manuscripta math. 169, 209–249 (2022)

Daniel Krashen · Eliyahu Matzri · Andrei Rapinchuk · Louis Rowen · David Saltman

Division algebras with common subfields

Received: 31 October 2019 / Accepted: 8 May 2021 / Published online: 12 July 2021

Abstract. We study the partial ordering on isomorphism classes of central simple algebras over a given field F, defined by setting $A_1 \leq A_2$ if $\deg A_1 = \deg A_2$ and every étale subalgebra of A_1 is isomorphic to a subalgebra of A_2, and generalizations of this notion to algebras with involution. In particular, we show that this partial ordering is invariant under passing to the completion of the base field with respect to a discrete valuation, and we explore how this partial ordering relates to the exponents of algebras.

1. Introduction

Throughout, F denotes a given field with separable closure F^s. A recurrent question in the study of central simple algebras or central division algebras is how much structural information is encoded in an algebra's subfields, or more generally, its étale subalgebras. In [4,7,23] (resp. [15]) central simple algebras having the same subfields (resp. splitting fields) were investigated. In this paper, we investigate central simple algebras split by all (commutative) étale subalgebras of a given central simple algebra, by introducing and analyzing the following partial order relation on central simple algebras:

Definition 1.1. Let A_1, A_2 be central simple algebras over F. We write $A_1 \preceq A_2$ if every commutative étale subalgebra of A_1 is isomorphic to a subalgebra of A_2. We write $A_1 \leq A_2$ if $A_1 \preceq A_2$ and the two algebras have equal degree.

This work was supported by the U.S.-Israel Binational Science Foundation (Grant No. 201049) and by the Israel Science Foundation (Grant No. 630/17)

The authors have no conflicts of interest to declare that are relevant to the content of this article. There is no extra data.

The authors thank the referee for correcting some slips and suggesting improved proofs.

E. Matzri · L. Rowen (✉): Bar-Ilan University, Ramat-Gan, Israel.
e-mail: rowen@math.biu.ac.il
D. Krashen: Rutgers University, New Brunswick, New Jersey, US.
e-mail: daniel.krashen@rutgers.edu
A. Rapinchuk: University of Virginia, Charlottesville, Virginia, US.
e-mail: asr3x@virginia.edu
D. Saltman: The Center for Communications Research, Princeton, New Jersey, US.
e-mail: saltman@idaccr.org

Mathematics Subject Classification: 16K50 · 16K20 · 11R52 · 11R58 · 12J10

https://doi.org/10.1007/s00229-021-01315-5

We consider the following questions:

Question 1.2. *Given a central simple algebra A, what can we say about the collection of algebras B such that $A \leq B$? For example, is the set of isomorphism classes of such B finite? Furthermore, is the exponent of B constrained in terms of the exponent of A?*

We show that for a large class of naturally arising fields F, those with "trivial unramified Brauer group," which we refer to as "transparent fields," (see Sect. 2.3), if $D \leq B$ for D a central division algebra, then the exponent of B divides the exponent of D (Theorem A).

Further, under the hypothesis that the unramified Brauer group of a field is finite, which we refer to as a translucent field (see Sect. 2.3), and under some mild additional hypothesis, we show that if D is a central division algebra, then the set of isomorphism classes of algebras A such that $D \leq A$ is finite (Theorem 4.22; Theorem 4.23 as a special case). In fact, for the finiteness of the genus it is enough to have the finiteness of the n-torsion in the Brauer group, which is a much easier condition to verify then the finiteness of the whole Brauer group.

On the other hand, we show that for more general fields, not finitely generated, that both of these statements are no longer true. We construct (central) division algebras D for which one can find a division algebra B such that $D < B$ but the exponent of B is strictly bigger than the exponent of D (Note that our construction in fact yields infinitely many choices for such B, cf. Corollary 3.6.)

In case that the algebras also happen to admit involutions, we similarly shall consider in 8 how much information is carried by those commutative étale subalgebras which are invariant under the involution. We get analogous results in Theorem 8.41, but lacking the case that the involution is of second kind with L_B cyclic over F^τ in the notation there.

2. Preliminaries

2.1. Notation

We write "csa" for an F-central simple algebra, and "cda" for an F-central, finite dimensional division algebra. At times we will write a central simple algebra A/F or a division algebra D/F when F is the center of A or D respectively. The **index** of A is the degree of its underlying division algebra. We let $A^\times$ denote the group of invertible elements of A. For a csa A/F and a subalgebra $B \subset A$, we write A^B to denote the centralizer of B in A. For an algebra B/F, we write rB to denote the direct product algebra $\times_r B$ of r copies of B. $F[[x]]$ denotes the ring of formal power series in one variable x over F, and $F((x))$ its field of fractions. For a field extension K/F, we write $res_{K/F} A$ for $A \otimes_F K$.

Remark 2.1. It is well known that any cda D of degree $n = p_1^{j_1} \dots p_t^{j_t}$, where $p_1, \dots, p_t$ are distinct primes, can be written as a tensor product $D_1 \otimes \cdots \otimes D_t$, where D_i is a central division F-algebra of degree $p_i^{j_i}$. Furthermore, a field extension K of F of degree n is F-isomorphic to a (maximal) subfield of D if and only if it splits D. (See [13, Ch. 4] or [22, Corollary 24.37, Theorem 4.66].)

2.2. Discrete valuations and ramification

Complete discrete valued fields will play an essential role in this paper. Many of the standard facts we recall here can be found (in a more general context) in [14] or in [32].

Let F be a field complete with a discrete valuation v, valuation ring R, uniformizer π, and residue field $\bar{F}$. F^{unr} denotes the compositum of the unramified extensions of F in F^s. For a division algebra D/F we may uniquely extend the valuation v to D, and we also denote this extension by v. Assume that the characteristic of F does not divide $n = \deg D$. We say that D is **tame** if D is split by an unramified extension of F; then, by ([14, Lemma 5.14]), D is Brauer equivalent to $D' \otimes \Delta(L/F, \sigma, \pi)$, where L/F is unramified with Galois group $\langle\sigma\rangle$, D'/F is unramified (which means $v(D') = v(F)$), and π is a uniformizer of F.

Identifying $Gal(\bar{F}^s/\bar{F}) = Gal(F^{unr}/F)$, the valuation on F^{unr} induces a so-called "ramification map," (also known as the residue map)

$$\rho_v : \mathrm{Br}(F^{unr}/F) \to H^2(\bar{F}, \mathbb{Z}) = H^1(\bar{F}, \mathbb{Q}/\mathbb{Z}).$$

Since $\mathbb{Q}/\mathbb{Z}$ here is a trivial Galois module, we may identify elements in the target of the ramification map as pairs $(\bar{L}/\bar{F}, \sigma)$ consisting of cyclic Galois extensions $\bar{L}/\bar{F}$, together with generators σ of their Galois groups.

Lemma 2.2. *Let D be a tame algebra over a field F of characteristic not dividing $n = \deg F$, with $D \cong D' \otimes \Delta(L/F, \sigma, \pi)$ for D' inertial and L/F unramified. Then $\rho([D]) = (\bar{L}/\bar{F}, \bar{\sigma})$. Further, $\rho([D]) = 0$ if and only if D is the lift of an Azumaya algebra over the valuation ring of F.*

Proof. By [14, Theorem 2.8], we may identify inertial algebras with Azumaya algebras over the valuation R ring of F, and by [8, Theorem VI.1.1], (after identifying Galois groups of unramified extensions with Galois groups of the corresponding extensions of valuation rings), we may therefore identify the inertial Brauer group with $H^2(Gal(F^{unr}/F), R^*)$. Hence we have an exact sequence

$$\mathrm{Br}(R) \to \mathrm{Br}(F^{unr}/F) \xrightarrow{\rho} H^1(Gal(F^{unr}/F), \mathbb{Q}/\mathbb{Z}).$$

It follows that $\rho([D']) = 0$. Direct inspection of the explicit 2-cocycle describing the cyclic algebra $\Delta(L/F, \sigma, \pi)$ then shows $\rho([D]) = \rho([\Delta(L/F), \sigma, \pi]) = (\bar{L}/\bar{F}, \bar{\sigma})$, as claimed. The result now follows. □

Note that this is somewhat different from the definition given in [14, Section 6]; however it is equivalent in the case of discrete valuations by [14, Lemma 6.2], and the fact that there are no tame and totally ramified division algebras over a complete discretely valued field (see, for example [31, Remark 3.2(a)]. We often assume that the degree of D is prime to the characteristic of F.

2.3. Translucency and transparency

Let F be a field, and v a discrete valuation v on F. Let F_v denote the completion of F with respect to v, and $D_v = D \otimes_F F_v$. We say that $\alpha \in \mathrm{Br}(F)$ is **tame at** v if the class α_{F_v} of D_v/F_v is tame. Let $\mathcal{V}$ be a collection of discrete valuations on F. We say that $\mathcal{V}$ is tame if every Brauer class $\alpha \in \mathrm{Br}(F)$ is tame at every valuation $v \in \mathcal{V}$. If $\mathcal{V}$ is tame, we write $\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ to denote the subgroup of the Brauer group consisting of those classes which are unramified at every valuation $v \in \mathcal{V}$. We say that F is **translucent with respect to** $\mathcal{V}$ if $\mathcal{V}$ is tame and $\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ is finite. Somewhat following [11], we say that F is **transparent with respect to** $\mathcal{V}$, if $\mathcal{V}$ is tame and $\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ is trivial. We say that F is translucent (resp. transparent) if it is translucent (resp. transparent) with respect to some collection $\mathcal{V}$ of discrete valuations. We similarly say that F is n-translucent (resp. n-transparent) at $\mathcal{V}$ if every class $\alpha \in {}_n\mathrm{Br}(F)$ is tame and the n-torsion subgroup ${}_n\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ is finite (resp. trivial). It is useful to understand when the conditions above might hold. We use [28] as a reference for local fields and their Brauer groups.

Lemma 2.3. (1) *If F is an algebraically closed field or a locally compact non-archimedean field, then F is transparent.*
(2) *If F is a global field without real places, then F is transparent. (See [6, Lemma 3.0] for the full picture.)*

Proof. Algebraically closed fields are transparent since they have trivial Brauer groups. The fact that local and global fields without real places are transparent follows from the standard computation of the Brauer groups of these fields in terms of ramification (see for [28, XIII.3, Prop. 6], and [18, Sections 18.4, 18.5]). □

Proposition 2.4. (1) *If (a field) F is transparent, then any purely transcendental extension $F(X) := F(x_1, \dots, x_r)$ is also transparent. (In fact $F(X)$ can be of infinite transcendence degree, seen by taking direct limits.)*
(2) *If F is a global field, and the characteristic of F does not divide n, then $F(X)$ is n-translucent.*

Proof. (1) The statement follows from Lemma 2.2 and [26, Proposition 10.5].
(2) The statement follows from [4, Theorem 8].

□

We also quote

Theorem 2.5. ([6]) *If F is finitely generated over its prime field, with characteristic prime to n, then F is n-translucent.*

3. One-sided genus: statement of the main results

Theorem A. *Suppose that F is a transparent field. Suppose that $E \leq D$ for a central simple algebra D and a central division algebra E. Then the exponent of D divides the exponent of E.*

The proof of Theorem A will be given at the beginning of 5.

Definition 3.1. The **upper genus** of a central simple algebra A, denoted $\overline{\mathrm{gen}}(A)$, is the set of isomorphism classes of central simple algebras A' such that $A \leq A'$.

Let $\mathbb{H}$ denote Hamilton's quaternion algebra $(-1,-1)_{F,2}$, generated by elements i and j such that $i^2 = j^2 = (ij)^2 = -1$.

Theorem B. *Let F be a field and $\mathcal{V}$ a set of discrete valuations on F. Let D be a central division algebra of degree n over F, and assume that F is translucent with respect to $\mathcal{V}$. Then $\overline{\mathrm{gen}}(D)$ is finite unless $D = \mathbb{H}$, and $F \cong K((x))$ for a Pythagorean field K. In this case, $\overline{\mathrm{gen}}(D) = \{(-1, f)_{F,2} \mid f \in K^\times$ or $f \in K^\times x\}$.*

This theorem will be reformulated and proved as Theorem 4.22.

The reason we do not consider the "lower genus" is that it often is infinite. For example, for $B = M_n(F)$, and any csa A of degree n, any maximal subfield (or maximal étale subalgebra) of A is embeddable in B via the regular representation. In particular, the lower genus of the algebra B contains the classes of all algebras of degree n. Besides this, even for number fields, one finds that the "lower genus" is always infinite:

Proposition 3.2. *Let F be a number field, and D a cda of degree n. Then the set of F- isomorphism classes of cda's D' such that $D' \leq D$ is infinite.*

Proof. By the Albert-Brauer-Hasse-Noether Theorem, a field extension K/F of degree n is a maximal subfield of D if and only if it splits all the ramifications of D. Let $\mathrm{ram}(D)$ be the set of valuations where D is ramified, a finite set. Then any csa A of degree n with $\mathrm{ram}(D) \subseteq \mathrm{ram}(A)$ satisfies $A \leq D$. Indeed, any maximal subfield of A splits all ramifications of A. In particular it splits all ramifications of D. Clearly there are infinitely many such A's, and we are done. □

Next we consider the two-sided genus considered in [4,5,23], which consists of the F-isomorphism classes of such csa's B that $A \leq B$ and $B \leq A$. Clearly given an algebra A, if an étale algebra K/F splits A then it splits A^m for any m and $A \leq A^m$, and if A^m generates the same subgroup of the Brauer group $\mathrm{Br}(F)$, we also get $A^m \leq A$. Thus the only case where the two-sided genus can contain only one element is if the exponent of A is two. Although over a finitely generated field the two-sided genus is finite, cf. [7], it can be infinite in the general case, [16,30]. We say F has the **vanishing genus property** if the two-sided genus of every algebra of exponent two has one element.

Proposition C. (Proposition 6.1) *Assume that F supports a set of discrete valuations, $\mathcal{V}$ as above, such that the 2-torsion part ${}_2\mathrm{Br}_{ur}(F)_{\mathcal{V}} = 0$. Then F has the vanishing genus property.*

Next let F be the function field $k(X)$ of a (normal) irreducible variety X over a field k, and consider the set $\mathcal{V}$ of all geometric valuations on F, that is the valuations that are trivial on k.

Theorem D. (Theorem 6.2) *Let $F = k(X)$, where X is a variety over a field k of characteristic $\neq 2$ such that, for the set $\mathcal{V}$ of all geometric valuations on F, the natural map ${}_2\mathrm{Br}(k) \to {}_2\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ is surjective and that the set of closed points of odd degree are dense in X. Assume that any finite field extension K/k of odd degree has the vanishing genus property. Then F has the vanishing genus property.*

In the case of Severi-Brauer varieties, one has the following result of [24, Proposition 5.8], which can also be seen as a special case of [17, Theorem B]. We provide an alternate proof.

Proposition E. (Proposition 6.3) *Let X/k be the Severi-Brauer variety of a k-csa A and let $\mathcal{V}$ be the set of all geometric valuations of $k(X)$. Then the natural map, $Br(k) \to \mathrm{Br}_{ur}(k(X))_{\mathcal{V}}$ is surjective.*

Corollary 3.3. *For k of characteristic $\neq 2$, if X is the Severi-Brauer variety of a division algebra D/k of odd degree, then $F = k(X)$ has the vanishing genus property.*

Proposition F. (Proposition 6.4) *Assume that any finite extension K/k has the vanishing genus property and let $F = k(X)$ where X is the Severi-Brauer variety of a k-csa D of index n and A_1, A_2 be F-cda's of exponent 2 such that $A_1 \leq A_2$ and $A_2 \leq A_1$. Then:*

(1) $A_1 \otimes A_2 \sim res_{F/k}(B)$ *for some* $B \in \mathrm{Br}(k)$.
(2) $A_1 \leq E$ *and* $A_2 \leq E$ *for E a representative of B_F, that is $E \in \overline{\mathrm{gen}}(A_i)$ for $i = 1, 2$.*
(3) *There exists a representative, E', for B/k with the same degree as D such that for any maximal subfield K of D where X has a point with residue field K and where A_1 is represented by an Azumaya algebra over the local ring of that point, we have that K is a maximal subfield of E'.*
(4) *If we assume that every finite extension K/k with $[K : k] = n$ has the vanishing genus property, then every maximal subfield of D is a maximal subfield of E', that is $D \leq E'$.*

Remark 3.4. Taking $X = \mathbb{P}^n$ in Proposition F yields the stability result for rational functions in n variables over k. Taking X the Severi-Brauer variety of a k-cda D and k a number field in Proposition F shows that $k(X)$ has the vanishing genus property.

3.1. Examples over large fields

In Sect. 7 we build various examples by means of index reduction formulas for Weil restrictions of Severi-Brauer varieties. We write $B \precsim A$ if every finite dimensional *separable* splitting field of B also splits A. If $\mathcal{A}, \mathcal{B}$ are collections of central simple algebras, we write $\mathcal{B} \precsim \mathcal{A}$ if $B \precsim A$ for every $A \in \mathcal{A}$, $B \in \mathcal{B}$.

We begin with a collection of central simple algebras over a field F, and then the collection obtained by a suitable base change F'/F. To implement this construction, we need to consider extensions that preserve basic arithmetic information about our central simple algebras. One of important properties in this respect is the notion of a conservative extension - see Definition 7.1.

Given a collection $\mathcal{A}$ of central simple F algebras, and a field extension F'/F, we will write $\mathcal{A}_{F'}$ to denote the collection of central simple F'-algebras of the form $A \otimes_F F'$ for $A \in \mathcal{A}$.

