_v \simeq L_w \times L_{w'} \simeq K_v \times K_v,$$

and

$$E \otimes_K K_v \simeq E \otimes_L (L \otimes_K K_v) \simeq (E \otimes_L L_w) \times (E \otimes_L L_{w'}).$$

Furthermore,

$$A \otimes_K K_v \simeq A \otimes_L (L \otimes_K K_v) \simeq (A \otimes_L L_w) \times (A \otimes_L L_{w'}). \tag{7}$$

It follows that the restriction of ι_v to the component $E \otimes_L L_w$ provides the required embedding ε_w. Now, by Proposition 2.7, the existence of the embeddings ε_w for $w \in V^L$ implies the existence of an L-embedding $\varepsilon\colon E \hookrightarrow A$, which we will fix.

Next, using Proposition 3.1, we can find an involution θ on A of the form

$$\theta = \tau \circ \operatorname{Int} g = \operatorname{Int} g^{-1} \circ \tau$$

that satisfies $\theta(\varepsilon(x)) = \varepsilon(\sigma(x))$ for all $x \in E$. Then according to Theorem 3.2, an L-embedding $\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$ as algebras with involutions exists if and only if we can find $a \in F^\times$, where $F = E^\sigma$, and $h \in A^\times$ so that

$$g = \tau(h) h \varepsilon(a). \tag{8}$$

For $v \in V^K$, the existence of ι_v implies the existence of $a_v \in (F \otimes_K K_v)^\times$ and $h_v \in (A \otimes_K K_v)^\times$ such that

$$g = \tau(h_v) h_v \varepsilon(a_v) \tag{9}$$

(to avoid cumbersome notations, we write ε and τ instead of $\varepsilon \otimes \mathrm{id}_{K_v}$ and $\tau \otimes \mathrm{id}_{K_v}$). Indeed, if $L \otimes_K K_v$ is a field, this immediately follows from Theorem 3.2.

To treat the case where $L \otimes_K K_v$ is not a field, we first note the following fact that will be used repeatedly: as in (7), we have an isomorphism $A \otimes_K K_v \simeq A_1 \times A_2$, where A_1, A_2 are simple K_v-algebras, and τ interchanges A_1 and A_2. Thus, A_2 can be identified with the opposite algebra A_1^{op}, and moreover, this identification can be chosen so that τ corresponds to the exchange involution $(x_1, x_2) \mapsto (x_2, x_1)$. It follows that any τ-symmetric element in $A \otimes_K K_v$ (i.e., any element in $A^\tau \otimes_K K_v$) can be written in the form $\tau(h_v) h_v$ for some $h_v \in A \otimes_K K_v$.[2] In particular, it follows that (9) has a solution with $a_v = 1$.

[2]We note here for future use that the the same argument shows that any τ-symmetric element in $A \otimes_K K_v$ with reduced norm 1 can be written in the form $\tau(h_v) h_v$ with $h_v \in A \otimes_K K_v$ of reduced norm 1 - one only needs to observe that the natural extension $\mathrm{Nrd}_{A \otimes_K K_v / L \otimes_K K_v}$ of the reduced norm map $\mathrm{Nrd}_{A/L}$ coincides with $(\mathrm{Nrd}_{A_1/K_v}, \mathrm{Nrd}_{A_2/K_v})$ in terms of the above identification.

Taking reduced norms in (9), we obtain

$$\mathrm{Nrd}_{A/L}(g) = N_{F\otimes_K K_v/K_v}(a_v)N_{L\otimes_K K_v/K_v}(b_v), \tag{10}$$

where $b_v = \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(h_v)$. We will now make use of the following.

Proposition 4.2. *Let L/K be an abelian Galois extension of degree m that satisfies the Hasse norm principle (which is automatically the case if L/K is cyclic), and F/K be a finite extension linearly disjoint from L over K. Then the pair F and L satisfies the Hasse multinorm principle over K, i.e.,*

$$N_{F/K}(J_F)N_{L/K}(J_L) \cap K^\times = N_{F/K}(F^\times)N_{L/K}(L^\times), \tag{11}$$

where J_F and J_L denote the group of idèles of F and L respectively.

Proof. Let $E = FL$. By our assumption, the restriction map

$$\mathrm{Gal}(E/F) \xrightarrow{\theta} \mathrm{Gal}(L/K)$$

is an isomorphism. Using the commutative diagram (cf. [5], Chapter VII, Proposition 4.3)

$$\begin{array}{ccc} J_F & \xrightarrow{\psi_{E/F}} & \mathrm{Gal}(E/F) \\ {\scriptstyle N_{F/K}}\downarrow & & \downarrow{\scriptstyle \theta} \\ J_K & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K), \end{array}$$

in which $\psi_{E/F}$ and $\psi_{L/K}$ are the corresponding Artin maps, we see that $N_{F/K}$ induces an isomorphism

$$J_F/F^\times N_{E/F}(J_E) \simeq J_K/K^\times N_{L/K}(J_L). \tag{12}$$

Now, suppose

$$a = N_{F/K}(x)N_{L/K}(y)$$

where $a \in K^\times$, $x \in J_F$ and $y \in J_L$. Then

$$N_{F/K}(x) = aN_{L/K}(y)^{-1}.$$

So, it follows from the isomorphism (12) that $x \in F^\times N_{E/F}(J_E)$, i.e.

$$x = x'N_{E/F}(z) \quad \text{with } x' \in F^\times,\ z \in J_E.$$

Then

$$aN_{F/K}(x')^{-1} = N_{L/K}(y)N_{E/K}(z) = N_{L/K}(yN_{E/L}(z)) \in N_{L/K}(J_L).$$

Since L/K satisfies the Hasse norm principle, we see that

$$aN_{F/K}(x')^{-1} = N_{L/K}(y') \quad \text{for some } y' \in L^\times,$$

as required. □

Continuing with the notations introduced in the previous proposition, we notice that given $z \in K^\times$, for any $v \in V_f^K$ which is unramified in both F and L, and z is a unit in $K_v^\times$, z is automatically the norm of a *unit*. Since all but finitely many $v \in V_f^K$ satisfy the above conditions, we see that if for every $v \in V^K$,

$$z \in N_{F\otimes_K K_v/K_v}((F \otimes_K K_v)^\times)N_{L\otimes_K K_v/K_v}((L \otimes_K K_v)^\times),$$

then actually

$$z \in N_{F/K}(J_F)N_{L/K}(J_L).$$

This remark in conjunction with (10) implies that Proposition 4.2 can be applied in our situation with $F = E^\sigma$, which yields the existence of $a \in F^\times, b \in L^\times$ such that

$$\mathrm{Nrd}_{A/L}(g) = N_{F/K}(a)N_{L/K}(b) = \mathrm{Nrd}_{A/L}(\varepsilon(a))N_{L/K}(b). \tag{13}$$

We claim that a solution (a, b) to (13) can be chosen so that

$$g\varepsilon(a)^{-1} \in \Sigma(v) := \{\tau(h_v)h_v \mid h_v \in (A \otimes_K K_v)^\times\} \tag{14}$$

and

$$b \in \Theta(v) := \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}((A \otimes_K K_v)^\times) \tag{15}$$

for all $v \in V_r^K$. To see this, we consider the K-torus

$$T = \{(x, y) \in \mathrm{R}_{F/K}(\mathrm{GL}_1) \times \mathrm{R}_{L/K}(\mathrm{GL}_1) \mid N_{F/K}(x)N_{L/K}(y) = 1\}.$$

Fix a solution (a, b) to (13). Then for $(a_v, b_v = \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(h_v))$, where (a_v, h_v) is a solution to (9), we have

$$t := (a_v a^{-1}, b_v b^{-1})_{v\in V_r^K} \in T(V_r^K) := \prod_{v\in V_r^K} T(K_v).$$

Since $\Sigma(v) = \Sigma(v)^{-1}$ and $\Theta(v) = \Theta(v)^{-1}$ are open in $(A^\tau \otimes_K K_v)^\times$ and $(L \otimes_K K_v)^\times$ respectively, the set $\Omega = \prod_{v\in V_r^K} \Omega(v)$, where

$$\Omega(v) = \{(x, y) \in T(K_v) \mid x \in \Sigma(v)g\varepsilon(a)^{-1},\ y \in \Theta(v)b^{-1}\},$$

is an open neighborhood of t in $T(V_r^K)$. However, T has the weak approximation property with respect to V_r^K (cf. [20], Proposition 7.8, or [30], §11.5). So, Ω contains an element $(a_0, b_0) \in T(K)$. Then

$$\mathrm{Nrd}_{A/L}(g) = N_{F/K}(a_0 a)N_{L/K}(b_0 b)$$

and $g\varepsilon(a_0a)^{-1} \in \Sigma(v)$ and $b_0b \in \Theta(v)$, for all $v \in V_r^K$. After replacing a with a_0a, and b with b_0b, we will assume that $a \in F^\times$ and $b \in L^\times$ satisfy (13), (14) and (15). Then it follows from Eichler's Norm Theorem (cf. [20], Theorem 1.13 and §6.7) that there exists $h_0 \in A^\times$ such that $\mathrm{Nrd}_{A/L}(h_0) = b$. To complete the argument, we need the following.

Lemma 4.3. *Let $\mathscr{S}$ be the variety of τ-symmetric elements in $M = \mathrm{SL}_{1,A}$. If $x \in \mathscr{S}(K)$ is such that $x \in \Sigma(v) = \{\tau(h_v)h_v \mid h_v \in (A \otimes_K K_v)^\times\}$ for all $v \in V_r^K$, then $x = \tau(h)h$ for some $h \in M(K)$.*

Proof. We can write $x = \tau(y)y$ for some $y \in M(K_{\mathrm{sep}})$, where K_{sep} is a separable closure of K. Then $\xi_\gamma := y\gamma(y)^{-1}$ for $\gamma \in \mathrm{Gal}(K_{\mathrm{sep}}/K)$ defines a Galois 1-cocycle ξ with values in $G = \mathrm{SU}(A, \tau)$. It is enough to show that ξ defines the trivial element of $H^1(K, G)$. Indeed, then there exists $z \in G(K_{\mathrm{sep}})$ with the property

$$\xi_\gamma = y\gamma(y)^{-1} = z^{-1}\gamma(z) \quad \text{for all } \gamma \in \mathrm{Gal}(K_{\mathrm{sep}}/K).$$

It follows that $h := zy \in M(K)$, and obviously, $x = \tau(h)h$, as required. It is known that $H^1(K, G)$ is trivial if K is either a global function field [11] or a totally imaginary number field (cf. [20], §6.7), so our assertion follows immediately. To prove the assertion in the general case, we will use the Hasse principle for G, i.e., the fact that the map

$$H^1(K, G) \longrightarrow \prod_{v \in V_r^K} H^1(K_v, G)$$

is injective (cf. [20], Theorem 6.6). So, it is enough to show that the image of ξ in $H^1(K_v, G)$ is trivial, for all $v \in V_r^K$, which, by the argument above, is equivalent to the fact that $x = \tau(h_v)h_v$ for some $h_v \in M(K_v)$. But if $L \otimes_K K_v$ is not a field, then according to the observation made in a footnote above, any $x \in \mathscr{S}(K_v)$ can be written in the form $\tau(h_v)h_v$ for some $h_v \in M(K_v)$, and there is nothing to prove. Thus, it remains to consider the case where $L \otimes_K K_v$ is a field (which, of course, coincides with $\mathbb{C}$). Let $H = \mathrm{U}(A, \tau)$. The fact that $x \in \Sigma(v)$ implies that the image of ξ in $H^1(K_v, H)$ is trivial, and it is enough to show that in this situation, the map $H^1(K_v, G) \to H^1(K_v, H)$ has trivial kernel. But over $K_v = \mathbb{R}$, we have compatible isomorphisms

$$H \simeq \mathrm{U}(f) \quad \text{and} \quad G \simeq \mathrm{SU}(f)$$

for some nondegenerate hermitian form f. The exact sequence

$$1 \longrightarrow \mathrm{SU}(f) \longrightarrow \mathrm{U}(f) \xrightarrow{\det} T \longrightarrow 1,$$

where $T = \mathrm{R}^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathrm{GL}_1)$, gives rise to the following exact cohomological sequence

$$\mathrm{U}(f)(\mathbb{R}) \xrightarrow{\det} T(\mathbb{R}) \longrightarrow H^1(\mathbb{R}, \mathrm{SU}(f)) \longrightarrow H^1(\mathbb{R}, \mathrm{U}(f)).$$

Since the first map is obviously surjective, the third map has trivial kernel, as required. □

We will now complete the proof of Theorem 4.1. It follows from our construction that $x = \tau(h_0)^{-1}(g\varepsilon(a)^{-1})h_0^{-1}$ satisfies the assumptions of Lemma 4.3. So, it can be written in the form $\tau(h)h$ for some $h \in A^\times$, and therefore the same is true for $g\varepsilon(a)^{-1}$, yielding the required presentation (8) for g. □

Remarks 4.4. (1) In the notations of Lemma 4.3, for any $v \in V_f^K$, we have $H^1(K_v, G) = \{1\}$, so the argument therein yields the following fact: any $x \in \mathscr{S}(K_v)$ can be written in the form $\tau(h_v)h_v$ for some $h_v \in (A \otimes_K K_v)^\times$. We will use this observation in the example below.

(2) Using Theorem 4.1, it has been proved in [9] that if either K is totally complex, or the degree n of A is odd, there exists a cyclic Galois extension F of K such that $(F \otimes_K L, \mathrm{id}_F \otimes \tau)$ embeds in (A, τ).

(3) Some sufficient conditions for the existence of ι_v at a particular $v \in V^K$ are given in [21], Propositions A.3 and A.4. We will use these conditions in the proof of the following corollary.

Corollary 4.5. *Let (A_1, τ_1) and (A_2, τ_2) be two central simple algebras with involutions of the second kind over a global field L. Assume that*

$$\dim_L A_1 = \dim_L A_2 =: n^2 \quad \text{and} \quad \tau_1|L = \tau_2|L =: \tau.$$

Then there exists a field extension E/L of degree n with an involutive automorphism σ satisfying $\sigma(L) = L$ and $\sigma|L = \tau$, such that (E, σ) embeds into (A_i, τ_i) as an algebra with involution, for $i = 1, 2$.

Proof. Let $G_i = \mathrm{SU}(A_i, \tau_i)$, and let V_i be the finite set of all $v \in V^K$ such that G_i is not quasi-split over K_v (cf. [20], Theorem 6.7). Set $V = V_1 \cup V_2$, and let

$$S_1 = \{v \in V \mid L \otimes_K K_v \simeq K_v \times K_v\}, \quad S_2 = V \setminus S_1.$$

Pick an extension F/K of degree n which is linearly disjoint from L over K and satisfies the following conditions: $F \otimes_K K_v$ is a field for $v \in S_1$, and $F \otimes_K K_v \simeq K_v^n$ for $v \in S_2$. Set $E = FL = F \otimes_K L$ and let σ be the involution $\mathrm{id}_F \otimes \tau$ of E. Then it follows from Proposition A.3 (resp., Proposition A.4) in [21] that there exist embeddings $\iota_v^i : (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A_i \otimes_K K_v, \tau_i \otimes \mathrm{id}_{K_v})$ for $v \in S_1$ (resp., $v \in S_2$) and $i = 1, 2$. On the other hand, for $v \notin V$ and any $i = 1, 2$, the existence of ι_v^i follows from the fact that G_i is quasi-split over K (cf. [20], p. 340). Applying Theorem 4.1, we obtain the existence of embeddings $\iota^i : (E, \sigma) \hookrightarrow (A_i, \tau_i)$, for $i = 1, 2$. □

We will now construct an example showing that the assertion of Theorem 4.1 does not extend to embeddings of étale algebras.

Example 4.6. Let K be a number field. Pick $a \in K^\times \setminus K^{\times 2}$ so that $a > 0$ in all real completions of K, and set $L = K(\sqrt{a})$. Furthermore, pick two nonarchimedean places v_1, v_2 of K so that $a \in K_{v_i}^{\times 2}$ for $i = 1, 2$, and then pick $b \in K^\times$ with the property $b \notin K_{v_i}^{\times 2}$ for $i = 1, 2$. Set

$$F_1 = K(\sqrt{b}), \quad F_2 = K(\sqrt{ab}),$$

and let

$$F = F_1 L = F_2 L = K(\sqrt{a}, \sqrt{b}).$$

Let $\sigma_i \in \mathrm{Gal}(F/F_i)$ be the nontrivial automorphism for $i = 1, 2$; notice that both σ_1 and σ_2 act nontrivially on L. Consider the commutative étale L-algebra $E = F \times F$ with the involutive automorphism $\sigma = (\sigma_1, \sigma_2)$; clearly, $E^\sigma = F_1 \times F_2$.

Now, let D_0 be the quaternion division algebra over K with local invariant $1/2 \in \mathbb{Q}/\mathbb{Z}$ at v_1 and v_2, and 0 everywhere else. Then both F_1 and F_2 are isomorphic to, and henceforth will be identified with, maximal subfields of D_0. Fix a basis 1, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ of D_0 over K such that $\boldsymbol{i}^2 = \alpha$, $\boldsymbol{j}^2 = \beta$ for some $\alpha, \beta \in K^\times$, and $\boldsymbol{ij} = \boldsymbol{k} = -\boldsymbol{ji}$. Let δ be the standard involution of D_0, and $D_0^+ = K$ and $D_0^- = K\boldsymbol{i} + K\boldsymbol{j} + K\boldsymbol{k}$ be the spaces of δ-symmetric and δ-skew-symmetric elements, respectively. Let $D = D_0 \otimes_K L$ with the involution $\mu = \delta \otimes \tau_0$, where τ_0 is the nontrivial automorphism of L/K, and let D^μ be the set of μ-symmetric elements.

Lemma 4.7. $\mathrm{Nrd}_{D/L}(D^\mu) = K$.

Proof. We obviously have

$$D^\mu = D_0^+ + \sqrt{a} D_0^- = K + \sqrt{a}(K\boldsymbol{i} + K\boldsymbol{j} + K\boldsymbol{k}),$$

from which it follows that $\mathrm{Nrd}_{D/L}(D^\mu)$ is the set of elements represented by $q = x_0^2 - a\alpha x_1^2 - a\beta x_2^2 + a\alpha\beta x_3^2$ over K. To show that this set coincides with K, it is enough to show that the quadratic form q is indefinite at all real places of K. But by our construction, at those places the algebra D_0 splits, so the form $\alpha x_1^2 + \beta x_2^2 - \alpha\beta x_3^2$ is not negative definite. Since $a > 0$, the same is true for the form $a(\alpha x_1^2 + \beta x_2^2 - \alpha\beta x_3^2)$, and the required fact follows. □

Now, we observe that

$$F_1 \otimes_K L \simeq F_2 \otimes_K L \simeq F,$$

and

$$(F_1 \otimes_K L)^\mu = F_2 \quad \text{and} \quad (F_2 \otimes_K L)^\mu = F_1.$$

Thus, F has two embeddings $v_i\colon F \to D$, where $i = 1, 2$, such that $v_i(F)$ is μ-invariant and

$$v_1^{-1} \circ \mu \circ v_1 = \sigma_2 \quad \text{and} \quad v_2^{-1} \circ \mu \circ v_2 = \sigma_1.$$

Consider the embedding

$$\varepsilon\colon E = F \times F \to M_2(D) =: A, \quad \varepsilon(x_1, x_2) = \begin{pmatrix} v_1(x_2) & 0 \\ 0 & v_2(x_1) \end{pmatrix}.$$

It follows from our construction that if we endow A with the involution $\theta((x_{ij})) = (\mu(x_{ji}))$, then $\varepsilon\colon (E, \sigma) \to (A, \theta)$ is an embedding of algebras with involutions.

We now need to recall the following, which is actually Exercise 5.2 in [5].

Lemma 4.8. *Let $F = K(\sqrt{a}, \sqrt{b})$ be a bi-quadratic extension of a number field K. Assume that for all $v \in V^K$, the local degree $[F_v : K_v]$ is $\leqslant 2$. Let $K_i = K(\sqrt{a_i})$ for $i = 1, 2, 3$, be the three quadratic subfields of F, and set*

$$N_i = N_{K_i/K}(K_i^\times) \quad \text{and} \quad N_i^v = N_{K_{iv}/K_v}(K_{iv}^\times) \quad \text{for } v \in V^K.$$

Then $N_1^v N_2^v N_3^v = K_v^\times$ for all $v \in V^K$, but $N_1 N_2 N_3 \neq K^\times$.

Proof. For those who did not have a chance to work out all the details in Exercise 5.2 in [5], we briefly sketch the argument. First, by our assumption, for any $v \in V^K$, we have $K_{iv} = K_v$ for at least one i, and therefore $N_1^v N_2^v N_3^v = K_v^\times$. Next, set $S_i = \{v \in V^K \mid K_{iv} = K_v\}$. Then, letting $(*, *)_v$ denote the Hilbert symbol over K_v, we can define the following homomorphism $\varphi\colon K^\times \to \{\pm 1\}$,

$$\begin{aligned} \varphi(x) &= \prod_{v \in S_1} (a_2, x)_v \overset{1)}{=} \prod_{v \in S_1} (a_3, x)_v \overset{2)}{=} \prod_{v \in S_2} (a_3, x)_v \\ &= \prod_{v \in S_2} (a_1, x)_v = \prod_{v \in S_3} (a_1, x)_v = \prod_{v \in S_3} (a_2, x)_v. \end{aligned}$$

We notice that equality 1) follows from the fact that for $v \in S_1$ we have $a_2 a_3^{-1} \in K_v^{\times 2}$. To prove equality 2), we observe that by our assumption $V^K = S_1 \cup S_2 \cup S_3$, so the product formula for the Hilbert symbol combined with the facts that $S_1 \cap S_2 \subset S_3$ and $a_3 \in K_v^{\times 2}$ for $v \in S_3$, yields

$$1 = \prod_{v \in V^K} (a_3, x)_v = \prod_{v \in S_1 \cup S_2} (a_3, x)_v = \prod_{v \in S_1} (a_3, x)_v \cdot \prod_{v \in S_2} (a_3, x)_v,$$

as required. All other equalities are established similarly. It follows from the appropriate description of φ that $\varphi(N_i) = 1$ for all $i = 1, 2, 3$. Thus, $\varphi(N_1 N_2 N_3) = 1$.

