PACIFIC JOURNAL OF MATHEMATICS
Vol. 167, No. 1, 1995

DISCRIMINANTS OF INVOLUTIONS ON HENSELIAN DIVISION ALGEBRAS

M. CHACRON, H. DHERTE,(*) J.-P. TIGNOL,
A.R. WADSWORTH AND V.I. YANCHEVSKIĬ

The discriminant of an involution of the first kind on a finite-dimensional division algebra over a field with a Henselian valuation of residue characteristic different from 2 is computed in terms of residue information. We also describe the set of discriminants of involutions on such division algebras. In the case where the residue involution is the identity, a stable decomposition of the division algebra into the tensor product of a semi-ramified and a totally ramified subalgebra is obtained.

Knus, Parimala and Sridharan have recently defined the discriminant of an involution of the first kind on a central simple algebra [**10**] (see also [**11**]), and they have shown how the discriminant can be used to determine whether an involution on a central simple algebra of degree 4 is decomposable, i.e. whether the central simple algebra decomposes into a tensor product of two quaternion algebras stable under the involution. Although the discriminant of an involution is in principle easy to calculate (the definition is recalled in section 2.), it may prove difficult to determine explicitly for a given central simple algebra. Our purpose in this paper is to show how the discriminant can be computed explicitly for involutions on division algebras over Henselian fields of residual characteristic different from 2, in terms of residue information.

Our results depend on the kind of the residue involution and on whether the division algebra is inertially split or not; they are collected in Theorem 4. In particular, they show that every involution on a division algebra of degree at least 4 which is not inertially split has discriminant 1. As an application of the main Theorem, we also compute the discriminant of the involution considered by Amitsur,

(*)author deceased

Rowen and Tignol in [**2**, Theorem 5.2]; the result thus obtained yields an alternative proof that the involution is not decomposable.

It is also worth pointing out that in the case where the residue involution is the identity, we obtain a stable decomposition of the division algebra into a semi-ramified and a totally ramified subalgebra; moreover, the totally ramified part has a stable decomposition into a tensor product of quaternion algebras (see Theorem 5). In particular, it follows that every involution on a totally ramified division algebra over a Henselian field of residual characteristic not 2 decomposes as a tensor product of involutions on quaternion algebras. Stable decompositions of semi-ramified division algebras over Henselian fields are further investigated in [**4**].

In the final section, we investigate the set of discriminants of orthogonal involutions on division algebras over Henselian fields. We show that in a large number of cases this set is the group of square classes of reduced norms. [1] In view of the fact that decomposable involutions have trivial discriminants, this result yields an efficient way of constructing division algebras with indecomposable involutions.

Notations and Terminology. All the division algebras considered in this paper are finite-dimensional over their center and of characteristic not 2. The *degree* $\deg D$ of a division algebra is the square root of its dimension over the center. An involution σ over a division algebra D with center F is *of the first kind* if it leaves F elementwise invariant; otherwise it is *of the second kind.* We denote:

$$(D,\sigma)_+ = \{x \in D \mid \sigma(x) = x\} \text{ and } (D,\sigma)_- = \{x \in D \mid \sigma(x) = -x\}.$$

If $\deg D = n$ and σ is of the first kind, then it can be proved that $\dim_F(D,\sigma)_+ = (n(n+1))/2$ or $n(n-1)/2$. The involution is called *of orthogonal type* or *type* $+1$ in the former case, of *symplectic type* or *type* -1 in the latter (see [**21**, Ch. 8; (7.6)]). If σ is an involution of the first kind, then every other involution τ of the first kind is the composite of σ with an inner automorphism $\mathrm{Int}(u) : x \mapsto uxu^{-1}$:

$$\tau = \mathrm{Int}(u) \circ \sigma$$

[1] This fact has now been proved for arbitrary central simple algebras of degree at least 4 by Parimala, Sridharan and Suresh [**14**].

for some $u \neq 0$ such that $\sigma(u) = \pm u$. The involutions σ and τ are of the same type if $\sigma(u) = u$; they are of opposite type if $\sigma(u) = -u$ (see [**21**, Ch. 8; (7.7)]).

The following observation, made independently by several authors [**23**, Proposition 3], [**16**, Proposition 5], [**18**, Proposition 5.3], characterizes the involutions of orthogonal type:

LEMMA 1. *If an involution σ on a division algebra D leaves a maximal subfield K elementwise invariant, then it is of orthogonal type.*

Proof. We include a proof for the reader's convenience: Let L be a splitting field of D such that $K \otimes_F L$ is a field. (One can for instance choose for L a generic splitting field of D.) Fix an isomorphism: $D \otimes_F L \simeq \mathrm{End}_L(V)$ for some L-vector space V of dimension $\deg D$. The elements in $K \otimes_F L$ are then identified to endomorphisms of V, hence V is endowed with a $K \otimes_F L$-vector space structure. Comparing dimensions over L, we must have $\dim_{K \otimes L} V = 1$. It is known (see for instance [**21**, p.302]) that every involution on $\mathrm{End}_L(V)$ is the adjoint involution with respect to some bilinear form on V, which is symmetric if the involution is of orthogonal type and alternating if the involution is of symplectic type. Let B be a bilinear form on V for which the extension of σ to $D \otimes_F L$ is the adjoint involution and let $v \in V$, $v \neq 0$. Since K is elementwise invariant under σ, we have for $\alpha, \beta \in K \otimes_F L$:

$$B(\alpha v, \beta v) = B(\beta\alpha v, v) = B(\alpha\beta v, v) = B(\beta v, \alpha v).$$

Therefore, B is symmetric and σ is of orthogonal type. □

We now review the basic notions of valuation theory on division algebras in the special case of interest for the present paper.

Let D be a central division algebra over a field F. Every Henselian valuation v on F extends to a valuation on D (see [**22**, p. 53]). We denote also by v the extension of the valuation to D. The value group $v(D^\times)$ is denoted by Γ_D; the valuation ring is $\mathcal{O}_D = \{x \in D \mid v(x) \geq 0\}$ and its maximal ideal is $\mathcal{M}_D = \{x \in D \mid v(x) > 0\}$. The residue division ring $\mathcal{O}_D/\mathcal{M}_D$ is denoted by $\overline{D}$.

The division algebras D considered in this paper are endowed with an involution of the first kind; it then follows that their exponent

is 2 (see [**21**, p. 305]), and hence their degree is a power of 2. We further assume that char $\overline{F} \neq 2$; hence the division algebras we consider are *tame* in the sense of [**9**, §6]. The "Ostrowski Theorem" [**7**] then yields:

$$[D : F] = [\overline{D} : \overline{F}].(\Gamma_D : \Gamma_F) \tag{1}$$

and it follows from [**17**, Theorem 3.18], [**9**, Corollary 6.10] that Γ_D/Γ_F is an elementary abelian group of exponent 2.

The algebra D is called *totally ramified* if $\overline{D} = \overline{F}$, *inertial* if $\Gamma_D = \Gamma_F$ and *semi-ramified* if $[\overline{D} : \overline{F}] = (\Gamma_D : \Gamma_F)$ $(= \deg(D))$ and $\overline{D}$ is commutative.

We recall also that the center $Z(\overline{D})$ of $\overline{D}$ is an abelian Galois extension of $\overline{F}$ and that there is a fundamental homomorphism:

$$\theta_D : \Gamma_D \to \mathrm{Gal}(Z(\overline{D})/\overline{F}), \tag{2}$$

defined by: $\theta_D(\alpha)(\bar{d}) = \overline{xdx^{-1}}$ where $x \in D$ is an arbitrary element of value $v(x) = \alpha$. This homomorphism is surjective [**9**, Proposition 1.7]; its kernel, which obviously contains Γ_F, is denoted by Λ_D. The division algebra D is called *inertially split* if it is split by an inertial extension of F or, equivalently by [**9**, Lemma 5.1], if $\Lambda_D = \Gamma_F$.

Finally, we note for further reference that if F is a Henselian valued field such that the residue field $\overline{F}$ has characteristic not 2, every element in $1 + \mathcal{M}_F$ is a square, hence the canonical map $\mathcal{O}_F^\times/\mathcal{O}_F^{\times 2} \to \overline{F}^\times/\overline{F}^{\times 2}$ is an isomorphism. Therefore, there is a canonical exact sequence

$$1 \to \overline{F}^\times/\overline{F}^{\times 2} \xrightarrow{i} F^\times/F^{\times 2} \xrightarrow{\overline{v}} \Gamma_F/2\Gamma_F \to 0 \tag{3}$$

where $\overline{v}$ is induced by the valuation and i is the composite of the isomorphism $\overline{F}^\times/\overline{F}^{\times 2} \simeq \mathcal{O}_F^\times/\mathcal{O}_F^{\times 2}$ and the inclusion $\mathcal{O}_F^\times/\mathcal{O}_F^{\times 2} \hookrightarrow F^\times/F^{\times 2}$.

1. Involutions on Henselian division algebras. Let D be a finite-dimensional central division algebra over a field F. Assume F is endowed with a Henselian valuation v such that the characteristic of the residue field $\overline{F}$ is not 2, and let σ be an involution of the first

kind on D. Since v is Henselian, it extends to D in a unique way; in particular, for all $x \in D$,

$$v(\sigma(x)) = v(x),$$

and hence σ induces an involution $\overline{\sigma}$ on the residue division algebra $\overline{D}$, by

$$\overline{\sigma}(\overline{u}) = \overline{\sigma(u)} \quad \text{for all } u \in \mathcal{O}^\times.$$

Since the center $Z(\overline{D})$ of $\overline{D}$ may be strictly larger than $\overline{F}$, it is not difficult to find examples where $\overline{\sigma}$ is of the second kind (see Proposition 4 below). Moreover, even when $\overline{\sigma}$ is of the first kind, there is in general no relation between the type of σ and the type of $\overline{\sigma}$. If for instance $D \simeq I \otimes_F T$ where I is an inertial division algebra and T is a totally ramified division algebra, and if σ_I, σ_T (resp. τ_I, τ_T) are involutions of orthogonal (resp. symplectic) type on I and T respectively, then $\sigma_I \otimes \sigma_T$ and $\tau_I \otimes \tau_T$ are of orthogonal type, $\sigma_I \otimes \tau_T$ and $\tau_I \otimes \sigma_T$ are of symplectic type, but

$$\overline{\sigma_I \otimes \sigma_T} = \overline{\sigma_I} = \overline{\sigma_I \otimes \tau_T} \quad \text{is orthogonal}$$

while

$$\overline{\tau_I \otimes \tau_T} = \overline{\tau_I} = \overline{\tau_I \otimes \sigma_T} \quad \text{is symplectic.}$$

Nevertheless, there is a relation in the case where D is inertially split, which we proceed to establish.