The starting point for our examples will rely on collections of algebras which are independent in the following sense:

Definition 3.5. Let A and B be central simple F-algebras. We say that B is independent of A if

$$\mathrm{ind}(B) = \gcd\{\mathrm{ind}(B \otimes A^i) \mid i = 0, \dots, \exp(A) - 1\}$$

We will say that a collection of central simple algebras $\mathcal{A}$ is independent if all pairs of distinct elements of $\mathcal{A}$ are independent.

Theorem G. *Suppose that $\mathcal{A}$, $\mathcal{B}$ are two collections of central simple algebras, all of the same prime power index p^n, such that every $A \in \mathcal{A}$ is independent of any $A' \in \mathcal{A} \setminus A$ and any $B \in \mathcal{B}$. Then there exists a field extension F'/F, conservative for both $\mathcal{A}$ and $\mathcal{B}$, and such that $\mathcal{B}_{F'} \precsim \mathcal{A}_{F'}$.*

As an application of this result, one can construct, for example, infinitely many central simple algebras of a fixed index p^n, with exponents chosen arbitrarily of the form p^i, $i \in \{1, \dots, n\}$, which all share the same finite separable splitting fields.

Corollary 3.6. *For any index set Λ and prime p, positive integer n, and family of integers $\{r_\lambda \in \{1, \dots n\} \mid \lambda \in \Lambda\}$, we can find a field F and a family of independent central simple F-algebras A_λ for $\lambda \in \Lambda$, having index p^n and exponent p^{r_λ} such that every pair of algebras A_λ, A_μ have the same collection of finite separable splitting fields. In particular, these also share the same maximal subfields.*

3.2. The involutory case

Let D be a central simple algebra over a field F, and let τ be an involution on D. Recall that τ is said to be of the first (resp. second) kind when it acts trivially (resp. nontrivially) on F. We say that two involutions of the second kind are **compatible** if they have the same action on the center. Note that this is stronger than merely saying that both are of the second kind.

Recall that τ is said to be of the first (resp. second) kind when it acts trivially (resp. nontrivially) on F. We say that two involutions of the second kind are **compatible** if they have the same action on the center. Note that this is stronger than merely saying that both are of the second kind.

A theorem of Albert [2, Theorem 10]-Riehm [21], says that when τ is an automorphism of F of degree 2, D has an involution of second kind fixing F^τ if and only if the corestriction $\mathrm{Cor}_{F/F^\tau}(D)$ is trivial as an element of the Brauer group of F^τ.

The next result refers to the notions given in Notation 2.1 below.

Theorem H. (Proposition 8.25) *Suppose $(D/F, \tau)$ is an algebra with involution of the second kind, and v is a valuation on F. Let $\bar{L}/\bar{F}$ be the ramification field of D. Suppose v is split with respect to τ. Then $\bar{L}/\bar{F} = \bar{L}/\bar{F}^\tau$ is also the ramification field at $\tau(v)$ (given by $\tau(v)(a) = v(\tau(a))$).*

Theorem I. (Theorem 8.39) *Suppose that $(D/F, \tau)$ is a τ-varied division algebra with involution (see Definition 8.31). Let L/F be a cyclic prime degree field extension such that L/F^τ is not cyclic when τ is of the second kind. Then there is a τ-invariant maximal separable subfield $K \subset D$ such that K/F does not contain a copy of L/F, unless $L = F(\sqrt{-1})$, $D = \mathbb{H} \otimes_F D'$, and F is a Pythagorean field. If τ is of the first kind, then $D = \mathbb{H}$.*

4. Étale subalgebras and ramification

4.1. Basic facts about the genus

For a central simple algebra of degree n over F, any commutative étale subalgebra is contained in a maximal one, which necessarily has degree n. It follows that for csa's A_1, A_2 over F, we have $A_1 \preceq A_2$ if and only if every maximal étale subalgebra of A_1 is isomorphic to a subalgebra of A_2. Similarly, $A_1 \leq A_2$ if and only if every maximal étale subalgebra of A_1 is a maximal étale subalgebra of A_2.

Lemma 4.1. *Suppose that A_1, A_2 are csa's over F, with $A_1 \leq A_2$. Then:*

(1) ind A_2 | ind A_1.
(2) *If $L \subset A_1$ with L/F a separable field extension, then for any inclusion $L \subset A_2$, we have $A_1^L \leq A_2^L$.*

Proof. (1) If $A_i = M_{r_i}(D_i)$ for division algebras D_i/F, and $A_1 \leq A_2$, then for any separable maximal subfield K of D_1, $r_1 K = K \oplus \ldots \oplus K$ is a maximal étale algebra of A_1 and hence $r_1 K$ is a maximal étale subalgebra of A_2. This implies that $r_2 \deg D_2 = r_1 \dim K$. If $e \in r_1 K$ is a primitive idempotent, $D_1 = eA_1e$ has the same degree as eA_2e and $D_1 \leq eA_2e$ so the index of A_2 divides the index of A_1.

(2) Since the maximal étale subalgebras of the centralizers A_i^L are the maximal étale subalgebras of A_i containing L, it follows that if $A_1 \leq A_2$ then $A_1^L \leq A_2^L$. □

Proposition 4.2. *For $A \in$ Br(F), the classes of all elements in $\overline{\text{gen}}(A)$ constitute a subgroup of* Br(F).

Proof. It is clear that if $A \leq B$ then $A \leq B^{op}$ so $\overline{\text{gen}}(A)$ is closed under inverses. Now let B, C be in $\overline{\text{gen}}(A)$. Any maximal subfield L of A is a maximal subfield of B and C. Thus, the index reduction factor of $B \otimes C$ [22, Theorem 24.34] is at least $[L : F] = \deg A$, implying the class of $B \otimes C$ has a representative E of the same degree as A. Then $E_L \sim B_L \otimes C_L \sim L$. Hence $A \leq E$ and we are done. □

4.2. Varied algebras

To understand when the exceptional cases in Theorem B can arise, we introduce the notion of varied division algebras:

Definition 4.3. A central division F-algebra D/F is said to be **varied** if there is no nontrivial cyclic extension K/F contained isomorphically in every maximal subfield of D/F.

Obviously to verify that D/F is varied it suffices to show there are no such K/F of prime degree. From this it follows that if $D = D_1 \otimes_F \ldots \otimes_F D_r$ and the D_i/F have distinct prime power degrees, then all D_i being varied implies that D is varied.

It is known that if F is a field finitely generated over a global field, then every division algebra D/F is varied, the only exception arising from $\mathbb{H}$, which denotes Hamilton's quaternion algebra $(-1,-1)_F$, generated by elements i and j such that $i^2 = j^2 = (ij)^2 = -1$. $\mathbb{H}$ need not be varied. But in fact this property holds much more generally due to the following result of Fein and Schacher. Recall that a field F is *Pythagorean* if the set of squares in F is additively closed.

Theorem 4.4. ([9])

Let D/F be a noncommutative division algebra and L/F a cyclic Galois extension of degree p. Suppose that every maximal subfield of a division algebra D/F contains an isomorphic copy of L/F. Then $p = 2$, D/F contains a copy of $\mathbb{H}$, and $L = F(\sqrt{-1})$. Furthermore, F is a Pythagorean field.

Theorem 4.4 says that a non-varied division algebra has the form $D = \mathbb{H} \otimes D'$, for some D'/F and F Pythagorean. If F is Pythagorean, $\mathbb{H}/F$ has the property that all maximal subfields are $F(\sqrt{-1})$. In [10] the authors provide an example of a non-varied division algebra with D' nontrivial, but there F is rather exotic, obtained by working inside the Pythagorean closure. They also provide examples of Pythagorean fields F over which necessarily a non-varied D must be $\mathbb{H}$. We can add:

Proposition 4.5. *Suppose $D = \mathbb{H} \otimes_F \Delta$, where Δ is a central division F-algebra of even degree d containing an element z that has degree $d/2$ over F. Then D is varied.*

Proof. First we assume that $\Delta = (a, b)$ is a quaternion algebra. Taking $x, y \in \Delta$ such that $x^2 = a$ and $y^2 = b$, with $xy = -yx$, note that the subfield generated by xi and yj has Galois group $C_2 \times C_2$, so its only square-central elements are in F, Fxi, Fyj, and $Fxiyj$, and their squares are squares of F times $1, -a, -b, ab$ respectively. If any of these are -1 we could assume that $a = 1, b = 1$, or $ab = -1$, contrary to Δ being a division algebra. (If $ab = 1$ then $(xy)^2 = -ab = -1$.)

In general, D contains $\mathbb{H} \otimes_F C_\Delta(z) = (\mathbb{H} \otimes_F F(z)) \otimes_{F(z)} C_\Delta(z)$, so we are done by the previous paragraph, taking $F(z)$ instead of F. □

Observing that certain classes of fields are known to be non-Pythagorean, we obtain the following.

Corollary 4.6. *D/F is necessarily varied under any of the following hypotheses:*

(1) *F is finitely generated over a local or global field.*
(2) *F is finitely generated over an algebraically closed or real field k, containing an element transcendental over k.*
(3) *D/F has odd degree.*
(4) *F contains $\sqrt{-1}$.*

4.3. Complete discretely valued fields

The main tool we will use to prove Theorems A and B is ramification. In this section we explore how discrete valuations factor into the partial order relation of Definition 1.1.

Proposition 4.7. *Suppose that v is a discrete valuation on F, and for $i = 1, 2$, we assume that A_i are F-central simple algebras with $A_1 \leq A_2$. Let F_v be the completion of F with respect to v and $A_{i,v} = A_i \otimes_F F_v$. Then $A_{1,v} \leq A_{2,v}$.*

The following proof follows [11, Lemma 3.1] closely. A different proof is possible along the lines of [4,23].

Proof. Suppose K_v is a maximal étale subalgebra of $A_{1,v}$. Then $K_v = F_v(\alpha_v)$. Because K_v is maximal, the reduced characteristic polynomial $f_v(x)$ (cf [22, Remark 24.67(iv)] of α_v is also its minimal polynomial and is separable. Since A_1 is dense in $A_{1,v}$ in the topology on the latter as a vector space over K, one can choose $\alpha \in A_1$ to be arbitrarily close to αv. Then the Cayley-Hamilton polynomial $f(x)$ of α will be close enough to $f_v(x)$ so that we can use Krasner's lemma [1] to conclude that $f(x)$ is separable and we can choose α such that $f(x)$ is its minimal polynomial, $f(x)$ is separable, and $F(\alpha) = F[x]/(f(x))$ satisfies $F(\alpha) \otimes_F F_v \cong F_v(\alpha_v)$. By assumption $F(\alpha) \subset A_2$ and so $K_v \cong F(\alpha) \otimes_F F_v \subset A_{2,v}$. □

Due to Proposition 4.7, the analysis of our one-sided relation to a significant degree reduces to the case of complete discretely valued fields, which we are going to discuss next. With this in mind, let us fix some objects and notation for the remainder of the section, recalling basic facts about division algebras over complete discretely valued fields.

Notation 4.8. Let F be a field complete with respect to a discrete valuation v, with valuation ring R and uniformizer π and residue field $\bar{F}$. Let D/F be a tame (i.e. inertially split) division algebra, and let v also denote the extension of the valuation v to D. We now recall some of the details of the structure of D. The algebra D has an extended valuation ring S with uniformizer Π such that $\Pi S = S\Pi$ is the maximum two-sided ideal and $S\Pi \cap R = R\pi$. Furthermore, $\bar{D} = S/\Pi S$ is a division algebra whose center we denote as $\bar{L}$. Since D is tame, the extension $\bar{L}/\bar{F}$ is always a cyclic Galois extension, with conjugation by Π inducing a generator $\bar{\sigma}$ of its Galois group ([14, Proposition 1.7]). We may identify $(\bar{L}/\bar{F}, \bar{\sigma})$ with the ramification of the Brauer class $[D]$ and we say that $\bar{L}$ or L is the **ramification**

field of D, cf. Theorem H. Since the automorphism of $\bar{L}$ extends to one of $\bar{D}$ via conjugation by Π, by Galois descent $\bar{D}$ is therefore the image (under restriction) of some $\bar{D}'$ with center $\bar{F}$. We can lift $\bar{D}'$ to an unramified division algebra D'/F, and D is Brauer equivalent to $D' \otimes \Delta(L/F, \sigma, \pi)$ (as in [14, Lemma 5.14]), where L/F is the unique unramified lifting of $\bar{L}/\bar{F}$, and σ the lift of $\bar{\sigma}$.

We note that if L'/F is unramified, then $D \otimes_F L'$ is unramified if and only if $\bar{L}'$ contains $\bar{L}$, or L' contains L.

Lemma 4.9. *Let E be the underlying division algebra of $D \otimes_F L$. Then $\bar{E} = \bar{D}$.*

Proof. Let $\bar{L} = \bar{F}(\bar{u})$, lift $\bar{u}$ to an element $u \in D$, and let L' be the maximal unramified subfield of $F(u) \subset D$. Then $\bar{L}' = \bar{L}$ and so $L' \cong L$. Thus $D \otimes_F L$ contains a primitive idempotent $e \in L' \otimes_F L$ with $E \cong e(D \otimes_F L)e = D^{L'}$. We know that E is unramified and $\bar{E} \subset \bar{D}$. Checking dimensions finishes the proof. □

Lemma 4.10. *Let D be a (tame) cda with ramification field L. If there exists a totally ramified extension K/F that splits D then $\bar{D} = \bar{L}$, hence is commutative. In particular, if D/F is also unramified, $D = F$.*

Proof. Of course KL splits D, and hence splits the underlying division algebra E of $D \otimes_F L$. Since E is unramified it is the image of $\alpha \in \operatorname{Br}(T)$ for $T \subset L$ the valuation ring. Let $T' \subset KL$ be the valuation ring in KL extending T. Since KL splits E, T' splits α. However KL/L is totally ramified so $\bar{T} = \bar{L} = \bar{T}'$ and $\operatorname{Br}(T') \to \operatorname{Br}(\bar{L})$ is an isomorphism. It follows that $\bar{E} = \bar{L}$ and we are done. □

Lemma 4.11. *Suppose K/F is unramified, and let E be the underlying division algebra of $D \otimes_F K$. Then $\bar{E}$ is the underlying division algebra of $\bar{D} \otimes_{\bar{L}} (\bar{K}\bar{L})$.*

Proof. Now KL/K is the ramification field of E and so $\bar{E}$ contains $\bar{K}\bar{L}$ as its center. If E' is the underlying division algebra of both $D \otimes_F KL$ and $E \otimes_K KL$ then, by Lemma 4.9, $\bar{E}'$ is $\bar{E}/(\bar{K}\bar{L})$. Replacing D by the underlying division algebra of $D \otimes_F L$ allows us to assume that D is unramified and now the assertion is clear. □

Proposition 4.12. *Suppose D/F has degree n and ramification field L/F of degree e_D. Let K/F be a field extension having degree m and ramification degree e_K, that splits D. Set $t = [(L \cap K) : F]$. Then the residue field $\bar{K}\bar{L}/\bar{L}$ splits $\bar{D}$, and $s = [\bar{K}\bar{L} : \bar{L}]/(n/e_D)$ is an integer. Furthermore, for $r = [K : F]/n$, the number $r/s = e_K/(e_D/t)$ is an integer.*

Proof. $\bar{D}$ has center $\bar{L}$, and the degree of $\bar{D}$ over $\bar{L}$ is n/e_D. Let K'/F be the maximal unramified subfield of K/F, which therefore has degree $\bar{m} = m/e_K$ and residue field $\bar{K}' = \bar{K}$. Since K/K' is totally ramified and L/F is unramified, $L \cap K' = L \cap K$ and $t = [(L \cap K') : F]$. Of course, $\bar{m}/t = [K'L : L] = [\bar{K}\bar{L}/\bar{L}]$. Also, $[L : L \cap K'] = e_D/t = [K'L : K']$. Let $D_{K'}$ be the underlying division algebra of $D \otimes_F K'$ and let n' be its degree. Since $D \otimes_F K'$ has ramification field $K'L/K'$, it follows that $e_{D_{K'}} = e_D/t$. Since $D_{K'}$ is split by K/K', $\overline{D_{K'}} = \bar{K}'\bar{L}$ is commutative and $n' = e_{D_{K'}} = e_D/t$. Since K/K' splits D'/K', the degree $[K : K'] = e_K$ is a multiple of $n' = e_D/t$.

Since $KL/K'L$ is totally ramified, $K'L$ splits D. Thus $\bar{K}'\bar{L}$ splits $\bar{D}$, s is an integer, and by definition $\bar{m}/t = \frac{n}{e_D}s$. Again, by definition, $[K : F] = e_K\bar{m} = nr$. Together we have $nr = e_K(ts)(n/e_D)$, or $r/s = e_K/(e_D/t)$, which is an integer.□

Corollary 4.13. *Let L/F be the ramification field of D. Then for any maximal subfield K of D satisfying $e_K = e_D$, the extensions K/F and L/F are linearly disjoint.*

Proof. In the notation of Proposition 4.12, $r = 1$ so $s = t = 1$. □

Proposition 4.14. *Suppose E/F and D/F are central division algebras with $E \leq M_r(D)$ and let L_D, L_E be the respective ramification fields. Assume that $\bar{E}/\bar{L}_E$ is varied (Definition 4.3). Then $L_D \subset L_E$.*

Proof. It suffices to show that L_E splits the ramification of D. Consider the centralizers E', A' of L_E in E and $M_r(D)$ respectively. Then E' is unramified and it suffices to show that A' is unramified. That is, we may assume that E is unramified. If K/F is a maximal separable subfield of E, necessarily unramified, then K/F splits D and hence contains L_D. That is, $\bar{K}$ contains $\bar{L}_D$. Since $\bar{E}$ is varied, $\bar{L}_D = \bar{F}$ and so $L_D = F$. □

Let D and E be as in Proposition 4.14. Pick a uniformizer $\Pi \in E$ and let K be a maximal subfield of E containing Π. Then $e_K = e_E$. Since K is linearly disjoint from L_E it is linearly disjoint from L_D and hence, in the notation of Proposition 4.12, $t = 1$. That is, $r/s = e_E/e_D$ an integer.