On the other hand, it follows from Chebotarev's Density Theorem that one can pick $u_1 \in S_1$ and $u_2 \notin S_1$ so that $a_2 \notin K_{u_j}^{\times 2}$ for $j = 1, 2$. Using Exercise 2.16 in [5][3], we can find $x \in K^\times$ satisfying

$$(a_2, x)_{u_1} = (a_2, x)_{u_2} = -1 \quad \text{and} \quad (a_2, x)_u = 1 \text{ for all } u \in V^K \setminus \{u_1, u_2\}.$$

Then $\varphi(x) = -1$, implying that $N_1 N_2 N_3 \neq K^\times$. □

We will assume henceforth that $a, b \in K^\times$ are chosen so that $F = K(\sqrt{a}, \sqrt{b})$ satisfies our previous assumptions and those of Lemma 4.8, i.e., the local degree $[F_v : K_v]$ is $\leqslant 2$ for all $v \in V^K$. (Explicit example: $K = \mathbb{Q}$, $a = 13$, $b = 17$; then one can take for v_1, v_2 the p-adic places of $\mathbb{Q}$ corresponding to the primes $p = 3$ and 23.) According to Lemma 4.8, one can choose $s \in K^\times$ so that

$$s \notin N_{K(\sqrt{a})/K}(K(\sqrt{a})^\times) N_{K(\sqrt{b})/K}(K(\sqrt{b})^\times) N_{K(\sqrt{ab})/K}(K(\sqrt{ab})^\times) \tag{16}$$

It follows from Lemma 4.7 that there exists $g \in A^\theta$ such that $\mathrm{Nrd}_{A/L}(g) = s$ (in fact, we can choose such a g of the form $\mathrm{diag}(t, 1)$ where $t \in D^\mu$). Consider the involution $\tau = \mathrm{Int}\, g \circ \theta$. We claim that the equation

$$g\varepsilon(x) = h\tau(h) \quad \text{for } x \in (E^\sigma)^\times,\ h \in A^\times, \tag{17}$$

is solvable everywhere locally, but not globally. Then one can embed $(E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v})$ into $(A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$ for all $v \in V^K$, but one cannot embed (E, σ) into (A, τ).

First, suppose (17) holds for some $x \in (E^\sigma)^\times$ and $h \in A^\times$. Since $E^\sigma = K(\sqrt{b}) \times K(\sqrt{ab})$, taking reduced norms, we obtain

$$\begin{aligned} s &= \mathrm{Nrd}_{A/L}(g) \\ &\in N_{K(\sqrt{a})/K}(K(\sqrt{a})^\times) N_{K(\sqrt{b})/K}(K(\sqrt{b})^\times) N_{K(\sqrt{ab})/K}(K(\sqrt{ab})^\times), \end{aligned}$$

which contradicts (16).

Now, fix $v \in V^K$. If $v \in V_r^K$, then by our construction $L \otimes_K K_v$ is not a field. Then every τ-symmetric element in $(A \otimes_K K_v)^\times$ can be written in the form $\tau(h_v)h_v$ for some $h_v \in (A \otimes_K K_v)^\times$, and there is nothing to prove. So, assume now that $v \in V_f^K$. Since v splits in at least one of the extensions $K(\sqrt{a})$, $K(\sqrt{b})$ and $K(\sqrt{ab})$, and $E^\sigma = K(\sqrt{b}) \times K(\sqrt{ab})$, we see that there exits $s_v \in (E^\sigma \otimes_K K_v)^\times$ and $t_v \in (L \otimes_K K_v)^\times$ such that

$$\mathrm{Nrd}_{A/L}(g) = N_{E^\sigma \otimes_K K_v / K_v}(s_v) N_{L \otimes_K K_v / K_v}(t_v).$$

[3]For the reader's convenience, we recall the statement of this result, which will be used again in §6: Let $a \in K^\times$, and suppose that for each $v \in V^K$, we are given $\varepsilon_v \in \{\pm 1\}$ so that the following three conditions are satisfied: (i) $\varepsilon_v = 1$ for all but finitely many v; (ii) $\prod_v \varepsilon_v = 1$; (iii) for each $v \in V^K$, there exists $x_v \in K_v^\times$ such that $(a, x_v)_v = \varepsilon_v$. Then there exists $x \in K^\times$ such that $(a, x)_v = \varepsilon_v$ for all v.

Furthermore, the homomorphism of reduced norm

$$\mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}\colon (A\otimes_K K_v)^\times \to (L\otimes_K K_v)^\times$$

is surjective, so there exists $z_v \in A\otimes_K K_v$ such that $\mathrm{Nrd}(z_v) = t_v$. Then

$$x = \tau(z_v)^{-1} g\varepsilon(s_v)^{-1} z_v^{-1}$$

is a τ-symmetric element in $A\otimes_K K_v$ of reduced norm one. So, using Remark 4.4 (1), we conclude that x can be written in the form $\tau(h_v)h_v$ with $h_v \in (A\otimes_K K_v)^\times$, and then the same is true for $g\varepsilon(a_v)^{-1}$, yielding a local solution to (17) at v.

Remark 4.9. It should be pointed out that the proof of the local–global principle for embeddings of fields with involution in a central simple algebra with an involution of the second kind (Theorem 4.1) depends in a very essential way on the multinorm principle (i.e., (11)). Proposition 4.2 describes one situation in which this principle holds; some other sufficient conditions are given in Proposition 6.11 of [20]. In fact, we are not aware of any examples where the multinorm principle (for two fields) fails, and it is probably safe to conjecture that it always holds if one of the fields satisfies the usual Hasse norm principle and the extensions are linearly disjoint over K. On the other hand, Lemma 4.8 demonstrates that the multinorm principle may fail for three fields, even when all the fields are quadratic extensions. It would be interesting to complete the investigation of the multinorm principle, and in particular, provide an explicit computation of the obstruction, at least in the case where all fields are Galois extensions.

After a preliminary version of this paper was circulated, J-L. Colliot-Thélène informed us about an unpublished joint work of his with J-J. Sansuc in which they gave two proofs of a multinorm principle for a pair of extensions, one of which is cyclic.

In the remainder of this paper, we will work exclusively with simple algebras A endowed with an involution τ of the first kind. The center of A, which is fixed pointwise under τ, will be denoted K (instead of L) and will be assumed to be a global field of characteristic $\neq 2$. E will be a commutative étale algebra of dimension $n = \sqrt{\dim A}$ equipped with an involution σ.

5. Algebras with a symplectic involution

In this section, A will denote a central simple K-algebra, of dimension n^2, with a *symplectic* involution τ (then, of course, n is necessarily even). Our goal is to prove the local–global principle for embedding of an n-dimensional commutative étale K-algebra E given with an involutive K-automorphism σ (Corollary 5.3). In fact, in

this case one has the following more convenient criterion for the existence of an embedding.

Theorem 5.1. *With notations as above, assume that there exists an embedding* $\varepsilon\colon E \hookrightarrow A$ *as algebras without involutions, and that for each* ***real*** $v \in V^K$ *there exists a* K_v*-embedding*

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$$

of algebras with involutions. Then there exists a K*-embedding*

$$\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$$

of algebras with involutions.

The proof relies on the following lemma which is analogous to Lemma 4.3. We will denote the involution $\tau \otimes \mathrm{id}_{K_v}$ of $A \otimes_K K_v$ simply by τ in the following lemma and in the proof of Theorem 5.1.

Lemma 5.2. *Let* $x \in A^\times$ *be a* τ*-symmetric element. Assume that for every real* $v \in V^K$*, there is* $h_v \in (A \otimes_K K_v)^\times$ *such that* $x = \tau(h_v)h_v$*. Then there is* $h \in A^\times$ *such that* $x = \tau(h)h$*.*

Proof. Since τ is symplectic, $G = \mathrm{U}(A, \tau) = \mathrm{SU}(A, \tau)$ is a form of Sp_n, hence it is connected, absolutely almost simple and simply connected. This implies that the map

$$H^1(K, G) \xrightarrow{\rho} \prod_{v \in V_r^K} H^1(K_v, G)$$

is bijective (cf. [20], Theorem 6.6, for number fields, and [11] for global fields of positive characteristic). Let K_{sep} be a fixed separable closure of K. Pick $y \in (A \otimes_K K_{\mathrm{sep}})^\times$ so that $x = \tau(y)y$. Then the map

$$\gamma \mapsto \xi_\gamma := y\gamma(y)^{-1}, \quad \gamma \in \mathrm{Gal}(K_{\mathrm{sep}}/K),$$

is a Galois 1-cocycle with values in G. The fact that $x = \tau(h_v)h_v$, with $h_v \in (A \otimes_K K_v)^\times$, for each $v \in V_r^K$, means that the corresponding cohomology class lies in the kernel of ρ. It follows from the injectivity of ρ that the class is trivial, i.e., there exist $z \in G(K_{\mathrm{sep}})$ such that

$$\xi_\gamma = y\gamma(y)^{-1} = z^{-1}\gamma(z) \quad \text{for all } \gamma \in \mathrm{Gal}(K_{\mathrm{sep}}/K).$$

Then $h := zy \in A^\times$ and $x = \tau(h)h$, as required. □

Proof of Theorem 5.1. By Proposition 3.1, there exists an involution $\theta = \tau \circ \mathrm{Int}\, g$ on A, where $g \in A^\times$ is τ-symmetric, such that $\varepsilon\colon (E, \sigma) \hookrightarrow (A, \theta)$ is an embedding of algebras with involutions. Set $F = E^\sigma$. It follows from our assumptions and the equivalence (i) $\Longrightarrow$ (iii) in Theorem 3.2 that for each $v \in V_r^K$ there exists $b_v \in (F \otimes_K K_v)^\times$ such that

$$g\varepsilon_v(b_v) = \tau(h_v)h_v \quad \text{for some } h_v \in (A \otimes_K K_v)^\times.$$

Since the subgroup $(F \otimes_K K_v)^{\times 2} \subset (F \otimes_K K_v)^\times$ is open, by weak approximation, there exists $b \in F^\times$ such that

$$b = b_v t_v^2 \quad \text{with } t_v \in (F \otimes_K K_v)^\times$$

for each $v \in V_r^K$. Using the facts that t_v is σ_v-symmetric and that ε intertwines σ and θ, one finds that $g\varepsilon_v(t_v) = \tau(\varepsilon_v(t_v))g$, so

$$g\varepsilon(b) = \tau(\varepsilon_v(t_v))g\varepsilon_v(b_v)\varepsilon_v(t_v) = \tau(h_v\varepsilon_v(t_v))(h_v\varepsilon_v(t_v)).$$

Then by Lemma 5.2, we have $g\varepsilon(b) = \tau(h)h$ for some $h \in A^\times$, and invoking Theorem 3.2, we see that there is an embedding $\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$. □

Corollary 5.3. *Let A and E be as above and assume that for every $v \in V^K$ there is a K_v-embedding*

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$$

of algebras with involutions. Then there exists a K-embedding

$$\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$$

of algebras with involutions.

Indeed, in view of Proposition 2.7, the existence of ι_v for all $v \in V^K$ implies the existence of an embedding $\varepsilon\colon E \hookrightarrow A$ of algebras without involutions.

6. Algebras with orthogonal involutions: nonsplit case

Let A be a central simple algebra over a global field K of characteristic $\neq 2$, of dimension n^2, endowed with an involution τ of the first kind. Then, if $A \simeq M_m(D)$, with D a division algebra, then the class $[D] \in \mathrm{Br}(K)$ has exponent $\leqslant 2$, and therefore either $D = K$, or D is a quaternion central division algebra over K (cf. [19], §18.6). Thus, either $A = M_n(K)$, or $A = M_m(D)$, where D is a quaternion central division algebra over K, and $n = 2m$. We will refer to the first possibility as the *split case,* and

to the second as the *nonsplit case*. Henceforth, we will work only with *orthogonal* involutions, and in this section will focus on the nonsplit case. Thus, n will be even throughout the section, and $m = n/2$.

Now, let E be an n-dimensional commutative étale K-algebra given with a K-involution σ such that $F = E^\sigma$ is of dimension m (so (1) of §1 holds). Then, according to Proposition 2.2 we can identify E with $F[x]/(x^2 - d)$ for some $d \in F^\times$ so that σ is defined by $x \mapsto -x$. Theorem 6.1 below (which implies assertion (iii) of Theorem A of the introduction) is formulated for the case where F is a field extension of K and m is odd, however most of our considerations apply to a much more general situation (cf., in particular, Theorem 6.7). So, we will assume that $F = \prod_{j=1}^r F_j$, F_j a separable field extension of K, and in terms of this decomposition the element $d \in F^\times$ that defines E is written as $d = (d_1, \dots, d_r)$.

Theorem 6.1. *In the above notations, assume that F is a field extension of K of degree m, and m is odd. If for every $v \in V^K$ there exists a K_v-embedding*

$$\iota_v \colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \longrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}),$$

then there exists a K-embedding $\iota \colon (E, \sigma) \hookrightarrow (A, \tau)$.

6.2. Some facts about Clifford algebras. The main difficulty in the proof of Theorem 6.1 is that orthogonal involutions on $A = M_m(D)$, where D is a quaternion division algebra, correspond to (the similarity classes of) m-dimensional skew-hermitian forms (with respect to the standard involution on D), and the Hasse principle for (the equivalence of) such forms generally fails (cf. [13], §5.11 or [26], Chapter 10, §4). However, one can still use local–global considerations via an analysis of the associated Clifford algebras. We refer the reader to [14], Chapter II, §8B, for the notion and the structure of the Clifford algebra $C(A, \nu)$ associated to a simple algebra A with an involution ν.

We will crucially use a result of Lewis and Tignol [15] which asserts that *for two orthogonal involutions τ_1 and τ_2 of A as above, $(A, \tau_1) \simeq (A, \tau_2)$* (that is, τ_1 and τ_2 are conjugate in the terminology of [15]) *if and only if they have the same signature at every real place v of K (i.e., $(A \otimes_K K_v, \tau_1 \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v})$), and the Clifford algebras $C(A, \tau_1)$ and $C(A, \tau_2)$ are K-isomorphic.* (This result follows from Theorems A and B (see also Proposition 11) of [15] since for a global field K, the fundamental ideal $I(K)$ of the Witt ring $W(K)$ has the property that $I(K)^3$ (which is commonly denoted by $I^3(K)$ in the literature) is torsion-free, and it is $\{0\}$ if K does not embed in $\mathbb{R}$, cf., for example, [26], Theorem 14.6 in Chapter 2 together with Corollary 6.6 (vi) in Chapter 6.)

Another ingredient is the computation of classes in the Brauer group corresponding to certain Clifford algebras. To formulate these results, we need to make some preliminary remarks. If $\mathscr{E} = \prod_{j=1}^r \mathscr{E}_j$ is a commutative étale algebra over a field

$\mathscr{K}$, where the $\mathscr{E}_j$'s are finite separable field extensions of $\mathscr{K}$, then $\mathrm{Br}(\mathscr{E})$ is defined to be $\bigoplus_{j=1}^{r} \mathrm{Br}(\mathscr{E}_j)$. Furthermore, the restriction and corestriction maps are defined by

$$\mathrm{Res}_{\mathscr{E}/\mathscr{K}}\colon \mathrm{Br}(\mathscr{K}) \longrightarrow \mathrm{Br}(\mathscr{E}), \quad \alpha \longmapsto (\mathrm{Res}_{\mathscr{E}_1/\mathscr{K}}(\alpha), \ldots, \mathrm{Res}_{\mathscr{E}_r/\mathscr{K}}(\alpha)),$$

and

$$\mathrm{Cor}_{\mathscr{E}/\mathscr{K}}\colon \mathrm{Br}(\mathscr{E}) \longrightarrow \mathrm{Br}(\mathscr{K}), \quad (\alpha_1, \ldots, \alpha_r) \longmapsto \mathrm{Cor}_{\mathscr{E}_1/\mathscr{K}}(\alpha_1) + \cdots + \mathrm{Cor}_{\mathscr{E}_r/\mathscr{K}}(\alpha_r).$$

For $a = (a_1, \ldots, a_r), b = (b_1, \ldots, b_r) \in \mathscr{E}^{\times}$, we define

$$(a, b)_{\mathscr{E}} = ((a_1, b_1)_{\mathscr{E}_1}, \ldots, (a_r, b_r)_{\mathscr{E}_r}) \in \mathrm{Br}(\mathscr{E}),$$

where $(a_j, b_j)_{\mathscr{E}_j}$ is the class in $\mathrm{Br}(\mathscr{E}_j)$ of the quaternion $\mathscr{E}_j$-algebra defined by the pair a_j, b_j. As usual, if $\mathscr{E}$ is a local field, then we identify $\mathrm{Br}(\mathscr{E})_2$ with $\{\pm 1\}$, which makes $(a, b)_{\mathscr{E}}$ into the Hilbert symbol. (If $\mathscr{F}$ is a global field and $v \in V^{\mathscr{F}}$, then instead of $(\cdot, \cdot)_{\mathscr{F}_v}$ we will occasionally write $(\cdot, \cdot)_v$ if this is not likely to lead to confusion.) We note that if $\mathscr{K}$ is a local field and $\mathscr{F}$ is a quadratic field extension of $\mathscr{K}$, then $\mathrm{Res}_{\mathscr{F}/\mathscr{K}}(\mathrm{Br}(\mathscr{K})_2) = 0$ (cf. [5], Theorem 1.3 in Chapter VI).

Let now A be a central simple K-algebra with an orthogonal involution ν. Then the center $Z(C(A, \nu))$ of the corresponding Clifford algebra $C(A, \nu)$ is a quadratic étale K-algebra (cf. [14], Chapter II, Theorem 8.10), i.e., either a (separable) quadratic field extension of K, or $K \times K$. Moreover, $C(A, \nu)$ is a "simple" $Z(C(A, \nu))$-algebra, which in the case $Z(C(A, \nu)) = K \times K$ means that $C(A, \nu) = C_1 \times C_2$, where C_1 and C_2 are simple K-algebras. In all cases, one can consider the corresponding class $[C(A, \nu)] \in \mathrm{Br}(Z(C(A, \nu)))$. Now, fix a quadratic étale K-algebra Z, and suppose that there exists a K-isomorphism $\phi\colon Z \to Z(C(A, \nu))$. Then one can consider the simple Z-algebra $C(A, \nu, \phi)$ obtained from $C(A, \nu)$ by change of scalars using ϕ, and also the corresponding class $[C(A, \nu, \phi)] \in \mathrm{Br}(Z)$. Let $\bar{\phi}\colon Z \to Z(C(A, \nu))$ be the other K-isomorphism. Then

$$[C(A, \nu, \bar{\phi})] - [C(A, \nu, \phi)] = \mathrm{Res}_{Z/K}([A]) \tag{18}$$

(cf. [14], (9.9) and Proposition 1.10). It follows that *if ν_1 and ν_2 are two orthogonal involutions of A such that the centers of $C(A, \nu_i)$ are isomorphic to Z for $i = 1, 2$, then $C(A, \nu_1) \simeq C(A, \nu_2)$ if and only if for some (equivalently, any) isomorphisms $\phi_i\colon Z \to Z(C(A, \nu_i))$, one of the following two conditions holds:*

$$[C(A, \nu_1, \phi_1)] = [C(A, \nu_2, \phi_2)]$$

or

$$[C(A, \nu_1, \phi_1)] = [C(A, \nu_2, \phi_2)] + \mathrm{Res}_{Z/K}([A]).$$

6.3. After the above recollections, we are ready to embark on our investigation of the local–global principle in the situation described prior to Theorem 6.1. First, we observe that the existence of K_v-embeddings ι_v, for all $v \in V^K$, as in the statement of Theorem 6.1 implies that

- there exists a K-embedding $\varepsilon\colon E \hookrightarrow A$ which may or may not respect involutions.

Next, using Proposition 3.1, we can construct an involution θ of A for which (3) holds. For $a \in F^\times$, we let θ_a denote the involution $\theta \circ \operatorname{Int}\varepsilon(a)$ (then (3), with θ replaced by θ_a, holds). According to Theorem 3.2, the existence of ι_v is equivalent to the existence of $a_v \in (F \otimes_K K_v)^\times$ such that

$$(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}) \simeq (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}). \tag{19}$$

We now observe that the centers of the Clifford algebras $C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v})$ and $C(A \otimes_K K_v, \theta \otimes \mathrm{id}_{K_v})$ are isomorphic - this follows from the description of the center given in [14], Theorem 8.10, the definition of the discriminant of an orthogonal involution, *loc. cit.*, §7A, and the fact that

$$\mathrm{Nrd}_{A\otimes_K K_v/K_v}(a_v) = N_{E\otimes_K K_v/K_v}(a_v) = N_{F\otimes_K K_v/K_v}(a_v)^2 \in K_v^{\times 2},$$

from which we deduce that

$$Z(C(A,\theta)) \otimes_K K_v \simeq Z(C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v})) \simeq Z(C(A,\tau)) \otimes_K K_v$$

for all $v \in V^K$. Using Chebotarev's Density Theorem, we conclude that

- $Z(C(A,\theta)) \simeq Z(C(A,\tau))$.

