Decomposition of Involutions on Inertially Split Division Algebras

Patrick J. Morandi B.A. Sethuraman

December 22, 2000

Abstract

Let F be a Henselian valued field with $\mathrm{char}(\overline{F}) \neq 2$, and let S be an inertially split F-central division algebra with involution σ^* that is trivial on an inertial lift in S of the field $Z(\overline{S})$. We prove necessary and sufficient conditions for S to contain a σ^*-stable quaternion F-subalgebra, and for (S, σ^*) to decompose into a tensor product of quaternion algebras. These conditions are in terms of decomposability of an associated residue central simple algebra $\overline{I}$ that arises from a Brauer group decomposition of S.

1 Introduction

Let S be a central simple algebra with center F. If S has an involution σ, then a fundamental problem is to determine when does (S, σ) decompose. In other words, when are there proper F-subalgebras S_1 and S_2 such that $S = S_1 \otimes_F S_2$ and $\sigma = \sigma_1 \otimes \sigma_2$ for some involutions σ_i on S_i? If $\deg(S) = 4$ and $\sigma|_F = \mathrm{id}$, then a theorem of Albert [**?**, Ch. XI, Thm. 9] says that S decomposes into a tensor product of quaternion algebras. However, it may not be the case that (S, σ) decomposes; the first example of an indecomposable involution was given by Amitsur, Rowen, and Tignol in [**?**]. In [**?**], Knus, Parimala, and Sridharan gave a necessary and sufficient condition on an algebra of degree 4 with involution (of the first kind) to decompose. For algebras with involution of larger degree, it is generally a difficult question to determine when it decomposes.

In [**?**] Dherte studied decomposability of involutions on certain Malcev-Neumann division algebras. More precisely, if K/F is an elementary Abelian 2-extension with Galois group G, and if $f \in Z^2(G, K^*)$, then one can construct the Malcev-Neumann series division ring $S(A/K/F)$, where A is the crossed product algebra $(K/F, G, f)$. The center $\widehat{F}$ of $S(A/K/F)$ is a field of formal series over F, and $S(A/K/F)$ has a maximal subfield $\widehat{K}$ such that $\mathrm{Gal}(\widehat{K}/\widehat{F}) = G$. Moreover, $S(A/K/F) = (\widehat{K}/\widehat{F}, G, \widehat{f})$ for a cocycle $\widehat{f}$ related to f. If $S(A/K/F) = \oplus_{g \in G} \widehat{K} z_g$ with $z_g z_h = \widehat{f}(g,h) z_{gh}$ and $A = \oplus_{g \in G} K x_g$ with $x_g x_h = f(g,h) x_{gh}$, then there is an involution σ^* on $S(A/K/F)$ with $\sigma^*|_{\widehat{K}} = \mathrm{id}$ and $\sigma^*(z_g) = z_g$, and an involution σ on A with $\sigma|_K = \mathrm{id}$ and $\sigma(x_g) = x_g$. Dherte proved that $S(A/K/F)$ has a

σ^*-stable $\widehat{F}$-central quaternion algebra if and only if A has a σ-stable F-central quaternion algebra, and also that $(S(A/K/F), \sigma^*)$ decomposes into a tensor product of quaternion algebras if and only if (A, σ) decomposes into a tensor product of quaternion algebras. A fundamental technique in [**?**] was valuation theory; the field $\widehat{F}$ has a Henselian valuation with residue field F, and so this valuation extends to $S(A/K/F)$.

In this paper we study the question of decomposability of involutions on inertially split division algebras defined over Henselian valued fields. To be more precise, let F be a Henselian valued field with $\mathrm{char}(\overline{F}) \neq 2$. If S is an F-central division algebra, then S is said to be inertially split if there is an inertial extension K/F such that K is a splitting field for S. The structure of inertially split division algebras was investigated by Jacob and Wadsworth in [**?**, Sec. 5]. In particular, by [**?**, Lemma 5.14], there is a natural but not unique decomposition of S, up to similarity, as $S \sim I \otimes_F N$, where I is similar to an inertial division algebra and N is a nicely semiramified division algebra (see [**?**, Sec. 2, 3] for definitions). For the Malcev-Neumann algebra $S(A/K/F)$ mentioned above, by viewing $f \in Z^2(G, \widehat{K}^*)$, the cocycle $\widehat{f}$ factors as $\widehat{f} = fc$ with c a symmetric cocycle having values in $\widehat{F}^*$, and this factorization gives a similarity relation $S(A/K/F) \sim (A \otimes_F \widehat{F}) \otimes_{\widehat{F}} (\widehat{K}/\widehat{F}, G, c)$, which is a special case of the decomposition of [**?**]. The algebra A, if it is a division algebra, is the residue algebra of the inertial algebra $A \otimes_F \widehat{F}$.

Suppose that $S \sim I \otimes_F N$ as above has exponent 2. By starting with an involution σ^* on S that is trivial on an inertial lift of $Z(\overline{S})$, and by representing S and I as generalized crossed products in a natural way, we produce an involution σ on I, and σ induces an involution $\overline{\sigma}$ on an $\overline{F}$-central simple algebra $\overline{I}$. The algebra $\overline{I}$ is, in some sense, the residue algebra of the central simple algebra I. We prove that S has an F-central quaternion subalgebra stable under σ^* if and only if $\overline{I}$ has an $\overline{F}$-central quaternion subalgebra stable under $\overline{\sigma}$, and (S, σ^*) decomposes into a tensor product of quaternion algebras if and only if $(\overline{I}, \overline{\sigma})$ decomposes into a tensor product of quaternion algebras. We thus extend Dherte's results to the context of inertially split algebras over a Henselian valued field with residue characteristic not 2. We remark that in [**?**, Thm. 5] it is proved that if D is a division algebra of exponent 2 over a Henselian valued field F (with $\mathrm{char}(\overline{F}) \neq 2$) and if D has an involution σ of the first kind with $\overline{\sigma} = \mathrm{id}$ on $\overline{D}$, then D can be decomposed as $D = S \otimes_F T$ with S inertially split and T totally ramified, and each of S and T are stable under σ. Moreover, $(T, \sigma|_T)$ decomposes into a tensor product of quaternion algebras. Thus, at least for involutions with $\overline{\sigma} = \mathrm{id}$, the question of decomposability reduces to the case of inertially split division algebras.

If F is a field with Henselian valuation v, recall (e.g., [**?**, Thm.]) that v extends uniquely to a valuation on any finite dimensional F-division algebra. If D is an F-central division algebra with valuation, we will denote the value group of D by Γ_D and the residue division algebra by $\overline{D}$. The group of valuation units of D will be denoted U_D, and the subgroup of 1-units by $U_{1,D}$. If d is in the valuation ring of D, we denote the image of d in $\overline{D}$ by $\overline{d}$. Recall that the valuation ring is stable under F-algebra automorphisms of D and under involutions of the first kind; this is a consequence of [**?**, Thm.]. Therefore, an F-algebra automorphism φ (resp. involution) of D induces an automorphism $\overline{\varphi}$ (resp. involution) of $\overline{D}$ by $\overline{\varphi}(\overline{d}) = \overline{\varphi(d)}$.

We give some more notation that we will use throughout this paper. If F is a field, then $\mathrm{Br}(F)$ is the Brauer group of classes of central simple F-algebras, and $\mathrm{Br}_2(F)$ is the 2-torsion subgroup of $\mathrm{Br}(F)$. If S is a central simple algebra and B is a subalgebra of S, then $C_S(B)$ is the centralizer of B in S. For $s \in S^*$, the inner automorphism $x \mapsto sxs^{-1}$ will be denoted by $\mathrm{Int}(x)$, and the group of F-algebra automorphisms of S by $\mathrm{Aut}_F(S)$. The reduced norm on S will be denoted by Nrd, or by Nrd_S if we are working with more than one central simple algebra.

