Pacific Journal of Mathematics

FINITE PRIMES IN SIMPLE ALGEBRAS

HOYT D. WARNER

Vol. 36, No. 1 November 1971

PACIFIC JOURNAL OF MATHEMATICS
Vol. 36, No. 1, 1971

FINITE PRIMES IN SIMPLE ALGEBRAS

HOYT D. WARNER

A "prime" in an arbitrary ring with identity, as defined by D. K. Harrison, is shown to be a generalization of certain objects occurring in the classical arithmetic of a central simple K-algebra $\sum$, i.e., the theory of maximal orders over Dedekind domains with quotient field K. Specifically, if K is a global field the "finite primes" of $\sum$ (in Harrison's sense) which contain a K-basis for $\sum$ are the generators of the Brandt Groupoids of normal R-lattices, R ranging over the nontrivial valuation rings of K. The situation when $\sum$ contains a finite prime invariant under all K-automorphisms is studied closely; when K is the rational numbers or char $(K) \neq 0$, and $\sum$ has prime power degree, such a prime exists if and only if $\sum$ is a division algebra.

The techniques developed here are applied to yield new information concerning the generators and factorization in the Brandt Groupoids over certain Dedekind domains.

Harrison showed in [7] that his definition of prime (see § 1) yields the finite and real infinite prime divisors of number fields, as well as yielding the "primes" (i.e., prime ideals) of the rings of integers of these fields. His conjecture ([7, p. 13, footnote]), that a suitable modification of this definition existed which would yield objects in the arithmetic of "noncommutative number fields", was the starting point for this investigation; § 3 contains the results.

NOTATION. Throughout this paper all algebras will be assumed finite dimensional and all fields considered will be assumed not locally finite unless explicitly stated otherwise. (By *locally finite* we mean each element is contained in a finite subfield.) $\boldsymbol{Z}$, $\boldsymbol{Q}$, and $\boldsymbol{R}$ will denote the integers, rationals, and reals, respectively. For sets A and B,

$$A \backslash B = \{x \in A \mid x \notin B\} .$$

1. Preliminaries. In this section we prepare for the body of the paper by fixing notation and definitions we will need and proving some preliminary general results. We refer the reader to [7] for all unproved assertions about primes.

A *preprime* of a ring R with identity 1 is a nonempty subset closed under addition and multiplication and not containing -1; a *prime* is a maximal preprime. A prime P is called *finite* if $1 \notin P$, which is equivalent to $a \in P$ if and only if $-a \in P$, i.e., P is an

additive subgroup of R; otherwise P is called *infinite*. If P is finite, $A_P = \{a \in R \mid aP \subseteq P \text{ and } Pa \subseteq P\}$ is a subring of R and $A_P/P = k_P$ is a locally finite field. If P is a finite prime of a field F, then A_P is a valuation ring of F with P its ideal of nonunits. When F is a global field the finite primes of F are thus in one-to-one correspondence with the finite prime divisors of F. We note also that for F a number field, the infinite primes which generate F as a ring (called real infinite primes in [7]) are in one-to-one correspondence with the real infinite prime divisors (i.e., the real places) of F [7, Proposition 3.5]. We will say a finite prime P of a field F is *discrete rank one* if the valuation determined by A_P is nontrivial and discrete rank one. If $R \subseteq S$ are rings, P and T are primes of R, S, respectively, we shall say "*T extends P*" if and only if $T \supseteq P$, which is equivalent to $T \cap R = P$. Note that if T extends P then T is finite if and only if P is finite.

The following lemma generalizes [7, Proposition 2.1] to noncentral elements of a ring.

LEMMA 1.1. *Let P be a finite prime of a ring R. Let $a, b \in R$. Then $aPb \subseteq P$ and $ab \in P$ imply $a \in P$ or $b \in P$.*

Proof. Suppose $aPb \subseteq P$, $ab \in P$, but neither a nor b are in P. For $i \geq 1$, let $W_i(a)$ be the set of all finite sums of elements of R of the form $\alpha_0 a \alpha_1 a \cdots \alpha_{i-1} a \alpha_i$, where $\alpha_j \in \boldsymbol{Z}\cdot 1 + P$ for $0 \leq j \leq i$; let $W_0(a) = P$ and note $W_i(a)$ is an additive group for each i. Let $T_a = \sum_0^\infty W_i(a)$; this is precisely the smallest additively and multiplicatively closed subset of R containing P and a, hence it must contain -1 since $a \notin P$ implies $T_a \supsetneq P$, and P is a maximal preprime. Likewise $-1 \in T_b$ (defined similarly). Write

$$-1 = \alpha + f_1(a) + \cdots + f_n(a) \tag{I}$$

and

$$-1 = \beta + g_1(b) + \cdots + g_m(b) \tag{II}$$

where $f_i(a) \in W_i(a)$, $g_i(b) \in W_i(b)$, α, β are in P, and where n and m are chosen minimal ($n \geq 1$, $m \geq 1$ as $-1 \notin P$). An easy induction argument shows that for $i \geq j \geq 1$, $W_i(a) W_j(b) \subseteq W_{i-j}(a)$ and for $1 \leq i \leq j$, $W_i(a) W_j(b) \subseteq W_{j-i}(b)$, because $aPb \subseteq P$ and $ab \in P$ implies $a(\boldsymbol{Z}\cdot 1 + P)b \subseteq P$. If now $n \leq m$, multiply (I) on the right by $-g_m(b)$ (after transposing α to the left side) which yields, by the preceeding remark, $(1 + \alpha) g_m(b) \in \sum_{m-n}^{m-1} W_j(b)$. Then multiply (II) on the left by $1 + \alpha$, transpose the $-\alpha$ to the right side and an expression like (II) results, but with the right side now in $\sum_0^{m-1} W_i(b)$, contradicting

the minimality of m. If $n \geqq m$, the argument is similar.

The facts in the following corollary were first observed by Manis and Harrison (unpublished).

COROLLARY 1.2. *Let P be a finite prime of R.*

(1) *If $\mathfrak{p}$ is the largest two sided ideal of R contained in P, then $\mathfrak{p}$ is a prime ideal.*

(2) *If $a, b \in$ center of R, $ab \in P$ implies $a \in P$ or $b \in P$, and $ab \in A_P$, $a \notin A_P$ imply $b \in P$.*

(3) *If R_1 is a subring of the center of R and $P_1 = P \cap R$ is a prime of R_1, then $A_P \cap R_1 = A_{P_1}$.*

(4) *If K is a subfield of the center of R then $P \cap K$ is a prime of K, and $A_{P \cap K} = A_P \cap K$.*

Proof. (1): If $\mathfrak{a} \cdot \mathfrak{b} \subseteqq \mathfrak{p}$, $\mathfrak{a}$ and $\mathfrak{b}$ two sided ideals then $\mathfrak{a}P\mathfrak{b} \subseteqq \mathfrak{a}R\mathfrak{b} \subset \mathfrak{p} \subseteqq P$, so if $\mathfrak{a} \nsubseteqq \mathfrak{p}$, i.e., $\mathfrak{a} \nsubseteqq P$, the lemma implies $\mathfrak{b} \subseteqq P$, i.e., $\mathfrak{b} \subseteqq \mathfrak{p}$. (2): $ab \in A_P$ and $a, b \in$ center implies $aP\mathfrak{b} = abP \subseteqq P$ so $a \notin A_P$ implies $a\alpha \notin P$ for some $\alpha \in P$, but $a\alpha P\mathfrak{b} \subseteqq aP\mathfrak{b} \subseteqq P$ and $(a\alpha)b \in aP\mathfrak{b} \subseteqq P$ then implies $b \in P$. (3): $A_P \cap R_1 \subseteqq A_{P_1}$ is clear. $P_1 \subseteqq P \subseteqq A_P$, so suppose $a \in A_{P_1} \backslash P_1$; then as A_{P_1}/P_1 is a locally finite field, $a^n - 1 \in P_1$ for some n; so $a^n \in 1 + P_1 \subseteqq 1 + P \subseteqq A_P$, and hence $a \in A_P$ by (2). (4): By (2), $A_P \cap K$ is a valuation ring; since $(A_P \cap K)/(P \cap K)$ is a subring, hence a subfield, of the locally finite field A_P/P, $P \cap K$ is the maximal ideal of $A_P \cap K$ and is a prime of K by [7, Proposition 2.5].

The following corollary shows that in studying the primes of a finite dimensional K-algebra Σ, it is sufficient to study the case when Σ is simple, as we shall do in this paper.

