

Characterization of Special Points of Orthogonal Symmetric Spaces

Andrew Fiori

Department of Mathematics and Statistics, McGill University, 1034 Burnside Hall, 805 Sherbrooke W., Montreal, QC, H3A 2K6, Canada

Abstract

We give a characterization of the fields or algebras which are associated to special points on the orthogonal symmetric space of a given quadratic form.

Keywords: special point, orthogonal group, tori, quadratic form, orthogonal symmetric space

The content of this article has been published as [Fio12].

It is available at <http://dx.doi.org/10.1016/j.jalgebra.2012.08.030>.

This document contains some minor corrections and changes.

This document also appears as Chapter 3 in my Ph.D. thesis [Fio13].

1. Introduction

Given an algebraic group G defined over \mathbb{Q} and its associated symmetric space $G(\mathbb{R})/K$, where K is a maximal compact subgroup, one is interested in the special points (see [Del71, 3.15]). They correspond to those algebraic tori $T \subset G$ which are maximal, defined over \mathbb{Q} and for which $T(\mathbb{R})$ is compact. To such a torus T one can associate a field F which is the special field for the corresponding point. This special field appears as part of an étale algebra E which is naturally associated to the torus. We wish to answer the following:

Question. Given a quadratic form q with its corresponding orthogonal group O_q , what are the conditions on an étale algebra E such that E is associated to a maximal torus T of O_q ?

This problem is taken up, to some extent, by Shimura in [Shi80]. Some work on the problem also appears in my masters thesis [Fio09] as well as several other papers. This work is in fact complementary to my masters thesis where an abstract classification in terms of group cohomology is given. The relationship between those results and these will be the subject of future work. The most useful description for our current purposes is the work of Brusamarello, Chuard-Koulmann and Morales [BCKM03], from which one can extract various necessary and sufficient conditions on the algebra E . In this paper we rephrase the conditions which can be derived from [BCKM03].

The primary goal of this work is thus to prove the following:

Theorem 1.1. *Let (V, q) be a quadratic space over a number field k of dimension $2n$ or $2n + 1$ and discriminant $D(q)$, and let (E, σ) be a degree $2n$ field extension E of k of discriminant $\delta_{E/k}$ together with an involution σ . Then O_q contains a torus of type (E, σ) if and only if the following three conditions are satisfied:*

1. E^ϕ splits the even Clifford algebra C_q^0 for all σ -types ϕ of E .
2. If $\dim(V)$ is even then $\delta_{E/k} = (-1)^n D(q)$.
3. Let ν be a real infinite place of k and let s be the number of homomorphisms from E to \mathbb{C} over ν for which σ corresponds to complex conjugation. The signature of q is of the form $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i)_\nu$ if the dimension is even and either $(n - \frac{s}{2} + 2i + 1, n + \frac{s}{2} - 2i)_\nu$ or $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i + 1)_\nu$ if $\nu((-1)^n D(q)\delta_{E/k})$ is respectively positive or negative when the dimension is odd, where $0 \leq i \leq \frac{s}{2}$.

Moreover, for any E satisfying condition (2) we have that $\sqrt{D(q)} \in E^\phi$ for every σ -type ϕ of E .

The notion of a σ -type will be introduced in Definition 2.2.

We remark that the conditions in the theorem above are independent of the choice of similarity class representative for the quadratic form that defines O_q . We also note that one can replace the first condition of Theorem 1.1

Email address: afiori@math.mcgill.ca (Andrew Fiori)

by the condition that for all primes p of k where the even Clifford algebra is not split, there exists a prime $\mathfrak{p}|p$ of E^σ such that \mathfrak{p} does not split in E . The equivalence of these conditions is the content of Lemma 5.9 and comes up in the proof of the main theorem.

We would also like to point out that the theorem above, which holds for fields with involutions, does not extend to arbitrary étale algebras with involution. It follows from our proof that the conditions in the theorem are sufficient to ensure that there exist local embeddings for all of the places of k . Thus, the only obstacle to generalizing to étale algebras is the existence of a local-global principle. We would like to thank Prof. Eva Bayer, for pointing out the recent work of Prasad and Rapinchuk [PR10] on this problem. In their paper they provide both a counterexample to the local-global principle for étale algebras as well as giving a sufficient condition for when a local-global principle still holds. We also refer the reader to the forthcoming work of Eva Bayer [BF13] which gives a complete description of the obstructions to the local-global principle.

The original motivation for this work came from the problem of determining which CM-fields could be associated to the special points of a given a orthogonal group. The following corollary answers this question.

Corollary 1.2. *Suppose in the theorem that $k = \mathbb{Q}$, the signature of q is $(2, \ell)$ and (E, σ) is a CM-field with complex conjugation σ . Then O_q contains a torus of type (E, σ) if and only if:*

1. *For each prime p of \mathbb{Q} with local Witt invariant $W(q)_p = -1$ there exists a prime $\mathfrak{p}|p$ of E^σ that does not split in E .*
2. *If ℓ is even, then $D(q) = (-1)^{(2+\ell)/2} \delta_{E/\mathbb{Q}}$. (No further conditions if ℓ is odd.)*

Corollary 1.3. *Suppose that $k = \mathbb{Q}$ and the signature of q is $(2, \ell)$. Let F be a totally real field. Then there exists a CM-field E with $E^\sigma = F$, such that the orthogonal group O_q contains a torus of type (E, σ) if and only if:*

1. *No condition if ℓ odd.*
2. *If ℓ is even, then (up to squares) $D(q) = N_{F/k}(\delta)$ for an element $\delta \in F$ which satisfies the condition that for all primes p of k with $W(q)_p = -1$ there is at least one prime $\mathfrak{p}|p$ of F such that δ is not a square in $F_{\mathfrak{p}}$.*

As a final application, we have the following which recovers classical results concerning the classification of CM-points, and answers the more recently raised question of classifying almost totally real cycles on the Hilbert modular surfaces associated to real quadratic fields (see [DL03]).

Corollary 1.4. *Let $d \in \mathbb{Q}$ be a squarefree positive integer. Consider the quadratic form:*

$$q_d = x_1^2 - x_2^2 + x_3^3 - dx_4^2.$$

This implies $\text{Spin}_{q_d}(\mathbb{R}) \simeq \text{SL}_2(\mathbb{R})^2$ is associated to the Hilbert modular surface for $\mathbb{Q}(\sqrt{d})$. Let (E, σ) be an algebra of dimension 4 with involution σ . Then O_q has a torus of type (E, σ) if and only if the σ -reflex fields of E all contain $\mathbb{Q}(\sqrt{d})$. In particular, the algebras associated to tori in Spin_{q_d} all contain $\mathbb{Q}(\sqrt{d})$.

2. Preliminaries

We begin by recalling a few of the basic notions relevant to the statement of the theorem.

For this section let k be a field of characteristic 0, fix an algebraic closure \bar{k} and let $\Gamma = \text{Gal}(\bar{k}/k)$ be the absolute Galois group.

2.1. Étale Algebras

By an **étale algebra** E over k of dimension n we mean a product of finite (separable) field extensions E_i/k where the dimension of E as a k -module is n . The **discriminant** $\delta(E/k)$ or $\delta_{E/k}$ is the product of the field discriminants $\delta_{E_i/k}$. We have that $E \otimes_k \bar{k} \simeq \times_{\rho} \bar{k} e_{\rho}$, where the e_{ρ} are orthogonal idempotents indexed by $\rho \in \text{Hom}_{k\text{-alg}}(E, \bar{k})$. The isomorphism is given by the map $x \otimes \alpha \mapsto \sum_{\rho} \alpha \rho(x) e_{\rho}$. The Galois group Γ acts on the collection $\{e_{\rho}\}$ by $\tau e_{\rho} = e_{\tau \circ \rho}$. This action, together with the natural action on coefficients, corresponds to having Γ act on $E \otimes_k \bar{k}$ via the second factor so that $(E \otimes_k \bar{k})^{\Gamma} \simeq E$. Thus, the descent data needed to fully specify the k -isomorphism class of an n -dimensional étale algebra is the Galois action on the collection $\{e_{\rho}\}$. For a more detailed discussion of the theory of Galois descent, in particular how it applies to this setting see [KMRT98, Ch. 18]. The key result is:

Proposition 2.1. *There exists a bijective correspondence between isomorphism classes of étale algebras over k of dimension n and isomorphism classes of Γ -sets of size n . The correspondences being $E \mapsto \text{Hom}_{k\text{-alg}}(E, \bar{k})$ and $\Omega \mapsto (\times_{\rho \in \Omega} \bar{k} e_{\rho})^{\Gamma}$.*

We will often use this result to construct étale algebras by specifying a Γ -set.

By an **étale algebra with involution** (E, σ) over k we shall mean an étale algebra E over k together with $\sigma \in \text{Aut}_{k\text{-alg}}(E)$ of exact order 2. We will denote by $E^\sigma = \{x \in E \mid \sigma(x) = x\}$ the fixed étale subalgebra of σ . The action of σ on E induces an action on idempotents given by $\sigma : e_\rho \mapsto e_{\rho \circ \sigma}$. We see immediately that this action commutes with the Galois action. Now, consider the disjoint collection of sets $\text{Hom}_{k\text{-alg}}(E, \bar{k}) = \sqcup \{\rho, \rho \circ \sigma\}$. Since the actions of σ and Γ on $\text{Hom}_{k\text{-alg}}(E, \bar{k})$ commute we find that Γ acts on the collection of sets $\{\rho, \rho \circ \sigma\}$. We can thus consider the étale algebra whose idempotents come with this action. It is the subalgebra E^σ of E under the inclusion map $e_{\{\rho, \rho \circ \sigma\}} \mapsto e_\rho + e_{\rho \circ \sigma}$.

Convention. For the remainder of this paper we restrict our attention to the case where $\dim_k(E^\sigma) = \left\lceil \frac{\dim_k(E)}{2} \right\rceil$. For the most part we shall also assume that $\dim_k(E)$ is even. Unless it is otherwise specified, all algebras with involution satisfy these additional properties.

We will now introduce the notions of σ -types and σ -reflex algebras. These generalize the notion of CM-types and CM-reflex algebras which are important in the theory of complex multiplication and have been extensively studied. We shall only mention the notions which will be of use to us. For a more detailed exposition of CM-types and CM-reflex fields see either [Lan83, 1.2 and 1.5] or [Mil06, 1.1, pp.12-19].

Definition 2.2. Let (E, σ) be an algebra with involution. A subset $\phi \subset \text{Hom}_{k\text{-alg}}(E, \bar{k})$ is said to be a **σ -type** of E if $\phi \sqcup \phi\sigma = \text{Hom}_{k\text{-alg}}(E, \bar{k})$. Denote the set of σ -types:

$$\Phi = \{\phi \subset \text{Hom}_{k\text{-alg}}(E, \bar{k}) \mid \phi \sqcup \phi\sigma = \text{Hom}_{k\text{-alg}}(E, \bar{k})\}.$$

Then both Γ and σ act on Φ and these actions commute. For a σ -type $\phi \in \Phi$ denote its orbit in Φ under Γ by $\Gamma\phi \subset \Phi$ and denote the stabilizer by $\Gamma_\phi = \{\gamma \in \Gamma \mid \gamma\phi = \phi\}$.

We define the **σ -reflex algebra** of ϕ to be (E^ϕ, σ) , where E^ϕ is the étale algebra whose idempotents are indexed by $\Gamma\phi \cup \Gamma\phi\sigma$ with the induced action of Γ and σ .

We define the **complete σ -reflex algebra** to be (E^Φ, σ) , which is the étale algebra whose idempotents are indexed by Φ with the natural action of Γ and σ .