LEMMA 1. *Let $\xi \in \overline{D}$. If $\overline{\sigma}(\xi) = \varepsilon\xi$ where $\varepsilon = \pm 1$, then there is an element $x \in \mathcal{O}_D$ such that $\overline{x} = \xi$, $\sigma(x) = \varepsilon x$ and $[F(x) : F] = [\overline{F}(\xi) : \overline{F}]$.*

Proof. Let $x_0 \in \mathcal{O}_D$ be an arbitrary lift of ξ. If $\overline{\sigma}(\xi) = \varepsilon\xi$, then

$$\sigma(x_0) = \varepsilon x_0 + m \quad \text{for some } m \in \mathcal{M}_D.$$

The element $x_1 = (x_0 + \varepsilon\sigma(x_0))/2 = x_0 + (\varepsilon m/2)$ then satisfies $\overline{x_1} = \overline{x_0} = \xi$ and $\sigma(x_1) = \varepsilon x_1$; hence the field $F(x_1)$ is stable under σ and $\overline{F(x_1)} \supset \overline{F}(\xi)$.

Since ξ is separable over $\overline{F}$ (because $[\overline{D} : \overline{F}]$ is a power of 2 and char.$\overline{F} \neq 2$) and since F is Henselian, it follows that $F(x_1)$ contains a unique inertial lift K of $\overline{F}(\xi)$, i.e. a unique subfield K such that

$\overline{K} = \overline{F}(\xi)$ and $[K : F] = [\overline{K} : \overline{F}]$. Since $\sigma(K)$ is an inertial lift of $\overline{F}(\overline{\sigma}(\xi)) = \overline{F}(\xi)$, we must have $\sigma(K) = K$.

Let $x_2 \in K$ be such that $\overline{x_2} = \xi$. Again, we have

$$\sigma(x_2) = \varepsilon x_2 + m' \quad \text{for some } m' \in \mathcal{M}_K.$$

Then let $x = (x_2 + \varepsilon\sigma(x_2))/2 = x_2 + (\varepsilon m'/2)$. We have $\overline{x} = \overline{x_2} = \xi$ and $\sigma(x) = \varepsilon x$. Moreover $x \in K$, and hence

$$[F(x) : F] \leq [K : F] = [\overline{F}(\xi) : \overline{F}].$$

On the other hand,

$$[F(x) : F] \geq [\overline{F}(\overline{x}) : \overline{F}] = [\overline{F}(\xi) : \overline{F}],$$

hence $[F(x) : F] = [\overline{F}(\xi) : \overline{F}]$. □

There is a corresponding result for representatives of values, which will be needed in section 4.:

LEMMA 2. *For every $\gamma \in \Gamma_D$ such that $\theta_D(\gamma) \neq \overline{\sigma}|_{Z(\overline{D})}$, there exists $x \in D^\times$ such that $v(x) = \gamma$ and $\sigma(x) = x$.*

Proof. Let $x_0 \in D^\times$ be an arbitrary element of value γ. Since $\theta_D(\gamma) \neq \overline{\sigma}|_{Z(\overline{D})}$, one can find an element $\zeta \in Z(\overline{D})$ such that

$$\theta_D(\gamma) \circ \overline{\sigma}(\zeta)^{-1}\zeta \neq -\overline{\sigma(x_0)x_0^{-1}}.$$

(Take $\zeta = 1$ if the right-hand side is not 1; otherwise, take any ζ which is not invariant under $\theta_D(\gamma) \circ \overline{\sigma}|_{Z(\overline{D})}$.) Then let $z \in \mathcal{O}_D$ be such that $\overline{z} = \zeta$ and let

$$x = zx_0 + \sigma(zx_0).$$

It is clear that $\sigma(x) = x$; moreover, since

$$\overline{\sigma(x_0)\sigma(z)x_0^{-1}} = \overline{\sigma(x_0)x_0^{-1}}.\theta_D(\gamma) \circ \overline{\sigma}(\overline{z}) \neq -\overline{z},$$

we have $\overline{xx_0^{-1}} = \overline{z} + \overline{\sigma(x_0)\sigma(z)x_0^{-1}} \neq 0$, and hence $v(x) = v(x_0) = \gamma$. □

PROPOSITION 3. *If D is inertially split and $\overline{\sigma}$ is of the first kind, then σ and $\overline{\sigma}$ are of the same type.*

Proof. Since $[D : F]$ is a power of 2 and char $\overline{F} \neq 2$, the maximal subfields of $\overline{D}$ are separable over $\overline{F}$. Let $\alpha \in \overline{D}$ be such that $\overline{F}(\alpha)$ is a maximal subfield of $\overline{D}$, and let $a \in \mathcal{O}_D$ be a lift of α. We have

$$[F(a) : F] \geq [\overline{F}(\alpha) : \overline{F}] = \deg(\overline{D}).[Z(\overline{D}) : \overline{F}]. \tag{4}$$

Since D is inertially split, we have $\Lambda_D = \Gamma_F$; hence $(\Gamma_D : \Gamma_F) = [Z(\overline{D}) : \overline{F}]$; hence Ostrowski's Theorem (see equation (1)) yields

$$\deg(D) = \deg(\overline{D}).[Z(\overline{D}) : \overline{F}].$$

Therefore, (4) shows that $F(a)$ is a maximal subfield of D.

By the Skolem-Noether Theorem, the restriction of $\overline{\sigma}$ to $\overline{F}(\alpha)$ extends to an inner automorphism of $\overline{D}$. Let $\beta \in \overline{D}$ be such that

$$\overline{\sigma}(\alpha) = \beta\alpha\beta^{-1}. \tag{5}$$

Replacing β by $\beta + \overline{\sigma}(\beta)$ or by $\beta - \overline{\sigma}(\beta)$ (whichever is non-zero), we may assume $\overline{\sigma}(\beta) = \varepsilon\beta$ with $\varepsilon = \pm 1$. Lemma 1 shows that there is a lift $b \in \mathcal{O}_D$ of β such that $\sigma(b) = \varepsilon b$. Let $\tau = \mathrm{Int}(b^{-1}) \circ \sigma$ be the composite of σ with the inner automorphism $\mathrm{Int}(b^{-1}) : x \mapsto b^{-1}xb$. Since $\sigma(b) = \varepsilon b$, the map τ is an involution of D. Clearly, $\overline{\tau} = \mathrm{Int}(\beta^{-1}) \circ \overline{\sigma}$, and (5) shows that $\overline{\tau}(\alpha) = \alpha$. From Lemma 1, it then follows that $\overline{\tau}$ is of type $+1$; hence the type of $\overline{\sigma}$ is ε.

We proceed to determine the type of τ, hence of σ. By the Skolem-Noether Theorem, there exists an element $d \in D^\times$ such that

$$\tau(a) = dad^{-1}.$$

Replacing d by $d + \tau(d)$ or by $d - \tau(d)$, we may assume $\tau(d) = \varepsilon' d$ where $\varepsilon' = \pm 1$. The map $\mathrm{Int}(d^{-1}) \circ \tau$ is then an involution of D which leaves $F(a)$ elementwise invariant; hence its type is $+1$, by Lemma 1. Thus, the type of τ is ε' and the type of $\sigma = \mathrm{Int}(b) \circ \tau$ is $\varepsilon\varepsilon'$. As the type of $\overline{\sigma}$ is ε, it only remains to prove $\varepsilon' = 1$. Since

$$\overline{\tau}(\overline{a}) = \overline{\tau}(\alpha) = \alpha = \overline{a}, \tag{6}$$

the automorphism of $\overline{D}$ which maps $\overline{u}$ to $\overline{dud^{-1}}$, for $u \in \mathcal{O}_D$, is the identity on $\overline{F}(\alpha)$, hence also on its subfield $Z(\overline{D})$. This means

that $\theta_D(v(d)) = I$, i.e. that $v(d) \in \Lambda_D$. Since D is inertially split, we have $\Lambda_D = \Gamma_F$; therefore, multiplying d by a factor in $F^\times$ if necessary, we may assume $v(d) = 0$. Equation (6) then yields

$$\overline{d}\alpha\overline{d}^{-1} = \alpha,$$

and it follows that $\overline{d} \in \overline{F}(\alpha)$ since $\overline{F}(\alpha)$ is a maximal subfield of $\overline{D}$. Therefore, $\overline{\tau}(\overline{d}) = \overline{d}$. On the other hand, $\overline{\tau}(\overline{d}) = \varepsilon'\overline{d}$ since $\tau(d) = \varepsilon' d$, and hence $\varepsilon' = 1$. □

REMARK. The inertial case of the preceding proposition is already contained in essence in a paper of Platonov and Yanchevskiĭ: see the proof of Proposition 5.9 of [**17**]. (To avoid misunderstanding the statement of this proposition, the reader should keep in mind that Platonov and Yanchevskiĭ assume throughout §5 of [**17**] that the given involution is of symplectic type.)

In the next proposition, we show that every involution on $\overline{D}$ can be lifted to an involution on D:

PROPOSITION 4. *For any involution t on $\overline{D}$ which leaves $\overline{F}$ elementwise invariant, there is an involution τ of the first kind on D such that $t = \overline{\tau}$. If t is of the second kind, then the type of τ can be arbitrarily chosen. Moreover, every automorphism of $Z(\overline{D})$ over $\overline{F}$ can be extended to an involution on $\overline{D}$.*

Proof. Let ρ be an automorphism of $Z(\overline{D})$ over $\overline{F}$ and let $T \subset D$ be an inertial lift of $Z(\overline{D})$ in D; i.e. T is a subfield of D such that $\overline{T} = Z(\overline{D})$ and $[T : F] = [Z(\overline{D}) : \overline{F}]$. The Galois group of T over F is then canonically isomorphic to the Galois group of $Z(\overline{D})$ over $\overline{F}$; hence ρ lifts to some automorphism of T over F which we again denote by ρ. By Proposition 3.1.67 of [**19**], there is an involution τ_ρ on D whose restriction to T is ρ; hence $\overline{\tau_\rho}$ is an involution on $\overline{D}$ which extends ρ. The last part of the proposition is thus proved.

Suppose now that t is a given involution on $\overline{D}$. The arguments above, taking for ρ the restriction of t to $Z(\overline{D})$, yield an involution τ_ρ on D such that $\overline{\tau_\rho}$ and t have the same action on $Z(\overline{D})$. Therefore, $t = \mathrm{Int}(\xi) \circ \overline{\tau_\rho}$ for some $\xi \in \overline{D}^\times$ such that $\overline{\tau_\rho}(\xi) = \varepsilon\xi$ with $\varepsilon = \pm 1$. Lemma 1 then yields an element $x \in \mathcal{O}_D$ such that $\tau_\rho(x) = \varepsilon x$ and $\overline{x} = \xi$. The involution $\tau = \mathrm{Int}(x) \circ \tau_\rho$ then satisfies $\overline{\tau} = t$.