COROLLARY 1.3. *Let Σ be a K-algebra, let C be the center of Σ. If T is any finite prime of Σ, $T \cap C$ is a finite prime of C. Every finite prime of Σ contains the radical* $\operatorname{rad}\Sigma$ *of Σ so there is a one-to-one correspondence between the primes of Σ and those of the semi-simple algebra $\bar{\Sigma} = \Sigma/\operatorname{rad}\Sigma$. The primes of a semi-simple algebra $\prod_1^n \Sigma_i$, Σ_i simple, are precisely those subsets of the form $T_i \cdot \prod_{j \neq i} \Sigma_j$ where T_i is a prime of Σ_i.*

Proof. Note that if R is a ring, $\mathfrak{a}$ a two sided ideal of R then $P \supseteqq \mathfrak{a}$ is a preprime or prime of R if and only if $P/\mathfrak{a}$ is a preprime or prime of $R/\mathfrak{a}$. Next observe that if P is a prime of R and $R = \mathfrak{b}_1 + \cdots + \mathfrak{b}_n$, $\mathfrak{b}_i$ two sided ideals with $\mathfrak{b}_i\mathfrak{b}_j \subseteqq P$ for $i \neq j$ then all but one of the $\mathfrak{b}_i$ is contained in P, by (1) of 1.2. Hence $P/(\sum_{j \neq i} \mathfrak{b}_j)$ is a prime of the ring $R/\sum_{j \neq i} \mathfrak{b}_j$. The last two assertions now follow

immediately, observing that as rad Σ is nilpotent, rad $\Sigma \subseteqq T$ for any finite prime T by (1) of 1.2. That $T \cap C$ is a prime of C follows from the preceeding remarks and (4) of 1.2.

In § 3 and § 4 below we shall be considering finite primes T of a simple K-algebra Σ which satisfy $K \cdot T = \Sigma$, i.e., such that T contains a K-basis for Σ. The following proposition suggests that, by analogy with the commutative case, it is not unreasonable to impose this condition on (finite) primes of a noncommutative algebra.

PROPOSITION 1.4. *Let Σ be a K-algebra.*

(1) *If Σ is commutative then $KT = \Sigma$ for any finite prime T of Σ.*

(2) *Σ always contains finite primes T with $KT = \Sigma$.*

(3) *Let C be the center of Σ, let L be any subfield of C such that Σ is finite dimensional over L. For a finite prime T of Σ, the following are equivalent:*

(a) $KT = \Sigma$

(b) $KC = \Sigma$

(c) $KL = \Sigma$.

Proof. First note that $T \cap K$, a prime of K by 1.3, is $\neq 0$ (as K is not locally finite) so $KT \supseteqq A_T$ as $T \supseteqq (T \cap K)A_T$; thus $KT = \Sigma$ if and only if $KA_T = \Sigma$. Proof of (1): If $a \in \Sigma$ then $[\Sigma : K] < \infty$ implies $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$ for $\alpha_i \in K$, not all zero. $T \cap K = P$ is a finite prime of K by 1.2, (4), and so $A_P = A_T \cap K$ is a valuation ring of K by [7, Proposition 2.5] and there exists $\alpha \neq 0$ in P with $\alpha\alpha_i \in P$ for $1 \leqq i \leqq n$. One checks that then αa is integral over A_P, so a fortiori over A_T, hence $\alpha a \in A_T$ as A_T is integrally closed by [7, Proposition 2.7]. Thus $a \in K \cdot A_T$, and (1) holds. (2): If Σ is arbitrary, let P be a finite prime of K; $P \neq \{0\}$ and A_P is a valuation ring of K. If $1 = x_1, x_2, \cdots, x_n$ is a K-basis of Σ and $x_i x_j = \sum_k \gamma_{ijk} x_k$, $\gamma_{ijk} \in K$ for $i, j \geqq 2$, we can choose $\alpha \neq 0$ in P such that $\alpha\gamma_{ijk} \in A_P$ for all i, j, k (using A_P a valuation ring of K); then one checks $S = P + \sum_2^n A_P(\alpha x_j)$ is a preprime of Σ containing P and a K-basis for Σ; any prime T containing S is as desired. (3): By Corollary 1.3, $T \cap C$ is a (finite) prime of C, and hence by (1) above, (since $[C : K] \leqq [\Sigma : K] < \infty$)$K \cdot (T \cap C) = C$; $[\Sigma : L] < \infty$ implies L also is not locally finite so also $L \cdot (T \cap C) = C$. Hence $K \cdot T = C \cdot T = L \cdot T$, proving the assertion.

DEFINITION 1.5. Let Σ be a K-algebra (recall we assume Σ finite dimensional, K not locally finite). A finite prime T of Σ will be called *spanning* if $K \cdot T = \Sigma$. Proposition 1.4 shows this definition does not depend on the choice of the (not locally finite) field K

over which Σ is finite dimensional and is equivalent to requiring $C \cdot T = \Sigma$ for C the center of Σ.

We conclude this section by stating the main result of [10] and deriving a corollary we will need.

PROPOSITION 1.6. ([10, *Th.* 3.2 *and Corollary* 2.2].) *Let k be a locally finite field, $\Sigma = \mathrm{Hom}_k(V, V)$ for V a finite dimensional k-vector space. Every prime T of Σ is finite and has the form $T = L(W, U) = \{f \in \Sigma \mid f(W) \subseteq U\}$ for uniquely determined k-subspaces $W \supseteq U$ of V with $\dim_k W/U = 1$ and conversely every such $L(W, U)$ (i.e., with $\dim_k W/U = 1$) is a prime of Σ.*

COROLLARY 1.7. *Situation as above, with $\dim_k V > 1$. Every prime T has the form $T = \varepsilon_1\Sigma + \Sigma\varepsilon_2$, where $1 = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, the ε_i are orthogonal idempotents, and ε_3 has rank 1 (so $\varepsilon_3 \neq 0$).*

Proof. $T = L(W, U)$, $\dim_k W/U = 1$ so $W = kx \oplus U$ for some x; write $V = W' \oplus W = U \oplus W' \oplus kx$. Let $\varepsilon_1, \varepsilon_2, \varepsilon_3$ be the idempotents associated with the decomposition (i.e., ε_1 = projection on U along $W' \oplus kx$, etc.). Then $\varepsilon_1\Sigma = L(V, U) \subseteq L(W, U)$ and $\Sigma\varepsilon_2 \subseteq L(W, 0) \subseteq L(W, U)$ so $T \subseteq \varepsilon_1\Sigma + \Sigma\varepsilon_2$. For the reverse inclusion, let $t \in T$. Then as $(1 - \varepsilon_2)V = (\varepsilon_1 + \varepsilon_3)V = U \oplus kx = W$ and as $t \cdot W \subseteq U \subseteq$ kernel of $1 - \varepsilon_1$, $(1 - \varepsilon_1)t(1 - \varepsilon_2) = 0$ so $t(1 - \varepsilon_2) - \varepsilon_1 t(1 - \varepsilon_2) = 0$ so $t = \varepsilon_1(t(1 - \varepsilon_2)) + t\varepsilon_2 \in \varepsilon_1\Sigma + \Sigma\varepsilon_2$.

2. Brandt groupoid generators over classical dedekind domains. First we recall some facts and establish notation. Throughout this section R will denote a Dedekind domain distinct from its quotient field K, and Σ will denote a separable (see [4]) K-algebra. We refer the reader to [4], [5], and [6] for the following facts. An R-lattice M in Σ is a finite (i.e., finitely generated) R-submodule of Σ with $K \cdot M = \Sigma$. An R-order in Σ is a subring which is an R-lattice; every R-order is contained in a maximal one. If M is an R-lattice, $O_l(M) = \{x \in \Sigma \mid xM \subseteq M\}$ and $O_r(M) = \{x \in \Sigma \mid Mx \subseteq M\}$ are R-orders, the left and right orders of M. M is called integral if $M \subseteq O_l(M)$ and normal if $O_l(M)$ is maximal; these definitions are really right-left symmetric. If Λ is an R-order then all nonzero prime (ring) ideals of Λ are maximal ideals and are R-lattices. If Λ is a maximal order the set of all R-lattices in Σ which are two sided Λ-modules forms an abelian group free on the maximal ideals of Λ as generators, with identity Λ and inverses $M^{-1} = \{x \in \Sigma \mid MxM \subseteq M\}$; when Σ is simple the set of all normal R-lattices forms a groupoid, called the Brandt Groupoid. Briefly, for M, N normal R-lattices, the product

$M \cdot N = \{\sum m_i n_i \mid m_i \in M, n_i \in N\}$ is allowed only when $O_r(M) = O_l(N)$; the maximal orders are the units; $N^{-1} = \{x \in \Sigma \mid NxN \subseteqq N\}$; $NN^{-1} = O_l(N)$, $N^{-1}N = O_r(N)$; every normal R-lattice $M = N_1 \cdot N_2^{-1}$ with N_1, N_2 integral, and every integral R-lattice M has an essentially unique decomposition $M = N_1 \cdots N_k$ (product in the groupoid) where the N_i are indecomposable (i.e., not expresible as a groupoid product of nonunit integral normal lattices); the indecomposable R-lattices are exactly the maximal one-sided ideals in the maximal R-orders in Σ, and are called the generators of the Brandt Groupoid (over R in Σ).

The main result of this section is a characterization of the generators of the Brandt Groupoid over R, when R satisfies the additional condition that each maximal ideal P of R is a prime of R, or equivalently R/P is a locally finite field for each maximal ideal P. We shall call such Dedekind domains "classical", since this condition is satisfied by all Dedekind domains whose quotient fields are (possibly infinite) algebraic number fields, and is also satisfied by the valuation rings of classical local fields; moreover, any Dedekind domain which is finitely generated (as a ring) is classical by [5, p. 68, Th. 3].

THEOREM 2.1. *Let R be a classical Dedekind domain, Σ a simple separable algebra over the quotient field K of R. The generators of the Brandt Groupoid over R in Σ are the maximal finite R-module preprimes of Σ. Moreover, each generator is a prime of any R-order containing it.*

Proof. Let $I = I_R$ be the set of generators of the Brandt Groupoid over R in Σ, and let $W = W_R$ be the set of all preprimes of Σ which are also finite R-submodules of Σ. We are to prove that I is the set of maximal elements of W.