We will denote this quadratic étale K-algebra by Z, and fix isomorphisms $\phi\colon Z \to Z(C(A,\theta))$ and $\psi\colon Z \to Z(C(A,\tau))$. A fundamental role in our analysis is played by the following computation of the class of the Clifford algebra $C(A,\theta_a)$ valid over an arbitrary field K of characteristic $\neq 2$ (cf. [4], Proposition 5.3):

$$[C(A,\theta_a,\phi_a)] = [C(A,\theta,\phi)] + \mathrm{Res}_{Z/K}\mathrm{Cor}_{F/K}((a,d)_F). \tag{20}$$

In our argument, we will not need the precise description of the isomorphism ϕ_a involved in this equation, the only property that will be used is that ϕ_a depends only on the coset $aN_{E/F}(E^\times) \in F^\times/N_{E/F}(E^\times)$, cf. [4], p. 99; in particular, $\phi_a = \phi$ if $a \in F^{\times 2}$.

According to Theorem 3.2, the existence of $\iota : (E,\sigma) \hookrightarrow (A,\tau)$ is equivalent to the existence of an $a \in F^\times$ such that $(A,\theta_a) \simeq (A,\tau)$, and we are now in a position to prove the following local–global principle for that.

Proposition 6.4. *Suppose that for each place $v \in V^K$ one can choose an element $a_v \in (F \otimes_K K_v)^\times$ so that the following conditions are satisfied:*

(a) $(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}) \simeq (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$ *for all* $v \in V_r^K$;

(b) *one of the following two families of equalities in* $\mathrm{Br}(Z \otimes_K K_v)$*:*

$$[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})] = [C(A, \tau, \psi) \otimes_K K_v]$$

and

$$[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})] = [C(A, \tau, \psi) \otimes_K K_v] + \mathrm{Res}_{Z \otimes_K K_v / K_v}[A \otimes_K K_v],$$

holds for all $v \in V^K$.

Assume also that the following condition holds:

(∗) *for any finite subset* V *of* V^K*, there exists* $v_0 \in V^K \setminus V$ *such that for* $j \leq r$*, if* $d_j \notin F_j^{\times 2}$*, then* $d_j \notin (F_j \otimes_K K_{v_0})^{\times 2}$*, and moreover,* $Z \otimes_K K_{v_0}$ *is a field if* Z *is a field.*

Then there exists an $a \in F^\times$ *such that* $(A, \theta_a) \simeq (A, \tau)$*. Furthermore, condition* (∗) *holds automatically if* F/K *is a field extension of odd degree.*

For the proof of this proposition, we need the following two lemmas about the Hilbert symbol. (In essence, these lemmas are well known, but we have not been able to locate suitable references for them.)

Lemma 6.5. *Let* $\mathscr{F}$ *be a global field of characteristic* $\neq 2$*, and* $t \in \mathscr{F}^\times$*. Suppose that for each* $v \in V^{\mathscr{F}}$ *we are given* $\alpha_v \in \{\pm 1\}$ *and* $s_v \in \mathscr{F}_v^\times$ *so that* $(s_v, t)_v = \alpha_v$ *for all* $v \in V^{\mathscr{F}}$*,* $\alpha_v = 1$ *for all but finitely many* $v \in V^{\mathscr{F}}$*, and* $\prod_{v \in V^{\mathscr{F}}} \alpha_v = 1$ *(here* $(\cdot,\cdot)_v$ *denotes the Hilbert symbol on* $\mathscr{F}_v$*). Then for any finite subset* $\mathcal{S}$ *of* $V^{\mathscr{F}}$*, there exists* $s \in \mathscr{F}^\times$ *such that* $(s, t)_v = \alpha_v$ *for all* $v \in V^{\mathscr{F}}$*, and* $s \in s_v \mathscr{F}_v^{\times 2}$ *for all* $v \in \mathcal{S}$*.*

Proof. The existence of $s_0 \in \mathscr{F}^\times$ satisfying $(s_0, t)_v = \alpha_v$ for all $v \in V^{\mathscr{F}}$ follows from the result described in the footnote in the proof of Lemma 4.8. So, we will only indicate how to modify s_0 so that the resulting s would also satisfy the additional condition $s \in s_v \mathscr{F}_v^{\times 2}$ for $v \in \mathcal{S}$. Let $\mathscr{E} = \mathscr{F}(\sqrt{t})$ and $\mathscr{E}_v = \mathscr{F}_v(\sqrt{t})$ for $v \in V^{\mathscr{F}}$, and consider the corresponding norm groups

$$N = N_{\mathscr{E}/\mathscr{F}}(\mathscr{E}^\times) \ , \ N_v = N_{\mathscr{E} \otimes_{\mathscr{F}} \mathscr{F}_v / \mathscr{F}_v}((\mathscr{E} \otimes_{\mathscr{F}} \mathscr{F}_v)^\times) = N_{\mathscr{E}_v/\mathscr{F}_v}(\mathscr{E}_v^\times).$$

It follows from the weak approximation property that N is dense in $\prod_{v \in \mathcal{S}} N_v$, and therefore,

$$\prod_{v \in \mathcal{S}} N_v = N \cdot \Big(\prod_{v \in \mathcal{S}} \mathscr{F}_v^{\times 2} \Big) \tag{21}$$

Since $(s_0,t)_v = (s_v,t)_v$ for all $v \in \mathcal{S}$, we see that $(s_0 s_v^{-1})_{v\in\mathcal{S}} \in \prod_{v\in\mathcal{S}} N_v$. So by (21), there exists $z \in N$ such that $s_0 s_v^{-1} z^{-1} \in \mathcal{F}_v^{\times 2}$ for all $v \in \mathcal{S}$. Then, for $s = s_0 z^{-1}$

$$(s,t)_v = (s_0,t)_v = \alpha_v \quad \text{for all } v \in V^{\mathcal{F}},$$

and $s \in s_v \mathcal{F}_v^{\times 2}$, as required. □

Lemma 6.6. *Let $\mathcal{F} = \prod_{j=1}^r \mathcal{F}_j$ be a commutative étale algebra over a global field $\mathcal{K}$, and $t = (t_1,\dots,t_r) \in \mathcal{F}^\times$. For $v \in V^{\mathcal{K}}$, let $\mathcal{F}_v = \mathcal{F} \otimes_{\mathcal{K}} \mathcal{K}_v$. Suppose we are given a finite subset $\mathcal{S} \subset V^{\mathcal{K}}$, and for each $v \in \mathcal{S}$, an element $s_v \in \mathcal{F}_v^\times$. Furthermore, let $v_0 \in V^{\mathcal{K}} \setminus \mathcal{S}$ be such that for each $j \leqslant r$ with $t_j \notin \mathcal{F}_j^{\times 2}$, we have $t_j \notin (\mathcal{F}_j \otimes_{\mathcal{K}} \mathcal{K}_{v_0})^{\times 2}$. Then there exists $s \in \mathcal{F}^\times$ such that $s s_v^{-1} \in \mathcal{F}_v^{\times 2}$ for all $v \in \mathcal{S}$, and $(s,t)_{\mathcal{F}_v} = 1$ for all $v \in V^{\mathcal{K}} \setminus (\mathcal{S} \cup \{v_0\})$.*

Proof. It is enough to consider the case where $\mathcal{F}$ is a field and $t \notin \mathcal{F}^{\times 2}$ (indeed, if $t \in \mathcal{F}^{\times 2}$, then everything boils down to proving the existence of an $s \in \mathcal{F}^\times$ such that $s \in s_v \mathcal{F}_v^{\times 2}$ for all $v \in \mathcal{S}$, which is obvious). We now define $\alpha_w \in \{\pm 1\}$ for all $w \in V^{\mathcal{F}}$ as follows. For $v \in V^{\mathcal{K}}$, we let $w^{(1)},\dots,w^{(\ell_v)}$ denote all the extensions of v to $\mathcal{F}$. Then we have

$$\mathcal{F}_v = \mathcal{F} \otimes_{\mathcal{K}} \mathcal{K}_v = \prod_{k=1}^{\ell_v} \mathcal{F}_{w^{(k)}}.$$

In particular, for $v \in \mathcal{S}$, in terms of this decomposition, we write

$$s_v = (s_{w^{(1)}},\dots,s_{w^{(\ell_v)}}),$$

and we then set $\alpha_{w^{(k)}} = (s_{w^{(k)}},t)_{\mathcal{F}_{w^{(k)}}}$ for $k \leqslant \ell_v$. Furthermore, if $w \in V^{\mathcal{F}}$ lies over $v \in V^{\mathcal{K}} \setminus (\mathcal{S} \cup \{v_0\})$, we set $\alpha_w = 1$. Finally, if $w_0^{(1)},\dots,w_0^{(\ell_0)}$ are the extensions of v_0, then by our assumption, there exists $k_0 \leqslant \ell_0$ such that $t \notin \mathcal{F}_{w_0^{(k_0)}}^{\times 2}$. We then set $\alpha_{w_0^{(k)}} = 1$ for $k \neq k_0$, and let $\alpha_{w_0^{(k_0)}} = \prod_{w\neq w_0^{(k_0)}} \alpha_w$ where the product is taken over all $w \in V^{\mathcal{F}} \setminus \{w_0^{(k_0)}\}$ (notice that the α_w's for all these places have already been defined). Then $\prod_{w\in V^{\mathcal{F}}} \alpha_w = 1$, and for each $w \in V^{\mathcal{F}}$, there exists $a_w \in \mathcal{F}_w^\times$ such that $(a_w,t)_{\mathcal{F}_w} = \alpha_w$: indeed, if $w|v$, where $v \in \mathcal{S}$, then one takes for a_w the w-component of s_v; for any $w \neq w_0^{(k_0)}$ lying over $v \in V^{\mathcal{K}} \setminus \mathcal{S}$ we can takes $a_w = 1$, and finally, such a_w exists for $w = w_0^{(k_0)}$ because $t \notin \mathcal{F}_w^{\times 2}$. Now, our claim follows from Lemma 6.5. □

Proof of Proposition 6.4. Let

$$S_1 = \{v \in V_f^K \mid A \otimes_K K_v \not\simeq M_n(K)\} \cup V_r^K,$$

$$S_2 = \{v \in V^K | \, [C(A, \theta, \phi) \otimes_K K_v] \neq [C(A, \tau, \psi) \otimes_K K_v] \text{ in } \mathrm{Br}(Z \otimes_K K_v)\},$$

and $S = S_1 \cup S_2$. Using $(*)$ for $V = S$, we can find $v_0 \in V^K \setminus S$ with the properties described therein, and then it follows from Lemma 6.6 that there exists an $a \in F^\times$ such that

$$aa_v^{-1} \in F_v^{\times 2} \text{ for all } v \in S \quad \text{and} \quad (a, d)_{F_v} = 1 \text{ for all } v \in V^K \setminus (S \cup \{v_0\}),$$

where $F_v = F \otimes_K K_v$. We claim that a is as required, i.e.,

$$(A, \theta_a) \simeq (A, \tau) \quad \text{as } K\text{-algebras with involution.} \tag{22}$$

According to the result of Lewis and Tignol mentioned above in 6.2, to establish (22), it is enough to show that θ_a and τ have the same signature at every real places of K, i.e.,

$$(A \otimes_K K_v, \theta_a \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}) \quad \text{for all } v \in V_r^K, \tag{23}$$

and

$$C(A, \theta_a) \simeq C(A, \tau) \quad \text{as } K\text{-algebras.} \tag{24}$$

We notice that (23) immediately follows from condition (a) in the statement of the proposition and the fact that $aa_v^{-1} \in (F \otimes_K K_v)^{\times 2}$ for all $v \in V_r^K$. To prove (24), we set $\psi_0 = \psi$ if the first family of equalities in condition (b) holds, and $\psi_0 = \overline{\psi}$, the other isomorphism between Z and $Z(C(A, \tau))$, if the second family of equalities in condition (b) hold. Then it follows from (18) that

$$[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})] = [C(A, \tau, \psi_0) \otimes_K K_v] \quad \text{for all } v \in V^K. \tag{25}$$

We now recall that by our construction, v_0 has the property that if Z/K is a quadratic field extension, then so is $Z \otimes_K K_{v_0}/K_{v_0}$, which implies that the map of the Brauer groups

$$\mathrm{Br}(Z) \longrightarrow \bigoplus_{v \neq v_0} \mathrm{Br}(Z \otimes_K K_v)$$

is injective. So, to prove that $[C(A, \theta_a, \phi_a)] = [C(A, \tau, \psi_0)]$ in $\mathrm{Br}(Z)$, which will immediately yield (24), it is enough to show that

$$[C(A, \theta_a, \phi_a) \otimes_K K_v] = [C(A, \tau, \psi_0) \otimes_K K_v] \quad \text{in } \mathrm{Br}(Z \otimes_K K_v), \tag{26}$$

for all $v \in V^K \setminus \{v_0\}$. If $v \in S$, then $aa_v^{-1} \in (F \otimes_K K_v)^{\times 2}$, so

$$[C(A, \theta_a, \phi_a) \otimes_K K_v] = [C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})],$$

and (26) follows from (25). Now, suppose $v \in V^K \setminus (S \cup \{v_0\})$. Since $v \notin S_2$, and by our construction $(a, d)_{F_v} = 1$, using (20), we obtain that

$$[C(A, \theta_a, \phi_a) \otimes_K K_v] = [C(A, \theta, \phi) \otimes_K K_v] = [C(A, \tau, \psi) \otimes_K K_v].$$

On the other hand, since $v \notin S_1$, according to (18), we have

$$[C(A, \tau, \psi) \otimes_K K_v] = [C(A, \tau, \psi_0) \otimes_K K_v],$$

and again (26) follows.

Finally, we will show that $(*)$ automatically holds if F/K is a field extension of odd degree. Indeed, if $d \in F^{\times 2}$ then all we need to prove is that there exists $v_0 \in V^K \setminus V$ such that $Z \otimes_K K_{v_0}$ is a field if Z is a field, which immediately follows from Chebotarev's Density Theorem. Thus, we may suppose that $d \notin F^{\times 2}$, so that $E = F(\sqrt{d})$ is a quadratic extension of F, and then we let $L = E$ if $Z = K \times K$, and let $L = EZ$ if Z/K is a quadratic field extension. Then L/F is a Galois extension with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In either case, there exists $\phi \in \mathrm{Gal}(L/F)$ that acts *nontrivially* on E, and also on Z if Z/K is a quadratic extension (notice that in this case $Z \not\subset F$ as F has odd degree over K). By Chebotarev's Density Theorem, there exist infinitely many $w_0 \in V_f^F$ such that L/F is unramified at w_0 and the corresponding Frobenius automorphism is ϕ. In particular, we can choose such a w_0 which lies over some $v_0 \in V^K \setminus V$, and then this v_0 is as required. □

We will derive Theorem 6.1 from the following result which applies also in the case where m is even.

Theorem 6.7. *Let $A = M_m(D)$, where D is a quaternion division algebra over a global field K of characteristic $\neq 2$, and τ be an orthogonal involution of A. Furthermore, let F be a commutative étale K-algebra of degree m, and $E = F[x]/(x^2 - d)$ for some $d \in F^\times$ with the involution $\sigma\colon x \mapsto -x$. Assume that for every $v \in V^K$ there exists a K_v-embedding*

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}).$$

Moreover, assume that condition $(*)$ of Proposition 6.4 holds along with the following condition:

(#) *for all $v \in V^K$ such that $A \otimes_K K_v \not\simeq M_n(K_v)$ and $Z \otimes_K K_v \simeq K_v \times K_v$, we have $d \notin (F \otimes_K K_v)^{\times 2}$.*

Then there exists a K-embedding $\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$. Furthermore, condition (#) holds automatically if m is odd.

Proof. We will keep the notations introduced earlier. By Theorem 3.2, the existence of ι_v is equivalent to the existence of $a_v \in (F \otimes_K K_v)^\times$ such that

$$(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}) \simeq (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}). \tag{27}$$

On the other hand, in view of Proposition 6.4, to prove the first assertion, it suffices to exhibit, for each $v \in V^K$, an element $c_v \in (F \otimes_K K_v)^\times$ for which the following two conditions hold:

$$(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{c_v}) \simeq (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}) \quad \text{for all } v \in V_r^K; \tag{28}$$

and

$$[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{c_v}, \phi_{c_v})] = [C(A, \tau, \psi) \otimes_K K_v] \quad \text{for all } v \in V^K. \tag{29}$$

We notice that (27) implies that there is an isomorphism of K_v-algebras

$$C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}) \simeq C(A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}),$$

so it follows from (9.9) and Proposition 1.10 of [14] (see 6.2 above) that either

$$[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})] = [C(A, \tau, \psi) \otimes_K K_v] \tag{30}$$

or

$$\begin{aligned}[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})] = [C(A, \tau, \psi) \otimes_K K_v] \\ + \mathrm{Res}_{Z \otimes_K K_v / K_v}[A \otimes_K K_v]\end{aligned} \tag{31}$$

holds. In particular, if $A \otimes_K K_v \simeq M_n(K_v)$, then (28) and (29) hold for $c_v = a_v$.

Assume now that $A \otimes_K K_v \not\simeq M_n(K_v)$. If such a v is real, then there is only one equivalence class of involutions (cf. [26], Theorem 3.7 in Chapter 10), and therefore (28) holds for any choice of c_v. Thus, in all cases, it suffices to find c_v satisfying only (29). If (30) holds, we can take $c_v = a_v$. So, suppose that (31) holds. We will look for c_v of the form $c_v = a_v b_v$ with $b_v \in (F \otimes_K K_v)^\times$. It follows from (20) that then

$$\begin{aligned}&[C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{c_v}, \phi_{c_v})] \\ &\quad = [C(A \otimes_K K_v, (\theta \otimes \mathrm{id}_{K_v})_{a_v}, \phi_{a_v})] \\ &\qquad + \mathrm{Res}_{Z \otimes_K K_v / K_v} \mathrm{Cor}_{F \otimes_K K_v / K_v}(b_v, d)_{F \otimes_K K_v}.\end{aligned}$$

Comparing this with (31), we see that it is enough to find $b_v \in (F \otimes_K K_v)^\times$ such that

$$\mathrm{Res}_{Z \otimes_K K_v / K_v} \mathrm{Cor}_{F \otimes_K K_v / K_v}(b_v, d)_{F \otimes_K K_v} = \mathrm{Res}_{Z \otimes_K K_v / K_v}[A \otimes_K K_v]. \tag{32}$$

If $Z \otimes_K K_v / K_v$ is a quadratic field extension, then $\mathrm{Res}_{Z \otimes_K K_v / K_v}(\mathrm{Br}(K_v)_2) = 0$. So, in this case (32) holds automatically for any b_v. Thus, it remains only to consider the case where $Z \otimes_K K_v \simeq K_v \times K_v$. Then (32) amounts to finding $b_v \in (F \otimes_K K_v)^\times$ such that

$$\mathrm{Cor}_{F \otimes_K K_v / K_v}(b_v, d)_{F \otimes_K K_v} = [A \otimes_K K_v], \tag{33}$$

which we will do making use of condition (#). First, we observe that since $[A \otimes_K K_v]$ is the only element of order two in $\mathrm{Br}(K_v)$, it is enough to find b_v for which $\mathrm{Cor}_{F\otimes_K K_v/K_v}(b_v, d)_{F\otimes_K K_v}$ is nontrivial. We have

$$F \otimes_K K_v = \prod_{j=1}^{\ell} F_{w_j}, \tag{34}$$

where $w_1, \dots, w_\ell$ are the extensions of v to F. If $d = (d_{w_1}, \dots, d_{w_\ell})$ in terms of this decomposition, then by (#) there exists $j_0 \in \{1, \dots, \ell\}$ such that $d_{w_{j_0}} \notin F_{w_{j_0}}^{\times 2}$. So, we can find $b_{w_{j_0}} \in F_{w_{j_0}}^{\times}$ such that $(b_{w_{j_0}}, d_{w_{j_0}})_{F_{w_{j_0}}}$ is nontrivial. We claim that $\mathrm{Cor}_{F_{w_{j_0}}/K_v}(b_{w_{j_0}}, d_{w_{j_0}})_{F_{w_{j_0}}}$ is also nontrivial. This is obvious for v real (because then $F_{w_{j_0}} = K_v = \mathbb{R}$), and follows from the next lemma for v nonarchimedean.

Lemma 6.8. *Let $\mathscr{L}/\mathscr{K}$ be a finite extension of nonarchimedean local fields. Then $\mathrm{Cor}_{\mathscr{L}/\mathscr{K}}\colon \mathrm{Br}(\mathscr{L}) \to \mathrm{Br}(\mathscr{K})$ is an isomorphism.*

Proof. Cf. [17], Corollary 7.1.4. □

We now see that the element $b_v = (1, \dots, b_{w_{j_0}}, \dots, 1)$ is as required, completing the proof of the first assertion of Theorem 6.7.

Finally, we will show that (#) holds automatically if m is odd. Let v be a place of K such that $A \otimes_K K_v \not\simeq M_n(K_v)$. In the decomposition (34), for some $j_0 \in \{1, \dots, \ell\}$, the degree $[F_{w_{j_0}} : K_v]$ is odd. We claim that then the corresponding component $d_{w_{j_0}} \notin F_{w_{j_0}}^{\times 2}$, and (#) will follow. Indeed, otherwise $E \otimes_K K_v$ would have the following structure:

$$\cdots \times F_{w_{j_0}} \times F_{w_{j_0}} \times \cdots,$$

which would prevent it from being a maximal commutative étale subalgebra of $A \otimes_K K_v$ as $(A \otimes_K K_v) \otimes_{K_v} F_{w_{j_0}}$ is a nontrivial element of $\mathrm{Br}(F_{w_{j_0}})$ (cf. Proposition 2.6). □

Corollary 6.9. *Let (A, τ) be as in Theorem 6.7, Z be the center of the Clifford algebra $C(A, \tau)$, and E/K be a field extension of degree $n = 2m$ with an automorphism σ of order two. Set $F = E^\sigma$, and write $E = F(\sqrt{d})$ with $d \in F^\times$. Assume that*

($\diamond$) if Z is a field, then so is $F \otimes_K Z$,

and that condition (#) of Theorem 6.7 holds. Then the existence of K_v-embeddings $\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$ for all $v \in V^K$ implies the existence of a K-embedding $(E, \sigma) \hookrightarrow (A, \tau)$.