If t (hence also $\overline{\tau_\rho}$) is of the second kind, then multiplying ξ by an element $\zeta \in Z(\overline{D})^\times$ such that $\tau_\rho(\zeta) = -\zeta$, we may change the sign of ε hence also the type of τ. □

2. Discriminants of involutions. Let D be a finite-dimensional central division algebra over a field F of characteristic not 2 and let σ be an involution of the first kind on D. Following [**10**], we define

$$\mathrm{Alt}(\sigma) = \{x \in D \mid \sigma(x) + \varepsilon x = 0\}$$

where ε is the type of σ. Thus, $\mathrm{Alt}(\sigma) = (D, \sigma)_-$ if σ is of orthogonal type and $\mathrm{Alt}(\sigma) = (D, \sigma)_+$ if σ is of symplectic type. Knus, Parimala and Sridharan [**10**, p. 94] then define the *discriminant* of σ as the image of the reduced norm of any element in $\mathrm{Alt}(\sigma) \cap D^\times$ in the group of square classes of F:

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(a).F^{\times 2} \in F^\times/F^{\times 2},$$

for any $a \in \mathrm{Alt}(\sigma) \cap D^\times$. In particular, one can take $a = 1$ if σ is of symplectic type, hence the discriminant of every involution of symplectic type is 1.

We denote by $\mathcal{D}(D)$ the set of discriminants of involutions of orthogonal type on D:

$$\mathcal{D}(D) = \bigcup_\sigma \mathrm{disc}(\sigma) \subset F^\times,$$

where σ runs over the set of orthogonal involutions on D and where $\mathrm{disc}(\sigma)$ is viewed as a coset of $F^{\times 2}$ in $F^\times$. If γ is an involution of symplectic type, then every involution σ of orthogonal type has the form $\sigma = \mathrm{Int}(u) \circ \gamma$ for some $u \in (D, \gamma)_- \cap D^\times$; then $u \in (D, \sigma)_- \cap D^\times$, and hence $\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(u).F^{\times 2}$. Therefore,

$$\mathcal{D}(D) = \mathrm{Nrd}_D((D, \gamma)_- \cap D^\times).F^{\times 2}.$$

Alternatively, if σ is any given involution of orthogonal type, then every other orthogonal involution has the form $\tau = \mathrm{Int}(u) \circ \sigma$ for some $u \in (D, \sigma)_+ \cap D^\times$. For $k \in (D, \sigma)_- \cap D^\times$, we have $uk \in (D, \tau)_- \cap D^\times$, and hence $\mathrm{disc}(\tau) = \mathrm{Nrd}_D(uk).F^{\times 2}$. Since $\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(k).F^{\times 2}$, we thus get

$$\mathcal{D}(D) = \mathrm{Nrd}_D((D, \sigma)_+ \cap D^\times).\mathrm{disc}(\sigma).$$

For example, when D is a quaternion algebra, the conjugation γ is an involution of symplectic type. Therefore, $\mathrm{disc}(\gamma) = 1$ and $\mathcal{D}(D) = \mathrm{Nrd}_D((D,\gamma)_- \cap D^\times)$ is the set of represented values of the 3-dimensional quadratic form $x \mapsto -x^2$ on the space of pure quaternions. This shows that the set $\mathcal{D}(D)$ is not necessarily a group. The subgroup of $F^\times$ generated by $\mathcal{D}(D)$ is easy to determine:[2]

PROPOSITION 1. *For every division algebra D with involution,*

$$\mathcal{D}(D) \subseteq Nrd_D(D^\times).F^{\times 2}$$

and every element in $Nrd_D(D^\times).F^{\times 2}$ is the product of two elements of $\mathcal{D}(D)$.

Proof. Since the discriminant of every involution is the square class of a reduced norm, the inclusion $\mathcal{D}(D) \subset \mathrm{Nrd}_D(D^\times).F^{\times 2}$ is clear. Let σ be an arbitrary involution of orthogonal type on D. Dieudonné has shown [**5**, Theorem 3] that every element of D is the product of two elements in $(D,\sigma)_+$. If $x \in D^\times$, let $s,t \in (D,\sigma)_+$ be such that $x = st$. Then $\mathrm{Nrd}_D(x) = \mathrm{Nrd}_D(s)\mathrm{Nrd}_D(t)$, and hence

$$\mathrm{Nrd}_D(x).F^{\times 2} = (\mathrm{Nrd}_D(s).\,\mathrm{disc}(\sigma)).(\mathrm{Nrd}_D(t).\,\mathrm{disc}(\sigma)),$$

which shows that $\mathrm{Nrd}_D(x).F^{\times 2}$ is the product of two elements of $\mathcal{D}(D)$. □

From here on, we assume that F is endowed with a Henselian valuation v, such that $\mathrm{char}\ \overline{F} \neq 2$. Our aim is to compute the discriminant of σ in terms of residue information. We first investigate the case where $\overline{\sigma}$ is of the second kind:

PROPOSITION 2. *If $\overline{\sigma}$ is of the second kind and* $\deg(D) > 2$, *then* $\mathrm{disc}(\sigma) = 1$.

Proof. Since the discriminant of every involution of symplectic type is 1, we may assume σ of orthogonal type. By hypothesis, the restriction of $\overline{\sigma}$ to $Z(\overline{D})$ is a nontrivial element of $\mathrm{Gal}(Z(\overline{D})/\overline{F})$,

[2]The equality $\mathcal{D}(D) \subseteq \mathrm{Nrd}_D(D^\times).F^{\times 2}$ has now been proved for arbitrary central simple algebras D of even degree $\deg D \geq 4$ by Parimala, Sridharan and Suresh [**14**].

which is an elementary abelian group of exponent 2, as we observed above. Therefore, there exists $\xi \in Z(\overline{D})$ such that $\overline{\sigma}(\xi) = -\xi$ and $\xi^2 \in \overline{F}^\times$. Lemma 1 yields an element $x \in D^\times$ such that $\sigma(x) = -x$, $\overline{x} = \xi$ and $[F(x) : F] = [\overline{F}(\xi) : \overline{F}] = 2$. Then, by [**6**, Corollary 4; p. 150] ,

$$\mathrm{Nrd}_D(x) = N_{F(x)/F}(x)^{\deg(D)/2} \in F^{\times 2},$$

and since $x \in \mathrm{Alt}(\sigma)$,

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(x).F^{\times 2} = 1.$$

□

Henceforth, we shall assume that $\overline{\sigma}$ is of the first kind. We next consider the case where $\overline{\sigma} \neq I$:

PROPOSITION 3. *Assume $\overline{\sigma}$ is an involution of the first kind, $\overline{\sigma} \neq I$. If D is inertially split, then* $\mathrm{disc}(\sigma) = i(N_{Z(\overline{D})/\overline{F}}(\mathrm{disc}(\overline{\sigma})))$, *where $i : \overline{F}^\times/\overline{F}^{\times 2} \to F^\times/F^{\times 2}$ is the canonical map described in* (3). *If D is not inertially split, then* $\mathrm{disc}(\sigma) = 1$.

Proof. Again, we assume that σ is of orthogonal type; otherwise $\mathrm{disc}(\sigma) = 1$ and, when D is inertially split, $\mathrm{disc}(\overline{\sigma}) = 1$ by Proposition 3, so the proposition is obvious.

Since $\overline{\sigma} \neq I$, one can find $\xi \in \overline{D}^\times$ such that $\overline{\sigma}(\xi) = -\xi$. Lemma 1 then yields $x \in \mathcal{O}_D$ such that $\overline{x} = \xi$ and $\sigma(x) = -x$; hence $x \in \mathrm{Alt}(\sigma) \cap \mathcal{O}_D^\times$. Then $v(\mathrm{Nrd}_D(x)) = 0$, and hence $\mathrm{Nrd}_D(x).F^{\times 2}$ is in the image of the map i, and

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(x).F^{\times 2} = i\left(\overline{\mathrm{Nrd}_D(x)}.\overline{F}^{\times 2}\right). \tag{7}$$

By [**8**, Corollary 2] ,

$$\overline{\mathrm{Nrd}_D(x)} = N_{Z(\overline{D})/\overline{F}}(\mathrm{Nrd}_{\overline{D}}(\overline{x})^\lambda), \tag{8}$$

where $\lambda = \sqrt{(\Lambda_D : \Gamma_F)}$. If D is not inertially split, then λ is even; hence $\mathrm{disc}(\sigma) = 1$. If D is inertially split, then $\lambda = 1$ and $\overline{\sigma}$ is an involution of orthogonal type on $\overline{D}$; hence $\overline{x} = \xi \in \mathrm{Alt}(\overline{\sigma})$. The proposition then readily follows from relations (7) and (8). □

The case where $\overline{\sigma} = I$ is more difficult to treat. It will be investigated in the next two sections.

3. Residually commutative division algebras. In this section, D denotes a finite-dimensional central division algebra with involution over a field F endowed with a Henselian valuation v. We assume char $\overline{F} \neq 2$ and $\overline{D}$ is commutative. For $x, y \in D^\times$, denote

$$C(x,y) = \overline{xyx^{-1}y^{-1}} \in \overline{D}^\times.$$

Since $x(yz)x^{-1}(yz)^{-1} = xyx^{-1}y^{-1}.y(xzx^{-1}z^{-1})y^{-1}$, we have

$$C(x,yz) = C(x,y).\theta_D(v(y))(C(x,z)). \tag{9}$$

By skew-symmetry of C (i.e. $C(x,y) = C(y,x)^{-1}$), the preceding relation also yields a formula for $C(xy,z)$:

$$C(xy,z) = \theta_D(v(x))(C(y,z)).C(x,z).$$

If $v(x) \in \Lambda_D$ and $v(y) \in \Gamma_F$, let $y = fu$ for some $f \in F^\times$ and some $u \in \mathcal{O}_D^\times$; then

$$C(x,y) = \overline{xux^{-1}}.\overline{u^{-1}} = \theta_D(v(x))(\overline{u}).\overline{u}^{-1} = 1,$$

and the preceding relation shows

$$C(x,yz) = C(x,z).$$

Therefore, there is a well-defined map $\gamma_x : \Gamma_D/\Gamma_F \to \overline{D}^\times$ defined by

$$\gamma_x(v(y) + \Gamma_F) = C(x,y) \quad \text{for all } y \in D^\times.$$

Equation (9) shows that this map is a crossed homomorphism (i.e. a 1-cocycle) for the action of Γ_D/Γ_F on $\overline{D}^\times$ through θ_D.