If S is an F-central simple algebra, then an involution σ on S is an anti-automorphism of S with $\sigma^2 = \mathrm{id}$. If $\sigma|_F = \mathrm{id}$, then σ is said to be of the first kind; otherwise σ is of the second kind. We will write $\mathrm{Sym}(S, \sigma)$ and $\mathrm{Skew}(S, \sigma)$ to denote the F-subspaces of symmetric and skew-symmetric elements of σ, respectively. If σ is of the first kind and if $n = \deg(S)$, then it is known that $\dim_F(\mathrm{Sym}(S, \sigma)) = \frac{1}{2}n(n + \varepsilon)$ with ε either 1 or -1. We refer to ε as the *type* of σ. Involutions of type 1 are often called orthogonal, and symplectic if they are of type -1. If σ is of the second kind and if F_0 is the fixed field of F under σ, then $\mathrm{Sym}(S, \sigma)$ is an F_0-subspace of S, and $\dim_{F_0}(\mathrm{Sym}(S, \sigma)) = \frac{1}{2}\dim_{F_0}(S)$.

In this paper we will use generalized crossed products, which we now describe briefly. More details and proofs about generalized cross products can be found in [**?**] or [**?**]. If Z/F is a finite Galois extension with $G = \mathrm{Gal}(Z/F)$ and if C is a Z-central simple algebra, then a *generalized cocycle* of G with values in C^* is a pair (ω, f) of maps with

$$\omega : G \to \mathrm{Aut}_Z(C),$$
$$f : G \times G \to C^*$$

such that $\omega_g|_Z = g$ for $g \in G$, and

$$\omega_g \circ \omega_h = \mathrm{Int}(f(g, h)) \circ \omega_{gh},$$
$$f(g, h)f(gh, k) = \omega_g(f(h, k))f(g, hk)$$

for all g, h, $k \in G$. We will refer to the set of generalized cocycles of G with values in C^* by $\mathcal{Z}(G, C^*)$.

Given a generalized cocycle $(\omega, f) \in \mathcal{Z}(G, C^*)$, we can construct the *generalized crossed product* $(C, G, (\omega, f)) = \oplus_{g\in G} C x_g$, where multiplication is determined by

$$x_g c = \omega_g(c)x_g,$$
$$x_g x_h = f(g, h)x_{gh}$$

for all $c \in C$ and $g, h \in G$. This is an F-central simple algebra containing C, and the centralizer of Z in $(C, G, (\omega, f))$ is precisely C. We will call the x_g *cocycle generators* for $(C, G, (\omega, f))$.

Conversely, if S is an F-central algebra containing Z, then set $C = C_S(Z)$. We can write S as a generalized crossed product in the following way. By the Noether-Skolem theorem, for each $g \in G$ there is an $x_g \in S^*$ with $\mathrm{Int}(x_g)|_Z = g$. Let $\omega : G \to \mathrm{Aut}_F(C)$ be given by $\omega_g = \mathrm{Int}(x_g)|_C$, and define $f : G \times G \to C^*$ by $f(g,h) = x_g x_h x_{gh}^{-1}$. A short calculation shows that $(\omega, f) \in \mathcal{Z}(G, C^*)$ and $S = \oplus_{g \in G} C x_g$, so $S = (C, G, (\omega, f))$.

If (ω, f) and (ω', f') are two generalized cocycles of G with values in C^*, then they are said to be *cohomologous* if there are elements $c_g \in C^*$ such that

$$\omega'_g = \mathrm{Int}(c_g) \circ \omega_g,$$
$$f'(g,h) = c_g \omega_g(c_h) f(g,h) c_{gh}^{-1}$$

for all $g, h \in G$. The F-algebras $(C, G, (\omega, f))$ and $(C, G, (\omega', f'))$ are isomorphic if and only if (ω, f) and (ω', f') are cohomologous.

2 Involutions on Generalized Crossed Products

In this section we investigate involutions on generalized crossed products. As pointed out in the introduction, if S is an inertially split F-central division algebra, we will decompose $S \sim I \otimes_F N$, and we will represent S and I as generalized crossed products, each of the form $(C, G, (\omega, f))$ with C a division algebra and $Z(C)$ an elementary Abelian 2-extension of F with Galois group G. We will use the results of this section to associate to an involution on S an involution on a residue algebra $\overline{I}$, and to write S, I, and $\overline{I}$ as generalized crossed products in a convenient way with regard to the involutions.

We will use the following lemma to show that if S has an involution of the first kind, then S has an involution that is the identity on the subfield $Z(C)$.

Lemma 2.1 *Let T be an F-central simple algebra of exponent 2. Suppose that Z is a subfield of T that contains F such that $C_T(Z)$ is a division algebra. Then there is an involution σ on T with $\sigma|_Z = \mathrm{id}$. Moreover, if σ is an involution on $C_T(Z)$ that is trivial on Z, then σ extends to an involution on T.*

Proof. Since $2[T] = 0$ in $\mathrm{Br}(F)$, there is an involution τ of the first kind on T by [**?**, §16, Thm. 1]. The field $\tau(Z)$ is F-isomorphic to Z, so there is an $x \in T^*$ with $xax^{-1} = \tau(a)$ for all $a \in Z$. Applying τ to the equation $xa = \tau(a)x$, we get $\tau(a)\tau(x) = \tau(x)a$. If $\varepsilon = \pm 1$, then

$$xax^{-1}(\tau(x) + \varepsilon x) = \tau(a)(\tau(x) + \varepsilon x) = (\tau(x) + \varepsilon x)a.$$

Multiplying by x^{-1} on the left gives

$$ax^{-1}(\tau(x) + \varepsilon x) = x^{-1}(\tau(x) + \varepsilon x)a$$

which implies that $x^{-1}(\tau(x) + \varepsilon x) \in C_T(Z)$, or $\tau(x) + \varepsilon x \in xC_T(Z)$. Since both $\tau(x) + x$ and $\tau(x) - x$ cannot be zero, one is invertible as $C_T(Z)$ is a division algebra. By conjugating σ by whichever is nonzero, we obtain an involution on T that is the identity on Z.

Now, suppose that σ is an involution of the first kind on $C_T(Z)$. Since $2[T] = 0$, there is an involution τ on T with $\tau|_Z = \mathrm{id}$ by the first paragraph. Then $\tau(C_T(Z)) = C_T(Z)$, so τ restricts to an involution of the first kind on $C_T(Z)$. Therefore, there is an $x \in C_T(Z)$ with $\sigma(x) = \pm x$ and $\tau|_{C_T(Z)} = \mathrm{Int}(x) \circ \sigma$. Then $\tau(x) = \pm x$, and so $\mathrm{Int}(x^{-1}) \circ \tau$ is an involution on T that extends σ. ■

Let Z/F be an elementary Abelian 2-extension with Galois group G. If C is a Z-central division algebra, we show that if $T = (C, G, (\omega, f))$ is a generalized crossed product that has an involution σ with $\sigma|_Z = \mathrm{id}$, then we may find new cocycle generators to represent $T = \oplus_g C x_g$ with $\sigma(x_g) = x_g$. Note that the previous lemma shows that T has an involution σ with $\sigma|_Z = \mathrm{id}$ provided that $[T] \in \mathrm{Br}_2(F)$.

Proposition 2.2 *Let C/Z be a division algebra and let $T = (C, G, (\omega, f)) = \oplus_g C x_g$ be a generalized crossed product. Suppose that σ is an involution on T with $\sigma|_Z = \mathrm{id}$. Then the generalized cocycle (ω, f) can be replaced by a cohomologous cocycle (ω', f') in such a way that σ can be extended to $T = (C, G, (\omega', f')) = \oplus_g D x'_g$ with $\sigma(x'_g) = x'_g$.*

Proof. We note a few things that we will use in the proof. First, let $\lambda_g = \omega_g \circ \sigma$, an antiautomorphism of C. The map λ_g^2 is an automorphism that fixes Z. Moreover, if $c_g = \sigma(x_g)x_g^{-1}$, then we claim that $c_g \in C^*$ and $\lambda_g^2 = \mathrm{Int}(c_g^{-1})|_C$. To see that $c_g \in C$, we must show that it commutes with Z. If $a \in Z$, then

$$\begin{aligned}\sigma(x_g)x_g^{-1}a &= \sigma(x_g)g(a)x_g^{-1} = \sigma(g(a)x_g)x_g^{-1} \\ &= \sigma(x_g a)x_g^{-1} = a\sigma(x_g)x_g^{-1}.\end{aligned}$$

