PACIFIC JOURNAL OF MATHEMATICS
Vol 109, No. 1, 1983

REALIZING CENTRAL DIVISION ALGEBRAS

R. S. PIERCE AND C. VINSONHALER

Let D be a finite dimensional division algebra over the rational field. We consider the question: for which primes p is D isomorphic to the quasi-endomorphism algebra of a p-local torsion free abelian group G whose rank is equal to the dimension of D? We show that D can be realized in this way for exactly those primes p such that $\hat{Q}_p \otimes D$ is not a product of division algebras.

1. Introduction. The question "which finite dimensional algebras over the field of rationals Q can be realized as quasi-endomorphism algebras of finite rank torsion free groups?" was first posed in [**3**]. The answer "all such algebras" came two years later in [**6**] as a corollary to Corner's Theorem: If R is a reduced, torsion free ring with rank $R = n < \infty$, then R is isomorphic to the endomorphism ring of a torsion free group G of rank $2n$. Corner also showed that it is not always possible to realize such a ring by the endomorphisms of a group of rank less than $2n$. However, in [**12**] Zassenhaus showed that if R is free as an abelian group, then the group G could be chosen to have rank n. Butler [**5**] showed that the same result is true under the weaker hypothesis that R is locally free. It follows from the theorems of Zassenhaus and Butler that every n dimensional rational algebra is the quasi-endomorphism algebra of a group G of rank n. This paper considers the question of what occurs when G is required to be p-local, that is $qG = G$ for all primes $q \neq p$.

Problem. For a finite dimensional, rational divison algebra D find all primes p such that there is a p-local group G with rank $G =$ dimension D and with D isomorphic to the ring of quasi-endomorphisms of G.

Our main result is that such a group G exists for exactly those primes p such that $\hat{Q}_p \otimes D$ is not a product of division algebras.

§§2, 3, and 4 of the paper set up some machinery that is used to construct groups with the required properties. The ideas described in these Sections are variations on standard themes, but for convenience, the proofs of the needed results are sketched. The main theorem is proved in §5.

NOTATION. The symbols Z, Q, F_p, $\hat{Z}_p$, and $\hat{Q}_p$ respectively denote the ring of integers, the field of rational numbers, the prime field of order p, the ring of p-adic integers, and the field of p-adic numbers. All groups under consideration are abelian and torsion free. Usually they have finite rank. Groups are generally denoted by G or H. The unadorned symbols $\otimes$ and Hom denote the tensor product and homomorphism functors in the category of abelian groups. The applications of these functors in other categories are distinguished by the usual subscripts. The expression $E(G)$ denotes the endomorphism ring of G, that is, $\mathrm{Hom}(G, G)$ with the usual ring structure. The prefixes rank and dim indicate the Z module rank and Q space dimension.

The expression QG can be interpreted as $Q \otimes G$ or the divisible hull of G. In both cases, we consider G as a subgroup of QG such that G is full in QG, that is, if $z \in QG$, then there is a natural number n such that $nz \in G$. We write $QE(G)$ for the quasi-endomorphism ring of G. Formally, $QE(G) = Q \otimes E(G)$. Alternatively, $QE(G)$ can be identified with $\{\phi \in E(QG) \mid n\phi \in E(G)$ for some natural number $n\}$. From both viewpoints, $QE(G)$ is a rational algebra, and we will always consider $E(G)$ as a full subring of $QE(G)$.

If X is any group (or ring), the expressions $\hat{X}$ or $\hat{X}_p$ will denote the $\hat{Z}_p$ module $\hat{Z}_p \otimes X$, except as noted in §4. We will consistently identify X with the subgroup $1 \otimes X \subset \hat{X}$. The identification of G with a subgroup of $\hat{G}$ is accompanied by an identification of $E(G)$ with a subring of $E_{\hat{Z}_p}(\hat{G})$: every $\phi \in E(G)$ extends uniquely to a $\hat{Z}_p$ module endomorphism of $\hat{G}$, namely $1 \otimes \phi$.

The letter D will always denote a rational division algebra that is finite dimensional over Q. In order to avoid uninteresting anomalies, assume that $\dim D > 1$. Since D is torsion free and divisible, the $\hat{Z}_p$ algebra $\hat{D}$ is actually a $\hat{Q}_p$ algebra. In fact, $\hat{D} = \hat{Z}_p \otimes D = \hat{Q}_p \otimes_Q D$. As we noted above, $E(D) = QE(D)$ will be considered as a subring of $E_{\hat{Z}_p}(\hat{D}) = E_{\hat{Q}_p}(\hat{D})$.

2. Constructing groups. If $D = QE(G)$ is a division algebra, then QG is a non-zero left D space, so that $\operatorname{rank} G = \dim QG \geq \dim D$. Our interest is in groups G such that $\operatorname{rank} G = \dim D$. In this case, D and QG are isomorphic as left D modules. Moreover, with a rational adjustment, the isomorphism will map the identity element 1 of D into G. These remarks lead to the following special case of a theorem due to J. D. Reid [**11**].