LEMMA 4. *For every homomorphism $\varphi : \Gamma_D/\Gamma_F \to \{\pm 1\}$, there exists an element $a \in D^\times$ such that $v(a) \in \Lambda_D$ and $\gamma_a = \varphi$. The element a is uniquely determined by φ up to multiplication by a factor in $F^\times.(1 + \mathcal{M}_D)$. Moreover, $a \in F^\times.(1 + \mathcal{M}_D)$ if and only if the restriction of φ to Λ_D/Γ_F is trivial.*

Proof. Let $K \subset D$ be an inertial lift of $\overline{D} = Z(\overline{D})$ (see [**9**, p. 135]). By [**9**, Lemma 1.8] , the centralizer $C_D K$ of K in D is a tame totally

ramified division algebra (over its center K) with value group Λ_D. By the non-degeneracy of the canonical pairing of a tame totally ramified division algebra [**24**, Proposition 3.1] , one can find $x \in C_D K$ such that

$$C(x, y) = \varphi(v(y) + \Gamma_F) \quad \text{for all } y \in (C_D K)^\times.$$

It then follows that $v(x) \in \Lambda_D$ and that the restrictions of γ_x and of φ to Λ_D/Γ_F are the same. Consider then the product $\gamma_x\varphi$: $\Gamma_D/\Gamma_F \to \overline{D}^\times$. Since this map is constant on cosets of Γ_D modulo Λ_D, it induces a well-defined map $\delta\,\Gamma_D/\Lambda_D \to \overline{D}^\times$, by

$$\delta(\alpha + \Lambda_D) = \gamma_x(\alpha + \Gamma_F)\varphi(\alpha + \Gamma_F), \quad \text{for } \alpha \in \Gamma_D.$$

Moreover, since γ_x and φ are 1-cocycles, δ also is a 1-cocycle of Γ_D/Λ_D in $\overline{D}^\times$ (for the action of Γ_D/Λ_D through θ_D). Now, θ_D induces an isomorphism of Γ_D/Λ_D with the Galois group of $\overline{D}/\overline{F}$; hence Hilbert's Theorem 90 shows that δ is a coboundary. Therefore, there is an element $u \in \mathcal{O}_D^\times$ such that

$$\gamma_x(\alpha + \Gamma_F)\varphi(\alpha + \Gamma_F) = \overline{u}.\theta_D(\alpha)(\overline{u})^{-1} \quad \text{for all } \alpha \in \Gamma_D.$$

This last equation can be rewritten as

$$C(x, y).\varphi(v(y) + \Gamma_F) = \overline{uyu^{-1}y^{-1}} = C(u, y) \quad \text{for all } y \in D^\times.$$

Then let $a = u^{-1}x$. We have $v(a) = v(x) \in \Lambda_D$ and the preceding relation yields

$$C(a, y) = \varphi(v(y) + \Gamma_F) \quad \text{for all } y \in D^\times,$$

as required.

Suppose now that $a, b \in D^\times$ are such that $v(a), v(b) \in \Lambda_D$ and $\gamma_a = \gamma_b$. It then readily follows from equation (9) that $C(x, ab^{-1}) = 1$ for all $x \in D^\times$. By the non-degeneracy of the canonical pairing of $C_D K$ (see [**24**, Proposition 3.1]), it then follows that $v(ab^{-1}) \in \Gamma_F$. Let $ab^{-1} = fu$ for some $f \in F^\times$ and some $u \in \mathcal{O}_D^\times$. We have

$$\theta_D(v(x))(\overline{u})\overline{u}^{-1} = C(x, u) = 1 \quad \text{for all } x \in D^\times;$$

hence $\overline{u} \in \overline{F}^\times$, and therefore $u \in F^\times.(1 + \mathcal{M}_D)$. This shows $a \equiv b \bmod F^\times.(1 + \mathcal{M}_D)$.

If $a \in F^{\times}.(1 + \mathcal{M}_D)$, then clearly $\gamma_a = 1$. Conversely, if $\gamma_a = 1$, then $\gamma_a = \gamma_1$ and from the part of the Lemma which has just been proved it follows that $a \equiv 1 \bmod F^{\times}.(1 + \mathcal{M}_D)$. □

THEOREM 5. *Let D be a finite-dimensional central division algebra with an involution σ of the first kind over a Henselian field F of residual characteristic different from 2. Assume $\overline{\sigma} = I$ (hence $\overline{D}$ is commutative); then there exist subalgebras S, T of D with the following properties:*

1. *S and T have center F and $D = S \otimes_F T$.*
2. *S and T are stable under σ.*
3. *S is semi-ramified and $\overline{S} = \overline{D}$; in particular, $\deg(S) = [\overline{D} : \overline{F}]$.*
4. *T is totally ramified and $\Gamma_T = \Lambda_D$; in particular, $[T : F] = (\Lambda_D : \Gamma_F)$.*
5. *$\Gamma_S \cap \Gamma_T = \Gamma_F$ and $\Gamma_D = \Gamma_S + \Gamma_T$.*
6. *T is a tensor product of quaternion subalgebras stable under σ.*

Proof. We argue by induction on the degree of D. If $\Lambda_D = \Gamma_F$, then we let $S = D$ and $T = F$. Suppose then $\Lambda_D \neq \Gamma_F$. We claim that it suffices to prove the existence of a central quaternion subalgebra Q of D stable under σ, totally ramified over F, such that $\Gamma_Q \subset \Lambda_D$ and $\Gamma_Q \cap \Gamma_{D'} = \Gamma_F$, where $D' = C_D Q$ is the centralizer of Q in D.

Indeed, if these conditions hold, then D' is also stable under σ and moreover, since $\overline{D'} \subset \overline{D}$, the restriction σ' of σ to D' also satisfies $\overline{\sigma'} = I$. By the induction hypothesis, $D' = S' \otimes_F T'$ for some subalgebras S', T' of D' satisfying conditions 1–6 with respect to D'. Then let $S = S'$ and $T = T' \otimes_F Q$. Conditions 1, 2 and 6 are clearly satisfied by S and T. Since $\Gamma_{D'} = \Gamma_{S'} + \Gamma_{T'}$ and $\Gamma_Q \cap \Gamma_{D'} = \Gamma_F$, we have $\Gamma_Q \cap \Gamma_{T'} = \Gamma_F$. A theorem of Morandi [**13**, Theorem 1] then shows that T is totally ramified and $\Gamma_T = \Gamma_{T'} + \Gamma_Q$. As $\Gamma_S \cap \Gamma_{T'} = \Gamma_F$, it follows that $\Gamma_S \cap \Gamma_T = \Gamma_F$. Since S is semi-ramified and T is totally ramified, conditions 3, 4 and 5 then follow from [**9**, Theorem 6.3] . This proves the claim.

In order to construct a quaternion subalgebra Q for which these conditions hold, we consider an arbitrary homomorphism

$\varphi : \Gamma_D/\Gamma_F \to \{\pm 1\}$ which is not trivial on Λ_D/Γ_F. (Recall from [**17**, Theorem 3.18] or [**9**, Corollary 6.10] that Γ_D/Γ_F is an abelian group of exponent 2; hence such homomorphisms exist.) By Lemma 4, there exists an element $a_1 \in D^\times$ such that $v(a_1) \in \Lambda_D$ and $\gamma_{a_1} = \varphi$. Let $\psi : \Gamma_D/\Gamma_F \to \{\pm 1\}$ be a homomorphism such that $\psi(v(a_1) + \Gamma_F) = -1$, and let $b_1 \in D^\times$ be such that $v(b_1) \in \Lambda_D$ and $\gamma_{b_1} = \psi$. We then have

$$C(a_1, b_1) = C(b_1, a_1)^{-1} = \psi(v(a_1) + \Gamma_F) = -1. \tag{10}$$

Moreover, relation (9) shows that for all $x \in D^\times$,

$$C(x, a_1^2) = C(x, a_1)^2 = \varphi(v(x) + \Gamma_F)^{-2} = 1;$$

similarly, $C(x, b_1^2) = 1$. Therefore, $\gamma_{a_1^2} = \gamma_{b_1^2} = 1$, and Lemma 4 shows that $a_1^2,\ b_1^2 \in F^\times.(1 + \mathcal{M}_D)$.

From the latter relation, it follows that $\overline{\sigma(a_1^2)a_1^{-2}} = 1$. Now, since $v(a_1) \in \Lambda_D$,

$$\overline{\sigma(a_1^2)a_1^{-2}} = \overline{\sigma(a_1)a_1^{-1}}.\overline{a_1(\sigma(a_1)a_1^{-1})a_1^{-1}} = \overline{\sigma(a_1)a_1^{-1}}^2,$$

and hence $\overline{\sigma(a_1)a_1^{-1}} = \pm 1$. We denote $\varepsilon = \overline{\sigma(a_1)a_1^{-1}} \in \{\pm 1\}$. Similarly, let $\varepsilon' = \overline{\sigma(b_1)b_1^{-1}} \in \{\pm 1\}$.

We proceed to construct elements $a,\ b \in D^\times$ which are congruent to $a_1,\ b_1$ respectively modulo $1 + \mathcal{M}_D$ and which generate a quaternion algebra Q with the required properties.

Let $a_2 = [a_1 + \varepsilon\sigma(a_1)]/2$. Clearly, $\sigma(a_2) = \varepsilon a_2$; moreover, since $\overline{\sigma(a_1)a_1^{-1}} = \varepsilon$, we have $\overline{a_2 a_1^{-1}} = 1$, and hence $a_2 \equiv a_1 \bmod 1 + \mathcal{M}_D$. In particular, it follows that $a_2^2 \in F^\times.(1 + \mathcal{M}_D)$. Let $f \in F^\times$ and $m \in \mathcal{M}_D$ be such that

$$a_2^2 = f(1 + m).$$

This equation shows that actually $m \in \mathcal{M}_{F(a_2^2)}$. Since F, hence also $F(a_2^2)$, is Henselian, the polynomial $X^2 - (1 + m)$ has a root in $\mathcal{O}_{F(a_2^2)}$ whose image in the residue field is 1. Let $1 + m_1$, with $m_1 \in \mathcal{M}_{F(a_2^2)}$, be this root. Since $\sigma(a_2) = \pm a_2$, it follows that the field $F(a_2^2)$ is elementwise invariant under σ; hence $\sigma(m_1) = m_1$. Then let $a = a_2(1 + m_1)^{-1}$. This element satisfies: $a^2 = f \in F^\times$, $\sigma(a) = \varepsilon a$ and $a \equiv a_2 \equiv a_1 \bmod 1 + \mathcal{M}_D$.