This proves that $c_g \in C^*$. Next, we have

$$\begin{aligned}\lambda_g^2 &= \omega_g \circ \sigma \circ \omega_g \circ \sigma = \mathrm{Int}(x_g)|_C \circ \sigma \circ \mathrm{Int}(x_g)|_C \circ \sigma \\ &= \mathrm{Int}(x_g)|_C \circ \mathrm{Int}(\sigma(x_g)^{-1})|_C \circ \sigma^2 = \mathrm{Int}(x_g\sigma(x_g)^{-1})|_C = \mathrm{Int}(c_g^{-1})|_C,\end{aligned}$$

which gives the second claim. Furthermore, since $\sigma(x_g) = c_g x_g$, applying σ to this equation yields $x_g = c_g x_g \sigma(c_g) = c_g \lambda_g(c_g) x_g$, giving $c_g \lambda_g(c_g) = 1$. We wish to find $b_g \in C^*$ so that $\sigma(b_g x_g) = b_g x_g$. For this to happen, we must have $c_g \lambda_g(b_g) = b_g$. To produce b_g for a fixed g, choose $u \in C$ so that if $b_g = u + c_g\lambda_g(u)$, then $b_g \neq 0$. Such a u exists; if $c_g \neq -1$, then set $u = 1$. If $c_g = -1$, then let $u \in Z$ be any element with $g(u) \neq u$. This will guarantee that $b_g = u + c_g\lambda_g(u) \neq 0$. We then get

$$\begin{aligned}\lambda_g(b_g) &= \lambda_g(u) + \lambda_g^2(u)\lambda_g(c_g) = \lambda_g(u) + c_g^{-1}uc_g\lambda_g(c_g) \\ &= \lambda_g(u) + c_g^{-1}u.\end{aligned}$$

Thus, $c_g\lambda_g(b_g) = u + c_g\lambda_g(u) = b_g$, as desired. Therefore, if we define new cocycle (ω', f') by

$$\omega'_g = \mathrm{Int}(b_g) \circ \omega_g,$$

$$f'(g,h) = b_g \omega_g(b_h) f(g,h) b_{gh}^{-1}$$

and set $x'_g = b_g x_g$, then we have the desired condition $\sigma(x'_g) = x'_g$. ■

Given an involution σ on $(C, G, (\omega, f)) = \oplus_{g \in G} C x_g$, we next determine necessary and sufficient conditions on a generalized cocycle (ω, f) for σ to satisfy $\sigma(x_g) = x_g$ for all $g \in G$.

Lemma 2.3 *Let $(C, G, (\omega, f)) = \oplus_g C x_g$ be a generalized crossed product. If σ is an involution of the first kind on C, then σ can be extended to $(C, G, (\omega, f))$ with $\sigma(x_g) = x_g$ if and only if for all g, $h \in G$,*

$$\omega_{gh}(\sigma(f(g,h))) = f(h,g),$$
$$(\omega_g \circ \sigma)^2 = \mathrm{id}\,.$$

Proof. First, suppose that σ satisfies $\sigma(x_g) = x_g$. For all $c \in C$, we have $\sigma(c x_g) = x_g \sigma(c) = \omega_g(\sigma(c)) x_g$. So,

$$\begin{aligned} c x_g &= \sigma(\sigma(c x_g)) = \sigma(\omega_g(\sigma(c)) x_g) \\ &= x_g \sigma(\omega_g(\sigma(c))) \\ &= \omega_g(\sigma(\omega_g(\sigma(c)))) x_g. \end{aligned}$$

Thus, $(\omega_g \circ \sigma)^2 = \mathrm{id}$ on C.

Next, we have $x_g x_h = f(g,h) x_{gh}$, so

$$\sigma(x_g x_h) = x_h x_g = f(h,g) x_{hg} = f(h,g) x_{gh}$$

and

$$\begin{aligned} \sigma(x_g x_h) &= \sigma(f(g,h) x_{gh}) = x_{gh} \sigma(f(g,h)) \\ &= \omega_{gh}(\sigma(f(g,h))) x_{gh}. \end{aligned}$$

Therefore,

$$f(h,g) = \omega_{gh}(\sigma(f(g,h))).$$

These calculations clearly reverse to show that given an involution σ on C, then σ extends to $(C, G, (\omega, f)) = \oplus_g C x_g$ with $\sigma(x_g) = x_g$ if and only if the cocycle (ω, f) satisfies

$$\omega_{gh}(\sigma(f(g,h))) = f(h,g),$$
$$(\omega_g \circ \sigma)^2 = \mathrm{id}$$

for all $g, h \in G$. ■

3 Involutions on Inertially Split Division Algebras

Let (F, v) be a Henselian valued field with $\mathrm{char}(\overline{F}) \neq 2$. If S is an inertially split F-central division algebra of exponent 2, we describe the involutions we will use and how we will write S as a generalized crossed product. By abuse of notation, we will write v for the unique extension of v to any finite dimensional division algebra containing F.

Let Z be an inertial lift in S of $Z(\overline{S})$. Then Z/F is Abelian Galois with $\mathrm{Gal}(Z/F) \cong \mathrm{Gal}(Z(\overline{S})/\overline{F}) \cong \Gamma_S/\Gamma_F$, and $\mathrm{Gal}(Z/F)$ is an elementary Abelian 2-group; these facts can be found in [**?**, Lemma 5.1, Cor. 6.10]. By Lemma 2.1, there is an involution σ^* on S with $\sigma^*|_Z = \mathrm{id}$. Let $C = C_S(Z)$. Then C/Z is inertial with $\overline{S} = \overline{C}$ by [**?**, Lemma 1.8]. The involution σ^* restricts to an involution of the first kind on C since $\sigma^*|_Z = \mathrm{id}$. We may write S as a generalized cocycle $S = (C, G, (\omega, k))$, where $G = \mathrm{Gal}(Z/F)$. Moreover, by Proposition 2.2, we may assume that $S = \oplus_{g\in G} C y_g$ with $\sigma^*(y_g) = y_g$ for all $g \in G$. As described in the proof of [**?**, Thm. 5.6(b)] we may factor our generalized cocycle as $(\omega, k) = (\omega, fc)$ such that (ω, f) is a generalized cocycle with $f(g, h) \in U_C$ for all $g, h \in G$ and $c \in Z^2(G, F^*)$ is a symmetric cocycle with values in F^*. Let $I = (C, G, (\omega, f))$. Then I is similar to an inertial division algebra, although I itself need not be a division algebra. The generalized cocycle (ω, f) satisfies the hypotheses of Lemma 2.3 because (ω, fc) satisfies them and c is symmetric with values in F^*. Therefore, there is an involution σ on $I = \oplus_{g\in G} C x_g$ with $\sigma|_C = \sigma^*|_C$ and $\sigma(x_g) = x_g$.

Our aim is to describe decomposability of (S, σ^*) in terms of decomposability of an associated involution on a residue algebra $\overline{I}$. Since I may not be a division algebra, we must define $\overline{I}$. The pair (ω, f) is a generalized cocycle with $f(g, h) \in U_C$ for each $g, h \in G$. Therefore, there is a well defined function $\overline{f} : G \times G \to \overline{C}^*$ given by $\overline{f}(g, h) = \overline{f(g, h)}$. Also, $\omega_g \in \mathrm{Aut}_F(C)$ with $\omega_g|_Z = g$, and since $v \circ g = v$, we see that $v \circ \omega_g$ is a valuation on C that extends v. Thus, by [**?**, Thm.], $v \circ \omega_g = v$. This implies that ω_g sends the valuation ring of C to itself, so there is an induced map $\overline{\omega_g} : \overline{C} \to \overline{C}$, and $\overline{\omega_g} \in \mathrm{Aut}_{\overline{F}}(\overline{C})$. If we define $\overline{\omega} : G \to \mathrm{Aut}_{\overline{F}}(\overline{C})$ by $\overline{\omega}_g = \overline{\omega_g}$, then it is easy to see that $(\overline{\omega}, \overline{f})$ is a generalized cocycle for G with values in $\overline{C}^*$. So, we have an $\overline{F}$-central simple algebra $(\overline{C}, G, (\overline{\omega}, \overline{f}))$, and we set $\overline{I} = (\overline{C}, G, (\overline{\omega}, \overline{f}))$. Alternatively, if V_F and V_C are the valuation rings of F and C, respectively, then $A = \oplus_{g\in G} V_C x_g$ is the unique up to isomorphism Azumaya V_F-order in I, and $A/J(A) = (\overline{C}, G, (\overline{\omega}, \overline{f})$. Finally, we describe the residue involution $\overline{\sigma}$ on $\overline{I}$. The involution $\sigma|_C$ on the division algebra C induces an involution $\overline{\sigma|_C}$ on $\overline{C}$. The generalized cocycle $(\overline{\omega}, \overline{f})$ clearly satisfies the hypotheses of Lemma 2.3, so there is an involution $\overline{\sigma}$ on $\overline{I} = \oplus_{g\in G} \overline{C}\,\overline{x_g}$ with $\overline{\sigma}|_{\overline{C}} = \overline{\sigma|_C}$ and $\overline{\sigma}(\overline{x_g}) = \overline{x_g}$.