PROPOSITION 2.1. *If $QE(G)$ is isomorphic to the division algebra D such that* rank $G = \dim D$, *then G is isomorphic to a full subgroup G' of D with the identity* 1 *of D in G'; and $E(G) \cong R(G') = \{d \in D \mid dG' \subset G'\}$ is a full subring of D.*

This result permits us to restrict our attention to certain subgroups of D. It is convenient to introduce notation for this class. For each prime p, denote by $\Gamma_p(D)$ the set of subgroups G of D such that (1) $R(G) = \{d \in D \mid dG \subset G\}$ is a full subring of D, (2) G is p-local, and (3) $1 \in G$.

In case $G \in \Gamma_p(D)$ also satisfies $QE(G) \cong D$, we will say that G *p-realizes D*, and D is p-realizable if it is p-realized by some G.

The conditions (1), (2), and (3) do not guarantee that every G in $\Gamma_p(D)$ satisfies $QE(G) \cong D$. However, condition (1) implies that $QE(G)$ contains a subalgebra that is isomorphic to D.

LEMMA 2.2. *If λ is the left regular representation of D in $E(D)$, then $\lambda(D) \subset QE(G)$ for all $G \in \Gamma_p(D)$.*

Proof. If $d \in D$, then $md \in R(G)$ for some natural number m. Consequently, $m\lambda(d)(G) = \lambda(md)(G) \subset G$. Thus, $\lambda(d) \in QE(G)$.

It follows from this lemma (by dimension counting) that a group G in $\Gamma_p(D)$ will p-realize D if and only if $QE(G) = \lambda(D)$. It is this condition that we must satisfy. Usually, $\lambda(D)$ will be identified with D, so that our aim is to construct $G \in \Gamma_p(D)$ such that $QE(G) = D$.

The proof of the principal result in §5 is based on a familiar connection between the quasi-equality classes of groups in $\Gamma_p(D)$ and the left ideals of $\hat{D}$. (See [**4**] and [**8**].) For the reader's convenience we describe this correspondence and sketch the proofs of its properties.

For each $G \in \Gamma_p(D)$, let $L(G) = d(\hat{Z}_p \otimes G)$, the maximal divisible subgroup of $\hat{G}$.

LEMMA 2.3. *If $G \in \Gamma_p(D)$, then $L(G)$ is a left ideal of $\hat{D}$.*

Proof. Since G is a left $R(G)$ module, $\hat{G}$ is a left $R(G)\hat{}$ module. The facts that $L(G)$ is fully invariant in $\hat{G}$ and is divisible imply that $L(G)$ is a left $QR(G)\hat{} = \hat{D}$ module.

Groups G and H such that $QG = QH$ are quasi-equal if $mG \subset H$ and $mH \subset G$ for some natural number m. If G and H are quasi-equal, then $QE(G) = QE(H)$. Thus, we can limit our attention to quasi-equality classes of groups.

LEMMA 2.4. *If G, H in $\Gamma_p(D)$ are quasi-equal, then $L(G) = L(H)$.*

Proof. Without loss of generality, it can be assumed that $mG \subset H \subset G$ for some natural number m. In this case, $d(\hat{G}) = d(m\hat{G}) \subset d(\hat{H}) \subset d(\hat{G})$.

Lemmas 2.3 and 2.4 show that $G \to L(G)$ induces a mapping from quasi-equality classes in $\Gamma_p(D)$ to left ideals of $\hat{D}$. We will construct an inverse of this mapping.

Let S be a full Z_p order in D: S is a full subring (with identity) of D that is finitely generated (hence free) as a Z_p module. For each left ideal L of $\hat{D}$, define $G(L) = (\hat{S} + L) \cap D$. Recall that D is identified as a subgroup of $\hat{D}$.

LEMMA 2.5. *If L is a left ideal of $\hat{D}$, then $G(L) \in \Gamma_p(D)$.*

Proof. Since L is a left ideal of $\hat{D}$, it follows that $S \subset R(G(L))$. Thus, $R(G(L))$ is full in D. The remaining conditions in the definition of $\Gamma_p(D)$ are obviously satisfied by $G(L)$.

If S and S' are full Z_p orders in D, then S and S' are quasi-equal because they are full and finitely generated. Consequently, $(\hat{S} + L) \cap D$ is quasi-equal to $(\hat{S}' + L) \cap D$; and up to quasi-equality, the definition of $G(L)$ is independent of the choice of S.