Now let P be an unramified maximal subfield of E containing L_E. Applying Proposition 4.12 again, we have $r/s = t/e_D = 1$. Thus, we have proved the following:

Proposition 4.15. *Let E/F and D/F be as in Proposition 4.14. Then e_D divides e_E and e_E/e_D divides r. In particular, if $r = 1$ then $L_E = L_D$.*

In Proposition 4.15, let E have degree e and D have degree d, so $e = rd$. Take $s = \frac{r}{e_E/e_D}$, so $\frac{e}{e_E} = s\frac{d}{e_D}$.

Corollary 4.16. *Let E/F and D/F be as above. Then $\bar{E} \leq M_s(\bar{D} \otimes_{\bar{L}_D} \bar{L}_E)$.*

Proof. The unramified maximal subfields of E all contain L_E and correspond to the maximal separable subfields of $\bar{E}$. An unramified extension K/F which splits D and contains L_E must split $D \otimes_F L_E$. Since $D \otimes_F L_E$ is unramified its residue division algebra must have the same Brauer class as $\bar{D} \otimes_{\bar{L}_D} \bar{L}_E$ and must be split by $\bar{K}$. □

We observe that the hypothesis in Proposition 4.14 that $\bar{E}/L_E$ be varied is necessary.

Lemma 4.17. *Let F be a field complete with respect to a discrete valuation, and having residue field $\bar{F} = \mathbb{R}$, the field of real numbers. (For a example, one could take $F = \mathbb{R}((x))$.) Let E be the quaternion division algebra $\mathbb{H} = (-1, -1)_F$, and let $D = (-1, \pi)_F$ where π is a prime element of F. Then $E/F \leq D/F$, $L_E = F$ and $L_D = F(\sqrt{-1})$. Thus L_D is not contained in L_E.*

Proof. E is unramified and every maximal subfield of $\bar{E}$ is the complex field $\mathbb{C}$. Thus every maximal subfield of E is $F(\sqrt{-1})$. It follows that $E/F \leq D/F$. Since E/F is unramified, $L_E = F$ and $L_D = F(\sqrt{-1})$ is clear. □

We will see that $(-1, -1)$ plays a prominent role in all D/F that are not varied.

Applying the argument of the paragraph following 4.14 to Theorem 4.4, we have:

Corollary 4.18. *Suppose F is a field complete with respect to a valuation and E/F and D/F are division algebras with ramification fields L_E and L_D. Assume that $E \leq M_s(D)$ for some s. Then $L_D L_E \subseteq L_E(\sqrt{-1})$. If $L_D = L_E(\sqrt{-1}) \neq L_E$, then L_E/F has odd degree and $F = K((\pi))$ for a Pythagorean field K.*

Proof. To prove the first statement, we take the centralizer of L_E in E and reduce the problem to the case that $L_E = F$, and hence E/F is unramified. Since all the maximal subfields of E are unramified and split D/F, they all contain L_D, implying $L_D \subseteq F(\sqrt{-1})$.

Assume that $L_D = L_E(\sqrt{-1}) \neq L_E$. Since $L_D/F = (L_E \otimes_F F(\sqrt{-1}))/F$ is cyclic Galois, it follows that L_E/F has odd degree. Since $\bar{F}$ must be Pythagorean and characteristic 0, F must be as given. □

Corollary 4.19. *Suppose D, E and F are as in* Corollary 4.18*, and take $r \geq 0$ such that 2^r divides $[L_D : F]$ but 2^r does not divide $[L_E : F]$. Then $r = 1$ and $\bar{E}$ has even degree.*

Proof. Let G_D and G_E be the respective Galois groups of L_D/F and L_E/F. If L_D is a proper subset of $L_E(\sqrt{-1})$, there is a surjection $G_E \oplus \mathbb{Z}/2\mathbb{Z} \to G_D$ with nontrivial kernel J. If J has odd order, then $J \subseteq G_E$ and $G_E/J \oplus \mathbb{Z}/2\mathbb{Z}$ is cyclic, implying G_E/J has odd order and $r = 1$. (Otherwise 2^r divides $|G_E|$, a contradiction.) Since D has even degree, $\bar{E}$ has even degree. □

4.4. Ramification

Suppose that the ground field F supports a tame class $\mathcal{V}$ of discrete valuations. For any division algebra D/F, the **ramification locus** R_D of D/F is the set of valuations $v \in \mathcal{V}$ such that D_v/F_v is ramified, and the **ramification data** is the set of triples $(v, L/\bar{F}_v, \sigma)$ where v is in R_D, $\bar{F}_v$ is the residue field, and $L/\bar{F}_v, \sigma$ is the ramification of D/F at v (where σ is the automorphism obtained by conjugation by the uniformizer Π). Note that L above is the ramification field of D_v, which we call the ramification field of D/F at v. If D/F and E/F are division algebras then we say the ramification data of E/F is **smaller** than that of D/F if $R_E \subseteq R_D$, and if for all $v \in R_E$, the ramification field of E at v can be injected into the ramification field of D at v.

Lemma 4.20. *Suppose F is a field and $\mathcal{V}$ a tame set of valuations on F. Suppose that D, E are division algebras over F with $E/F \leq M_r(D)/F$. If E/F has odd degree, or if none of the residue fields F_v have Pythagorean finite extension fields, then the ramification data of D/F is smaller than that of E/F.*

Proof. This is an immediate consequence of Proposition 4.15. □

Definition 4.21. D is **exceptional** if $D = \mathbb{H}$ over $F = K((\pi))$, where K is a Pythagorean field.

Theorem 4.22. *Let D be a cda of degree n and assume that ${}_n\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ is finite, and the ramification locus R_D is finite. Then $\overline{\mathrm{gen}}(D)$ is finite unless $D = \mathbb{H}$ is exceptional, with a bound given in the proof. In this case,*

$$\overline{\mathrm{gen}}(D) = \{(-1, f)_{F,2} \mid f \in K^\times \text{ or } f \in K^\times x\}.$$

Proof. (Parallel to [5, Theorem 2.2].) First we assume that D is not exceptional. Then, by Proposition 4.14, for any $D' \in \overline{\mathrm{gen}}(D)$, we have $R := R_{D'} \subseteq R_D$. At every $\nu \in R$ there are at most n possible images for $[D']$ under the ramification map ρ_ν. Hence the total number of $D \leq D''$ with $R_{D''} = R$ is bounded by $|\operatorname{Br}_{ur}(F)_{\mathcal{V}}|n^r$ where $r = |R|$. Summing over all subsets of R_D shows that $|\overline{\mathrm{gen}}(D)|$ is finite. Explicitly,

$$|\overline{\mathrm{gen}}(D)| \leq |{}_n\mathrm{Br}_{ur}(F)_{\mathcal{V}}| \cdot n^r \tag{1}$$

where $r = |R_D|$.

Hence we may assume that D is exceptional. Let D' be in $\overline{\mathrm{gen}}(D)$. By assumption $F[\sqrt{-1}] \subset D'$; hence $D' = (-1, f)_{F,2}$ and we may take $f \in K[[x]]$. If f is a unit in $K[[x]]$ we may assume that $f \in K^\times$, or else $f = kx$ for a unit $k \in K[[x]]$ and again we may take $k \in K^\times$. □

[5] gives a sufficient condition (called Condition (A)) for R_D to be finite. However, this fails in general: one could take the extension F of Q obtained by adjoining the square roots of all primes $p \cong 1 \pmod 8$. Then the dyadic place of $\mathbb{Q}$ has infinitely many extensions v to F, and $F_v = \mathbb{Q}_2$ for any extension we have. It follows that $\mathbb{H} = (-1, -1)_F$ ramifies at all these places.

Theorem 4.23. *If F is finitely generated and char$(F) \not| $ ind(A), then $\overline{\mathrm{gen}}(A)$ is finite.*

The estimate in (1) yields the finiteness of the genus once we know the finiteness of ${}_n\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ and of r. In [6], every finitely generated field F is equipped with a set $\mathcal{V}$ of discrete valuations (assuming that $\mathrm{ind}(A)$ is primes to $\mathrm{char}(F)$) for which all assumptions of Theorem 4.22 hold (in fact, these assumptions hold for any divisorial set of places of F).

5. The exponent

In this section we will be interested in how this one-sided relation interacts with exponents. Looking at the anomalous case in Corollary 4.19 we have the following. Suppose $\mathcal{V}$ is a set of discrete valuations on F as above and for each $v \in \mathcal{V}$ let $\rho_v : \mathrm{Br}(F) \to H^1(\bar{F}_v, \mathbb{Q}/\mathbb{Z})$ be the ramification map (only defined under the condition of tameness). Recall $\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ from 2.3.

We now give the proof of Theorem A, which we restate explicitly:

Suppose that $\mathcal{V}$ is a collection of discrete valuations on a transparent field F such that ${}_n\mathrm{Br}_{ur}(F)_{\mathcal{V}} = 0$. Suppose that $E \leq D$ for a central simple algebra D and a central division algebra E. Then the exponent of D divides the exponent of E.

Proof of Theorem A. The exponent of E/F is the l.c.m. of the orders of all the $\rho_v(E)$ and these orders are the degrees of the ramification fields. For $v \in \mathcal{V}$ let E_v be the division algebra underlying $E \otimes_F F_v$.

For an odd prime p it is obvious that if p^r divides the exponent of D it divides the exponent of E, so we need only check $p = 2$. If r is maximal such that 2^r divides the exponent of D then there is a $v \in \mathcal{V}$ such that 2^r divides the order of $\rho_v(D)$. By Corollary 4.19, either $r > 1$ so 2^r divides the exponent of $\rho_v(E)$ and hence the exponent of E, or $r = 1$ implying $\bar{E}_v$ has even exponent and so E has even exponent. □

We call the conclusion of Theorem A, **the exponent divisibility property**.

Next we consider $F = k(X)$ where X is a variety over a field k, and instead of taking all discrete valuations we only consider the geometric ones, that is ones which are trivial on k.

Theorem 5.1. *Let X be a variety over a field k such that $\mathrm{Br}_{ur}(k(X)) = \mathrm{Br}(k)$ and $X(k)$ is Zariski-dense in X. If k has the exponent divisibility property then $F = k(X)$ has this property too.*

Proof. Take E/F with $E \leq B$. Suppose $\exp(E) = n$ and consider $A = E \otimes B^{-1}$. By the same reasoning as in the proof of Theorem A we see that $A^n \in \mathrm{Br}_{ur}(F) = \mathrm{Br}(k)$. Thus $A^n = res_{F/k}(D)$ for some $D \in \mathrm{Br}(k)$, and it is enough to show that D is trivial. Choose a rational point $p \in X(k)$ such that E is represented by an Azumaya algebra (of the same degree as E) over the local ring of p so that we can take residues (which is possible due to the assumption of the density of k-rational points). Consider the residues $\overline{E}^p$, $\overline{B}^p$ over k and get: $D = A^n = (\overline{E}^p)^n \otimes (\overline{B^{-1}}^p)^n$ but as $E^n \sim F$ we get $D = (\overline{B^{-1}}^p)^n$. Now notice that the residues satisfy $\overline{E}^p \leq \overline{B}^p$. (Details will be given in the proof of Theorem 6.2.) Now, $\overline{E}^{pn} \sim k$ implies $\overline{B^{-1}}^{pn} \sim k$ since k has the exponent divisibility property. We thus conclude $D = k$ and we are done. □

Corollary 5.2. *Let $F = k(X)$ as above. If E, B have the same maximal subfields then* $\exp(E) = \exp(B)$.

Remark 5.3. Taking $X = \mathbb{P}^n$ in 5.1 gives the stability of the exponent divisibility property with respect to rational functions in n variables over k.

6. Severi–Brauer varieties

Proposition 6.1. *Assume that $\sqrt{-1} \in F$ and F supports a set of discrete valuations, $\mathcal{V}$ as above, such that ${}_2\mathrm{Br}_{ur}(F)_{\mathcal{V}} = 0$. Then F has the vanishing genus property.*

Proof. Let A_1, A_2 be F-csa's of exponent 2, with $A_1 \leq A_2$ and $A_2 \leq A_1$. Consider the characters χ_1, χ_2 corresponding to A_1, A_2 respectively under the ramification map at some valuation ν. Since A_i are of exponent 2 and ${}_2\mathrm{Br}_{ur}(F)_{\mathcal{V}} = 0$, one has

$\chi_1 = \chi_2$ iff $\mathrm{Ker}(\chi_1) = \mathrm{Ker}(\chi_2)$. Thus A_1, A_2 sharing the same maximal subfields implies (via $\mathrm{Ker}(\chi_1) = \mathrm{Ker}(\chi_2)$) that $\chi_1 = \chi_2$, so we have $A_1 \otimes A_2 \in \mathrm{Br}_{ur}(F) = \{F\}$ implying $A_1 \cong A_2$. □

Theorem 6.2. *Let $F = k(X)$, where X is a variety over k such that ${}_2\mathrm{Br}_{ur}(F)_{\mathcal{V}}$ lies in the image of the natural map $\mathrm{Br}(k) \to \mathrm{Br}_{ur}(F)_{\mathcal{V}}$, where $\mathcal{V}$ is the set of all geometric valuations on F, and that the set of closed points of odd degree is Zariski-dense in X. Assume that any K/k of odd degree has the vanishing genus property. Then F has the vanishing genus property.*

Proof. Suppose there are two F-cda's A_1, A_2 of exponent 2 such that $A_1 \leq A_2$ and $A_2 \leq A_1$. As before one sees that $A_1 \otimes A_2 \in \mathrm{Br}(F)_{\mathcal{V}}$. Thus $A_1 \otimes A_2 = res(D)$ for $D \in \mathrm{Br}(k)$. Since the set of closed points of odd degree is Zariski-dense, by [12, Chapter 2, Corollary 8.16] we can find a smooth point, p, of odd degree, ensuring that $R := k[X]_p$ is regular, thus integrally closed, and we have Azumaya algebras of the same degree as A_i, $O_p(A_i)/k[X]_p$ over the local ring of p representing A_i. Write $B_i = O_p(A_i)$, and $\bar{A}_i = B_i/MB_i$ where M is the maximal ideal of R. Then $A_i = B_i \otimes_R F$ where F is the field of fractions of R. Let $K = R/M$. Writing $\overline{A_i}^p$ for the residue $O_p(A_i)/I(p)$ we have,

$$\overline{(A_1 \otimes A_2)}^p = \overline{A_1}^p \otimes \overline{A_2}^p = res_{K/k}(D)$$

But, since A_1 and A_2 have the same maximal separable étale subalgebras, the same holds for $\overline{A_1}^p$ and $\overline{A_2}^p$. Indeed let L be a maximal separable étale subalgebra of $\overline{A_1}$, write $L = K[t]$, choose a pre-image a of t in $O_p(A_1)$, and let $k[X]_p[a] \subset O_p(A_1)$. Lift a maximal separable étale subalgebra $\bar{L}_1 \subset \bar{A}_1$ to a maximal étale subalgebra S_1 of B_1 . By assumption $L_1 \cong L_2 \subseteq A_2$. Then S_1 is the integral closure of R in L_1 and corresponds to $S_2 \subset L_2$. Since S_2 lifts a maximal étale subalgebra, it is étale over R. Now since R is regular and any étale extension of a regular ring is regular, (cf. [3, Proposition 6.9.3], proved in [19, p. 75]) we see that S_2 is regular. Hence, the map $\mathrm{Br}(S_2) \to \mathrm{Br}(L_2)$ is injective by [3, Theorem 6.9.10]. Since L_2 splits A_2, wee see that S_2 splits B_2. Thus, there is a B_2' in the same Brauer class as B_2 with S_2 as a maximal étale subalgebra. Now $B_2/M \cong B_2'/M$ because these are central separable algebras of the same degree, Brauer equivalent, over K. Now $S_2/M \cong S_1/M = \bar{L}_1$ is a subfield of $\bar{A}_2$.

Thus by assumption $\overline{A_1}^p \cong \overline{A_2}^p$ and we get that $res_{K/k}(D) = K$ which in turn implies $D = k$ since $[K : k]$ is odd and D is of exponent 2. □

We turn our attention to the Severi-Brauer variety of a central simple algebra A [27, Chapter 13], defined as the variety of right ideals of A having minimal dimension. By the generic splitting field $F(A)$ we mean the function field of the Severi-Brauer variety of A, cf. [27, Theorem 13.11]. By [27, Theorem 13.12], if $A = M_r(D)$, $F(A)$ is a rational extension of $F(D)$.