To help us go between S and $\overline{I}$, we will use the "leading monomial" map on S. Recall that on $S = \oplus_g C y_g$, where $\mathrm{Int}(y_g)|_C = \omega_g$ and $y_g y_h = (fc)(g, h) y_{gh}$, we have $\mathrm{Int}(y_g)|_Z = g$. Under the map $\theta_S : \Gamma_S/\Gamma_F \to \mathrm{Gal}(\overline{Z}/\overline{F})$ of [**?**, Prop. 1.7], we have $\theta_S(v(y_g) + \Gamma_F) = \overline{g}$. Therefore, via the identification $\theta_S : \mathrm{Gal}(Z/F) \cong \Gamma_S/\Gamma_F$, we have $v(y_g) + \Gamma_F = g$. Consequently, the values $v(y_g)$ are distinct modulo $\Gamma_F = \Gamma_C$. So, for an arbitrary $a = \sum_g a_g y_g \in S$, we have $v(a) = v(a_g y_g)$ for a uniquely determined "monomial" $a_g y_g$. We set $\mu(a) = a_g y_g$, and call

$\mu(a)$ the leading monomial of a. We point out the properties of the leading monomial map in the following lemma.

Lemma 3.1 *Let μ be the leading monomial map on S. Then $v(\mu(a)) = v(a)$. Also, $\mu(\sigma^*(a)) = \sigma^*(\mu(a))$. Finally, $\mu(a) = au$ for some 1-unit u.*

Proof. The first property comes immediately from the definition of μ. For the second, we note that if $a_g \in C$, then $\sigma^*(a_g y_g) = y_g \sigma(a_g) = \omega_g(\sigma(a_g))y_g$, so σ^* takes monomials to monomials. Moreover, Both ω_g and σ are value preserving. These two facts imply that $\mu \circ \sigma^* = \sigma^* \circ \mu$. Lastly, $\mu(a)a^{-1}$ is a 1-unit because $v(\mu(a)) = v(a)$ and a is the sum of $\mu(a)$ and other terms of value strictly greater than $v(\mu(a))$. ■

The leading monomial map is not multiplicative. However, as a consequence of the lemma above, we have $\mu(ab) \equiv ab \bmod (U_{1,S})$.

The involutions we have constructed are all of the first kind. We note in the next result that all them are of the same type.

Proposition 3.2 *The involutions σ^*, σ, $\sigma|_C$, and $\overline{\sigma}$ are all of the same type.*

Proof. We prove this by considering the following situation: $T = (C, G, (\omega, f)) = \oplus_g C x_g$ and σ is an involution on T that is trivial on Z with $\sigma(x_g) = x_g$. Then $\sigma(c_g x_g) = x_g \sigma(c_g) = \omega_g(\sigma(c_g))x_g$. Let $\lambda_g = \omega_g \circ \sigma$. Then, by Lemma 2.3, we see that $\lambda_g^2 = \mathrm{id}$. The map λ_g is an antiautomorphism of C, so λ_g is an involution of C. Note that $\lambda_g|_Z = g$, so λ_g is an involution of the second kind when $g \neq 1$. Also, $\sigma(c_g x_g) = c_g x_g$ if and only if $\lambda_g(c_g) = c_g$. Consequently, $\mathrm{Sym}(T, \sigma) = \oplus_g \mathrm{Sym}(C, \lambda_g)x_g$. Let $n = \deg(T)$ and $m = \deg(C)$. Then $n = m[Z : F]$. If ε is the type of $\sigma|_C$, then, as $\dim_F(\mathrm{Sym}(C, \lambda_g)) = \frac{1}{2}\dim_F C$ for all $g \neq 1$,

$$\begin{aligned}
\dim_F(\mathrm{Sym}(T, \sigma)) &= \sum_{g \in G} \dim_F(\mathrm{Sym}(C, \lambda_g)) \\
&= \dim_F(\mathrm{Sym}(C, \sigma|_C) + (|G| - 1)\frac{1}{2}\dim_F(C) \\
&= [Z : F]\left(\frac{1}{2}m(m + \varepsilon) + ([Z : F] - 1)\frac{1}{2}m^2\right) \\
&= \frac{1}{2}n(m + \varepsilon) + \frac{1}{2}n^2 - \frac{1}{2}nm = \frac{1}{2}n(n + \varepsilon).
\end{aligned}$$

Therefore, the type of σ on T is ε. We can apply this result to S and to I to get that the types of σ and σ^* are equal to the type of $\sigma|_C$. Also, applying it to $\overline{I} = (\overline{C}, G, (\overline{\omega}, \overline{f}))$, we see that the type of $\overline{\sigma}$ is equal to the type of $\overline{\sigma}|_C$, which is equal to the type of $\sigma|_C$, by [**?**, §1, Prop. 3]. This shows that the types of σ^*, σ, $\sigma|_C$, and $\overline{\sigma}$ are all equal. ■

We now relate the discriminants of the various involutions. Recall that if (T, τ) is a central simple algebra with involution of the first kind, then the discriminant $\mathrm{disc}(\tau)$ of τ is defined as follows. If $\varepsilon = \pm 1$ is the type of τ, then $\mathrm{disc}(\tau) = (-1)^{\deg(T)}\,\mathrm{Nrd}(a)F^{*2} \in F^*/F^{*2}$ for any $a \in T^*$ with $\tau(a) = -\varepsilon a$. This definition, for $\varepsilon = 1$, can be found in [**?**, Def. 7.2], and for general ε in [**?**, p. 94]. To define a notation used in the following proposition, recall that there is a split exact sequence

$$1 \longrightarrow U_F/U_F^2 \longrightarrow F^*/F^{*2} \longrightarrow \Gamma_F/2\Gamma_F \longrightarrow 1,$$

and $U_F/U_F^2 \cong \overline{F}^*/\overline{F}^{*2}$ since F is Henselian with $\mathrm{char}(\overline{F}) \neq 2$. Therefore, there is a group monomorphism $i : \overline{F}^*/\overline{F}^{*2} \to F^*/F^{*2}$ given by $i(\overline{u}\overline{F}^{*2}) = uF^{*2}$ for any lift $u \in U_F$ of $\overline{u}$.

Proposition 3.3 *We have* $\mathrm{disc}(\sigma^*) = \mathrm{disc}(\sigma) = N_{Z/F}(\mathrm{disc}(\sigma|_C))$*, and these are equal to* $i(\mathrm{disc}(\overline{\sigma}))$.

Proof. Let $n = \deg(S)$ and $m = \deg(C)$, and let ε be the type of σ. If $a \in C^*$ with $\sigma(a) = -\varepsilon a$, then $\mathrm{disc}(\sigma|_C)$ is $(-1)^m \operatorname{Nrd}_C(a)$. Since we know, by Proposition 3.2, that the types of σ^*, σ, and $\sigma|_C$ are all the same, we have $\mathrm{disc}(\sigma^*) = (-1)^n \operatorname{Nrd}_S(a)$ and $\mathrm{disc}(\sigma) = (-1)^n \operatorname{Nrd}_I(a)$. However,

$$\operatorname{Nrd}_A(a) = N_{Z/F}(\operatorname{Nrd}_C(a)) = \operatorname{Nrd}_I(a),$$

so $\mathrm{disc}(\sigma^*) = N_{Z/F}(\mathrm{disc}(\sigma|_C)) = \mathrm{disc}(\sigma)$. The equality $\mathrm{disc}\,\sigma = i(\mathrm{disc}\,\overline{\sigma})$ is proved in [**?**, §2, Prop. 3]. ■

4 Decompositions of Involutions

In this section we prove the main theorems of this paper. We continue to use the same notation as in the previous section: F is a Henselian valued field with $\mathrm{char}(\overline{F}) \neq 2$, $S = (C, G, (\omega, fc))$ is an inertially split division algebra, $I = (C, G, (\omega, f))$ is similar to an inertial division algebra, and $\overline{I} = (\overline{C}, G, (\overline{\omega}, \overline{f}))$. We have involutions σ^* on S and σ on I with $\sigma^*|_C = \sigma|_C$ an involution of the first kind on C. Moreover, if $S = \oplus_{g\in G} C y_g$ with $\mathrm{Int}(y_g)|_C = \omega_g$ and $y_g y_h = (fc)(g,h) y_{gh}$, and if $I = \oplus_{g\in G} C x_g$ with $\mathrm{Int}(x_g)|_C = \omega_g$ and $x_g x_h = f(g,h)x_{gh}$, then $\sigma^*(ay_g) = \omega_g(\sigma(a))y_g$ and $\sigma(ay_g) = \omega_g(\sigma(a))x_g$ for all $a \in C$. We have an induced involution $\overline{\sigma}$ on $\overline{I} = (\overline{C}, G, (\overline{\omega}, \overline{f}))$ that satisfies $\overline{\sigma}(\overline{ax_g}) = \overline{\omega}_g(\overline{\sigma}(\overline{a}))\overline{x_g}$.