Now let $b_2 = [b_1+\varepsilon'\sigma(b_1)-ab_1a^{-1}-\varepsilon'a\sigma(b_1)a^{-1}]/4$. Since $a^2 \in F^\times$, we have $a^{-1}b_1a = ab_1a^{-1}$; since moreover $\sigma(a) = \pm a$, a straightforward calculation shows that $\sigma(b_2) = \varepsilon' b_2$ and $ab_2a^{-1} = -b_2$. In order to compute $\overline{b_2 b_1^{-1}}$, observe that

$$\begin{aligned}\overline{a\sigma(b_1)a^{-1}b_1^{-1}} &= \overline{a\sigma(b_1)b_1^{-1}a^{-1}}.\overline{ab_1a^{-1}b_1^{-1}} \\ &= \theta_D(v(a))(\overline{\sigma(b_1)b_1^{-1}}).C(a,b_1).\end{aligned}$$

The first factor on the right-hand side equals ε'. Moreover, since $a \equiv a_1 \bmod 1+\mathcal{M}_D$, we have $C(a,b_1) = C(a_1,b_1)$. In view of equation (10), it then follows

$$\overline{a\sigma(b_1)a^{-1}b_1^{-1}} = -\varepsilon',$$

and hence

$$\overline{b_2b_1^{-1}} = [1+\varepsilon'^2 - C(a,b_1) - \varepsilon'(-\varepsilon')]/4 = 1.$$

This equation shows $b_2 \equiv b_1 \bmod 1+\mathcal{M}_D$. Since $b_1^2 \in F^\times.(1+\mathcal{M}_D)$, we have

$$b_2^2 = g(1+m')$$

for some $g \in F^\times$ and some $m' \in \mathcal{M}_D$. Arguing as we did with a_2 above, we find $m_1' \in \mathcal{M}_{F(b_2^2)}$ such that $(1+m_1')^2 = 1+m'$. Since b_2^2 is invariant under σ and commutes with a, the same holds true for m_1'; therefore, the element $b = b_2(1+m_1')^{-1}$ satisfies $b^2 = g \in F^\times$, $\sigma(b) = \varepsilon' b$, $aba^{-1} = -b$ and $b \equiv b_2 \equiv b_1 \bmod 1+\mathcal{M}_D$.

It is now clear that a and b generate a quaternion subalgebra Q of D which is stable under σ. The value group Γ_Q contains $v(a) = v(a_1)$ and $v(b) = v(b_1)$. Now, equation (10) shows that $v(a_1) \notin \Gamma_F$ and that $v(b_1) \notin \Gamma_F \cup (v(a_1)+\Gamma_F)$, because $C(a_1,b_1) = \varphi(v(b_1)+\Gamma_F) = -1$; hence the subgroup of Γ_D generated by $v(a_1)$ and $v(b_1)$ has order 4. Since $[Q : F] = 4$, it follows that this subgroup is Γ_Q and that Q is totally ramified (over F).

If x is a non-zero element in the centralizer D' of Q, then $C(a,x) = C(b,x) = 1$; hence $v(x)+\Gamma_F$ is in $\operatorname{Ker}(\varphi) \cap \operatorname{Ker}(\psi)$. From the description of Γ_Q above, it readily follows that $\Gamma_Q \cap \Gamma_{D'} = \Gamma_F$, so the quaternion algebra Q meets all the requirements. □

REMARKS. 1. The algebras S and T are not uniquely determined by conditions 1–6, as the following example illustrates: suppose $v(u) = 0$, $\overline{u} \notin \overline{F}^2$ and x, y, $z \in F^\times$ have $\mathbb{F}_2$-independent values in $\Gamma_F/2\Gamma_F$; let D be the tensor product of quaternion algebras

$$D = (u, x)_F \otimes (y, uz)_F,$$

and let σ be the tensor product of the canonical involutions on each factor.

We can take $S = (u, x)_F$ and $T = (y, uz)_F$. However, if $(1, i_S, j_S, k_S)$ and $(1, i_T, j_T, k_T)$ are the standard bases of S and T, the subalgebras S' of D generated by i_S and $j_S i_T$ and the subalgebra T' generated by i_T and $i_S j_T$ satisfy the same conditions 1–6 as S and T.

2. The theorem shows, as a particular case, that every totally ramified division algebra with involution of the first kind over a Henselian field of residual characteristic different from 2 decomposes into a tensor product of quaternion algebras stable under the involution. This result has also been proved by Chacron and Wadsworth [**3**, Theorem 2.1] . (The hypotheses in [**3**] are somewhat different, since it is assumed that the valuation v on D is a c-valuation, not necessarily totally ramified over F. However, this hypothesis is used only once in the proof of [**3**, Theorem 2.1] , to show that $s^2 \in F^\times.(1 + \mathcal{M}_D)$ for all $s \in (D, \sigma)_+$. In the case where D is totally ramified, this property readily follows from the fact that Γ_D/Γ_F has exponent 2 and that $\overline{D} = \overline{F}$.)

3. There is an analogue of this theorem which holds for arbitrary tame division algebras over a Henselian field [**26**]: such a division algebra D decomposes as a tensor product $D = S \otimes_F T$ with S inertially split and T totally ramified such that $\Gamma_S \cap \Gamma_T = \Gamma_F$ if and only if Λ_D/Γ_F is a direct summand of Γ_D/Γ_F.

COROLLARY 6. *If* $\overline{\sigma} = I$, $\deg(D) > 2$ *and* D *is not semi-ramified, then* $\operatorname{disc}(\sigma) = 1$.

Proof. The preceding Theorem yields a non-trivial decomposition of D into stable subalgebras:

$$D = S \otimes T.$$

If $x \in \mathrm{Alt}(\sigma) \cap S^\times$, then

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(x).F^{\times 2} = \mathrm{Nrd}_S(x)^{\deg(T)}.F^{\times 2};$$

hence $\mathrm{disc}(\sigma) = 1$ since the degree of T is even. □

4. Semi-ramified division algebras. In this section, D denotes a finite-dimensional central division algebra with involution σ of the first kind over a field F with a Henselian valuation v such that char $\overline{F} \neq 2$. We suppose that D is semi-ramified and that $\overline{\sigma}$ is the identity on $\overline{D}$, which implies that σ is of orthogonal type, by Proposition 3. From the hypotheses, it readily follows that $\overline{D}/\overline{F}$ is a Galois extension with elementary abelian Galois group of exponent 2 and order $\deg(D)$. Since the discriminant of an involution on a quaternion algebra is easily computed (see section 2.), we will always assume $\deg(D) > 2$ in this section. This will allow us to use the following easy observation:

LEMMA 1. *Let K/k be an elementary abelian Galois extension of exponent 2 of fields of characteristic different from 2 and let $\rho \in \mathrm{Gal}(K/k)$, $\rho \neq I$. Suppose $[K : k] > 2$. If $x \in K^\times$ is such that $\rho(x) = \pm x$, then $N_{K/k}(x) \in k^{\times 2}$.*

Proof. Let L be the subfield of K elementwise invariant under ρ. Since $\rho \neq I$ and $[K : k] > 2$, the degrees $[K : L]$ and $[L : k]$ are both even. Now, if $\rho(x) = x$, then

$$N_{K/k}(x) = N_{L/k}(x^{[K:L]}) \in k^{\times 2}.$$

If $\rho(x) = -x$, then the minimal polynomial of x over L is $X^2 - x^2$, hence $N_{L(x)/L}(x) = -x^2$. Therefore,

$$N_{K/k}(x) = N_{L/k}(N_{L(x)/L}(x))^{[K:L(x)]} = N_{L/k}(-x^2)^{[K:L(x)]}.$$

Since $[L : k]$ is even, $N_{L/k}(-1) = 1$, and hence the preceding equation shows that $N_{K/k}(x)$ is a square. □

The next proposition shows that the discriminant of σ can also be determined from symmetric elements:

PROPOSITION 2. *Assume* $\deg(D) > 2$. *For all* $x \in D^\times$ *such that* $\overline{\sigma(x)x^{-1}} = 1$ *and* $v(x) \notin \Gamma_F$,

$$\operatorname{disc}(\sigma) = \operatorname{Nrd}_D(x).F^{\times 2} \in F^\times/F^{\times 2}.$$

Proof. Let $a \in \mathcal{O}_D$ be such that $\sigma(a) = a$ and $\theta_D(v(x))(\overline{a}) \neq \overline{a}$. (Such an element can be obtained by lifting an element $\alpha \in \overline{D}$ such that $\theta_D(v(x))(\alpha) \neq \alpha$, using Lemma 1.) Let also $u = (\sigma(x)x^{-1} + 1)/2$ and $y = ux = (x + \sigma(x))/2$. Then $\overline{u} = 1$; hence $v(y) = v(x)$. Since moreover $\sigma(y) = y$, we have $ay - ya \in \operatorname{Alt}(\sigma) \cap D^\times$; hence

$$\operatorname{disc}(\sigma) = \operatorname{Nrd}_D(ay - ya).F^{\times 2} \in F^\times/F^{\times 2}.$$

Now,

$$\begin{aligned}\operatorname{Nrd}_D(ay - ya) &= \operatorname{Nrd}_D(a - yay^{-1}) \operatorname{Nrd}_D(y) \\ &= \operatorname{Nrd}_D(a - yay^{-1}) \operatorname{Nrd}_D(u) \operatorname{Nrd}_D(x).\end{aligned}$$

Since $\overline{u} = 1$, we have $\operatorname{Nrd}_D(u) \in F^{\times 2}$, by [**8**, Corollary 2] , so the proof is complete if we show $\operatorname{Nrd}_D(a - yay^{-1}) \in F^{\times 2}$.

We have $\overline{a - yay^{-1}} = \overline{a} - \theta_D(v(y))(\overline{a}) \neq 0$; hence $v(a - yay^{-1}) = 0$ and, by [**8**, Corollary 2]

$$\operatorname{Nrd}_D(a - yay^{-1}).F^{\times 2} = i(N_{\overline{D}/\overline{F}}(\overline{a} - \theta_D(v(y))(\overline{a})).\overline{F}^{\times 2}),$$

where $i : \overline{F}^\times/\overline{F}^{\times 2} \to F^\times/F^{\times 2}$ is the canonical map defined in (3). Since $\theta_D(v(y))$ maps $\overline{a} - \theta_D(v(y))(\overline{a})$ to its opposite, Lemma 1 shows that the norm of this element is a square; hence $\operatorname{Nrd}_D(a - yay^{-1}) \in F^{\times 2}$ and the proof is complete. □

Now let $x, y \in D^\times$ be such that $v(x)$, $v(y)$ are $\mathbb{F}_2$-independent in Γ_D/Γ_F, and such that $\sigma(x) = x$ and $\sigma(y) = y$. (Such elements can be obtained by Lemma 2.)

THEOREM 3.

$$\overline{xyx^{-1}y^{-1}} = \theta_D(v(xy))(\alpha)\alpha^{-1} \quad \text{for some } \alpha \in \overline{D}^\times.$$

Moreover, for any $\alpha \in \overline{D}^\times$ *satisfying this relation,*

$$\operatorname{disc}(\sigma) = i(N_{\overline{D}/\overline{F}}(\alpha)).$$

Proof. For the first part, it suffices, by Hilbert's Theorem 90, to show that

$$\overline{xyx^{-1}y^{-1}}.\theta_D(v(xy))(\overline{xyx^{-1}y^{-1}}) = 1.$$

We observe that

$$\overline{xyx^{-1}y^{-1}} = \overline{\sigma}(\overline{xyx^{-1}y^{-1}}) = \overline{\sigma(xyx^{-1}y^{-1})} = \overline{y^{-1}x^{-1}yx};$$

hence

$$\begin{aligned}\theta_D(v(xy))(\overline{xyx^{-1}y^{-1}}) &= \overline{xy(y^{-1}x^{-1}yx)y^{-1}x^{-1}} \\ &= \overline{yxy^{-1}x^{-1}} = \overline{xyx^{-1}y^{-1}}^{-1},\end{aligned}$$

as claimed.