Proposition 6.3. *Let X/k be the Severi-Brauer variety of a k-csa A and let $\mathcal{V}$ be the set of all geometric valuations of X. Then the natural map $\mathrm{Br}(k) \to \mathrm{Br}_{ur}(F(X))_{\mathcal{V}}$ is surjective.*

Proof. Let L/k be a Galois extension (with group G) such that $X \times L$ is projective space over L. Assume $B \in \mathrm{Br}(X)$. Then $B_{L(X)} = B_1 \otimes_L L(X)$ for a csa B_1/L. B_1 corresponds to an element of $H^2(G', \bar{k}^*)$, cf. [27, Corollary 13.15] where $G' = Gal(\bar{k}/L)$ and $\bar{k}$ is the separable closure of k. Note the exact sequence $1 \to G \to Gal(\bar{k}/k) \to G' \to 1$. Now up to stable equivalence we can assume $k(X) = L(I[G])^G$, where

$$0 \to I[G] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \tag{2}$$

is the usual augmentation lattice, in which the image of $I[G]$ is generated by $\{g - 1 : g \in G\}$, and the exact sequence $0 \to L^* \to L[I[G]]^* \to I[G] \to 0$ splits as abelian groups. B defines an element of $H^2(G', \bar{k}[I[G]]^*)$, since $\bar{k}(X)$ splits B and $L[I[G]]$ is a PID. Note that $H^2(G, I[G]) = 0$ from (2). This implies that

$$H^3(G, L^*) \to H^3(G, L[I[G]]^*)$$

is injective. We want to show that B_1 is the image of an element of $\mathrm{Br}(k)$. Hochschild-Serre (Teichmuller cocycle) says the obstruction is in $H^3(G, L^*)$ and the above injection says this is 0. Thus B_1 is the image of some B_2 and replacing B_1 by B_2 we may assume that $L(I[G])$ and hence $L[I[G]]$ splits B. But $H^2(G, L^*) \to H^2(G, L[I[G]]^*)$ is surjective and we are done. □

Proposition 6.4. *Let $F = k(X)$ where X is the Brauer-Severi variety of a k-csa D of index n and A_1, A_2 be F-cda's of exponent 2 such that $A_1 \leq A_2$ and $A_2 \leq A_1$. Then:*

(1) *$A_1 \otimes A_2 \sim res(B)$ for some $B \in \mathrm{Br}(k)$.*
(2) *$A_1 \leq E$ and $A_2 \leq E$ for E a representative of B_F, that is $E \in \overline{\mathrm{gen}}(A_i)$ for $i = 1, 2$.*
(3) *There exists a representative E' for B/k, of the same degree as D, such that for any maximal subfield K of D, where K has the vanishing genus property and where A_1 is represented by an Azumaya algebra over the local ring of a point with residue K, we have that K is a maximal subfield of E'.*
(4) *If we assume that every finite extension K/k with $[K : k] = n$ has the vanishing genus property, then every maximal subfield of D is a maximal subfield of E', that is $D \leq E'$.*

Proof. (1) This is clear as $A_1 \otimes A_2 \in \mathrm{Br}_{ur}(F)_{\mathcal{V}}$ for $\mathcal{V}$ the set of all geometric valuations on F (since X is a Severi-Brauer variety).
(2) It is enough to prove $A_1 \leq E_F$ for some csa E. Choose a maximal subfield K of A_1. Then $B_K = (A_1 \otimes A_2)_K = 0$. Thus the class of B_F has a representative E of the same degree as A_1, A_2. Now for any maximal subfield L of A_1 we have again $E_L \sim (A_1 \otimes A_2)_L \sim L$. Hence $E \in \overline{\mathrm{gen}}(A_i)$.
(3) Choose a point $p \in X$ of the same degree as D with residue field K/k, such that A_1 (and thus also A_2) is represented by an Azumaya algebra over the local ring of this point (which is possible as X has a dense set of points with residue K and A_1 can only ramify at a closed subset of X). Then taking residues we

have $\bar{A}_1 \otimes \bar{A}_2 \sim B_K$. Since the residues also have the same maximal subfields and K has the vanishing genus property we see that $B_K \sim K$. Thus B has a representative E' of the same degree as D and clearly K is a maximal subfield of E'.

(4) This is a direct result of the assumption and part (3).

□

7. Examples over large fields

As discussed in the introduction, given a collection $\mathcal{A}$ of central simple F algebras, and a field extension F'/F, we will write $\mathcal{A}_{F'}$ to denote the collection of central simple F'-algebras of the form $A \otimes_F F'$ for $A \in \mathcal{A}$.

Definition 7.1. Let $\mathcal{A}$ be a collection of central simple F-algebras, and F'/F a field extension. We say that F' is $\mathcal{A}$-conservative if $\operatorname{ind}(A) = \operatorname{ind}(A_{F'})$ and $\exp(A) = \exp(A_{F'})$ for all $A \in \mathcal{A}$.

Before proceeding to prove Corollary 3.6, it will be useful to record the following index reduction formula:

Lemma 7.2. *Let $\{B, B_\lambda : \lambda \in \Lambda\}$ be central simple algebras over a field F, and let F' be a compositum of the generic splitting fields $F(B_\lambda)$ of the algebras B_λ. Then*

$$\operatorname{ind} B \otimes_F F' = \gcd\{\operatorname{ind} B \otimes B_{\lambda_1}^{n_1} \otimes \cdots B_{\lambda_r}^{n_r}\}$$

where the gcd is taken over all finite tuples $\lambda_1, \ldots, \lambda_r \in \Lambda$ and all choices of $n_i \in \mathbb{Z}$.

Proof. For a finite subset $\Lambda_0 \subset \Lambda$, we write $F(\Lambda_0)$ for the compositum of the fields $F(B_\lambda)$ for $\lambda \in \Lambda_0$ (which in this case is the fraction field of the tensor product of these fields). It is easy to check that the index of $B_{F'}$ is the gcd of the indices of algebras $B_{F(\Lambda_0)}$ over all finite sets Λ_0. The result will follow when we show

$$\operatorname{ind} B_{F(\Lambda_0)} = \gcd\left\{\operatorname{ind} B \otimes \bigotimes_{\lambda \in \Lambda_0} B_\lambda^{n_\lambda} \mid n_\lambda \in \mathbb{Z}\right\}$$

We prove this by induction on the order of Λ_0. Therefore, assume that we know the result for a set Λ_0' and let $\Lambda_0 = \Lambda_0' \cup \{\mu\}$. We may then regard $F(\Lambda_0) = F(\Lambda_0')(B_\mu)$ and we have, by [29],

$$\begin{aligned}
\operatorname{ind} B_{F(\Lambda_0)} &= \gcd\left\{\operatorname{ind} B_{F(\Lambda_0')} \otimes_{F(\Lambda_0')} (B_\lambda)^{n_\mu}_{F(\Lambda_0')} \,\middle|\, n_\mu \in \mathbb{Z}\right\} \\
&= \gcd\left\{\operatorname{ind}(B \otimes_F B_\mu^{n_\mu})_{F(\Lambda_0)} \mid n_\mu \in \mathbb{Z}\right\} \\
&= \gcd\left\{\gcd\left\{\operatorname{ind}(B \otimes_F B_\mu^{n_\mu}) \otimes_F \bigotimes_{\mu \in \Lambda_0'} B_\lambda^{n_\lambda} \,\middle|\, n_\lambda \in \mathbb{Z}\right\} \,\middle|\, n_\mu \in \mathbb{Z}\right\} \\
&= \gcd\left\{\operatorname{ind} B \otimes \bigotimes_{\lambda \in \Lambda_0} B_\lambda^{n_\lambda} \,\middle|\, n_\lambda \in \mathbb{Z}\right\},
\end{aligned}$$

as desired. □

Proof of Corollary 3.6, based on Theorem G. Let F_0 be an arbitrary field containing a primitive p^n-th root of unity ε, and let $F_1 = F_0(x_\lambda, y_\lambda \mid \lambda \in \Lambda)$ be a rational function field with two generators for each element of Λ. Let D_λ be the symbol algebra $(x_\lambda, y_\lambda)_\varepsilon$. For each λ, let $F_\lambda = F_1(D_\lambda^{p^{r_\lambda}})$ be the generic splitting field of $D^{p^{r_\lambda}}$, and let F be a compositum of the fields F_λ, $\lambda \in \Lambda$. We claim that the collection of algebras $A_\lambda = D_\lambda \otimes_{F_1} F$ is independent, cf. Definition 3.5. This would then complete the proof by Theorem G. We therefore need to show that $A_\lambda \otimes_F A_\mu^i = (D_\lambda \otimes_{F_1} D_\mu^i) \otimes_{F_1} F$ has index divisible by the index of A_λ for all i and all $\lambda \neq \mu$. By Lemma 7.2, we have

$$\operatorname{ind}(D_\lambda \otimes_{F_1} D_\mu^i) \otimes_{F_1} F = \gcd\{\operatorname{ind} D_\lambda \otimes_{F_1} D_\mu^i \otimes \bigotimes_{\eta \in \Lambda_0} D_\eta^{p^{r_\eta} j_\eta}\}$$

where the gcd is taken over all finite sets $\Lambda_0 \subset \Lambda$ and all integers j_η. Assuming without loss of generality that $\lambda, \mu \in \Lambda_0$, we are then looking at the gcd of indices of algebras of the form:

$$D_\lambda^{1+p^{r_\lambda} j_\lambda} \otimes_{F_1} D_\mu^{i+p^{r_\mu} j_\mu} \otimes \bigotimes_{\eta \in \Lambda_0 \setminus \{\lambda, \mu\}} D_\eta^{p^{r_\eta} j_\eta}$$

But it is straightforward to check that the index of such an algebra is the product of the indices of the factors $D_\lambda^{1+p^{r_\lambda} j_\lambda}$, $D_\mu^{i+p^{r_\mu} j_\mu}$, and those of the form $D_\lambda^{p^{r_\eta} j_\eta}$. Consequently this is divisible by $\operatorname{ind} D_\eta^{1+p^{r_\lambda}} = \operatorname{ind} D_\lambda$. □

Let A be a central simple F algebra, K/F a separable field extension, and let $F_K(A)$ denote the function field of $R_{K/F} V_{A_K}$, the Weil restriction of the Severi-Brauer variety of A_K.

Lemma 7.3. *$K_{F_K(A)}$ is a splitting field for $A_{F_K(A)}$.*

Proof. To see this, we need to know that $V_{A_{F_{K(A)}}}(K_{F_{K(A)}}) \neq \emptyset$. But we have for any L/F regular,

$$V_{A_L}(L_K) = V_{A_K}(L_K) = R_{K/F} V_{A_K}(L),$$

where the second equality follows from the natural property of the Weil restriction. In particular, if $L = F_K(A)$ is the function field of $R_{K/F} V_A$, then the identity morphism tells us that our desired set is nonempty. □

The main ingredient in the proof of Theorem G is an index reduction formula, which is essentially a special case of [25, Proposition 3.6]:

Lemma 7.4. (Index reduction formula) *Let F^s be a fixed separable closure of F. Suppose that A, B are central simple F-algebras and let $K \subset F^s$ be a finite separable field extension of F. Then* ind $B_{F_K(A)}$ *is the greatest common divisors of numbers of the form:*

$$[E : F] \operatorname{ind}\left(\left(B \otimes A^{j(K:E)}\right)_E\right), \tag{3}$$

where E/F ranges over all finite separable extensions, j is a positive integer not exceeding $\deg(A)$, *and*

$$(K : E) = \gcd\left\{[g(K)E : E] \;\middle|\; g \in Gal(F)\right\},$$

where $g(K)E$ denotes the field compositum taken in F^s.

Proof. By [25, Proposition 3.6], $\mathrm{ind}\, B_{F_K(A)}$ is the greatest common divisor of numbers of the form

$$[G : J]\,\mathrm{ind}\left(\left(B \otimes_F L^J\right) \otimes_{L^J} \left(\otimes_g \mathrm{cor}^J_{J\cap H^g}\left(A^g_K \otimes_{g(K)} L^{J\cap H^g}\right)^{n_g}\right)\right) \tag{4}$$

where L/F is any Galois extension containing K/F with group G and which splits both A and B, where g runs through a set of double coset representatives for J, H in G, $H = \mathrm{Gal}(L/K)$, and where $J \subset G$ runs through all subgroups.

Writing $L^{J\cap H^g} = L^J g(K)$, we note that

$$\begin{aligned}\mathrm{cor}^J_{J\cap H^g}\left(A^g_K \otimes_{g(K)} L^J g(K)\right)^{n_g} &= \mathrm{cor}_{L^J g(K)/L^J}\, A^{n_g}_{L^J g(K)} \\ &= (A^{[L^J g(K):L^J]n_g})_{L^J}\end{aligned}$$

and so we may rewrite (4) as

$$[L^J : F]\,\mathrm{ind}\left(\left(B \otimes A^{\sum_g n_g [L^J g(K):L^J]}\right)_{L^J}\right). \tag{5}$$

But now, by taking L to be a larger Galois extension as needed, we may let L^J range through all separable extensions of F, and by taking appropriate choices for n_g not exceeding $\deg(A)$, our exponent may be chosen to be any multiple of $(K : E)$. The result follows. □

A consequence of this index reduction formula is that for sufficiently large K/F, the restriction map on the Brauer groups is injective.

Lemma 7.5. *Suppose A is a central simple algebra over F, and K/F is a separable extension with* $(\exp A) | [K : F]$. *Then* $\mathrm{Br}(F) \to \mathrm{Br}(F_K(A))$ *is injective.*

Proof. By Lemma 7.4, for a central simple algebra B, we have that $\mathrm{ind}\, B_{F_K(A)}$ is the greatest common divisors of numbers of the form:

$$[E : F]\,\mathrm{ind}\left(\left(B \otimes A^{j(K:E)}\right)_E\right), \tag{6}$$

where E ranges over finite separable field extensions of F. Let p be any prime that divides the index of B, and choose i maximal such that p^i divides the exponent of A. By passing to splitting fields of the prime-to-p factors of the primary decompositions of A and B, we may assume that $\mathrm{ind}\, A$, $\mathrm{ind}\, B$ are p-powers.

If the gcd from the statement of Lemma 7.4 is 1, it must happen that for some field extension E/F, the above number is not divisible by p. In particular, $[E : F]$ must not be divisible by p. But since $[K : F]$ is divisible by $\exp A$, we must also have p^i divides $[K : F]$ and hence also divides $[g(K)E : E]$ for any Galois conjugate $g(K)$ of K. But therefore p^i divides $(K : E)$ and $A^{j(K:E)}$ is split. We therefore have $(B \otimes A^{j(K:E)})_E \sim B_E$, and since $[E : F]$ is prime-to-p, $\mathrm{ind}\, B = \mathrm{ind}\, B_E \neq 1$, contradicting the expression (6) being 1. □

Corollary 7.6. *Suppose A is a central simple algebra over F and K/F is a separable extension with* $(\exp A) | [K : F]$. *Then the map* $\mathrm{Br}(F) \to \mathrm{Br}(F_K(A))$ *preserves exponents.*

Lemma 7.7. *Suppose that A and B are central simple algebras. If B is A-independent then* $\operatorname{ind} B_{F_K(A)} = \operatorname{ind} B$ *for all K/F finite and separable.*

Proof. Using the hypothesis together with the fact that $\operatorname{ind} C \mid [E : F] \operatorname{ind} C_E$ for every central simple F algebra C (see [18, Corollary 13.4(iii), p. 243]), we have:

$$\operatorname{ind} B \mid \operatorname{ind} B \otimes A^{j(K:E)} \mid [E : F] \operatorname{ind}(B \otimes A^{j(K:E)})_E,$$

for every finite separable field extension E/F and for every positive integer j. But by Lemma 7.4, this implies $\operatorname{ind} B \mid \operatorname{ind} B_{F_K(A)}$, and so $\operatorname{ind} B = \operatorname{ind} B_{F_K(A)}$ as claimed. □

Lemma 7.8. *Let A be a central simple F algebra and K/F a separable field extension with* $\operatorname{ind}(A) \mid [K : F]$. *Then* $\operatorname{ind}(A) = \operatorname{ind}(A_{F_K(A)})$.

Proof. Take p^n dividing $\operatorname{ind}(A)$. By Lemma 7.4, we must show that p^n divides the expression

$$[E : F] \operatorname{ind}\left(\left(A \otimes A^{j(K:E)}\right)_E\right)$$

for every finite separable extension E, and for every positive integer j. Choose such a separable extension and integer j. If $p \mid (K : E)$, then we are done since in this case,

$$\operatorname{ind}(A_E \otimes A_E^{j(K:E)}) = \operatorname{ind}(A_E^{j(K:E)+1}) = \operatorname{ind}(A_E^{rp+1})$$

which has the same p-power factor as $\operatorname{ind}(A_E)$ and so

$$p^n \mid \operatorname{ind}(A) \mid [E : F] \operatorname{ind}(A_E) = [E : F] \operatorname{ind}(A \otimes A^{j(K:E)})_E$$

as desired.

On the other hand, suppose that $p \nmid (K : E)$. By definition of $(K : E)$ this means that we have some conjugate of K, say $g(K)$ such that $[g(K)E : E]$ is relatively prime to p. But since $p^n \mid [g(K) : F] \mid [g(K)E : F]$ it follows that $p^n \mid [E : F]$. Consequently we have

$$p^n \mid [E : F] \mid [E : F] \operatorname{ind}(A \otimes A^{j(K:E)})_E$$

as desired.

□

Lemma 7.9. *Let A, B be central simple F-algebras, and suppose that B is A-independent. Suppose that K is a splitting field of B with* $\operatorname{ind}(A) \mid [K : F]$. *Let $F' = F_K(A)$. Then:*

- *F' is $\{A, B\}$-conservative,*
- *$K_{F'} = K \otimes_F F'$ is a splitting field of $A_{F'}$, and*

- *$B_{F'}$ is $A_{F'}$-independent.*

Proof. By Corollary 7.6, since $\exp(A) \mid \operatorname{ind}(A) \mid [K : F]$, it follows that $\exp A = \exp A_{F'}$ and $\exp B = \exp B_{F'}$. Lemma 7.7 shows us that $\operatorname{ind} B = \operatorname{ind} B_{F'}$ and Lemma 7.8 shows that $\operatorname{ind} A = \operatorname{ind} A_{F'}$. By Lemma 7.3 we know that $K'_{F'}$ is a splitting field of $A_{F'}$.

