JOURNAL OF ALGEBRA 133, 404–423 (1990)

Minimal Embeddings of Central Simple Algebras

BURTON FEIN*

Department of Mathematics, Oregon State University, Corvallis, Oregon 97331

DAVID J. SALTMAN†

Department of Mathematics, University of Texas at Austin, Austin, Texas 78712

AND

MURRAY SCHACHER‡

Department of Mathematics, University of California at Los Angeles, Los Angeles, California 90024

Communicated by Susan Montgomery

Received October 13, 1988

IN MEMORY OF I. N. HERSTEIN, A TEACHER, COLLABORATOR, AND FRIEND

1. INTRODUCTION

Let L be a finite algebraic extension of a field K and let A be a finite-dimensional simple algebra with center L. The theory developed in this paper arises from the following question: what are the "minimal" finite-dimensional simple algebras with center K in which A is embeddable?

Before clarifying what we mean by "minimal" in the above context we introduce some terminology. We say that A/L is central simple if A is a central simple algebra finite-dimensional over its center L; if A is a division ring we refer to A as an L-division ring. If A/L is central simple and L/K is a finite-dimensional extension of fields, we say that A/L is embeddable in a central simple B/K if there exists a K-algebra monomorphism φ from A into B such that $\varphi(1_A) = 1_B$; if φ exists we usually identify A with its image

* Research supported by NSF Grant DMS-8800687.
† Research supported by NSF Grant DMS-8601279.
‡ Research supported by NSF Grant DMS-8801051.

0021-8693/90 $3.00

in B. We shall show in Section 2 that there is no loss of generality in assuming that out embeddings preserve identities. That A/L is actually embeddable in some central simple B/K is clear; the left regular representation, for example, embeds A/L in $M_u(K)/K$, where $u=[A:K]$.

The most natural notions of minimality in our context are those of degree minimality and matrix size minimality. Let B/K be central simple. Then $B \cong M_t(D)$, where D is a K-division ring. We refer to D as the skew field component of B. The index, $\mathrm{ind}(B)$, of B equals $\sqrt{[D:K]}$. The degree, $\deg(B)$, of B, equals $\sqrt{[B:K]}$; we have $\deg(B)=t\cdot \mathrm{ind}(B)$. We refer to t as the *matrix size* of B.

DEFINITION. Let L/K be a finite-dimensional extension of fields and let A/L be central simple. We define $d_K(A)$ by:

$$d_K(A)=\min\{\deg(B) \mid B/K \text{ is a central simple } K\text{-algebra and } A \text{ embeds in } B/K\}.$$

Similarly, $ms_K(A)$ is defined by:

$$ms_K(A)=\min\{t \mid A/L \text{ embeds in a central simple } K\text{-algebra of matrix size } t\}.$$

If A/L embeds in a central simple B/K and $\deg(B)=d_K(A)$ (resp. the matrix size of B equals $ms_K(A)$), we say that B/K is degree minimal for A/L (resp. matrix size minimal for A/L).

It is an easy consequence of the Double Centralizer Theorem (see Section 2) that the minimum value possible for $d_K(A)$ is $\deg(A)\cdot[L:K]$. Although A/L is always embeddable in some central simple B/K, there need not exist any such B/K of this minimum possible degree. This is the case even when K and L are number fields. It is instructive to compare this situation with some of the results in the literature concerning embeddings in division rings. Suppose, for simplicity, that A is an L-division ring and K and L are number fields. If A is embeddable in a K-division ring D, then, as above, the minimal possible degree of D is $\deg(A)\cdot[L:K]$. Examples exist of L-division rings A which are not embeddable in any K-division ring; if, however, an L-division ring A is embeddable in some K-division ring then A is embeddable in a K-division ring of minimal possible degree $\deg(A)\cdot[L:K]$ [3, Theorem 1]. This is in marked contrast with the situation for embeddings in central simple algebras.

Throughout this paper L/K will be a finite extension of fields and A/L will be central simple. We denote the class of A/L in the Brauer group, $B(L)$, of L by $[A]$. The order of $[A]$ in $B(L)$ is denoted $\exp(A)$. We say that L is *stable* if $\text{ind}(A) = \exp(A)$ for every central simple A/L. Examples of stable fields are the global and local fields of class field theory. (By a global field we mean either an algebraic number field or an algebraic function field in one variable over a finite constant field.) We let A^{op} be the opposite algebra of A; $[A] + [A^{\text{op}}] = [L]$. The p-primary component of $B(L)$ is denoted $B(L)_p$ and the maximal divisible subgroup of $B(L)$ is denoted $DB(L)$. The restriction map from $B(K)$ to $B(L)$ is denoted $\text{Res}_{L/K}$; here $\text{Res}_{L/K}([B]) = [B \otimes_K L]$. The relative Brauer group, $B(L/K)$, is the kernel of this restriction map.

If n is a positive integer and p is a prime, we let n_p denote the p-part of n; $n = n_p n'$, where $(n_p, n') = 1$. Now suppose G is a group and $\alpha \in G$ has order $n = n_p n'$. Then α is uniquely expressible as a product $\alpha = \alpha_p \cdot \alpha'$ of two commuting elements of G where α_p, the *p-component* of α, has order a power of p and α', the *p-regular* component of α, has order prime to p. If $1 = un_p + vn'$, then $\alpha_p = \alpha^{vn'}$ and $\alpha' = \alpha^{un_p}$. If A/L is central simple, then $A \cong \bigotimes_p A_p$, where the tensor products are taken over L and over all primes p and where $\deg(A_p)$ is a power of p [4, p. 256]. We have $[A_p] = [A]_p$. We will say that a numerical invariant μ of central simple L-algebras *localizes* if $\mu(A)_p = \mu(A_p)$. Finally, we point out one easy fact that we will use repeatedly in what follows. Suppose φ is a homomorphism from a group H to G and $\alpha \in \varphi(H)$. Since both α_p and α' are powers of α, both α_p and $\alpha' \in \varphi(H)$. In particular, if $[A] \in \text{Res}_{L/K}(B(K))$, then $[A_p] \in \text{Res}_{L/K}(B(K))$ and $[A'] \in \text{Res}_{L/K}(B(K))$.

We begin our discussion of the invariants $d_K(A)$ and $ms_K(A)$ in Section 2 by reducing to the case when A is an L-division ring. More precisely, if $A \cong M_n(\Delta)$, we show that $d_K(A) = n \cdot d_K(\Delta)$ and $ms_K(A) = n \cdot ms_K(\Delta)$. The next step in our discussion is to reduce to the case when $\text{ind}(A)$ is a prime power. Since neither $d_K(A)$ nor $ms_K(A)$ localize, we need to introduce some additional invariants of A/L. Suppose A/L embeds in a central simple B/K. Let Y be the centralizer of A in $C_B(L)$, the centralizer of L in B. Then $\deg(B) = \deg(A) \cdot \deg(Y) \cdot [L:K]$ and $[A] + [Y] \in \text{Res}_{L/K}(B(K))$. Thus B/K will be degree minimal for A/L provided $\deg(Y)$ is as small as possible. Since we may reduce easily to the case when Y is an L-division ring, we are led to consider the following invariant of A/L:

DEFINITION. Let L/K be a finite extension of fields and let A/L be central simple. $r_K(A)$ is defined to be the minimum index of an L-division ring Y such that $[A] + [Y] \in \text{Res}_{L/K}(B(K))$.

We show in Section 2 that $r_K(A)$ localizes and that $d_K(A) = [L:K] \cdot \deg(A) \cdot r_K(A)$; this localizes the computation of $d_K(A)$. The localization of the computation of $ms_K(A)$ is more subtle and will be discussed in Section 2. For arbitrary fields K and L we are also able to show that if A/L

embeds in a central simple B/K, then $d_K(A)$ divides $\deg(B)$ and $ms_K(A)$ divides the matrix size of B.

We are able to say more in Section 3 where we assume that K and L are stable fields. In particular, we show that there exists a B/K which is both matrix size minimal and degree minimal for A/L. This permits us to obtain more precise information regarding the relationship between $d_K(A)$, $ms_K(A)$, and $r_K(A)$ in this situation.