For later use, we also observe that Proposition 2 yields

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(x).F^{\times 2} = \mathrm{Nrd}_D(y).F^{\times 2};$$

hence

$$\mathrm{Nrd}_D(xy) \in F^{\times 2}. \tag{11}$$

Suppose now $\overline{xyx^{-1}y^{-1}} = \theta_D(v(xy))(\alpha)\alpha^{-1}$. If $\overline{xyx^{-1}y^{-1}} = 1$, then $\alpha = \theta_D(v(xy))(\alpha)$. As $v(xy) \notin \Gamma_F$ since $v(x)$ and $v(y)$ are $\mathbb{F}_2$-independent in Γ_D/Γ_F, we have $\theta_D(v(xy)) \neq I$; hence Lemma 1 shows that $N_{\overline{D}/\overline{F}}(\alpha) \in \overline{F}^{\times 2}$. We thus have to show $\mathrm{disc}(\sigma) = 1$. In order to do that, observe that $\overline{\sigma(yx)(yx)^{-1}} = 1$ since $\overline{xyx^{-1}y^{-1}} = 1$; hence by Proposition 2

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(yx).F^{\times 2} = \mathrm{Nrd}_D(xy).F^{\times 2}.$$

Relation (11) then shows $\mathrm{disc}(\sigma) = 1$, completing the proof in the case where $\overline{xyx^{-1}y^{-1}} = 1$.

If $\overline{xyx^{-1}y^{-1}} \neq 1$, then $xy - yx \in (D,\sigma)_- \cap D^\times$; hence

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(xy - yx).F^{\times 2} \in F^\times/F^{\times 2}.$$

We have $\mathrm{Nrd}_D(xy - yx) = \mathrm{Nrd}_D(xyx^{-1}y^{-1} - 1)\,\mathrm{Nrd}_D(xy)$; hence, in view of relation (11),

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(xyx^{-1}y^{-1} - 1).F^{\times 2}. \tag{12}$$

Now, by [8, Corollary 2],

$$(13)\quad \mathrm{Nrd}_D(xyx^{-1}y^{-1}-1).F^{\times 2} = i(N_{\overline{D}/\overline{F}}(\overline{xyx^{-1}y^{-1}}-1).\overline{F}^{\times 2}),$$

where $i : \overline{F}^{\times}/\overline{F}^{\times 2} \to F^{\times}/F^{\times 2}$ is the canonical map defined in (3). Now,

$$\begin{aligned} N_{\overline{D}/\overline{F}}(\overline{xyx^{-1}y^{-1}}-1) &= N_{\overline{D}/\overline{F}}(\theta_D(v(xy))(\alpha)\alpha^{-1}-1) \\ &= N_{\overline{D}/\overline{F}}(\theta_D(v(xy))(\alpha)-\alpha)N_{\overline{D}/\overline{F}}(\alpha^{-1}) \end{aligned}$$

and since $\theta_D(v(xy))(\alpha)-\alpha$ is mapped to its opposite by $\theta_D(v(xy))$, its norm is a square, by Lemma 1. Therefore,

$$N_{\overline{D}/\overline{F}}(\overline{xyx^{-1}y^{-1}}-1).\overline{F}^{\times 2} = N_{\overline{D}/\overline{F}}(\alpha^{-1}).\overline{F}^{\times 2} = N_{\overline{D}/\overline{F}}(\alpha).\overline{F}^{\times 2}.$$

The theorem now follows from equations (12) and (13). □

Summing up the results in Proposition 2, Proposition 3, Corollary 6 and Theorem 3, we get

THEOREM 4. *Let σ be an involution of the first kind on a finite-dimensional central division algebra D over a Henselian field F such that* $\mathrm{char}\,\overline{F} \neq 2$. *Assume* $\deg(D) > 2$.

If D is not inertially split, then $\mathrm{disc}(\sigma) = 1$.

If D is inertially split, then

- *if $\overline{\sigma}$ is of the second kind,*

$$\mathrm{disc}(\sigma) = 1;$$

- *if $\overline{\sigma}$ is of the first kind, $\overline{\sigma} \neq I$,*

$$\mathrm{disc}(\sigma) = i(N_{Z(\overline{D})/\overline{F}}(\mathrm{disc}(\overline{\sigma})));$$

- *if $\overline{\sigma} = I$,*

$$\mathrm{disc}(\sigma) = i(N_{\overline{D}/\overline{F}}(\alpha))$$

for any $\alpha \in \overline{D}$ such that there exist x, $y \in D^{\times}$ with $\sigma(x) = x$, $\sigma(y) = y$, $v(x)$ and $v(y)$ $\mathbb{F}_2$-independent in Γ_D/Γ_F and $\overline{xyx^{-1}y^{-1}} = \theta_D(v(xy))(\alpha)\alpha^{-1}$.

We conclude this section with an example directly inspired by [**2**]. Let K/k be a Galois extension of fields (of characteristic not 2) with elementary abelian Galois group of order 4:

$$\mathrm{Gal}(K/k) = \{1, \alpha_1, \alpha_2, \alpha_3\} \quad \text{with } \alpha_i^2 = 1 \text{ for all } i = 1, 2, 3,$$

and let $u \in K^\times$. We define a division ring A by iterating the twisted Laurent series construction:

$$A = K((t_1; \alpha_1))((t_2; \alpha_2^*)),$$

where α_2^* is the automorphism of $K((t_1; \alpha_1))$ which extends α_2 on K and maps t_1 to ut_1 (see for instance [**15**, §19.7]); thus, the elements of A are formal power series of the form

$$s = \sum_{i_2=r_2}^{\infty} \left(\sum_{i_1=r_1(i_2)}^{\infty} a_{i_1,i_2} t_1^{i_1} \right) t_2^{i_2} \quad (a_{i_1,i_2} \in K),$$

and multiplication is defined through the following relations:

$$t_i a = \alpha_i(a) t_i \quad \text{for } i = 1, 2 \text{ and } a \in K$$
$$t_2 t_1 = u t_1 t_2.$$

There is a valuation on A with value group $\Gamma_A = \mathbb{Z}^2$ (with the reverse lexicographic ordering), which maps the element s above to $(r_1(r_2), r_2) \in \mathbb{Z}^2$ if $a_{r_1(r_2),r_2} \neq 0$.

A straightforward computation shows that the center of $K((t_1; \alpha_1))$ is $K_1((t_1^2))$, where K_1 is the subfield of K elementwise invariant under α_1, and that $\alpha_2^{*2}(t_1^2) = N_{K/k}(u) t_1^2$. Therefore, if $N_{K/k}(u) = 1$, then α_2^* has inner order 2 and the degree of A is 4 (see [**15**, §19.7]).

The center of A, which we denote by F, is easy to determine explicitly: if $N_{K/k}(u) = 1$, Hilbert's Theorem 90 yields elements $b_1, b_2 \in K^\times$ such that

$$\alpha_i(b_i) = b_i \quad \text{for } i = 1, 2 \quad \text{and} \quad u\alpha_1(u) = b_1 \alpha_2(b_1)^{-1},$$
$$u\alpha_2(u) = b_2 \alpha_1(b_2)^{-1}.$$

Then $F = k((b_1 t_1^2))((b_2^{-1} t_2^2))$, and hence $\Gamma_F = 2\mathbb{Z} \times 2\mathbb{Z} \subset \Gamma_A$.

PROPOSITION 5. *If $u\alpha_3(u) = 1$, then there is an involution of the first kind σ on A which leaves K, t_1 and t_2 elementwise invariant.*

The involution σ is uniquely determined by these conditions; it is of orthogonal type and its discriminant is

$$\operatorname{disc}(\sigma) = N_{K/k}(s).F^{\times 2}$$

for any $s \in K^\times$ such that $u = \alpha_3(s)s^{-1}$. In particular, σ is decomposable if and only if $N_{K/k}(s) \in k^{\times 2}$.

Proof. Using the relation $t_2 t_1 = u t_1 t_2$, it is easy to determine, for all integers i_1, i_2, coefficients $c(i_1, i_2) \in K^\times$ such that

$$t_2^{i_2} t_1^{i_1} = c(i_1, i_2) t_1^{i_1} t_2^{i_2}.$$

Moreover, if $u\alpha_3(u) = 1$, one can check that

$$c(i_1, i_2)\alpha_1^{i_1}\alpha_2^{i_2}(c(i_1, i_2)) = 1 \quad \text{for all } i_1, i_2 \in \mathbb{Z}$$

and it follows that the formula

$$\sigma\left(\sum_{i_1,i_2} a_{i_1,i_2} t_1^{i_1} t_2^{i_2}\right) = \sum_{i_1,i_2} t_2^{i_2} t_1^{i_1} a_{i_1,i_2} = \sum_{i_1,i_2} \alpha_1^{i_1}\alpha_2^{i_2}(a_{i_1,i_2}) c(i_1, i_2) t_1^{i_1} t_2^{i_2}$$

defines an involution on A. From the description of the center F above, it readily follows that σ is of the first kind. Uniqueness of σ is clear and since σ leaves the maximal subfield $K((b_1 t_1^2))((b_2^{-1} t_2^2))$ invariant, Lemma 1 shows that σ is of orthogonal type.

The computation of the discriminant of σ is a direct application of Theorem 3 with $x = t_2$ and $y = t_1$; then $\theta_A(v(xy)) = \alpha_3$ and if $s \in K^\times = \overline{A}^\times$ is such that

$$\alpha_3(s)s^{-1} = \overline{t_2 t_1 t_2^{-1} t_1^{-1}} = u,$$

then

$$\operatorname{disc}(\sigma) = i(N_{\overline{A}/\overline{F}}(s).\overline{F}^{\times 2}) = N_{K/k}(s).F^{\times 2}.$$

By [**10**, Theorem 3.2] (see also [**11**, Theorem 3.1]), σ is decomposable if and only if its discriminant is trivial. Since $k^\times \cap F^{\times 2} = k^{\times 2}$, the preceding equality shows that this condition is also equivalent to: $N_{K/k}(s) \in k^{\times 2}$. □

If $k = \mathbb{Q}(\lambda)$, where λ is an indeterminate, $K = k(\sqrt{2}, \sqrt{\lambda})$ and

$$u = \frac{-\sqrt{\lambda} + 1 + \sqrt{2}}{\sqrt{\lambda} + 1 - \sqrt{2}},$$

then one gets a Laurent series analogue of the example in [**2**, Theorem 5.2]. The corresponding involution is indecomposable, since

$$N_{K/k}\left(\sqrt{\lambda}+1-\sqrt{2}\right)=\lambda^2-6\lambda+1\notin k^{\times 2}.$$

Of course, simpler examples are easy to construct; the preceding proposition shows that it suffices to find an extension K/k of degree 4 with elementary abelian Galois group and an element $s\in K^\times$ such that $N_{K/k}(s)\notin k^{\times 2}$. One can take for instance $k=\mathbb{Q}$, $K=k(\sqrt{2},\sqrt{3})$ and $s=1+\sqrt{2}+\sqrt{3}$.