Let $K = F(\sqrt{a_1}, \dots, \sqrt{a_n})$ be an elementary Abelian extension of F of degree 2^n and let A be an F-central simple algebra of degree 2^n containing K. If A decomposes into a tensor product of quaternion algebras as $A = (a_1, b_1) \otimes_F \cdots \otimes_F (a_n, b_n)$ for some $b_i \in F^*$, we say that A has a *decomposition adapted to* K into quaternion algebras.

We now extend [**?**, Thm. 4.1] to the case of inertially split division algebras over a Henselian valued field of residue characteristic not 2. To help with the argument, we point out that if Q is a quaternion algebra with an involution σ of the first kind, then Q has quaternion generators i and j with $\sigma(i) = \pm i$ and $\sigma(j) = \pm j$. We give a proof of this fact for the convenience of the reader. If σ is symplectic, then this is clear. If σ is orthogonal, let γ be the unique symplectic involution on Q. There is an element v with $\gamma(v) = -v$ and $\sigma = \mathrm{Int}(v) \circ \gamma$. Recall that the square of any element in $\mathrm{Skew}(Q, \gamma)$ is in F. By dimension count, there is a σ-symmetric element $u \in \text{Skew}(Q, \gamma)$. Then $u^2 \in F$ and

$$u = \sigma(u) = v\gamma(u)v^{-1} = -vuv^{-1},$$

so u and v anticommute. Then u and v are quaternion generators of Q with $\sigma(u) = u$ and $\sigma(v) = -v$.

Theorem 4.1 *The following statements are equivalent.*

1. *S contains an F-central quaternion algebra stable under σ^*;*
2. *$\overline{I}$ contains an $\overline{F}$-central quaternion algebra generated by monomials $\overline{ax_g}$ and $\overline{b}\overline{x_h}$ that are each either symmetric or skew-symmetric with respect to $\overline{\sigma}$;*
3. *$\overline{I}$ contains an $\overline{F}$-central quaternion algebra Q stable under $\overline{\sigma}$ with $[Q \cap \overline{Z} : \overline{F}] = 2$ and $[C_{\overline{I}}(Q) \cap \overline{Z} : \overline{F}] = \frac{1}{2}[\overline{Z} : \overline{F}]$;*
4. *$\overline{Z}$ contains a quadratic extension L of $\overline{F}$ such that $C_{\overline{I}}(L) = L \otimes_{\overline{F}} A$ for some $\overline{F}$-central subalgebra A of $\overline{I}$ that is stable under $\overline{\sigma}$ and with $[A \cap \overline{Z} : \overline{F}] = \frac{1}{2}[\overline{Z} : \overline{F}]$.*

Proof. (1) $\Rightarrow$ (2): Let Q be an F-central quaternion subalgebra of S stable under σ^*. As pointed out above, we may assume that Q has generators i and j with $\sigma^*(i) = \pm i$ and $\sigma^*(j) = \pm j$. We may write $i = ay_g v_g$ and $j = by_h v_h$ with $a, b \in C$ and v_g, v_h 1-units in S by Lemma 3.1. We may also assume that a and b are units in C since $\Gamma_C = \Gamma_F$ and scalar multiples of quaternion generators are still quaternion generators. For convenience we view ω_g as acting on S via $\text{Int}(y_g)$. Since $i^2 \in F^*$, we have

$$\begin{aligned} i^2 &= (ay_g v_g)(ay_g v_g) = a\omega_g(v_g a)(fc)(g,g)v_g \\ &= a\omega_g(v_g)\omega_g(a)f(g,g)c(g,g)v_g. \end{aligned}$$

Therefore, as $c(g,g) \in F^*$, we have $a\omega_g(v_g)\omega_g(a)f(g,g)v_g \in F$. Moreover, this element is a unit in S. Therefore, taking residues and using the fact that v_g is a 1-unit, we have $\overline{a\omega_g}(\overline{a})\overline{f}(g,g) \in \overline{F}^*$. This shows that $\overline{ax_g} \in \overline{I}$ satisfies $(\overline{ax_g})^2 \in \overline{F}^*$. Similarly, $(\overline{b}\overline{x_h})^2 \in \overline{F}^*$. Furthermore, we have $ji = -ij$, and simplifying the equation

$$(by_h v_h)(ay_g v_g) = -(ay_g v_g)(by_h v_h)$$

gives

$$b\omega_h(v_h a)(fc)(h,g)y_{hg}v_g = -a\omega_g(v_g b)(fc)(g,h)y_{gh}v_h.$$

Since $gh = hg$ and $c(g,h) = c(h,g) \in F^*$, this yields

$$b\omega_h(v_h a)f(h,g)\omega_{gh}(v_g) = -a\omega_g(v_g b)f(g,h)\omega_{gh}(v_h).$$

Again, both sides are units, and by taking residues we get $\overline{b}\overline{\omega_h}(\overline{a})\overline{f}(h,g) = -\overline{a}\overline{\omega_g}(\overline{b})\overline{f}(g,h)$. Therefore, $\overline{ax_g}$ and $\overline{b}\overline{x_h}$ anticommute. They then generate an $\overline{F}$-central quaternion algebra in $\overline{I}$. For stability under $\overline{\sigma}$ of this quaternion algebra, since $\sigma^*(i) = \pm i$, we have

$$\pm a y_g v_g = \sigma^*(a y_g v_g) = \sigma^*(v_g)\omega_g(\sigma(a))y_g,$$

or $\sigma^*(v_g)\omega_g(\sigma(a)) = \pm a\omega_g(v_g)$. Taking residues, we get $\overline{\omega_g}(\overline{\sigma}(\overline{a})) = \pm\overline{a}$ in $\overline{S} = \overline{C}$. Therefore, $\overline{\sigma}(\overline{ax_g}) = \pm\overline{ax_g}$. Similarly, $\overline{\sigma}(\overline{b}\overline{x_h}) = \pm\overline{b}\overline{x_h}$. Therefore, $\overline{I}$ contains an $\overline{F}$-central quaternion algebra stable under $\overline{\sigma}$ that is generated by monomials, both of which are either symmetric or skew under $\overline{\sigma}$.

(2) $\Rightarrow$ (1): Let $\widetilde{Q}$ be an $\overline{F}$-central quaternion algebra in $\overline{I}$ with quaternion generators $\overline{ax_g}$ and $\overline{b}\overline{x_h}$ satisfying $\overline{\sigma}(\overline{ax_g}) = \pm\overline{ax_g}$ and $\overline{\sigma}(\overline{b}\overline{x_h}) = \pm\overline{b}\overline{x_h}$. Let z be a unit in Z such that $g(z) = -z$ and $g'(z) = z$ for all $g' \neq g$ in G. Then $z^2 \in F^*$; moreover, $g(\overline{z}) = -\overline{z}$ and $\overline{z}^2 \in \overline{F}^*$. Thus, $(\overline{ax_g})\overline{z} = -\overline{z}(\overline{ax_g})$. Therefore, $\overline{ax_g}$ and $\overline{z}$ generate an $\overline{F}$-central quaternion algebra in $\overline{I}$ that satisfies the same conditions as $\widetilde{Q}$. If we can find a lift $a' \in C$ of $\overline{a}$ with $(a'y_g)^2 \in F$ and $\sigma^*(a'y_g) = \pm a'y_g$, then $a'x_g$ and z will generate a σ^*-stable quaternion algebra in S.