Although the invariant $r_K(A)$ of A/L succeeds in localizing the computation of $d_K(A)$, it is not a particularly natural invariant to consider. $r_K(A)$ is, however, closely related to a much more natural and more easily computed invariant of A/L, the order of $[A]$ modulo the image of the restriction map; we denote this order by $\exp_K(A)$. We also define $k_K(A)$ to be the maximum index of a K-division ring D such that $\mathrm{Res}_{L/K}[D] = \exp_K(A)[A]$. We show in Section 3 that if K and L are stable and $B(K)_p$ is divisible for all primes dividing $\mathrm{ind}(A)$, then $d_K(A) = [L: K] \cdot \deg(A) \cdot \exp_K(A)$, and $ms_K(A) = [L: K] \cdot \deg(A)/k_K(A)$. Finally, in Section 4 we provide an example which illustrates the computation of the invariants that we have introduced and which also shows that the formulas for $d_K(A)$ and $ms_K(A)$ are not, in general, valid if $B(K)_p$ is not divisible for some prime p dividing $\mathrm{ind}(A)$.

2. Arbitrary Fields

In this section we will obtain results about embedding questions which are valid for arbitrary fields. We will maintain the following context.

Context. Throughout this section L/K is a finite extension of fields and A/L is central simple.

We begin by justifying our assertion that no generality is lost by requiring that our embeddings preserve identity elements.

Proposition 1. *Let the context be as above and suppose that φ is a K-algebra monomorphism of A/L into $B = M_n(D)$, where D/K is central simple. Suppose $\varphi(1_A) \neq 1_B$. Then there exists $r < n$ such that A/L is embeddable in $M_r(D)$.*

Proof. Let $e = \varphi(1_A)$. Then $e = e_1 + e_2 + \cdots + e_r$, where the $\{e_i\}$ are a set of primitive orthogonal idempotents of B. Then $e_i B e_i \cong D$ so $\varphi(A) = e\varphi(A)e \subset eBe \cong M_r(D)$. We note that $r < n$ since $e \neq 1_B$. Since e is the identity of eBe, it follows that φ is an embedding of A/L into $M_r(D)/K$. ∎

Our next result will allow us, when convenient, to restrict our attention to L-division rings.

PROPOSITION 2. *Let the context be as above and suppose that* $A \cong M_n(\Delta)$, *where* Δ/L *is central simple. Let* A/L *be embeddable in* $M_m(D)$, D *a K-division ring. Then* $n \mid m$ *and* Δ *is embeddable in* $M_k(D)$, *where* $m = nk$.

Proof. Let φ be an embedding of A into $B = M_m(D)$ and let $e_i = \varphi(e_{ii})$, where e_{ii} is the $n \times n$ matrix having a 1 in the (i, i) position and 0's elsewhere. Since $\varphi(1_A) = 1_B$, $1_B = e_1 + e_2 + \cdots + e_n$. Since e_i is an idempotent in B, $e_i B e_i \cong M_{u_i}(D)$, where e_i is a sum of u_i primitive orthogonal idempotents in B. Since e_{ii} and e_{jj} have the same Jordan form in $M_n(L)$, there is an invertible $w \in B$ such that $w e_i w^{-1} = e_j$. It follows that $e_i B e_i \cong e_j B e_j$ and so $u_i = u_j$. Let $k = u_i$. Then $m = nk$. Also, $\Delta \cong e_{11} A e_{11}$ and $\varphi(e_{11} A e_{11}) \subset e_1 B e_1 \cong M_k(D)$. Since e_{11} is the identity of $e_{11} A e_{11}$ and $\varphi(e_{11}) = e_1$ is the identity of $e_1 B e_1$, it follows that Δ is embeddable in $M_k(D)$. ∎

COROLLARY 3. *Let the context be as above and suppose that* $A \cong M_n(\Delta)$, n *a positive integer. Then* $d_K(A) = n \cdot d_K(\Delta)$ *and* $ms_K(A) = n \cdot ms_K(\Delta)$.

Proof. Let A be embeddable in $B = M_m(D)$, where $\deg(B) = d_K(A)$. Then $n \cdot d_K(\Delta) \leqslant d_K(A)$ by Proposition 2. If Δ is embeddable in a central simple K-algebra B' with $\deg(B') = d_K(\Delta)$, then A is embeddable in $M_n(B')$ so $d_K(A) = n \cdot d_K(\Delta)$. Thus $n \cdot d_K(\Delta) = d_K(A)$ and similarly $n \cdot ms_K(\Delta) = ms_K(A)$. ∎

Recall that we denote the centralizer in B of a subalgebra E by $C_B(E)$. Our next result collects some standard results about the centralizer of a simple subalgebra of B/K.

PROPOSITION 4. *Let the context be as above and suppose that* A/L *embeds in a central simple* B/K. *Let* Y *be the centralizer of* A *in* $C_B(L)$. *Then*:

(a) Y/L *is central simple such that* $C_B(L) \cong A \otimes_L Y$

(b) $B \otimes_K L \cong M_r(C_B(L))$, *where* $r = [L : K]$

(c) $\deg(B) = \deg(A) \cdot \deg(Y) \cdot [L : K]$ *and* $[A] + [Y] \in \mathrm{Res}_{L/K}(B(K))$

(d) $\deg(A) \cdot [L : K] \leqslant d_K(A) \leqslant \deg(A) \cdot \deg(Y) \cdot [L : K]$.

Proof. This is immediate from [4, p. 94–96]. ∎

Our next result shows that the minimum possible value for $d_K(A)$ is attained precisely when $[A] \in \mathrm{Res}_{L/K}(B(K))$.

PROPOSITION 5. *Let the context be as above. Then* $d_K(A) = \deg(A) \cdot [L : K]$ *if and only if* $[A] \in \mathrm{Res}_{L/K}(B(K))$. *Moreover, if* $[A] = [D \otimes_K L]$, D *a*

K-division ring, then there is an integer w such that A/L is embeddable in $B = M_w(D)$ so that $A = C_B(L)$ and $\deg(B) = \deg(A)[Lw\ K] = d_K(A)$.

Proof. Suppose first that $d_K(A) = \deg(A) \cdot [L: K]$ and let A/L be embedded in B/K, where $\deg(B) = d_K(A)$. By Proposition 4(c), $A = C_B(L)$ and $[A] \in \mathrm{Res}_{L/K}(B(K))$. Conversely, suppose $[A] = [D \otimes_K L]$, D a K-division ring. Taking matrices over D if necessary, we may assume that L is a subfield of $E = M_v(D)$. By Proposition 4 (with $A = L$), $[C_E(L)] = [\mathrm{Res}_{L/K}([D])] = [A]$. Thus $M_s(A) \cong M_t(C_E(L))$ for integers s and t. Let $F = M_t(E)$. Since $M_t(C_E(L)) \cong C_F(L)$, we have $M_s(A) \cong C_F(L)$. We identify $M_s(A)$ with $C_F(L)$. Since $M_s(K)$ is a K-subalgebra of $M_s(A)$, $M_s(K) \subset F$. Let B be the centralizer of $M_s(K)$ in F. Then $L \subset B$ because L centralizes $M_s(K)$. $C_B(L)$ consists of all $\alpha \in F$ which commute with all elements of $L \cdot M_s(K)$. Under our identifications, $C_B(L)$ consists of all $\alpha \in M_s(A)$ which commute with all elements of $M_s(K)$. It follows that $A \cong C_B(L)$ and so A/L embeds in B. By Proposition 4, $\deg(B) = \deg(A)[L: K]$. Finally, by [4, pp. 94–96], $F \cong M_s(K) \otimes_K B$ so $[B] = [D]$. ∎

Recall that in Section 1 we defined $r_K(A)$ to be the minimum index of an L-division ring Y such that $[A] + [Y] \in \mathrm{Res}_{L/K}(B(K))$. Our next result establishes the basic relationship between $d_K(A)$ and $r_K(A)$.

THEOREM 6. *Let L/K be a finite extension of fields and let A/L be central simple. Then $d_K(A) = [L: K] \cdot \deg(A) \cdot r_K(A)$.*

Proof. Let Y be an L-division ring such that $\mathrm{ind}(Y) = r_K(A)$ and $[A \otimes_L Y] = [A] + [Y] \in \mathrm{Res}_{L/K}(B(K))$. By Proposition 5, there is a central simple B/K in which $A \otimes_L Y$ embeds such that $\deg(B) = [L: K] \cdot \deg(A) \cdot \mathrm{ind}(Y)$. Thus $d_K(A) \leqslant [L: K] \cdot \deg(A) \cdot r_K(A)$. By Proposition 4(c), $d_K(A) \geqslant [L: K] \cdot \deg(A) \cdot r_K(A)$, which establishes the result. ∎

We record a consequence of Theorem 6 for future reference.