If $S \in W$ then $R + S$ is a subring which is a finite R-module so is contained in an R-order Λ (Proposition 1.1 of [4]) so $S \subseteqq \Lambda$; thus the elements of S are integral over R. A key step is the following:

LEMMA 2.2. *Let $S \in W$. Let P be any maximal ideal of R with $P \supseteqq S \cap R$. Let Λ be any R-order containing S. Then there exists a positive integer n with $P^n\Lambda + S \in W$, i.e., $P^n\Lambda + S$ is a preprime.*

Proof. $1 \notin S$ so $S \cap R$ is a proper ideal of R and P exists. $P^n\Lambda + S \notin W$ for all positive integers n means $1 \in P^n\Lambda + S$ for all n (as $P^n\Lambda + S$ is a finite R-module closed under $+$ and $\cdot$). Let R_P be the localization of R at P, let $M_P = R_P \cdot M$ for any R-submodule of Σ. Then $1 \in P_P^n \Lambda_P + S_P$ for all n which implies, as R_P is a Noetherian local ring and Λ_P is a finite R_P-module, that $1 \in S_P$

(Proposition 6, of Chapt. 3, § 3, no. 3 of [5]). But then there exists $s \in R \backslash P$ such that $s \cdot 1 = s \in S$ i.e., $s \in S \cap R \subseteq P$, a contradiction.

Combining the initial remarks with the lemma above, any $S \in W$ is contained in $S_1 \in W$ with $S_1 \cdot K = \Sigma$. Now apply Zorn's lemma to the inductive collection of preprimes T of Σ such that $T \supseteq S_1$, T is an R-submodule of Σ and T consists of elements of Σ integral over R; let T be maximal such. Then $R + T$ is a ring of elements integral over R and $K(R + T) \supseteq K \cdot S_1 = \Sigma$ so $R + T$ is an R-order of Σ hence a finite R-module, hence $T \in W$, and clearly T is maximal in W (since we noted any $S \in W$ consists of integral elements). Thus any element S of W is contained in a maximal element T of W.

Now suppose T is any maximal element of W. $T \cap R = P$ is a maximal ideal (as $T \cap R \subseteq P$, a maximal ideal of R, implies $T + P$ is a preprime and a finite R-module so $T = T + P$) and P is a prime of R as R is classical. Next let Λ be any R-order containing T, we claim T is a prime of Λ. For suppose $T \subseteq T_1$ a prime of Λ. Then $T_1 \cap R$ is a preprime of R containing the prime $P = T \cap R$ of R, so $T_1 \cap R = P$, and hence by Corollary 1.2, (3) $R = A_P = A_{T_1} \cap R$, i.e., T_1 is an R-module. But $T_1 \subseteq \Lambda$ a finite R-module so T_1 is a finite R-module so $T_1 \in W$ and $T_1 = T$ by maximality of T in W.

Now let Λ be any maximal R-order containing T, a maximal element of W. We contend T is either a left or a right ideal of Λ, hence a maximal left or right ideal of Λ (as all proper ideals of Λ are in W) and hence a generator of the Brandt Groupoid. By Lemma 2.2, T contains a nonzero two-sided ideal of Λ so by Corollary 1.2, (1), the largest two-sided ideal $\mathfrak{p}$ of Λ contained in T is a nonzero prime ideal hence a maximal ideal of Λ. Hence (as T is a prime of Λ) $\bar{T} = T/\mathfrak{p}$ is a prime of the simple $\bar{R} = R/P$ algebra $\bar{\Lambda} = \Lambda/\mathfrak{p}$. But $\bar{R}$ is a locally finite field so any finite dimensional division algebra over $\bar{R}$ is again a locally finite field (see [7]), so either $\bar{\Lambda}$ is a locally finite field or $\bar{\Lambda} \cong \mathrm{Hom}_k(V, V)$, k locally finite, $2 \leqq \dim_k V < \infty$. In the first case $\bar{T} = \{0\}$ i.e., $T = \mathfrak{p}$ and we are done (this is always the case when Σ is commutative). In the second case, by Corollary 1.7, $\bar{T} = \varepsilon_1 \bar{\Lambda} + \bar{\Lambda} \varepsilon_2$ with $1 = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$ in $\bar{\Lambda}$, ε_i orthogonal idempotents in $\bar{\Lambda}$, and $\varepsilon_3 \neq 0$. Choose $e_i \in \Lambda$, $1 \leqq i \leqq 3$ with $e_1 + \mathfrak{p} = \varepsilon_1$, $e_2 + \mathfrak{p} = \varepsilon_2$, $e_3 = 1 - (e_1 + e_2)$, so $e_3 + \mathfrak{p} = \varepsilon_3$ and $1 = e_1 + e_2 + e_3$. Then $T = e_1 \Lambda + \Lambda e_2 + \mathfrak{p}$. Our assertion about T will be proven if we can show either $e_1 \in \mathfrak{p}$ or $e_2 \in \mathfrak{p}$ (as then $T = e_1 \Lambda + \mathfrak{p}$, a right ideal, or $= \Lambda e_2 + \mathfrak{p}$, a left ideal). So suppose both e_1 and e_2 are not in $\mathfrak{p}$. Let $S = T + e_1 \mathfrak{p}^{-1} e_2$; using $e_i e_j \in \mathfrak{p}$ if $i \neq j$ (as $\varepsilon_i \varepsilon_j = 0$ if $i \neq j$) one checks that S is closed under multiplication as well as addition. If $-1 \in S$, then $1 \in S$ (as $-S \subseteq S$) so as $-e_1 - e_2 \in T \subseteq S$,

$e_3 = 1 - e_1 - e_2 \in S$. But then $e_3e_3e_3 \in e_3Se_3$ which one checks (using again $e_ie_j \in \mathfrak{p}$ if $i \neq j$) is contained in $\mathfrak{p}$, so $\varepsilon_3 = (\varepsilon_3)^3 = (e_3)^3 + \mathfrak{p} = 0$, a contradiction. Hence $-1 \notin S$, so $S \in W$ (as S is clearly a finite R-module), and hence $S = T$ as T is maximal in W. Then $e_1\mathfrak{p}^{-1}e_2 \subsetneqq S = T \subsetneqq \Lambda$, but as $\Lambda(e_i + \mathfrak{p})\Lambda = \Lambda$ since $e_i \notin \mathfrak{p}$ for $i = 1, 2$, $e_1\mathfrak{p}^{-1}e_2 \subsetneqq \Lambda$ implies $\mathfrak{p}^{-1} = \Lambda\mathfrak{p}^{-1}\Lambda = \Lambda(e_1 + \mathfrak{p})\Lambda\mathfrak{p}^{-1}\Lambda(e_2 + \mathfrak{p})\Lambda \subsetneqq \Lambda$, a contradiction.

To complete the proof of 2.1 it remains to show that any $T \in I$, i.e., any generator of the Brandt Groupoid, is maximal in W; but if T were not maximal we would have $T \subsetneqq T_1$ maximal in W, but then $T_1 \in I$ and (by Satz. 16, p. 76 of [6]) $T = MT_1N$ for M, N normal integral T-lattices, M or N not a unit in the groupoid, contradicting T indecomposable.

REMARKS. (1) If Σ is a separable field extension then I_R is the set of nonzero prime ideals of the integral closure $\bar{R}$ of R in Σ, so the theorem characterizes them "intrinsically".

(2) The final assertion of the theorem shows that a maximal R-order Λ in Σ again is "classical" since the maximal one-sided ideals of Λ are primes of Λ.

(3) The finite R-module preprimes S with $KS = \Sigma$ are precisely the proper integral R-lattices (M proper meaning $M \subsetneqq 0_l(M)$), so the theorem shows every proper integral R-lattice is contained in a maximal one, which is in fact a normal lattice.

(4) It follows immediately from the proof above (or use [6]) that if T is a generator of the Brandt Groupoid over R in Σ, then T is contained in exactly two maximal R-orders, namely $O_l(T)$ and $O_r(T)$.

3. Spanning primes of a simple algebra. In this section we apply Theorem 2.1 in the special case when R is the valuation ring A_P of a discrete rank one prime P and Σ is central, to show that the generators of the Brandt Groupoid of normal A_P-lattices are then precisely the spanning primes of Σ extending P. With this we can characterize spanning primes over global fields. A close analysis of the case when A_P is complete and use of Rutherford's Theorem (Proposition 1.6) yields some apparently new information about the factorization of the unique maximal ideal of a maximal A_P-order as a product of generators.

THEOREM 3.1. *Let Σ be a central simple K-algebra. Let P be a discrete rank one finite prime of K. For $T \subsetneqq \Sigma$ the following are equivalent:*

(1) *T is a spanning prime of Σ extending P;*

(2) *T is a prime of Σ extending P and T is a finite A_P-module;*

(3) *T is a generator of the Brandt Groupoid of normal A_P-lattices in Σ.*

Proof. We first assume that A_P is a *complete* discrete rank one valuation ring and prove 3.1, then deduce the general case. The proof depends on the special case when Σ is a division algebra, in which the situation is particularly simple.