Proof. We only need to show that ($\diamond$) implies condition ($*$) of Proposition 6.4. For this, we observe that the extension EZ/F admits an automorphism ϕ that restricts

nontrivially to both E and Z. Then the required fact is established by the argument used in last paragraph of the proof of Proposition 6.4. □

Proof of Theorem 6.1. If F/K is a field extension of odd degree, then conditions $(*)$ and (#) hold automatically. So, our assertion follows from Theorem 6.7. □

7. Orthogonal involutions: split case

In this section, we examine the local–global principle for embeddings in the case where $A = M_n(K)$ with an orthogonal involution τ. For n even, these considerations, in principle, can be built into the analysis given in §6 for the nonsplit case, however this would make the statements somewhat cumbersome. In any case, one would still need to consider the case of n odd. It turns out that the theory of quadratic forms provides a natural framework for treating both cases (i.e., n even and n odd) and in fact all we need in our analysis is the Hasse-Minkowski Theorem and the classification of quadratic forms over the completions K_v of a global field K of characteristic $\neq 2$. For the reader's convenience, we recall that two nondegenerate quadratic forms q_1 and q_2 of equal rank over K_v are equivalent if and only if (1) $v \in V_r^K$ and q_1 and q_2 have the same signature over $K_v = \mathbb{R}$; (2) $v \in V_f^K$ and q_1 and q_2 have the same determinant and the same Hasse invariant (if $q = a_1x_1^2 + \cdots + a_nx_n^2$, then the determinant and the Hasse invariant are given by $d_v(q) = a_1 \ldots a_n K_v^{\times 2}$ (in $K_v^\times/K_v^{\times 2}$) and $h_v(q) = \prod_{i<j}(a_i, a_j)_v$ respectively, where $(\cdot,\cdot)_v \in \{\pm 1\}$ is the Hilbert symbol over K_v), cf. [26], Chapter 6, §4. Even though the arguments in this section are considerably simpler than those in §6, they use similar ideas, and the same auxiliary statements. The fact that the local–global principle holds for the equivalence of quadratic forms (while it fails for the skew-hermitian forms over quaternion division algebras) is the reason why the split case is easier to analyze than the nonsplit case.

First, let us write τ in the form $\tau(x) = Q^{-1}x^tQ$ for some nondegenerate symmetric matrix Q (cf. [14], Proposition 2.7), and let $b(v, w) = v^tQw$ be the corresponding bilinear form on K^n (notice that b is determined, up to a scalar multiple, by the property $b(xv, w) = b(v, \tau(x)w)$ for $x \in A$ and all $v, w \in K^n$). Let q be the quadratic form associated with b.

Now, let E be a commutative étale K-algebra of dimension n, with an involutive K-automorphism σ. Set $F = E^\sigma$. Then for any $a \in F^\times$, the bilinear form $b_a(v, w) := \mathrm{Tr}_{E/K}(av\sigma(w))$ on E is symmetric and satisfies

$$b_a(xv, w) = b_a(v, \sigma(x)w) \quad \text{for all } v, w, x \in E.$$

Let q_a denote the corresponding quadratic form. The following proposition is valid over an arbitrary field of characteristic $\neq 2$. It is essentially Proposition 3.9 of [4]

formulated in our context; it follows from Theorem 3.2, however we give a simple direct proof.

Proposition 7.1. *An embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ as algebras with involution exists if and only if there is an $a \in F^\times$ such that (E, b_a) and (K^n, b) are isometric.*

Proof. First, we observe that for a symmetric bilinear form f on E

$$f(xv,w) = f(v,\sigma(x)w) \quad \text{for all } v,w,x \in E \tag{35}$$

if and only if there is an $a \in F$ for which $f = b_a$. Indeed, suppose (35) holds. Since E/K is étale, the trace form $(v,w) \mapsto \mathrm{Tr}_{E/K}(vw)$ is nondegenerate and therefore we can write $f(v,w) = \mathrm{Tr}_{E/K}(v\varphi(w))$ for some $\varphi \in \mathrm{End}_K(E)$. Then (35) implies that

$$\mathrm{Tr}_{E/K}(xv\varphi(w)) = \mathrm{Tr}_{E/K}(v\varphi(\sigma(x)w))$$

and, consequently, $x\varphi(w) = \varphi(\sigma(x)w)$, for all $w,x \in E$. It follows that for $\psi = \varphi \circ \sigma$ we have $\psi(xw) = x\psi(w)$. Let $\psi(1) = a \in E$. Then $\psi(x) = ax$, and hence, $\varphi(w) = a\sigma(w)$. Thus,

$$f(v,w) = \mathrm{Tr}_{E/K}(av\sigma(w)) = b_a(v,w).$$

Finally, the fact that f is symmetric implies that $\sigma(a) = a$. Conversely, for any $a \in F$, the form b_a is bilinear and symmetric, and satisfies (35).

Now, we identify E with K^n as a K-vector space in some way, and use the resulting identification of $\mathrm{End}(E)$ with $\mathrm{End}(K^n) = A$. Let $\lambda\colon E \to \mathrm{End}_K(E)$ be the left regular representation. Pick $\alpha \in \mathrm{Aut}_K(E)$ and consider the embedding $\iota\colon E \hookrightarrow \mathrm{End}_K(E)$ given by $\iota(x) = \alpha\lambda(x)\alpha^{-1}$. Set $\tilde{b}(v,w) = b(\alpha(v),\alpha(w))$. We claim that the following

$$\tilde{b}(xv,w) = \tilde{b}(v,\sigma(x)w) \tag{36}$$

is equivalent to the fact that $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ respects involutions. We have

$$\tilde{b}(xv,w) = b(\alpha(xv),\alpha(w)) = b(\iota(x)\alpha(v),\alpha(w)) = b(\alpha(v),\tau(\iota(x))\alpha(w)).$$

On the other hand,

$$\tilde{b}(v,\sigma(x)w) = b(\alpha(v),\alpha(\sigma(x)w)) = b(\alpha(v),\iota(\sigma(x))(\alpha(w))),$$

and our claim follows.

Suppose now that there exists an embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ of algebras with involution. Then ι is of the form $\iota(x) = \alpha\lambda(x)\alpha^{-1}$ for some $\alpha \in \mathrm{Aut}_K(E)$, and (36) holds for the corresponding form $\tilde{b}$. The first part of the proof shows that $\tilde{b} = b_a$ for some $a \in F^\times$ (notice that $\tilde{b}$ is nondegenerate), and then α defines an isometry between (E, b_a) and (K^n, b). Conversely, if α yields such an isometry, then $b = b_a$, and consequently (36) holds. This implies that $\iota\colon E \hookrightarrow A$ given by $\iota(x) = \alpha\lambda(x)\alpha^{-1}$ respects the involutions. □

We will now use Proposition 7.1 to reduce the problem of the existence of an embedding $(E,\sigma) \hookrightarrow (A,\tau)$ to the case of even n.

Proposition 7.2. *Let $A = M_n(K)$ with n odd, and let τ be an orthogonal involution of A. Furthermore, let (E,σ) be an n-dimensional étale K-algebra with an involution σ such that* (1) *of* §1 *holds. Then*

(i) *$E = E' \times K$ for some σ-invariant subalgebra E' of E for which* (1) *of* §1 *holds for $\sigma' = \sigma|E$.*

(ii) *Assume that for each $v \in V^K$, there exists an embedding*

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}).$$

Then there exists an involution $\tilde{\tau}$ on A given by $\tilde{\tau}(x) = \tilde{Q}^{-1}x^t\tilde{Q}$ with $\tilde{Q}$ symmetric of the form $\tilde{Q} = \mathrm{diag}\,(Q',\alpha)$, such that $(A,\tau) \simeq (A,\tilde{\tau})$ and for $A' = M_{n-1}(K)$ with the involution $\tau'(x) = (Q')^{-1}x^tQ'$, there exists an embedding

$$\iota'_v\colon (E' \otimes_K K_v, \sigma' \otimes \mathrm{id}_{K_v}) \hookrightarrow (A' \otimes_K K_v, \tau' \otimes \mathrm{id}_{K_v})$$

for all $v \in V^K$.

(iii) *With τ' as in* (ii), *the existence of an embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$ is equivalent to the existence of an embedding $\iota'\colon (E',\sigma') \hookrightarrow (A',\tau')$.*

Proof. (i) was actually established in the proof of Proposition 2.1 (2). Set $F' = (E')^{\sigma'}$. To prove (ii), given $a' \in (F')^\times$, we let $b'_{a'}$ denote the bilinear form on E' defined by $b'_{a'}(x',y') = \mathrm{Tr}_{E'/K}(a'x'\sigma'(y'))$. It is easy to see that the determinant d' of $b'_{a'}$ is independent of a' (cf. [4], Proposition 4.1), and we set $\alpha = d/d'$, where d is the determinant of b. We claim that α is represented by q over K. Indeed, by the Hasse-Minkowski Theorem, it is enough to show that α is represented by q over K_v for all $v \in V^K$. According to Proposition 7.1, it follows from the existence of ι_v that there is an $a_v = (a'_v,\alpha_v) \in (F \otimes_K K_v)^\times = (F' \otimes_K K_v)^\times \times K_v^\times$ such that $b_{a_v} = b'_{a'_v} \perp \langle\alpha_v\rangle$, where $\langle\alpha_v\rangle$ is the 1-dimensional form corresponding to α_v, is K_v-equivalent to b. As we observed above, the determinant of $b'_{a'_v}$ is d', so

$$\det b_{a_v} = \det b'_{a'_v} \cdot \alpha_v = d' \cdot \alpha_v = \det b = d \quad \text{in } K_v^\times/K_v^{\times 2},$$

which implies that $\alpha/\alpha_v \in K_v^{\times 2}$. So b, which is equivalent to $b_{a_v} = b'_{a'_v} \perp \langle\alpha_v\rangle$, is equivalent to $b'_{a'_v} \perp \langle\alpha\rangle$. Hence, α is a value assumed by q over K_v for all v, and therefore, also over K. This implies that Q is equivalent to a symmetric matrix $\tilde{Q}$ of the form $\tilde{Q} = \mathrm{diag}\,(Q',\alpha)$, and we will show that the corresponding involution $\tilde{\tau}$ is as required. Since $(A,\tau) \simeq (A,\tilde{\tau})$, we can actually assume that $Q = \tilde{Q}$, and we let b' denote the bilinear form corresponding to Q'.

As $Q = \operatorname{diag}(Q', \alpha)$, b is equivalent to $b' \perp \langle\alpha\rangle$. We have seen above that it is also equivalent to $b'_{a'_v} \perp \langle\alpha\rangle$. Now, it follows from the Witt Cancelation Theorem (cf. [26], Chapter I, §5) that $b'_{a'_v} \simeq b'$, and therefore by Proposition 7.1 there exists an embedding $\iota'_v\colon (E' \otimes_K K_v, \sigma' \otimes \mathrm{id}_{K_v}) \hookrightarrow (A' \otimes_K K_v, \tau' \otimes \mathrm{id}_{K_v})$.

Finally, to prove (iii), we observe that the existence of $\iota'\colon (E', \sigma') \hookrightarrow (A', \tau')$ obviously implies the existence of $\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$. Conversely, if ι exists, then by Proposition 7.1 there exists $a = (a', \beta) \in F^\times = (F')^\times \times K^\times$ such that $b_a = b'_{a'} \perp \langle\beta\rangle$ is equivalent to $b = b' \perp \langle\alpha\rangle$. Taking determinants, we obtain

$$\det b_a = d' \cdot \beta = \det b = d = d' \cdot \alpha \quad \text{in } K^\times/K^{\times 2},$$

so $\alpha/\beta \in K^{\times 2}$. It follows that $b'_{a'} \perp \langle\alpha\rangle$ is equivalent to $b = b' \perp \langle\alpha\rangle$, so by the Witt Cancelation Theorem $b'_{a'} \simeq b'$, implying the existence of ι'. □

Henceforth, we will assume that n is even and (E, σ) is an n-dimensional étale K-algebra with involution satisfying (1) of §1. Then, according to Proposition 2.2, we have $E \simeq F[x]/(x^2 - d)$ where $F = E^\sigma$ is an étale K-algebra of dimension $m = n/2$ and $d \in F^\times$. We write $F = \prod_{j=1}^r F_j$, where F_j is a separable extension of K, and suppose that in terms of this decomposition $d = (d_1, \dots, d_r)$. The following result contains assertion (ii) of Theorem A of the introduction as a particular case.

Theorem 7.3. *Assume that for every $v \in V^K$ there exists a K_v-embedding*

$$\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}).$$

If the following condition holds:

($\diamond$) *for any finite subset $V \subset V^K$, there exists $v_0 \in V^K \setminus V$ such that for $j \leqslant r$, if $d_j \notin F_j^{\times 2}$, then $d_j \notin (F_j \otimes_K K_{v_0})^{\times 2}$;*

then there exists an embedding $\iota\colon (E, \sigma) \hookrightarrow (A, \tau)$. Furthermore, ($\diamond$) automatically holds if F is a field.

Proof. We need to show that if for every $v \in V^K$, there exists an $a_v \in (F \otimes_K K_v)^\times$ such that q_{a_v} is equivalent to q over K_v, then there exists an $a \in F^\times$ such that q_a is equivalent to q over K. Let $\tilde{q} = q_a$ for $a = 1$. For any $v \in V^K$, we have the following equalities of determinants

$$d(\tilde{q}) = d(q_{a_v}) = d(q) \quad (\text{in } K_v^\times/K_v^{\times 2}).$$

It follows that $d(\tilde{q}) = d(q)$ in $K^\times/K^{\times 2}$, and therefore, $d(q_a) = d(q)$ for all $a \in F^\times$. So, our task is to find an $a \in F^\times$ such that

(1) q_a is equivalent to q over K_v for all $v \in V_r^K$,

(2) $h_v(q_a) = h_v(q)$ for all $v \in V^K$.

We will use the following formula (written in the additive notation) for the Hasse invariant ([4], Theorem 4.3):

$$h_v(q_a) = h_v(\tilde{q}) + \mathrm{Cor}_{F\otimes_K K_v/K_v}(a,d)_{F\otimes_K K_v} \quad \text{for all } v \in V^K. \tag{37}$$

Let V be the (finite) set of places of K containing all the archimedean ones and those nonarchimedean v for which $h_v(\tilde{q}) \neq h_v(q)$, and choose v_0 as in ($\diamond$) for this V. By Lemma 6.6, there exists $a \in F^\times$ such that

(i) $aa_v^{-1} \in (F \otimes_K K_v)^{\times 2}$ for all $v \in V$, and

(ii) $(a,d)_{F\otimes_K K_v} = 1$ for all $v \in V^K \setminus (V \cup \{v_0\})$.

Then (i) implies that $q_a \simeq q$ over K_v, and in particular, $h_v(q_a) = h(q)$, for all $v \in V$. On the other hand, it follows from (ii) and (37) that for $v \in V^K \setminus (V \cup \{v_0\})$ we have

$$h_v(q_a) = h_v(\tilde{q}) = h_v(q).$$

Thus, $h_v(q_a) = h_v(q)$ for all $v \neq v_0$. But the product formula for the Hilbert symbol implies that

$$\prod_v h_v(q_a) = \prod_v h_v(q) = 1,$$

whence $h_v(q_a) = h_v(q)$ holds also for $v = v_0$. So, a is as required.

Finally, if F is a field and $d \notin F^{\times 2}$, then letting L denote a finite Galois extension of K containing $F(\sqrt{d})$, we can choose $\phi \in \mathrm{Gal}(L/F)$ which acts nontrivially on $\sqrt{d}$. Then by Chebotarev's Density Theorem, we can find $v_0 \in V^K \setminus V$ such that the Frobenius automorphism of L/K at v_0 is ϕ, and this v_0 is as required. □

Corollary 7.4. *Let $(E,\sigma) = (E',\sigma') \times (K, \mathrm{id}_K)$ where E'/K is a field extension with a K-automorphism σ' of order two, $n = \dim_K E$. Let $A = M_n(K)$ with an orthogonal involution τ. Then the existence of embeddings $\iota_v\colon (E \otimes_K K_v, \sigma \otimes \mathrm{id}_{K_v}) \hookrightarrow (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v})$ for all $v \in V^K$ implies the existence of an embedding $\iota\colon (E,\sigma) \hookrightarrow (A,\tau)$.*

This follows from Theorem 7.3 and Proposition 7.2.

Example 7.5. We will now construct an example of an étale K-algebra E of dimension $n = 6$ with an involution σ satisfying (1) of §1, and an orthogonal involution τ of $A = M_6(K)$ such that the local–global principle for embeddings of (E,σ) into (A,τ) fails. (Notice that then Proposition 7.2 enables one to construct a similar counter-example also for $n = 7$.)

We begin with the following general observation. Let K be a number field, and let $a, b \in K^\times$ be chosen so that $F = K(\sqrt{a}, \sqrt{b})$ is a degree four extension of

K. Let V denote the subset of V^K consisting of all archimedean places, and those nonarchimedean places which ramify in F/K. Set $F_1 = K$, $F_2 = K(\sqrt{a})$, and $d_1 = a$, $d_2 = b$. Let $v \notin V$ be such that $d_1 \notin K_v^{\times 2} = (F_1 \otimes_K K_v)^{\times 2}$. Then $[K_v(\sqrt{a}) : K_v] = 2$. Since FK_v/K_v is unramified, hence cyclic, we conclude that $K_v(\sqrt{a}, \sqrt{b}) = K_v(\sqrt{a})$, i.e., $d_2 \in K_v(\sqrt{a})^{\times 2} = (F_2 \otimes_K K_v)^{\times 2}$. Thus, for every $v \notin V$, $d_j \in (F_j \otimes_K K_v)^{\times 2}$ for at least one $j \in \{1, 2\}$.

Let $K = \mathbb{Q}$, and p_1, p_2 be two distinct primes of the form $4k + 1$, with one of them of the form $8k + 1$, such that $\left(\frac{p_1}{p_2}\right) = 1$ (one can take, for example, $p_1 = 13$ and $p_2 = 17$). Set

$$F_1 = \mathbb{Q}, \quad F_2 = \mathbb{Q}(\sqrt{p_1}), \quad F = F_1 \times F_2, \quad d = (p_1, p_2)$$

and $E = F[x]/(x^2 - d)$ with the involution σ defined by $x \mapsto -x$. Let $\tilde{q}$ be the 6-dimensional quadratic form on E corresponding to the bilinear form $\mathrm{Tr}_{E/\mathbb{Q}}(x\sigma(y))$. Now, Let q be the quadratic form which is equivalent to $\tilde{q}$ over $\mathbb{Q}_v$ for all $v \neq v_{p_1}, v_{p_2}$ (including the unique real place), and which has the Hasse invariant $h_v(q) = h_v(\tilde{q}) + 1/2$ for $v = v_{p_1}, v_{p_2}$ (in the additive notation). It follows from [26], Theorem 6.10 in Chapter 6, or [27], Chapter IV, 3.3, that such a form exists, and we let τ denote the orthogonal involution on $A = M_6(K)$ corresponding to (the matrix of) q. We claim that for each $v \in V^{\mathbb{Q}}$ there exists $a_v \in (F \otimes_{\mathbb{Q}} \mathbb{Q}_v)^\times$ such that the quadratic form q_{a_v}, corresponding to the bilinear form $\mathrm{Tr}_{E/K}(a_v x\sigma(y))$, is equivalent to q over $\mathbb{Q}_v$, but there is no $a \in F^\times$ such that q_a is equivalent to q. (In view of Proposition 7.1, this will yield the existence of local embeddings ι_v for all $v \in V^{\mathbb{Q}}$, but the absence of a global embedding ι.)

For the local assertion, we observe that we only need to consider $v \in \{v_{p_1}, v_{p_2}\}$. For $v = v_{p_1}$, we pick $s \in \mathbb{Q}_{p_1}^\times$ such that $(s, p_1)_{p_1} = -1$, and then $a_{v_{p_1}} = (s, 1) \in \mathbb{Q}_{p_1}^\times \times \mathbb{Q}_{p_1}(\sqrt{p_1})^\times = (F \otimes_{\mathbb{Q}} \mathbb{Q}_{p_1})^\times$ is as required. Similarly, for $v = v_{p_2}$, we pick $t \in \mathbb{Q}_{p_2}^\times$ so that $(t, p_2)_{p_2} = -1$, and then $a_{v_{p_2}} = (1, t, 1) \in \mathbb{Q}_{p_2}^\times \times \mathbb{Q}_{p_2}^\times \times \mathbb{Q}_{p_2}^\times = (F \otimes_{\mathbb{Q}} \mathbb{Q}_{p_2})^\times$ is as required.