COROLLARY 7. *Let the context be as above and let Y be an L-division ring of index $r_K(A)$ such that $[A] + [Y] = [D \otimes_K L]$, D a K-division ring. Let $A \otimes_L Y$ be embeddable in $B = M_w(D)$ so that $A \otimes_L Y \cong C_B(L)$. Then* $\deg(B) = d_K(A)$.

Proof. The existence of w and B follows from Proposition 5 applied to $A \otimes_L Y$. By Proposition 4, (c), (c), $\deg(B) = \deg(A) \cdot \deg(Y) \cdot [L: K]$. The result now follows from Theorem 6. ∎

We next show that $r_K(A)$ localizes.

PROPOSITION 8. *Let the context be as above. Then $(r_K(A))_p = r_K(A_p)$.*

Proof. Let U be an L-division ring such that $[A_p]+[U]\in \mathrm{Res}_{L/K}(B(K))$ and $\mathrm{ind}(U)=r_K(A_p)$. Then $[A_p]+[U_p]=([A_p]+[U])_p\in \mathrm{Res}_{L/K}(B(K))$ so $U=U_p$. Thus $r_K(A_p)$ is a power of p. Now let Y be an L-division ring such that $\mathrm{ind}(Y)=r_K(A)$ and $[A]+[Y]\in \mathrm{Res}_{L/K}(B(K))$. Since $[A_p]+[Y_p]\in \mathrm{Res}_{L/K}(B(K))$ we have $(r_K(A))_p\geqslant r_K(A_p)$. Since $[A']+[Y']\in \mathrm{Res}_{L/K}(B(K))$ and $[A_p]+[U]\in \mathrm{Res}_{L/K}(B(K))$, we have $[A]+[U\otimes_L Y']\in \mathrm{Res}_{L/K}(B(K))$. By definition of $r_K(A)$ we have $r_K(A_p)\geqslant (r_K(A))_p$. Thus $(r_K(A))_p=r_K(A_p)$. ∎

As mentioned previously, $d_K(A)$ does not localize. Since $r_K(A)$ localizes, however, we are able to obtain a simple relationship between $d_K(A)$ and the various $d_K(A_p)$.

COROLLARY 9. *Let the context be as above. Then:*

$$d_K(A)=[L\colon K]\cdot\prod_p \frac{d_K(A_p)}{[L\colon K]}.$$

Proof. By Theorem 6 and Proposition 8,

$$\prod_p \frac{d_K(A_p)}{[L\colon K]}=\prod_p \deg(A_p)\cdot r_K(A_p)=\deg(A)\cdot r_K(A)=\frac{d_K(A)}{[L\colon K]}.\quad ∎$$

We note two further consequences of Proposition 8.

COROLLARY 10. *Let the context be as above and let Y be an L-division ring such that $[A]+[Y]\in \mathrm{Res}_{L/K}(B(K))$. Then $r_K(A)$ divides* $\mathrm{ind}(Y)$.

Proof. For each prime p, $[A_p]+[Y_p]\in \mathrm{Res}_{L/K}(B(K))$, and so it follows that $\mathrm{ind}(Y_p)\geqslant r_K(A_p)=(r_K(A))_p$. ∎

COROLLARY 11. *Let the context be as above. Then $r_K(A)$ divides* $\mathrm{ind}(A)$.

Proof. Let Y be the division ring component of $[A^{op}]$. Since $[A]+[A^{op}]=[L]$, Corollary 10 implies that $r_K(A)$ divides $\mathrm{ind}(Y)=\mathrm{ind}(A)$. ∎

We finally have enough to prove that the degree of a degree minimal central simple algebra for A/L divides the degree of any central simple B/K in which A/L is embeddable.

THEOREM 12. *Let L/K be a finite extension of fields and let A/L be central simple. If A/L embeds in a central simple B/K, then $d_K(A)$ divides* $\deg(B)$.

Proof. Let A embed in a central simple B/K. Let Y/L be central simple such that $C_B(L) \cong A \otimes_L Y$. By Proposition 4(c), $\deg(B) = \deg(A) \cdot \deg(Y) \cdot [L: K]$. The result now follows from Theorem 6 and Corollary 10. ∎

We turn our attention next to $ms_K(A)$. We begin with a preliminary result.

LEMMA 13. *Let the context be as above and let p be an arbitrary prime. Let $\mathfrak{M}_p$ be the set of rational numbers of the form* $\mathrm{ind}(Y_p)/\mathrm{ind}(D_p)$ *where Y_p is an L-division ring of p-power index, D_p is a K-division ring of p-power index, and $[A_p] + [Y_p] = [D_p \otimes_K L]$. Then $\mathfrak{M}_p$ has a minimum element.*

Proof. Suppose Y_p is an L-division ring of p-power index, D_p is a K-division ring of p-power index, and $[A_p] + [Y_p] = [D_p \otimes_K L]$. By Proposition 5 there is an integer $w(p)$ such that $A_p \otimes_L Y_p$ embeds in $M_{w(p)}(D_p)$ with $w(p) \cdot \mathrm{ind}(D_p) = [L: K] \cdot \deg(A_p) \cdot \mathrm{ind}(Y_p)$. Thus each element of $\mathfrak{M}_p$ becomes an integer when multiplied by $[L: K] \cdot \deg(A_p)$ so $\mathfrak{M}_p$ has a minimal element. ∎

Lemma 13 enables us to introduce the following invariant of A/L which by its very definition localizes.

DEFINITION. *Let L/K be a finite dimensional extension of fields and let A/L be central simple. For each prime p let $\mathfrak{M}_p$ be defined as in Lemma* 13. *We define $v_K(A_p)$ to be the minimum element of $\mathfrak{M}_p$ and we set $v_K(A) = \prod_p v_K(A_p)$.*

It should be noted that $v_K(A_p)$ is not, in general, trivial if p does not divide $\mathrm{ind}(A)$. For such p, the value of $v_K(A_p)$ depends on the structure of the relative Brauer group $B(L/K)$. Since our next result shows that $v_K(A)$ is related to $ms_K(A)$ in the same way that $r_K(A)$ is related to $d_K(A)$, this explains why $ms_K(A)$ is a subtler invariant than $d_K(A)$.

THEOREM 14. *Let L/K be a finite extension of fields and let A/L be central simple. Then $ms_K(A) = [L: K] \cdot \deg(A) \cdot v_K(A)$.*

Proof. We show first that $ms_K(A) \leq [L: K] \cdot \deg(A) \cdot \prod_p v_K(A_p)$. For each prime p choose Y_p an L-division ring of p-power index and D_p a K-division ring of p-power index such that $[A_p] + [Y_p] = [D_p \otimes_K L]$ and $v_K(A_p) = \mathrm{ind}(Y_p)/\mathrm{ind}(D_p)$. Let $Y = \bigotimes_p Y_p$ and $D = \bigotimes_p D_p$, the tensor products being taken over L and K, respectively. Then $[A] + [Y] = [D \otimes_K L]$ so by Proposition 5 there is an integer u such that $A \otimes_L Y = C_B(L)$, where $B = M_u(D)$. By Proposition 4(c), $u = [L: K] \cdot \deg(A) \cdot \prod_p v_K(A_p)$. Thus

$$ms_K(A) \leq [L: K] \cdot \deg(A) \cdot \prod_p v_K(A_p).$$

Now let $t = ms_K(A)$ and suppose E is a K-division ring such that A/L is embeddable in $B = M_t(E)$. Let $A \otimes_L X = C_B(L)$. Suppose $X \cong M_r(U)$. Then $A \otimes_L X \cong M_r(A \otimes_L U)$. By Proposition 2, $ms_K(A) = kr$ and $A \otimes_L U$ is embeddable in $M_k(E)$. But then A/L is embeddable in $M_k(E)$ and so $r = 1$ by the minimality of $ms_K(A)$. By Proposition 4(c), we have

$$[L:K] \cdot \deg(A) \cdot \prod_p \operatorname{ind}(X_p)/\operatorname{ind}(E_p)) = ms_K(A)$$
$$\leqslant [L:K] \cdot \deg(A) \cdot \prod_p v_K(A_p).$$

But $[A_p] + [X_p] = [E_p \otimes_K L]$ so $(\operatorname{ind}(X_p)/\operatorname{ind}(E_p)) \geqslant v_K(A_p)$ for each prime p. It follows that $(\operatorname{ind}(X_p)/\operatorname{ind}(E_p)) = v_K(A_p)$ for each prime p and so $ms_K(A) = [L:K] \cdot \deg(A) \cdot v_K(A)$. ∎

Suppose B/K is matrix size minimal for A/L, where $[B] = [E]$, E a K-division ring. Let $A \otimes_L X = C_B(L)$. For future reference we note that the above proof shows that X is an L-division ring and $(\operatorname{ind}(X_p)/\operatorname{ind}(E_p)) = v_K(A_p)$ for every prime p. In particular, $\operatorname{ind}(X) = \operatorname{ind}(E) \cdot v_K(A)$.