5. The set of discriminants. Recall from section 2 that for an arbitrary division algebra D with involution, $\mathcal{D}(D)$ denotes the set of discriminants of orthogonal involutions on D. Our aim in this final section is to investigate $\mathcal{D}(D)$ and the group $\mathrm{Nrd}_D(D^\times).F^{\times 2}$ in the case where F is Henselian.[3]

Throughout this section, we assume D is a finite-dimensional central division algebra with involution over a Henselian field F of residue characteristic different from 2. Since explicit computations are easy when D is a quaternion algebra (see section 2), we will often assume $\deg D\geq 4$. This restriction is not necessary however for our first result:

PROPOSITION 1. *If D is not inertially split, then*

$$\mathcal{D}(D)=\mathrm{Nrd}_D(D^\times).F^{\times 2}=F^{\times 2}.$$

Proof. Theorem 4 readily yields $\mathcal{D}(D)=F^{\times 2}$. The other equality follows, since Proposition 1 shows that $\mathrm{Nrd}_D(D^\times).F^{\times 2}$ is the subgroup of $F^\times$ generated by $\mathcal{D}(D)$. □

We next investigate the square classes of reduced norms:

LEMMA 2. *If $\deg D\geq 4$, then for every $\alpha\in\Gamma_D$ there exists an element $d_\alpha\in D^\times$ such that $v(d_\alpha)=\alpha$ and $\mathrm{Nrd}_D(d_\alpha)\in F^{\times 2}$.*

Proof. In view of the preceding proposition, it suffices to consider the case where D is inertially split. Let $\alpha\in\Gamma_D$ and $\rho=\theta_D(\alpha)\in$

[3]See the footnote to Proposition 1.

$\mathrm{Gal}(Z(\overline{D})/\overline{F})$. If $\rho = I$, then $\alpha \in \Gamma_F$ since D is inertially split; hence an appropriate d_α may be found in $F^\times$.

If $\rho \neq I$, we use Lemma 5.6 of [**17**] in the case where D is semi-ramified and Lemma 5.4 of [**17**] in the case where D is not semi-ramified to find an element $g_\rho \in D^\times$ which is symmetric for some involution of symplectic type and such that $\theta_D(v(g_\rho)) = \rho$. Lemma 1 shows that $F(g_\rho)$ is not a maximal subfield of D, hence; if K is a maximal subfield containing g_ρ,

$$\mathrm{Nrd}_D(g_\rho) = N_{K/F}(g_\rho) = N_{F(g_\rho)/F}(g_\rho)^{[K:F(g_\rho)]} \in F^{\times 2}.$$

On the other hand, we have $v(g_\rho) - \alpha \in \mathrm{Ker}(\theta_D)$ and $\mathrm{Ker}(\theta_D) = \Gamma_F$ since D is inertially split, hence there exists $f \in F^\times$ such that $\alpha = v(fg_\rho)$. We may then set $d_\alpha = fg_\rho$. □

We thus get a description of the group $\mathrm{Nrd}_D(D^\times).F^{\times 2}$ for an inertially split division algebra with involution:

PROPOSITION 3. *If D is inertially split and* $\deg D \geq 4$, *then*

$$\mathrm{Nrd}_D(D^\times).F^{\times 2} = i\left(N_{Z(\overline{D})/\overline{F}}(\mathrm{Nrd}_{\overline{D}}(\overline{D}^\times)).\overline{F}^{\times 2}\right),$$

where i is the canonical map described in (3).

Proof. Let $a \in D^\times$ and $\alpha = v(a)$. The preceding lemma yields an element d_α such that $\mathrm{Nrd}_D(d_\alpha) \in F^{\times 2}$ and $v(d_\alpha) = v(a)$. Then for $u = ad_\alpha^{-1} \in \mathcal{O}_D^\times$ we have

$$\mathrm{Nrd}_D(a).F^{\times 2} = \mathrm{Nrd}_D(u).F^{\times 2}$$

and, by [**8**, Corollary 2] ,

$$\overline{\mathrm{Nrd}_D(u)} = N_{Z(\overline{D})/\overline{F}}(\mathrm{Nrd}_{\overline{D}}(\overline{u})).$$

Therefore, $\mathrm{Nrd}_D(a).F^{\times 2} = i\left(N_{Z(\overline{D})/\overline{F}}\left(\mathrm{Nrd}_{\overline{D}}(\overline{u})\right).\overline{F}^{\times 2}\right)$. □

We now turn to a description of the set $\mathcal{D}(D)$:

PROPOSITION 4. *If D is semi-ramified and* $\deg D \geq 4$, *then*

$$\mathcal{D}(D) = \mathrm{Nrd}_D(D^\times).F^{\times 2} = i\left(N_{\overline{D}/\overline{F}}\left(\overline{D}^\times\right).\overline{F}^{\times 2}\right).$$

Proof. Since the second equality is a particular case of the preceding proposition and since $\mathcal{D}(D)$ is always included in $\mathrm{Nrd}_D(D^\times).F^{\times 2}$ (see Proposition 1), it suffices to show that the square class of every reduced norm is the discriminant of an orthogonal involution. Moreover, the same argument as in the preceding proposition shows that it suffices to consider reduced norms of units $u \in \mathcal{O}_D^\times$.

Assume first that $\mathrm{Nrd}_D(u) \notin F^{\times 2}$. Then $N_{\overline{D}/\overline{F}}(\overline{u}) \notin \overline{F}^{\times 2}$, hence $\overline{F}(\overline{u}) = \overline{D}$ and $F(u)$ is a maximal subfield of D, which is an inertial lift of $\overline{D}$. The extension $F(u)/F$ is then Galois with an elementary abelian Galois group of exponent 2. Let $\rho \in \mathrm{Gal}(F(u)/F)$, $\rho \neq I$. By Lemma 5.3 of [**17**], there exists a symplectic involution τ_ρ on D whose restriction to $F(u)$ is ρ. Moreover, Lemma 5.6 of [**17**] yields an element $d_\rho \in D^\times$ such that

$$d_\rho u d_\rho^{-1} = \rho(u), \quad \tau_\rho(d_\rho) = -d_\rho \quad \text{and} \quad \mathrm{Nrd}_D(d_\rho) \in F^{\times 2}.$$

Then, $\tau_\rho(d_\rho u) = -\rho(u)d_\rho = -d_\rho u$; hence $\sigma = \mathrm{Int}(d_\rho u) \circ \tau_\rho$ is an involution of orthogonal type. We have $d_\rho u \in (D,\sigma)_- \cap D^\times$, and hence

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_D(d_\rho u).F^{\times 2} = \mathrm{Nrd}_D(u).F^{\times 2},$$

completing the proof when $\mathrm{Nrd}_D(u) \notin F^{\times 2}$.

It only remains to consider the case where $\mathrm{Nrd}_D(u) \in F^{\times 2}$, which amounts to proving the existence of orthogonal involutions of trivial discriminant. Let T be an inertial lift of $\overline{D}$ in D and let $\rho \in \mathrm{Gal}(T/F)$, $\rho \neq I$. Also let $t \in T$ be such that $t^2 \in F^\times$ and $\rho(t) = -t$. By [**19**, Proposition 3.1.67] (or by Lemma 5.3 of [**17**] again), there exists a symplectic involution τ_ρ on D whose restriction to T is ρ. Then $\sigma = \mathrm{Int}(t) \circ \tau_\rho$ is an orthogonal involution of trivial discriminant. □

We finally investigate the case where D is inertially split but not semi-ramified. For the statement of the next proposition, we extend in a natural way the definition of the norm map $N_{Z(\overline{D})/\overline{F}}$ to subsets of $Z(\overline{D})^\times$ which are unions of cosets of $Z(\overline{D})^{\times 2}$. Thus,

$$N_{Z(\overline{D})/\overline{F}}(\mathcal{D}(\overline{D})) = \left\{ N_{Z(\overline{D})/\overline{F}}(d).f^2 \mid d \in \mathcal{D}(\overline{D}), f \in \overline{F}^\times \right\}.$$

PROPOSITION 5. *Assume D is inertially split but not semi-ramified and* $\deg D \geq 4$.

- *If $Z(\overline{D}) \neq \overline{F}$, then* $\mathcal{D}(D) = F^{\times 2} \cup i\left(N_{Z(\overline{D})/\overline{F}}\left(\mathcal{D}(\overline{D})\right)\right)$.

- *If* $Z(\overline{D}) = \overline{F}$, *then* $\mathcal{D}(D) = i\left(N_{Z(\overline{D})/\overline{F}}\left(\mathcal{D}(\overline{D})\right)\right)$.

Proof. The hypotheses on D ensure that $\overline{D}$ is not commutative, and hence $\overline{\sigma} \neq I$ for every involution σ on D. Propositions 2 and 3 then readily show that $\mathcal{D}(D)$ is contained in $F^{\times 2} \cup i(N_{Z(\overline{D})/\overline{F}}(\mathcal{D}(\overline{D})))$, and even in $i(N_{Z(\overline{D})/\overline{F}}(\mathcal{D}(\overline{D})))$ when $Z(\overline{D}) = \overline{F}$ since in this case $\overline{\sigma}$ cannot be of the second kind.

The reverse inclusion $i\left(N_{Z(\overline{D})/\overline{F}}\left(\mathcal{D}(\overline{D})\right)\right) \subset \mathcal{D}(D)$ follows from the fact that every orthogonal involution on $\overline{D}$ is of the form $\overline{\sigma}$ for some orthogonal involution σ on D, by Proposition 4. Moreover, if $Z(\overline{D}) \neq \overline{F}$, then Proposition 4 yields an orthogonal involution σ on D such that $\overline{\sigma}$ is of the second kind. For such an involution we have $\mathrm{disc}(\sigma) = F^{\times 2}$, by Proposition 2, hence $F^{\times 2} \subset \mathcal{D}(D)$. □

In [**20**], Rowen and Saltman ask whether there exists an orthogonal involution of trivial discriminant on every division algebra of degree at least 4. Propositions 1, 4 and 5 answer this question in the affirmative in the case where the center is Henselian with residue characteristic different from 2, except when $[D : F] = [\overline{D} : \overline{F}]$. In the latter case, the existence of an orthogonal involution with trivial discriminant on D is equivalent to the existence of such an involution on $\overline{D}$.