THEOREM 2.6. *The correspondences $G \to L(G)$ and $L \to G(L)$ induce inverse bijections between the quasi-equality classes of groups in $\Gamma_p(D)$ and the left ideals of $\hat{D}$.*

Proof. The equality $L(G(L)) = L$ for a left ideal L of $\hat{D}$ is a consequence of $G(L)\hat{} = \hat{S} + L$, since $\hat{S}$ is a finitely generated $\hat{Z}_p$ module. Clearly, $G(L)\hat{} \subset \hat{S} + L$ and $\hat{S} \subset G(L)\hat{}$. The inclusion $L \subset G(L)\hat{} = G(L)\hat{} + \hat{S}$ is obtained by an easy calculation, using the observations that $\hat{S}$ is full in $\hat{D}$ and $\hat{S} = S + p^k \cdot \hat{S}$. To show that if $G \in \Gamma_p(D)$, then $G(L(G))$ is quasi-equal to G, it is sufficient to prove that $\hat{G}$ is quasi-equal to $\hat{S} + d(\hat{G})$. Indeed, D/G is a torsion group and $\hat{G}/G$ is torsion free, so that $(\hat{G} \cap D)/G = 0$. the structure theory for finite rank torsion free $\hat{Z}_p$ modules (see [7]) implies that $\hat{G} = N \oplus d(\hat{G})$, where N is a finitely generated $\hat{Z}_p$ module. Since $\hat{S}$ is also finitely generated, it is clear that $\hat{S} + d(\hat{G})$ is quasi-equal to $N \oplus d(\hat{G})$.

More complete proofs of Theorem 2.6 can be found in [4] and [**8**].

The p-rank, $\dim_{F_p} G/pG$, of a group $G \in \Gamma_p(D)$ is related to the $\hat{Q}_p$ dimension of $L(G)$ in the following way.

COROLLARY 2.7. *If $G \in \Gamma_p(D)$, then the p-rank of G is* $\dim D - \dim_{\hat{Q}_p} L(G)$.

Proof. Using the notation of the proof of Theorem 2.6, we have $\dim_{F_p} G/pG = \dim_{F_p} \hat{G}/p\hat{G} = \dim_{F_p} (N \oplus d(\hat{G}))/(pN \oplus d(\hat{G})) = \dim_{F_p} N/pN = \dim D - \dim_{\hat{Q}_p} L(G)$. See also **[8]**, Lemma 1.2.

PROPOSITION 2.8. *If $G \in \Gamma_p(D)$, then $QE(G) = \{\phi \in E(D) \mid \phi(L(G)) \subset L(G)\}$.*

The statement of this proposition tacitly identifies $E(D)$ with a subring of the $\hat{Q}_p$-endomorphisms of $\hat{D}$. We follow this custom in the remaining sections of the paper.

Routine calculations show that if $\phi \in E(D)$ satisfies $m\phi(G) \subset G$ for a natural number m, then $\phi(L(G)) = \phi(d(\hat{G})) \subset d(\hat{G}) = L(G)$. Conversely, if $\phi(L(G)) \subset L(G)$, then $m\phi(\hat{S} + L(G)) \subset \hat{S} + L(G)$ and $m\phi(G(L(G))) \subset G(L(G))$ for a suitable m. A detailed proof of Proposition 2.8 can be found in **[4]**.

3. The domain of definition. In **[11]**, Reid showed that the condition $QE(G) = D$, a division algebra, is satisfied if and only if G is strongly indecomposable and irreducible. When D is an algebraic number field, it was shown in **[10]** that G is strong indecomposable if and only if D is the smallest domain of definition for $L(G)$.

DEFINITION. A left ideal L of $\hat{D}$ is defined over the subalgebra A of the algebra D (and A is a domain of definition for L) if there is a set $\{u_i \mid i \in I\} \subset \hat{A}$ such that $L = \Sigma_{i\in I} \hat{D}u_i$.

THEOREM 3.1. *If D is a finite dimensional division algebra over Q and $G \in \Gamma_p(D)$, then $QE(G) = D$ if and only if D is the smallest domain of definition for $L(G)$.*

Proof. Assume that there is a proper subalgebra A of D and a set $\{u_i \mid i \in I\} \subset \hat{A}$ such that $L(G) = \Sigma_{i\in I} \hat{D}u_i$. Since D is a finite dimensional division algebra, so is A. Thus, if D is viewed as a right D space and a right A space, then $\lambda(D) = E_D(D) \underset{\neq}{\subset} E_A(D)$. Moreover, if $\phi \in E_A(D)$, then $\phi \in E_{\hat{A}}(\hat{D})$ and $\phi(L(G)) = \Sigma_{i\in I} \Phi(\hat{D}u_i) = \Sigma_{i\in I} \phi(\hat{D})u_i \subset \Sigma_{i\in I} \hat{D}u_i = L(G)$. By Proposition 2.8, $QE(G) \supset E_A(D)$ and hence $QE(G) \neq D$.

Conversely, assume that D is the smallest domain of definition for $L(G)$. To show $QE(G) = D$, it is sufficient by Proposition 2.8 to show that if $\phi \in E(D)$ satisfies $\phi(L(G)) \subset L(G)$, then $L(G)$ is defined over

$A = \{d \in D \mid \phi(cd) = \phi(c)d \text{ for all } c \in D\}$. That is, $L(G) \subset N = \Sigma \hat{D}u_i$, where the sum is over $u_i \in \hat{A} \cap L(G)$.