Finally, to see that the resulting algebras are independent, we note that since

$$\operatorname{ind} B \mid \operatorname{ind} B \otimes A^i \otimes A^{j(K:E)}$$

for all E, i, j (since B is A-independent), and $\operatorname{ind} B_{F'} = \operatorname{ind} B$, and

$$\operatorname{ind}(B \otimes A^i)_{F'} = \gcd\{\operatorname{ind} B \otimes A^i \otimes A^{j(K:E)}\},$$

it follows that

$$\operatorname{ind} B_{F'} \mid \operatorname{ind} A^i_{F'} \otimes B_{F'}$$

for all i, as desired. □

Proof of Theorem G. For a collection of central simple algebras $\mathcal{D}$, let $\mathcal{K}_{\mathcal{D}}$ denote the set of all maximal separable subfields of all central simple algebras of the form $M_\ell(D)$ for $D \in \mathcal{D}$. Note that this contains every finite separable splitting field of every D up to isomorphism.

Let $\mathcal{A}$, $\mathcal{B}$ be as in the statement of the theorem. We inductively define a sequence of field extensions of F by setting $F_0 = F$ and F_{i+1} to be the compositum of all field extensions of the form $F_K(A)$ for $K \in \mathcal{K}_{\mathcal{B}_{F_i}}$ and $A \in \mathcal{A}_{F_i}$. Note that there are natural inclusions $F_i \subset F_{i+1}$. Let F_∞ be the union of the fields F_i. It follows from Lemma 7.9 that the field F_∞ is $\mathcal{A} \cup \mathcal{B}$-conservative.

To complete the proof, we need to show that for every $B \in \mathcal{B}$ and every splitting field K of B_{F_∞}, we have that K also splits every $A \in \mathcal{A}$. Choose A, K, B as above. We may write $K = F_\infty[x]/f$ for $f \in F_i[x]$ for some i. For $j \geq i$, write K_j for the field $F_j[x]/f$. Note that $K_j \subset K_{j+1}$ and $\bigcup K_j = K$. Since B is split by K, it must therefore also be split by one of the fields K_j. But therefore $K_j \in \mathcal{K}_{\mathcal{B}_{F_j}}$ (or at least is isomorphic to a field in this collection), and so $F_{K_j}(A_{F_j}) \subset K_{j+1}$. This tells us that $(K_j)_{F_{K_j}(A_{F_j})} \subset K_{j+1}$. But by Lemma 7.3, $(K_j)_{F_{K_j}(A_{F_j})}$ splits A_{F_j}, and so K_{j+1} splits A. Since $K_{j+1} \subset K$, K splits A as well, and we are done. □

8. csa's with involution

Recall that an involution on a central simple algebra A/F is an antiautomorphism $\tau A \to A$ such that $\tau^2 = 1$. That is, $\tau(xy) = \tau(y)\tau(x)$ and $\tau(\tau(x)) = x$ for all $x, y \in A$. It follows that $\tau(F) = F$. We say that τ is of the first kind if τ is the identity on F and of the second kind if τ has order 2 on F. Recall further that involutions of the first kind can be either be orthogonal or symplectic type. If A^τ are the τ fixed or symmetric elements of A, then A^τ/F has dimension $n(n+1)/2$ over F where n is the degree of A/F. If τ is of symplectic type then A^τ has dimension $n(n-1)/2$ over F. If A has a symplectic involution then n must be even. We also say that two involutions of the first kind are **compatible** if they are both of orthogonal type or both of symplectic type.

Finally we recall ([BI] Theorem 3.1 p, 31) that A has an involution of the first kind if and only if the Brauer class of A/F has order 2. If σ is an automorphism of F of order 2, then A has an involution of the second kind if and only if the corestriction of the Brauer class of A to $\mathrm{Br}(F^\sigma)$ is trivial.

It will be useful to recall one way the above two results are proven.

Lemma 8.1. *Let A/F be a central simple algebra.*

$A \otimes_F A$ has an automorphism τ defined by $\tau(a \otimes b) = b \otimes a$. There is a one to one correspondence between involutions, σ, of the first kind and right ideals generated by primitive τ fixed idempotents $e \in (A \otimes A)$ defined by the relationship $(a \otimes 1 - 1\sigma(a))e = 0$. $(A \otimes A)^\tau \cong A_o \oplus A_s$ the direct sum of csa's corresponding to the trivial and sign representations of $< \tau >$. This corresponds to orthogonal and symplectic involutions.

Also assume F/F^η is a degree two Galois extension with Galois group $< \eta >$. Now define $\tau(a \otimes b) = b \otimes a$ to be the η semilinear automorphism of $A \otimes_\eta A$. As before, involutions, σ, of the second kind extending η correspond to right ideals of $A \otimes_\eta A$ generated by τ fixed primitive idempotents, e, via the same relation $(a \otimes 1 - 1\sigma(a))e = 0$.

Lemma 8.2. *Writing D as a tensor product $D_1 \otimes \cdots \otimes D_t$ of cda's, with each D_i of prime power degree, as in Remark 2.1, D has an involution of second kind fixing F^τ iff each D_i has an involution of second kind fixing F^τ.*

Proof. Apply the corestriction to the decomposition, to get

$$\mathrm{Cor}_{F/F^\tau}(D_1) \otimes \cdots \otimes \mathrm{Cor}_{F/F^\tau}(D_t) \sim 1.$$

□

Since the involution is part of the structure, we want to see what happens when we change the involution. The following is completely standard.

Lemma 8.3. *For any involutions σ, τ of A having the same kind, there is $d \in A^\times$ with $\sigma(a) = d\tau(a)d^{-1}$ for all $a \in A$ where $\tau(d) = \sigma(d) = \pm d$. If τ, σ are of the same type, we may assume that $\tau(d) = \sigma(d) = d$.*

Now assume that τ, σ are of the first kind. Let A^+ and A^- be the τ-symmetric and τ-skew symmetric elements of A respectively. If $\tau(d) = d(= \sigma(d))$, then dA^+ and dA^- are the σ-symmetric and σ-skew elements respectively. If $\tau(d) = -d$, then dA^+ and dA^- are the σ-skew and σ-symmetric elements, implying τ and σ have different types.

Proof. Since σ and τ differ by an automorphism, $\sigma(a) = d\tau(a)d^{-1}$ for some $d \in A^*$ defined up to multiplication by F^*. Since σ has order 2, $a = d\tau(d)^{-1}a\tau(d)d^{-1}$ for all $a \in A$ so $\tau(d) = \gamma d$ for $\gamma \in F^*$. Since τ has order 2, $\gamma\tau(\gamma) = 1$. If τ is of the second kind, there is an $x \in F^*$ with $\gamma = x/\tau(x)$ and replacing d by xd yields the needed result. If τ is of the first kind then $\gamma = \pm 1$. The statements about symmetric and skew elements are immediate, and this proves the relationship between the types. □

We occasionally write a^σ and a^τ for $\sigma(a)$ and $\tau(a)$ respectively.

Proposition 8.4. *The following assertions are equivalent, for two involutions σ, τ of A of the same kind:*

- *There is an isomorphism $(A, \tau) \cong (A, \sigma)$.*
- *The d from* Lemma 8.3 *is of the form $d \in Fu^\sigma u$.*
- *The d from* Lemma 8.3 *is of the form $d \in Fv^\tau v$.*

Proof. The isomorphism is inner, so there is $u \in D^\times$ such that $\sigma(uau^{-1}) = u\tau(a)u^{-1}$, so

$$\begin{aligned} uau^{-1} &= \sigma(\sigma(uau^{-1})) = \sigma(u)^{-1}\sigma\tau(a)\sigma(u) \\ &= \sigma(u)^{-1}d\tau(\tau(a))d^{-1}\sigma(u) = \sigma(u)^{-1}dad^{-1}\sigma(u) \end{aligned}$$

for all $a \in A$, implying $d^{-1}u^\sigma u \in F$. The argument is reversible. Likewise for τ. □

Often it is easier to treat division algebras with involution than csa's with involution, but we need the more general case and we can bridge the gap by observing:

Lemma 8.5. *Suppose $A = M_r(D)$ is a central simple algebra with involution τ.*

(a) *Assume that D is nontrivial, or τ is not symplectic. Then A has a minimal idempotent e with $e^\tau = e$.*
(b) *Suppose $e \in A$ is an idempotent with $e^\tau = e$. Then the involution τ', induced by τ on eAe, is of the same type.*

Proof. (a). Under our assumptions, D has an involution σ of the same type as A. If τ is symplectic, then D, if nontrivial, has 2-power index, and D has a symplectic involution. Then A has a different involution τ' given by $(d_{ij})^{\tau'} = (\sigma(d_{ji}))$ which has the same type as σ and hence as τ. We know that that there is an element $u \in A^*$ such that $\tau(x) = u\tau'(x)u^{-1}$ where $\tau'(u) = \tau(u) = u$. If $\tau(a) = \pm a$, then $a = ua'$ where $\tau'(a') = \pm a'$. Write $u = (d_{ij})$, so $\sigma(d_{11}) = d_{11}$.

Claim: We can change basis and assume that $d_{11} \neq 0$. Indeed, if any diagonal entry of u is nonzero, we permute bases and are done. If all diagonal entries are zero, we choose the first two basis elements and by block matrix arguments we may assume that u is a 2 by 2 matrix. Now the claim is an easy exercise, since we can conjugate u by a symmetric matrix to get a non-zero element in the 1-1 position.

Let a' be the matrix with d_{11}^{-1} in the 1,1 position and zeroes everywhere else. Then $\tau'(a') = a'$ and $e = ua'$ has zeroes in all columns except the first, and 1 in the 1,1 position. Now $e^2 = e$ and $e^\tau = e$.

(b). τ and τ' are of the same kind since F embeds into eAe, and thus compatible if of the second kind. Thus we may assume that τ and τ' are both of the first kind. Write

$$A = eAe \oplus eA(1-e) \oplus (1-e)Ae \oplus (1-e)A(1-e)$$

and let τ'' be the induced involution on $(1-e)A(1-e)$. Any τ-symmetric element is a tuple (a, b, b^τ, d) where a is τ' symmetric and d is τ'' symmetric, while b is arbitrary. Let n, r, s be the ranks of A, eAe, and $(1-e)A(1-e)$ respectively, so $n = r + s$ and $eA(1-e)$, $(1-e)Ae$ both have dimension rs. The dimension of the τ-symmetric space is maximized if τ is orthogonal and then is

$$\frac{n(n+1)}{2} = \frac{(r+s)(r+s+1)}{2} = \frac{1}{2}(r^2 + s^2 + 2rs + r + s)$$
$$= \frac{r(r+1)}{2} + \frac{s(s+1)}{2} + rs,$$

and similarly minimized if τ is symplectic, and then is

$$\frac{n(n-1)}{2} = \frac{(r+s)(r+s-1)}{2} = \frac{r(r-1)}{2} + \frac{s(s-1)}{2} + rs.$$

It is now clear by matching dimensions that τ' and τ'' must be compatible to τ. □

Note that the added assumption of Lemma 8.5(a) is needed because a symplectic involution on $M_{2n}(F)$ never preserves a minimal idempotent.

Proposition 8.6. *Suppose $A = M_r(D)$ is a central simple algebra with involution τ, and D is nontrivial or τ is not symplectic. Then there is a complete set of minimal orthogonal idempotents $e_1, \ldots, e_r$ with $e_i^\tau = e_i$ and involutions τ_i on D, such that τ_i is induced on D via $D = e_iAe_i$. Furthermore, the étale subalgebra of A, $L_1e_1 \oplus \ldots \oplus L_re_r$ is τ-invariant if and only if the $L_i \subset D$ are τ_i invariant.*

Proof. This is basically induction on r. Using Lemma 8.5 we can choose $e = e_1$ and then by induction on $(1-e)A(1-e)$ we have all the e_i. The rest is obvious.□

We need to define our one-sided relationship in the involutorial case. As a first step, we observe that preserving maximal étale subalgebras often amounts to containing certain symmetric or skew symmetric elements.

Lemma 8.7. *Let L/F be an étale extension of the field F of degree n and let τ be an F-automorphism of L of order 1 or 2. If τ has order 2, assume that L^τ/F has degree $n/2$. Then there is an $x \in L$ such that $L = F(x)$ and $\tau(x) = \pm x$. If $\tau : L \cong L$ has order 2 when restricted to F, then $L = F(x)$ for $x^\tau = x$.*

Proof. To prove the first statement, it suffices to show that such x form a Zariski open subset. If τ is the identity this is obvious so we assume that τ has order 2. Let $\bar{F}$ be the algebraic closure of F, and $\bar{L} = L \otimes_F \bar{F} = \bar{F} \oplus \ldots \oplus \bar{F}$. If $x = (x_1, \ldots, x_n) \in \bar{L}$ then $\bar{L} = \bar{F}(x)$ if and only if all the x_i are distinct. Also, if this $x \in L$, then $L = F(x)$ if and only if $\bar{L} = \bar{F}(x)$. Let $e_1, \ldots, e_n$ be the primitive idempotents of $\bar{L}$ which must be permuted by τ. Since $\bar{L}^\tau/\bar{F}$ has degree $n/2$, there must be an ordering of the e_i such that $\tau(e_i) = e_{n-i+1}$. That is, $x \in \bar{L}$ is a skew symmetric element if and only $x_i = -x_{n-i+1}$. The set of all such with distinct x_i (and necessarily $x_i \neq 0$) is nonempty Zariski open and defined over F.

As for the second statement, $L = L^\tau \otimes_{F^\tau} F$ by Galois descent and L^τ/F^τ is étale, so $L^\tau = F^\tau(x)$ for some x. □

In particular, if the involution τ is of the second kind, and K/F is a τ-invariant subfield, then $K = K^\tau \otimes_{F^\tau} F$.

The above degree condition is, of course, automatic when L is a field. In other cases, the degree condition must be assumed.

Example 8.8. If $L = L_1 \oplus L_2$ and τ has order 1 on L_1 and order 2 on L_2, then L cannot be generated by a skew or symmetric element. This can happen when τ is of orthogonal type, for example when $L = Fe_1 \oplus Fe_2 \oplus Fe_3$, $A = \mathrm{End}(V)$, $V = Fv_1 \oplus Fv_2 \oplus Fv_3$, $e_i(v_j) = 0$ for $i \neq j$, $e_i(v_i) = v_i$, and q is the quadratic form $q(v_1, v_1) = q(v_2, v_2) = q(v_i, v_3) = 0$ for $i \neq 3$, with $q(v_1, v_2) = q(v_3, v_3) = 1$. In this case $n/2 < \deg(L^\tau/F) < n$.

However when τ is symplectic this situation cannot occur.

Lemma 8.9. *Suppose $A/F, \tau$ is a central simple algebra of degree n with symplectic involution τ. Assume that $L \subset A$ is a maximal étale subalgebra which is τ-invariant. Then τ cannot be the identity on L, and L^τ/F has degree $n/2$.*

Proof. We can reduce to the case $A = M_n(F)$, and $L \subset A$ are the diagonal matrices and τ preserves L. Clearly τ permutes the idempotents of L and we need to show all the orbits of this permutation have length 2. This is clear when τ is symplectic since no primitive idempotent can be symmetric. □

This example forces us to strengthen our hypothesis for τ-invariant $L \subset A$.

Definition 8.10. Let n be the degree of a central simple algebra A with involution τ. We say $L \subset A$ is a τ-**maximal** étale subalgebra of (A, τ) if L is a maximal étale subalgebra, $\tau(L) = L$, and L^τ/F has degree n or $n/2$.

(This condition is stronger than simply saying that τ acts nontrivially on L, seen in Example 8.8.) Note that this requires n to be even, but anyway when n is odd and A has an involution of first kind, we know that $A = M_n(F)$. Now we can define our one-sided relationship in the involutorial case.

Definition 8.11. Let (A, τ), (B, σ) be central simple algebras with involutions of equal degree. We say $(A, \tau) \leq (B, \sigma)$ if and only if every τ-maximal étale subalgebra of A is isomorphic to a σ-maximal étale subalgebra of B.

We also define such a relation when σ is trivial: $(A, \tau) \leq B$ if and only if every τ-maximal étale subalgebra of A is isomorphic to a maximal étale subalgebra of B.

Proposition 8.6 allows us to deduce index results from the above relationship.

Lemma 8.12. *Suppose $(A/F, \tau) \leq B$. Then the index of B divides the index of A.*

Proof. If A has index $m > 1$ or τ is not symplectic, then A has a τ-maximal invariant étale subalgebra of the form $L_1 \oplus \ldots \oplus L_n$, where the degree of each L_i/F equals m. Since the L_i split B we are done in this case.