We first find a lift a' of $\overline{a}$ that satisfies $(a'y_g)^2 \in F$. Set $H = \langle g\rangle$, and let a be any lift of $\overline{a}$ in C. We have $(ay_g)^2 = a\omega_g(a)f(g,g)c(g,g)$. If $(\overline{ax_g})^2 = \overline{\alpha}$, then $\overline{a\omega_g}(\overline{a})\overline{f}(g,g) = \overline{\alpha}$. Therefore, $a\omega_g(a)f(g,g) = \alpha u$ for some 1-unit u in C. We consider the restricted generalized cocycle $(\omega', f') = \mathrm{res}^G_H(\omega, f) \in \mathcal{Z}(H, C^*)$. By setting $a_g = a$ and $a_{\mathrm{id}} = 1$, we get a cocycle (θ, e) equivalent to (ω', f'), defined by

$$\theta_h = \mathrm{Int}(a_h) \circ \omega'_h,$$
$$e(h,k) = a_h\omega'_h(a_k)f'(h,k)a_{hk}^{-1}$$

for all $h, k \in H$. If α' is the normalized cocycle in $Z^2(H, F^*)$ with $\alpha'(g,g) = \alpha$, then $(\theta, e/\alpha')$ is a generalized cocycle. If we set $u' = e/\alpha'$, then $u'(g,g) = u$. We thus have $H = \mathrm{Gal}(Z/Z^g)$ and a generalized cocycle $(\theta, u) \in \mathcal{Z}(H, C^*)$ with values in the group of 1-units of C. By [**?**, Thm. 1.1], there is a group homomorphism $\psi : H \to \mathrm{Aut}(C)$ with $(\theta, u') \sim (\psi, 1)$. Therefore, there is a $b_g \in U_{1,C}$ with $b_g\theta_g(b_g)u'(g,g) = 1$. Replacing a by $a' = b_g a$ then gives a monomial $a'y_g$ that satisfies $(a'y_g)^2 = \alpha c(g,g) \in F^*$. Note that $\overline{a'} = \overline{a}$ since b is a 1-unit.

We now adjust our monomial $M = a'y_g$ to get a monomial N with $\sigma^*(N) = \pm N$, but preserving the property $N^2 \in F^*$. Set $\beta = \alpha c(g,g)$. Recall that since $\overline{\sigma}(\overline{ax_g}) = \varepsilon\overline{ax_g}$, where $\varepsilon = \pm 1$, we have $\overline{\omega_g}(\overline{\sigma}(\overline{a})) = \varepsilon\overline{a}$. Moreover,

$$\sigma^*(M) = \omega_g(\sigma(a'))y_g = (\omega_g(\sigma(a'))(a')^{-1})a'y_g.$$

Set $v = \varepsilon\omega_g(\sigma(a'))(a')^{-1}$. Then v is a 1-unit in C, and $\sigma^*(M) = \varepsilon vM$. Let $\psi = \mathrm{Int}(M)|_{F(v)}$. Since $M^2 = \beta \in F$, we have $\sigma^*(M)^2 = \beta$, which yields $v\psi(v) = 1$. Note that $\sigma^*(v) = v$ is an easy consequence of the equations $\sigma^*(M) = \varepsilon vM$ and $v\psi(v) = 1$. We will produce an

$s \in F(v)$ with $\sigma^*(sM) = \pm sM$ and $(sM)^2 \in F^*$. Because $\sigma^*|_{F(v)} = \text{id}$, these conditions are equivalent to

$$v\psi(s) = \pm s,$$
$$s\psi(s) \in F^*.$$

The equation $v\psi(v) = 1$ gives $\psi(v) = v^{-1}$, which implies that ψ is an F-automorphism of the field $F(v) \subseteq C$. Moreover, $\psi^2 = \text{id}$ since $M^2 \in F^*$. We have a 1-cocycle $\varphi \in H^1(\langle\psi\rangle, U_{1,F(v)})$ given by $\varphi(1) = 1$ and $\varphi(g) = v$. Since $U_{1,F(v)}$ is uniquely divisible by $2 = |\langle\psi\rangle|$, this cohomology group is trivial. Thus, there is a $w \in U_{1,F(v)}$ with $v = w/\psi(w)$. Since w is a 1-unit, $w\psi(w)$ is also a 1-unit, so there is a $t \in U_{1,F(v)}$ with $w\psi(w) = t$. If $s = w/t$, then a short calculation shows that $v\psi(s) = \pm s$ and $s\psi(s) = \pm 1$. Therefore, the monomial sM satisfies $(sM)^2 = \pm\beta$ and $\sigma^*(sM) = \pm sM$. Thus, as mentioned in the first paragraph of (2)$\Rightarrow$(1), $sM = sa'y_g$ and z are monomials that generate a σ^*-invariant F-central quaternion algebra in S.

(2) $\Rightarrow$ (3): Let $\widetilde{Q}$ be an $\overline{F}$-central quaternion algebra in $\overline{I}$ with quaternion generators $\overline{ax_g}$ and $\overline{bx_h}$ that are each either symmetric or skew with respect to $\overline{\sigma}$. Let z be a unit in Z such that $g(z) = -z$ and $g'(z) = z$ for all $g' \neq g$. Then $z^2 \in F$. Moreover, $(\overline{ax_g})\overline{z} = -\overline{z}(\overline{ax_g})$. So, $\overline{ax_g}$ and $\overline{z}$ generate an $\overline{F}$-central quaternion algebra Q' in $\overline{I}$ with the same properties as $\widetilde{Q}$. We have $Q' \cap \overline{Z} = \overline{F}(\overline{z})$, so $[Q' \cap \overline{Z} : \overline{F}] = 2$. Also, it is clear that $C_{\overline{I}}(Q') \cap \overline{Z} = \overline{Z}^g$ since $\text{Int}(\overline{ax_g}) = \text{Int}(\overline{x_g})$ induces g on $\overline{Z}$. So, $[C_{\overline{I}}(Q') \cap \overline{Z} : \overline{F}] = \frac{1}{2}[\overline{Z} : \overline{F}]$.

(3) $\Rightarrow$ (2): Let Q be a $\overline{\sigma}$-stable $\overline{F}$-central quaternion algebra in $\overline{I}$ that contains a quadratic extension L of $\overline{F}$ inside $\overline{Z}$ and for which $[C_{\overline{I}}(Q) \cap \overline{Z} : \overline{F}] = \frac{1}{2}[\overline{Z} : \overline{F}]$. Set $L' = C_{\overline{I}}(Q) \cap \overline{Z}$. Then, by dimension count, $\overline{Z} = L \otimes_{\overline{F}} L'$. Let $g \in \text{Gal}(\overline{Z}/\overline{F})$ satisfy $L' = \overline{Z}^g$ and $g|_L \neq \text{id}$. Choose $\overline{z} \in L$ with $g(\overline{z}) = -\overline{z}$. Then there is a $j \in Q$ with $j\overline{z} = -\overline{z}j$. Moreover, $\text{Int}(j)$ is the identity on L' since $L' \subseteq C_{\overline{I}}(Q)$. So, $\text{Int}(j)$ is equal to g on $\overline{Z}$. Thus, $\text{Int}(\overline{x_g}j^{-1})$ is the identity on $\overline{Z}$, so $\overline{x_g}j^{-1} \in C_{\overline{I}}(\overline{Z}) = \overline{C}$, and so $\overline{x_g}j^{-1} = \overline{u}$ for some $u \in C$. Thus, $j = \overline{ux_g}$ is a monomial. We now show that we can alter j to assume $\overline{\sigma}(j) = \pm j$. Since Q is stable under $\overline{\sigma}$ and $\overline{\sigma}$ is trivial on $\overline{Z}$, we see that $\overline{\sigma}(j)\overline{z}\,\overline{\sigma}(j)^{-1} = j\overline{z}j^{-1}$. Thus, $\overline{\sigma}(j) = bj$ for some $b \in L = \overline{F}(\overline{z})$. Then $j = \overline{\sigma}(bj) = bjb = bg(b)j$. Therefore, $bg(b) = 1$, so $b = b'/g(b')$ for some $b' \in L$ by Hilbert Theorem 90. Then $b'j$ is a new monomial that satisfies $\overline{\sigma}(b'j) = b'j$ and $(b'j)^2 = j^2 \in \overline{F}$. The monomials $\overline{z}$ and $b'j$ then generate a $\overline{\sigma}$-stable quaternion subalgebra of $\overline{I}$.