Every non-zero element of $\hat{D}$ has a representation $w = \Sigma_{j=1}^{r} \alpha_j c_j$, $\alpha_j \in \hat{Q}_p$, $c_j \in D$, in which r is minimal. The minimality of r guarantees that $\alpha_j \neq 0$ and $c_j \neq 0$ for all j. If $L(G) \neq N$, then there exists $w \in L(G) - N$ such that the number r in a minimal representation $w = \Sigma_{j=1}^{r} \alpha_j c_j$ is as small as possible. Denote $w' = \alpha_1^{-1} c_1^{-1} w = 1 + \Sigma_{j=2}^{r} \beta_j d_j \in L(G)$, where $\beta_j = \alpha_1^{-1}\alpha_j \in \hat{Q}_p$ and $d_j = c_1^{-1} c_j \in D$. Since $\phi \in E(D)$, it follows that

$$\Delta(c) = \sum_{j=2}^{r} \beta_j\big(\phi(c)d_j - \phi(cd_j)\big) = \phi(c)w' - \phi(cw') \in L(G)$$

for all $c \in D$. If $\phi(cd_j) = \phi(c)d_j$ for all $c \in D$, then $d_j \in A$ for $2 \leq j \leq r$, $w' \in \hat{A} \cap L(G)$, and $w \in \hat{D}w' \subset N$, contrary to hypothesis. Thus, $r \geq 2$ and there exists $c \in D$ and $j \geq 2$ such that $e = \phi(c)d_j - \phi(cd_j) \neq 0$. Without loss of generality, assume that $j = r$. The minimal property of r guarantees that $d_r e^{-1}\Delta(c)$ and

$$w' - d_r e^{-1}\Delta(c) = 1 + \sum_{j=2}^{r-1} \beta_j\big(d_j - d_r e^{-1}\big(\phi(c)d_j - \phi(cd_j)\big)\big)$$

are members of N. Hence $w' \in N$ and $w \in N$. This final contradiction completes the proof that $L(G)$ is defined over A.

It is useful to have a criterion for determining when D is the smallest domain of definition of a left ideal. The following simple result is sufficient for our needs.

COROLLARY 3.2. *If L is a left ideal of $\hat{D}$ such that $\{x \in D \mid Lx \subset L\}$ is the center of D, then $QE(G(L)) = D$.*

Proof. By Theorems 2.6 and 3.1, it is sufficient to note that if L is defined over the subalgebra A of D, then $A = D$. In fact, if $x \in D$ centralizes A, then $Lx = \hat{D}(\hat{A} \cap L)x = \hat{D}x(\hat{A} \cap L) \subset L$, so that x belongs to the center of D by hypothesis. Since D is a finite dimensional division algebra over Q, so is A. Thus the Double Centralizer Theorem ([**9**], Theorem 12.6) yields the desired conclusion $A = D$. (In the notation of [**9**], $C_D(A) = Z(D)$, so $D = C_D(Z(D)) = A$.)

To verify the hypothesis of Corollary 3.2, it is helpful to note that if $L = \hat{D}e$, with $e^2 = e$, then $Lx \subset L$ if and only if $ex = exe$.

4. The structure of $\hat{D}_p$. We next consider the structure of the algebra $\hat{D}_p$. As before $Z(D) = F$, and J will denote the ring of integers in F. If $pJ = P_1^{e(1)} \cdots P_k^{e(k)}$ is the factorization of p into powers of distinct prime ideals in J, then there are exactly k non-equivalent (normalized) extensions $v_1,\dots,v_k$ of the p-adic valuation v_p to F. Furthermore, if $\hat{F}_i$ is the completion of F in the v_i-topology, then,

$$(1) \qquad \hat{Q}_p \otimes F \simeq \hat{F}_1 \dotplus \cdots \dotplus \hat{F}_k \qquad \text{(as algebras).}$$

A discussion of this material can be found in **[9]** (in particular, see Lemma 18.1 and Proposition 18.2).

LEMMA 4.1. *Let D be a finite dimensional division algebra over Q with $Z(D) = F$, J the ring of integers in F, p a prime and $pJ = P^{e(1)} \cdots P^{e(k)}$ the factorization of p in J. Then*

$$\hat{D}_p = \hat{Q}_p \otimes D \simeq \hat{F}_1 \otimes_F D \dotplus \cdots \dotplus \hat{F}_k \otimes_F D,$$
$$\text{where } \hat{Q}_p \otimes F \simeq \hat{F}_1 \dotplus \cdots \dotplus \hat{F}_k \text{ as in (1).}$$

Proof. Since $\hat{D}_p$ is a finite dimensional semisimple $\hat{Q}_p$ algebra, $\hat{D}_p = B_1 \dotplus \cdots \dotplus B_l$, where each B_i is a simple, finite dimensional $\hat{Q}_p$ algebra. Moreover, $\hat{F}_1 \dotplus \cdots \dotplus \hat{F}_k \simeq \hat{Q}_p \otimes F \simeq Z(\hat{D}_p) = Z(B_1) \dotplus \cdots \dotplus Z(B_l)$. Hence, $l = m$ and without loss of generality, $\hat{F}_i = Z(B_i)$. Let $\rho_i\colon \hat{D}_p \to B_i$ be the ith projection, and $D_i = \rho_i(1 \otimes D)$, $F_i = \rho_i(1 \otimes F)$. Then D_i is a central simple F_i algebra that is isomorphic (as an F algebra) to D, F_i is a subfield of $Z(B_i)$ and

$$D_i Z(B_i) = \rho_i(1 \otimes D) \cdot \rho_i\big(Z\big(\hat{D}_p\big)\big) \supset \rho_i(1 \otimes D) \cdot \rho_i\big(\hat{Q}_p \otimes 1\big)$$
$$= \rho_i\big(\hat{D}_p\big) = B_i.$$