Using Theorem 14 we obtain the analog of Corollary 9 for $ms_K(A)$.

COROLLARY 15. *Let the context be as above. Then:*

$$ms_K(A) = [L:K] \cdot \prod_p \frac{ms_K(A_p)}{[L:K]}.$$

Proof. By Theorem 14,

$$\prod_p \frac{ms_K(A_p)}{[L:K]} = \prod_p \deg(A_p) \cdot v_K(A_p) = \deg(A) \cdot v_K(A) = \frac{ms_K(Z)}{[L:K]}. \quad ∎$$

We next prove the analog of Theorem 12 for $ms_K(A)$.

THEOREM 16. *Let the context be as above. If A/L embeds in a central simple B/K, then $ms_K(A)$ divides the matrix size of B.*

Proof. Let $C_B(L) \cong A \otimes_L Y$, where Y/L is central simple. Let $B \cong M_w(D)$, where w is the matrix size of B. To show that $ms_K(A)$ divides w it is sufficient to show that $ms_K(A)$ divides w/k for some divisor k of w; thus by Proposition 2 we may assume that Y is an L-division ring. By Proposition 4, $w = [L:K] \cdot \deg(A) \cdot \prod_p(\operatorname{ind}(Y_p))/\operatorname{ind}(D_p))$. Since $[A_p] + [Y_p] = [D_p \otimes_K L]$, $v_K(A_p) \leqslant (\operatorname{ind}(Y_p)/\operatorname{ind}(D_p))$. It follows that $w/ms_K(A) = \prod_p ((\operatorname{ind}(Y_p)/\operatorname{ind}(D_p)) \cdot (v_K(A_p))^{-1}$ is an integer. ∎

3. Stable Fields

In this section we will refine the results of Section 2 under the assumption that K and L are stable fields. Recall that a field L is called stable if $\exp(A) = \operatorname{ind}(A)$ for every central simple A/L and that global and local fields are stable. We will adhere to the:

Context. Throughout this section L/K is a finite extension of stable fields and A/L is central simple.

Our main results for stable fields will follow by showing that there exists a B/K which is both matrix size minimal and degree minimal for A/L. The proof of this follows from an abelian group argument which we next proceed to isolate.

Let G and H be abelian groups (written additively) and let $\Phi: G \to H$ be a homomorphism such that the kernel, $\ker(\Phi)$, of Φ has bounded exponent. Let p be a fixed prime and let $\alpha, \beta \in H_p$ with $\alpha + \beta \in \Phi(G)$. Define $m_\alpha(\beta)$ to be the minimum of $\exp(\beta)/\exp(\delta)$, the minimum taken over all $\delta \in G_p$ such that $\Phi(\delta) = \alpha + \beta$. (We are denoting the order of β by $\exp(\beta)$.) We note that this minimum exists because of our assumption that $\ker(\Phi)$ has bounded exponent.

Lemma 17. *Let* $\alpha, \beta, \beta' \in H_p$ *with* $\alpha + \beta, \alpha + \beta' \in \Phi(G)$ *and* $\exp(\beta') > \exp(\beta)$. *Then*: $m_\alpha(\beta') \geqslant \min\{m_\alpha(\beta), m_\alpha(\beta + p(\beta' - \beta)), m_\alpha((p-1)^2 \beta - p(p-2)\beta')\}$. *In particular, there exists* $\gamma \in H_p$ *with* $\alpha + \gamma \in \Phi(G)$ *and with* $\exp(\gamma) < \exp(\beta')$ *such that* $m_\alpha(\beta') \geqslant m_\alpha(\gamma)$.

Proof. Let $\delta, \delta' \in G_p$ with $\Phi(\delta) = \alpha + \beta$, $\Phi(\delta') = \alpha + \beta'$, $m_\alpha(\beta) = \exp(\beta)/\exp(\delta)$, and $m_\alpha(\beta') = \exp(\beta')/\exp(\delta')$. If $\exp(\delta') \leqslant \exp(\delta)$ then clearly $m_\alpha(\beta') \geqslant m_\alpha(\beta)$. Suppose $\exp(\delta') > \exp(\delta)$. Let $\eta = \delta + p(\delta' - \delta)$ so $p(\exp(\eta) \leqslant \exp(\delta')$ and $\Phi(\eta) = \alpha + (\beta + p(\beta' - \beta))$. We note that $p \cdot \exp(\beta + p(\beta' - \beta)) \leqslant \exp(\beta')$. Suppose first that $p \cdot (\exp(\eta) = \exp(\delta')$. Then,

$$m_\alpha(\beta') = \frac{\exp(\beta')}{p \cdot \exp(\eta)} \geqslant \frac{\exp(\beta + p(\beta' - \beta))}{\exp(\eta)} \geqslant m_\alpha(\beta + p(\beta' - \beta)).$$

Finally, suppose that $p \cdot (\exp(\eta) < \exp(\delta')$. Then $p \cdot \exp(p\delta' - (p-1)\eta) = \exp(\delta')$. An easy computation shows that $\Phi(p\delta' - (p-1)\eta) = \alpha + (p-1)^2 \beta - p(p-2)\beta'$. Then,

$$m_\alpha((p-1)^2 \beta - p(p-2)\beta') \leqslant \frac{\exp((p-1)^2 \beta - p(p-2)\beta')}{\exp(p\delta' - (p-1)\eta)}$$

$$\leqslant \frac{\exp(\beta')}{\exp(\delta')} = m_\alpha(\beta'). \quad \blacksquare$$

THEOREM 18. *Let L/K be a finite extension of stable fields, and let A/L be central simple. Then there exists a central simple B/K such that*:

(a) *B/K is degree minimal for A/L,*

(b) *B/K is matrix size minimal for A/L, and*

(c) *$C_B(L) = A \otimes_L X$, where X is an L-division ring of index $r_K(A)$.*

Proof. Let $t = ms_K(A)$ and let $C \cong M_t(E)$ be matrix size minimal for A/L, where E is a K-division ring. Let $C_C(L) = A \otimes_L V$. It follows from the remark following Theorem 14 that V is an L-division ring and for each prime p, $v_K(A_p) = \text{ind}(V_p)/\text{ind}(E_p)$. Let p be an arbitrary prime. Let $G = B(K)$, $H = B(L)$, and let $\Phi = \text{Res}_{L/K}$. If $[D] \in \ker(\Phi)$, D a K-division ring, then L splits D, so $\exp(D)$ divides $[L:K]$. Thus $\ker(\Phi)$ has bounded exponent and so Lemma 17 applies in this situation. Suppose $\text{ind}(V_p) > r_K(A_p)$. Let $\alpha = [A_p]$, $\beta' = [V_p]$, and let $\beta = [Y_p]$, where Y is as in Corollary 7. Since K and L are stable, we have $\text{ind}(V_p) = \exp(V_p)$. By Lemma 17 there is a K-division ring W_p of p-power index and an L-division ring X_p of p-power index with $\exp(X_p) < \exp(V_p)$ such that $[A_p] + [X_p] = \Phi([W_p])$ and $v_K(A_p) \geqslant \exp(X_p)/\exp(W_p)$. By definition of $v_K(A_p)$ we must have $v_K(A_p) = \exp(X_p)/\exp(W_p)$. We also have $r_K(A_p) \leqslant \exp(X_p) < \exp(V_p)$. By repeated application of Lemma 17 we may assume that $\exp(X_p) = r_K(A_p)$. Let W (resp. X) be the K-division ring (resp. L-division ring) having p-primary component W_p (resp. X_p) for each prime p. Since $[A_p] + [X_p] = \Phi([W_p])$ for each prime p, $[A] + [X] = \Phi([W])$. By Proposition 8, $\text{ind}(X) = r_K(A)$. Let $A \otimes_L X$ be embeddable in $B = M_w(W)$ so that $A \otimes_L X \cong C_B(L)$. By Corollary 7, B/K is degree minimal for A/L. By Theorem 14, $ms_K(A) = [L:K] \cdot \deg(A) \cdot v_K(A)$. But

$$v_K(A) = \prod_p v_K(A_p) = \prod_p \exp(X_p)/\exp(W_p) = \deg(X)/\deg(W)$$

and so $ms_K(A) \cdot \deg(W) = [L:K] \cdot \deg(A) \cdot \deg(X)$. It follows from Proposition 4(c), that $ms_K(A) \cdot \deg(W) = \deg(B) = w \cdot \deg(W)$. Thus $w = ms_K(A)$ and so B/K is both degree minimal and matrix size minimal for A/L. ∎