PROPOSITION 3.2. *Let D be a (not necessarily central) division algebra over K. Let P be a finite prime of K with A_P a complete discrete rank one valuation ring. Then there is a unique prime T of D extending P. Namely, T is the unique maximal one or two-sided ideal of the unique maximal A_P-order Δ in D. T is a spanning prime of D and T is a finite A_P-submodule of D.*

Proof. Let T be any prime of D with $T \supseteq P$; such a T always exists by Zorn's lemma, and T is a finite prime if P is. Then $T \cap K = P$ and $A_P \subseteq A_T$ (by Corollary 1.2, (3)) so that T is an A_P-submodule of D. To show $T = \mathfrak{p}$, the unique maximal one or two-sided ideal of Δ, it suffices to show $T \subseteq \Delta$. For then T is a finite A_P-module and so a maximal finite A_P-module preprime, hence by Theorem 2.1, $T = \mathfrak{p}$, as $\mathfrak{p}$ is the only maximal one-sided ideal of a maximal A_P-order in D. Let $t \in T$. If $t \in K$ then $t \in T \cap K = P \subseteq A_P \subseteq \Delta$. If $t \in T \setminus K$ let $f(x) = \sum_0^n a_i x^i$ be the monic minimum polynomial for t over K, so $a_n = 1$. Since Σ is a division algebra and $t \neq 0$, f is irreducible. Let v be the (exponential) valuation determined by A_P. Then $v(a_0) > \min\{v(a_i) \mid 1 \leqq i \leqq n\}$, for if not, we have $v(a_0^{-1}a_i) \geqq 0$, $1 \leqq i \leqq n$, so $a_0^{-1}f(x) = a_0^{-1}a_n x^n + \cdots + a_0^{-1}a_1 x + 1$ has all its coefficients in $A_P \subseteq A_T$, but then $0 = a_0^{-1}a_n t_n + \cdots + a_0^{-1}a_1 t + 1$ implies $-1 = a_0^{-1}a_n t^n + \cdots + a_0^{-1}a_1 t \in A_T \cdot T \subseteq T$, a contradiction. Hensel's Lemma holds in K so ([11, Lemma 21, p. 52]), $f(x)$ irreducible over K implies $\min\{v(a_i) \mid 1 \leqq i \leqq n-1\} \geqq \min\{v(a_0), v(a_n)\}$. Now, $\min\{v(a_0), v(a_n)\} = v(a_n) = v(1) = 0$ by what we just showed, so $v(a_i) \geqq 0$ for all i and $f(x) \in A_P[x]$, proving t is integral over A_P, and hence $t \in \Delta$. Done.

Proof of 3.1 *in the case that A_P is complete, and Σ is not a division algebra*: applying Theorem 2.1, we see immediately that (2) implies (3) since (2) implies T is a maximal element of the set of finite A_P-module preprimes in Σ; moreover, as T is then a normal R-lattice, $K \cdot T = \Sigma$, so also (2) implies (1).

To show (1) implies (2) we identify Σ with $(D)_n$ where D is a division algebra finite dimensional (and central) over K, and $n > 1$. Let T satisfy (1) and let $\{\varepsilon_{ij} \mid 1 \leqq i, j \leqq n\}$ be the usual matrix units (ε_{ij} has 1 in i,j-th spot, 0 elsewhere). Let π be a prime element of

A_P, i.e., $\pi A_P = P$. Then $KT = \Sigma$ implies there exists a positive integer k with $\pi^k \varepsilon_{ij} \in T$ for all i, j. We assert that $T \subseteqq (\pi^{-2k} T_0)_n$ where T_0 is the unique prime of D extending P (see 3.2); if so then since $T \cap K = P$ implies T is an A_P-module (by (3) of Corollary 1.2) and since T_0 is a finite A_P-module (by Proposition 3.2), T will be a finite A_P-module, proving (2) holds. Identify D with the set of "scalar matrices", i.e., matrices of the form diag $\{a, a, \cdots, a\}$ where $a \in D$. Since D is a subring of Σ, $T \cap D$ is a preprime of D, and $T \cap D$ extends P, so $T \cap D$ must be contained in T_0, the *unique* prime of D extending P. To prove $T \subseteqq (\pi^{-2k} T_0)_n$ it then suffices to show $\pi^{2k} M_{ij} \subseteqq T \cap D$ where $M_{ij} = \{a \in D \mid a$ is the i, j-th entry of some matrix in $T\}$. Let $a \in M_{ij}$, say $a = a_{ij}$ for $t = (a_{lm}) \in T$. Then diag $\{\pi^{2k} a, \cdots, \pi^{2k} a\} = \sum_{l=1}^{n} (\pi^k \varepsilon_{li}) t (\pi^k \varepsilon_{jl}) \in T \cdot T \cdot T \subseteqq T$ so $\pi^{2k} a \in T \cap D$ as asserted.

Thus (1) is equivalent to (2). Finally if (3) holds, i.e., T is a generator of the groupoid, let T_1 be any prime of Σ containing T; then $KT_1 \supseteqq KT = \Sigma$ so (1) holds for T_1, hence (2) holds for T_1, so $T_1 \in W_{AP}$ so $T_1 = T$ as T is maximal in W_{AP} by Theorem 2.1. Thus (2) and (1) hold for T, concluding the proof of 3.1 when A_P is complete.

To deduce the general case we apply the following well known lemma:

LEMMA 3.3. *Let V be a finite dimensional K-vector space. Let A be a discrete rank one valuation ring of K, with maximal ideal P. Let A^* denote the P-adic completion of A.*

(1) *If M is any A-submodule of V, $(M \otimes_A A^*) \cap V = M$.*

(2) *If N^* is any A^*-lattice in $V \otimes_A A^*$, then $N^* \cap V = N$ is an A-lattice in V and $N \otimes_A A^* = N^*$.*

Proof. See Chapter 7 of [5]. One easily checks that M need not be a finitely generated A-module in (1).

Proof of Theorem 3.1. Suppose first that T satisfies (1) of Theorem 3.1. Then T is an A_P-submodule of Σ and $KT = \Sigma$. Hence (letting $(\,)_P^*$ denote P-adic completion) $T^* = T \otimes A_P^*$ is an A_P^*-submodule of $\Sigma_P^* = \Sigma \otimes K_P^*$, $T^* \supseteqq P \cdot A_P^* = P^*$ the maximal ideal of A_P^* (a prime of K_P^*) and T^* spans Σ_P^*; moreover T^* is a preprime of Σ_P^* as $-1 \in T^*$ implies $-1 \in T^* \cap \Sigma = T$ (by 3.3, (1)), a contradiction. Now, letting T_1 be any prime of Σ_P^* with $T_1 \supseteqq T^*$, T_1 is a spanning prime extending P^* and hence a finite A_P^*-module. This proves T^* is an A_P^*-lattice in Σ_P^*, so $T = T^* \cap \Sigma$ is an A_P-lattice in Σ by 3.3, (2), and (2) of Theorem 3.1 holds. (2) immediately implies (3) by Theorem

2.1. Finally, if (3) holds, suppose T is not a prime, and let T_1 be any prime of Σ containing T. Then $KT_1 \supset KT = \Sigma$ (as T is an A_P-lattice) so T_1 is a spanning prime and hence by what we just showed T_1 is a finite A_P-module. But T is a *maximal* finite A_P-module preprime by Theorem 2.1 so $T = T_1$, a contradiction. Thus 3.1 is proven.

REMARK. If Σ is a division algebra, (1)-(3) of Theorem 3.1 are equivalent to: T is a prime of Σ extending P and T consists of A_P-integral elements. For suppose this condition holds and let $KT = \Sigma_0 \subseteq \Sigma$. As Σ is a division algebra, Σ_0 is a division algebra with center $L \supseteq K$. Let $S = T \cap L$, a prime of L by Corollary 1.2, (4). $KT = \Sigma_0$ implies T is a spanning prime of Σ_0 (by Proposition 1.4) so (as A_S must again be a discrete rank one valuation ring) T is a finite A_S-module by 3.1. As $S \subseteq T$ all elements of S are A_P-integral so by [5, p. 151, Proposition 6], A_S is the integral closure of A_P in L. Therefore A_S and hence T is a finite A_P-module. But then $K \cdot T = \Sigma$ by 3.1 so (1) of 3.1 holds. Conversely if T satisfies (1) hence (3) of 3.1 then T is contained in an A_P-order of Σ so the elements of T are A_P-integral.

Theorem 3.1 essentially verifies Harrison's conjecture in [7, p. 13, footnote 3]. Explicitly:

THEOREM 3.4. *Let K be a field such that all its (nontrivial) valuations are discrete rank one, or equivalently such that all its finite primes are discrete rank one; for example, any global field. Let Σ be a central simple K-algebra. Then the spanning finite primes of Σ are the generators of the Brandt Groupoids over the nontrivial valuation rings of Σ. Specifically, if T is spanning then $T \cap K = P$ is a finite prime of K and T is a generator of the Brandt Groupoid of normal A_P-lattices in Σ.*

Proof. Immediate from Corollary 1.2 and Theorem 3.1.

Turning again to the situation of Theorem 3.1 we study the complete case more closely, with the aid of Rutherford's Theorem (Proposition 1.6), and obtain information on the groupoid generators, i.e., spanning primes in Σ, which divide the maximal ideal of a maximal order.