Proposition 2.3 (Alternate definition of reflex field). *Let ϕ be a σ -type of E and define $\widetilde{E}^\phi = \bar{k}^{\Gamma_\phi}$. If $\Gamma\phi = \Gamma\phi\sigma$ then E^ϕ is a field and $E^\phi \simeq \widetilde{E}^\phi$. Otherwise, if $\Gamma\phi \neq \Gamma\phi\sigma$ then $E^\phi = \widetilde{E}^\phi \times \widetilde{E}^\phi$.*

Proof. We claim that \widetilde{E}^ϕ naturally has idempotents corresponding to $\Gamma\phi$. Indeed, the idempotents of $\widetilde{E}^\phi = \bar{k}^{\Gamma_\phi}$ correspond to $\text{Hom}_k(\bar{k}^{\Gamma_\phi}, \bar{k})$, which is naturally identified with Γ/Γ_ϕ as Γ -sets. The map sends $\gamma\Gamma_\phi$ to $\gamma \circ \text{Id}$ where $\text{Id} : \bar{k}^{\Gamma_\phi} \rightarrow \bar{k}$ is the identity inclusion. Likewise we can identify Γ/Γ_ϕ and $\Gamma\phi$ as Γ -sets via the map $\gamma\Gamma_\phi \mapsto \gamma\phi$. By the correspondence between Γ -sets and étale algebras we conclude \widetilde{E}^ϕ is isomorphic to the étale algebra whose idempotents are $\Gamma\phi$. If $\Gamma\phi = \Gamma\phi\sigma$ this gives us the result. Otherwise, E^ϕ has idempotents $\Gamma\phi \sqcup \Gamma\phi\sigma$. As the action of Γ is from the left on $\Gamma\phi\sigma$ it follows that as Γ -sets $\Gamma\phi\sigma$ is isomorphic to $\Gamma\phi$. Thus we conclude $E^\phi = \widetilde{E}^\phi \times \widetilde{E}^\phi$. \square

Definition 2.4. Let (E, σ) be an étale algebra with involution over k and let ϕ be a σ -type of E . There is a natural map $N_\phi : E \rightarrow E^\phi$ which is defined by:

$$N_\phi \left(\sum_\rho a_\rho e_\rho \right) = \sum_{\phi_i \in (\Gamma\phi \cup \Gamma\phi\sigma)} \left(\prod_{\rho \in \phi_i} a_\rho \right) e_{\phi_i}.$$

This map is called the **σ -reflex norm** of the σ -type ϕ .

We want to show that this map, which a priori maps $E \otimes_k \bar{k}$ to $E^\phi \otimes_k \bar{k}$, actually maps E to $E^\phi = (E^\phi \otimes_k \bar{k})^\Gamma$. Since $E = (E \otimes_k \bar{k})^\Gamma$ we have that for $\gamma \in \Gamma$ and $\sum_\rho a_\rho e_\rho \in E$ the formula:

$$\sum_\rho a_\rho e_\rho = \gamma \left(\sum_\rho a_\rho e_\rho \right) = \sum_\rho \gamma(a_\rho) e_{\gamma \circ \rho}$$

implies that $\gamma(a_\rho) = a_{\gamma \circ \rho}$. Using this we check that:

$$\gamma \left(\prod_{\rho \in \phi_i} a_\rho \right) = \prod_{\rho \in \phi_i} \gamma(a_\rho) = \prod_{\rho \in \phi_i} a_{\gamma \circ \rho} = \prod_{\rho \in \gamma(\phi_i)} a_\rho.$$

Finally we may check that:

$$\begin{aligned}
\gamma \left(N_\phi \left(\sum_\rho a_\rho e_\rho \right) \right) &= \sum_{\phi_i \in (\Gamma\phi \cup \Gamma\phi\sigma)} \gamma \left(\prod_{\rho \in \phi_i} a_\rho \right) e_{\gamma\phi_i} \\
&= \sum_{\phi_i \in (\Gamma\phi \cup \Gamma\phi\sigma)} \left(\prod_{\rho \in \gamma(\phi_i)} a_\rho \right) e_{\gamma\phi_i} \\
&= N_\phi \left(\sum_\rho a_\rho e_\rho \right).
\end{aligned}$$

Hence we conclude that $N_\phi \left(\sum_\rho a_\rho e_\rho \right) \in (E^\phi \otimes_k \bar{k})^\Gamma = E^\phi$.

Proposition 2.5 (Computing σ -reflex algebras). *We summarize some results which allow for the computation of σ -reflex algebras.*

1. Let E be a field with σ an involution of E and let ϕ be a σ -type of E . Then $E^\phi = \widetilde{E}^\phi$ as above.
2. Let F be an étale algebra and let $(E, \sigma) = (F \times F, \sigma)$, where σ interchanges the factors F . Then there are a number of different σ -types of E :
 - (a) Let $\phi = \text{Hom}(F, \bar{k}) \subset \text{Hom}(F \times F, \bar{k})$ correspond to maps on the first factor. Then $E^\phi = k \times k$ where σ acts by interchanging factors.
 - (b) Fix one element $\rho \in \text{Hom}(F, \bar{k})$ and set $\phi = (\text{Hom}(F, \bar{k}) \setminus \{\rho\}) \cup \{\rho \circ \sigma\}$. Then $E^\phi = \rho(F) \times \rho(F)$ where σ acts by interchanging factors.
 - (c) More generally one any choice of $S \subset \text{Hom}(F, \bar{k})$ one can take $\phi = (\text{Hom}(F, \bar{k}) \setminus S) \cup S\sigma$. Then $E^\phi = L \times L$ where σ acts by interchanging factors and where $L = \widetilde{E}^\phi \subseteq \bigcup_{\rho \in S} \text{im}(\rho)$.
3. Let (E_1, σ_1) and (E_2, σ_2) be algebras with involutions. A σ -type for $(E, \sigma) = (E_1 \times E_2, \sigma_1 \times \sigma_2)$ is of the form $\phi = \phi_1 \sqcup \phi_2$, where the ϕ_i are σ_i -types for E_i . Then $\widetilde{E}^\phi \simeq \widetilde{E}_1^{\phi_1} \widetilde{E}_2^{\phi_2}$ and so the factors of E^ϕ are the composite of those of the $E_i^{\phi_i}$.

Proof. In each case the proof amounts to a direct application of Proposition 2.3 together with a computation of Γ_ϕ . For case (1), where E is a field, Proposition 2.3 is the complete result. For case (2) where $E = F \times F$ and the factors are interchanged by σ , we note that the orbits of Γ on $\text{Hom}_{k\text{-alg}}(E, \bar{k})$ can be decomposed into those factoring through the first F factor and those factoring through the second. Thus Γ_ϕ is just $\{\gamma \in \Gamma \mid \gamma S = S\}$ where $S \subset \text{Hom}(F, \bar{k})$ is the set describing ϕ as in each of the subcases of (2). It is then clear that Γ_ϕ contains $\bigcap_{\rho \in S} \text{Gal}(\bar{k}/\text{im}(\rho))$. From this one concludes the result in the special cases of $S = \emptyset$ or $S = \{\rho\}$. In case (3) where $E = E_1 \times E_2$, it is clear that $\Gamma_\phi = \Gamma_{\phi_1} \cap \Gamma_{\phi_2}$ which implies the result. \square

Corollary 2.6. *Write $(E, \sigma) = \times_i (E_i, \sigma_i)$ as a direct product where each $E_i^{\sigma_i}$ is a field. Then E^Φ is a product of even degree field extensions if and only if E_i is a field for at least one i .*

Proof. If every factor E_i is of the form $E_i^\sigma \times E_i^\sigma$ with σ_i interchanging factors then $E = F \times F$ for $F \simeq \times_i E_i^\sigma$ with σ interchanging factors. Then by the proposition above there exists ϕ with $E^\phi = k \times k$ and thus one of the direct factors of E^Φ is k .

Conversely, by the computations above every factor of \widetilde{E}^ϕ is formed as a composite extension of $\widetilde{E}_i^{\phi_i}$. If there exists a factor E_i which is a field then for all ϕ_i the field $\widetilde{E}_i^{\phi_i}$ is even degree. It follows that every factor of E^Φ contains an even degree subextension of the form $\widetilde{E}_i^{\phi_i}$ and so E^Φ is a product of even degree field extensions. \square

Proposition 2.7 (Localization of Reflex Algebras). *Suppose k is a number field, p be a prime of k (finite or infinite) and let k_p be the completion of k at p . By the localization of (E, σ) and (E^ϕ, σ) at p we mean the algebras $(E_p = E \otimes_k k_p, \sigma_p)$ and $((E^\phi)_p = E^\phi \otimes_k k_p, \sigma_p)$. Let $G = \text{Gal}(k_p/k_p) \setminus \Gamma / \Gamma_\phi$, then:*

$$(E^\phi)_p = \times_{\bar{g} \in G} (E_p)^{(g\phi)_p},$$

where g is any representative of the coset \bar{g} . In particular, $(E^\Phi)_p = (E_p)^{\Phi_p}$.

Proof. The idempotents of E_p and $(E^\phi)_p$ are in natural bijection with those of E and E^ϕ , respectively. That is, by fixing a single map $\bar{k} \hookrightarrow \bar{k}_p$ we obtain a Galois equivariant bijection $\text{Hom}_{k\text{-alg}}(E, \bar{k}) \simeq \text{Hom}_{k_p\text{-alg}}(E_p, \bar{k}_p)$ with respect to the associated inclusion $\Gamma_p = \text{Gal}(\bar{k}_p/k_p) \hookrightarrow \text{Gal}(\bar{k}/k)$. This naturally induces a bijection between the set of σ -types for (E, σ) and σ_p -types for (E_p, σ_p) . However, because Γ_p is only a subgroup of Γ , the Galois orbit of ϕ_p in Φ_p under Γ_p may be strictly smaller than the Galois orbit of ϕ in Φ under Γ . Hence, it may happen that $(E_p)^{\phi_p} \neq (E^\phi)_p$. In order to capture all of the orbits recall $G = \Gamma_p \backslash \Gamma / \Gamma_\phi$ so that:

$$\Gamma\phi = \bigsqcup_{\bar{g} \in G} \Gamma_p(g\phi),$$

where g is any representative of the coset \bar{g} . It follows that:

$$(E^\phi)_p = \prod_{\bar{g} \in G} (E_p)^{(g\phi)_p}.$$

□

2.2. Algebraic Tori

We now recall some basic properties of algebraic tori in linear algebraic groups.

Definition 2.8. A k -algebraic group is an **algebraic torus** T if it satisfies any of the following equivalent properties (see [Bor91, 8.4 and 8.5] for a proof of the equivalence):

1. T is connected and diagonalizable over \bar{k} .
2. T is connected, abelian and all its elements are semisimple.
3. $\bar{k}[T]$ is spanned by $X^*(T) = \text{Hom}_{\bar{k}}(T, \mathbb{G}_m)$.
4. $T_{\bar{k}} \simeq \mathbb{G}_m^n$ for some n .

Given any k -rational representation of T into GL_m there exists a collection $\Omega \subset X^*(T)$ of characters that appear once the representation is diagonalized over \bar{k} . We may consider the map:

$$T_{\bar{k}} \rightarrow \prod_{\chi \in \Omega} \mathbb{G}_m \quad t \mapsto (\chi(t))_{\chi \in \Omega}$$

where the natural Galois action of Γ on T is by permuting the χ as per the action of Γ on $X^*(T)$. The descent data needed to recover the isomorphism class of a k -torus of rank n from its \bar{k} -isomorphism with \mathbb{G}_m^n is the specification of the Galois action on $X^*(T) \simeq \mathbb{Z}^n$. See [PR94, 2.2.4] for a discussion of Galois descent as it relates to the classification of tori. The key result is:

Proposition 2.9. *There exists a contravariant equivalence of categories between k -isomorphism classes of algebraic tori of rank n and $\mathbb{Z}[\Gamma]$ -modules which as \mathbb{Z} -modules are torsion free and of rank n . The equivalence takes $T \mapsto X^*(T)$.*

Specifying a Galois action on $X^*(T)$ is equivalent to specifying the Galois action on any Galois stable spanning set $\Omega \subset X^*(T)$, in particular those spanning sets arising from faithful representations. Moreover, for a fixed reductive group G of rank n and for any two \bar{k} -conjugate tori $T_1, T_2 \subset G$, the sets $\Omega_{T_1}, \Omega_{T_2}$ can be identified (non-canonically). In particular, to classify the k -isomorphism classes of maximal tori contained in G , it suffices to consider a single such spanning set $\Omega \subset \mathbb{Z}^n$. Then any k -torus in G gives a Galois action on Ω which in turn gives rise to a representation $\Gamma \rightarrow \text{GL}_n(\mathbb{Z})$. One may then study the tori knowing only that they arise from a Γ -set Ω which spans \mathbb{Z}^n . One should note that the condition $T \subset G$ may impose further conditions on which Γ -actions on Ω are possible.