It is not true, in general, that if B/K is degree minimal (resp. matrix size minimal) for A/L, then B/K is also matrix size minimal (resp. degree minimal) for A/L. Assume, for example, that p and q are distinct primes, K is a global field, and $[L:K] = q$. Let D_1 be a K-division ring of index p. By [1, Corollary 4] $B(L/K)$ is infinite. Let D_2 be a K-division ring such that $[D_2] \in B(L/K)$. Let $\Delta = D_1 \otimes_K L$. Then Δ is an L-division ring of index p. By Theorem 6, $d_K(\Delta) = pq$. Let $B = M_q(D_1)$. By Proposition 5, B/K is degree minimal for Δ. B/K is, however, not matrix size minimal for Δ, since Proposition 5 also shows that Δ embeds in the K-division ring

$D_1 \otimes_K D_2$. If r is a prime distinct from p and q and D_3 is a K-division ring of index r, then Δ embeds in the K-division ring $D_1 \otimes_K D_2 \otimes_K D_3$. Thus $D_1 \otimes_K D_2 \otimes_K D_3$ is matrix size minimal for Δ but it clearly is not degree minimal.

Using Theorem 18 we can read off the relationship between the main invariants of A/L that we have been considering.

COROLLARY 19. *Let L/K be a finite extension of stable fields and let A/L be central simple. Then $d_K(A) \cdot v_K(A) = ms_K(A) \cdot r_K(A)$.*

Proof. Let B/K be as in the statement of Theorem 18 and let $C_B(L) = A \otimes_L X$. Let E be the skew field component of B. Then $v_K(A) = \mathrm{ind}(X)/\mathrm{ind}(E)$ and $\deg(B) = d_K(A) = ms_K(A) \cdot \mathrm{ind}(E)$. Thus $d_K(A) \cdot v_K(A) = ms_K(A) \cdot r_K(A)$. ∎

With notation as in Theorem 18, we note that $v_K(A_p) = r_K(A_p)/\mathrm{ind}(D_p)$ for each prime p. Let us define $m_K(A_p)$ to be the maximum index of a K-division ring Δ_p of p-power index such that for some L-division ring V_p with $\mathrm{ind}(V_p) = r_K(A_p)$ we have $[A_p] + [V_p] = [\Delta_p \otimes_K L]$. If we then define $m_K(A)$ to be $\prod_p m_K(A_p)$, then $m_K(A) = \mathrm{ind}(D)$ and by Corollary 19 we have $ms_K(A) = d_K(A)/m_K(A)$. $m_K(A)$ is an answer to the following problem: it is the maximal degree of a K-division ring D so that $[A] + [Y] = [D \otimes_K L]$ and Y is an L-division ring of degree $r_K(A)$. We will, however, not be concerned with $m_K(A)$ in what follows.

The invariants $r_K(A)$ and $v_K(A)$ of A/L are useful for localizing the computation of $d_K(A)$ and $ms_K(A)$ for arbitrary fields L and K. Unfortunately, both $r_K(A)$ and $v_K(A)$ suffer from the defect that their definition involves considering central simple Y/L such that $[A] + [Y] \in \mathrm{Res}_{L/K}(B(K))$; this makes their computation difficult. We next introduce two additional invariants of A/L, $\exp_K(A)$ and $k_K(A)$. These new invariants are more natural and more readily computable than $r_K(A)$ and $v_K(A)$. While their exact relationship to $d_K(A)$ and $ms_K(A)$ is unclear for arbitrary fields, we are able to obtain simple expressions for $d_K(A)$ and $ms_K(A)$ in terms of $\exp_K(A)$ and $k_K(A)$ in many important cases.

DEFINITION. Let L/K be a finite dimensional extension of fields and let A/L be central simple. We define $\exp_K(A)$ to be the order of $[A] + \mathrm{Res}_{L/K}(B(K))$ in $B(L)/\mathrm{Res}_{L/K}(B(K))$ and $k_K(A)$ to be the maximum index of a K-division ring D such that $\mathrm{Res}_{L/K}([D]) = \exp_K(A)[A]$.

We note that $k_K(A)$ does not, in general, localize because of the possible existence of primes p not dividing $\mathrm{ind}(A)$ such that $B(L/K)_p \neq \{0\}$.

LEMMA 20. *Let the context be as above. Then*:

(a) *for each prime p*, $k_K(A_p)_p = k_K(A)_p$

(b) $\exp_K(A)$ *divides* $r_K(A)$

Proof. (a) Let Γ be a K-division ring of index $k_K(A)$ with $\mathrm{Res}_{L/K}([\Gamma]) = \exp_K(A)[A]$. Then $[\Gamma_p \otimes_K L] = \exp_K(A)[A_p]$. Let $\exp_K(A) = v \cdot \exp_K(A_p)$ and let $rv \equiv 1 \bmod \exp(A_p)$. Since $r[\Gamma_p \otimes_K L] = \exp_K(A_p)[A_p]$ and $r[\Gamma_p]$ has exponent $k_K(A)_p$, it follows that $k_K(A)_p \leqslant k_K(A_p)_p$. Now let Θ be a K-division ring of index $k_K(A_p)$ such that $[\Theta \otimes_K L] = \exp_K(A_p)[A_p]$. Then $[\Theta_p \otimes_K L] = \exp_K(A_p)[A_p]$ so $[(\Theta_p \otimes_K \prod_{q \neq p} \Gamma_q) \otimes_K L] = \exp_K(A)[A]$. It follows that $k_K(A_p)_p \leqslant k_K(A)_p$, proving (a). Now let B/L be as in the statement of Theorem 18 and let $C_B(L) \cong A \otimes_L X$. Then X is an L-division ring of index $r_K(A)$ such that $[A] + [X] \in \mathrm{Res}_{L/K}(B(K))$. Thus $r_K(A)[A] = r_K(A)[A] + r_K(A)[Y] \in \mathrm{Res}_{L/K}(B(K)$ so $\exp_K(A)$ divides $r_K(A)$. ∎

In order to obtain the desired expressions for $d_K(A)$ and $ms_K(A)$ in terms of $\exp_K(A)$ and $k_K(A)$ it will be necessary at a crucial point in the argument to take an appropriate root of an element of $B(K)$. Since $B(K)$ is not always divisible, this will not always be possible. It is, however, well known that if K is a global field then $2B(K)$ is always divisible; this follows easily, for example, from [4, (32.13)]. This motivates the somewhat technical condition in the next lemma.

LEMMA 21. *Let the context be as above. Let p be a prime and let* Γ_p *be a K-division ring of index* $k_K(A)_p$ *such that* $\mathrm{Res}_{L/K}([\Gamma_p]) = \exp_K(A_p)[A_p]$. *Let n be minimal such that there exists* $[\Delta] \in B(K)_p$ *satisfying* $p^n \cdot \exp_K(A)_p\, [A] = p^n[\Gamma]$. *Then there are integers u, r with* $0 \leqslant u, r \leqslant n$ *with*

$$d_K(A_p) = p^u \cdot [L\colon K] \cdot \deg(A)_p \cdot \exp_K(A)_p$$

$$ms_K(A_p) = p^r \cdot [L\colon K] \cdot \deg(A)_p / k_K(A)_p.$$

Proof. In view of Theorems 6 and 14 we need to show that there are integers u, r with $0 \leqslant u, r \leqslant n$ such that $r_K(A)_p = p^u \cdot \exp_K(A)_p$ and $v_K(A)_p = p^r / k_K(A)_p$. Let V be the L-division ring such that $[V] = [\Delta \otimes_K L] - [A_p]$. Since

$$p^n \cdot \exp_K(A)_p\, [V] = p^n \cdot \exp_K(A)_p\, [\Delta \otimes_K L] - p^n \cdot \exp_K(A)_p\, [A_p]$$

and

$$p^n \cdot \exp_K(A)_p\, [\Delta \otimes_K L] = p^n([\Gamma_p \otimes_K L] = p^n \cdot \exp_K(A)_p\, [A_p],$$

it follows that $\exp(V)$ divides $p^n \cdot \exp_K(A)_p$. But $[A_p] + [V] \in \mathrm{Res}_{L/K}(B(K)$ so $r_K(A)_p$ divides $\exp(V)$ by Corollary 10. Thus $\exp(V) = p^v \cdot \exp_K(A)_p$ for some $v \leqslant n$ and so by Lemma 20(b) $r_K(A)_p = p^u \cdot \exp_K(A)_p$ for some $u \leqslant v \leqslant n$.