THEOREM 3.5. *Let Σ be a central simple K-algebra. Let P be a discrete rank one finite prime of K. Let Λ be a maximal A_P-order of Σ with unique maximal ideal $\mathfrak{p}$.*

(1) *The primes of Σ which contain $\mathfrak{p}$ are precisely those generators of the Brandt Groupoid of normal A_P-lattices which divide,*

i.e., contain $\mathfrak{p}$.

(2) *The map* $T \to {}^*(T \cap \Lambda)/\mathfrak{p}$ *gives one-to-one correspondence between the generators which divide* $\mathfrak{p}$ *and the set of finite primes of the finite dimensional simple* $k_P = \Lambda_P/P$*-algebra* $\bar{\Lambda} = \Lambda/\mathfrak{p}$, *which set is completely described by Rutherford's Theorem* (Proposition 1.6).

(3) *For each generator* T *which divides* $\mathfrak{p}$ *there is an integer* $r = r(T, \mathfrak{p}) \geqq 1$ *such that* T *can only appear as the* r*-th term in any factorization of* $\mathfrak{p}$ *as a product (in the groupoid) of generators.*

Proof. (1) is an immediate consequence of Theorem 3.1, as $T \supseteqq \mathfrak{p}$ implies $KT \supseteqq K\mathfrak{p} = \Sigma$ and $T \cap K \supseteqq \mathfrak{p} \cap K = P$. To prove (2) and (3) it suffices to consider the case when Λ_P is complete, for $M \to M \otimes \Lambda_P^*$ and $M^* \to M^* \cap \Sigma$ gives an isomorphism between the Brandt Groupoid in Σ over Λ_P and that in Σ_P^* over Λ_P^* (see § 11 of Chapter 6 of [6]). If Σ_P^* is a division algebra then $\mathfrak{p}$ is already a prime, $\bar{\Lambda}$ is a locally finite field and there is nothing to prove. Hence we assume Λ_P is complete and we identify Σ with $\mathrm{Hom}_D(V, V)$, D a central division algebra over K, V a right D-vector space with $2 \leqq \dim_D V < \infty$. Let Δ be the unique maximal Λ_P-order in D with unique maximal ideal $\pi\Delta = \Delta\pi$ (where π is not necessarily in K); Δ is a (noncommutative) discrete rank one valuation ring of D (cf. [11, Chap. 2]).

For M and N right Δ-submodules of V let

$$L(M, N) = \{a \in \Sigma \mid aM \subseteqq N\} .$$

Let Λ be the fixed maximal Λ_P-order of Σ. Then $\Lambda = L(E, E) \cong \mathrm{Hom}_\Delta(E, E)$ for a free Δ-submodule E of V with $\mathrm{rank}_\Delta E = n = \dim_D V$, and the unique maximal ideal $\mathfrak{p}$ of Λ i.e., the radical of Λ, equals $L(E, E\pi)$. Let Ω_E denote the set of all free, rank n, Δ-submodules F of V such that $F \subseteqq E$ but $F \not\subseteqq E\pi$.

CLAIM. (a) every maximal R-order Λ' equals $L(F, F)$ for a unique $F \in \Omega_E$; (b) every prime T of Σ with $T \supseteqq \mathfrak{p}$ has the form $T = L(W_T, U_T)$ for a unique pair of free, rank n, Δ-submodules of E, with $W_T \supseteqq U_T \supseteqq E\pi$ and $\mathrm{rank}_\Delta(W_T/U_T) = 1$.

Proof. (a) follows since $ED = V$ and $L(F, F) = L(F', F')$ if and only if $F' = F\pi^k$ for some k. For (b), let $O_l(T) = L(F, F)$ with $F \in \Omega_E$. Then $T \supseteqq \mathfrak{p}' = L(F, F\pi)$, the radical of $O_l(T)$, and $T/\mathfrak{p}'$ is a maximal left ideal of $O_l(T)/\mathfrak{p}' = \mathrm{Hom}_{\bar{\Delta}}(\bar{F}, \bar{F})$ where $\bar{F} = F/F\pi$ is an n-dimensional $\bar{\Delta} = \Delta/\pi\Delta$ vector space. But then $T/\mathfrak{p}' = \mathrm{Hom}_{\bar{\Delta}}(\bar{F}, \bar{U})$ for a uniquely determined $(n-1)$-dimensional $\bar{\Delta}$-subspace of $\bar{F}$. Letting $U \supseteqq F\pi$ be the unique Δ-submodule of F with $U/F\pi = \bar{U}$, we see that $T \subseteqq L(F, U)$; but $L(F, U)$ is a preprime (as $F \supsetneqq U$) so $T =$

$L(F, U)$. Letting $W_T = F$, $U_T = U$ we have $E \supseteq W_T \supseteq U_T$ and $\operatorname{rank}_\Delta W_T/U_T = 1$; it remains to show $U_T \supseteq E\pi$. Now as $W_T \in \Omega_E$, there exists $x \in W_T \backslash E\pi$. By Nakayama's Lemma, E has a free Δ-basis $x = x_1, x_2, \cdots, x_n$; then $E\pi = \sum x_i \pi \Delta$. For each i let $t_i \in L(E, E)$ be defined by $t_i x_j = \delta_{ij} x_i \pi$ (Kronecker δ). Then $t_i \in L(E, E\pi) = \mathfrak{p} \subseteq T$ so $x_i\pi = t_i x \in t_i W_T \subseteq U_T$ for $i = 1, \cdots, n$ proving $E\pi \subseteq U_T$. Assertion (b) is proven.

Now, if $T \supseteq p$ and $T = L(W_T, U_T)$ as in (b) above, let $\bar{W}_T = W_T/E\pi$, $\bar{U}_T = U_T/E\pi$. Then $(T \cap \Lambda)/\mathfrak{p} = \{\bar{a} \in \bar{\Lambda} = \Lambda/\mathfrak{p} \mid \bar{a}\bar{W}_T \subseteq \bar{U}_T\}$ which, by Rutherford's Theorem, is a prime of $\bar{\Lambda} = \operatorname{Hom}_{\bar{\Delta}}(\bar{E}, \bar{E})$ (where $\bar{E} = /E\pi$) since $\bar{W}_T \subseteq \bar{U}_T$ are $\bar{\Lambda}$-subspaces with $\dim_{\bar{\Delta}} \bar{W}_T/\bar{U}_T = 1$. Conversely, by lifting back to Λ and then extending to a prime of Σ, any prime of $\bar{\Lambda}$ has the form $(T \cap \Lambda)/\mathfrak{p}$ for some prime $T \supseteq \mathfrak{p}$. Thus $T \to (T \cap \Lambda)/\mathfrak{p}$ is onto the primes of $\bar{\Lambda}$; that the map is one-to-one follows from the uniqueness part of Rutherford's Theorem and the uniqueness of the representation of T as $L(W_T, U_T)$.

Thus (2) is proven. To prove (3), let $T \supseteq \mathfrak{p}$ and suppose $T = L(W_T, U_T)$ where W_T, U_T are chosen as in the claim above. We claim $r = \operatorname{rank}_{\bar{\Delta}}(W_T/E\pi)$ has the property claimed in (3). First, note that $O_r(T) = L(W_T, W_T)$ and $O_l(T) = L(U_T, U_T)$. In any factorization $\mathfrak{p} = T_1 \cdot \cdots \cdot T_n$, $O_r(T_i) = O_l(T_{i+1})$ so $W_{T_i} = U_{T_{i+1}}$ and the factorization corresponds to the chain $E\pi = U_{T_1} \subsetneq W_{T_1} = U_{T_2} \subsetneq \cdots \subsetneq W_{T_{n-1}} = U_{T_n} \subsetneq W_{T_n} = E$, with $\operatorname{rank}_\Delta(W_{T_i}/E\pi) = i$ as $\operatorname{rank}_\Delta W_{T_i}/W_{T_{i-1}} = 1$.

COROLLARY 3.6. *Suppose A_P/P is a finite field (which is always true for the classical fields). Then the maximal ideal $\mathfrak{p}$ of a maximal A_P-order Λ is divisible by only finitely many generators of the Brandt Groupoid over A_P (although there are in general (see § 4) infinitely many distinct maximal A_P-orders in Σ.)*

Proof. $\Lambda/\mathfrak{p}$ is a finite ring.

4. **The Non-split case; self conjugate primes.** In this section we study the special situation which arises when a discrete rank one prime P of K does not have infinitely many extensions to spanning primes of Σ, and give a characterization of division algebras of prime power degree.

THEOREM 4.1. *Let Σ be a central simple K-algebra, and P a discrete rank one finite prime of K. Then the following four conditions are equivalent:*

(1) *Σ contains only finitely many spanning primes extending P;*

(2) *there is a unique prime T of Σ extending P;*

(3) *Σ_P^* is a division algebra (where $\Sigma_P^* = \Sigma \otimes K_P^*$, the P-adic completion);*

(4) *there is a prime T of Σ extending P which is "self-conjugate" in Σ, i.e., $aTa^{-1} = T$ for all units $a \in \Sigma$.*

Moreover, the following two conditions are equivalent and are implied by the first four; they are equivalent to the first four if K is a global field:

(5) *every prime T of Σ extending P is spanning;*

(6) *Σ is a division algebra and P has a unique extension to each subfield L of Σ containing K.*

Remarks. In condition (5), "is spanning" can be replaced by "is a finite A_P-module" or by "consists of A_P-integral elements". (2), (3) and either one of these alternate versions of (5) are equivalent when Σ is merely simple and separable, e.g., when Σ is a separable field extension of K.