Proposition 2.10. *Let Ω be a finite Γ -invariant set of generators of $X^*(T)$. Let $E = E_\Omega$ be the étale algebra whose idempotents are the Γ -set Ω . Consider the torus $T_E := \text{Res}_{E/k}(\mathbb{G}_m)$, that is, the torus such that for any k -algebra R we have $T_E(R) = (E \otimes R)^*$. Then $T \hookrightarrow T_E$.*

Proof. First we note that $X^*(T_E) = \mathbb{Z}^\Omega$. We thus obtain a natural \mathbb{Z} -linear map from $X^*(T_E) \rightarrow X^*(T)$ by taking Ω , the basis of $X^*(T_E)$, to Ω as a spanning set of $X^*(T)$. This map is surjective and Γ -equivariant thus inducing a surjective map $k[T_E] \rightarrow k[T]$ which corresponds to an injective map $T \hookrightarrow T_E$. □

Definition 2.11. If E is an étale algebra over k we say a k -torus S is of **type** E if $S \hookrightarrow T_E$ and E contains no proper subalgebras with this property.

Note that any embedding of $S \hookrightarrow T_E$ (where S is of type E) arises as above. To see this consider the representation of S arising from the regular representation of T_E on E . Note also that the Galois closure of the composition of fields which comprise E is a minimal splitting field for the torus S .

Example. Let $L \subset E$ be étale algebras over k and consider $\chi \in \text{Hom}_k(T_E, T_L)$ corresponding to $\chi = N_{E/L}$, then $\text{Ker}(\chi)^0 \subset T_E$ is a torus of type E .

Definition 2.12. Let (E, σ) be an étale algebra with involution over k and put $\chi = N_{E/E^\sigma}$. Then we define:

$$T_{E,\sigma} = \text{Ker}(\chi)^0 = \{t \in T_E \mid t\sigma(t) = 1\}.$$

We remark that under the natural action of T_E on E as a k -vector space, $T_{E,\sigma}$ preserves the bilinear forms defined by:

$$B_{E,\sigma,\lambda}(x, y) = \text{Tr}_{E/k}(\lambda x \sigma(y)),$$

where $\lambda \in E^\sigma$. Moreover, $T_{E,\sigma}$ is a maximal torus in the orthogonal group attached to this bilinear form.

In the case where E is of dimension $2n + 1$ but E^σ has dimension n , we find that $E = E' \times k$, where σ acts trivially on the k summand. The only difference with the even case is that one must then take the connected component of the identity to ensure the resulting group is connected.

Proposition 2.13. *Let q be a quadratic form over k and let O_q be the associated orthogonal group. Let $T \subset O_q$ be a maximal k -torus. Then there exists an étale algebra with involution (E, σ) over k such that $T = T_{E,\sigma}$. Moreover, suppose $T_{E,\sigma} \subset O_q$ is a maximal torus. Then $q(x) = q_{E,\lambda}(x) = \frac{1}{2} \text{Tr}_{E/k}(\lambda x \sigma(x))$ for some choice of $\lambda \in (E^\sigma)^*$.*

Proof. We shall give a sketch of the construction that all tori are of this form, for details see [BCKM03, Prop. 3.3]. As in the discussion relating descent data of tori to étale algebras we observe that for any $T \subset O_q$ the set of characters Ω_T which appear in the representation is of the form:

$$\Omega_T = \{\chi_1, \dots, \chi_n, \chi_1^{-1}, \dots, \chi_n^{-1}\}$$

(including also the trivial character with multiplicity one if $\dim(q)$ is odd) with the χ_i forming a basis of $X^*(T)$. One checks easily that on the étale algebra E which has idempotents indexed by Ω_T one can construct an involution σ by interchanging χ_i and χ_i^{-1} for each i . It is straightforward to check that $T \cong T_{E,\sigma}$, and σ restricts to the adjoint involution with respect to q .

The statement concerning the structure of quadratic forms preserved by such tori is the content of any of [Shi80, Prop. 5.4], [BCKM03, Prop. 3.9] and [Fio09, Thm. 4.4.1]. We present the argument of [BCKM03]. By interpreting the quadratic space as a rank one E -module, we may consider the adjoint maps for the two quadratic forms (that is, q and $q_{E,1}$), both of which are preserved by T , as being isomorphisms from E to its linear dual. Hence, composing one with the inverse of the other, $\alpha = \text{ad}(q_{E,1})^{-1} \circ \text{ad}(q) : E \rightarrow E$ gives an E -automorphism of E which must correspond to multiplication by a unit λ . We may then conclude that $q = q_{E,\lambda}$. \square

2.3. Clifford Algebras

Definition 2.14. Let (V, q) be a quadratic space over k . We define the associated **Clifford algebra** to be:

$$C_q = \bigoplus_{i \geq 0} V^{\otimes i} / \langle x \otimes x - q(x) \rangle.$$

The involution $v \mapsto -v$ on V induces an involution of C_q . We define the even and odd parts of the Clifford algebra to be respectively the $+1$ and -1 eigenspaces for this involution and denote them C_q^0 and C_q^1 .

The structure of the Clifford algebra as a graded algebra is well known; in particular we have:

Theorem 2.15. *If $m = \dim(V)$ is odd then:*

1. $Z(C_q) \simeq k(\sqrt{d})$, where $d = (-1)^{(m-1)/2} D(q)$ and $D(q)$ is the discriminant of q ,
2. C_q^0 is a central simple algebra over k and $C_q \simeq C_q^0 \hat{\otimes} Z(C_q)$ (where $\hat{\otimes}$ is the graded tensor product), and
3. C_q is a central simple algebra over $Z(C_q)$ (if the centre is not a field we mean $C_q \simeq C_q^0 \times C_q^0$).

If $m = \dim(V)$ is even then:

1. C_q is a central simple algebra over k ,
2. $Z(C_q^0) = k(\sqrt{d})$, where $d = (-1)^{m/2} D(q)$ and $D(q)$ is the discriminant of q , and
3. if $C_q \simeq M_t(A)$ (where A is a division algebra) then $C_q^0 \simeq M_{t/2}(A \otimes Z(C_q^0))$.

Proof. The above theorem is essentially the content of [Lam05, V.2.4-5]. The final statement in the even case is not explicitly stated in [Lam05] but follows from the proof of [Lam05, IV.3.8]. \square

Definition 2.16. Let (V, q) be a non-degenerate quadratic space over k of dimension m with an orthogonal basis $\{e_i\}$, where we write $q(e_i) = a_i$. We then define the following invariants:

- The **discriminant** $D(q) = \prod_i a_i$ viewed as an element of $k^*/(k^*)^2$.
- The **Hasse invariant** $H(q) = \prod_{i < j} (a_i, a_j)$, where (a_i, a_j) is the Hilbert symbol (see [Ser73, Ch. III] and [Ser79, Ch. XIV]), viewed as an element of $\text{Br}(k) = H^2(\Gamma, \pm 1)$.
- The **Witt invariant** $W(q) = \begin{cases} [C_q^0], & m \equiv 1 \pmod{2}, \\ [C_q], & m \equiv 0 \pmod{2} \end{cases}$, where $[B]$ denotes the Brauer class of B , viewed as an element of $\text{Br}(k) = H^2(\Gamma, \pm 1)$.
- The **signature** $(r_\rho, s_\rho)_\rho$ at each real infinite place ρ of k .
- The **orthogonal discriminant** $D^{\text{orth}}(q) = \delta(Z(C_q^0)/k)$ viewed as an element of $k^*/(k^*)^2$.
- The **orthogonal Witt invariant** $W^{\text{orth}}(q) = [C_q^0]$ viewed as an element of $\text{Br}(Z(C_q^0))$.

Remark. The first four invariants are properly invariants of q , indeed when k is a number field they entirely determine q . The latter three are invariants of the orthogonal group associated to q . That is, O_q determines q only up to similarity (rescaling by k^*). Likewise, the signature, orthogonal discriminant and orthogonal Witt invariant determine q up to similarity.

The last two invariants are not standard.

Proposition 2.17. *Let $m = \dim(V)$. We have the following relations among the above invariants:*

1. $D(q) = \begin{cases} (-1)^{(m-1)/2} \delta(Z(C_q)), & m \equiv 1 \pmod{2}, \\ (-1)^{m/2} \delta(Z(C_q^0)), & m \equiv 0 \pmod{2}, \end{cases}$
2. $H(q) = W(q) \cdot (-1, D(q))^{(m-1)(m-2)/2} \cdot (-1, -1)^{(m+1)m(m-1)(m-2)/8}$, where the product is in the Brauer group,
3. $W^{\text{orth}}(q) = [W(q) \otimes Z(C_q^0)]$.

These properties are the content of [Lam05, V.2.5, V.3.20 and V.2.4-5], respectively.

Theorem 2.18. *Let (E, σ) be an étale algebra with involution over k such that $T_{E, \sigma} \hookrightarrow O_q$ as a maximal subtorus. Then E^Φ embeds into C_q^0 as a maximal étale algebra stable under the canonical involution of C_q . Moreover, the canonical involution restricts to σ on E^Φ .*

Proof. We claim that it is sufficient to consider the case of $\dim(V)$ even. Indeed, if $\dim(V)$ is odd then we can decompose $V = V' \oplus \text{span}_k(\vec{v})$ where $T_{E, \sigma}$ acts trivially on \vec{v} . With $q' = q|_{V'}$ and $T_{E, \sigma} \hookrightarrow O_{q'}$ and using that $C_{q'} \hookrightarrow C_q$ we obtain the result.

We may identify the space V with E . Thus $V \otimes_k \bar{k}$ is identified with $E \otimes_k \bar{k}$. Suppose under the isomorphism of V with E we have that $q(x) = \frac{1}{2} \text{Tr}_{E/k}(\lambda x \sigma(x))$. We use $\{e_\rho\}_{\rho \in \text{Hom}_{k\text{-alg}}(E, \bar{k})}$ as the generators for the Clifford algebra after base change to \bar{k} . We note that we recover both C_q^0 and V as the Galois invariants of $C_q^0 \otimes_k \bar{k}$ and $V \otimes_k \bar{k}$, respectively. Moreover, as the inclusion $V \hookrightarrow C_q$ is k -rational, the Galois actions on the $\{e_\rho\}$ viewed as elements of $V \otimes_k \bar{k}$ or as elements of $C_q \otimes_k \bar{k}$ is the same.

For each $\rho \in \text{Hom}_{k\text{-alg}}(E, \bar{k})$ set $\delta_\rho = \frac{1}{\rho(\lambda)} e_\rho \otimes e_{\rho \circ \sigma} \in C_q^0$. These elements satisfy the following properties:

1. The action of σ on δ_ρ agrees with the canonical involution of C_q ,
2. $\delta_\rho^2 = \delta_\rho$,
3. $\delta_\rho \sigma(\delta_\rho) = 0$ and $\delta_\rho + \sigma(\delta_\rho) = 1$,
4. the δ_ρ all commute, and
5. the Galois action on $\{\delta_\rho\}$ is the same as that on $\{e_\rho\}$.

Now for each σ -type $\phi \in \Phi$ of E set $\delta_\phi = \prod_{\rho \in \phi} \delta_\rho$. These elements then satisfy the following properties:

1. $\delta_\phi^2 = \delta_\phi$,
2. $\delta_{\phi_1} \delta_{\phi_2} = 0$ for $\phi_1 \neq \phi_2$,
3. $\sum_\phi \delta_\phi = \prod_\rho (\delta_\rho + \delta_{\rho \circ \sigma}) = 1$, and
4. the Galois action on $\{\delta_\phi\}_{\phi \in \Phi}$ is the same as that on $\{\phi\}_{\phi \in \Phi}$.

Thus the δ_ϕ are Galois stable orthogonal idempotents and hence by taking Galois invariants give an étale subalgebra of C_q^0 . As the Galois action on idempotents matches that of E^Φ , this gives an embedding of E^Φ into C_q^0 . Moreover, this algebra is preserved by the canonical involution of C_q , and the involution restricts to σ on it.