Propositions 1 and 4 actually prove more: they show that, with the possible exception of inertially split but not semi-ramified algebras D, one has:

$$\mathcal{D}(D) = \mathrm{Nrd}_D(D^\times).F^{\times 2}$$

when $\deg D \geq 4$. (This equality has also been proved for arbitrary division algebras of degree 4: see [**25**].) From Propositions 3 and 5, it readily follows that this equality holds for D inertially split and not semi-ramified if it holds for $\overline{D}$. As a final result, we show that this equality also holds for the inertially split division algebras whose residue algebra is a quaternion algebra (where it is easy to construct examples where the equality does not hold for $\overline{D}$).

PROPOSITION 6. *Suppose* D *is inertially split,* $\deg D \geq 4$. *If* $\overline{D}$ *is a quaternion algebra, then*

$$\mathcal{D}(D) = \mathrm{Nrd}_D(D^\times).F^{\times 2}.$$

Proof. Since $\deg D \geq 4$ and $\deg \overline{D} = 2$, we have $[Z(\overline{D}) : \overline{F}] \geq 2$. Propositions 3 and 5 yield the following descriptions of $\mathcal{D}(D)$ and $\mathrm{Nrd}_D(D^\times).F^{\times 2}$:

$$\mathrm{Nrd}_D(D^\times).F^{\times 2} = i\left(N_{Z(\overline{D})/\overline{F}}(\mathrm{Nrd}_{\overline{D}}(\overline{D}^\times))\overline{F}^{\times 2}\right),$$
$$\mathcal{D}(D) = i\left(\overline{F}^{\times 2} \cup N_{Z(\overline{D})/\overline{F}}(\mathcal{D}(\overline{D}))\right).$$

Since i is injective and since $\mathcal{D}(D) \subset \mathrm{Nrd}_D(D^\times).F^{\times 2}$, it suffices to show

$$N_{Z(\overline{D})/\overline{F}}\left(\mathrm{Nrd}_{\overline{D}}(\overline{D}^\times)\right) \subset \overline{F}^{\times 2} \cup N_{Z(\overline{D})/\overline{F}}\left(\mathcal{D}(\overline{D})\right).$$

Let K be an intermediate field between $Z(\overline{D})$ and $\overline{F}$, of codimension 2 in $Z(\overline{D})$. By Proposition 4, $\overline{D}$ has an involution of the second kind which leaves K elementwise invariant. A theorem of Albert [**1**, Theorem 10.21] then shows that

$$\overline{D} \simeq Q \otimes_K Z(\overline{D}) \tag{14}$$

for some quaternion algebra Q over K. Let φ be the reduced norm form on Q, which is a 4-dimensional quadratic form over K. Also let $\varphi_{Z(\overline{D})}$ denote the quadratic form on $Z(\overline{D})$ obtained by extending scalars; this is the reduced norm form on $\overline{D}$. The reduced norms of $\overline{D}^\times$ are then the similarity factors of $\varphi_{Z(\overline{D})}$:

$$\mathrm{Nrd}_{\overline{D}}(\overline{D}^\times) = G\left(\varphi_{Z(\overline{D})}\right)$$

and it follows from Scharlau's norm principle (see [**21**, Theorem2.8.6]) that

$$N_{Z(\overline{D})/K}(\mathrm{Nrd}_{\overline{D}}(\overline{D}^\times)) \subset G(\varphi) \cap N_{Z(\overline{D})/K}(Z(\overline{D})^\times)$$
$$= \mathrm{Nrd}_Q(Q^\times) \cap N_{Z(\overline{D})/K}(Z(\overline{D})^\times).$$

Let $d \in K^\times$ be a non-square in $N_{Z(\overline{D})/K}(\mathrm{Nrd}_{\overline{D}}(\overline{D}^\times))$. Theorem 4.2 of [**12**] then proves the existence of a quadratic extension L of $Z(\overline{D})$ which splits Q and whose discriminant as a quartic extension of K is $dK^{\times 2}$. Let $L = Z(\overline{D})(\sqrt{z})$ for some $z \in Z(\overline{D})$. A direct computation yields $dK^{\times 2} = N_{Z(\overline{D})/K}(z)K^{\times 2}$. Moreover, since L

splits Q, we may view L as a subfield of $Q \otimes_K Z(\overline{D}) = \overline{D}$. If $\overline{\sigma}$ is an orthogonal involution on $\overline{D}$ which induces on L the non-trivial automorphism over $Z(\overline{D})$, we then have

$$N_{Z(\overline{D})/K}(\mathrm{disc}(\overline{\sigma})) = N_{Z(\overline{D})/K}\left(-zZ(\overline{D})^{\times 2}\right) = N_{Z(\overline{D})/K}(zZ(\overline{D})^{\times 2}).$$

Therefore, every non-square in $N_{Z(\overline{D})/K}\left(\mathrm{Nrd}_{\overline{D}}\left(\overline{D}^{\times}\right)\right)$ is in $N_{Z(\overline{D})/K}(\mathcal{D}(\overline{D}))$, and

$$N_{Z(\overline{D})/K}\left(\mathrm{Nrd}_{\overline{D}}\left(\overline{D}^{\times}\right)\right) \subset K^{\times 2} \cup N_{Z(\overline{D})/K}(\mathcal{D}(\overline{D})). \tag{15}$$

The proposition follows by taking the norm of both sides from K down to $\overline{F}$. □

Alternatively, after obtaining relation (14), one may consider the Laurent series field $K' = K((X))$, the quaternion algebra $Q' = (Z(\overline{D})((X))/K', X)_{K'}$ and $D' = Q \otimes_{K'} Q'$. The algebra D' is a division algebra of degree 4; therefore, by [**25**],

$$\mathcal{D}(D') = \mathrm{Nrd}_{D'}(D'^{\times}).K'^{\times 2}.$$

On the other hand, the X-adic valuation on K' extends to a valuation on D' for which $\overline{D'} = \overline{D}$. Propositions 3 and 5 then readily yield inclusion (15).

References

[1] A. A. Albert, *Structure of Algebras*, Amer. Math Soc. Coll Pub. 24, Providence, R.I., 1961.

[2] S. A. Amitsur, L. H. Rowen, and J.-P. Tignol, *Division algebras of degree 4 and 8 with involution*, Israel H. Math., **33** (1979), 133-148.

[3] M. Chacron and A. Wadsworth, *On devomposing c-valued division rings*, J. Algebra, **134** (1990), 182-208.

[4] M. Chacron, *Decomposing and ordering a certain crossed product*, Private papers, 1992.

[5] J. Dieudonné, *On the structure of unitary groups*, Trans. Amer. Math. Soc., **72** (1952), 367-385.

[6] P. Draxl, *Skew Field*, London Mat. Soc. Lecture note Series 81. Cambridge Univ. Press, Cambridge, 1983.

[7] P. Draxl, *Ostrowski's theorem for Henselian valued skew fields*, J. Reine Angew. Math., **354** (1984), 213-218.

[8] Yu. Ershov, *henselian valuations of deveseon rengs and the group* K_1, Mate. Sbornik, **117 (159)** (1982), 60-68, (English trans. Math. USSR Sbornik, **45** (1983), 63-71.

[9] B. Jacob and A. Wadsworth, *Division algebras over Henselian fields*, J. Algebra, **128** (1990), 126-179.

[10] M.-A. Knus, R. Parimala and R. Sridharan, *On the discriminant of an involution*, Bull. soc. Math belgique, Sér. A, **43** (1991), 89-98.

[11] M.-A. Knus, R. Parimala and R. Sridharan, *Involutions on rank* 16 *central simple algebras*, J. Indian Math. Soc., **57** (1991), 143-151.

[12] T. Y. Lam, D. B. Leep and J.-P. Tignol, *Biquaternion algebras and quartic extensions*, preprint PAM-526, Univ. California, Berkeley, 1991.

[13] P. Morandi, *the Henselisation of a valued division algebra*, J. Algebra, **122** (1989), 232-243.

[14] R. Parimala, R. Sridharan and v. Suresh, *A question on the discriminants of involutions of central division algebras*, preprint, October 1992.

[15] R. S. Pierce, *Associative Algebras*, Graduate Text Math. 88, Springer-Verlag, New York, 1982.

[16] V. P. Platonov, *Dieudonné's conjecture and the nonsurjectivity on k-points of coverings of algebraic groups*, Dokl. Akad Nauk SSSR, **216** (1974), 986-989, (English trans. Soviet Math. Dokl., **15** (1974), 927-931).

[17] V. P. Platonov and V. I. Yanchevskiĭ, *Dieudonné's conjecture on the structure of unitary groups over a division ring, and hermitian* K*- theory*, Izv. Akad. Nauk SSSR, Ser. Mat., **48** (1984) 1266-1294, (English trans. Math. USSR-Izv., **25** (1985), 573-599).

[18] L. H. Rowen, *Central simple algebras*, Israel J. Math., **29** (1978), 285-301.

[19] L. H. Rowen, *Polynomial Identities in Ring Theory*, Academic Press, New York, 1980.

[20] L. H. Rowen and D. J. Saltman, *The discriminant of an involution*, preprint.

[21] W. Scharlau, Quadratic and Hermitian Forms, Grundlehren Math. Wiss. 270, Springer-Verlag, Berlin, 1985.

[22] O. F. G. Schilling, *The Theory of Valuations*, Math. Surveys 4. Amer. Math. Soc., Providence, R.I., 1950.

[23] J. Tits, *Formes quadratiques, groupes orthogonaux et algbres de Clifford*, Invent. Math., **5** (1968), 19-41.

[24] J.-P. Tignol and A. Wadsworth, *Totally ramified valuations on finite dimensional division algebras*, Trans. Amer. Math. Soc., **302** (1987), 223-250.

[25] J.-P. Tignol, *Discriminants of involutions on biquaternion algebres, after Knus and Lam*, private papers, 1991.

[26] A. Wadsworth, private papers.

Received June 9, 1992 and in revised form October 1, 1992. Supported in part by the F.N.R.S. The third author would like to thank the first author and Carleton University, Ottawa for their hospitality while the research for this paper was initiated. The forth author was supported in part by the N.S.F. The fifth author would like to thank the third author and the Université Catholique de Louvain for their hospitality while part of the work for this paper was being done.

CARLETON UNIVERSITY
OTTAWA, CANADA K1S 5B6
E-mail address: mathstat@carleton.ca

INSTITUT DE MATHÉMATIQUE PURE ET APPLIQUÉE
UNIVERSITÉ CATHOLIQUE DE LOUVAIN
B 1348 LOUVAIN-LA-NEUVE, BELGIUM
E-mail address: tignol@agel.ucl.ac.be

UNIVERSITY OF CALIFORNIA, SAN DIEGO
LA JOLLA, CALIFORNIA 92093-0112
E-mail address: arwadsworth@ucsd.edu

INSTITUTE OF MATHEMATICS
ACADEMY OF SCIENCES OF BELARUS
MINSK, BELARUS 220072
E-mail address: imanb@adonis.ias.msk.su