The remaining case is when $A = M_n(F)$ and τ is symplectic. In this case n is even, and we can write $A = M_{n/2}(F) \otimes_F M_2(F)$ where $\tau = \sigma \otimes \eta$, η is the symplectic involution, and σ is the transpose. It follows that $M_n(F)$ has a τ-maximal étale subalgebra of the form $F \oplus \ldots \oplus F$, and thus B is also split and has index 1. □

8.1. Involutions and valuations

Suppose $(D/F, \tau)$ is a division algebra with involution and v is a valuation on F. As in previous sections we would like to go to the completion of F at v, draw some conclusions, and then pull back results to F when we can. In this section we will always assume that the degree of D is prime to the characteristic of the residue field $\bar{F}$ of v and this residue characteristic is not 2. When τ is of the first kind there is no difficulty. If F_v is the completion, $D_v = D \otimes_F F_v$ is a csa with involution $\tau \otimes 1$ of the first kind. However, if τ is of the second kind, complications arise. First of all, τ may not preserve v and so one cannot define an extension of τ to D_v. When this happens, there are two valuations on F, v and $\tau(v)$ given by

$$\tau(v)(a) = v(\tau(a)).$$

These valuations, of course, agree on the fixed field F^τ. In this case we say that v is a **split** valuation with respect to $(D/F, \tau)$. Of course it may happen that $\tau(v) = v$, but even here there are two cases. If F/F^τ is ramified at v, we say that v is a **ramified** valuation with respect to $(D/F, \tau)$. Note that in this case the residue fields $\bar{F} = \bar{F}^\tau$ are equal. The other case happens when F/F^τ is unramified and nonsplit at v, and in this case we say that v is **unramified** with respect to $(D/F, \tau)$. Note that here $\bar{F}/\bar{F}^\tau$ has degree 2. Also note that if v is ramified with respect to (D, τ), then there is no prime $\pi \in F$ fixed by τ and some such π with $\tau(\pi) = -\pi$. If v is unramified with respect to (D, τ) then there is some prime $\pi \in F$ with $\tau(\pi) = \pi$ and some other prime $\pi' \in F$ with $\tau(\pi') = -\pi'$. $\tau(\pi') = -\pi'$

When we can, we will argue by going to the completion and so we are very interested in studying the case where F is complete with respect to v. Note that in this case D has a unique maximal order S which has a unique maximal ideal $\Pi S = S\Pi$. Thus $\tau(S) = S$ and $\tau(\Pi S) = \Pi S$. Set $\bar{D} = S/\pi S$ which is a division algebra with an induced involution $\bar{\tau}$. Let $\bar{L}$ be the center of $\bar{D}$. Then conjugation by Π induces an automorphism of $\bar{D}$ we call η. Of course, η restricts to an automorphism, σ, of $\bar{L}$. Whereas η depends on the choice of Π, all such choices differ by a an element of S^* and so σ is the unique automorphism defined in this way on $\bar{L}$. Also, $(\bar{L}/\bar{F}, \bar{\sigma})$ is the ramification of D at v.

We require some well known and basic results about how ramification behaves with respect to restriction and corestriction.

Theorem 8.13. *Let F be a field complete with respect to a valuation v with residue field $\bar{F}$, and F/F' a finite field extension of degree m and ramification index e. Let* $\mathrm{Br}(F)'$, $H^1(\bar{F}, \mathbb{Q}/\mathbb{Z})'$ *etc. the parts of these groups prime to the characteristic of the residue field, and* $\mathrm{ram} : \mathrm{Br}(F)' \to H^1(\bar{F}, \mathbb{Q}/\mathbb{Z})'$ *and* $\mathrm{ram} : \mathrm{Br}(F')' \to H^1(\bar{F}', \mathbb{Q}/\mathbb{Z})'$ *the ramification maps. Set Res :* $\mathrm{Br}(F')' \to \mathrm{Br}(F)'$ *and Res : $H^1(F', \mathbb{Q}/\mathbb{Z})' \to H^1(F, \mathbb{Q}/\mathbb{Z})'$ to be the restriction maps. Let* Cor *be the corestriction maps* $\mathrm{Br}(F)' \to \mathrm{Br}(F')'$ *and* $H^1(F, \mathbb{Q}/Z)' \to H^1(F', \mathbb{Q}/\mathbb{Z})'$. *Then* $\mathrm{ram} \circ Res = e(Res \circ \mathrm{ram})$ *and* $\mathrm{ram} \circ \mathrm{Cor} = \mathrm{Cor} \circ \mathrm{ram}$.

Proof. The restriction and corestriction of unramified Brauer classes are unramified, so it is enough to consider some primes π' of F' and π of F and compute the ramification of the restriction of $\Delta(L'/F', \pi')$ and the corestriction of $\Delta(L/F, \pi)$. It is also enough to separately consider the cases F/F' totally ramified and unramified. In the ramified case we may assume $N(\pi) = \pi' = u\pi^e$ where N is the norm and u is a unit. Then $L = L' \otimes_{F^\tau} F$ so $\mathrm{Cor}(\Delta(L/F, \pi)) = \Delta(L'/F', N(\pi)) = \Delta(L'/F', \pi')$ and the restriction of $\Delta(L'/F', \pi')$ is $\Delta(L/F, u\pi^e)$ proving the ramified case.

When F/F' is unramified, we can choose $\pi = \pi'$. The corestriction of $\Delta(L/F, \pi')$ is $\Delta(L'/F', \pi')$ where L'/F' is the corestriction of L/F. The restriction of $\Delta(L'/F', \pi)$ is $\Delta(L/F, \pi')$ where $L = L' \otimes_{F'} F$. □

We needed the above results to conclude:

Corollary 8.14. *Suppose D/F is a division algebra over the complete field F, v with ramification $\bar{L}/\bar{F}$. If K/F is unramified and splits D, then $K \supset L$ where L/F is the unique lift of $\bar{L}/\bar{F}$.*

Suppose F/F' is totally ramified and D/F has trivial corestriction. Then D/F is unramified.

Proposition 8.15. *Consider the map taking an umramified maximal subfield $K \subset D$ to $\bar{K} \subset \bar{D}$. This is one to one and onto on isomorphism classes. In particular, D contains a copy of L, the unique lift of the ramification field $\bar{L}$. If τ is an involution on D inducing $\bar{\tau}$ on $\bar{D}$, then the above map restricts to one taking τ preserving subfields to $\bar{\tau}$ preserving subfields. In particular, any τ preserves a copy of L.*

Proof. The map $K \to \bar{K}$ is injective on isomorphism classes by general facts. If $\bar{K}$ is a maximal subfield of $\bar{D}$ we can set $\bar{K} = \bar{F}(\alpha)$, so α has degree $n = e(n/e)$ over $\bar{F}$. Let $\beta \in D$ be a preimage of α. Since must have degree at least and at most n, $F(\beta)$ is a maximal subfield with residue degree n and so must be unramified. It must therefore contain a copy of L. If $\tau(\alpha) = \pm\alpha$, then replacing β by $(1/2)(\beta + \tau(\beta))$ or $(1/2)(\beta - \tau(\beta))$ suffices. If $\tau(K) = K$, then L is the unique subfield of K which is a lift of $\bar{L}$, and so $\tau(L) = L$. □

One consequence of the above is a description of D as a so-called generalized cyclic algebra. Let $L \subset D$ be a choice of lift of $\bar{L}$ with centralizer $E \subset D$.

Theorem 8.16. *$D = E \oplus E\Pi \oplus \ldots \oplus E\Pi^{e-1}$ where $\Pi E \Pi^{-1} = E$ and $\Pi^e \in E^*$. That is, D is a generalized cyclic algebra.*

Proof. The automorphism $\bar{\eta}$ on $\bar{E}$ corresponds to an idempotent of $\bar{E} \otimes_{\bar{\sigma}} E^\circ$ and therefore there is an automorphism $\eta : E \cong E$ which lifts $\bar{\eta}$ and extends σ on L. Thus there is a $u \in D^*$ such that $uxu^{-1} = \eta(x)$ for all $x \in E$. Write $u = s\Pi^r$ for some r. Since η reduces to $\bar{\eta}$, r is congruent to 1 modulo e. Since E/L is unramified, $\Pi^e = t\pi$ where $t \in S^*$ and π is a prime of F. Thus we can modify u by powers of π such that $u = s\Pi$ and then rename. □

Using idempotents gives a convenient way to view well known facts about extending involutions. Note that there is no complete valuation in this result.

Lemma 8.17. *Let σ be an automorphism of F of order 2 and D/F a division algebra. Suppose $L \subset D$ is a subfield and σ extends to an automorphism of L of order 2. Let $E \subset D$ be the centralizer of L. Suppose D/F has an involution of the second kind extending σ. Then any involution of the second kind of E, extending σ, can itself be extended to an involution of the second kind of D.*

Proof. Let μ be the σ semilinear automorphism of $D \otimes_{F,\sigma} D$ defined by $\mu(a \otimes b) = b \otimes a$. By assumption $B = (D \otimes_{F,\sigma} D)^{\mu}$ is a matrix algebra over F^{σ}. We have $(L \otimes_{\sigma} L)^{\mu} \subset B$. There is an idempotent $e \in (L \otimes_{\sigma} L)^{\mu}$ generating the kernel of $phi : (L \otimes_{\sigma} L)^{\mu} \to L^{\sigma}$ defined by $\phi(x \otimes y) = x\sigma(y)$ which we note satisfies $\phi \circ \mu = \sigma \circ \phi$. Then $E \otimes_{L,\sigma} E \subset e(D \otimes_{F,\sigma} D)e \subset (D \otimes_{F,\sigma} D)$ defines an embedding $(E \otimes_{L,\sigma} E)^{\mu} \subset B$. An involution of E defines an idempotent f of $(E \otimes_{L,\sigma} E)^{\mu}$ and when f is viewed as an element of B it can be written as a sum of primitive idempotents each of which defines an involution of D extending the given one of E. □

A basic way that involutions behave well in the complete case is the following. Note that there are many versions of this that are well known in the commutative case.

Lemma 8.18. *Let D/F be a division algebra where F is complete with respect to a discrete valuation v. Let τ be an involution on D which must preserve the maximal order $S \subset D$ and maximal ideal $\Pi S \subset S$. Assume $\tau(\Pi) = \pm\Pi$. Suppose $u \in 1 + \Pi S$ is fixed by τ. Then there is a $v \in 1 + \Pi S$ such that $u = v\tau(v)$.*

Proof. To begin with set $x_1 = 1$ and assume, by induction, $x_i u \tau(x_i) = 1 + s_i \Pi^i$ for $s_i \in S$. If $\tau(\Pi) = \Pi$ then s_i is τ fixed and if $\tau(\Pi) = -\Pi$ then $\tau(s_i) = -s_i$. In the first case we can choose z such that $z + \tau(z) = s_i$. Other wise we choose z such that $s_i = z - \tau(z)$. Set $x_{i+1} = (1 - z\pi^i)x_i$. Then $x_{i+1} u \tau(x_{i+1}) = (1 - z\pi^i)(1 + s_i\pi^i)\tau(1 - z\pi^i) = 1 + s_{i+1}\pi^{i+1}$ for some s_{i+1} as needed. Let x be the limit of the x_i so $xu\tau(x) = 1$. Then we are done if we set $v = x^{-1}$. □

Combining the above results give results about lifting involutions uniquely.

Lemma 8.19. *Let A/F be unramified over F and π a prime of F which is therefore also a prime of S. Let σ be an automorphism of F or order one or two and $\bar{\sigma}$ the induced automorphism of $\bar{F}$. Let $\bar{\tau}$ be an involution of $\bar{A}$ which extends $\bar{\sigma}$. Then $\bar{\tau}$ lifts to an involution τ of A extending σ. If $\eta = 1$ then τ is orthogonal if and only if $\bar{\tau}$ is orthogonal. All choices of τ are isomorphic.*

Proof. Set $B' = A \otimes_{F,\sigma} A$ and $B = B'^{\mu}$ where $\mu(x \otimes y) = y \otimes x$. Then involutions of A correspond to minimal right ideals of B which are generated by idempotents. Since idempotents lift over complete dvrs we have that involutions lift. If τ and τ' are two lifts then $\tau' = u\tau u^{-1}$ where u is τ fixed. Since π is central, we can assume $u \in S^*$. Adjusting u by an element of f we can assume $u \in 1 + \pi S$. By the above lemma $u = v\tau(v)$ and this shows τ and τ' are isomorphic. □

We can begin giving detailed descriptions of involutions of the second kind. The first case is when v is τ ramified.

Proposition 8.20. *Suppose D/F and v are as above and D/F has an involution, τ, of the second kind. Set $F' = F^{\tau}$. Finally assume v is τ ramified. Then D/F is unramified and has order 2. $D \cong D' \otimes F^{\tau}F$ for D' of order two. If η is the restriction of τ to F, then τ is isomorphic to $\sigma \otimes \eta$ where σ is an involution on D' of the first kind.*

Proof. First of all since the above theorem says corestriction of F/F^{τ} is the identity on ramification, it follows that D/F is unramified. Since $\bar{D}$ has center $\bar{F} = \bar{F}'$ there is a division algebra D'/F' which maps to $\bar{D}$. It follows that $D = D' \otimes_{F'} F$. Now $\bar{D} = S/\pi S$ has center $\bar{F}$ and where π is a prime of F and $\tau(\pi) = -\pi$. τ induces an involution $\bar{\tau}$ which is of the first kind since τ acts trivially on $\bar{F}$. Thus $\bar{D}$ and hence D' has order 2 in the Brauer group. If η is the restriction of τ to F, then $1 \otimes \eta$ is an automorphism of D extending η. Let σ be an involution of the first kind on D' lifting $\bar{\tau}$ and $\sigma \otimes \eta$ is another involution of the second kind that also lifts $\bar{\tau}$. We saw above they must be isomorphic. □

The above corollary is a pretty complete description of involutions of the second kind where F/F^{τ} is ramified. To deal with the other case we need to work more, and particularly to understand ramification better. We begin with a technical result describing how τ and Π interact.

Lemma 8.21. *Suppose F is a field complete with respect to a discrete valuation v and D/F is a division algebra. Let τ be an involution of any kind on D which must preserve the valuation on F.Then there is a choice of Π such that $\tau(\Pi) = \pm\Pi$.*

Assume that $D \neq F$ and that for all choices is of Π as above we have $\tau(\Pi) = -\Pi$. Then the following further properties hold. First, that $\bar{D}$ is commutative, the ramification field of D has degree 2, and D is quaternion. Moreover, if τ is of the first kind, τ is symplectic. Finally, if τ is of the second kind, $D = D' \otimes_{F^{\tau}} F$ and τ has the form $\tau' \otimes \eta$ where τ' is symplectic and η is the restriction of τ to F. In addition, F/F^{τ} is unramified.

Proof. Let η be the automorphism of $\bar{D}$ induced by conjugation by Π. Now it is obvious that $\tau(\Pi) = u\Pi$ where $u \in S^*$. If $1 + u \notin \Pi S$, then $\Pi + \tau(\Pi)$ is a uniformizer and τ-symmetric. Thus we assume $1 + u \in \Pi S$ for all such u. All choices of Π have the form $s\Pi$ where $s \in S^*$. Thus if no choice of Π is τ symmetric, we must have $s\Pi + u\Pi\tau(s) \in S\Pi$ for all $s \in S^*$. That is, for all $\bar{s} \in \bar{D}$,

$$\bar{s} = \eta(\tau(\bar{s})), \quad \forall \bar{s} \in \bar{D}.$$

This is impossible unless $\bar{D} = \bar{L}$ is commutative and η has order 2. In particular, $\bar{L}/\bar{F}$ has degree 2 and so D has degree 2. Let $\bar{y} \in \bar{L}$ be such that $\tau(\bar{y}) = -\bar{y}$. If $y' \in S^*$ is a preimage of y, then $y = (1/2)(y' - \tau(y'))$ also maps to $\bar{y}$ and $\tau(y) = -y$. It follows that $L = F(y) \subset D$ is a maximal subfield, is unramified, and has residue field $\bar{L}$. Moreover $a = y^2 \in F$. Also, $\Pi^2 = s\pi$ where $s \in S^*$ and π is a prime in F. If $z \in D^*$ is such that $zyz^{-1} = -y$, write $z = s'\Pi^r$ for $s' \in S^*$. Since conjugation by z is nontrivial on $\bar{L}$, r must be odd. Altering z by a power of π, we can assume $z = s'\Pi$ which we can can rename as Π. Since y and

Π must generate D, $\Pi^2 \in F^*$ and we rename Π^2 as π. Altogether, $D = (a, \pi)$ is generated by y and Π such that $y^2 = a$, $\Pi^2 = \pi$, $y\Pi = -\Pi y$, and $\tau(y) = -y$. It follows that $\tau(\Pi) = u\Pi$ where $u \in L^*$. Furthermore,

$$\Pi = \tau^2(\Pi) = \tau(u\Pi) = u\Pi\sigma(u) = u^2\Pi,$$

and so $u = \pm 1$.

If τ is of the first kind, and $\tau(\Pi) = -\Pi$, then τ is symplectic by definition.

If τ is of the second kind, let μ be the symplectic involution. Then $\mu\tau$ is an automorphism which is the identity on $D' = F^\tau(\alpha, \Pi)$ and clearly $D = D' \otimes_{F^\tau} F$. If F/F^τ were ramified, the uniformizer in F would have the same valuation as Π (since $F^\tau(\Pi)/F^\tau$ has degree 2), a contradiction. □

Note that in the case $D = (a, \pi)$ it can be the case that $\tau(\Pi) = \Pi$ is never true.

Once again, let η be the automorphism induced on $\bar{D}$ by conjugation by Π. Using the above lemma we have

$$\tau(\Pi u \Pi^{-1}) = \Pi^{-1} u \Pi$$

and so $\tau\eta = \eta^{-1}\tau$ on $\bar{D}$.

We return to studying D/F with involution τ of the second kind and complete F, v where v is τ unramified and D/F is ramified.

Definition 8.22. Suppose τ is an automorphism of F of order 2, i.e., F/F^τ has degree 2, and L/F is any cyclic extension. We define

$$\tau L = L \otimes_\tau F,$$

where the τ in the subscript says that F is viewed as a twisted F-module via τ. If $\tau L \cong L$ over F, this implies that τ on F extends to L and we use the same symbol τ for a choice of this extension. Let σ be a generator of the Galois group of L/F. If $\tau(L) \cong L$ and $\tau\sigma = \sigma^{-1}\tau$ we say that L/F is **dihedral**.

As before let $\bar{D}$ have center $\bar{L}$ and recall that we can assume $L \subset D$. If E is the centralizer of L in D then $\bar{E} = \bar{D}$. Note that if σ is the restriction of τ to L, the above relationship shows that $\bar{L}/\bar{F}^\tau$ is dihedral (note that the Klein four group is called "dihedral" here). It follows that L/F^τ is dihedral.