The algebra is maximal as an étale subalgebra for dimension reasons. \square

Remark. We have the map $\varphi : E \rightarrow C_q^0$ given by:

$$\varphi \left(\sum_{\rho} x_{\rho} e_{\rho} \right) = \sum_{\phi \in \Phi} \left(\prod_{\rho \in \phi} x_{\rho} \right) \delta_{\phi} = \prod_{\rho \in \phi'} (x_{\rho} \delta_{\rho} + x_{\rho \circ \sigma} \delta_{\rho \circ \sigma})$$

where ϕ' is any σ -reflex type of E . It is a multiplicative map (it is the reflex norm followed by the inclusion). Moreover, the image of $T_{E,\sigma}$ lies in the spin group, with φ being a section of the natural covering map $\theta : \text{Spin}_q \rightarrow \text{O}_q$. Indeed, we have $\theta(\varphi(\sum_{\rho} x_{\rho} e_{\rho}))(1_E) = \sum_{\rho} x_{\rho} x_{\rho \circ \sigma}^{-1} e_{\rho}$. Note that $T_{E,\sigma}$ consists of those elements where $x_{\rho} = x_{\rho \circ \sigma}^{-1}$, and hence $\theta \circ \phi = x^2$ on $T_{E,\sigma}$.

3. Computing Invariants

In this section we will compute the invariants of the forms $\text{Tr}_{E/k}(\lambda x \sigma(x))$.

Recall that for L/F a finite extension of fields and \mathcal{O} an order of L , the discriminant $\delta_{\mathcal{O}/\mathcal{O}_F}$ of \mathcal{O} is that of the F -quadratic form $Q(x) = \text{Tr}_{L/F}(x^2)$ on \mathcal{O} .

Lemma 3.1. *Let F be a number field or a p -adic field and let $L = F(z)$ be an algebraic extension of degree m with $f_z(X) \in \mathcal{O}_F[X]$ the minimal (monic) polynomial of z . Let $\delta_{L/F}(z)$ be the discriminant of the order $\mathcal{O}_F[z] \subset L$. Let $\lambda \in L^*$ and consider the quadratic form $Q(x) = \text{Tr}_{L/F}(\lambda x^2)$. Then:*

$$\begin{aligned} D(Q) &= N_{L/F}(\lambda) \delta_{\mathcal{O}_F[z]/\mathcal{O}_F}(z) \\ &= N_{L/F}(\lambda) \left(\prod_{i < j} (\rho_i(z) - \rho_j(z)) \right)^2 \\ &= N_{L/F}(\lambda) (-1)^{m(m-1)/2} N_{L/F}(f'_z(z)), \end{aligned}$$

where ρ_i are the m embeddings $L \hookrightarrow \overline{F}$.

Proof. These are well-known equalities. To compute $\det(\text{Tr}_{L/F}(\lambda z^{\ell} z^j))_{\ell j}$ factor the matrix as:

$$(\text{Tr}_{L/F}(\lambda z^{\ell} z^j))_{\ell j} = (\rho_i(\lambda z^{\ell}))_{\ell i} \cdot (\rho_i(z^j))_{ij} = \text{diag}(\rho_i(\lambda)) \cdot (\rho_i(z)^{\ell})_{\ell i} \cdot (\rho_i(z)^j)_{ij}.$$

By applying the Vandermonde determinant formula and a comparing the result to $N_{L/F}(f'_z(z))$ yields the result. \square

Lemma 3.2. *Let L/F be an extension of either number fields or local fields. The corestriction (or transfer map) $\text{Cor}_{L/F} : \text{Br}(L)[2] \rightarrow \text{Br}(F)[2]$ satisfies:*

$$\text{Cor}_{L/F}((a, b)_L) = (a, N_{L/F}(b))_F$$

for all $a \in F^*, b \in L^*$.

This is [Ser79, Ex. XIV.3.4].

The second part of the following result is the main theorem of the paper of Brusamarello–Chuard–Koulmann–Morales and will be important in the sequel.

Theorem 3.3. *Let (E, σ) be an étale algebra with involution over k of dimension $2n$ and let $\lambda \in E^{\sigma*}$. Then the invariants of $q_{E,\lambda}(x) = \frac{1}{2} \text{Tr}_{E/k}(\lambda x \sigma(x))$ are:*

1. $D(q_{E,\lambda}) = (-1)^n \delta_{E/k}$,
2. $H(q_{E,\lambda}) = H(q_{E,1}) \cdot \text{Cor}_{E^{\sigma}/k}(\lambda, \delta_{E/E^{\sigma}})$,
3. $W(q_{E,\lambda}) = W(q_{E,1}) \cdot \text{Cor}_{E^{\sigma}/k}(\lambda, \delta_{E/E^{\sigma}})$.

Proof. The first statement is well known, though we include a proof for the convenience of the reader. By writing $E = E^\sigma(\sqrt{d}) := E^\sigma[y]/(y^2 - d)$ we may write $x \in E$ as $x = s + t\sqrt{d}$. Then we observe that $q_{E,\lambda}(x) = \text{Tr}_{E^\sigma/k}(\lambda s^2) + \text{Tr}_{E^\sigma/k}(-\lambda dt^2)$. Set $Q_\lambda(s) = \text{Tr}_{E^\sigma/k}(\lambda s^2)$ and $Q_{-\lambda d}(t) = \text{Tr}_{E^\sigma/k}(-\lambda dt^2)$ so that $q_{E,\lambda} \simeq Q_\lambda \oplus Q_{-\lambda d}$. We thus have $D(q_{E,\lambda}) = D(Q_\lambda)D(Q_{-\lambda d})$. By Lemma 3.1 this gives:

$$\begin{aligned} D(q_{E,\lambda}) &= N_{E^\sigma/k}(\lambda) \cdot \delta_{E^\sigma/k} \cdot N_{E^\sigma/k}(-\lambda d) \cdot \delta_{E^\sigma/k} \\ &= N_{E^\sigma/k}(-d) = (-1)^n N_{E^\sigma/k}(d) \pmod{(k^*)^2}. \end{aligned}$$

By observing that $\delta_{E/k} = N_{E^\sigma/k}(\delta_{E/E^\sigma})\delta_{E^\sigma/k}^2$ (see [Ser79, Prop. III.4.8]) and that $\delta_{E^\sigma(\sqrt{d})/E^\sigma} = d \pmod{(k^*)^2}$ we conclude the result.

The second statement is the content of [BCKM03, Thm. 4.3]. The final statement follows from the first two statements by using Proposition 2.17. The proposition states that the Hasse and Witt invariants differ by a constant depending only on the discriminant. As $D(q_{E,\lambda}) = D(q_{E,1})$ the second and third statement are thus equivalent. \square

The above theorem, together with some easy special cases, is largely sufficient for the proof of our main result (see the proof of Lemma 5.5 for how it comes into play). However, we would like to give more precise formulas for the Hasse and Witt invariants that can be directly computed from the data describing the fields. This has the advantage of giving the information we need in the special cases, as well as being of interest in its own right. The first step is a lemma which is useful for explicitly calculating traces.

Lemma 3.4 (Euler). *Let $L = F(z)$ be a finite separable extension of F of degree m with $f_z(x) \in \mathcal{O}_F[x]$ the minimal (monic) polynomial of z . We then have:*

$$\text{Tr}_{L/F} \left(\frac{z^\ell}{f'_z(z)} \right) = \begin{cases} 1, & \ell = m - 1 \\ 0, & 0 \leq \ell < m - 1. \end{cases}$$

This is [Ser79, III.6, Lem. 2].

The next step is to show that the fields in which we are interested are always primitively generated in a simple way.

Proposition 3.5. *Let F/k be any finite separable extension of infinite fields of characteristic not 2, and let E/F be a quadratic extension. Then there exists $\alpha \in E$ such that $E = k(\alpha)$ and $F = k(\alpha^2)$.*

Proof. Suppose $E = F(\sqrt{\beta})$ with $\beta \in F$ and $F = k(\gamma)$. We claim it suffices to show that there exists an $\ell \in k$ such that $F = k((\ell + \gamma)^2\beta)$. Indeed, if $F = k((\ell + \gamma)^2\beta)$ then $F \subset k((\ell + \gamma)\sqrt{\beta})$ and so $\gamma \in k((\ell + \gamma)\sqrt{\beta})$. Hence $\sqrt{\beta} \in k((\ell + \gamma)\sqrt{\beta})$ and thus $F(\sqrt{\beta}) = k((\ell + \gamma)\sqrt{\beta})$. Consequently, taking $\alpha = (\ell + \gamma)\sqrt{\beta}$ gives the result.

Now let $\ell_1, \ell_2, \ell_3 \in k$ be distinct values such that $k((\ell_i + \gamma)^2\beta)$ are all the same field, say L . Since all these values are in the same field, so are their linear combinations. We compute that:

$$\frac{(\ell_1 + \gamma)^2\beta}{(\ell_2 - \ell_1)(\ell_3 - \ell_1)} + \frac{(\ell_2 + \gamma)^2\beta}{(\ell_1 - \ell_2)(\ell_3 - \ell_2)} + \frac{(\ell_3 + \gamma)^2\beta}{(\ell_1 - \ell_3)(\ell_2 - \ell_3)} = \beta.$$

This shows that $\beta \in L$. We then observe that:

$$\frac{1}{(\ell_2 - \ell_1)} ((\ell_2 + \gamma)^2 - (\ell_1 + \gamma)^2) - \ell_2 - \ell_1 = 2\gamma.$$

This proves that $\gamma \in L$, and hence $L = F = k((\ell_1 + \gamma)^2\beta)$. \square

The following lemma combines the above two results to show that for a particular choice of $\lambda \in E^\sigma$ the invariants of $q_{E,\lambda}$ can be computed explicitly.

Lemma 3.6. *Let F/k be an extension of number fields of degree m . Suppose $F = k(z)$. Let $E = F(\sqrt{z}) = k(\sqrt{z})$ and σ be the non-trivial element of $\text{Gal}(E/F)$. Let f_z be the minimal (monic) polynomial for z over k . View E as a $2m$ -dimensional k -vector space equipped with the quadratic form $Q(x + y\sqrt{z}) = q_{E,-f'_z(z)^{-1}}(x + \sqrt{z}y)$. Then:*

1. $H(Q) = (-1, -1)_k^{m(m-1)/2} \cdot (N_{F/k}(z), -1)_k^{m-1}$, and
2. $W(Q) = 1$.

Proof. Let $\tilde{E} = F(\sqrt{-z}) = k(\sqrt{-z})$ and notice that $f_{\sqrt{-z}}(X) = f(-X^2)$ is the minimal polynomials of $\sqrt{-z}$. Hence $f'_{\sqrt{-z}}(X) = -2X f'_z(-X^2)$, in particular $f'_{\sqrt{-z}}(\sqrt{-z}) = -2\sqrt{-z} f'_z(z)$. Therefore under the identification of $F \times F$, using its natural basis, with \tilde{E} under the basis $1, \sqrt{-z}$ and writing $w = x + y\sqrt{-z}$ we compute:

$$\begin{aligned} q_{E, -f'_z(z)^{-1}}(x + \sqrt{z}y) &= \text{Tr}_{F/k} \left(\frac{-1}{f'_z(z)} (x^2 - zy^2) \right) \\ &= \text{Tr}_{\tilde{E}/k} \left(\frac{-1}{2f'_z(z)} w^2 \right) \\ &= \text{Tr}_{\tilde{E}/k} \left(\frac{\sqrt{-z}}{f'_{\sqrt{-z}}(\sqrt{-z})} w^2 \right). \end{aligned}$$

Now, by Lemma 3.4, for any extension $k(\alpha)/k$ of degree n , the matrix for the quadratic form

$$\tilde{Q}(x) = \text{Tr}_{k(\alpha)/k} \left(\frac{\alpha}{f'_\alpha(\alpha)} x^2 \right)$$

in the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ has the shape:

$$\begin{pmatrix} 0 & \cdots & 1 & a_1 \\ & & 1 & a_1 & a_2 \\ \vdots & \ddots & & & \\ & 1 & \ddots & & \vdots \\ 1 & a_1 & & & \\ a_1 & a_2 & \cdots & & a_n \end{pmatrix},$$

for some values $a_i \in k$. Note that the form is non-degenerate on the span of $\{1, \alpha, \dots, \alpha^{n-2}\}$ and let β be a generator for the orthogonal complement. Then $\{1, \alpha, \dots, \alpha^{n-2}, \beta\}$ is a basis and the matrix for \tilde{Q} with respect to it is:

$$A = \begin{pmatrix} 0 & \cdots & 1 & 0 \\ & & 1 & a_1 & 0 \\ \vdots & \ddots & & & \\ & 1 & \ddots & & \vdots \\ 1 & a_1 & & & \\ 0 & 0 & \cdots & & Y \end{pmatrix},$$

for some $Y \in k$.