By Proposition 5 there is an integer w such that $A_p \otimes_L V$ is embeddable in $M_w(\Delta)$ so that $w \cdot \exp(\Delta) = [L: K] \cdot \deg(A_p) \cdot \exp(V)$. Since $\exp(\Delta) = \exp_K(A)_p \cdot k_K(A)_p$ we have $w = p^v \cdot [L: K] \cdot \deg(A_p)/k_K(A)_p$. But $ms_K(A_p)$ divides w by Theorem 16, so $[L: K] \cdot \deg(A_p) \cdot v_K(A)_p$ divides $p^v \cdot [L: K] \cdot \deg(A_p)/k_K(A)_p$. Thus $k_K(A)_p \cdot v_K(A)_p \leqslant p^v$. It remains to show that $k_K(A)_p \cdot v_K(A)_p \geqslant 1$.

Let B/L be as in the statement of Theorem 18. Let D be the skew field component of B and let $C_B(L) \cong A \otimes_L Y$. By Theorem 18, Y is an L-division ring of index $r_K(A)$ and $\exp(D_p) = r_K(A_p)/v_K(A_p)$. We have

$$\exp_K(A)_p\, [D_p \otimes_K L] = \exp_K(A)_p\, [A_p] + \exp_K(A)_p\, [Y_p]. \tag{1}$$

Let $G = B(K)_p$, $H = B(L)_p$, and let $\Phi = \mathrm{Res}_{L/K}$. Let $\alpha = \exp_K(A)_p\, [A_p]$, $\beta = [L]$, and $\beta' = \exp_K(A)_p\, [Y_p]$. Since $r_K(A)_p = p^u \cdot \exp_K(A)_p$ for some $u \leqslant n$, we have $\exp(\beta') = p^u \geqslant 1$. If $u = 0$ then $r_K(A)_p = \exp_K(A)_p$. This implies that $\mathrm{Res}_{L/K}(\exp_K(A)_p\, [D_p]) = \exp_K(A)_p\, [A_p]$. By definition of $k_K(A)$, $k_K(A)_p \geqslant \exp(\exp_K(A)_p\, [D_p]) = 1/v_K(A)_p$. Thus $k_K(A)_p \cdot v_K(A)_p \geqslant 1$ and so we may assume that $u \geqslant 1$. We have

$$\exp_K(A_p)[A_p] + [L] = \mathrm{Res}_{L/K}([\Gamma_p]) \tag{2}$$

Now $\exp(\beta') > \exp(\beta)$ so Lemma 17 applies for (1) and (2). Note that in (2) we have $m_\alpha(\beta) = 1/k_K(A_p)$, and the choice of Γ_p makes this value minimal. Using (1), we have $m_\alpha(\beta') = v_K(A_p)$. Lemma 17 says $m_\alpha(\beta') \geqslant m_\alpha(u)$, where u has order strictly smaller than β'. Iterating this conclusion reduces us to the case $u = 0$. But (2) returns the minimal value among all $m_\alpha(0)$. Thus $v_K(A)_p \geqslant 1/k_K(A)_p$, so again, $v_K(A)_p\, k_K(A)_p \geqslant 1$, as desired. ∎

We record some consequences of Lemma 21 in the special case when various p-Sylow components of $B(L/K)$ are divisible. These conditions will hold over global fields for all odd p. The proofs are all immediate from Lemma 21.

COROLLARY 22. *Let L, K, A satisfy the hypotheses of this section, i.e., we are assuming that K and L are stable. If for some prime p dividing* $\exp(A)$ *we have* $B(K)_p$ *is divisible, then* $r_K(A_p) = \exp_K(A_p)$. *If* $B(K)_p$ *is divisible for all primes p dividing* $\exp(A)$ *then*

(1) $r_K(A) = \exp_K(A)$

(2) $d_K(A) = [L: K] \cdot \deg(A) \cdot \exp_K(A)$

(3) $ms_K(A) = [L: K] \cdot \deg(A)/k_K(A)$.

In case $B(K)_p$ is not divisible but $p^n B(K)_p$ is divisible, the conclusion of Lemma 21 is that the estimates of (2) and (3) of Corollary 22 are "off by at most p^n" for that local component.

We are finally able to give our main result relating $d_K(A)$ to $\exp_K(A)$ and $ms_K(A)$ to $k_K(A)$ when L/K is a finite extension of global fields. We will freely use the classification theory of central simple algebras over global fields by means of Hasse invariants; we refer the reader to [4, Section 32] for the relevant theory assumed. We denote the Hasse invariant of $[A]$ at a prime π of K by $\mathrm{inv}_\pi[A]$. Let $\mathrm{inv}_\pi[A] = s/m \in \mathbb{Q}/\mathbb{Z}$, where $(s, m) = 1$. Then m is called the *local index of A at π* and denoted by $\mathrm{l.i.}_\pi[A]$; $\mathrm{l.i.}_\pi[A] = \exp(A \otimes_K K_\pi)$, where K_π denotes the completion of K at π. We let ∞ denote the infinite prime of $\mathbb{Q}$.

THEOREM 23. *Let L/K be a finite extension of global fields and let A/L be central simple. Then $d_K(A) = [L\colon K] \cdot \deg(A) \cdot \exp_K(A)$ and $ms_K(A) = [L\colon K] \cdot \deg(A)/k_K(A)$ if any of the following conditions are satisfied*:

(1) *K has positive characteristic*

(2) $\mathrm{ind}(A)$ *is odd*

(3) $[L\colon K]$ *is odd*

(4) *K has no real embeddings*

(5) *L is totally real*

(6) $\exp_K(A)$ *is odd*

(7) *$B(L/K)_2$ is infinite.*

In any case, $d_K(A) = 2^u \cdot [L\colon K] \cdot \deg(A) \cdot \exp_K(A)$ and $ms_K(A) = 2^r \cdot [L\colon K] \cdot \deg(A)/k_K(A)$, where $0 \leqslant u, r \leqslant 1$.

Proof. Suppose Γ_p is a K-division ring of index $k_K(A)_p$ such that $\mathrm{Res}_{L/K}([\Gamma_p]) = \exp_K(A_p)[A_p]$. The crux of the matter in Lemma 21 is whether $[\Gamma_p]$ is in $DB(K)$. By [4, (32.12)], $[\Gamma_p] \in DB(K)$ unless $p = 2$ and K has a real infinite prime π such that $\mathrm{inv}_\pi[\Gamma_p] = \frac{1}{2}$. In particular, if $p \neq 2$ or if $p = 2$ and one of (1), (2), (4), or (6) hold, then by Lemma 21 we have $d_K(A_p) = [L\colon K] \cdot \deg(A)_p \cdot \exp_K(A)_p$ and $ms_K(A_p) = [L\colon K] \cdot \deg(A)_p/k_K(A)_p$. Since $d_K(A) = [L\colon K] \cdot \prod_p (d_K(A_p)/[L\colon K])$ and $ms_K(A) = [L\colon K] \cdot \prod_p (ms_K(A_p)/[L\colon K])$, we may assume that $p = 2$, A has index a power of 2, and none of conditions (1), (2), (4), or (6) hold. We set $\Gamma = \Gamma_2$. By the criterion mentioned above for $[\Gamma]$ to be in $DB(K)$, we may assume that K has a real infinite prime π such that $\mathrm{inv}_\pi[\Gamma] = \frac{1}{2}$. Since $\exp_K(A)$ is even, $\mathrm{inv}_\mu(\exp_K(A)[A]) = 0$ for all infinite primes μ of L. But $[\Gamma \otimes_K L] = \exp_K(A)[A]$ and so $[L_\mu\colon K_\pi] \cdot \mathrm{inv}_\pi[\Gamma] = \mathrm{inv}_\mu[\Gamma \otimes_K L] = 0$ for all extensions μ of π to L. In particular, all extensions of π to L must be complex so we may assume that (5) does not hold. Since $[L\colon K] = \sum_\mu [L_\mu\colon K_\pi]$, we are also finished if (3) holds. Finally, suppose (7) holds. Then there exist infinitely many finite primes τ of K with the property that $[L_\sigma: K_\tau]$ is even for all extensions σ of τ to L (see, for example, the proof of [1, Theorem 2]). For each infinite prime ϕ of K with $\text{inv}_\phi[\Gamma_p] = \frac{1}{2}$ we choose a different finite prime τ as above and let $\Omega(\phi)$ be the K-division ring such that $\text{inv}_\phi[\Omega(\phi)] = \text{inv}_\tau[\Omega(\phi)] = \frac{1}{2}$ and $\text{inv}_\rho[\Omega(\phi)] = 0$ for all other primes ρ of K. Let $\Delta = \Gamma \otimes_K (\otimes_\phi \Omega(\phi))$. Then $\Delta \in DB(K)$ and $[\Delta \otimes_K L] = [\Gamma \otimes_K L]$, so we are also finished if (7) holds. ∎

We remark that the precise conditions under which the u and r of Theorem 22 equal 1 are complicated and involve the existence of primes of K with certain local behavior in L; we omit these calculations. In the next section we will give an example to show that the case when $u = r = 1$ does arise. Although we will not prove it here, one can show that if $u = 1$ then also $r = 1$. We also give an example in the next section to show the case $u = 0$ and $r = 1$ occurs.