(3) $\Leftrightarrow$ (4): Suppose that Q is a $\overline{\sigma}$-stable $\overline{F}$-central quaternion subalgebra of $\overline{I}$ with $[Q \cap \overline{Z} : \overline{F}] = 2$ and $[C_{\overline{I}}(Q) \cap \overline{Z} : \overline{F}] = \frac{1}{2}[\overline{Z} : \overline{F}]$. If we set $L = Q \cap \overline{Z}$, then $C_{\overline{I}}(L) = L \otimes_{\overline{F}} C_{\overline{I}}(Q) \subseteq Q \otimes_{\overline{F}} C_{\overline{I}}(Q)$. Moreover, since Q is stable under $\overline{\sigma}$, its centralizer $C_{\overline{I}}(Q)$ is also stable under $\overline{\sigma}$. Therefore, setting $A = C_{\overline{I}}(Q)$ gives (4). Conversely, if $L \subseteq \overline{Z}$ is a quadratic extension of $\overline{F}$ with $C_{\overline{I}}(L) = L \otimes_{\overline{F}} A$ for some $\overline{\sigma}$-stable $\overline{F}$-central subalgebra A that satisfies $[A \cap \overline{Z} : \overline{F}] = \frac{1}{2}[\overline{Z} : \overline{F}]$, then we may write $\overline{I} = C_{\overline{I}}(A) \otimes_{\overline{F}} A$ by the double centralizer theorem, and $L \subseteq C_{\overline{I}}(A)$. Furthermore, dimension count shows that $C_{\overline{I}}(A)$ is a quaternion algebra. It is stable under $\overline{\sigma}$ since A is stable under $\overline{\sigma}$. Finally, $C_{\overline{I}}(Q) = A$ by the double centralizer

theorem, so $[C_{\overline{J}}(Q)\cap\overline{Z}:\overline{F}]=[A\cap\overline{Z}:\overline{F}]=\frac{1}{2}[\overline{Z}:\overline{F}]$. ■

The next two results will be used in the proof of Proposition 4.4 below. That proposition is a special case of the second of our main results, Theorem 4.5, and it will be used in the proof of Theorem 4.5.

Lemma 4.2 *Let J be an inertial F-central division algebra. If τ is an involution on $\overline{J}$ of the first kind, then there is a unique up to isomorphism involution σ on J with $\overline{\sigma}=\tau$.*

Proof. By [**?**, §1, Prop. 4], there is an involution σ on J with $\overline{\sigma}=\tau$. Suppose that σ' is a second lift of τ. Then $\overline{\sigma}=\overline{\sigma'}=\tau$. There is a $u\in J$ with $\sigma(u)=\pm u$ and $\sigma'=\operatorname{Int}(u)\circ\sigma$. Since $\Gamma_J=\Gamma_F$, we may assume that u is a unit. Then $\tau=\operatorname{Int}(\overline{u})\circ\tau$, so $\overline{u}\in\overline{F}^*$. We then may further modify u to assume that $\overline{u}=\overline{1}$. By Hensel's lemma, $u=x^2$ for some $x\in F(u)\subseteq J$. Moreover, since the type of σ and σ' are the same, being equal to the type of τ by [**?**, §1, Prop. 3], $\sigma(u)=u$. This yields $\sigma(x)=x$, so $u=\sigma(x)x$. Therefore, $\sigma'=\operatorname{Int}(\sigma(x)x)\circ\sigma$, which proves that σ' and σ are isomorphic as involutions. ■

Proposition 4.3 *Let J be an F-central inertial division algebra and let σ be an involution of the first kind on J. If $\widetilde{B}$ is an $\overline{F}$-central subalgebra of $\overline{J}$ with $\overline{\sigma}(\widetilde{B})=\widetilde{B}$, then there is an inertial lift B of $\widetilde{B}$ in J with $\sigma(B)=B$.*

Proof. Let B be an inertial lift of $\widetilde{B}$ in J; existence of B follows from [**?**, Thm. 2.9]. Set $B'=C_J(B)$. Then $J=B\otimes_F B'$ by the double centralizer theorem. Also, $\overline{B'}=C_{\overline{J}}(\widetilde{B})$ and $\overline{J}=\overline{B}\otimes_{\overline{F}}\overline{B'}$. By hypothesis, $\overline{\sigma}$ restricts to an involution on $\overline{B}$, and so it also restricts to an involution on $\overline{B'}=C_{\overline{J}}(\overline{B})$. We have $\exp(B)=\exp(\overline{B})\leq 2$ by the isomorphism $\operatorname{IBr}(F)\to\operatorname{Br}(\overline{F})$ of [**?**, Thm. 2.8], so B has an involution of the first kind. Similarly, B' has an involution of the first kind. Then, by [**?**, §1, Prop. 4], there are involutions τ and ρ on B and B', respectively, with $\overline{\tau}=\overline{\sigma}|_{\overline{B}}$ and $\overline{\rho}=\overline{\sigma}|_{\overline{B'}}$. By [**?**, §1, Prop. 3], τ and $\overline{\tau}$ are of the same type, σ and $\overline{\sigma}$ are of the same type, and ρ and $\overline{\rho}$ are of the same type. Therefore, as $\overline{\sigma}=\overline{\sigma}|_{\overline{B}}\otimes\overline{\sigma}|_{\overline{B'}}$, the involutions σ and $\tau\otimes\rho$ are of the same type on J. Thus, there is a $u\in J^*$ with $\sigma(u)=u$ and $\tau\otimes\rho=\operatorname{Int}(u)\circ\sigma$. We may assume that $v(u)=0$ since $\Gamma_J=\Gamma_F$. So, $\overline{\tau\otimes\rho}=\operatorname{Int}(\overline{u})\circ\overline{\sigma}$. However, since τ and ρ both reduce to $\overline{\sigma}$, this gives $\overline{\sigma}=\operatorname{Int}(\overline{u})\circ\overline{\sigma}$. From this we see that $\overline{u}\in\overline{F}^*$. So, we may further modify u to assume that $\overline{u}=\overline{1}$. Since $\operatorname{char}(\overline{F})\neq 2$, there is an $x\in F(u)\subseteq J$ with $u=x^2$. This forces $\sigma(x)=x$. In particular, we see that $\operatorname{Int}(u)=\operatorname{Int}(\sigma(x)x)$. This yields

$$B=\rho(B)=u\sigma(B)u^{-1}=(\sigma(x)x)B(\sigma(x)x)^{-1},$$

which then implies that $\sigma(B)=(\sigma(x)x)^{-1}B\sigma(x)x$, so $\sigma(x^{-1}Bx)=x^{-1}Bx$. Therefore, $x^{-1}Bx$ is an inertial lift of $\widetilde{B}$ that is stable under σ. ■

As mentioned earlier, the following proposition will be used in the proof of Theorem 4.5.

Proposition 4.4 *Let J be an F-central inertial division algebra and let σ be an involution of the first kind on J. Then (J,σ) decomposes into a tensor product of quaternion algebras* *if and only if $(\overline{J}, \overline{\sigma})$ decomposes into a tensor product of quaternion algebras. Furthermore, if J contains a maximal subfield K that is an elementary Abelian 2-extension of F, then J has a decomposition adapted to K into quaternion algebras stable under σ if and only if $\overline{J}$ has a decomposition adapted to $\overline{K}$ into quaternion algebras stable under $\overline{\sigma}$.*

Proof. First note that the second statement implies the first since any tensor product of quaternion algebras has a decomposition adapted to an appropriate Kummer extension. More concretely, if $A = (a_1, b_1) \otimes_F \cdots \otimes_F (a_n, b_n)$ is a division algebra, then A has a decomposition adapted to $F(\sqrt{a_1}, \ldots, \sqrt{a_n})$. We therefore prove only the second statement.

Let K be an elementary Abelian 2-extension of F that is a maximal subfield of J. Note that K/F is inertial since J/F is inertial. If $J = \otimes_{i=1}^n Q_i$ is a decomposition adapted to K into σ-stable quaternion algebras, then there are quadratic subextensions K_i of K with $K = K_1 \cdots K_n$ and $K_i \subseteq Q_i$. Since J/F is inertial, it is clear that $\overline{J} = \otimes_{i=1}^n \overline{Q_i}$, and $\overline{\sigma}(\overline{Q_i}) = \overline{Q_i}$ since $\sigma(Q_i) = Q_i$. Moreover, $\overline{K_i} \subseteq \overline{Q_i}$, so this decomposition of $\overline{J}$ is adapted to $\overline{K}$.