We will say P is *nonsplit in Σ* if any of (1)–(4) above hold.

Proof. By § 3 there is a one-to-one correspondence between the spanning primes of Σ extending P and the spanning primes of the P-adic completion Σ_P^* of Σ which extend P^* (the prime of K_P^*). Either there is exactly one maximal A_P^*-order in Σ_P^* or there are infinitely many, according as Σ_P^* is a division algebra or is not. With 3.1, 3.2 and the remark at the end of § 2, this implies that Σ_P^* contains exactly one prime, or contains infinitely many spanning primes according as it is a division algebra or not. Thus (1) is equivalent to (3). Clearly (2) implies (1); (3) implies (2) for if T_1 is any prime of Σ extending P then by Lemma 3.3 (1), $T_1 \cdot A_P^*$ is a preprime of Σ_P^* which extends P^*, so $T_1 \cdot A_P^* \subseteqq T^*$ the unique prime in Σ_P^* extending P^*, hence $T^* \cap \Sigma \supseteqq T_1$ which implies (as $T^* \cap \Sigma$ is a preprime) $T_1 = T^* \cap \Sigma$, the unique spanning prime of Σ extending P. Thus (1), (2), and (3) are equivalent.

(2) clearly implies (4). Suppose (4) holds and let T be self conjugate. Suppose that (3) does not hold, i.e., that Σ_P^* is not a division algebra. Then there are infinitely many maximal A_P-orders in Σ which are all conjugate under inner automorphisms of Σ (by Proposition 3.5 of [4]) and hence (using remark at end of § 2 and Th. 3.1) given any spanning prime it has infinitely many distinct conjugates. Thus T cannot be spanning. But we show that it is: for let $\Sigma_0 = K \cdot T = \{\sum \alpha_i t_i \mid \alpha_i \in K, t_i \in T\}$, the K-subalgebra generated by T (as $T \cdot T \subseteqq T$). We assert that $K \cdot T$ contains every unit of Σ. If so, we are done, as one checks Σ has a basis consisting of units. Let u be a unit in Σ and suppose $u \notin KT$. Then $u \notin A_T$ (as $T \cap K = P \neq 0$ implies $A_T \subseteqq KT$) so $uT = Tu \nsubseteqq T$ and there exists $t \in T$ with

$ut \notin T$; but $u^{-1}(ut) \in T$ and $u^{-1}TuT = T \cdot t \subseteqq T$ so by Lemma 1.1, $u^{-1} \in T \subseteqq KT$. But KT is a K-subalgebra of Σ so $u^{-1} \in KT$ implies $u \in KT$, a contradiction. This completes the proof of the equivalence of conditions (1) to (4).

(5) is equivalent to (6): if (5) holds then Σ must be a division algebra, for otherwise there exists $a \in \Sigma$ with $a^2 = 0$ and then $P + Ka$ is a preprime of Σ containing P which is not a finite A_P-module, so cannot be contained in a spanning prime. (5) is equivalent to the assertion that every preprime T of Σ containing P is a finite A_P-module, hence in particular every prime of a subfield $L \supseteqq K$ of Σ which extends P must be a finite A_P-module. But this implies, by [5, p. 151, Proposition 6] that P has a unique extension to each such L, and (6) holds. Now suppose (6) holds and suppose T is a prime of Σ extending P. Each $x \in T$ is in the unique extension of P to the subfield $K(x)$ of Σ, and so x is integral over A_P by the result of [5] just quoted. Hence T is spanning by the remark following Theorem 3.3.

Clearly (2) implies (5) so any one of the first four conditions implies the last two. We conclude by showing that if K is a global field (i.e., an algebraic number field or an algebraic function field over a finite field) then (6) implies (3), so that all the conditions are equivalent. Suppose then (6) holds and suppose that Σ_P^* is not a division algebra.[1] Let n be the degree of $\Sigma (n^2 = [\Sigma : K])$. We have $\Sigma_P^* \cong (D)_k$, $k > 1$ and degree $D = m < n$, with $m \mid n$. Let $P = P_0, P_1, \cdots, P_s$ be a finite set of finite primes of K including all the finite primes Q at which Σ is not unramified, i.e., all those Q with Σ_Q^* not split. By the Grunwald-Wang Theorem [3, p. 106, Th. 5] there exists a normal field extension L of K (which is even a cyclic extension) with the following properties (letting $n_P = [L_S^* : K_P^*]$ for S any extension of P to L): $n_P = m$, $n_{P_i} = n$ for $i = 1, \cdots, s$, $n_Q = 2$ for each real infinite prime Q of K for which Σ_Q^* is not split, *and* $[L : K] = n$. Then by construction, for every finite or real infinite prime Q of K, the Q-index of Σ (i.e., the index of Σ_Q^*) divides the Q-degree of L over K. Thus the Q-index of $\Sigma \otimes_K L$ is 1 for all Q and $\Sigma \otimes_K L \cong (L)_n$ by Hasse's theorem ([12, p. 206, Th. 2]). But then by [6, p. 46, Satz 14] and the fact that $[L : K] = n =$ degree of Σ, L is isomorphic to a maximal subfield of Σ. Therefore, P has a unique extension to a prime of L, which implies the P-degree of L over K must be n (as the P-degree $= \mathrm{e} \cdot \mathrm{f}$ which equals n as $efg = n$, $g = 1$) a contradiction to our construction of L with P-degree $= m < n$.

REMARK. The equivalence of (2) and (5) when K is a global field shows that in general there exist nonspanning primes in Σ, see § 6.

[1] The following argument was suggested by M. Schacher.

PROPOSITION 4.2. *Let Σ, K and P be as in Theorem* 4.1 *and suppose P is nonsplit in Σ. Let T be the unique prime of Σ extending P. Then A_T is the unique maximal A_P-order in the division algebra Σ, T is its unique maximal ideal (one or two sided). The Brandt Groupoid over A_P in Σ is the cyclic group consisting of all powers of T. Moreover, A_T is a (noncommutative) discrete rank one valuation ring of Σ (see* [11]*), with T its ideal of nonunits. $k_T = A_T/T$ is a finite field extension of $k_P = A_P/P$, the value group Γ_T of the valuation associated with A_T is a finite extension of the value group Γ_P of the A_P valuation, and $[\Gamma_T\colon \Gamma_P]\cdot[k_T\colon k_P] = [\Sigma\colon K]$ (i.e., "$ef = n$").*

Proof. It suffices to prove the assertions of the last two sentences, the rest being immediate consequences of previous results. As $xA_Tx^{-1} = A_T$ for all $x \neq 0$ in A_T, to show A_T is a valuation ring we need only show $x \notin A_T$ implies $x^{-1} \in A_T$. But $x \notin A_T$ implies (as $xT = Tx$) that $xT \not\subseteq T$, say $xt \notin T$ for $t \in T$. Then $x^{-1}xt \in T$ and $x^{-1}Txt \subseteq T$ so by Lemma 1.1, $xt \notin T$ implies $x^{-1} \in T$, as required. The associated valuation is discrete rank one since T is a principal ideal of A_T by Corollary to Proposition 3.3 of [4]. By hypothesis Σ_P^* is a division algebgra. $T^* = T\cdot A_P^*$ is the prime of Σ_P^* extending $P^* = P\cdot A_P^*$ and A_T^* is a (noncommutative) valuation ring of Σ_P^* with $[\Gamma_{T^*}\colon \Gamma_{P^*}]\cdot[k_{T^*}\colon k_{P^*}] = [\Sigma_P^*\colon K_P^*]$ ([11, p. 54, Th. 11]). But $A_{T^*}/T^* \cong A_T/T$ (see [6]) and $A_{P^*}/P^* \cong A_P/P$, and also $P\cdot A_T = T^e$ and $P^*\cdot A_{T^*} = (T^*)^e$ so by order theory (see [6]) $[\Gamma_{T^*}\colon \Gamma_{P^*}] = e = [\Gamma_T\colon \Gamma_P]$, proving the last assertion.

We conclude this section by showing that over a global field the existence of a self conjugate finite *or infinite* prime characterizes the division algebras among all central simple algebras of prime power degree. Indeed when char $(K) \neq 0$ and K has only discrete rank one valuations, Theorem 4.1 shows this result is equivalent, for algebras of prime degree, to the Hasse local splitting theorem (i.e., "Σ is a matrix algebra if and only if Σ_P^* is a matrix algebra for all primes P of K"). This suggests proving the Hasse splitting theorem for, say, (generalized) quaternion algebras over an arbitrary field of nonzero characteristic whose valuations are discrete rank one by directly proving the existence of a self-conjugate prime in such algebras. The author is indebted to D. K. Harrison for these observations and for conjecturing the following result.

PROPOSITION 4.3. *Let K be a global field. Let Σ be a central simple K-algebra of degree p^k where p is a prime number. If $K = Q$ or* char $(K) \neq 0$, *then Σ is a division algebra if and only if there exists a self-conjugate prime in Σ.*

More generally, if K is any global field then Σ is a division algebra if and only if Σ contains a self conjugate prime T, finite or infinite.