It is natural to ask whether there is a unique matrix size minimal or degree minimal B/K for a central simple A/L. Our final result shows that for global fields one always has infinitely many non-isomorphic choices for such a B.

THEOREM 24. *Let L/K be a non-trivial finite extension of global fields and let A/L be central simple. Then there exist infinitely many non-isomorphic central simple B/K which are both matrix size minimal and degree minimal for A/L.*

Proof. Let p be a prime such that $B(L/K)$ has infinitely many elements of order p; the existence of such a p follows from [1, Corollary 4]. Let B/K be as in the statement of Theorem 18 and let D be the skew component of B. Then $\deg(B) = d_K(A)$. We claim that p divides $\text{ind}(D)$. Suppose not. Let $C_B(L) \cong A \otimes_L Y$. By Theorem 18, Y is an L-division ring of index $r_K(A)$. Let D_1 be a K-division ring of index p split by L. Then $[A \otimes_L Y] = [(D \otimes_K D_1) \otimes_K L]$ and $D \otimes_K D_1$ is a K-division ring. By Proposition 5 there is an integer w such that $A \otimes_L Y/L$ is embeddable in $B_1 = M_w(D \otimes_K D_1)$ so that $C_{B_1}(L) \cong A \otimes_L Y/L$. Since $\text{ind}(Y) = r_K(A)$, we have $\deg(B_1) = d_K(A) = \deg(B)$ by Corollary 7. Since $\deg(D \otimes_K D_1) > \deg(D)$, the matrix size of B_1 is strictly smaller than the matrix size of B. Since B/K is matrix size minimal for A/L we conclude that p divides $\text{ind}(D)$ as asserted.

Let $\mathcal{T}$ be the set of primes π of K such that p divides the local degree $[L_\gamma: K_\pi]$ for every extension γ of π to L. By [1, Theorem 2], $\mathcal{T}$ is infinite. Let μ and ν be distinct primes in $\mathcal{T}$ such that $\text{inv}_\mu[D] = \text{inv}_\nu[D] = 0$ and let E be the K-division ring such that $\text{inv}_\mu[E] = 1/p$, $\text{inv}_\nu[E] = -1/p$, and $\text{inv}_\pi[E] = 0$ for all other primes π of K; the existence of E follows from

[4, (32.13)]. Our assumptions imply that $[E] \in B(L/K)$. Let Δ be the skew field component of $D \otimes_K E$. By [4, Theorem 32.19], $\text{ind}(\Delta) = \text{ind}(D)$. Since $[A] + [Y] = [\Delta \otimes_K L]$, Corollary 7 implies that $A \otimes_L Y$ is embeddable in $B_2 = M_t(\Delta)$, where $\deg(B_2) = d_K(A) = \deg(B)$. Since $\text{ind}(\Delta) = \text{ind}(D)$ and B/K is matrix size minimal for A/L, we conclude that $t = ms_K(A)$ and so B_2 is also matrix size minimal for A/L. Since there are infinitely many choices for μ and ν, there are infinitely many choices for B_2. In particular, B_2/K is degree minimal for A/L. ∎

4. An Example

In this section we will give an example of number fields L/K and a central simple A/L such that $d_K(A) = 2 \cdot [L: K] \cdot \deg(A) \cdot \exp_K(A)$ and $ms_K(A) = 2 \cdot [L: K] \cdot \deg(A)/k_K(A)$.

Example. Let $f(x) = x^4 + 18x^2 + 24x + 117 \in \mathbb{Q}[x]$. Using any of the standard computational packages available (e.g., Maple or Macsyma), one can easily check that $f(x)$ is irreducible in $\mathbb{Q}[x]$, has square discriminant $2^{18}3^6$, and has an irreducible factor of degree 3 when viewed in $\mathbb{Z}_5[x]$. It follows that the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to A_4. One can also easily verify that $f(x)$ has no real roots and factors into linear factors when viewed in $\mathbb{Z}_{71}[x]$. Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. Then E is totally imaginary, the rational prime 71 splits completely in E, and $\text{Gal}(E/\mathbb{Q}) \cong A_4$.

We next construct our base field K so that K is totally real, EK/K is unramified at all finite primes, and $\text{Gal}(EK/K) \cong A_4$. Let E_p denote the splitting field of $f(x)$ over $\mathbb{Q}_p$ for $p \in \{2, 3\}$. By [6, Proposition 4-10-5], $[E_p: \mathbb{Q}_p]$ divides 12. Let $r_p = 12/[E_p: \mathbb{Q}_p]$ and let $g_p(x)$ be a product of r_p distinct monic irreducible polynomials in $\mathbb{Q}_p[x]$ each of whose roots is a primitive element for E_p over $\mathbb{Q}_p$. Let $g_{71}(x) = x^{12} - 71 \in \mathbb{Q}_{71}[x]$ and let $g_\infty(x) = \prod_{i=1}^{12} (x - i) \in \mathbb{R}[x]$. We note that $g_p(x)$ is separable for $p = 2, 3, 71$, and ∞. By the Approximation Theorem [6, Theorem 1-2-3], Krasner's lemma [5, Lemma 5.5], and continuity considerations one can find a $g(x) \in \mathbb{Q}[x]$ sufficiently close p-adically to $g_p(x)$ for $p = 2, 3, 71$, and ∞ so that if $K = \mathbb{Q}(\alpha)$, where α is a root of $g(x)$, then K is totally real and EK/K is unramified at all finite primes of K. Moreover, since the rational prime 71 splits completely in E but is totally ramified in K, it follows that $E \cap K = \mathbb{Q}$ and so $\text{Gal}(EK/K) \cong A_4$.

Let $M = EK$. Then M/K is Galois with $\text{Gal}(M/K) \cong A_4$, K is totally real, M is totally imaginary, and each finite prime of K is unramified in M. Let L and T be, respectively, the fixed fields of distinct involutions σ and τ of $\text{Gal}(M/K)$. Since σ and τ are conjugate in $\text{Gal}(M/K)$, $L \cong T$. Since $M = LT$

and M is totally imaginary, each of L and T must also be totally imaginary. For future reference we note the following two properties of L/K:

(∗) if π is an infinite prime of L extending the prime ρ of K, then $[L_\pi : K_\rho] = 2$

(∗∗) if τ is a finite prime of K, then there is a prime β of L extending τ such that $[L_\beta : K_\tau]$ is odd.

Property (∗) follows from the fact L is totally imaginary while K is totally real and Property (∗∗) is proved exactly as in [3, Example 1, p. 184].