Given a τ as above, there is an induced $\bar{\tau}$ on $\bar{D}/\bar{L}$ and then a lifted τ' on E/L where E is the centralizer of L. We also denote by τ' an extension of τ' to D. Note that all extensions have the same induced $\bar{\tau}'$ on $\bar{D}$. We have $\tau = u\tau' u^{-1}$ for a τ' fixed u. Write $u = v\Pi^r$ where $v \in S^*$. Since $\bar{\tau}$ and $\bar{\tau}'$ are equal to σ on $\bar{L}$, we have that e divides r. Write $\Pi^e = w\pi$ where π is a prime of F^σ. After adjusting by a power of π, we can assume $u \in S^*$. Since $\bar{\tau} = \bar{\tau}'$, it follows that u maps to $\bar{u} \in \bar{L}$ and $\bar{u}$ is clearly $\bar{\tau}'$ fixed. Lift $\bar{u}$ to $y \in L^{\tau'}$ and write $u = u'y$. Then $u' \in 1 + \Pi S$ and set $\tau'' = y\tau' y^{-1}$. Note that τ'' is another choice of extension from E, and that u' is τ'' fixed. By the above lemma, $u' = v\tau''(v)$. We have shown:

Lemma 8.23. *Suppose τ is an involution of the second kind on D and F/F^τ is unramified. Let $L \subset D$ be a lift of the ramification field with centralizer E so $\bar{E} = \bar{D}$. Let τ' be an involution on E lifting $\bar{\tau}$. Then there is an extension of τ' to D which is isomorphic to τ. In particular, there is another list of $\bar{L}$ to D which is preserved by τ.*

Next we fix such a τ and assume $L \subset D$ is preserved by τ as above. Again let E be the centralizer of L which is therefore also preserved by τ. We saw above that there is a prime Π such that $\tau(\Pi) = \Pi$ and a possibly different Π' such that $\Pi' E \Pi'^{-1} = E$. Let $T \subset E$ be the maximal order. Since E/L and L/F^τ are unramified, T has maximal ideal πT where π is a prime of F^τ. Now Π and Π' induce different automorphisms, $\bar{\eta}$ and $\bar{\eta}'$ on $\bar{D} = \bar{E}$ but both extend the unique $\bar{\tau}$ on $\bar{L}$. Thus $\bar{\eta}(x) = \bar{u}\bar{\eta}'(x)\bar{u}^{-1}$ for $\bar{u} \in \bar{E}^*$. Now $\bar{u}$ has a preimage $u \in E^*$ and changing Π' to $u\Pi'$ we can assume $\bar{\eta} = \bar{\eta}'$. In particular, $\bar{\tau}\bar{\eta}'\bar{\tau} = \bar{\eta}'^{-1}$ or $(\bar{\eta}'\bar{\tau})^2 = 1$.

Write $\tau(\Pi') = d\Pi'$ and note that changing Π' to $s\Pi'$ for $s \in E^*$ changes d to $d\eta'\tau(s)s^{-1}$. Also, we have $dEd^{-1} = E$ and $d \in S^*$. Let η' be the automorphism of E induced by Π'. Then $\tau^2(\Pi') = \tau(d\Pi) = d\Pi\tau(d) = d\eta'\tau(d)\Pi'$ and so $d\eta'\tau(d) = 1$. For any $s \in S^*$, $s\Pi' = \tau^2(s\Pi') = \tau(d\Pi'\tau(s)) = \tau(d\eta'\tau(s)\Pi') = d\Pi'\tau\eta'\tau(s)\tau(d) = d\eta'\tau\eta'\tau(s)\eta'(\tau(d))\Pi' = d(\eta'\tau)^2(s)d^{-1}\Pi'$ and so $(\eta'\tau)^2(s) = d^{-1}sd$ for all $s \in S^*$.

Since $(\bar{\eta}'\bar{\tau})^2 = 1$ we have that $\bar{d} \in \bar{L}^*$. Since $\bar{d}x\bar{d}^{-1} = x$ for all $x \in \bar{L}$, we have that d commutes with L. Thus $d \in T^* = S^* \cap E$. Also, $\bar{d}\bar{\eta}\bar{\tau}(\bar{d}) = 1$ so $\bar{d} = \bar{\eta}\bar{\tau}(\bar{v})(\bar{v})^{-1}$ for $\bar{v} \in \bar{L}$. Lift $\bar{v}$ to $v \in L^* \cap T^*$ and replace Π' by $v^{-1}\Pi'$. We calculate that now $\bar{d} = 1$.

We define $d_i, s_i \in T^*$ and primes Π_i as follows. Set $d_1 = d, s_1 = 1, \Pi_1 = \Pi'$. Assume $d_i \in 1 + \pi^i T$ are defined such that $\tau(\Pi_i) = d_i\Pi_i$ and $\Pi_E\Pi_i^{-1} = E$. Let η_i be the automorphism of E defined by Π_i. Note that $(\eta_i\tau)^2$ induces the identity on $\bar{E}$ and $d_i\tau_i\eta(d_i) = 1$. Write $d_i = 1 + t_i\pi^i$ and compute that $d_i\eta_i\tau(d_i) \in 1 + (t_i + \eta_i\tau(t_i))\pi^i + \pi^{i+1}T$ which implies that $t_i = -\eta_i\tau(t_i)$ modulo π. Since $\eta_i\tau$ has order 2 modulo π, we can write $t_i = \eta_i\tau(t) - t$ and set $s = 1 - t\pi^i$. If $\Pi_{i+1} = s\Pi_i$ then $\tau(\Pi_{i+1}) = d_{i+1}\Pi_{i+1}$ where $d_{i+1} = d_i\eta_i\tau(s)s^{-1} = 1 + (t_i - \eta_i(t) + t)\pi^i + z\pi^{i+1}$ for some $z \in T$ or $d_{i+1} = 1 + t_{i+1}\pi^{i+1}$ for some t_{i+1}. Having defined all the Π_i we can take the limit, call it Π and note that $\tau(\Pi) = \Pi$ and $\Pi E \Pi^{-1} = E$. If Π induces η on D then $\tau\eta = \eta^{-1}\tau$.

Theorem 8.24. *Let D/F be a division algebra over a complete field F, v and let τ be an involution of the second kind such that F/F^τ is unramified. Then there is a subfield $L \subset D$ such that $\bar{L}/\bar{F}\sigma$ is the ramification of D, $\tau(L) = L$. Let $E \subset D$ be the centralizer of L so E/L is unramified. There is a choice of prime Π of D such that $\tau(\Pi) = \Pi$ and Π induces an automorphism η in E such that $\tau\eta\tau = \eta^{-1}$. All of this defines the extension of τ from E to $D = \Delta(E/L, \eta, \Pi^e)$ viewed as a generalized cyclic algebra.*

Without the benefit of the completion, there is at least a little we can say in the split case.

Proposition 8.25. *Suppose $(D/F, \tau)$ is an algebra with involution of the second kind, and v is a valuation on F. Let $\bar{L}/\bar{F}$ be the ramification field of D. Suppose v is split with respect to τ. Then $\bar{L}/\bar{F} = \bar{L}/\bar{F}^{\tau}$ is also the ramification field at $\tau(v)$.*

Proof. Let w be the restriction of the valuation v to F^{τ}. For clarity, let σ be the restriction of τ to F, an automorphism of order 2. We know that v and $\sigma(v)$ are the two distinct extensions of w to F. Let F_w be the completion of F^{σ} at w. Since the natural inclusion ${F^{\tau}}_w \subset F_v$ is surjective, $F \otimes_{F^{\sigma}} F_w = F_w \oplus F_w$. The two induced maps $F \to F_w$ are the two completions (The fields F_v and $F_{\sigma(v)}$ can be identified as F_w-algebras, but these completion maps are different). Moreover, $\sigma \otimes 1$ switches the two fields in the direct sum, and so $(\sigma \otimes 1)(\alpha, \beta) = (\beta, \alpha)$. Then $D \otimes_{F^{\sigma}} F_w \cong D_v \oplus D_{\sigma(v)}$. Looking at $\tau \otimes 1$ as an involution, we have that $D_v \cong D^{\circ}_{\sigma(v)}$ over F_w. It follows that the ramification of D_v and $D_{\sigma(v)}$ are inverse to each other, so the ramifications fields over $\bar{F}_v = \bar{F}_{\sigma(v)} = \bar{F}_w$ are the same. □

We will also need a lemma relating the τ-invariant subfields of $\bar{D}$ and D.

Lemma 8.26. *Let F be a field complete with respect to a discrete valuation v and $(D/F, \tau)$ a division algebra with involution such that τ preserves v. Let L_D be the ramification field of D. There is a 1:1 correspondence between the τ-invariant maximal subfields of $\bar{D}$ and the unramified τ-invariant maximal subfields of D all of which contain a copy of L_D.*

Proof. If $L \subset D$ is maximal, unramified, and τ-invariant then $\bar{L} \subset \bar{D}$ is also maximal and obviously τ-invariant. Conversely, suppose $\bar{L} \subset \bar{D}$ is maximal, separable, and τ-invariant. Let n be the degree of D/F and $e = [L_D : F]$ the ramification index. By Lemma 8.7 there is an $\bar{x} \in \bar{L}$ such that $\bar{L} = \bar{F}(\bar{x})$ and $\tau(\bar{x}) = \pm\bar{x}$. If $(D/F, \tau)$ is of the first kind, the characteristic of $\bar{F}$ is not 2, and there is a preimage $x \in D$ such that $\tau(x) = \pm x$. Set $L = F(x)$ and let $L' \subset L$ be the maximal intermediate field unramified over F. Then L' contains L_D and $\bar{L}' \supseteq \bar{F}(\bar{x})$ so $[\bar{L}' : F] = [\bar{L}' : L_D]e = (n/e)e = n$ implying that $L' = L$ and $\bar{L}' = \bar{L}$. □

We need to consider involutions of the first kind.

Proposition 8.27. *Suppose $(D/F, \tau)$ is a division algebra with involution of the first kind and F is complete with respect to a valuation v. Then τ induces an involution on $\bar{D}$. Let L_D be the ramification field which has degree at most 2 over F. If L_D/F has degree 2, let η generate its Galois group.*

(a) *If D/F is unramified then $(\bar{D}, \tau)$ is of the same type as (D, τ).*
(b) *Otherwise, τ restricts to the identity or η on $\bar{L}_D$, and τ is of the first or second kind respectively. Both possibilities always occur for any given D.*

Proof. This is mostly obvious. Note that if $\tau(\Pi) = \pm\Pi$, then $x \to \Pi\tau(x)\Pi^{-1}$ has the other possible behavior on L_D. □

Suppose $(A/F, \tau)$ and $(B/F, \sigma)$ are csa's with compatible involutions. Assume that v is a discrete valuation on F with completion F_v. Except when τ, σ are of the second kind and split, they induce involutions τ, σ on $A_v = A \otimes_F F_v$ and

$B_v = B \otimes_F F_v$. If τ, σ are of the second kind and split, let w be the restriction of v, and hence of $v' = \sigma(v) = \tau(v)$, to F^τ, let F_w be the completion of F^τ at w, and write $A \otimes_{F^\tau} F_w \cong A_v \oplus A_{v'}$; similarly for B.

Proposition 8.28. *Suppose $A/F, \tau$ and $B/F, \sigma$ are central simple algebras with compatible involutions. Let v be a discrete valuation on F. Assume that A/F and B/F have the same degree, and $(A/F, \tau) \leq (B/F, \sigma)$.*

(a) *If τ, σ are not of the second kind or not split with respect to v, then $(A_v, \tau) \leq (B_v, \sigma)$.*
(b) *If τ, σ are of the second kind and split with respect to v, then $A_v \leq B_v$ and $A_{v'} \leq B_{v'}$ where $v' = \tau(v)$.*

A similar result holds if we just assume that $(A, \tau) \leq B$.

Proof. This argument closely follows that of Proposition 4.7. The two parts are also similar, with b) a bit more unusual so we will do only that one explicitly. Recall that $A \otimes_{F^\tau} F_v \cong A_v \oplus A_{\tau(v)}$ and $A_{\tau(v)} \cong A_v^\circ$. Let $L_v \subset A_v$ be an étale maximal subalgebra. Then $L_v = F_v(a')$. Consider $(a', a') \in A_v \oplus A_{\tau(v)}$, which makes sense. Clearly (a', a') is $\tau \otimes 1$-symmetric. Note that $A^\tau \otimes_{F^\tau} F_v$ is the τ-symmetric subspace of $A_v \oplus A_{\tau(v)}$. Thus there is an $a \in A^\tau$ which is as close as we need to a'. We form $F(a) = L$ which is τ-invariant and use Krasner's lemma to assure that $L \otimes_F F_v \cong L_v$. Since $L \subset B$ is σ-invariant by assumption, $L_v \subset B_v$ as needed.□

8.2. An involutory version of the Fein–Schacher Theorem

To pass from cda's to cda's with involution, we need to generalize [9].

Lemma 8.29. *Suppose D/F is a quaternion algebra with involution τ.*

(a) *Then D is generated by α, β with $\alpha\beta + \beta\alpha = 0$, α^2, $\beta^2 \in F$, $\tau(\alpha) = \pm\alpha$ and $\tau(\beta) = \pm\beta$.*
(b) *Suppose further that all τ-invariant maximal subfields are isomorphic. Then α, β from a) can also be assumed to satisfy $\alpha^2 = -1 = \beta^2$. Moreover, F is Pythagorean.*

Proof. (a) This is well known. If τ is symplectic all maximal subfields are τ-invariant. If τ is orthogonal, it is well known that there are anti-commuting elements α and β with $\tau(\alpha) = \alpha$ and $\tau(\beta) = -\beta$, so assume that τ is of the second kind. Let σ be the symplectic involution. Then $\tau\sigma\tau$ is also an involution. If $\tau\sigma\tau(x) = x$ then $\sigma(\tau(x)) = \tau(x)$, implying $\tau(x) \in F$, and $x \in F$. Thus $\tau\sigma\tau$ is also symplectic (which is unique), so $\tau\sigma\tau = \sigma$, i.e., $\tau\sigma = \sigma\tau$.

Of course $\sigma\tau$ is an automorphism extending an automorphism on F, and so the fixed ring is a division ring D'/L, with involution induced by σ, where F/L is quadratic with automorphism τ. Thus there are σ-antisymmetric α, β which anti-commute and are $\sigma\tau$ fixed. That is, $\tau(\alpha) = \sigma(\alpha) = -\alpha$ and $\tau(\beta) = \sigma(\beta) = -\beta$. This proves a).

(b) Note that $\alpha^2 = a$ and $\beta^2 = b$ are τ fixed. Furthermore, $(\alpha\beta)^2 = -ab$ with $\tau(\alpha\beta) = \pm\alpha\beta$. By assumption, $a = c^2 b$, and so $ab = -c^2 b^2$. Thus $\gamma = (\alpha\beta)/(bc)$

satisfies $\tau(\gamma) = \pm\gamma$ and $\gamma^2 = -1$. Again by assumption, the fields $F(\alpha)$, $F(\beta)$ are both isomorphic to $F(\sqrt{-1})$. If τ is of the first kind, then $F(\alpha)$ contains $i = \sqrt{-1}$ and it is clear that $\tau(i) = \pm i$. Of course the same is true for $F(\beta)$. If τ is of the second kind, then we saw above that we may assume that $\tau(\alpha) = -\alpha$ and we know that $\alpha^2 = -a^2$ for $a \in F$. Clearly a^2 is τ-fixed, so $\tau(a) = \pm a$ and $\tau(\frac{\alpha}{a}) = \mp a$.

As for the last point, suppose $a, b \in F$ and consider $\gamma = a\alpha + b\alpha\beta$ where we may assume that $\tau(\beta) = -\beta$. Then $\tau(\gamma) = \pm\gamma$ and $\gamma^2 = -a^2 - b^2$ which must have the form $-c^2$. □

Lemma 8.30. *Suppose D/F is a division algebra of degree n, with an involution τ, such that every maximal τ-invariant subfield contains a copy of the cyclic field extension L/F of prime degree p.*

(a) *Assume that $\tau(L) \cong L$ over F. (This is the case when τ is of the first kind.) If $F \subset L \subset K \subset D$ and K is a τ-invariant field, then $\tau(L) = L$.*
(b) *Assume that τ is of the second kind, and $\tau(L)$ is not isomorphic to L. Then $L \otimes \tau(L)$ contains a cyclic field extension L'/F such that $(\tau \otimes \tau)(L') = L'$, $\tau L' \cong L'$ (see* Definition 8.22*), and L'/F^τ is dihedral. Let K be a maximal subfield which is τ-invariant. Then K contains a isomorphic copy of L' as well.*
(c) *Suppose $K \subset D$ is a non-maximal τ-invariant subfield which commutes with but does not contain $L \subset D$. Then K does not contain another copy of L.*
(d) *Suppose $K \subset D$ is a non-maximal subfield not containing L. Then the centralizer D^K has the property that every maximal subfield contains a copy of KL/K. If K is τ-invariant, then every τ-invariant maximal subfield of D contains a copy of KL/K.*

Proof. (a) Since $\tau(L) \otimes_F L$ has zero divisors, no field contains it, implying $\tau(L) = L$. A similar observation proves (c).
(b) If $\tau(L)$ and L are not isomorphic then $L \otimes_F \tau L$ is a field Galois over F^τ with group the wreath product $(\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. The existence of L' is immediate. Any τ-invariant maximal subfield K contains a copy of $\tau(L) \otimes_F L$, and thus L'.
(d) Let K' be a maximal subfield of D^K, τ-invariant when required. Then K' is a maximal subfield of D and contains a copy of L. Moreover $K \neq KL \subset K'$ as needed. □

Given the above, we will always assume that $\tau(L) \cong L$.

Definition 8.31. Suppose that τ is an involution on D. We say that D/F is τ-**varied** if there is no nontrivial cyclic extension K/F contained isomorphically in every maximal (with respect to being τ-fixed) τ-fixed subfield of D/F.

F is τ-**varied** if every central division algebra of odd degree > 2 over F is τ-varied.