Lemma 3.7. *The matrices:*

$$\begin{pmatrix} 0 & \cdots & 1 & \\ \vdots & \ddots & & \\ 1 & a_1 & \cdots & a_n \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & \cdots & 1 & \\ \vdots & \ddots & & \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

represent the same quadratic form. In particular, denoting by $\langle y_1, \dots, y_n \rangle$ the diagonal form with diagonals y_i , the quadratic form associated to either matrix is isomorphic to one of:

$$\langle 1, -1 \rangle^{\frac{n-1}{2}} \oplus \langle 1 \rangle \quad \text{or} \quad \langle 1, -1 \rangle^{\frac{n}{2}}$$

depending on the parity of n .

Proof. This is a simple inductive argument using the similarity-transform defined by:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ -a_1 & 1 & & \\ -a_2 & 0 & \ddots & \vdots \\ \vdots & & & \\ -a_{n-1} & & & \\ -\frac{1}{2}a_n & 0 & \cdots & 1 \end{pmatrix}.$$

□

It follows from the lemma that \tilde{Q} is isomorphic to one of:

$$\langle 1, -1 \rangle_k^{\frac{n-2}{2}} \oplus \langle 1, Y \rangle \quad \text{or} \quad \langle 1, -1 \rangle_k^{\frac{n-1}{2}} \oplus \langle Y \rangle.$$

Next, by Lemma 3.1 we know that the discriminant of \tilde{Q} is:

$$N_{k(\alpha)/k}(\alpha)N_{k(\alpha)/k}(f'_\alpha(\alpha)^{-1})\delta_{k(\alpha)/k} = N_{k(\alpha)/k}(\alpha)(-1)^{n(n-1)/2}.$$

We conclude that $Y = N_{k(\alpha)/k}(\alpha)(-1)^{n-1}$ up to squares. In particular, in the case $\alpha = \sqrt{-z}$, we can immediately see that the Hasse invariant of the quadratic form is:

$$\begin{aligned} H(Q) &= (-1, -1)_k^{m(m-1)/2} \cdot (N_{k(\sqrt{-z})/k}(\sqrt{-z}), -1)_k^{m-1} \\ &= (-1, -1)_k^{m(m-1)/2} \cdot (N_{k(z)/k}(z), -1)_k^{m-1}. \end{aligned}$$

Moreover, since the quadratic form has discriminant $(-1)^m N_{k(z)/k}(z)$ we compute using Proposition 2.17 that the Witt invariant is:

$$\begin{aligned} W(Q) &= ((-1)^m N_{k(z)/k}(z), -1)_k^{m-1} \cdot (-1, -1)_k^{m(m-1)/2} \\ &\quad (-1, -1)_k^{m(m-1)/2} \cdot (N_{k(z)/k}(z), -1)_k^{m-1} \\ &= 1. \end{aligned}$$

□

Combining the above two results, we may now give a general formula for the Hasse and Witt invariants for the forms $q_{E,\lambda}$.

Theorem 3.8. *Let $F = k(z)$ be an extension of degree m , let $E = k(\sqrt{z})$, and let $\lambda \in F$. Consider the quadratic form $q_{E,\lambda}(x) = \frac{1}{2} \text{Tr}_{E/k}(\lambda N_{E/F}(x))$. Then:*

1. $H(q_{E,\lambda}) = \text{Cor}_{F/k}((-\lambda f'_z(z), z)_F) \cdot (N_{k(z)/k}(z), -1)_k^{m-1} \cdot (-1, -1)_k^{m(m-1)/2}$, and
2. $W(q_{E,\lambda}) = \text{Cor}_{F/k}((-\lambda f'_z(z), z)_F)$.

Proof. From Theorem 3.3 we have the following two equations:

$$\begin{aligned} H(q_{E,\lambda}) &= H(q_{E,1}) \cdot \text{Cor}_{F/k}((\lambda, z)_F), \text{ and} \\ H(q_{E,-f'_z(z)^{-1}}) &= H(q_{E,1}) \cdot \text{Cor}_{F/k}((-f'_z(z), z)_F). \end{aligned}$$

Solving for $H(q_{E,1})$ and substituting the results of Lemma 3.6 yields:

$$\begin{aligned} H(q_{E,\lambda}) &= H(q_{E,-f'_z(z)^{-1}}) \cdot \text{Cor}_{F/k}(\lambda f'_z(z)) \\ &= (-1, -1)_k^{m(m-1)/2} \cdot (N_{F/k}(z), -1)_k^{m-1} \cdot \text{Cor}_{F/k}((-\lambda f'_z(z), z)_F). \end{aligned}$$

The Witt invariant computation follows similarly. □

4. Local Invariant Computations for $\text{Tr}(\lambda x^2)$

The above gives us a global cohomological description of the invariants of the quadratic forms in which we are interested. However, the quadratic forms $\text{Tr}(\lambda x^2)$, which were studied extensively by Serre (see [Ser84]) and others, are not in general covered by the previous section. Moreover, we have further interest in a detailed local description of these forms as this has applications to computing local densities and discriminant groups. Similar calculations can be found in the work of Epkenhans (see [Epk89, Lem. 1]). The current section gives a description of these quadratic forms in terms of basic combinatorial data regarding the ramification structure of the field extensions involved.

Lemma 4.1. *Let F/k be an unramified extension of non-Archimedean local fields of degree f , with residue characteristic different from 2. Let π_k be a uniformizer of k . Let Q_F be any quadratic form on a vector space V over F of dimension n . View V as a k -vector space via restriction of scalars. The form $Q_k(x) = \text{Tr}_{F/k}(Q_F(x))$ on V has invariants:*

$$D(Q_k) = N_{F/k}(D(Q_F))\delta_{F/k}^n, \text{ and}$$

$$H(Q_k) = H(Q_F) \left[(\pi_k, N_{F/k}(D(Q_F)))_k (\pi_k, \delta_{F/k})_k (\pi_k, -1)_k^{f(f-1)/2} \right]^{\nu_{\pi_F}(D(Q_F))}.$$

(By abuse of notation we identify the 2-torsion in the Brauer groups of F and k via the natural isomorphism.)

Proof. It suffices to check the formula for a member of each isomorphism class of quadratic space over V . If $n \geq 3$ by checking the Hasse invariants and discriminants one finds that every isomorphism class of non-degenerate quadratic space over V is represented by one of:

$$\langle 1 \rangle^{n-3} \oplus \langle b, \pi_k, ab\pi_k \rangle \quad \text{or} \quad \langle 1 \rangle^{n-2} \oplus \langle b, ab\pi_k \rangle,$$

for some $a, b \in \mathcal{O}_F^*$. We refer to these as the first and second cases. In either case by decomposing the form into the diagonal pieces with trivial and non-trivial valuations we may write:

$$\text{Tr}_{F/k}(Q_F) \cong M_1 \oplus \pi_k M_2.$$

In the first case, M_1 has discriminant $\delta_{F/k}^{n-2} N_{F/k}(b)$ and dimension $f \cdot (n-2)$, whereas M_2 has discriminant $N_{F/k}(ab)$ and dimension $2f$. One then computes in the first case that:

$$\begin{aligned} H(Q_k) &= (\pi_k, -1)_k^f \cdot (N(ab), \pi_k)_k \\ &= (\pi_k, -1)_F \cdot (ab, \pi_k)_F \\ &= H(Q_F). \end{aligned}$$

In the second case, M_1 has discriminant $\delta_{F/k}^{n-1} N_{F/k}(b)$ and M_2 has discriminant $\delta_{F/k} N_{F/k}(ab)$. Thus we have:

$$\begin{aligned} H(Q_k) &= (\pi_k, N_{F/k}(b))_k \cdot (\pi_k, N_{F/k}(a))_k^{f-1} \cdot (\pi_k, \delta_{F/k})_k^{fn-1} \cdot (\pi_k, -1)_k^{f(f-1)/2} \\ &= (\pi_k, N_{F/k}(a))_k^{f-1} \cdot (\pi_k, \delta_{F/k})_k \cdot (\pi_k, -1)_k^{f(f-1)/2} \\ &= H(Q_F) \left[(\pi_k, N_{F/k}(D(Q_F)))_k \cdot (\pi_k, \delta_{F/k})_k \cdot (\pi_k, -1)_k^{f(f-1)/2} \right]. \end{aligned}$$

Here we have used the fact that $\delta_{F/k}^f$ is a square in k for an unramified extension.

For the cases $n = 1, 2$ we must check that similar formulas hold for: $\langle b\pi_k, ab\pi_k \rangle, \langle 1, a \rangle, \langle a \rangle, \langle a\pi_k \rangle$. We omit these calculations. \square

The results on the structure of trace forms for ramified extensions will rely on the following lemma.

Lemma 4.2. *Let L/F be a totally ramified extension of local fields. Let $z = \pi_L$ be a uniformizer of \mathcal{O}_L and $f_z(x)$ be the minimal (monic) polynomial of z . Then f_z is an Eisenstein polynomial and the collection $1, z, z^2, \dots, z^{m-1}$ is an \mathcal{O}_F -basis of \mathcal{O}_L and $N_{L/F}(z)$ is a uniformizer of F .*

See [Ser79, Prop. I.6.18] for a proof.

Before proceeding with the next two lemmas we will introduce some notation. Let L/F be a totally ramified extension of local fields of degree m . Let π_L be a uniformizer of L and set $\pi_F = N_{L/F}(\pi_L)$ to be a uniformizer of F . Let $f = f_{\pi_L}$ be the minimal monic polynomial of π_L over F . Suppose $u \in \mathcal{O}_L^*, v \in \mathcal{O}_F^*, 0 \leq \ell \leq m, k \in \mathbb{Z}$ and set $\lambda = \frac{\pi_F^k}{uv^2 \pi_L^\ell f'(\pi_L)}$. We remark that if the residue characteristic is not 2, then for any given $\lambda \in L^*$ there exists corresponding u, v, ℓ, k . Now denote by $Q(x)$ the F -quadratic form on L given by $Q(x) = \text{Tr}_{L/F}(\lambda x^2)$ and consider $M_1 = \text{span}\{uvz^\ell, \dots, uvz^{m-1}\}$ and $M_2 = \text{span}\{v, \dots, vz^{\ell-1}\}$ as quadratic subspaces of L .

Lemma 4.3. *With the notation as above, we have the following properties of Q, M_1, M_2 :*

1. *The discriminant of Q is $D(Q) = (-1)^{m(m-1)/2} u^{-m} \pi_F^{mk-\ell}$.*
2. *The decomposition $L = M_1 \oplus M_2$ is orthogonal with respect to Q .*

3. The discriminants of $\frac{1}{\pi_F^k}Q|_{M_1}$ and $\frac{1}{\pi_F^{k-1}}Q|_{M_2}$ are respectively:

$$D\left(\frac{1}{\pi_F^k}Q|_{M_1}\right) = (-1)^{(m-\ell)(m-\ell-1)/2}u^{m-\ell} \text{ and}$$

$$D\left(\frac{1}{\pi_F^{k-1}}Q|_{M_2}\right) = (-1)^{\ell(\ell+1)/2-m\ell}u^{-\ell}.$$

Hence these forms are unimodular.

4. The Hasse invariant is:

$$H(Q) = (\pi_F, u)^{(m-\ell)\ell} \cdot (\pi_F, -1)^{k(m^2(m-1)/2+\ell^2(1-m))-\ell(m-\ell)(m-\ell-1)/2}.$$

Proof. The formula for the discriminant of Q is Lemma 3.1. The orthogonal decomposition is an elementary calculation which follows from Lemma 3.4 and Lemma 4.2.