Let γ be the prime of K extending the rational prime 71 and let $\delta_1, \delta_2, ..., \delta_6$ denote the primes of L extending γ. By [4, (32.13)] there exists an L-division ring A such that $\mathrm{inv}_{\delta_i}[A] = \frac{1}{4}$ for $i \in \{1, 2, 3\}$, $\mathrm{inv}_{\delta_i}[A] = \frac{3}{4}$ for $i \in \{4, 5, 6\}$, and $\mathrm{inv}_\rho[A] = 0$ for all other primes ρ of L. We shall show that $\exp_K(A) = 2$ but $r_K(A) = 4$ and that $k_K(A) = 6$ but $v_K(A) = \frac{1}{3}$. In view of Theorems 6 and 14, this will show that

$$d_K(A) = 2 \cdot [L : K] \cdot \deg(A) \cdot \exp_K(A)$$

and

$$ms_K(A) = 2 \cdot [L : K] \cdot \deg(A)/k_K(A).$$

We show first that $\exp_K(A) = 2$ and $k_K(A) = 6$. By [4, Theorem 32.19], $\exp(A) = 4$. Let π be a fixed infinite prime of K and let Δ be the K-division ring such that $\mathrm{inv}_\gamma[\Delta] = \frac{1}{2}$, $\mathrm{inv}_\pi[\Delta] = \frac{1}{2}$, and $\mathrm{inv}_\rho[\Delta] = 0$ for all other primes ρ of K. By Property (∗) and [4, Theorems 31.9 and (32.13)], $\mathrm{Res}_{L/K}[\Delta] \cong 2[A]$ and so $\exp_K(A)$ divides 2. Suppose $\exp_K(A) = 1$. Then there exists a K-division ring Ω such that $\mathrm{Res}_{L/K}[\Omega] \cong [A]$. Since $[L_{\delta_1} : K_\gamma] = 1$, $\mathrm{inv}_\gamma[\Omega] = \frac{1}{4}$. But then $\mathrm{inv}_{\delta_4}(\mathrm{Res}_{L/K}[\Omega] = \frac{1}{4}$ while $\mathrm{inv}_{\delta_4}[A] = \frac{3}{4}$. Thus $\exp_K(A) = 2$. By [1, Corollary 3], $B(L/K)_3$ is infinite so there exists a K-division ring Υ of index 3 in $B(L/K)$. Then $\mathrm{Res}_{L/K}([\Delta \otimes_K \Upsilon]) = \exp_K(A)[A]$ so $k_K(A) \geqslant 6$. Suppose $k_K(A) > 6$ and let Ψ be a K-division ring of index $k_K(A)$ such that $[\Psi \otimes_K L] = 2[A]$. Then $2[\Psi] \in B(L/K)$ so Ψ has index dividing 12 [4, Theorem 28.5]. It follows that Ψ must have index 12. There must exist a prime ν of K such that $\mathrm{l.i.}_\nu[\Psi_2] = 4$. Clearly ν is a finite prime so by Property (∗∗) there is an extension ζ of ν to L such that $[L_\zeta : K_\nu]$ is odd. But then $\mathrm{inv}_\zeta 2[A] = [L_\zeta : K_\nu] \cdot \mathrm{inv}_\nu[\Psi]$ and so $\mathrm{l.i.}_\zeta 2[A] = 4$, a contradiction. Thus $k_K(A) = 6$.

We show next that $r_K(A) = 4$. By Corollary 11, $r_K(A)$ divides 4. Since $[A] \notin \mathrm{Res}_{L/K}(B(K))$, $r_K(A) \neq 1$. Suppose $r_K(A) = 2$ and Y is an L-division ring of index 2 such that $[A]+[Y] \in \mathrm{Res}_{L/K}(B(K)$. Let $[A]+[Y]= \mathrm{Res}_{L/K}[\Delta]$, where Δ is a K-division ring. Since $\mathrm{inv}_{\delta_i}([A]+[Y])= \mathrm{inv}_{\delta_j}([A]+[Y])=\mathrm{inv}_\gamma[\Delta]$ for $i \in \{1, 2, 3\}$ and $j \in \{4, 5, 6\}$ it follows that we may assume that $\mathrm{inv}_{\delta_i}[Y]=0$ for $i \in \{1, 2, 3\}$ and $\mathrm{inv}_{\delta_j}[Y]=\frac{1}{2}$ for $j \in \{4, 5, 6\}$. Let $\mathscr{S}$ denote the set of primes μ of L such that $\mu \notin \{\delta_4, \delta_5, \delta_6\}$ and $\mathrm{inv}_\mu[Y] \neq 0$. Since the sum of the invariants of $[Y]$ is an integer and Y has exponent 2, we must have $\mathrm{inv}_\mu[Y]=\frac{1}{2}$ for all primes $\mu \in \mathscr{S}$ and $|\mathscr{S}|$ is odd. Fix a prime τ of K, $\tau \neq \gamma$, and let $\mu_1, ..., \mu_r$ denote the primes of L extending τ. Since $\tau \neq \gamma$, $\mathrm{inv}_{\mu_i}[A]=0$ for $i=1, ..., r$. Suppose $\mathrm{inv}_{\mu_1}[Y]=\frac{1}{2}$. If $[L_\mu: K_\tau]$ is even then $\mathrm{l.i.}_\tau[\Delta]$ is divisible by 4. In particular, τ must be a finite prime. By Property $(**)$ there exists an i such that $[L_{\mu_i}: K_\tau]$ is odd. But $[L_{\mu_i}: K_\tau] \cdot \mathrm{inv}_\tau[\Delta]=\mathrm{inv}_{\mu_i}[Y]$, contradicting the fact that Y has exponent two. It follows that $[L_{\mu_1}: K_\tau]$ is odd and $\mathrm{inv}_\tau[\Delta]=\frac{1}{2}$. This implies that $\mathrm{inv}_{\mu_i}[Y]=\frac{1}{2}$ for all i such that $[L_{\mu_i}: K_\tau]$ is odd. But $\sum_i [L_{\mu_i}: K_\tau]=6$ so there are an even number of i with $[L_{\mu_i}: K_\tau]$ odd. This implies that $|\mathscr{S}|$ is even, a contradiction, proving that $r_K(A)=4$.

Finally, we show that $v_K(A)=\frac{1}{3}$. Let B/K be as in the statement of Theorem 18, let D be the skew field component of B, and let $C_B(L) \cong A \otimes_L Y$. By Theorem 18, $\exp(Y)=4$, $[D \otimes_K L]=[A]+[Y]$, and $v_K(A)=4/\exp(D)$. Then $4[D] \in B(L/K)$ so $\exp(D)$ divides 24. Suppose $\exp(D)=24$. Then there exists a prime τ of K such that $8 \mid \mathrm{l.i.}_\tau[D]$. τ is clearly finite and $\tau \neq \gamma$. By Property $(**)$, $[L_\beta: K_\tau]$ is odd for some extension β of τ. Since $\mathrm{inv}_\beta[A]=0$, $8 \mid \mathrm{l.i.}_\beta[Y]$, contradicting $\exp(Y)=4$. Thus $\exp(D) \leqslant 12$ and so $v_K(A) \geqslant \frac{1}{3}$. Let η be a prime of K splitting completely in L, $\eta \neq \gamma$. (Since the rational prime 197 splits completely in E, if we require $g(x)$ to be sufficiently close 197-adically to $x^{12}-197$, we can take η to be the prime of K extending 197.) Let Δ_2 be the K-division ring such that $\mathrm{inv}_\gamma[\Delta_2]=\frac{1}{4}$, $\mathrm{inv}_\eta[\Delta_2]=\frac{3}{4}$, and $\mathrm{inv}_\rho[\Delta_2]=0$ for all other primes ρ of K. Let $\Delta=\Delta_2 \otimes_K \Upsilon$, where $[\Upsilon] \in B(L/K)$ with $\exp(\Upsilon)=3$. Let $[Y]= [\Delta \otimes_K L]-[A]$. Then Y has exponent four and so $v_K(A) \leqslant \frac{4}{12}$. Thus $v_K(A)=\frac{1}{3}$, as was to be shown.

We can also construct an example to show that the case $u=0$, $r=1$ occurs. With notation as in the example, let π be a fixed infinite prime of K and let π_1 be an extension of π to L. Let A be the L-division ring with invariants as follows: $\mathrm{inv}_{\delta_1}=\frac{1}{2}$, $\mathrm{inv}_{\pi_1}=\frac{1}{2}$, all other invariants 0. Then one can easily check that $\exp_K(A)=r_K(A)=k_K(A)=2$ but $v_K(A)=1$.

REFERENCES

1. B. FEIN, W. M. KANTOR, AND M. SCHACHER, Relative Brauer groups, II, *J. Reine Angew. Math.* **328** (1981), 39–57.

2. B. FEIN AND M. SCHACHER, Finite groups occuring in finite dimensional division algebras, *J. Algebra* **32** (1974), 332–338.
3. B. FEIN AND M. SCHACHER, Relative Brauer groups, I. *J. Reine Angew. Math.* **321** (1981), 179–194.
4. I. REINER, "Maximal Orders," Academic Press, New York, 1975.
5. D. J. SALTMAN, Generic Galois extensions and problems in field theory, *Adv. in Math.* **43** (1982), 250–283.
6. E. WEISS, "Algebraic Number Theory," McGraw–Hill, New York, 1963.