Proof. First suppose Σ is a division algebra. The degree of Σ = exponent of Σ (in the Brauer Group of K) = the least common multiple of the P-exponents m_p of Σ, i.e., of the exponents of the completions Σ_P^* of Σ at the primes P (finite and real infinite) of K. But all the P-exponents are divisors of p^k, hence powers of p, and so for some P, the P-exponent of Σ *equals* p^k, i.e., the index of Σ_P^* is p^k. Since p^k is the degree of Σ_P^*, Σ_P^* is a division algebra. If P is a finite prime we are done; when char $(K) = p \neq 0$ this must happen. So suppose char $(K) = 0$ and P is real infinite. If $K = \boldsymbol{Q}$, so that P is the unique infinite prime of $\boldsymbol{Q}$, then $\Sigma_P^* = H$ the ordinary (Hamiltonian) quaternions, so degree $\Sigma = 2$, and since by Hasse Reciprocity $\sum_{\text{all}P}(\Sigma \mid P) \equiv 0 \pmod 1$ (where $(\Sigma \mid P)$ is the Hasse invariant of Σ at P), there must exist a finite prime P' with $(\Sigma \mid P) \not\equiv 0 \pmod 1$, hence with $m_{P'} > 1$, hence with $m_{P'} = 2$ (as $m_{P'} \mid$ degree Σ) hence with $\Sigma_{P'}^*$ a division algebra. Finally suppose K is any algebraic number field. We have Σ_P^* a division algebra, i.e., $\Sigma_P^* = H$. Then degree $\Sigma = 2$, Σ is a (generalized) quaternion division algebra over K. We assert that P is in fact an (infinite) prime *of* Σ and hence (as $P \subseteqq K$) a self-conjugate prime of Σ as required. Suppose $P \subsetneqq T$ a prime of Σ. Then (as P is a prime of K) $T \not\subseteqq K$, so let $a \in T \backslash K$. The subfield $K(a)$ of Σ is a quadratic extension of K, in fact $K(a) = K(b)$ for some $b \in \Sigma$ with $b^2 \in K$. Let T_0 be any infinite prime of $K(b)$ containing a and extending P (T_0 exists as a and P are in the preprime $T \cap K(b)$). By [7], T_0 is an archimedean order in the subfield L of $K(b)$ which it generates; but (as P is real infinite so is the cone of an ordering of K—see [7]) $L \supseteqq K$ and (as $a \in T_0$) $a \in L$ so $L = K(a) = K(b)$. Hence T_0 is an order in $K(b)$ so $b^2 \in T_0$, hence in $T_0 \cap K = P$. But now consider $\sum_P^* = H$, and identify K with a subfield of $\boldsymbol{R}$ via the unique isomorphism $K \rightarrow T$ which sends P into $\boldsymbol{R}^+$, the non-negative reals. Then $b \in H$ and $b^2 = r \in P \subseteqq \boldsymbol{R}^+$, and $r \neq 0$. Hence $r = t^2$ for some real number t and we have $(b - r)(b + r) = 0$ with $b - r$ and $b + r \neq 0$ as b is not in the center K of Σ, so not in the center $\boldsymbol{R}$ of H, which is a contradiction since H is a division algebra.

Now suppose Σ is any central simple algebra over the global field K of arbitrary degree, and suppose T is a self-conjugate prime of Σ. We show Σ must be a division algebra. If T is finite then we are done, by Theorem 4.1 (for condition (4) of 4.1 then holds with $P = K \cap T$). Hence suppose T is infinite and suppose $\Sigma \cong (D)_n$ with $n > 1$, D a central K-division algebra. First, if $T \subseteqq K$ then for any

$a \in \Sigma$ with $a^2 = 0$, $T + Ka$ is a preprime properly containing T, a contradiction. Thus $T \not\subseteq K$. Let $T^+ = \{a \in T \mid -a \notin T\}$. Then by Proposition 1.6 of [7], $G = T^+ \cap U(\Sigma)$ is a multiplicative subgroup of $U(\Sigma)$, the units of Σ, which is $GL(n, D)$. Moreover, G is a normal subgroup of $GL(n, D)$ since $aTa^{-1} = T$ implies $aT^+a^{-1} = T^+$ for all $a \in U(\Sigma)$. G is not contained in the center $K^\times$ (multiplicative group of K) (for let $a \in T \backslash K$, and choose n a positive integer such that $-n$ is not an eigenvalue of the matrix $a \in (D)_n$, then $a + n \cdot I \in G \backslash K$.) Hence by Theorem 4.9 of [2], $G \supseteq SL(n, D)$ the unimodular group and hence for all $a \in U(\Sigma)$, $a \in G$ if and only if $\det a \in \det G = \{\det b \mid b \in G\} \subseteq D^\times/(D^\times)'$ (commutator factor group of $D^\times$). If n is even we are done immediately, for then $\det(I) = \det((-1) \cdot I)$ (I = identity of Σ) so $-I \in G \subseteq T^+ \subseteq T$ a contradiction. So suppose n is odd. Then $\det(I) = \det(\text{diag}\{1, \cdots, 1\}) = \det(\text{diag}\, -1, \cdots, -1, 1\})$ (since $(-1)^{n-1} = 1$ if n is odd) and hence $\text{diag}\{-1, \cdots, -1, 1\} \in G \subseteq T^+$. Then $\text{diag}\{0, \cdots, 0, 1\}$, which is the matrix unit ε_{nn}, is in $T^+ + T^+ \subseteq T^+$. As T^+ is self-conjugate this implies $\varepsilon_{ii} \in T^+$ for $i = 1, \cdots, n$. Finally, as for $i \neq j$, $\det(I + \varepsilon_{ij}) = 1 = \det(I - \varepsilon_{ij})$, both $I + \varepsilon_{ij}$ and $I - \varepsilon_{ij}$ are in T^+, hence (multiply by ε_{ii} on left, ε_{jj} on right) both ε_{ij} and $-\varepsilon_{ij}$ are in T^+, contradicting the definition of T^+. The proof is complete.

5. **Miscellaneous results.** In this brief section we prove the analogue, for a central simple algebra Σ over a global field K, of the fact that each unit (i.e., nonzero element) of K is contained in only finitely many primes of the field, and we discuss the topology on the space of all finite primes of Σ.

Let $X_S(\Sigma, P) = X_S(P)$ be the set of spanning primes of Σ which extends the finite prime P of K. $X_S(P) \neq \varnothing$ by Proposition 1.4.

PROPOSITION 5.1. *Let Σ be a central simple K-algebra, let P be a discrete rank one finite prime of K. Any two elements of $X_S(P)$ are conjugate under a K-automorphism of Σ. If $X_S(P)$ is infinite, then*

$$P = \bigcap \{T \mid T \in X_S(P)\}, \quad A_P = \bigcap \{A_T \mid T \in X_S(P)\}.$$

Proof. The first assertion follows from Theorem 3.1, [2, Proposition 3.5], and the fact that maximal left ideals in a fixed maximal order are conjugate. The second assertion follows from the corresponding assertion about $X_S(\Sigma_P^*, P^*)$ (P-adic completions), which holds as Σ_P^* is not a division algebra by Theorem 4.1.

PROPOSITION 5.2. *Let K be a global field, Σ a central simple*

K-algebra. For $a \in \Sigma$, a is an element of some $T \in X_S(\Sigma, P)$ for at most finitely many primes P of K if and only if a is a unit in Σ.

Proof. Let $f(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$ be the minimum polynomial for a over K; a is a unit of Σ if and only if $\alpha_n \neq 0$. The set $\{\alpha_1, \cdots, \alpha_n\} \subseteq A_P$ for all but a finite number of finite primes P of K, as K is a global field. If $\{\alpha_1, \cdots, \alpha_n\} \subseteq A_P$ then $a \in T$ for a spanning prime T of Σ extending P if and only if $\alpha_n \in P$. For, $a \in T$ implies $\alpha_n = -a^n - \alpha_1 a^{n-1} - \cdots - \alpha_{n-1} a \in A_P \cdot T \subseteq T$ so $\alpha_n \in T \cap K = P$, while conversely if $\alpha_n \in P$, $a \cdot A_P[a]$ is a finitely generated A_P-module (since a is integral over A_P by hypothesis) and a preprime (as it is a proper ideal); therefore by § 2 and § 4, $a \cdot A_P[a]$, and hence a, is contained in a spanning prime extending P. Thus a can be in some $T \in X_S(\Sigma, P)$ for infinitely many P if and only if $\alpha_n \in P$ infinitely many P if and only if $\alpha_n = 0$.