Next, noticing that $u \in F$ we can use Lemma 3.4 to compute that the matrix representations of $\frac{1}{\pi_F^k}Q|_{M_1}$ and $\frac{1}{\pi_F^{k-1}}Q|_{M_2}$. We see that they are respectively:

$$u \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & 0 & 1 & * \\ \vdots & \ddots & & * & \\ & 0 & \ddots & \vdots & \\ 0 & 1 & * & & \\ 1 & * & \cdots & & * \end{pmatrix} \text{ and } \frac{1}{u} \begin{pmatrix} * & \cdots & * & a \\ & & a & 0 \\ \vdots & \ddots & & \vdots \\ * & a & 0 & \vdots \\ a & 0 & \cdots & 0 \end{pmatrix},$$

where $a = \frac{\pi_F}{f(0)} = (-1)^m$. One can explicitly calculate the $*$ terms from the coefficients of f , but what is of particular importance is that in both cases one finds that $a_{ij} = a_{lk}$ whenever $i + j = l + k$. As a consequence of this using Lemma 3.7 we can explicitly find a change of basis matrix so that the result is of form:

$$u \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & 0 & 1 & 0 \\ \vdots & \ddots & & 0 & \\ & 0 & \ddots & \vdots & \\ 0 & 1 & 0 & & \\ 1 & 0 & \cdots & & 0 \end{pmatrix} \text{ and } \frac{1}{u} \begin{pmatrix} X & 0 & \cdots & 0 \\ 0 & & & 0 & 1 \\ \vdots & \ddots & & 1 & 0 \\ & & \ddots & \vdots & \\ 0 & 0 & 1 & & \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}.$$

The determinants of the matrices are then:

$$(-1)^{(m-\ell)(m-\ell-1)/2}u^{m-\ell} \text{ and } (-1)^{(\ell-1)(\ell-2)/2}u^{-\ell}X,$$

respectively. Thus knowing $D(Q)$ we have that up to squares X is:

$$X = (-1)^{(\ell-1)(\ell-2)/2+\ell(\ell+1)/2-m\ell}u^{-\ell-m-\ell+m} = (-1)^{m\ell+1}.$$

The computation of the discriminants of the M_i and then the Hasse invariant of Q are direct calculations. \square

Remark. If the residue characteristic is not 2 the above gives us a method to calculate the invariants of forms $\text{Tr}_{L/F}(\lambda x^2)$ for an arbitrary λ .

We now restrict ourselves to the case that the residue characteristic is not 2. In addition to the above notation, suppose that E/L is a quadratic extension with involution σ . Fix w a non-square element of \mathcal{O}_F^* . Writing $x = x_1 + x_2\sqrt{\delta_{E/E^\sigma}}$ consider the quadratic form on E

$$q_{E/F,\lambda}(x) = \frac{1}{2} \text{Tr}_{E/F}(\lambda x \sigma(x)) \simeq \text{Tr}_{E^\sigma/F}(\lambda x_1^2) - \text{Tr}_{E^\sigma/F}(\lambda \delta_{E/E^\sigma} x_2^2).$$

Then set $\lambda' = \lambda \delta_{E/E^\sigma}$, $k' = k$ and choose u', v', ℓ' so that $\lambda' = \frac{\pi_F^k}{u'v'^2\pi_L^{\ell'}f'(\pi_L)}$. Let Q', M'_i be defined similarly to Q, M_i using λ' instead of λ so that $q_{E/F,\lambda}(x) = Q(x_1) - Q'(x_2)$. Now define $N_i = M_i \oplus -M'_i$ and $\widetilde{N}_1 = \frac{1}{\pi_F^k}N_1$ and $\widetilde{N}_2 = \frac{1}{\pi_F^{k-1}}N_2$ their unimodular rescalings.

Lemma 4.4. *With the notation as above we have the following:*

1. *If $\delta_{E/E^\sigma} = w$ then $\ell' = \ell$ and $u' = wu$. Then:*

$$D(\widetilde{N}_1) = (-1)^{\ell-m} w^{\ell-m} \text{ and } D(\widetilde{N}_2) = (-1)^{-\ell} w^{-\ell}.$$

It follows that:

$$\begin{aligned} D(q_{E/F,\lambda}(x)) &= (-1)^m w^m \pi_F^{2(mk-\ell)}, \text{ and} \\ H(q_{E/F,\lambda}(x)) &= (\pi_F, w)^{km-\ell}. \end{aligned}$$

2. *If $\delta_{E/E^\sigma} = \pi_{E^\sigma}$ then $\ell' = \ell - 1$ and $u' = u$. Then:*

$$D(\widetilde{N}_1) = (-1)u \text{ and } D(\widetilde{N}_2) = (-1)^{m+1}u.$$

It follows that:

$$\begin{aligned} D(q_{E/F,\lambda}(x)) &= (-1)^m \pi_F^{2(mk-\ell)+1}, \text{ and} \\ H(q_{E/F,\lambda}(x)) &= (\pi_F, u) \cdot (\pi_F, -1)^{k(\ell-m-1)+m+\ell(\ell+1)/2}. \end{aligned}$$

3. *If $\delta_{E/E^\sigma} = w\pi_{E^\sigma}$ then $\ell' = \ell - 1$ and $u' = wu$. Then:*

$$D(\widetilde{N}_1) = (-1)uw^{\ell-m+1} \text{ and } D(\widetilde{N}_2) = (-1)^{m-1}uw^{1-\ell}.$$

It follows that:

$$\begin{aligned} D(q_{E/F,\lambda}(x)) &= (-1)^m w^m \pi_F^{2(mk-\ell)+1}, \text{ and} \\ H(q_{E/F,\lambda}(x)) &= (\pi_F, u) \cdot (\pi_F, w)^{(m\ell-m-\ell^2-1)} \cdot (\pi_F, -1)^{k(\ell-m-1)+m+\ell(\ell+1)/2}. \end{aligned}$$

4. *If E^σ/F is still an extension of fields but $E = E^\sigma \times E^\sigma$, $\delta_{E/E^\sigma} = 1$, then $\ell' = \ell$ and $u' = u$. Then:*

$$D(\widetilde{N}_1) = (-1)^{\ell-m} \text{ and } D(\widetilde{N}_2) = (-1)^{-\ell}.$$

It follows that:

$$\begin{aligned} D(q_{E/F,\lambda}(x)) &= (-1)^m \pi_F^{2(mk-\ell)}, \text{ and} \\ H(q_{E/F,\lambda}(x)) &= 1. \end{aligned}$$

Proof. The proof is a direct, although tedious, calculation based on Lemma 4.3. □

Remark. By combining the results above for totally ramified extensions with those of Lemma 4.1 one obtains results for arbitrary extensions.

In the formulas above the parameter m is determined by the ramification degree of E^σ . The parameters k and ℓ are controlled together by both the higher ramification degrees of E^σ and the valuation of λ . Finally the square class of u is controlled by the square class of λ .

The following two lemmas are direct computations.

Lemma 4.5. *Let F/k be an extension of local fields of residue characteristic 2. Then when viewed as a quadratic form on $F \times F$ the Witt invariant of $\text{Tr}_{F/k}(x^2 - y^2)$ is 1.*

Lemma 4.6. *Let $F = \mathbb{R}$ or $F = \mathbb{C}$, then as a quadratic form on $F \times F$ the Witt invariants of $\text{Tr}_{F/\mathbb{R}}(x^2 + y^2)$ and $\text{Tr}_{F/\mathbb{R}}(x^2 - y^2)$ are 1, and the Witt invariant of $\text{Tr}_{F/\mathbb{R}}(-x^2 - y^2)$ is -1 .*

5. The Main Results

We recall the main result:

Theorem 5.1. *Let O_q be an orthogonal group over a number field k defined by a quadratic form q of dimension $2n$ or $2n + 1$, and let (E, σ) be a field extension of k with an involution and of dimension $2n$. Then O_q contains a torus of type (E, σ) if and only if the following three conditions are satisfied:*

1. *E^ϕ splits the even Clifford algebra $W^{\text{orth}}(q)$ for all σ -types ϕ of E .*
2. *If $\dim(q)$ is even then $\delta_{E/k} = (-1)^n D(q)$.*

3. Let ν be a real infinite place of k and let s be the number of homomorphisms from E to \mathbb{C} over ν for which σ corresponds to complex conjugation. The signature of q is of the form $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i)_\nu$ if the dimension is even and either $(n - \frac{s}{2} + 2i + 1, n + \frac{s}{2} - 2i)_\nu$ or $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i + 1)_\nu$ if $\nu((-1)^n D(q)\delta_{E/k})$ is respectively positive or negative when the dimension is odd, where $0 \leq i \leq \frac{s}{2}$.

Moreover, for any E satisfying condition (2) we have that $\sqrt{D(q)} \in E^\phi$ for every σ -type ϕ of E .

By Proposition 2.13 the entire theorem is reduced to showing that the conditions are equivalent to the existence of $\lambda \in (E^\sigma)^*$ such that the quadratic form $q_{E,\lambda} = \frac{1}{2} \text{Tr}_{E/k}(\lambda x \sigma(x))$ has the same invariants as q . We now proceed with a series of lemmas which will conclude with the result.

Lemma 5.2. *Let (E, σ) be an étale algebra over k with involution and let $\lambda \in E^\sigma$. For a real infinite place ν of k the quadratic form $q_{E,\lambda} = \frac{1}{2} \text{Tr}_{E/k}(\lambda x \sigma(x))$ has signature $(n + \frac{r}{2} - \frac{s}{2}, n - \frac{r}{2} + \frac{s}{2})_\nu$ where s (respectively r) is the number of real embeddings $\rho \in \text{Hom}_{k\text{-alg}}(E^\sigma, \mathbb{R})$ of E^σ which are ramified in E with $\rho(\lambda) > 0$ (respectively $\rho(\lambda) < 0$).*

Proof. This is an immediate check. □

Lemma 5.3. *Let F be a number field, let $e_\nu = \pm 1$ be a collection of numbers indexed by the places of F , and let $\delta \in F$. Then there exist $\lambda \in F$ with $(\lambda, \delta)_\nu = e_\nu$ if and only if the following three conditions are satisfied:*

1. All but finitely many e_ν are 1.
2. An even number of the e_ν are -1 .
3. For each ν there exists $\lambda_\nu \in F_\nu$ with $(\lambda_\nu, \delta)_{F_\nu} = e_\nu$.

Proof. This is well known. For the result over \mathbb{Q} see [Ser73, Thm. 2.2.4], for the result over an algebraic number field see [O'M00, 71:19a]. □

Corollary 5.4. *Let (E, σ) be an extension of a number field k of degree $2n$ together with an involution. For each place ν of k let $e_\nu \in \{\pm 1\}$, and for each infinite place let $(s_\nu, r_\nu)_\nu$ be such that $s_\nu, r_\nu \in \mathbb{N}$ and $s_\nu + r_\nu = 2n$. Then there exists $\lambda \in E^\sigma$ with $q_{E,\lambda}$ having signatures $(s_\nu, r_\nu)_\nu$ and Hasse invariants e_ν if and only if the following three conditions are satisfied:*

1. All but finitely many e_ν are 1.
2. An even number of the e_ν are -1 .
3. For each ν there exists $\lambda_\nu \in E_\nu^\sigma$ such that $H(q_{E_\nu, \lambda_\nu}) = e_\nu$ and moreover, the signature of q_{E_ν, λ_ν} is $(s_\nu, r_\nu)_\nu$ if ν is an infinite place of k .

Proof. Supposing there exists a λ , then conditions (1), (2) and (3) are immediate.

Let us prove the converse. For $\mu \in (E^\sigma)^*$ denote by $Q_{E/E^\sigma, \mu}(x) = \frac{1}{2} \text{Tr}_{E/E^\sigma}(\mu x \sigma(x))$ the E^σ -quadratic form on E . First we recall Theorem 3.3 tells us that:

$$H(q_{E, \mu})_\nu = H(q_{E, 1})_\nu \prod_{u|\nu} H(Q_{E/E^\sigma, \mu})_u,$$

where the u run over places of E^σ over ν . Now for each place u of E^σ define $f_u \in \{\pm 1\}$ as follows:

- If $u|\nu$ is an infinite place, set $f_u = H(Q_{E/E^\sigma, \lambda_\nu})_u$.
- If $u|\nu$ is a finite place and $H(q_{E, 1})_\nu e_\nu = 1$, set $f_u = 1$.
- If $u|\nu$ is a finite place and $H(q_{E, 1})_\nu e_\nu = -1$, set $f_u = H(Q_{E/E^\sigma, \lambda_\nu})_u$.