By **[9]**, Lemma 12.4a, any F_i basis of D_i is a $Z(B_i)$ basis of B_i. Thus $B_i \simeq Z(B_i) \otimes_{F_i} D_i \simeq \hat{F}_i \otimes_F D$. The lemma follows.

By Lemma 4.1, the left ideals of $\hat{D}_p$ are direct sums of left ideals in the $\hat{F}_i \otimes_F D$. We therefore focus our attention on the latter algebras, adopting the simpler notation $\hat{F} = \hat{F}_i$ for some i, and $\hat{D} = \hat{F} \otimes_F D$. The assumption that D is central over F implies that $\hat{D} = \hat{F} \otimes_F D$ is a central simple $\hat{F}$ algebra (see **[9]**, Proposition 12.4b). Thus, $\hat{D} \cong M_r(C)$, where C is a central division algebra over $\hat{F}$ and r is a divisor of the degree n of D. If $r = 1$, then $\hat{D}$ is a division algebra. Hence, we assume that $r > 1$. In this case, there exist matrix units $\{e_{ij} \mid 1 \le i, j \le r\} \subset \hat{D}$ with $e_{ij}e_{kl} = 0$ if $j \ne k$ and $e_{ij}e_{jl} = e_{il}$. Moreover, $\hat{D}$ contains a subalgebra that can be identified with the division algebra C. Consequently, C centralizes all of the matrix units e_{ij} and $\hat{D} = \bigoplus_{1 \le i, j \le r} Ce_{ij}$. For calculations it is often convenient to represent the elements of $\hat{D}$ as r by r matrices. Let $u_1, u_2, \ldots, u_s$ be an $\hat{F}$ space basis of C, where $s = (n/r)^2$, and $u_1 = 1$.

LEMMA 4.2. *There is a finite set $T \subset \hat{F}$ such that if $K = F(T) \subset \hat{F}$, then $\{e_{ij} \mid i \leq i, j \leq r\} \cup \{u_k \mid 1 \leq k \leq s\} \subset K \otimes D$. Thus, $K \otimes D = M_r(B)$, where $B = \bigoplus_{1 \leq k \leq s} Ku_k$ is a central division algebra over K and $\hat{F}B = C$.*

This lemma is obvious because the elements e_{ij} and u_k are finite linear combinations of the elements of D with coefficients in $\hat{F}$.

Henceforth, let T, K, and B have the meanings that were attached to them in Lemma 4.2.

LEMMA 4.3. *If X is a subset of $\hat{F}$ that is algebraically independent over K, then X is algebraically independent over $K \otimes_F D$.*

Proof. If $\mu_1, \mu_2, \ldots, \mu_m$ are distinct monomials that are products of elements from X, then this sequence of elements is linearly independent over K by assumption. Let $w_1, \ldots, w_m \in K \otimes_F D$ be such that $\mu_1 w_1 + \cdots + \mu_m w_m = 0$. We can write $w_i = \sum_{j=1}^{k} \alpha_{ij} x_j$ with $\alpha_{ij} \in K$ and $x_1, \ldots, x_k$ a linearly independent subset of D. Then $\sum_{i,j} \mu_i \alpha_{ij} x_j = 0$ implies $\sum_{i=1}^{m} \mu_i \alpha_{ij} = 0$ for $1 \leq j \leq k$ by a standard property of tensor products over fields. Thus, $\alpha_{ij} = 0$ for all i, j, and $w_1 = \cdots = w_m = 0$.

We can now prove the key lemma of this section.

LEMMA 4.4. *If $1 \leq t < r$, then there is a left ideal L of $\hat{D}$ such that*
(a) $\dim_{\hat{F}} L = tn^2/r$, *and*
(b) *if $x \in D$ satisfies $Lx \subset L$, then $x \in F$.*

Proof. Since $\hat{F}$ has infinite transcendence degree over F, there is a set $X = \{\alpha_{ijk} \in \hat{F} \mid 1 \leq i \leq t,\ 1 \leq j \leq r - t,\ 1 \leq k \leq s\}$ that is algebraically independent over K. Define $a_{ij} = \sum_{k=1}^{s} \alpha_{ijk} u_k \in C$, $\gamma = [a_{ij}]$, and $e = \left(\begin{smallmatrix} \iota & \gamma \\ 0 & 0 \end{smallmatrix}\right) \in M_r(C) = \hat{D}$, where ι is the t by t identity matrix. Note that $e^2 = e$. Let $L = \hat{D}e$, a left ideal of $\hat{D}$. By definition, L is a direct sum of t minimal ideals of $M_r(C)$ (generated by the non-zero rows of e). Hence the $\hat{F}$ dimension of L is $t(n/r)n$. Suppose that $x \in D$ satisfies $Lx \subset L$, that is, $ex = exe$. The assumption that $x \in D$ implies that the matrix entries of x are in $B \subset K \otimes_F D$. If