Now, suppose there exists $a = (a_1, a_2) \in F^\times = F_1^\times \times F_2^\times$ such that q_a is equivalent to q over $\mathbb{Q}$. Then

$$h_{v_{p_1}}(q_a) = h_{v_{p_1}}(\tilde{q}) + \mathrm{Cor}_{F \otimes \mathbb{Q}_{p_1}/\mathbb{Q}_{p_1}}(a, d)_{F \otimes_{\mathbb{Q}} \mathbb{Q}_{p_1}} = h_{v_{p_1}}(\tilde{q}) + 1/2,$$

so $\mathrm{Cor}_{F \otimes \mathbb{Q}_{p_1}/\mathbb{Q}_{p_1}}(a, d)_{F \otimes_{\mathbb{Q}} \mathbb{Q}_{p_1}} = 1/2$. Since $p_2 \in {\mathbb{Q}_{p_1}^\times}^2$, we necessarily have $(a_1, p_1)_{p_1} = -1$. So, by the product formula, there exists a $v \neq v_{p_1}$ such that $(a_1, p_1)_v = -1$. Since $p_1 \in {\mathbb{Q}_{p_2}^\times}^2, \mathbb{R}^{\times 2}$, we have $v \neq v_{p_2}, v_\infty$. But it is easy to see that $F = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ is unramified outside $V = \{v_{p_1}, v_{p_2}\}$, so according to the observation made earlier, since $p_1 \notin \mathbb{Q}_v^{\times 2}$, we necessarily have $p_2 \in (F_2 \otimes \mathbb{Q}_v)^{\times 2}$. Then $\mathrm{Cor}_{F \otimes_{\mathbb{Q}} \mathbb{Q}_v/\mathbb{Q}_v}(a, d)_v = 1/2$, which contradicts $h_v(q_a) = h_v(q) = h_v(\tilde{q})$.

8. Invariant maximal subfields distinguish locally isomorphic algebras, of degree a multiple of 4, with orthogonal involutions

Let A be a central simple algebra over a global field K, of dimension n^2, and let τ be an orthogonal involution of A. In this section, we will deal with the set $\mathscr{I} = \mathscr{I}(A, \tau)$ of all orthogonal involutions η of A such that

$$(A \otimes_K K_v, \eta \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v, \tau \otimes \mathrm{id}_{K_v}). \tag{38}$$

for all $v \in V^K$. To put this notion in a more traditional context, we recall that if $A = M_m(D)$, with D being a division algebra, then D itself admits an involution $^-$ (which may be trivial) and then any involution ν of A can be written in the form $\nu(x) = Q_\nu^{-1} x^* Q_\nu$, where $(x_{ij})^* = (\overline{x_{ji}})$ and $Q_\nu^* = \pm Q_\nu$. In this case, we let h_ν denote the corresponding m-dimensional (skew)-hermitian form. Then, according to Proposition 3.3, we have $(A, \eta) \simeq (A, \tau)$ if and only if the corresponding forms h_η and h_τ are *similar*, i.e., a scalar multiple of h_η is equivalent to h_τ. So, the elements of $\mathscr{I}$ correspond to the (classes of proportional) forms that are similar to h_τ at every place of K, and the investigation of $\mathscr{I}$ essentially boils down to the Hasse principle for similarity of forms of a specific type. The analysis of the latter was recently completed in [16].

For orthogonal involutions ν, we either have $A = M_n(K)$, with Q_ν symmetric, making h_ν a quadratic form (split case), or $A = M_m(D)$, with D a quaternion division algebra, $^-$ being the canonical involution of D, and Q_ν satisfying $Q_\nu^* = -Q_\nu$, in this case h_ν is a skew-hermitian form (nonsplit case). It is known (cf. the references in [16], or Proposition 8.7 below) that the Hasse principle does hold for similarity of quadratic forms, which implies that in the split case $\mathscr{I}$ consists of a single isomorphism class. On the other hand, in the nonsplit case, $\mathscr{I}$ often contains more than one isomorphism class (cf. [16]), and therefore in this section we will entirely focus on this case. In particular, unless stated otherwise, A will denote an algebra of the form $M_m(D)$, where D is a quaternion division algebra, so that $n = 2m$. (For the sake of completeness, we mention that the Hasse principle is known to hold for similarity of hermitian forms over quaternion division algebras with the standard involution, and also for similarity of hermitian forms over division algebras with an involution of the second kind, cf. [16] and the references therein, so the nonsplit case above is the *only* case where $\mathscr{I}$ may not reduce to a single isomorphism class.) Our goal is to show that when m is even, the isomorphism class of each $\eta \in \mathscr{I}$ is determined by the isomorphism classes of η-invariant maximal fields in A. To give a precise statement of this result, we need to make some preliminary remarks and introduce some notations. First, we observe that the isomorphism (38) leads to an isomorphism

$$C(A, \eta) \otimes_K K_v \simeq C(A, \tau) \otimes_K K_v$$

of the corresponding Clifford algebras for every $v \in V^K$. In particular,

$$Z(C(A,\eta)) \otimes_K K_v \simeq Z(C(A,\tau)) \otimes_K K_v \quad \text{for all } v \in V^K,$$

so by applying Chebotarev's Density Theorem we see that there exists a quadratic étale K-algebra Z such that the center $Z(C(A,\eta))$ is isomorphic to Z for every $\eta \in \mathscr{I}$. We let V denote the finite set of all $v \in V^K$ such that

$$A \otimes_K K_v \not\simeq M_n(K_v) \quad \text{and} \quad Z \otimes_K K_v \simeq K_v \times K_v.$$

The following theorem, together with Corollary 8.5, implies assertion (ii) of Theorem B (of the introduction). Assertion (i) of that theorem is contained in Proposition 9.4.

Theorem 8.1. *Assume that m is even.*

(i) *Given $\eta \in \mathscr{I}$, there is an n-dimensional η-invariant commutative étale subalgebra E_η of A such that $(E_\eta, \eta|E_\eta)$ is isomorphic as algebra with involution to $(F_\eta[x]/(x^2 - d), \theta)$, where $F_\eta = (E_\eta)^\eta$, $d \in F_\eta^\times$ is such that $d \in (F_\eta \otimes_K K_v)^{\times 2}$ for all $v \in V$, and θ is defined by $\theta(x) = -x$.*

(ii) *Let $\eta \in \mathscr{I}$ and let E_η be any commutative étale subalgebra of A with the properties described in* (i). *If $v \in \mathscr{I}$ and there exists an embedding $(E_\eta, \eta|E_\eta) \hookrightarrow (A, v)$, then $(A, v) \simeq (A, \eta)$.*

We begin by constructing the required subalgebras over the completions K_v for $v \in V$.

Lemma 8.2. *Let $v \in V$, and assume that m is even. Then for any $\eta \in \mathscr{I}$, the algebra $A_v = A \otimes_K K_v$ contains an n-dimensional commutative étale K_v-subalgebra E_v which is invariant under $\eta_v = \eta \otimes \mathrm{id}_{K_v}$ and for which there is an isomorphism of algebras with involution*

$$(E_v, \eta_v|E_v) \simeq (F_v[x]/(x^2 - 1), \theta_v),$$

where $F_v := E_v^{\eta_v}$, and θ_v is defined by $x \mapsto -x$.

Proof. We have $A_v = M_m(D_v)$, where $D_v = D \otimes_K K_v$ is a division algebra as $v \in V$. We will first construct certain K_v-algebras and their embeddings into $M_2(D_v)$. Pick a maximal field L_v in D_v, and let $g_v \in D_v^\times$ be an element such that Int g_v induces the nontrivial automorphism of L_v; notice that $\overline{g_v} = -g_v$ where $^-$ denotes the canonical involution of D_v. Consider the algebra $C_v = L_v[x]/(x^2-1)$ with the involution τ_v defined by $x \mapsto -x$. Then (C_v, τ_v) is isomorphic to $(L_v \times L_v, \varepsilon_v)$, where ε_v is the involution $(a,b) \mapsto (b,a)$. Let * be the (symplectic) involution of $M_2(D_v)$ given by $(a_{ij})^* = (\overline{a_{ji}})$. Then the matrix $Q = \left(\begin{smallmatrix} 0 & g_v \\ g_v & 0 \end{smallmatrix}\right)$ obviously satisfies

$Q^* = -Q$, so σ given by $\sigma(a) = Q^{-1}a^*Q$ is an orthogonal involution of $M_2(D_v)$. Now, it is easy to check that $(a, b) \mapsto \mathrm{diag}(a, b)$ defines an embedding

$$\epsilon_v \colon (C_v, \tau_v) \simeq (L_v \times L_v, \varepsilon_v) \hookrightarrow (M_2(D_v), \sigma)$$

of algebras with involution.

By our assumption, m is even, say $m = 2r$. Let S_v be the direct product of r copies of L_v, and let $R_v = S_v[x]/(x^2-1)$ with the involution θ_v defined by $x \mapsto -x$. Then, obviously,

$$(R_v, \theta_v) \simeq \prod_{i=1}^{r} (C_v, \tau_v) \quad \text{and} \quad R_v^{\theta_v} = S_v.$$

For $(a_1, \ldots, a_r) \in R_v$, where $a_i \in C_v$, we set

$$\iota_v(a_1, \ldots, a_r) = \mathrm{diag}\,(\epsilon_v(a_1), \ldots, \epsilon_v(a_r)) \in M_m(D_v).$$

Then ι_v yields an embedding of algebras with involution

$$(R_v, \theta_v) \hookrightarrow (M_m(D_v), \mu_v) \quad \text{with } \mu_v(a) = M^{-1}a^*M,$$

where, again, * is defined by $(a_{ij})^* = (\overline{a_{ji}})$, and $M = \mathrm{diag}(Q, \ldots, Q)$. It follows from the definitions that the discriminant of μ_v equals $\mathrm{discr}(\sigma) \in K_v^{\times 2}$ (cf. [14], Chapter II, §7). On the other hand, since $v \in V$, we have $Z \otimes K_v = K_v \times K_v$, which implies that $\mathrm{discr}(\eta_v) \in K_v^{\times 2}$ (cf. [14], Chapter II, Theorem 8.10). But then $(A_v, \mu_v) \simeq (A_v, \eta_v)$ (cf. [26], Chapter 10, Theorem 3.6 for the nonarchimedean case and Theorem 3.7 for the real case). Thus, there exists an embedding $(R_v, \theta_v) \hookrightarrow (A_v, \eta_v)$, the image of which furnishes a subalgebra E_v of A_v with the desired properties. □

Proof of Theorem 8.1 (i). For each $v \in V$, pick a commutative étale subalgebra E_v of $A_v := A \otimes_K K_v$ as in the preceding lemma. Using Proposition 2.4, we find an n-dimensional η-invariant commutative étale subalgebra E of A which satisfies (1) of §1 and for which

$$(E \otimes_K K_v, (\eta|E) \otimes \mathrm{id}_{K_v}) \simeq (E_v, \eta_v|E_v).$$

By Proposition 2.2, we have

$$(E, \eta|E) \simeq (F[x]/(x^2 - d), \theta)$$

where $F = E^\eta$, $d \in F^\times$ and θ is defined by $x \mapsto -x$. Then by our construction, for every $v \in V$ we have

$$(F \otimes_K K_v)[x]/(x^2 - d) \simeq (F \otimes_K K_v)[x]/(x^2 - 1),$$

implying that $d \in (F \otimes_K K_v)^{\times 2}$, as required. □

Proof of Theorem 8.1 (ii). The argument relies on characterizing the isomorphism classes in $\mathscr{I}$ as fibers of a certain map δ, which we will now construct. For each $\eta \in \mathscr{I}$ we fix an isomorphism $\phi_\eta \colon Z \to Z(C(A,\eta))$, and then let $C(A,\eta,\phi_\eta)$ denote $C(A,\eta)$ with the structure of Z-algebra defined using ϕ_η. Consider the following subgroup:

$$\mathcal{B} = \prod_{v\in V} \langle \operatorname{Res}_{Z\otimes_K K_v/K_v}([A\otimes_K K_v])\rangle \subset \prod_{v\in V} \operatorname{Br}(Z\otimes_K K_v).$$

Furthermore, let $\mathcal{B}_0$ be the subgroup of $\mathcal{B}$ generated by the element

$$(\operatorname{Res}_{Z\otimes_K K_v/K_v}([A\otimes_K K_v]))_{v\in V},$$

and let $\bar{\mathcal{B}} = \mathcal{B}/\mathcal{B}_0$. This group will be the target of the required map δ. To define it, we need to *fix* an element of $\mathscr{I}$; to keep our notations simple, we will pick the the involution τ used to define $\mathscr{I} = \mathscr{I}(A,\tau)$ as the fixed element, but in fact any other element of $\mathscr{I}$ can be utilized equally well. Given $\eta \in \mathscr{I}$, for any $v \in V^K$ there is an isomorphism as in (38). Then with an appropriate choice of an isomorphism $\psi \colon Z\otimes_K K_v \to Z(C(A\otimes_K K_v, \eta\otimes \mathrm{id}_{K_v}))$, we will obtain an isomorphism

$$C(A\otimes_K K_v, \eta\otimes\mathrm{id}_{K_v}, \psi) \simeq C(A\otimes_K K_v, \tau\otimes\mathrm{id}_{K_v}, \phi_\tau\otimes\mathrm{id}_{K_v})$$

of $(Z\otimes_K K_v)$-algebras. Using (18) of §6, we see that in $\operatorname{Br}(Z\otimes K_v)$ the following difference

$$\delta(\eta,\phi_\eta,v) := [C(A,\eta,\phi_\eta)\otimes_K K_v] - [C(A,\tau,\phi_\tau)\otimes_K K_v]$$

equals either 0 or $\operatorname{Res}_{Z\otimes_K K_v/K_v}([A\otimes_K K_v])$. In fact, $\delta(\eta,\phi_\eta,v) = 0$ for all $v \notin V$, which leads us to consider the element $(\delta(\eta,\phi_\eta,v))_{v\in V} \in \mathcal{B}$. Now, for a different isomorphism $\phi'_\eta \colon Z \to Z(C(A,\eta))$, again by (18) in §6, we have

$$[C(A,\eta,\phi'_\eta)] - [C(A,\eta,\phi_\eta)] = \operatorname{Res}_{Z/K}([A]).$$

This means that the coset

$$\delta(\eta) := (\delta(\eta,\phi_\eta,v))_{v\in V} + \mathcal{B}_0 \in \bar{\mathcal{B}}$$

depends only on η, not on the choice of ϕ_η, and therefore the map

$$\delta \colon \mathscr{I} \longrightarrow \bar{\mathcal{B}}, \quad \eta \longmapsto \delta(\eta),$$

is well-defined.

Lemma 8.3. *For $\eta, \nu \in \mathscr{I}$, the condition $\delta(\eta) = \delta(\nu)$ implies that $(A,\eta) \simeq (A,\nu)$.*

Proof. Indeed, $\delta(\eta) = \delta(v)$ means that after replacing ϕ_η with another isomorphism $\phi'_\eta\colon Z \to Z(C(A,\eta))$ if necessary, we can assume that

$$[C(A,\eta,\phi_\eta) \otimes_K K_v] = [C(A,v,\phi_v) \otimes_K K_v] \tag{39}$$

in $\mathrm{Br}(Z \otimes_K K_v)$ for all $v \in V$. At the same time, as we observed above, the fact that $\eta, v \in \mathscr{I}$ automatically implies (39) for $v \in V^K \setminus V$. Using the injectivity of $\mathrm{Br}(Z) \to \bigoplus_{v \in V^K} \mathrm{Br}(Z \otimes_K K_v)$, we conclude that

$$[C(A,\eta,\phi_\eta)] = [C(A,v,\phi_v)],$$

and in particular, $C(A,\eta) \simeq C(A,v)$ as K-algebras. Since in addition we have

$$(A \otimes_K K_v, \eta \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v, v \otimes_K K_v) \quad \text{for all } v \in V_r^K,$$

by the result of Lewis and Tignol [15] recalled in 6.2 we have $(A,\eta) \simeq (A,v)$. □

Let now $\eta \in \mathscr{I}$, and let E_η be a commutative étale subalgebra of A as in Theorem 8.1 (i). Furthermore, let $v \in \mathscr{I}$, and suppose that there is an embedding $\iota\colon (E_\eta, \eta|E_\eta) \hookrightarrow (A,v)$. By Lemma 8.3, to show that $(A,\eta) \simeq (A,v)$ it is enough to show that $\delta(\eta) = \delta(v)$. Observing that for the involution θ in Theorem 3.2 which extends $\eta|E_\eta$, one can take η itself, we see that the existence of ι implies that there is an $a \in F_\eta^\times$ such that $(A,\eta_a) \simeq (A,v)$, where $\eta_a = \eta \circ \mathrm{Int}\, a$. Then $\eta_a \in \mathscr{I}$ and $\delta(\eta_a) = \delta(v)$. So, to prove Theorem 8.1 (ii), it remains only to show that

$$\delta(\eta_a) = \delta(\eta). \tag{40}$$

But according to (20) in §6, for any $v \in V^K$, we have

$$\begin{aligned}[C(A \otimes_K K_v, \eta_a \otimes \mathrm{id}_{K_v}, (\phi_\eta)_a \otimes \mathrm{id}_{K_v})] \\ = [C(A \otimes_K K_v, \eta \otimes \mathrm{id}_{K_v}, \phi_\eta \otimes \mathrm{id}_{K_v})] \\ + \mathrm{Res}_{Z \otimes_K K_v / K_v} \mathrm{Cor}_{F_\eta \otimes_K K_v / K_v}(a,d)_{F_\eta \otimes_K K_v}.\end{aligned}$$

If now $v \in V$, then the assumption that $d \in (F \otimes_K K_v)^{\times 2}$ implies that

$$[C(A \otimes_K K_v, \eta_a \otimes \mathrm{id}_{K_v}, (\phi_\eta)_a \otimes \mathrm{id}_{K_v})] = [C(A \otimes_K K_v, \eta \otimes \mathrm{id}_{K_v}, \phi_\eta \otimes \mathrm{id}_{K_v})],$$

i.e.,

$$\delta(\eta_a, (\phi_\eta)_a, v) = \delta(\eta, \phi_\eta, v),$$

and (40) follows. □

Corollary 8.4. *Let $A = M_m(D)$, where D is a quaternion division algebra over K and m is even, and let τ be an orthogonal involution of A. Suppose we are given $\eta \in \mathscr{I} = \mathscr{I}(A,\tau)$, a finite set $\mathscr{S} \subset V^K \setminus V$, and for each $v \in \mathscr{S}$, an n-dimensional*

(with $n = 2m$) commutative étale subalgebra $E(v)$ of $A_v := A \otimes_K K_v$ invariant under $\eta_v = \eta \otimes \mathrm{id}_{K_v}$ such that $\dim_{K_v} E_v^{\eta_v} = m$. Then there exists an n-dimensional η-invariant commutative étale subalgebra E of A with the properties described in Theorem 8.1 (i) *(with "E_η" replaced by "E" and "F_η" by "F"), and such that for every $v \in \mathscr{S}$ we have*

$$E(v) = g_v^{-1}(E \otimes_K K_v)g_v \quad \text{for a } g_v \in G_\eta(K_v), \tag{41}$$

where $G_\eta = \mathrm{SU}(A, \eta)$.

Proof. Let E_η be a commutative étale subalgebra of A as in Theorem 8.1 (i), and for $v \in V$, set $E(v) = E_\eta \otimes_K K_v$. Applying Proposition 2.4 we can find an n-dimensional η-invariant commutative étale subalgebra E of A such that

$$E(v) = g_v^{-1}(E \otimes_K K_v)g_v \quad \text{with } g_v \in G_\eta(K_v) \text{ for all } v \in \mathscr{S} \cup V.$$

Then (41) holds automatically. On the other hand, writing E_η and E in the form

$$E_\eta = F_\eta[x]/(x^2 - d) \quad \text{and} \quad E = F[x]/(x^2 - d'),$$

where $F_\eta = (E_\eta)^\eta$, $F = E^\eta$, and $d \in F_\eta^\times$, $d' \in F^\times$ (cf. Proposition 2.2), we observe that for $v \in V$, the fact that the isomorphism

$$\phi_v \colon E \otimes_K K_v \longrightarrow E(v) = E_\eta \otimes_K K_v, \quad a \longmapsto g_v^{-1} a g_v,$$

commutes with η_v, implies that $\phi_v(F \otimes_K K_v) = F_\eta \otimes_K K_v$, and $\phi_v(d') \in d \cdot (F_\eta \otimes_K K_v)^{\times 2}$. Since by our construction, $d \in (F_\eta \otimes_K K_v)^{\times 2}$, we obtain that $d' \in (F \otimes_K K_v)^{\times 2}$, as required. □

Combining this corollary with the results of [22], we obtain the following stronger assertion, which we will need in §9.