We now notice that for each place ν of k we have:

$$\prod_{u|\nu} f_u = \prod_{u|\nu} H(Q_{E_\nu/E_\nu^\sigma, \lambda_\nu})_u = H(q_{E, 1})_\nu H(q_{E_\nu, \lambda_\nu}) = H(q_{E, 1})_\nu e_\nu$$

and moreover, that only finitely many $f_u \neq 1$. It follows that $\prod_u f_u = \prod_\nu H(q_{E, 1})_\nu e_\nu = 1$. Finally we have that if $f_u \neq 1$ then $f_u = H(Q_{E/E^\sigma, \lambda_\nu})_\mu = (\lambda_\nu, \delta_{E/E^\sigma})_u$. The values f_u thus satisfy the conditions of Lemma 5.3 and we conclude that there exists $\lambda \in E^\sigma$ with $(\lambda, \delta_{E/E^\sigma})_u = f_u$. By the choices of the f_u we find:

$$H(q_{E, \lambda})_\nu = H(q_{E, 1})_\nu \prod_{u|\nu} H(Q_{E_\nu/E_\nu^\sigma, \lambda})_u = H(q_{E, 1})_\nu \prod_{u|\nu} f_u = e_\nu.$$

Finally, by Lemma 5.2 the signature of $q_{E,\lambda}$ at a real infinite place ν is given by:

$$\left(\frac{1}{2} \sum_{u|\nu} m_u(H(Q_{E_\nu/E_\nu^\sigma}, \lambda)_u + 1), \frac{1}{2} \sum_{u|\nu} m_u(H(Q_{E_\nu/E_\nu^\sigma}, -\lambda)_u + 1) \right),$$

where $m_u = 1$ if $E_u = \mathbb{R} \times \mathbb{R}$ and $m_u = 2$ if $E_u = \mathbb{C}$. Since $H(Q_{E_\nu/E_\nu^\sigma}, \lambda)_u = H(Q_{E_\nu/E_\nu^\sigma, \lambda_\nu})_u$ for all u it follows that the signature of $q_{E,\lambda}$ at ν is the same as that of q_{E_ν, λ_ν} , which is to say it is precisely $(s_\nu, r_\nu)_\nu$. \square

Lemma 5.5. *Let (E, σ) be an étale algebra with involution. Let $E_{\mathfrak{p}} = \times_i E_{\mathfrak{p}i}$ be a decomposition into a product of fields. Then there exists values $\lambda_+, \lambda_- \in E^\sigma$ such that the \mathfrak{p} -adic part of the Hasse invariant for $\frac{1}{2} \text{Tr}_{E/k}(\lambda_\pm x\sigma(x))$ is respectively $+1, -1$ if and only if the involution σ restricts to an automorphism of $E_{\mathfrak{p}i}$ for one of the constituent fields $E_{\mathfrak{p}i}$ of the étale algebra $E_{\mathfrak{p}}$. Moreover, if $W(q_{E,\lambda})_{\mathfrak{p}}$ is independent of λ then $W(q_{E,\lambda})_{\mathfrak{p}} = 1$ for all λ .*

Proof. From Theorem 3.3 recall that we have:

$$W(q_{E,\lambda}) = C_E \cdot \text{Cor}_{E^\sigma/k}((\lambda, \delta_{E/E^\sigma})_{E^\sigma}),$$

for some constant C_E which does not depend on λ . Thus, both λ_\pm exist if and only if $\text{Cor}_{E^\sigma/k_{\mathfrak{p}}}((\lambda, \delta_{E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma})_{E_{\mathfrak{p}}^\sigma})$ is not constant as a function of λ . Writing $E_{\mathfrak{p}}^\sigma = \times_j E_{\mathfrak{p}j}^\sigma$ let ρ_j be the projection of $E_{\mathfrak{p}}^\sigma$ onto the j th factor. Using the fact that the cohomology and the corestriction maps factor as products we have:

$$\text{Cor}_{E_{\mathfrak{p}}^\sigma/k_{\mathfrak{p}}}((\lambda, \delta_{E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma})_{E_{\mathfrak{p}}^\sigma}) = \prod_j \text{Cor}_{E_{\mathfrak{p}j}^\sigma/k_{\mathfrak{p}}}((\rho_j(\lambda), \rho_j(\delta_{E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma}))_{E_{\mathfrak{p}j}^\sigma}).$$

We thus conclude that both λ_\pm exist if and only if for at least one j the function $\text{Cor}_{E_{\mathfrak{p}j}^\sigma/k_{\mathfrak{p}}}((\rho_j(\lambda), \rho_j(\delta_{E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma}))_{E_{\mathfrak{p}j}^\sigma})$ is not constant with respect to λ . The corestriction map being injective for local fields, this is equivalent to $(\lambda_j, \rho_j(\delta_{E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma}))_{E_{\mathfrak{p}j}^\sigma}$ being non-constant. This last assertion is the same as saying that $\rho_j(\delta_{E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma})$ is a non-square or that σ acts as the non-trivial field automorphism on the factor $E_{\mathfrak{p}i}$ of $E_{\mathfrak{p}}$ that is over $E_{\mathfrak{p}j}^\sigma$.

For the second part, we need to show that whenever $W(q_{E,\lambda})_{\mathfrak{p}}$ is independent of λ then $W(q_{E,\lambda})_{\mathfrak{p}} = 1$. Indeed if $W(q_{E,\lambda})_{\mathfrak{p}}$ does not depend on λ , then by the first part of the lemma $E_{\mathfrak{p}}/E_{\mathfrak{p}}^\sigma$ has no factors which are field extensions. Thus the element z appearing in the formula in Theorem 3.8 is a square and this implies $W(q_{E,\lambda})_{\mathfrak{p}} = \text{Cor}_{E_{\mathfrak{p}}^\sigma/k_{\mathfrak{p}}}((-\lambda f'_z(z), z)_{E_{\mathfrak{p}}^\sigma}) = 1$. \square

Corollary 5.6. *Let E/k be an extension of number fields. Let q be a quadratic form of dimension $2n$. Then O_q has a torus of type (E, σ) if and only if the following three conditions are satisfied:*

1. *For all primes \mathfrak{p} of k where none of the factors of $E_{\mathfrak{p}}$ are proper field extensions of factors of $E_{\mathfrak{p}}^\sigma$, we have $W(q)_{\mathfrak{p}} = 1$.*
2. *We have $(-1)^n \delta_{E/k} = D(q)$ (equivalently $(-1)^n \delta_{E_{\mathfrak{p}}/k_{\mathfrak{p}}} = D(q_{\mathfrak{p}})$ for all \mathfrak{p}).*
3. *The signature conditions of Theorem 5.1.*

Proof. By Proposition 2.13 we have that O_q has a torus of type (E, σ) if and only if there exists $\lambda \in (E^\sigma)^*$ such that the quadratic form $q_{E,\lambda} = \frac{1}{2} \text{Tr}_{E/k}(\lambda x\sigma(x))$ has the same invariants as q . Thus we must show that the existence of such a λ is equivalent to the conditions of the corollary.

For each place ν of k set $e_\nu = H(q)_\nu$ and for each infinite places set $(s_\nu, r_\nu)_\nu$ to be the signature of q . Then the $e_\nu, (s_\nu, r_\nu)_\nu$ satisfy (1) and (2) of Corollary 5.4 as they arise from the quadratic form q . We thus have by Corollary 5.4 that the question of existence is local.

We now check that conditions (1), (2) and (3) are equivalent to the local conditions on the existence of λ_ν for all places ν of k . For a finite place ν of k a λ_ν exists with $q_{E_\nu, \lambda_\nu} \simeq q$ if and only if a λ_ν exists with both $D(q_{E_\nu, \lambda_\nu}) = D(q)$ and $H(q_{E_\nu, \lambda_\nu}) = H(q)_\nu$. Theorem 3.3 tells us that (2) (at ν) is equivalent to the discriminant condition and Lemma 5.5 tells us that (1) (at ν) is equivalent to the Hasse invariant condition. For an infinite place ν we have by Lemma 5.2 that the existence of a λ_ν is equivalent to (3) at ν . Note that for infinite places (3) implies (1) and (2). We have thus shown that the existence of a global λ is equivalent to (1), (2) and (3) for all ν , which completes the result. \square

Corollary 5.7. *Let E/k be an extension of number fields. Let q be a quadratic form of dimension $2n + 1$. Then O_q has a torus of type (E, σ) if and only if the following two conditions are satisfied:*

1. *For all primes \mathfrak{p} of k where none of the factors of $E_{\mathfrak{p}}$ are proper field extensions of factors of $E_{\mathfrak{p}}^\sigma$, we have $W(q)_{\mathfrak{p}} = 1$.*

2. The signature conditions of Theorem 5.1.

Proof. We proceed as in the previous corollary, except we now have the added flexibility of choosing what the orthogonal complement of the sub-quadratic space $q_{E,\lambda}$ looks like. In particular, O_q has a torus of type (E, σ) if and only if $q \simeq q_{E,\lambda} \oplus \langle a \rangle$ for some $\lambda \in (E^\sigma)^*$. In order for q and $q_{E,\lambda} \oplus \langle a \rangle$ to have equal discriminants it is necessary that $a = (-1)^n D(q)/\delta_{E/k}$. As this can always be done there is no discriminant condition in this case. Again as above, by Corollary 5.4 the question of the existence of λ is local.

We must find the local condition on Witt invariants. Knowing the discriminants of $q_{E,\lambda}$ and $\langle a \rangle$ we see that $H(q_{E,\lambda} \oplus \langle a \rangle)_{\mathfrak{p}}$ depends on λ if and only if $H(q_{E,\lambda})_{\mathfrak{p}}$ does. Hence this also holds for the Witt invariants. Furthermore, the obstructions to changing Witt invariants arise at the same places as in Corollary 5.6. Now, we compute that $W(q)_{\mathfrak{p}} = W(-aq_{E,\lambda})_{\mathfrak{p}} = W((-1)^{n+1} D(q)\delta_{E/k}q_{E,\lambda})_{\mathfrak{p}}$ (see [Lam05, V.2.9]). Next, by Theorem 3.8 we know that if the Witt invariant of $q_{E,\lambda}$ is independent of λ then $W(q_{E,\lambda})_{\mathfrak{p}} = 1$ independently of λ , and consequently independently of rescaling. In particular it follows that $W(q)_{\mathfrak{p}} = W((-1)^{n+1} D(q)\delta_{E/k}q_{E,\lambda})_{\mathfrak{p}} = 1$. This gives us the condition on Witt invariants (1).

Finally, the signature conditions (2) are precisely those of Lemma 5.2 together with the sign contribution that is dictated by the $\langle a \rangle$ piece at each ν . \square

Remark. The condition “ $E_{\mathfrak{p}}$ contains no field extensions of factors of $E_{\mathfrak{p}}^{\sigma}$,” can be rephrased as “for all constituent fields E_i of E and all the primes \mathfrak{p}_i above \mathfrak{p} in E_i^{σ} , there exists at least one \mathfrak{p}_i which does not split in E_i .”

This condition thus says that for some computable collection of primes which divide the discriminant of the quaternion algebra, none are totally split between E^{σ} and E . We point out that there is no condition on the behaviour of these primes between k and E^{σ} . We also point out that primes which divide the discriminant of E to odd degree ramify for at least one place, and so automatically satisfy this condition.

Lemma 5.8. *Let (E, σ) be an étale algebra with involution. Then every reflex algebra of (E, σ) contains an element y such that $y^2 = \delta_{E/k}$.*

Proof. Suppose $E = E^{\sigma}(\sqrt{x})$ with x chosen so that $\delta_{E/E^{\sigma}} = x$. Then we have $\delta_{E/k} = (-1)^n N(x)$. Let ϕ be a σ -type of E . Then let:

$$y = \prod_{\rho \in \phi} \rho(\sqrt{x}) \in E^{\phi},$$

and moreover, we see that $\sigma(y) = (-1)^n y$ and $y\sigma(y) = N(x) = (-1)^n \delta_{E/k}$. The result follows. \square

Lemma 5.9. *Let (E, σ) be an étale algebra over k with involution, and let A be a quaternion algebra over k . Then E^{ϕ} splits A for all σ -types ϕ of E if and only if we have $[A_{\mathfrak{p}}] = 1$ for every place \mathfrak{p} where $E_{\mathfrak{p}}$ contains no factors which are quadratic extensions of factors of $E_{\mathfrak{p}}^{\sigma}$.*

Proof. We first state some facts concerning the splitting of quaternion algebras. A quaternion algebra is split by an étale algebra E if it is split by each factor. A quaternion algebra is split by a field L if it is split locally everywhere, that is, for each prime \mathfrak{p}_L in L . A local field L splits a nonsplit quaternion algebra if and only if L contains a quadratic subextension.