$$x = \begin{pmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{pmatrix}$$

is partitioned like e, then the condition $ex = exe$ takes the form

$$\begin{pmatrix} \xi_{11} + \gamma\xi_{21} & \xi_{12} + \gamma\xi_{22} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \xi_{11} + \gamma\xi_{21} & \xi_{11}\gamma + \gamma\xi_{21}\gamma \\ 0 & 0 \end{pmatrix},$$

or $\xi_{12} + \gamma\xi_{22} = \xi_{11}\gamma + \gamma\xi_{21}\gamma$. It follows from Lemma 4.3 that $\xi_{12} = 0$, $\xi_{21} = 0$, and $\gamma\xi_{22} = \xi_{11}\gamma$. If $\xi_{11} = [x_{hi}]$, $\xi_{22} = [y_{jk}]$, then $\xi_{11}\gamma = \gamma\xi_{22}$ implies $\Sigma_{i=1}^{t} x_{hi}a_{ij} = \Sigma_{j=1}^{r-t} a_{ij}y_{jk}$. Using Lemma 4.3 again, it follows that $x_{hi} = 0$ if $h \neq i$, $y_{jk} = 0$ if $k \neq j$, and $x_{ii}a_{ij} = a_{ij}y_{jj}$ for $1 \leq i \leq t$, $1 \leq j \leq r - t$. Thus, $\Sigma_{k=1}^{s} \alpha_{ijk}(x_{ii}u_k - u_k y_{jj}) = 0$, so that $x_{ii}u_k = u_k y_{jj}$ for all k by Lemmas 4.2 and 4.3. Therefore, $x_{11} = \cdots = x_{tt} = y_{11} = \cdots = y_{n-t,n-t}$, and this element is in the center $\hat{F}$ of C. That is, $x \in F$, since $\hat{F} \cap D = F$.

5. Realizing division algebras. In this section we apply the machinery developed in §§2, 3, and 4 to determine for which primes p a central division algebra D of degree n over an algebraic number field F is p-realizable.

NOTATION. Using Lemma 4.1 and the subsequent discussion, we can assume that,

(1) $\hat{Q}_p \otimes F = \hat{F}_1 \dotplus \cdots \dotplus \hat{F}_k$, and

(2) $\hat{D}_p = \hat{Q}_p \otimes D = M_{r(1)}(C_1) \dotplus \cdots \dotplus M_{r(k)}(C_k)$,

where for each i, $r(i)$ is a positive integer and C_i is a central division algebra over $\hat{F}_i$. If we let $d = \dim_Q F$ and $d_i = \dim_{\hat{Q}_p} \hat{F}_i$, then $d = \Sigma_{i=1}^{k} d_i$ and $dn^2 = \Sigma_{i=1}^{k} d_i(n/r(i))^2 r(i)^2$, so that $n/r(i)$ is the degree of C_i over $\hat{F}_i$.

DEFINITION. A set of positive integers $\{t_i \mid 1 \leq i \leq k\}$ is said to be *applicable* for $\hat{D}_p$ provided that for each i, $0 \leq t_i \leq r(i)$, and for at least one i, $1 \leq t_i < r(i)$.

Note that this definition subsumes $r(i) > 1$ for some i.

THEOREM 5.1. *If D is a central division algebra of degree n over an algebraic number field F and p is a prime, then D is p-realizable if and only if $\hat{D}_p$ is not a direct product of division algebras. In this case, if $\hat{D}_p \cong \bigoplus_{i=1}^{k} M_{r(i)}(C_i)$ with $r(i) \geq 1$ and C_i a division algebra, then for each applicable set of integers $\{t_i \mid 1 \leq i \leq k\}$ there is a p-local group G of rank dn^2 and p-rank $\Sigma_{i=1}^{k} d_i t_i n^2/r(i)$ such that $QE(G) \cong D$.*

Proof. If $\hat{D}_p = C_1 \dotplus \cdots \dotplus C_k$ is a product of division algebras, then the only left ideals of $\hat{D}_p$ have the form $L = \Sigma_{i \in I} C_i$, where I is some subset of $\{1,\ldots,k\}$. By Lemma 4.1, each such L is defined over F, and D is not p-realizable by Theorem 3.1.

The rest of the theorem is a consequence of Lemma 4.4, using the results of §§2 and 3 (explicitly, Theorem 2.6, Corollary 2.7, and Corollary 3.3).

It is clear from Corollary 2.7 and (2) that every $G \in \Gamma_p(D)$ has p-rank of the form $\sum_{i=1}^{k} d_i t_i n^2/r(i)$ for some applicable set of t_i. If $t_i = 0$ or $r(i)$ for each i, then $L(G)$ is defined over F, so that G will not p-realize D in these cases. Thus, the result on p-ranks in the theorem is optimal.