This concept is relevant because of the following result.

Proposition 8.32. *Every csa A of degree n with an involution τ of the second kind has arbitrarily many subfields with disjoint Galois closures, whose Galois groups over F are all the symmetric group S_n.*

Proof. By [20, section 2], the maximal étale τ-invariant subalgebras of A correspond to the maximal tori of the corresponding (special) unitary group G. On the other hand, a simpler form of this result can be obtained directly from Hilbert's Irreducibility Theorem, so that over a finitely generated field there are always generic tori. Thus A always contains a maximal subfield E which is τ-invariant and such that the Galois group of its Galois closure over F is S_n. In fact, one can find an arbitrarily large number of such tori that their Galois closures are disjoint over F. See [20] for further details. □

Corollary 8.33. *Every finitely generated field is τ-varied.*

Proof. The group S_n of the Galois closure of such a maximal subfield cannot have a nontrivial normal subgroup of odd degree. □

We would like to prove that if D has degree p, then it is impossible that some nontrivial τ-invariant F-subfield L' of D is isomorphic to $F[b]$. Then L contains some $b' = aba^{-1}$, i.e., $b'a = ab$. But then applying τ yields $\tau(a)b' = b\tau(a)$, so $\tau(a)a$ centralizes b, i.e., $\tau(a)a \in F[b]$. Conversely, if $\tau(a)a = d \in F[b]$ then $b' = aba^{-1}$ is τ-symmetric since

$$\tau(b') = \tau(a)^{-1}b\tau(a) = ad^{-1}bda^{-1} = ad^{-1}dba^{-1} = aba^{-1} = b'.$$

So does any τ-invariant F-subfield contain aba^{-1} where $\tau(a)a \in F[b]$? This could lead to a generic counterexample, where we show that the generic τ-symmetric element does not have this form.

Another way of obtaining τ-symmetric elements is simply to take $b+\alpha b'$ where $\alpha \in F_0$. But so far neither of these approaches tends to work.

As before, $\mathbb{H}$ denotes $(-1,-1)_F$.

Proposition 8.34. *Again, suppose that D/F is a cda of degree $n = p^t$, with an involution τ. Assume that L is a cyclic extension of F, which is noncyclic over F^τ in case τ is of second kind, and every maximal (with respect to being τ-fixed) τ-fixed subfield of D/F contains a copy of L.*

Then $p = 2$, $L = F(\sqrt{-1})$, and $D = D' \otimes_F \mathbb{H}$ for some cda D'.

Proof. First we prove that $p = 2$. Of course $p = 2$ if τ is of the first kind, so we assume that τ is of the second kind, and let $F_0 = F^\tau$ and $L_0 = L^\tau$. Then L/F_0 is Galois, with group generated by σ and τ. Write $L_0 = F_0[b]$, where $b^p \in F$. then $L = F[b]$.

Let $u \in D$ satisfy $uLu^{-1} = L$ but u does not commute with the elements of L. Let σ be the automorphism of L/F defined by u, so $u\ell u^{-1} = \sigma(\ell)$, implying $\tau\sigma(\tau(\ell)) = \tau(u)^{-1}\tau^2(\ell)\tau(u) = \tau(u)^{-1}\ell\tau(u)$. If τ is of the first kind, τ restricts to an an element of the cyclic Galois group of L/F, and $\tau\sigma\tau = \sigma$.

$\tau\sigma\tau$ fixes F and thus is a power of σ^k of σ. Now

$$\sigma = \tau(\tau\sigma\tau)\tau = \sigma^{k^2},$$

implying $k \cong \pm 1 \pmod p$. Thus either τ commutes with σ or together they generate a dihedral group.

For any $a \in L$,

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

which is $\sigma(a)$ in the dihedral case and $\sigma^{-1}(a)$ if τ commutes with σ. In the dihedral case, $d = \tau(u)u$ induces σ^2 on L, so we may replace u by $\tau(u)u$ and assume that $u^\tau = u$.

Thus we have proved the claim that $p = 2$.

By a parallel induction, D has a τ-invariant subfield of codegree 2 not containing L, which we call K'. Consider the centralizer $D^{K'}$. By Lemma 8.29 we have $D^{K'} = (-1, -1)_{K'}$. Let $\alpha, \beta \in D^{K'}$ be as in Lemma 8.29(b). Then α, β generate, over F, a τ-invariant subalgebra of D isomorphic to $\mathbb{H}$. Thus $D = D' \otimes_F \mathbb{H}$.

We still need to show that L has the required form. We know that $LK'/K' = K'(\sqrt{-1})$. Write $L = F(\sqrt{a})$. We are done if $-a$ is a square in F. Assume not. We know that $-a$ is a square in K'; that is, K' contains $F(\sqrt{-a})$. Note that this argument applies to any τ-invariant K' of codegree 2. In particular any τ-invariant maximal subfield of D' contains $F(\sqrt{-a})$ and by induction this equals $F(\sqrt{-1})$, a contradiction since $D' \otimes_F \mathbb{H}$ is a division algebra. □

Remark 8.35. We have not been able to handle the case where L is cyclic over F^τ and τ is of second kind, although we suspect that it also holds since one can construct an assortment of τ-fixed subfields of D/F. The difficulty is showing that one does not contain a copy of L.

For convenience, we assumed above that L/F had prime degree. This case turns out to be sufficient because of the following very familiar result, whose proof we include for convenience.

Lemma 8.36. *Suppose $F(\sqrt{-1})/F$ is nontrivial. Then there is no cyclic field extension L/F of degree 4 containing $F(\sqrt{-1})$.*

Proof. Set $i = \sqrt{-1}$. Suppose L/F exists and η generates its Galois group. Then $L = F(i)(\sqrt{a+bi})$ where $a, b \in F$ and $\eta(\sqrt{a+bi}) = \sqrt{a+bi}\,\beta$ for $\beta = c+di \in F(i)$. Then $\eta^2(\sqrt{a+bi}) = \sqrt{a+bi}\,\beta\eta(\beta)$ and so $\beta\eta(\beta) = -1$, implying $c^2 + d^2 = -1$ since η is conjugation on $F(i)$. Squaring both sides yields

$$a - bi = (a+bi)(c^2 + d^2 + 2cdi) = (a+bi)(-1+2cdi),$$

implying $(-1)^2 - 4c^2d^2 = 1$, or $cd = 0$. But then $(a-bi) = (-1)(a+bi)$, yielding $a = 0$. If $d = 0$ then $c^2 = 1$ contradicting the nontriviality of $F(i)/F$. Hence, $c = 0$ and $d = \pm 1$ and $\beta = \pm i$. But $\eta(\pm i)(\pm i) = -i(i) = 1$ a contradiction. □

In the involutory case there are many situations where we can prove that D' of Proposition 8.34 must be trivial. We begin with an easy lemma.

Lemma 8.37. *Suppose (D, τ) is a division algebra with involution of the first kind. Then D has a τ-invariant subfield of codegree 2.*

Proof. By induction it suffices to show that when D has degree larger than 2, D has a nonmaximal noncentral τ-invariant subfield. If τ is symplectic, any symmetric element generates a nonmaximal subfield. If τ is orthogonal, let $u \in D$ be a skew element and we are done unless for all such u, u^2 is central. Of course in this case $F(u)$ itself will do. □

Proposition 8.38. *Suppose $D = D' \otimes_F \mathbb{H}$ has an involution of first kind, with respect to which $\mathbb{H}$ is τ-invariant, and every maximal subfield of D contains $F(\sqrt{-1})$. Then $D' = F$.*

Proof. By the above lemma we may assume that D' has degree 2, and so $D' = (a, b)$ is quaternion. Let α β be as in Lemma 4. Then αi and βj commute and generate the maximal invariant subfield $F(\sqrt{-a}, \sqrt{-b})$. Since this is assumed to contain $\sqrt{-1}$, we have that a is a square, b is a square, or ab is a square. The first two violate that D' is a division algebra, and in the third case $D' = (a, b) = (a, -ab) = (a, -1)$ which violates that $D' \otimes (-1, -1)$ is a division algebra. □

We have proved:

Theorem 8.39. *Suppose $(D/F, \tau)$, is a τ-varied division algebra with involution. Let L/F be a cyclic prime degree field extension such that L/F^τ is not cyclic when τ is of the second kind. Then there is a τ-invariant maximal separable subfield $K \subset D$ such that K/F does not contain a copy of L/F, unless $L = F(\sqrt{-1})$, $D = \mathbb{H} \otimes_F D'$, and F is a Pythagorean field. If τ is of the first kind, then $D = \mathbb{H}$.*

We obtain the exceptional case by means of [10]:

Example 8.40. Suppose λ is a commuting indeterminate over a field F containing a primitive n-th root ε of 1. Then for any $a \in F$, the symbol algebra (a, λ) (given by $\alpha^n = a$, $\beta^n = \lambda$, and $\alpha\beta = \varepsilon\beta\alpha$) has involution of the second kind, given by $\alpha^\tau = \alpha$, $\beta^\tau = \beta^{-1}$, and $(\alpha\beta)^\tau = \beta^\tau\alpha^\tau = \beta^{-1}\alpha$. Indeed, we only have to show that τ is an anti-homomorphism, since obviously it has order 2. But applying τ to the relation $\alpha\beta = \varepsilon\beta\alpha$ gives

$$(\beta\alpha)^\tau = \varepsilon^{-1}(\alpha\beta)^\tau = \varepsilon^{-1}\beta^{-1}\alpha = \alpha\beta^{-1} = \alpha^\tau\beta^\tau,$$

as desired.

Now take the fields $F \subset K$ as in [10], and taking $E = F(t)$ in their notation $(t = \lambda)$, we see that their symbol algebra A has an involution of the second kind over the fixed field E^τ where $\tau(t) = t$, and thus their algebra $D = \mathbb{H} \otimes_E A$ has an involution obtained by taking the tensor product over E.

8.3. Main result

The following is the involutory analog of Corollary 4.18.

Theorem 8.41. *Suppose $(A/F, \tau)$ is a csa with an involution, and $(A/F, \tau) \leq B/F$. We assume that B also has an involution of the same kind. Also assume that F has a valuation v and L_A, L_B are the respective ramification fields, with L_B not cyclic over F^τ in case τ is of second kind. Then $L_B \subseteq L_A(\sqrt{-1})$.*

Proof. If τ is split with respect to v, then by Proposition 8.28, $A_v \leq B_v$ and the result follows from Corollary 4.18.

Suppose then that τ preserves v. By Proposition 8.28 we may assume that F is complete with respect to v. Let D be the underlying division algebra of A, so $L_A = L_D$. Assume first that D/F is nontrivial or τ is not symplectic. Then there are a complete set of orthogonal idempotents $e_1, \ldots, e_n$ such that the e_i are τ-symmetric and the involution τ_i induced by τ on $D = e_i A e_i$ is compatible to τ. If $L_i \subset D$ is maximal separable and τ_i-invariant, then $L = L_1 e_1 \oplus \ldots \oplus L_n e_n$ is τ-maximal étale in A and hence splits B. Note that this implies that all the L_i split B. If $L \subset D$ is an unramified maximal τ_1-invariant subfield, then L appears in a τ-maximal étale $K \subset A$ and therefore L splits B. Since L/F is unramified, $L \supset L_B$. By Lemma 8.26 $\bar{L}_A \bar{L}_B$ is contained in every maximal subfield of $\bar{D}$.

If τ is of the second kind, then L_B/F is dihedral and it follows that $L_B L_A / L_A$ is dihedral. If τ is of the first kind, then L_A/F and L_B/F have degree at most 2. If τ_1 acts nontrivially on $\bar{L}_A$, then $\bar{L}_B \bar{L}_A$ is dihedral over L_A^{τ}. By Theorem 8.39, $L_B L_A \subset L_A(\sqrt{-1})$. □

The above result is unsatisfying, in the sense that we would like to remove the assumption that the involutions are of the same kind and the non-cyclicity of L_B over F^{τ}. To do so, one may have to resolve Remark 8.35. From Proposition 8.34 we have:

Proposition 8.42. *In the above theorem, if L_B is not contained in L_A, then $\bar{L}_A$ is Pythagorean and $\bar{D} = D' \otimes_{\bar{L}_A} \mathbb{H}$. If τ is of the first kind, then $\bar{D}/\bar{L}_A = \mathbb{H}/\bar{L}_A$.*

Proof. The first statement is clear. To prove the second, we must prove that D' has a maximal subfield of codegree 2. Even though τ on $\bar{D}$ could be of the second kind, acting nontrivially on $\bar{L}_A$, it is certainly still true that $\bar{D}$ has order 2 in the Brauer group. □

References

[1] Alexander, W.K.N., Jürgen, S.: Cohomology of Number Fields, volume 323. Springer-Verlag, Berlin, ISBN = 978-3-540-37888-4,. Grundlehren der Mathematischen Wissenschaften, (Second ed.) (2008)

[2] Adrian Albert, A.: Involutorial algebras and real riemann matrices. Ann. Math. **36**, 886–964 (1935)

[3] Caenepeel, S.: Brauer Groups, Hopf Algebras and Galois Theory. *K*-Monographs in Mathematics, vol. 4. Kluwer Academic Publishers, Dordrecht (1998)

[4] Chernousov, V.I., Rapinchuk, A.S., Rapinchuk, I.A.: On the genus of a division algebra. C. R. Math. Acad. Sci. Paris **350**(17–18), 807–812 (2012)

[5] Chernousov, V.I., Rapinchuk, A.S., Rapinchuk, I.A.: The genus of a division algebra and the unramified brauer group. Bull. Math. Sci. **3**(2), 211–240 (2013)

[6] Chernousov, V.I., Rapinchuk, A.S., Rapinchuk, I.A.: On the size of the genus of a division algebra. Proc. Steklov Inst. Math. **292**(1), 63–93 (2016)

[7] Chernousov, V.I., Rapinchuk, A.S., Rapinchuk, I.A.: The finiteness of the genus of a finite dimensional division algebra, and some generalizations. Israel J. Math. **236**, 747–799 (2020)

[8] DeMeyer, F., Ingraham, E.: Separable Algebras over Commutative Rings. Springer-Verlag, Berlin (1971)

[9] Fein, B., Schacher, M.: The ordinary quaternions over a Pythagorean field. Proc. Am. Math. Soc. **60**(16–18), 1976 (1977)

[10] Fein, B., Schacher, M., Wadsworth, A.: Division rings and the square root of –1. J. Algebra **65**(2), 340–346 (1980)

[11] Garibaldi, S., Saltman, D.J.: Quaternion algebras with the same subfields. In: Quadratic Forms, Linear Algebraic Groups, and Cohomology, volume 18 of Dev. Math., pp. 225–238. Springer, New York, (2010)

[12] Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer-Verlag, New York (1977)

[13] Herstein, I.: Noncommutative Rings. Mathematical Association of America, Providence, R.I., Carus Mathematical Monographs 15 (1968)

[14] Jacob, B., Wadsworth, A.: Division algebras over Henselian fields. J. Algebra **128**(1), 126–179 (1990)

[15] Krashen, D., McKinnie, K.: Distinguishing division algebras by finite splitting fields. Manuscr. Math. **134**, 171–182 (2011)

[16] Meyer, J.S.: Division algebras with infinite genus. Bull. Lond. Math. Soc. **46**(3), 463–468 (2014)

[17] Merkurjev, A.S., Tignol, J.-P.: The multipliers of similitudes and the brauer group of homogeneous varieties. J. Reine Angew. Math. **461**, 13–47 (1995)

[18] Pierce, R.S.: Associative Algebras. Studies in the History of Modern Science, vol. 9. Springer-Verlag, New York (1982)

[19] Raynaud, M.: Anneaux locaux henséliens. Lecture Notes in Mathematics, vol. 169. Springer-Verlag, Berlin-New York (1970)

[20] Prasad, G., Rapinchuk, A.: Irreducible tori in semisimple groups. Int. Math. Res. Not. **461**, 1229–1242 (2001)

[21] Riehm, C.: The corestriction of algebraic structures. Invent. Math. **11**, 73–98 (1970)

[22] Rowen, L.H.: Graduate Algebra: A noncommutative view, volume 91. American Mathematical Society, Providence, RI. Graduate Studies in Mathematics (2008)

[23] Rapinchuk, A.S., Rapinchuk, I.A.: On division algebras having the same maximal subfields. Manuscr. Math. **132**(3–4), 273–293 (2010)

[24] Rapinchuk, A., Rapinchuk, I.: Some finiteness results for algebraic groups and unramifiedcohomology over higher-dimensional fields. (3), 463–468 (2020)

[25] Saltman, D.J.: The Schur index and Moody's theorem. K-Theory **7**(4), 309–332 (1993)

[26] Saltman, D.J.: Lectures on division algebras. Published by American Mathematical Society, Providence, RI (1999)

[27] Saltman, D.J.: Lectures on division algebras. CBMS Regional Conference Series in Mathematics, vol. 94. Published by American Mathematical Society, Providence, RI (1999)

[28] Serre, J-P.: *Local fields*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg

[29] Schofield, A., Van den Bergh, M.: The index of a Brauer class on a Brauer-Severi variety. Trans. Am. Math. Soc. **333**(2), 729–739 (1992)

[30] Tikhonov, S.V.: Division algebras of prime degree with infinite genus. Proc. Steklov Inst. Math. **292**(1), 256–259 (2016)

[31] Tignol, J.-P., Wadsworth, A.R.: Totally ramified valuations on finite-dimensional division algebras. Trans. Am. Math. Soc. **302**(1), 223–250 (1987)

[32] Wadsworth, A.: Valuation theory on finite dimensional division algebras. In: Valuation Theory and Its Applications, vol. I., volume 32 of Fields Inst Commun, pp. 385–449. Amer. Math. Soc., Providence, RI (2002)