Thus, every reflex algebra E^{ϕ} splits a quaternion algebra A if and only if E^{Φ} does. This happens if and only if $E_{\mathfrak{p}}^{\Phi}$ splits A for every prime \mathfrak{p} of k . Consequently E^{Φ} splits a quaternion algebra A if and only if for each \mathfrak{p} we have that $A_{\mathfrak{p}}$ nonsplit implies $(E_{\mathfrak{p}})^{\phi}$ has even degree for all ϕ .

It follows from Corollary 2.6 that $(E_{\mathfrak{p}})^{\phi}$ has even degree for all ϕ if and only if at least one factor of $E_{\mathfrak{p}}/E_{\mathfrak{p}}^{\sigma}$ is a field extension. Thus, the only condition for E^{Φ} to split A is that if $A_{\mathfrak{p}}$ is not already split, then $E_{\mathfrak{p}}/E_{\mathfrak{p}}^{\sigma}$ must contain a field extension. \square

Proof of Theorem 5.1. What remains to show is that the conditions of Corollaries 5.6 and 5.7 in the even and odd cases, respectively, are equivalent to those of Theorem 5.1. We see immediately that the conditions on signatures and discriminants are the same and that the additional data about discriminants in the even case is provided by Lemma 5.8. What remains to show is that the Witt invariant conditions agree.

Lemma 5.9 tells us precisely that the condition of the corollaries (for all primes \mathfrak{p} of k where none of the factors of $E_{\mathfrak{p}}$ are proper field extensions of factors of $E_{\mathfrak{p}}^{\sigma}$, we have $W(q)_{\mathfrak{p}} = 1$) is equivalent to the statement that all the σ -reflex fields of E split $W(q)$. Thus we want to show that we can replace $W(q)$ by $W^{\text{orth}}(q)$ in the condition of the previous sentence. In the odd dimensional case there is nothing to show as these are equal. For the even case, since $W^{\text{orth}}(q) = W(q) \otimes_k Z(C_q^0)$ and $Z(C_q^0) \subset E^{\phi}$ it follows that:

$$W^{\text{orth}}(q) \otimes_k E^{\phi} = W(q) \otimes_k Z(C_q^0) \otimes_k E^{\phi} = (W(q) \otimes_k E^{\phi}) \oplus (W(q) \otimes_k E^{\phi}).$$

It follows that E^ϕ splits $W(q)$ if and only if it splits $W^{\text{orth}}(q)$. This gives us the equivalence of the final condition of the theorem with those of the corollaries and thus completes the proof. \square

6. Applications

One of the primary motivations for this work is to understand the possible special fields associated to the special points on Shimura varieties of orthogonal type (see [Del71]). We now give some applications in this direction.

Corollary 6.1. *Suppose in Theorem 5.1 that $k = \mathbb{Q}$, the signature of q is $(2, \ell)$ and (E, σ) is a CM-field with complex conjugation σ . Then O_q contains a torus of type (E, σ) if and only if:*

1. *For each prime p of \mathbb{Q} with local Witt invariant $W(q)_p = -1$ there exists a prime $\mathfrak{p}|p$ of E^σ that does not split in E .*
2. *If ℓ is even, then $D(q) = (-1)^{(2+\ell)/2} \delta_{E/\mathbb{Q}}$. (No further conditions if ℓ is odd.)*

Proof. We have put ourselves in a situation in which the signature condition is automatic. We thus must check only the remaining conditions. The discriminant condition remains the same, and the Witt invariant condition is precisely that of Corollary 5.6. \square

Corollary 6.2. *Suppose that $k = \mathbb{Q}$ and the signature of q is $(2, \ell)$. Let F be a totally real field. Then there exists a CM-field E with $E^\sigma = F$, and the orthogonal group O_q containing a torus of type (E, σ) if and only if:*

1. *No condition if ℓ odd.*
2. *If ℓ is even, then (up to squares) $D(q) = N_{F/k}(\delta)$ for an element $\delta \in F$ which satisfies the condition that for all primes p of k with $W(q)_p = -1$ there is at least one prime $\mathfrak{p}|p$ of F such that δ is not a square in $F_{\mathfrak{p}}$.*

Proof. In this case we are now looking for any CM-field extension.

The norm condition in the even dimension is precisely the condition required so that we have a quadratic extension of the desired discriminant and the desired primes are not totally split. To eliminate entirely the Witt invariant conditions in the odd case we note that we can simply force these to be ramified in the quadratic extension. \square

Remark. In order to satisfy the condition that the primes where $W(q)_p = -1$ will not split in the quadratic extension for δ one is looking to modify δ by an element of square norm which is not a square modulo some prime \mathfrak{p} over p . Elements of square norm tend to be contained in quadratic subextensions. Let $L \subset F$ be a degree 2 subextension. We claim that L contains an element which is not a square in $\mathcal{O}_{F_{\mathfrak{p}}}$. Indeed, if \mathfrak{p} is ramified or inert over L one may take any representative of a nonsquare in $\mathcal{O}_L/(\mathfrak{p} \cap \mathcal{O}_L)$. If \mathfrak{p} is split take any representative of a uniformizer of $\mathcal{O}_{L(\mathfrak{p} \cap \mathcal{O}_L)}$.

Corollary 6.3. *Let $d \in \mathbb{Q}$ be a squarefree positive integer. Consider the quadratic form:*

$$q_d = x_1^2 - x_2^2 + x_3^2 - dx_4^2.$$

This implies $\text{Spin}_{q_d}(\mathbb{R}) \simeq \text{SL}_2(\mathbb{R})^2$ is associated to the Hilbert modular space for $\mathbb{Q}(\sqrt{d})$. Let (E, σ) be a field of dimension 4 with involution σ . Then O_q has a torus of type (E, σ) if and only if the σ -reflex fields of E all contain $\mathbb{Q}(\sqrt{d})$.

Proof. Firstly, a computation using Proposition 2.17 together with the fact that $H(q_d) = (-1, -d)$ shows $W(q_d) = 1$. Thus all the σ -reflex fields E^ϕ automatically split the even Clifford algebra. Since Theorem 5.1 already states that if O_q has a torus of type (E, σ) then $\sqrt{d} \in E^\phi$ for all ϕ . It thus remains only to show, that under the present conditions, $\sqrt{d} \in E^\phi$ for all ϕ implies both the discriminant and signature conditions of Theorem 5.1 hold. To this end, we introduce some further notation.

Let $m \in \mathbb{Q}$ be such that $E^\sigma = \mathbb{Q}(\sqrt{m})$, let τ be the non-trivial automorphism of E^σ and let $\delta = a + b\sqrt{m} \in E^\sigma$ be such that $E = E^\sigma(\sqrt{\delta})$. Let N be the normal closure of E over \mathbb{Q} , then one checks that $N = \mathbb{Q}(\sqrt{m}, \sqrt{\delta\tau(\delta)}, \sqrt{\delta})$ has degree 4 or 8 over \mathbb{Q} . Set $M = \mathbb{Q}(\sqrt{\delta\tau(\delta)}, \sqrt{\delta} + \sqrt{\tau(\delta)}) \subseteq N$. Notice that σ extends to N and that on its restriction to M we have $M^\sigma = \mathbb{Q}(\sqrt{\delta\tau(\delta)})$.

We now must divide the argument into two cases depending on $\text{Gal}(N/\mathbb{Q})$. In the first case suppose $\text{Gal}(N/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$. Then we may assume $\delta \in \mathbb{Q}$ and so the two σ -reflex fields of E are $M = \mathbb{Q}(\sqrt{\delta})$ and $\mathbb{Q}(\sqrt{m\delta})$ with their intersection being \mathbb{Q} . It follows that $\sqrt{d} \in E^\phi$ for all ϕ implies d is a square. Moreover, as E is biquadratic, $\delta_{E/\mathbb{Q}}$ is a square and E is either CM or totally real. Thus $\sqrt{d} \in E^\phi$ for all ϕ is equivalent to $d = \delta_{E/\mathbb{Q}} \bmod \text{squares}$. (Notice that the case of d a square is technically excluded from the statement of the corollary.)

Now in the second case suppose $\text{Gal}(N/\mathbb{Q}) \neq (\mathbb{Z}/2\mathbb{Z})^2$. Then $\text{Gal}(N/\mathbb{Q})$ is either $\mathbb{Z}/4\mathbb{Z}$ or D_8 . In either case a check shows that M is (up to isomorphism) the unique σ -reflex field for E and M^σ is the only quadratic subextension of M . Moreover, the discriminant of E is $\delta_{E/\mathbb{Q}} = \delta\tau(\delta)$ and $M^\sigma = \mathbb{Q}(\sqrt{\delta\tau(\delta)})$ hence $\sqrt{d} \in E^\phi$ for all ϕ is equivalent to $d = \delta\tau(\delta) = \delta_{E/\mathbb{Q}} \pmod{\text{squares}}$. Finally, since $b^2m = (a^2 - \delta\tau(\delta))$ it follows that $\delta = a + \sqrt{a^2 - \delta\tau(\delta)}$. Thus using that $\delta\tau(\delta) = r^2d > 0$ we find that E is either totally complex or totally real.

We have thus shown that in all cases, $\sqrt{d} \in E^\phi$ for all ϕ implies that $d = \delta_{E/\mathbb{Q}}$ and that E is either totally complex or totally real. One now observes that E being totally complex or totally real implies the signature condition and this concludes the proof. \square

Remark. It follows that the tori in Spin_q are all associated to algebras which are two dimensional over $\mathbb{Q}(\sqrt{d})$. This is well known for the tori associated to CM-points, but we have shown the analogous fact also holds for those associated to so-called almost totally real cycles (for the definition see the discussion following [DL03, Prop. 2.4]). It is worth noting that these E can never be ATR extensions, that is extensions with only one complex place. It is the reflex fields of these E which may be ATR extensions.

Acknowledgements

I would like to thank my supervisor Prof. Eyal Goren as well as Cameron Franc and Victoria de Quehen for their help in editing various drafts of this paper. I would also like to thank the reviewer for their helpful suggestions. I would also like to thank Prof. Eva Bayer, for her many useful comments. I would like to thank NSERC and the ISM for their financial support while doing this research.

References

- [BCKM03] Rosali Brusamarello, Pascale Chuard-Koulmann, and Jorge Morales, *Orthogonal groups containing a given maximal torus*, J. Algebra **266** (2003), no. 1, 87–101.
- [BF13] E. Bayer-Fluckiger, *Embeddings of maximal tori in orthogonal groups*, Ann. Inst. Fourier (Grenoble) (2013), (To Appear).
- [Bor91] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.
- [Del71] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389, Springer, Berlin, 1971, pp. 123–165. Lecture Notes in Math., Vol. 244.
- [DL03] Henri Darmon and Adam Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*, Int. Math. Res. Not. (2003), no. 40, 2153–2180.
- [Epk89] Martin Epkenhans, *Trace forms of normal extensions over local fields*, Linear and Multilinear Algebra **24** (1989), no. 2, 103–116.
- [Fio09] Andrew Fiori, *Special points on orthogonal symmetric spaces*, Master’s thesis, McGill University, 2009.
- [Fio12] ———, *Characterization of special points of orthogonal symmetric spaces*, Journal of Algebra **372** (2012), no. 0, 397 – 419.
- [Fio13] ———, *Questions in the theory of orthogonal Shimura varieties*, Ph.D. thesis, McGill University, 2013.
- [KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits.
- [Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005.
- [Lan83] Serge Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 255, Springer-Verlag, New York, 1983.
- [Mil06] James S. Milne, *Complex multiplication*, 2006, Available at www.jmilne.org/math/, p. 113.

- [O'M00] O. Timothy O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition.
- [PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.
- [PR10] Gopal Prasad and Andrei S. Rapinchuk, *Local-global principles for embedding of fields with involution into simple algebras with involution*, Comment. Math. Helv. **85** (2010), no. 3, 583–645.
- [Ser73] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York, 1973, Translated from French.
- [Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.
- [Ser84] ———, *L'invariant de Witt de la forme $\text{Tr}(x^2)$* , Comment. Math. Helv. **59** (1984), no. 4, 651–676.
- [Shi80] Goro Shimura, *The arithmetic of certain zeta functions and automorphic forms on orthogonal groups*, Ann. of Math. (2) **111** (1980), no. 2, 313–375.