REMARK. The proof of the theorem can be refined to show that for each admissible p-rank, there are continuum many pairwise non-quasi-isomorphic groups $G \in \Gamma_p(D)$ of that p-rank such that $QE(G) = D$. Indeed, G and H in $\Gamma_p(D)$ are quasi-isomorphic if and only if there is a non-singular linear transformation ϕ of D such that $\phi(L(G)) = L(H)$ (see **[3]**, Theorem 5.25). The estimate of the number of G that p-realize D therefore follows from the observations that $E_Q(D)$ is countable and that the transcendence degree of $\hat{F}_i$ over F is the cardinal number of the continuum for each i.

COROLLARY 5.2. *Let D be a central division algebra over F of degree $q_1^{e(1)} \cdots q_r^{e(r)}$, where $q_1, \ldots, q_r$ are distinct primes. If $D = D_1 \otimes_F \cdots \otimes_F D_r$ is the primary decomposition of D (that is, D_i is a central division algebra over F of degree $q_i^{e(i)}$) then for any prime p, D is not p-realizable if and only if none of the D_i are p-realizable.*

This is clear from Theorem 5.1, since

$$\hat{D}_p = \hat{Q}_p \otimes D = \left(\hat{F}_1 \dotplus \cdots \dotplus \hat{F}_k\right) \otimes_F D$$
$$= \prod_{i=1}^{k} \left(\hat{F}_i \otimes_F D_1\right) \otimes_{\hat{F}_i} \cdots \otimes_{\hat{F}_i} \left(\hat{F}_i \otimes_F D_r\right),$$

and $\hat{D}_p$ is a product of division algebras if and only if for each $i \leq i \leq k$, $1 \leq j \leq r$, $\hat{F}_1 \otimes_F D_j$ is a division algebra (see **[9]**, Theorem 14.4 and Proposition 13.4).

The result in Theorem 5.1 can be formulated in terms of the local invariants of the division algebra D. Given a (normalized) valuation v of F, let $\hat{F}_v$ denote the completion of F in the v-topology, and $\hat{D}_v = \hat{F}_v \otimes_F D$. For each such v, there is a monomorphism INV_v: $B(\hat{F}_v) \to Q/Z$ of the Brauer group of $\hat{F}_v$ to the rationals mod Z. If v is non-archimedean, then INV_v is surjective. When v is archimedean, then the image of INV_v is $(1/2)Z/Z$ or 0 in the respective cases that v is real or complex. The elements $\mathrm{INV}_v(\hat{D}_v)$ are called the local invariants of D. They determine the algebra D uniquely to within isomorphism. The order of $\mathrm{INV}_v(\hat{D}_v)$ is the Schur index of $\hat{D}_v$. In particular, $\hat{D}_v$ is a division algebra if and only if the order of $\mathrm{INV}_v(\hat{D}_v)$ is equal to the degree of D. By using this observation and some standard facts about local invariants (see **[9]** Chapter 18), we can deduce some interesting implications of Theorem 5.1.

Since $\mathrm{INV}_v(\hat{D}_v)$ is zero for almost all normalized valuations v (see **[9]**, Proposition 18.5), the hypotheses of Theorem 5.1 are satisfied for almost all primes p. Thus, Theorem 5.1 implies the following result.

COROLLARY 5.3. *Let D be a finite dimensional central division algebra over an algebraic number field. Then for almost all primes p, D is p-realizable.*

The local invariants satisfy the general reciprocity law: $\Sigma_v \mathrm{INV}_v(\hat{D}_v) = 0$. Conversely, given elements $c_v \in Q/Z$ such that $c_v = 0$ for almost all v, $c_v \in (1/2)Z/Z$ if v is real archimedean, $c_v = 0$ if v is complex archimedean, there is a central division algebra D over F such that $\mathrm{INV}_v(\hat{D}_v) = c_v$ for all v. This deep theorem ([**9**], Theorem 18.5), together with the result that the degree of D is the least common multiple of the orders of the local invariants of D, leads to existence theorems for p-realizable division algebras.

COROLLARY 5.4. *Let F be an algebraic number field with $F \neq Q$. If $n > 1$ is a natural number and Π is a finite (possibly empty) set of rational primes, then there is a division algebra D with center F and degree n such that D is p-realizable if and only if $p \notin \Pi$.*