Corollary 8.5. *Keep the notations of Corollary* 8.4. *Then there exists an n-dimensional η-invariant commutative étale subalgebra E of A which has the properties described in Theorem* 8.1 (i) *(with "E_η" replaced by "E" and "F_η" by "F"), satisfies* (41) *for all $v \in \mathscr{S}$, and for which the corresponding maximal K-torus T_η of $G_\eta = \mathrm{SU}(A, \eta)$ is generic over K ("generic" in the sense of* §2). *This algebra E is automatically a field extension of K.*

Proof. The group G_η is semisimple, and we let r denote the number of nontrivial conjugacy classes in the Weyl group of G_η. Using Chebotarev's Density Theorem, we choose a subset $S \subset V_f^K \setminus (\mathscr{S} \cup V)$ of cardinality r so that G_η splits over K_v for all $v \in S$. Then, according to Theorem 3 of [22] (cf. also Theorem 3.1 in [23]), one can pick a maximal K_v-torus $T(v)$ of G_η, for each $v \in S$, so that every maximal K-torus

which is conjugate to $T(v)$ by an element of $G_\eta(K_v)$, for all $v \in S$, is generic over K. By Proposition 2.3, $T(v)$ corresponds to an n-dimensional η_v-invariant commutative étale subalgebra $E(v)$ of A_v satisfying (1) of §1. Using Corollary 8.4, we can find an n-dimensional η-invariant commutative étale subalgebra E of A which possesses the properties described in Theorem 8.1 (i) (with "E_η" replaced by "E" and "F_η" by "F") and for which $E \otimes_K K_v$ is conjugate to $E(v)$ by an element of $G_\eta(K_v)$, for all $v \in S \cup \mathscr{S}$ (in particular, yielding (41) for all $v \in \mathscr{S}$). Let T_η be the maximal K-torus of G_η corresponding to E. Then T_η is conjugate to $T(v)$ by an element of $G(K_v)$, for all $v \in S$, hence is generic. The fact that E is a field extension of K now follows from Proposition 2.5. □

Remark 8.6. Assume that m is even, and let η and $\nu \in \mathscr{I}$. Then for any η-invariant étale subalgebra E of A and any $v \in V$, there is an embedding

$$(E \otimes_K K_v,\ (\eta|E) \otimes \mathrm{id}_{K_v}) \longrightarrow (A \otimes_K K_v, \eta \otimes \mathrm{id}_{K_v}) \simeq (A \otimes_K K_v,\ \nu \otimes \mathrm{id}_{K_v}).$$

Now, let E_η be a subalgebra having the properties described in Theorem 8.1 (i); notice that according to Corollary 8.5 we can even choose E_η to be a field extension of K. Then according to Theorem 8.1 (ii) there is an embedding $(E_\eta, \eta|E) \hookrightarrow (A, \nu)$ if and only if $(A, \eta) \simeq (A, \nu)$. Since $\mathscr{I}$ typically contains more than one isomorphism class (cf. [16] in conjunction with Proposition 3.3 of this paper), we see that the local–global principle for embeddings of fields with involution usually fails for even m.

We close this section with the Hasse principle for similarity of quadratic forms. As we already mentioned earlier, an important consequence of this result in our context is that the set $\mathscr{I}$ in the split case reduces to a single isomorphism class. This fact will be used in §9. The Hasse principle in question is known (cf. [18], [8]), but unfortunately it is not recorded in the standard books on quadratic forms. So, we decided to sketch the argument for the sake of completeness, especially since it uses nothing more than Lemma 6.6.

Proposition 8.7. *Let f and g be two nondegenerate quadratic forms of the same dimension n over a global field K of characteristic $\neq 2$. If for every $v \in V^K$ there exists $\lambda_v \in K_v^\times$ such that g is equivalent to $\lambda_v f$ over K_v, then there exists $\lambda \in K^\times$ such that g is equivalent to λf over K.*

Proof. We will use $d(\cdot)$ and $h_v(\cdot)$ to denote the determinant and the Hasse invariant over K_v, respectively (cf. §7). It is easy to check that

$$d(\lambda f) = \lambda^n d(f) \quad \text{and} \quad h_v(\lambda f) = (\lambda, \delta(f))_v \cdot h_v(f) \tag{42}$$

where $\delta(f) = (-1)^{n(n-1)/2} \cdot d(f)$.

Let now n be odd. Set $\lambda = d(g)/d(f)$. Then $d(g) \equiv d(\lambda f)$ in $K^\times/K^{\times 2}$. For $v \in V^K$, since g and $\lambda_v f$ are equivalent over K_v, by taking determinants we obtain $\lambda \equiv \lambda_v$ in $K_v^\times/K_v^{\times 2}$. So, being equivalent to $\lambda_v f$, the form g is equivalent to λf over K_v, for any $v \in V^K$. Applying the Hasse-Minkowski Theorem, we obtain that g is equivalent to λf.

Now, we consider the case of even n. Notice that for any $v \in V^K$ we have

$$d(g)/d(f) \equiv d(\lambda_v f)/d(f) \equiv 1 \quad \text{in } K_v^\times/K_v^{\times 2}.$$

So, $d(g) \equiv d(f)$ in $K^\times/K^{\times 2}$, and therefore, $d(g) \equiv d(\lambda f)$ for any $\lambda \in K^\times$. First, assume that $\delta(f) \in K^{\times 2}$. Then it follows from (42) that for any $v \in V^K$ we have

$$h_v(g) = h_v(\lambda_v f) = h_v(f),$$

consequently

$$h_v(g) = h_v(\lambda f)$$

for any $\lambda \in K^\times$. In particular, this means that g and λf are equivalent over K_v for any $\lambda \in K^\times$ and any $v \in V_f^K$. Now, choose $\lambda \in K^\times$ so that $\lambda\lambda_v^{-1} \in K_v^{\times 2}$ for all $v \in V_r^K$. Then g is equivalent to λf over K_v for all $v \in V^K$, hence over K.

Finally, we consider the case where $\delta(f) \notin K^{\times 2}$. Let S be a finite set of places of K containing all the archimedean ones and those nonarchimedean v for which $h_v(f) \neq h_v(g)$. By Chebotarev's Density Theorem, we can find $v_0 \in V^K \setminus S$ such that $\delta(f) \notin K_{v_0}^{\times\, 2}$. Then by Lemma 6.6 there exists $\lambda \in K^\times$ such that $\lambda\lambda_v^{-1} \in K_v^{\times 2}$ for all $v \in S$ and $(\lambda, \delta(f))_v = 1$ for all $v \in V^K \setminus (S \cup \{v_0\})$. Using (42), we see that $h_v(g) = h_v(\lambda f)$ for all $v \neq v_0$. Since

$$\prod_v h_v(g) = \prod_v h_v(\lambda f) = 1,$$

we infer that $h_{v_0}(g) = h_{v_0}(\lambda f)$ as well. Arguing as above, we conclude that g and λf are equivalent over K. □

9. Application to weakly commensurable arithmetic subgroups

In this section, we will show how our previous results (particularly, Theorem 8.1) can be used to complete the analysis of weakly commensurable arithmetic subgroups in the case that was left open in the original version of [23], viz. where the ambient algebraic groups are of type D_{2r}, with $r \geqslant 3$ (for obvious reasons, type D_4 requires a special treatment, we hope to study groups of this type later).

We first recall the notion of weak commensurability introduced in [23]. Let G_1 and G_2 be two connected semi-simple algebraic groups defined over a field F of

characteristic zero. Semi-simple elements $\gamma_i \in G_i(F)$, where $i = 1, 2$, are said to be *weakly commensurable* if there exist maximal F-tori T_i of G_i such that $\gamma_i \in T_i(F)$, and for some characters χ_i of T_i (defined over an algebraic closure $\bar{F}$ of F) we have

$$\chi_1(\gamma_1) = \chi_2(\gamma_2) \neq 1.$$

Furthermore, (Zariski-dense) subgroups Γ_i of $G_i(F)$ are *weakly commensurable* if given a semi-simple element $\gamma_1 \in \Gamma_1$ of infinite order, there is a semi-simple element $\gamma_2 \in \Gamma_2$ of infinite order which is weakly commensurable to γ_1, and conversely, given a semi-simple element $\gamma_2 \in \Gamma_2$ of infinite order, there is a semi-simple element $\gamma_1 \in \Gamma_1$ of infinite order weakly commensurable to γ_2. In the present paper, we will be concerned exclusively with the situation where *both* groups G_1 and G_2 are absolutely almost simple of the same type D_{2r} with $r \geq 3$. (We note that in general, for absolutely almost simple groups G_i, the existence of finitely generated weakly commensurable Zariski-dense subgroups Γ_i of $G_i(F)$, for $i = 1, 2$, implies that either G_1 and G_2 are of the same type, or one of them is of type B_n and the other of type C_n, cf. Theorem 1 in [23].) It is easy to show that weak commensurability of finitely generated Zariski-dense subgroups is preserved by the F-isogenies of ambient algebraic groups ([23], Lemma 2.4). So, by replacing the given groups G_i's with isogenous ones and enlarging the field F if necessary, we reduce our analysis of weakly commensurable subgroups to the situation where $G_1 = G_2 = G$, and moreover, G is a F-form of SO_n, hence F-isomorphic to $\mathrm{SU}(A, \tau)$ for some central simple n^2-dimensional F-algebra A with an orthogonal involution τ.

One of the central issues in [23] was to determine when weak commensurability of S-arithmetic subgroups implies their commensurability, which in turn led to some interesting results about length-commensurable and isospectral locally symmetric spaces (see [24] for a nontechnical exposition of these results). We used the following definition of S-arithmeticity. Let G be a connected absolutely almost simple algebraic group defined over a field F of characteristic zero, $\bar{G}$ be its adjoint group and $\pi : G \to \bar{G}$ be the natural isogeny. Two subgroups Γ', Γ'' of $G(F)$ are said to be *commensurable up to an F-automorphism of $\bar{G}$* if there exists an F-automorphism σ of $\bar{G}$ such that $\sigma(\pi(\Gamma'))$ and $\pi(\Gamma'')$ are commensurable in the usual sense. Now, suppose we are given a number field K, an embedding $K \hookrightarrow F$, and a connected semi-simple algebraic K-group $\mathscr{G}$ such that the F-group ${}_F\bar{\mathscr{G}}$ obtained from the adjoint group $\bar{\mathscr{G}}$ of $\mathscr{G}$ by extension of scalars $K \hookrightarrow F$, is F-isomorphic to $\bar{G}$ (in other words, $\bar{\mathscr{G}}$ is an F/K-form of $\bar{G}$). Then we have an embedding $\bar{\iota}$: $\bar{\mathscr{G}}(K) \hookrightarrow \bar{G}(F)$ which is well defined up to an F-automorphism of $\bar{G}$. Now, given a subset S of V^K containing V_∞^K, but not containing any nonarchimedean places where $\mathscr{G}$ is anisotropic, a subgroup Γ of $G(F)$ such that $\pi(\Gamma)$ is commensurable with $\bar{\iota}(\bar{\mathscr{G}}(\mathcal{O}_K(S)))$ (where $\mathcal{O}_K(S)$ is the ring of S-integers of K) up to an F-automorphism of $\bar{G}$ is called a $(\bar{\mathscr{G}}, K, S)$-*arithmetic subgroup*. We note that in the situation at hand, i.e., where G is a form of SO_n, with $n = 4r$ and $r \geq 3$, for every F/K-form $\bar{\mathscr{G}}$ of $\bar{G}$, there exists a unique

F/K-form $\mathscr{G}$ of G admitting a K-isogeny $\mathscr{G} \to \overline{\mathscr{G}}$ compatible with π. Furthermore, two F/K-forms $\overline{\mathscr{G}}_1$ and $\overline{\mathscr{G}}_2$ of $\overline{G}$ are K-isomorphic if and only if the corresponding F/K-forms $\mathscr{G}_1$ and $\mathscr{G}_2$ of G are K-isomorphic. Finally, a subgroup Γ of $G(F)$ is $(\overline{\mathscr{G}}, K, S)$-arithmetic if and only if it is commensurable up to an F-automorphism of G with $\iota(\mathscr{G}(\mathcal{O}_K(S)))$ where $\iota\colon \mathscr{G}(K) \hookrightarrow G(F)$ is the natural embedding lifting $\bar{\iota}$ (in view of this, $(\overline{\mathscr{G}}, K, S)$-arithmetic subgroups of $G(F)$ may be referred to as $(\mathscr{G}, K, S)$-arithmetic subgroups, as we will often do in this section).

We showed in [23], for a general absolutely almost simple algebraic F-group G, that if Γ_i is a Zariski-dense $(\overline{\mathscr{G}}_i, K_i, S_i)$-arithmetic subgroup of $G(F)$ for $i = 1, 2$, then the weak commensurability of Γ_1 and Γ_2 implies that $K_1 = K_2$ and $S_1 = S_2$ (Theorem 3 of [23]), and then their commensurability up to an F-automorphism of $\overline{G}$ is equivalent to the assertion that $\overline{\mathscr{G}}_1 \simeq \overline{\mathscr{G}}_2$ over K (Proposition 2.5 of [23]). Furthermore, we showed that the latter follows from weak commensurability of Γ_1 and Γ_2 if G is of type different from A_n, D_n, and E_6. On the other hand, we showed that groups of types A_n $(n > 1)$, D_n (n odd), and E_6 contain weakly commensurable, but not commensurable, S-arithmetic subgroups (cf. Examples 6.5, 6.6 and §9 in [23]). The only unresolved question in the original version of [23] involved the groups of type D_n, with n even. We are now able to show that, as far as weak commensurability is concerned, these groups behave like "good groups" if $n > 4$.

Theorem 9.1. *Let G be an absolutely almost simple algebraic group of type D_{2r}, with $r > 2$, defined over a field F of characteristic zero, and let Γ_i be a Zariski-dense $(\mathscr{G}_i, K, S)$-arithmetic subgroup of $G(F)$ for $i = 1, 2$. If Γ_1 and Γ_2 are weakly commensurable, then $\overline{\mathscr{G}}_1 \simeq \overline{\mathscr{G}}_2$ (hence $\mathscr{G}_1 \simeq \mathscr{G}_2$) over K, and consequently Γ_1 and Γ_2 are commensurable up to an F-automorphism of $\overline{G}$.*

The proof of the theorem relies on Theorem 8.1 and a connection, valid over arbitrary fields, between weak commensurability of elements and isomorphism of commutative étale subalgebras associated to the corresponding maximal tori, which we will now describe. As we explained earlier, we may (and we will) assume that $G = \mathrm{SU}(A, \tau)$ where A is a central simple F-algebra of dimension n^2 (if G is of type D_{2r}, then $n = 4r$, $r > 2$, but some of our considerations are valid for arbitrary $n \geqslant 3$, $n \neq 8$) and τ is orthogonal involution of A. Then any F/K-form $\mathscr{G}$ of G equals $\mathrm{SU}(\mathscr{A}, \tau_{\mathscr{A}})$ for a suitable central simple n^2-dimensional algebra $\mathscr{A}$ over K equipped with an orthogonal involution $\tau_{\mathscr{A}}$ such that $(\mathscr{A} \otimes_K F, \tau_{\mathscr{A}} \otimes \mathrm{id}_F) \simeq (A, \tau)$ (cf. Lemma 9.3 (1) below). So, as a preparation for the proof of Theorem 9.1, we first consider the following general situation. For $i = 1, 2$, let A_i be two central simple algebras over the same (infinite) field K, of dimension n^2, endowed with orthogonal involutions τ_i. Furthermore, let F/K be a field extension such that

$$(A_1 \otimes_K F, \tau_1 \otimes \mathrm{id}_F) \simeq (A_2 \otimes_K F, \tau_2 \otimes \mathrm{id}_F);$$

we will denote this common F-algebra with involution by (A, τ). Then $\mathscr{G}_i := \mathrm{SU}(A_i, \tau_i)$ is an F/K-form of $G := \mathrm{SU}(A, \tau)$ for $i = 1, 2$, and in the sequel, we will view the groups $\mathscr{G}_i(K)$ as subgroups of the group $G(F)$. We refer the reader to §2 for the definition of a *generic* maximal K-torus.

Proposition 9.2. *Assume that $n \geq 3$, $n \neq 4, 8$, and let L_i be the minimal Galois extension of K over which $\mathscr{G}_i$ becomes an inner form. Furthermore, let E_i be a τ_i-invariant maximal commutative étale subalgebra of A_i satisfying* (1) *of* §1, *and let $\mathscr{T}_i$ be the corresponding maximal K-torus of $\mathscr{G}_i$. Assume that*

(a) $L_1 = L_2$;

(b) *$\mathscr{T}_1$ is a generic maximal K-torus of $\mathscr{G}_1$.*

If there exists an element $\gamma_1 \in \mathscr{T}_1(K)$ of infinite order which is weakly commensurable to some $\gamma_2 \in \mathscr{T}_2(K)$, then $(E_1, \tau_1|E_1) \simeq (E_2, \tau_2|E_2)$ as algebras with involution.

Proof. We begin with the following lemma, which is valid for all $n \geq 3$ (and also for symplectic involutions).

Lemma 9.3. (1) *Let F/K be a field extension, and let $\varphi\colon \mathscr{G}_1 \to \mathscr{G}_2$ be an F-isomorphism of algebraic groups. Then φ extends uniquely to an isomorphism*

$$\tilde{\varphi}\colon (A_1 \otimes_K F, \tau_1 \otimes \mathrm{id}_F) \longrightarrow (A_2 \otimes_K F, \tau_2 \otimes \mathrm{id}_F)$$

of algebras with involution.

(2) *For $i = 1, 2$, let $\mathscr{T}_i$ be a maximal K-torus of $\mathscr{G}_i$, and let E_i be the corresponding maximal commutative étale K-subalgebra of A_i. If $\varphi\colon \mathscr{G}_1 \to \mathscr{G}_2$ is a $\bar{K}$-isomorphism of algebraic groups such that $\varphi(\mathscr{T}_1) = \mathscr{T}_2$, and the restriction $\varphi|\mathscr{T}_1$ is defined over K, then $(E_1, \tau_1|E_1) \simeq (E_2, \tau_2|E_2)$ as algebras with involution.*

Proof. (1) As the referee has pointed out, the first assertion follows from Theorem 26.15 of [14], but for the convenience of the reader we give the following direct proof. Since both involutions are orthogonal, there exists an isomorphism

$$\tilde{\psi}\colon (A_1 \otimes_K \bar{F}, \tau_1 \otimes \mathrm{id}_{\bar{F}}) \longrightarrow (A_2 \otimes_K \bar{F}, \tau_2 \otimes \mathrm{id}_{\bar{F}})$$

of algebras with involution. We let $\psi : \mathscr{G}_1 \to \mathscr{G}_2$ denote the induced isomorphism between the special unitary groups, and observe that $\alpha := \psi^{-1} \circ \varphi$ is an $\bar{F}$-automorphism of $\mathscr{G}_1$. But it is well known that any $\bar{F}$-automorphism of $\mathscr{G}_1 = \mathrm{SU}(A_1, \tau_1)$ is conjugation by a suitable $h \in \mathscr{H}_1(\bar{F})$ where $\mathscr{H}_1 := \mathrm{U}(A_1, \tau_1)$. (Indeed, over $\bar{F}$, we have $\mathscr{G}_1 \simeq \mathrm{SO}_n$ and $\mathscr{H}_1 \simeq \mathrm{O}_n$. If n is odd, then $\mathscr{G}_1$ is of type B_r, and every automorphism of $\mathscr{G}_1$ is inner. For n even, the group of outer automorphisms of $\mathscr{G}_1$ has order two, and conjugation by any element $h \in \mathscr{H}_1(\bar{F}) \setminus \mathscr{G}_1(\bar{F})$ does give an outer automorphism of $\mathscr{G}_1$. Thus, any $\bar{F}$-automorphism of $\mathscr{G}_1$ is conjugation by an element of $\mathscr{H}_1(\bar{F})$.)

So, we can pick $h \in \mathscr{H}_1(\bar{F})$ such that $\varphi = \psi \circ \mathrm{Int}\, h$. Then $\tilde{\varphi} := \tilde{\psi} \circ \mathrm{Int}\, h$ is an isomorphism $(A_1 \otimes_K \bar{F}, \tau_1 \otimes \mathrm{id}_{\bar{F}}) \to (A_2 \otimes_K \bar{F}, \tau_2 \otimes \mathrm{id}_{\bar{F}})$ of algebras with involution. It is easy to check that $\mathscr{G}_i(\bar{F})$ spans $A_i \otimes_K \bar{F}$ as a $\bar{F}$-vector space, so the Zariski-density of $\mathscr{G}_i(F)$ in $\mathscr{G}_i$ (cf. [1], 18.3) implies that $\mathscr{G}_i(F)$ spans $A \otimes_K F$ as a F-vector space. Since $\varphi(\mathscr{G}_1(F)) = \mathscr{G}_2(F)$, we see that $\tilde{\varphi}(A_1 \otimes_K F) = A_2 \otimes_K F$, as required.

(2) By (1), φ extends to an isomorphism $\tilde{\varphi}\colon (A_1 \otimes_K \bar{K}, \tau_1 \otimes \mathrm{id}_{\bar{K}}) \to (A_2 \otimes_K \bar{K}, \tau_2 \otimes \mathrm{id}_{\bar{K}})$ of algebras with involution. Since $\varphi(\mathscr{T}_1(K)) = \mathscr{T}_2(K)$ and E_i coincides with the K-subalgebra generated by $\mathscr{T}_i(K)$ (cf. the proof of Proposition 2.3), we obtain that $\tilde{\varphi}(E_1) = E_2$, and assertion (2) follows. □

To prove Proposition 9.2, we pick simply connected coverings $\tilde{\mathscr{G}}_i \xrightarrow{\pi_i} \mathscr{G}_i$ of $\mathscr{G}_i$ defined over K, and set $\tilde{\mathscr{T}}_i = \pi_i^{-1}(\mathscr{T}_i)$. In view of our assumptions (a) and (b), the fact that γ_1 and γ_2 are weakly commensurable implies the existence of a $\bar{K}$-isomorphism $\tilde{\varphi}\colon \tilde{\mathscr{G}}_1 \to \tilde{\mathscr{G}}_2$ such that $\tilde{\varphi}|\tilde{\mathscr{T}}_1$ is an isomorphism of $\tilde{\mathscr{T}}_1$ onto $\tilde{\mathscr{T}}_2$ defined over K (cf. Theorem 4.2 and Remark 4.4 in [23]). Since $n > 8$, we automatically have $\tilde{\varphi}(\ker \pi_1) = \ker \pi_2$, and therefore $\tilde{\varphi}$ descends to a $\bar{K}$-isomorphism $\varphi\colon \mathscr{G}_1 \to \mathscr{G}_2$ such that $\varphi|\mathscr{T}_1$ is defined over K. Then our assertion follows from Lemma 9.3 (2). □

The following proposition establishes assertion (i) of Theorem B. As we already noted in §8, assertion (ii) of that theorem is implied by Theorem 8.1 and Corollary 8.5.