Conversely, suppose that $\overline{J} = \otimes_{i=1}^n \widetilde{Q_i}$ is a tensor product of $\overline{\sigma}$-stable quaternion algebras, and that this decomposition is adapted to $\overline{K}$. There are quadratic subextensions $\widetilde{K_i}$ of $\overline{K}$ with $\widetilde{K_i} \subseteq \widetilde{Q_i}$. By Proposition 4.3, there are σ-stable quaternion algebras $Q_i \subseteq J$ with $\overline{Q_i} = \widetilde{Q_i}$. Let $\sigma_i = \sigma|_{Q_i}$. If $J' = \otimes_{i=1}^n Q_i$ and $\sigma' = \otimes_{i=1}^n \sigma_i$, then J' is a division algebra with $\overline{J'} = \overline{J}$ by [**?**, Thm. 1]. By the uniqueness of inertial lifts [**?**, Thm. 2.8], we have $J' \cong J$. We then identify $J' = J$. From this we see that $\overline{\sigma'} = \overline{\sigma}$, so, by Lemma 4.2, σ' and σ are isomorphic involutions on J. Since (J, σ') decomposes as a tensor product of quaternion algebras, (J, σ) also decomposes as a tensor product of quaternion algebras; in particular, if $\sigma = \mathrm{Int}(\sigma'(x)x) \circ \sigma'$, then (J, σ) decomposes as $\otimes_{i=1}^n \sigma'(x) Q_i \sigma'(x)^{-1}$. Moreover, this decomposition is adapted to K because, by uniqueness of inertial lifts, $\sigma'(x) Q_i \sigma'(x)^{-1}$ contains a lift K_i of $\widetilde{K_i}$. ■

In the following theorem, we give necessary and sufficient conditions on when S decomposes into a tensor product of quaternion algebras stable under the involution σ^*. This theorem extends [**?**, Thm. 4.3] to the case of inertially split division algebras. We will consider the case where $\overline{S} = \overline{Z}$, or, equivalently, when Z is a maximal subfield of S; we then only need to work with crossed products and not generalized crossed products. Recall that a crossed product $(Z/F, G, h)$ decomposes into a tensor product of quaternion algebras adapted to Z if and only if h is similar to a symmetric cocycle with values in F^* by [**?**, Cor. 1.4]. We will write $Z^2(G, F^*)_{\mathrm{sym}}$ for the group of all symmetric cocycles for G with values in F^*, and we will use [**?**, Cor. 1.4] in the proof below. If $A = \otimes_{r=1}^n (a_r, b_r)$ is a tensor product of quaternion algebras, and if $i_r, j_r \in (a_r, b_r)$ with $i_r^2 = a_r$, $j_r^2 = b_r$ and $j_r i_r = -i_r j_r$, then we will refer to the set $\{i_1, j_1, \ldots, i_n, j_n\}$ in the proof below as a set of *quaternion generators* for A.

Theorem 4.5 *With the notation of this section, suppose further that $\overline{S} = \overline{Z}$. Then the following conditions are equivalent.*

1. *The algebra S decomposes into a tensor product of quaternion algebras stable under σ^*;*

2. *The algebra S has a decomposition adapted to Z as a tensor product of quaternion algebras stable under σ;*

3. *The algebra I has a decomposition adapted to Z as a tensor product of quaternion algebras stable under σ;*

4. *The algebra $\overline{I}$ has a decomposition adapted to $\overline{Z}$ as a tensor product of quaternion algebras stable under $\overline{\sigma}$.*

Proof. (2) $\Rightarrow$ (1): This is clear.

(1) $\Rightarrow$ (4): we use the same ideas as in the argument for (1) $\Rightarrow$ (2) of Theorem 4.1. Suppose that $\{u_1, v_1, \ldots, u_n, v_n\}$ forms a set of quaternion generators for S with each u_i and v_i either symmetric or skew-symmetric with respect to σ^*. We may write $u_i = c_i y_{g_i} w_i$ and $v_i = d_i y_{h_i} z_i$ with $c_i, d_i \in Z$ and w_i, z_i 1-units in S by Lemma 3.1. Moreover, by replacing u_i and v_i by scalar multiples, we may assume that c_i and d_i are units since $\Gamma_Z = \Gamma_F$. A calculation similar to that of the proof of Theorem 4.1 shows that $\left\{\overline{c_i x_{g_i}}, \overline{d_i x_{h_i}} : 1 \leq i \leq n\right\}$ forms a set of quaternion generators for $\overline{I}$. Since $\overline{S} = \overline{Z}$, we see that $h_j \neq h_i$ if $j \neq i$, because $\mathrm{Int}(\overline{x_{h_i}}) = h_i$ sends $\overline{c_i x_{g_i}}$ to $-\overline{c_i x_{g_i}}$ and fixes $\overline{c_j x_{g_j}}$ if $j \neq i$. Let $a_i \in Z$ be a unit that satisfies $h_i(a_i) = -a_i$ and $h_j(a_i) = a_i$ if $j \neq i$. Then $\left\{\overline{a_1}, \overline{d_1 x_{h_1}}, \ldots, \overline{a_n x_{h_n}}\right\}$ forms a set of quaternion generators for $\overline{I}$, and the corresponding decomposition is adapted to $\overline{Z}$. Furthermore, since $\overline{\sigma}(\overline{d_i x_{h_i}}) = \pm \overline{d_i x_{h_i}}$, the quaternion factors are each stable under $\overline{\sigma}$.

(4) $\Leftrightarrow$ (3): This is the second statement of Proposition 4.4.

(3) $\Rightarrow$ (2). Suppose that $I = (Z/F, G, f) = \oplus_{g \in G} Z x_g$ is a tensor product of quaternion algebras each stable under σ. Then we can write $I = (Z/F, G, e)$ with $e \in Z^2(G, F^*)_{\mathrm{sym}}$ by [**?**, Cor. 1.4]. Moreover, by considering how one writes a tensor product of quaternion algebras as a crossed product, we can write $I = \oplus Z z_g$ with $z_g z_h = e(g,h) z_{gh}$, and each z_g is a product of (commuting) elements of a set of quaternion generators of I. By the stability under σ of these quaternion subalgebras together with the fact that $\sigma|_Z = \mathrm{id}$, we see that each of the quaternion generators is fixed by σ. We thus have $\sigma(z_g) = z_g$. For the algebra S we have $S = (Z/F, G, ec)$, and since $c \in Z^2(G, F^*)_{\mathrm{sym}}$, so also is $ec \in Z^2(G, F^*)_{\mathrm{sym}}$. Moreover, if $z_g = c_g x_g$ for some $c_g \in Z$, then $g(c_g) = c_g$ because $\sigma(z_g) = z_g$. Therefore, for $S = (Z/F, G, fc) = \oplus Z y_g$, if we set $w_g = c_g y_g$, we have $\sigma^*(w_g) = y_g c_g = g(c_g) y_g = w_g$ and $w_g^2 = (ec)(g,g) \in F^*$. So, S is a tensor product of quaternion algebras each stable under σ^*; if we write $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ and let Z_i be the fixed field of $\Pi_{j \neq i} \langle g_j \rangle$, then the quaternion algebras are $Z_i \oplus Z_i w_{g_i}$, which are stable under σ^* since $\sigma^*|_Z = \mathrm{id}$ and $\sigma^*(w_{g_i}) = w_{g_i}$. This decomposition is clearly adapted to Z since the quaternion algebra $Z_i \oplus Z_i w_{g_i}$ contains the field Z_i. ■

In [**?**, Thm. 4.3] the analogue of condition (2) does not appear. However, the argument given for (2) $\Rightarrow$ (1) in that paper does in fact show that the analogue of this condition is equivalent to the other three conditions of [**?**, Thm. 4.3].

References

Department of Mathematical Sciences, New Mexico State University, Las Cruces, New Mexico 88003

E-mail address: pmorandi@nmsu.edu

Department of Mathematics, California State Univerisity, Northridge, Northridge, California 91330

E-mail address: al.sethuraman@email.csun.edu