Proof. Let q and r be distinct primes not in Π such that in the ring J of integers in F, Jq and Jr are products of two or more distinct prime factors, say $Jq = P_1 P_2 \cdots$, and $Jr = Q_1 Q_2 \cdots$. Such primes exist by the Tchebotarev Density Theorem ([**9**], §18.7) because $[F\colon Q] \geq 2$. For each normalized non-archimedean valuation v of F, denote by P_v the set $\{x \in F \mid v(x) < 1\}$. The mapping $v \to P_v$ is bijective between valuations and non-zero prime ideals of J. Let $v(1), \ldots, v(m)$ be the (possibly empty) set of valuations such that $P_{v(i)} \supset Jp$ for some $p \in \Pi$; and let $v(0)$ and w be the valuations such that $P_{v(0)} = P_1$, $P_w = Q_1$. Define D to be the division algebra with center F such that $\mathrm{INV}_{v(i)}(\hat{D}_{v(i)}) = 1/n + Z$ for $0 \leq i \leq m$, $\mathrm{INV}_w(\hat{D}_w) = -(\Sigma_{i=0}^m \mathrm{INV}_{v(i)}(\hat{D}_{v(i)}))$, and $\mathrm{INV}_v(\hat{D}_v) = 0$ if v is not among w, $v(0), \ldots, v(m)$. The order of $\mathrm{INV}_{v(i)}(D_{v(i)})$ is clearly n; the order of $\mathrm{INV}_w(\hat{D}_w)$ divides n; and the (multiplicative) order of all other local invariants divides n. Thus the degree of D is n. By construction, if $p \in \Pi$, then $\hat{D}_p$ is a product of division algebras. If p is q or r, then $\hat{D}_p$ is not a product of division algebras because $\mathrm{INV}_v(\hat{D}_v) = 0$ if $P_v = P_2$ or Q_2. Finally, if $p \notin \Pi$ and $p \neq q$ or r, then $\mathrm{INV}_v(\hat{D}_v) = 0$ for all valuations v such that $v(p) < 1$; hence $\hat{D}_p$ is a product of matrix rings of the form $M_n(\hat{F}_v)$. It follows from Theorem 5.1 that D is p-realizable if and only if $p \in \Pi$.

For division algebras with center Q, the situation is somewhat different. When n is not a prime power, then the construction in Corollary 5.4 can be modified to obtain the same result in the case $F = Q$. Similarly, if $n = q^e$ is a prime power and $|\Pi| \geq 2$, or if $n = 2$ and $|\Pi| = 1$, then the argument can be modified to produce a division algebra D with center Q such that Π is the set of primes at which D is not p-realizable. Our final corollary shows that these restrictions on Π cannot be omitted.

COROLLARY 5.5. *If $n = q^e > 1$ is a prime power, then every central division algebra D of degree n over Q is not p-realizable for at least one prime p, and for at least two primes if $n > 2$.*

Proof. Suppose that $Z(D) = Q$ and $\mathrm{Deg}\, D = n$. Since n is the least common multiple of the orders of $\mathrm{INV}_v(\hat{D}_p)$ and $\mathrm{INV}_\infty(\hat{D}_\infty)$ (corresponding to the absolute value on Q), it follows that $\mathrm{INV}_p(\hat{D}_p) = a_p/q^{f(p)} + Z$ (with a_p zero or not divisible by q, $f(p) \leq e$), $\mathrm{INV}_\infty(\hat{D}_\infty) = 0$ if $q \neq 2$, $\mathrm{INV}_\infty(\hat{D}_\infty) = 0$ or $1/2 + Z$ if $q = 2$, and (since $\Sigma\, \mathrm{INV}_p(\hat{D}_p) + \mathrm{INV}_\infty(\hat{D}_\infty) = 0$) there are two or more local invariants of D whose orders are n. Thus, $\mathrm{INV}_p(\hat{D}_p)$ has order n for at least two primes p if $n > 2$, and for at least one prime p if $n = 2$. The corollary therefore follows from Theorem 5.1.

REFERENCES

[1] A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloquium Publ. Vol. 24, Amer. Math. Soc., Providence, R. I., (1935).

[2] R. A. Beaumont and R. S. Pierce, *Subrings of algebraic number fields*, Acta. Sci. Math., (Szeged) **22** (1961), 202–216.

[3] _____, *Torsion-free groups of rank two*, Mem. Amer. Math. Soc., **38** (1961).

[4] _____, *Torsion-free rings*, Illinois J. Math., **5** (1961), 61–98.

[5] M. C. R. Butler, *On locally free torsion-free rings of finite rank*, J. London Math. Soc., **15** (1965), 297–300.

[6] A. L. S. Corner, *Every countable reduced torsion-free ring is an endomorphism ring*, Proc. London Math. Soc., **13** (1963), 687–710.

[7] I. Kaplansky, *Infinite Abelian Groups*, University of Michigan press, Ann Arbor, Michigan (1969).

[8] E. L. Lady, *Splitting fields for torsion-free modules over discrete valuation rings*, I, J. Algebra, **49** (1977), 261–275.

[9] R. S. Pierce, *Associative Algebras*, Springer-Verlag, New York (1982).
[10] _____, *Subrings of simple algebras*, Michigan Math. J., **7** (1960), 241–243.
[11] J. D. Reid, *On the ring of quasi-endomorphisms of a torsion-free group*, Topics in Abelian Groups, Chicago, Illinois (1963), 51–68.
[12] H. Zassenhaus, *Orders as endomorphism rings of modules of the same rank*, J. London Math. Soc., **42** (1967), 180–182.

Received February 10, 1982, and in revised form April 19, 1982.

UNIVERSITY OF ARIZONA
TUCSON, AZ 85721

AND

UNIVERSITY OF CONNECTICUT
STORRS, CT 06268