Proposition 9.4. *For $i = 1, 2$, let A_i be a central simple algebra over a number field K, of dimension n^2, with $n \geqslant 3$, endowed with an orthogonal involution τ_i, and let $\mathscr{G}_i = \mathrm{SU}(A_i, \tau_i)$. Assume that* ***either***

(a) *(A_1, τ_1) and (A_2, τ_2) have the same isomorphism classes of n-dimensional commutative étale subalgebras invariant under the involutions and satisfying* (1) *(i.e., for any n-dimensional τ_1-invariant commutative étale subalgebra E_1 of A_1 satisfying* (1)*), there exists an embedding $(E_1, \tau_1|E_1) \hookrightarrow (A_2, \tau_2)$, and vice versa),*

or

(b) *$n \neq 4$, and for some finite $S \subset V^K$, for $i = 1, 2$, any $(\mathscr{G}_i, K, S)$-arithmetic subgroup Γ_i of $\mathscr{G}_i(K)$ is Zariski-dense in $\mathscr{G}_i$, and Γ_1 and Γ_2 are weakly commensurable.*

Then

(i) *$A_1 \simeq A_2$ (in other words, A_1 and A_2 involve the same division algebra in their description);*

(ii) *$(A_1 \otimes_K K_v, \tau_1 \otimes \mathrm{id}_{K_v}) \simeq (A_2 \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v})$ for all $v \in V^K$.*

If n is even, then the same conclusion holds if A_1 and A_2 just have the same isomorphism classes of maximal ***subfields*** *invariant under the involutions.*

Proof. We begin by establishing the following two key properties of the K-groups $\mathscr{G}_i = \mathrm{SU}(A_i, \tau_i)$:

(α) $\mathrm{rk}_{K_v} \mathscr{G}_1 = \mathrm{rk}_{K_v} \mathscr{G}_2$ for all $v \in V^K$;

(β) $L_1 = L_2$, where L_i is the minimal Galois extension of K over which $\mathscr{G}_i$ becomes an inner form.

These properties have been proven in [23], Theorems 6.2 and 6.3, if (b) holds, so we will prove them assuming that (a) holds. (In condition (b) we have assumed that $n \neq 4$ since if $n = 4$, the corresponding special unitary groups are semi-simple but not absolutely simple, which prevents us from using the results of [23].) To prove (α) we basically repeat the argument given in the proof of Theorem 6.2 in [23]. More precisely, by symmetry it is enough to show that

$$\mathrm{rk}_{K_v} \mathscr{G}_1 \leqslant \mathrm{rk}_{K_v} \mathscr{G}_2. \tag{43}$$

Let $\mathscr{T}_1(v)$ be a maximal K_v-torus of $\mathscr{G}_1$ that contains a maximal K_v-split torus, and let $E_1(v)$ be the corresponding commutative étale subalgebra of $A_1 \otimes_K K_v$. By Proposition 2.4, there exists a τ_1-invariant commutative étale subalgebra E_1 of A_1 satisfying (1) of §1 such that the corresponding K-torus $\mathscr{T}_1$ is conjugate to $\mathscr{T}_1(v)$ by an element of $\mathscr{G}_1(K_v)$; in particular, $\mathrm{rk}_{K_v} \mathscr{T}_1 = \mathrm{rk}_{K_v} \mathscr{T}_1(v)$. By our assumption, there exists an embedding $(E_1, \tau_1|E_1) \hookrightarrow (A_2, \tau_2)$, which implies that there is a K-embedding $\mathscr{T}_1 \hookrightarrow \mathscr{G}_2$, and (43) follows.

Next, we observe that the argument given in the proof of Theorem 6.3 in [23] shows that (β) is a consequence of (α). Indeed, there exists a finite subset S of V^K such that $\mathscr{G}_1$ and $\mathscr{G}_2$ are quasi-split over K_v for any $v \in V^K \setminus S$ (cf. [20], Theorem 6.7). Then (α) implies that a place $v \in V^K \setminus S$ splits in L_1 if and only if it splits in L_2, and then $L_1 = L_2$ by Chebotarev's Density Theorem.

(i) We will now use (α) and (β) to prove (i). For n odd, we have $A_1 \simeq M_n(K) \simeq A_2$, and there is nothing to prove. So, we assume that n is even and write $A_i = M_m(D_i)$ for some quaternion central simple K-algebra D_i, where $m = n/2$. To show that $D_1 \simeq D_2$ (which will prove our claim) it is enough to show that D_1 and D_2 are ramified at exactly the same places. By symmetry it suffices to show that for $v \in V^K$ if $D_{1v} := D_1 \otimes_K K_v$ is a division algebra, then $D_{2v} := D_2 \otimes_K K_v$ is also a division algebra. Assume the contrary. First, let us show that $\mathscr{G}_2$ is K_v-isotropic. This is obvious if $n > 4$ and $v \in V_f^K$. If $v \in V_r^K$, then our assumption that D_{1v} is a division algebra implies that $\mathscr{G}_1$ is K_v-isotropic (cf. [26], Chapter 10, Theorem 3.7). But then, by (α), $\mathscr{G}_2$ must also be K_v-isotropic. It remains to consider the case $n = 4$ and $v \in V_f^K$. Here we need to use (β) and the description of L_i in terms of discriminant ([14], Chapter 2, Theorem 8.10). The unique anisotropic quadratic form in four variables over K_v has determinant (which coincides with its discriminant) in $K_v^{\times 2}$, so if $\mathscr{G}_2$ happens to be K_v-anisotropic, then v splits in L_2. But then v must split in L_1, which means that the binary skew-hermitian form over D_{1v}

corresponding to τ_1 has determinant (discriminant) in $K_v^{\times 2}$. However, it is known that any such form is necessarily isotropic ([26], Chapter 10, Theorem 3.6). So, $\mathscr{G}_1$ is K_v-isotropic, contradicting (α).

Now, the assumption that $A_2 \otimes_K K_v = M_n(K_v)$ and $\mathscr{G}_2$ is isotropic means that $(A_2 \otimes_K K_v, \tau_2 \otimes \mathrm{id}_{K_v})$ is isomorphic to $(M_n(K_v), \sigma_2)$ where $\sigma_2(x) = Q_2^{-1} x^t Q_2$ with $Q_2 = \mathrm{diag}(R, T)$ and $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Notice that if ϵ is the nontrivial K_v-automorphism of $K_v \times K_v$, then the map $(a, b) \mapsto \mathrm{diag}(a, b)$ defines an embedding $(K_v \times K_v, \epsilon) \hookrightarrow (M_2(K_v), \rho)$ where $\rho(x) = R^{-1} x^t R$. Using Proposition 2.4 we now see that there exists a n-dimensional τ_2-invariant commutative étale subalgebra E_2 of A_2 satisfying (1) of §1 such that $(E_2 \otimes_K K_v, (\tau_2 | E_2) \otimes \mathrm{id}_{K_v})$ contains $(K_v \times K_v, \epsilon)$ as a direct factor. By our assumption, $(E_2, \tau_2 | E_2)$ can be embedded into (A_1, τ_1). But then $A_1 \otimes_K K_v$ contains an n-dimensional commutative étale subalgebra which has $K_v \times K_v$ as a direct factor which, by Proposition 2.6, contradicts the assumption that D_{1v} is a division algebra.

If n is even, we will let D denote the common quaternion central *simple* K-algebra involved in the description of A_1 and A_2 (D may be $M_2(K)$), and assume (as we may) in the rest of the proof that A_1 and A_2 coincide with $A = M_m(D)$.

(ii) In this paragraph, we treat the case where n is odd. Then $A_1 = A_2 = M_n(K)$, and $\tau_i(x) = Q_i^{-1} x^t Q_i$ with Q_i symmetric, $i = 1, 2$. Let q_i be the quadratic form with matrix Q_i. We need to show that for any $v \in V^K$, the forms q_1 and q_2 are similar over K_v (cf. Proposition 3.3). By (α), the groups $\mathscr{G}_1$ and $\mathscr{G}_2$ have the same K_v-rank, and therefore the forms q_1 and q_2 have the same Witt index over K_v. For $v \in V_r^K$, this immediately implies that q_1 is equivalent to $\pm q_2$, as required. Let now $v \in V_f^K$. Replacing one of the forms by a proportional form, we can assume that $d(q_1) = d(q_2)$ in $K_v^\times / K_v^{\times 2}$ (cf. (42)). We can write $q_i = q_i^h \perp q_i^a$ where q_i^h is hyperbolic and q_i^a is anisotropic over K_v. Then q_1^a and q_2^a have the same dimension s (which can only be 1 or 3) and the same determinant. But then q_1^a and q_2^a are equivalent: for $s = 1$, this is obvious, and for $s = 3$ it follows from the fact that, up to equivalence, there is a unique anisotropic ternary quadratic form of a given determinant. Thus, q_1 and q_2 are equivalent over K_v, and the required isomorphism in (ii) follows from Proposition 3.3.

Let now n be even, $m = n/2$ and $A = M_m(D)$, where D is a quaternion central simple K-algebra. Notice that it follows from (β) that the involutions τ_1 and τ_2 have the same discriminant (equivalently, the same determinant). Let $v \in V^K$ be such that $D_v = D \otimes_K K_v$ is a division algebra. Write τ_i in the form $\tau_i(x) = Q_i^{-1} x^* Q_i$, where $(x_{ij})^* = (\overline{x_{ji}})$ and $\bar{}$ is the standard involution of D_v, $Q_i \in M_m(D_v)$ is an invertible skew-hermitian matrix, and let h_i be the corresponding skew-hermitian form. Then h_1 and h_2 have the same discriminant, and therefore are equivalent over D_v: for v nonarchimedean this follows from Theorem 3.6 of [26], Chapter 10, and for v real it follows from Theorem 3.7 of loc. cit. As above, this leads to the required isomorphism.

Next, we consider the case where $D_v \simeq M_2(K_v)$, and hence $A \simeq M_n(K_v)$. Then the involutions $\tau_i \otimes \mathrm{id}_{K_v}$, which for simplicity we will denote by τ_i, can be written in the form $\tau_i(x) = Q_i^{-1} x^t Q_i$, where $Q_i \in M_n(K_v)$ is an invertible symmetric matrix. Let q_i be the quadratic form with matrix Q_i. As above, we conclude that q_1 and q_2 have the same Witt index (over K_v) and the same determinant: $d(q_1) = d(q_2)$, or, equivalently, the same discriminant: $\delta(q_1) = \delta(q_2)$, where $\delta(q) = (-1)^{n/2} \cdot d(q)$, and to establish our claim we need to show that q_1 and q_2 are similar over K_v. If $v \in V_r^K$, then the mere fact that q_1 and q_2 have the same Witt index implies that q_1 is equivalent to $\pm q_2$, yielding the required fact. Let now $v \in V_f^K$. First, suppose that the common discriminant $\delta \in K_v^{\times 2}$. Since binary forms whose discriminant is a square, are isotropic, the common value of the Witt index of q_1 and q_2 can only be $n/2$ or $(n-4)/2$. It is well known that there is a unique anisotropic quadratic form over K_v in four variables (viz., the reduced norm form of the unique quaternion division algebra over K_v), so in both cases, q_1 and q_2 are equivalent. It remains to consider the case where the common discriminant $\delta \notin K_v^{\times 2}$. Let q be any n-dimensional quadratic form with discriminant δ, and let $\lambda \in K_v^\times$ be such that the Hilbert symbol $(\delta, \lambda)_v = -1$ (which exists as $\delta \notin K_v^{\times 2}$). Then it follows from (42) that the Hasse invariant $h_v(\lambda q)$ equals $-h_v(q)$, and therefore the forms q and λq represent the two equivalence classes of n-dimensional forms of discriminant δ. This, clearly, implies that in our situation q_1 and q_2 are similar, as required.

Finally, we note that arguing as in the proof of Corollary 8.5, we see that the subalgebras E used in the above argument can be chosen so that the corresponding K-torus $\mathscr{T}$ is generic. If n is even, then such an E is automatically a field extension of K (Proposition 2.5), so effectively our argument only relies on the assumption that A_1 and A_2 contain the same isomorphism classes of maximal fields invariant under the given involutions. □

Using the fact that for $A = M_n(K)$ and any orthogonal involution τ, the set $\mathscr{I} = \mathscr{I}(A, \tau)$ reduces to a single isomorphism class (Proposition 8.7), we obtain the following interesting consequence of Proposition 9.4.

Corollary 9.5. *Let A_i, $i = 1, 2$, be central simple algebras over a number field K, of dimension n^2, where $n \geq 3$, $n \neq 4$, given with orthogonal involutions τ_i, and let $\mathscr{G}_i = \mathrm{SU}(A_i, \tau_i)$. Assume that for some finite $S \subset V^K$, for $i = 1, 2$, any $(\mathscr{G}_i, K, S)$-arithmetic subgroup Γ_i of $\mathscr{G}_i(K)$ is Zariski-dense in $\mathscr{G}_i$, and Γ_1 and Γ_2 are weakly commensurable. Then, if one of the algebras is isomorphic to $M_n(K)$, the groups $\mathscr{G}_1$ and $\mathscr{G}_2$ are K-isomorphic, and hence the S-arithmetic subgroups Γ_1 and Γ_2 are commensurable.*

Proof of Theorem 9.1. There exist central simple algebras with orthogonal involutions (A_1, τ_1) and (A_2, τ_2) over K, of dimension n^2, where $n = 4r$ and $r > 2$, such

that $\mathscr{G}_i = \mathrm{SU}(A_i, \tau_i)$. We need to show that the existence of Zariski-dense weakly commensurable S-arithmetic subgroups Γ_1 of $\mathscr{G}_1(K)$ and Γ_2 of $\mathscr{G}_2(K)$ implies that $(A_1, \tau_1) \simeq (A_2, \tau_2)$. According to Proposition 9.4 (i), A_1 and A_2 involve the same division algebra D in their description. If $D = K$ (i.e., $A_1 = A_2 = M_n(K)$), then the assertion of the theorem follows from Corollary 9.5. So, we can assume in the rest of the proof that D is a quaternion division algebra over K, and A_1 and A_2 coincide with $A = M_m(D)$, where $m = 2r$. Let $\mathscr{I} = \mathscr{I}(A, \tau_1)$. Using Corollary 8.5, one can find for each $\eta \in \mathscr{I}$, an n-dimensional η-invariant commutative étale subalgebra E_η of A satisfying (1) of §1 so that if $\mathscr{T}_\eta$ is the corresponding maximal K-torus of $\mathscr{G}_\eta := \mathrm{SU}(A, \eta)$, and V is the finite set of places of K described just before the statement of Theorem 8.1, then the following conditions hold:

(a) E_η is as in Theorem 8.1 (i);

(b) $\mathscr{T}_\eta$ is generic (in the sense of §2);

(c) $\mathscr{T}_{\eta S} := \prod_{v \in S} \mathscr{T}_\eta(K_v)$ is noncompact.

Indeed, first assume that there exists $v_0 \in S \cap V$. Then applying Corollary 8.5 with $\mathscr{S} = \emptyset$ we find a subalgebra E_η such that (a) and (b) hold. To see that (c) holds automatically in this case, one needs to observe that since $(E_\eta, \eta|E_\eta) = (F_\eta[x]/(x^2 - d), \theta)$ (notations as in Theorem 8.1) and $d \in (F_\eta \otimes_K K_{v_0})^{\times 2}$, there is a K_{v_0}-isomorphism $\mathscr{T}_\eta \simeq \mathrm{R}_{F_\eta \otimes_K K_{v_0}/K_{v_0}}(\mathrm{GL}_1)$, implying that $\mathscr{T}_\eta(K_{v_0})$ is noncompact. It remains to consider the case where $S \cap V = \emptyset$. Since $\mathscr{G}_1(K)$ contains a Zariski-dense S-arithmetic group, the group $\mathscr{G}_{1S} := \prod_{v \in S} \mathscr{G}_1(K_v)$ is noncompact, i.e., there exists $v_0 \in S$ such that $\mathscr{G}_1(K_{v_0})$ is noncompact. But the groups $\mathscr{G}_1$ and $\mathscr{G}_\eta$ are isomorphic over K_{v_0}, so $\mathscr{G}_\eta(K_{v_0})$ is noncompact as well.[4] Then $\mathscr{G}_\eta$ contains a maximal K_{v_0}-torus $\mathscr{T}_0$ such that $\mathscr{T}_0(K_{v_0})$ is noncompact, and we let $E(v_0)$ denote the corresponding commutative étale subalgebra of $A \otimes_K K_{v_0}$. Applying Corollary 8.5 to $\mathscr{S} = \{v_0\}$, we can find E_η so that both (a) and (b) hold, and in addition

$$(E_\eta \otimes_K K_{v_0}, (\eta \otimes \mathrm{id}_{K_{v_0}})|E_\eta \otimes_K K_{v_0}) \simeq (E(v_0), (\eta \otimes \mathrm{id}_{K_{v_0}})|E(v_0)).$$

Then $\mathscr{T}_\eta \simeq \mathscr{T}_0$ over K_{v_0}, implying that $\mathscr{T}_\eta(K_{v_0})$ is noncompact and yielding (c).

Now, let $\mathscr{T}_1 := \mathscr{T}_{\tau_1}$ in the above notation. Then $\mathscr{T}_1$ is K-anisotropic, so the quotient $\mathscr{T}_{1S}/\mathscr{T}_1(\mathcal{O}(S))$ is compact ([20], Theorem 5.7), where $\mathscr{T}_{1S} = \prod_{v \in S} \mathscr{T}_1(K_v)$, and $\mathcal{O}(S)$ is the ring of S-integers in K. Since, by (c), $\mathscr{T}_{1S}$ is noncompact, the group $\mathscr{T}_1(\mathcal{O}(S))$ is infinite, and therefore there exists an element $\gamma_1 \in \mathscr{T}_1(K) \cap \Gamma_1$ of infinite order. By our assumption, γ_1 is weakly commensurable to some semi-simple $\gamma_2 \in \Gamma_2$. Let $\mathscr{T}_2$ be a maximal K-torus of $\mathscr{G}_2$ containing γ_2, and let E_1 and E_2 be the n-dimensional commutative étale subalgebras of A corresponding to $\mathscr{T}_1$ and $\mathscr{T}_2$ respectively. By Theorem 6.3 of [23], we have $L_1 = L_2$, where L_i is the minimal Galois

[4] This, in particular, shows that S-arithmetic subgroups in $\mathscr{G}_\eta$ are Zariski-dense, for any $\eta \in \mathscr{I}$.

extension of K over which $\mathscr{G}_i$ becomes an inner form. So, condition (b) above permits an application of Proposition 9.2, from which we get $(E_1, \tau_1|E_1) \simeq (E_2, \tau_2|E_2)$. In particular, there is an embedding $(E_1, \tau_1|E_1) \hookrightarrow (A, \tau_2)$. Due to condition (a), we can apply Theorem 8.1 (ii), to obtain $(A, \tau_1) \simeq (A, \tau_2)$. □

Remark 9.6. Theorem 9.1 implies that if K is a number field and G is a connected absolutely simple K-group of type D_{2r} with $r > 2$, then any K-form G' of G having the same set of isomorphism classes of maximal K-tori as G, is necessarily K-isomorphic to G; see Theorem 7.5 in [23].

9.7. We take this opportunity to point out the following corrections in [23]. (i) In assertion (2) of Theorem 4.2, replace the condition "*if* $L_1 = L_2$," by "*if* $L_1 = L_2 =: L$, *and* $\theta_{T_1}(\mathrm{Gal}(\mathrm{L}_{\mathrm{T}_1}/\mathrm{L})) \supset \mathrm{W}(\mathrm{G}_1, \mathrm{T}_1)$,". (ii) In the proof of Proposition 5.6, after the proof of Lemma 5.7, replace "G", occurring without a subscript, with "G_2" everywhere. (iii) In the fourth line of the proof of Theorem 4 (in §6), replace "G" by "G_1", and in the next line, replace "obtained from $\mathscr{G}$" by "obtained from $\overline{\mathscr{G}}$".

Appendix

The goal of this appendix is to describe a Galois-cohomological approach to the problem of embedding of a commutative étale algebra with an involutive automorphism into a simple algebra with an involution, and also to interpret the latter as a problem of finding rational points on certain homogeneous spaces. Even though these methods do provide some additional insight, it appears that neither of them is likely to yield any simplification in the proofs of our embedding theorems, nor can they be used to give an alternative proof of Theorem 8.1, which is one of the central results of the current paper. For this reason, we chose to present the results in the main body of the paper in the set-up of simple algebras with involution and their subalgebras, and confine a discussion of relevant Galois-cohomological techniques to this appendix.

As in the main body of the paper, we let (A, τ) denote a central simple L-algebra, with $\dim_L A = n^2$, endowed with an involution τ. Furthermore, we let (E, σ) be an n-dimensional commutative étale L-algebra with an involutive automorphism σ that leaves L invariant and satisfies $\sigma|L = \tau|L$ and also condition (1) §1. Set $K = L^\tau$. To streamline the exposition, we will leave out the case where τ is of the first kind and n is odd as otherwise we find ourselves in the split case which is well-understood in terms of the classical results of the theory of quadratic forms, cf. §7. So we will assume that either τ is of the second kind, or τ is of the first kind (hence $K = L$), n is even and $\dim_K F = n/2$ where $F = E^\sigma$. Then it follows from Propositions 2.1 and 2.2 that E is a 2-dimensional free F-module, and hence the corresponding unitary group $\mathrm{U}(E, \sigma)$ is a torus which we will denote by T. Clearly,

$$T \simeq \mathrm{R}_{F/K}(\mathrm{R}^{(1)}_{E/F}(\mathrm{GL}_1)) \tag{A1}$$

in the standard notations. Furthermore, we let H denoted the unitary group $\mathrm{U}(A, \tau)$ regarded as an algebraic K-group.