We recall the topology on the space $Y(\Sigma)$ of all primes of Σ, as defined in [7]. A subbase for the open sets consists of the sets $W(a) = \{T \in Y(\Sigma) \mid a \notin T\}$ for all $a \in \Sigma$. The topology is T_1 and is not Hausdorff (in general $Y(R)$ is Hausdorff if and only if R is a generalized Boolean ring: for all $a \in R$ there exists $n > 1$ with $a^n = a$). $Y(\Sigma)$ and the subspace $X(\Sigma)$ of all finite primes are both (quasi-) compact. A nonempty subset U of a topological space X is called *irreducible* if and only if U is not the union of two nonempty closed proper subsets (or, every nonempty open subset is dense)

PROPOSITION 5.3. *Let $X_S(\Sigma)$ denote the space of spanning finite primes of the central simple K-algebra Σ, K a global field. Then $\bigcap \{T \mid T \in X_S(\Sigma)\} = \{0\}$. $X_S(\Sigma)$ is a dense irreducible subset of $X(\Sigma)$ and $Y(\Sigma)$; thus the latter spaces are irreducible.*

Proof. The first assertion follows from Proposition 5.1, the observation that Σ_P^* is a division algebra for at most finitely many P, and the corresponding fact for K. For the second assertion it suffices to show: if $E = \{a_1, \cdots, a_n\}$ is any finite set of nonzero elements of Σ then there exists $T \in X_S(\Sigma)$ with $T \cap E = \varnothing$. Let $f_i(x)$ be the minimal K-polynomial for a_i, with constant term α_i. If all the $\alpha_i \neq 0$ then choosing $P \in X(K)$ with $f_i(x) \in A_P[x]$ for all i but with $\alpha_i \notin P$ for all i we have $T \cap E = \varnothing$ for any spanning prime T of Σ extending P, by the argument of the proof of 5.2. In particular this proves the assertion when Σ is a division algebra. If some $\alpha_i = 0$ then $\Sigma \cong (D)_n$, $n > 1$. Since the a_i are nonzero one can choose a matrix representation for Σ over D in which the matrices for the a_i all have nonzero last columns. Let $E_0 = \{\delta \in D \mid \delta \neq 0, \ \delta$ is a last-column entry in the matrix of some $a_i\}$. By the first argument, there exists a spanning prime T_0 of D with $T_0 \cap E_0 = \varnothing$. Let T be

the set of matrices with last column entries in T_0, all other entries in $\Lambda_0 = O_l(T_0)$. One checks T is a maximal left ideal of the maximal order $(\Lambda_0)_n$ in $(D)_n \cong \Sigma$, hence T is a spanning prime of Σ by 4.1. By construction, $T \cap E = \varnothing$, and we are done.

6. Examples. In this section we give some examples of finite primes in simple algebras which are not spanning primes of the algebra.

The first set of example arises from an important description of finite primes containing idempotents, due to M. E. Manis (unpublished).

PROPOSITION 6.1. *Let R be a ring, let e be an idempotent of R, let $f = 1 - e$.*

(a) *Let $P = ePe$ be a finite prime of the ring eRe, with unit element e. A finite prime of R may be constructed as follows: let M_0 be any additive subgroup of eRf; let $N = \{x \in fRe \mid M_0 x \subseteq ePe = P\}$, let $M = \{x \in eRf \mid xN \subseteq P\}$ and finally let $B = \{x \in fRf \mid xN \subseteq N\}$. Then $T = B + N + M + P = fBf + fNe + eMf + ePe$ is a finite prime of R. Note that $f \in T$, $e \notin T$.*

(b) *If T is any prime of R with $f \in T$, then $eTe = P$ is a finite prime of eRe; T can be recovered from P and, say, $M_0 = eTf$ by the construction in (a).*

Proof. Straightforward checking.

Manis showed that in case R is a full matrix ring over a locally finite field k the above construction, with e any idempotent of rank one, yields all the finite primes of R, giving an approach to the description of the primes of R differing from that in [10].

Applying Proposition 6.1 to the construction of nonspanning primes in a matrix algebra $\Sigma = (D)_n$, $n > 1$ over a division ring D, let S be a finite prime of the center K of D, let P be any prime of D extending S. Let $\{e_{ij} \mid 1 \leqq i, j \leqq n\}$ be a set of matrix units in Σ. In the notation of 6.1, let $e = e_{nn}$, let $M_0 = \{0\}$. Then $N = f\Sigma e$, $M = \{0\}$, $B = f\Sigma f$. One checks that T is the set of matrices with arbitrary entries in the first $n - 1$ rows, and 0 entries in all but the n-th column of the n-th row, the (n, n) entries being in P. Clearly T does not span Σ over K.

The preceding construction yields nonspanning primes in Σ whether or not D contains nonspanning primes. In case D is a noncommutative central K-division algebra for K an algebraic number field, the existence of nonspanning primes in D follows from Theorem 4.1, or more directly from the fact that for any subfield L of D properly containing K, there are finite primes P of K which split in L. For to say P splits in L is to say that the primes $S_1, \cdots, S_k$ of

L extending P are not integral over A_P, so that if T is any prime of Σ extending S_1, say, T cannot be integral over A_P, hence (by 4.1) T cannot be a spanning prime.

We now give a final example which shows that a prime of a central simple algebra may span a "small" subalgebra. Let K be any (nonlocally finite) field, L a cyclic Galois extension of K with group $G = \langle\sigma\rangle$ of order n. Let $\Sigma = (L, \sigma, a)$ be a cyclic algebra ($\Sigma = \sum \bigoplus_{i=0}^{n-1} Lu^i$ with $u^i\alpha = \sigma^i(\alpha)u^i$ for $\alpha \in L$ and $u^n = a \in K$—see [1] or [4]). Suppose P is a finite prime of K which splits completely in L, i.e., P has n distinct extensions $T_1, \cdots, T_n$ to a prime of L. Then each T_i is a prime *of* Σ, with $K \cdot T_i = L$, $[L: K] = n = [\Sigma: K]^{1/2}$. Such primes exist in any algebra Σ central simple over a global field K, as Σ is then a cyclic algebra (see [1] or [6]), say $\Sigma = (L, \sigma, a)$ for some cyclic extension L of K, and it can be shown (e.g., using the zeta function) that there exist in fact infinitely many finite primes of K which split completely in L.

The author wishes to thank Professor Harrison who directed the thesis, from part of which this paper was developed. His enthusiasm and imagination were invaluable and the germs of many ideas herein were his.

BIBLIOGRAPHY

1. A. A. Albert, *Structure of Algebras*, A. M. S. Colloq. Pub. **24**, Amer. Math. Soc., Providence 1961.
2. E. Artin, *Geometric Algebra*, New York, 1957.
3. E. Artin and J. Tate, *Classified Theory*, Benjamin, New York, 1967.
4. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960) 1-24.
5. N. Bourbaki, *Algebre Commutative*, Chaps. 5 et 6 A. S. I. 1308, Hermann, Paris, 1964.
6. M. Deuring, *Algebren*, Springer Verlag, Berlin, 1968.
7. D. K. Harrison, *Finite and infinite primes for rings and fields*, Memoirs Amer. Math. Soc. **68** (1966).
8. N. Jacobson, *Theory of Rings*, Amer. Math. Soc. Survey **11**, A. M. S. Providence, 1943.
9. ———, *Structure of Rings*, Amer. Math. Soc. Colloq. Pub. **37**, Amer. Math. Soc. Providence, 1956.
10. H. Rutherford, *Characterizing primes in some non commutative rings*, Pacific J. Math. **27** (1968), 387-392.
11. O. F. G. Schilling, *The Theory of Valuations*, Amer. Math. Soc. Survey **4**, Amer. Math. Soc. New York, 1950.
12. A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1967.

Received August 11, 1969. Supported by N. S. F. Grant #GP-5340 and by a postdoctoral fellowship at the University of Illinois.

UNIVERSITY OF OREGON EUGENE, OREGON
UNIVERSITY OF ILLINOIS URBANA, ILLINOIS

PACIFIC JOURNAL OF MATHEMATICS

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 36, No. 1 November, 1971

Norman Larrabee Alling, *Analytic and harmonic obstruction on nonorientable Klein surfaces* 1
Shimshon A. Amitsur, *Embeddings in matrix rings* 21
William Louis Armacost, *The Frobenius reciprocity theorem and essentially bounded induced representations* 31
Kenneth Paul Baclawski and Kenneth Kapp, *Topisms and induced non-associative systems* 45
George M. Bergman, *The index of a group in a semigroup* 55
Simeon M. Berman, *Excursions above high levels for stationary Gaussian processes* 63
Peter Southcott Bullen, *A criterion for n-convexity* 81
W. Homer Carlisle, III, *Residual finiteness of finitely generated commutative semigroups* 99
Roger Clement Crocker, *On the sum of a prime and of two powers of two* 103
David Eisenbud and Phillip Alan Griffith, *The structure of serial rings* 109
Timothy V. Fossum, *Characters and orthogonality in Frobenius algebras* 123
Hugh Gordon, *Rings of functions determined by zero-sets* 133
William Ray Hare, Jr. and John Willis Kenelly, *Characterizations of Radon partitions* 159
Philip Hartman, *On third order, nonlinear, singular boundary value problems* 165
David Michael Henry, *Conditions for countable bases in spaces of countable and point-countable type* 181
James R. Holub, *Hilbertian operators and reflexive tensor products* 185
Robert P. Kaufman, *Lacunary series and probability* 195
Erwin Kreyszig, *On Bergman operators for partial differential equations in two variables* 201
Chin-pi Lu, *Local rings with noetherian filtrations* 209
Louis Edward Narens, *A nonstandard proof of the Jordan curve theorem* 219
S. P. Philipp, Victor Lenard Shapiro and William Hall Sills, *The Abel summability of conjugate multiple Fourier-Stieltjes integrals* 231
Joseph Earl Valentine and Stanley G. Wayment, *Wilson angles in linear normed spaces* 239
Hoyt D. Warner, *Finite primes in simple algebras* 245
Horst Günter Zimmer, *An elementary proof of the Riemann hypothesis for an elliptic curve over a finite field* 267