Next, we assume that there is an embedding $\varepsilon\colon E \hookrightarrow A$ which may or may not respect involutions. In the sequel, we will use the same notations ε, τ for the natural extensions of these maps to $E \otimes_K K_{\mathrm{sep}}$, $A \otimes_K K_{\mathrm{sep}}$ etc. According to Proposition 3.1, there exists a τ-symmetric $g \in A^\times$ such that

$$\varepsilon(\sigma(x)) = g^{-1}\tau(\varepsilon(x))g \quad \text{for all } x \in E. \tag{A2}$$

Pick $s \in (A \otimes_K K_{\mathrm{sep}})^\times$ so that

$$g = \tau(s)s. \tag{A3}$$

In the sequel, we will use the standard notation and conventions from Galois cohomology of algebraic groups (cf., for example, [20], Chapter VI, or [28], Chapter III); in particular, for an algebraic K-group G we let $Z^1(K, G)$ denote the set of 1-cocycles on $\mathrm{Gal}(K_{\mathrm{sep}}/K)$ with values in $G(K_{\mathrm{sep}})$, and let $H^1(K, G)$ denote the corresponding cohomology set.

Proposition A. (i) *Given* $\xi = \{\xi_\theta\} \in Z^1(K, T)$, *set* $\zeta_\theta = s\varepsilon(\xi_\theta)\theta(s)^{-1}$. *Then* $\zeta = \{\zeta_\theta\} \in Z^1(K, H)$. *Furthermore, the correspondence* $\xi \mapsto \zeta$ *yields a well-defined map*

$$\varphi\colon H^1(K, T) \longrightarrow H^1(K, H).$$

(ii) *The equation* $g\varepsilon(b) = \tau(h)h$ *has a solution* $(b, h) \in F^\times \times A^\times$ (*which is equivalent to the existence of an embedding* $(E, \sigma) \hookrightarrow (A, \tau)$ *as algebras with involutions – cf. Theorem* 3.2) *if and only if* $\mathrm{Im}\,\varphi$ *contains the trivial element of* $H^1(K, H)$.

Proof. (i) First, we observe that

$$s\varepsilon(T)s^{-1} \subset H. \tag{A4}$$

Indeed, for any $x \in T(K)$, using (A2) and (A3), we obtain

$$\begin{aligned}\tau(s\varepsilon(x)s^{-1})(s\varepsilon(x)s^{-1}) &= \tau(s)^{-1}\tau(\varepsilon(x))g\varepsilon(x)s^{-1}\\ &= \tau(s)^{-1}g\varepsilon(\sigma(x)x)s^{-1}\\ &= \tau(s)^{-1}gs^{-1} = 1.\end{aligned}$$

It follows that for any $\theta \in \mathrm{Gal}(K_{\mathrm{sep}}/K)$, we have

$$\zeta_\theta = (s\varepsilon(\xi_\theta)s^{-1})(s\theta(s)^{-1}) \in H(K_{\mathrm{sep}})$$

as

$$g = \tau(s)s = \theta(g) = \theta(\tau(s))\theta(s) = \tau(\theta(s))\theta(s),$$

hence $s\theta(s)^{-1} \in H(K_{\text{sep}})$. Furthermore, for any $\theta_1, \theta_2 \in \text{Gal}(K_{\text{sep}}/K)$, we have

$$\zeta_{\theta_1}\theta_1(\zeta_{\theta_2}) = s\varepsilon(\xi_{\theta_1\theta_2})(\theta_1\theta_2)(s)^{-1} = \zeta_{\theta_1\theta_2},$$

proving that $\zeta = \{\zeta_\theta\} \in Z^1(K, H)$. Finally, we show that the correspondence $\xi \mapsto \zeta$ takes cohomologus cocycles into cohomologus cocycles. Indeed, for any $t \in T(K_{\text{sep}})$ we have

$$s\varepsilon(t\xi_\theta\theta(t)^{-1})\theta(s)^{-1} = (s\varepsilon(t)s^{-1})\zeta_\theta\theta(s\varepsilon(t)s^{-1})^{-1},$$

which defines a cocycle cohomologus to ζ_θ, in view of (A4). So, the correspondence $\xi \mapsto \zeta$ gives rise to a well-defined map $\varphi\colon H^1(K, T) \to H^1(K, H)$.

(ii) First, recall that if $a \in A^\times$ is τ-symmetric and $a = \tau(x)x$ with $x \in (A \otimes_K K_{\text{sep}})^\times$, then $\zeta = \{\zeta_\theta\}$, where $\zeta_\theta = x\theta(x)^{-1}$, is a cocycle in $Z(K, H)$, which is cohomologus to the trivial cocycle if and only if the equation $a = \tau(x)x$ has a solution in $A^\times$. Next, it follows from (A1) that

$$H^1(K, T) \simeq F^\times/N_{E/F}(E^\times), \tag{A5}$$

and the inverse of this isomorphism can be described as follows. Given $b \in F^\times$, pick $c \in (E \otimes_K K_{\text{sep}})^\times$ so that $b = \sigma(c)c$ $(= N_{E/F}(c))$, and for $\theta \in \text{Gal}(K_{\text{sep}}/K)$ set $\xi_\theta = c\theta(c)^{-1}$. Then $\xi = \{\xi_\theta\} \in Z^1(K, T)$, and the correspondence

$$bN_{E/F}(E^\times) \mapsto (\text{class of } \xi)$$

gives the inverse of the isomorphism (A5).

Now, suppose that the equation $g\varepsilon(b) = \tau(h)h$ has a solution $(b, h) \in F^\times \times A^\times$. We then choose $c \in (E \otimes_K K_{\text{sep}})^\times$ and construct $\xi \in Z^1(K, T)$ as in the previous paragraph, for that b. Then with s as in (A3), we have

$$g\varepsilon(b) = g\varepsilon(\sigma(c)c) = \tau(\varepsilon(c))g\varepsilon(c) = \tau(s\varepsilon(c))(s\varepsilon(c)). \tag{A6}$$

So, $x := s\varepsilon(c)$ is a solution to $g\varepsilon(b) = \tau(x)x$, which also has the solution $h \in A^\times$. By the remark above, this means that the cocycle $\zeta \in Z^1(K, H)$, corresponding to x, given by

$$\zeta_\theta = x\theta(x)^{-1} = s\varepsilon(c\theta(c)^{-1})\theta(s)^{-1}, \tag{A7}$$

lies in the trivial class in $H^1(K, H)$. On the other hand, $\varphi(\xi) = \zeta$, and therefore Im φ contains the trivial element of $H^1(K, H)$. Conversely, suppose $\xi \in Z^1(K, T)$ is such that $\varphi(\xi)$ represents the trivial element of $H^1(K, H)$. Using (A5) and subsequent remarks, we can write $\xi = \{\xi_\theta\}$, where

$$\xi_\theta = c\theta(c)^{-1} \text{ for some } c \in (E \otimes_K K_{\text{sep}})^\times \text{ such that } b := \sigma(c)c \in F^\times.$$

Then (A6) shows that $x = s\varepsilon(c)$ satisfies $g\varepsilon(b) = \tau(x)x$, and (A7) combined with the definition of φ implies that the class in $H^1(K, H)$ corresponding to x, coincides with $\varphi(\xi)$, hence is trivial. So, the equation $g\varepsilon(b) = \tau(h)h$ has a solution $h \in A^\times$, as required. □

We can now reformulate the question about the local–global principle for the existence of an embedding $(E,\sigma) \hookrightarrow (A,\tau)$ as algebras with involutions as follows. For $v \in V^K$, define the corresponding local map $\varphi_v\colon H^1(K_v,T) \to H^1(K_v,H)$ just as we defined φ in Proposition A1 (i). *Does the fact that* $\operatorname{Im}\varphi_v$ *contains the trivial element of* $H^1(K_v,H)$ *for all* $v \in V^K$ *imply that* $\operatorname{Im}\varphi$ *contains the trivial element of* $H^1(K,H)$*?* To analyze this question, we consider the following diagram

$$\begin{array}{ccc} H^1(K,T) & \xrightarrow{\quad\varphi\quad} & H^1(K,H) \\ \Big\downarrow{\scriptstyle\alpha} & & \Big\downarrow{\scriptstyle\beta} \\ \prod_{v\in V^K} H^1(K_v,T) & \xrightarrow{\Phi} & \prod_{v\in V^K} H^1(K_v,H), \end{array} \tag{A8}$$

in which $\Phi = \prod \varphi_v$ and α, β are induced by restrictions. Clearly, the above question is much more tractable if β is injective, i.e., H satisfies the Hasse principle for Galois cohomology. The Hasse principle may fail for orthogonal involutions in the non-split case - see below, but it is valid in all other cases at hand. We will now use this to explain why the proof of Theorem 5.1, which yields the unconditional local–global principle for embeddings if τ is symplectic, was so easy. In this case, H is connected and simply connected (of type C_ℓ, for $\ell = n/2$), so $H^1(K_v,H) = 1$ for all $v \in V_f^K$ (cf. [20], Theorem 6.4). So, instead of (A8), we can work with the following:

$$\begin{array}{ccc} H^1(K,T) & \xrightarrow{\quad\varphi\quad} & H^1(K,H) \\ \Big\downarrow{\scriptstyle\alpha} & & \Big\downarrow{\scriptstyle\beta} \\ \prod_{v\in V_\infty^K} H^1(K_v,T) & \xrightarrow{\Phi} & \prod_{v\in V_\infty^K} H^1(K_v,H). \end{array} \tag{A9}$$

It is known that α is surjective ([20], Proposition 6.17), and β is injective (in fact, bijective) ([20], Theorem 6.6). So, a simple diagram chase shows that if $\operatorname{Im}\varphi_v$ contains the trivial class in $H^1(K_v,H)$ for all $v \in V_\infty^K$, then $\operatorname{Im}\varphi$ contains the trivial class in $H^1(K,H)$, as required. (Notice that this is not an alternative proof of Theorem 5.1, but rather a cohomological interpretation of the argument given in §5.)

Next, we consider the case where τ is of the second kind. Then H is a connected reductive group, whose commutator subgroup $G = \mathrm{SU}(A,\tau)$ is simply connected. So, $H^1(K_v,G) = 1$ for all $v \in V_f^K$, however $H^1(K_v,H) \neq 1$ for $v \in V_f^K$ that do not split in L, and therefore it is not enough to work with (A9) in this case. To study cohomology of H we consider the exact sequence

$$1 \longrightarrow G \longrightarrow H \xrightarrow{\det} S \longrightarrow 1, \tag{A10}$$

where $S = \mathrm{R}^{(1)}_{L/K}(\mathrm{GL}_1)$, and det is the homomorphism of reduced norm, and the corresponding sequence of cohomology

$$H^1(K,G) \xrightarrow{\gamma} H^1(K,H) \xrightarrow{\delta} H^1(K,S).$$

We have an isomorphism $H^1(K,S) \simeq K^\times/N_{L/K}(L^\times)$ similar to (A5), and it is easy to compute that in terms of these isomorphisms the composite map $\delta\circ\varphi$ can be described as follows

$$H^1(K,T) \ni bN_{E/F}(E^\times) \xrightarrow{\delta\circ\varphi} (\mathrm{Nrd}_{A/L}(g)\cdot N_{F/K}(b))N_{L/K}(L^\times) \in H^1(K,S).$$

The compositions $\delta_v\circ\varphi_v$, where $\delta_v\colon H^1(K_v,H)\to H^1(K_v,S)$ is obtained from (A10) over K_v, have a similar description. For every $v\in V^K$, there exists $b_v\in (F\otimes_K K_v)^\times$ such that for the corresponding cocycle $\xi_v\in H^1(K_v,T)$, the element $\varphi_v(\xi_v)\in H^1(K_v,H)$ is trivial. Applying δ_v and using the above description, we obtain that

$$\mathrm{Nrd}_{A/L}(g)\cdot N_{F\otimes_K K_v/K_v}(b_v)\in N_{L\otimes_K K_v/K_v}((L\otimes_K K_v)^\times).$$

Now, assuming that E/L is a field extension, which enables us to use the multinorm principle (Proposition 4.2) and the subsequent argument in §4, we conclude that there exists $b\in F^\times$ such that

$$\mathrm{Nrd}_{A/L}(g)\cdot N_{F/K}(b)\in N_{L/K}(L^\times) \tag{A11}$$

and

$$b\in b_v N_{E\otimes_K K_v/F\otimes_K K_v}((E\otimes_K K_v)^\times) \quad \text{for all } v\in V_\infty^K. \tag{A12}$$

We claim that if $\xi\in H^1(K,T)$ is the cocycle corresponding to b then $\zeta:=\varphi(\xi)$ is trivial. Indeed, (A11) implies that $\delta(\zeta)=1$, and therefore $\zeta\in\gamma(H^1(K,G))$. But for any $v\in V_f^K$ we have $H^1(K_v,G)=1$, which yields that the image of ζ in $H^1(K_v,G)$ is trivial. On the other hand, due to (A12), for any $v\in V_\infty^K$, the image of ζ in $H^1(K_v,H)$ coincides with that $\varphi_v(\xi_v)$, hence is also trivial. Thus, $\beta(\zeta)=1$, so the injectivity of β (which is equivalent to Landherr's theorem, cf. [20], §6.7, implies that $\zeta=1$, as required. (Again, this argument is simply the cohomological version of the proof of Theorem 4.1.)

For an orthogonal involution τ, the group H is no longer connected, and more importantly, may fail to satisfy the Hasse principle for Galois cohomology, i.e., β need not be injective, in the nonsplit case (cf. [13], §5.11, or [20], §6.6). This is a serious obstacle to obtaining a purely cohomological proof of Theorem 6.1. To overcome this obstacle, we were forced to introduce some new techniques in §6 and study the classes $[C(A,\nu,\phi)]$.

Finally, one can view Theorem 3.2 as the assertion that the existence of an embedding $(E,\sigma)\hookrightarrow(A,\tau)$ is equivalent to the existence of a K-rational point on the variety

$$Y:=\{(b,h)\in \mathrm{R}_{F/K}(\mathrm{GL}_1)\times \mathrm{GL}_{1,A}\mid g\varepsilon(b)=\tau(h)h\}.$$

So, we would like to point out that Y is in fact a homogeneous space of the group $\mathscr{G}:=H\times \mathrm{R}_{E/K}(\mathrm{GL}_1)$ under the following action

$$(x,z)\cdot(b,h)=(\sigma(z)bz,\ xhz).$$

Furthermore, in our previous notations, $(1, s) \in Y$, and the stabilizer of this point is the torus $\{(st^{-1}s^{-1}, t) \mid t \in T\}$. Thus, the question about the local–global principle for the existence of an embedding $(E, \sigma) \hookrightarrow (A, \tau)$ fits into the general framework of the Hasse principle for homogeneous spaces of linear algebraic groups. Among early results in this area one can mention the validity of the Hasse principle for projective homogeneous varieties (Harder [10]) and for symmetric spaces of absolutely simple simply connected groups (Rapinchuk [25]). Later, Borovoi in a series of papers developed cohomological methods for analyzing the Hasse principle for homogeneous spaces with connected stabilizers, of an arbitrary connected group whose maximal semi-simple subgroups are simply connected. In particular, in [2], he proved that the Brauer–Manin obstruction is the only obstruction to the Hasse principle in this situation, and in [3], computed this obstruction in terms of Galois cohomology (some methods for computing the Brauer group of a compactification of a given homogeneous space are given in [7]). It would probably be interesting to use these techniques to show that the Brauer–Manin obstruction for Y is trivial if τ is a symplectic involution, and to compute it precisely when τ is of the second kind (apparently, it is related to the Tate–Shafarevich group of the multinorm torus associated with the pair of ètale algebras (F, L)). However, because of the concrete description of Y, one can give a direct Galois-cohomological analysis of the existence of a K-rational point on it which results in the condition described in Proposition A (ii). We feel that the general results on homogeneous spaces are unlikely to lead to an alternative proof of our results. Moreover, for an orthogonal involution τ, the group $\mathscr{G}$ is disconnected, which makes Borovoi's results inapplicable, but this can serve as a motivation to extend these results to some class of disconnected groups which includes $\mathscr{G}$.

References

[1] A. Borel, *Linear algebraic groups*. 2nd enlarged edition, Grad. Texts. in Math. 126, Springer-Verlag, New York 1991. Zbl 0726.20030 MR 1102012

[2] M. Borovoi, The Brauer-Manin obstruction for homogeneous spaces with connected or abelian stabilizer. *J. Reine Angew. Math.* **473** (1996), 181–194. Zbl 0844.14020 MR 1390687

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

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

[5] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*. Academic Press, London 1967. Zbl 0153.07403 MR 0215665

[6] P. Chuard-Koulmann and J. Morales, Extending involutions on Frobenius algebras. *Manuscripta Math.* **108** (2002), 439–451. Zbl 1027.11026 MR 1923532

[7] J.-L. Colliot-Thélène and B. E. Kunyavskii, Groupe de Picard et groupe de Brauer des compactifications lisses d'espaces homogènes. *J. Algebraic Geom.* **15** (2006), 733–752. Zbl 05141405 MR 2237268

[8] A. Cortella, Le principe de Hasse pour les similitudes de formes bilinéaires. PhD Thesis, Université de Franche-Comté, Besançon 1993.

[9] P. Gille and S. Garibaldi, Algebraic groups with few subgroups. Preprint, 2008.

[10] G. Harder, Bericht über neuere Resultate der Galoiskohomologie halbeinfacher Matrizengruppen. *Jahresber. Deutsch. Math.-Verein.* **70** (1968), 182–216. Zbl 0194.05701 MR 0242838

[11] G. Harder, Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. *J. Reine Angew. Math.* **274–275** (1975), 125–138. Zbl 0317.14025 MR 0382469

[12] M. Kneser, Starke Approximation in algebraischen Gruppen. *J. Reine Angew. Math.* **218** (1965), 190–203. Zbl 0143.04701 MR 0184945

[13] M. Kneser, *Lectures on Galois cohomology of classical groups*. Tata Institute of Fundamental Research Lectures on Mathematics 47, Tata Institute of Fundamental Research, Bombay, 1969. Zbl 0246.14008 MR 0340440

[14] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions.* Amer. Math. Soc. Colloq. Publ. 44, Amer. Math. Soc., Providence, R.I., 1998. Zbl 0955.16001 MR 1632779

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

[16] D. W. Lewis, T. Unger, and J. Van Geel, The Hasse principle for similarity of Hermitian forms. *J. Algebra* **285** (2005), 196–212. Zbl 1147.11315 MR 2119111

[17] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*. Grundlehren Math. Wiss. 323, Springer-Verlag, Berlin 2000. Zbl 0948.11001 MR 1737196

[18] T. Ono, Arithmetic of orthogonal groups. *J. Math. Soc. Japan* **7** (1955), 79–91. Zbl 0065.01201 MR 0069823

[19] R. S. Pierce, *Associative algebras*. Grad. Texts. in Math. 88, Springer-Verlag, New York 1982. Zbl 0497.16001 MR 0674652

[20] V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory.* Pure Appl. Math. 139, Academic Press, Boston, Mass., 1994. Zbl 0841.20046 MR 1278263

[21] G. Prasad and A. S. Rapinchuk, Computation of the metaplectic kernel. *Inst. Hautes Études Sci. Publ. Math.* **84** (1996), 91–187. Zbl 0941.22019 MR 1441007

[22] G. Prasad and A. S. Rapinchuk, Existence of irreducible $\mathbb{R}$-regular elements in Zariski-dense subgroups. *Math. Res. Lett.* **10** (2003), 21–32. Zbl 1029.22020 MR 1960120

[23] G. Prasad and A. S. Rapinchuk, Weakly commensurable arithmetic groups and isospectral locally symmetric spaces. *Inst. Hautes Études Sci. Publ. Math.* **109** (2009), 113–184. Zbl 1176.22011 MR 2511587

[24] G. Prasad and A. S. Rapinchuk, Number-theoretic techniques in the theory of Lie groups and differential geometry. In *Proceedings of the 4th Internernational Congress of Chinese Mathematicians* (Hangzhou, 2007), Vol. I, Higher Education Press, Beijing 2007, 216–232.

[25] A. S. Rapinchuk, The Hasse principle for symmetric spaces. *Dokl. Akad. Nauk BSSR* **31** (1987), 773–776 (in Russian). Zbl 0679.14027 MR 0912956

[26] W. Scharlau, *Quadratic and Hermitian forms*. Grundlehren Math. Wiss. 270, Springer-Verlag, Berlin, 1985. Zbl 0584.10010 MR 0770063

[27] J-P. Serre, *A course in arithmetic*. Grad. Texts in Math. 7, Springer-Verlag, New York 1973. Zbl 0256.12001 MR 0344216

[28] J-P. Serre, *Galois cohomology*. Springer-Verlag, Berlin 1997. Zbl 0902.12004 MR 1466966

[29] J. Tits, Classification of algebraic semisimple groups. In *Algebraic groups and discontinuous groups*, Proc. Sympos. Pure Math. 9, Amer. Math. Soc., Providence, R.I., 1966, 33–62. Zbl 0238.20052 MR 0224710

[30] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*. Transl. Math. Monogr. 179, Amer. Math. Soc., Providence, R.I., 1998. Zbl 0974.14034 MR 1634406

Received July 21, 2008

Gopal Prasad, Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, U.S.A.

E-mail: gprasad@umich.edu

Andrei S. Rapinchuk, Department of Mathematics, University of Virginia, Charlottesville, VA 22904, U.S.A.

E-mail: asr3x@virginia.edu