

INDECOMPOSABLE DIVISION ALGEBRAS

B. A. SETHURAMAN

(Communicated by Maurice Auslander)

ABSTRACT. We present a direct construction of indecomposable division algebras of all indices p^n and exponents p^m ($n \geq m \geq 2$) that does not rely on generic methods.

1. INTRODUCTION

All division algebras will be finite dimensional over their centers. If D is a division algebra with center F , then D is said to admit a nontrivial decomposition if $D \cong D_1 \otimes_F D_2$, where $1 < \dim_F(D_i) < \dim_F(D)$ ($i = 1, 2$). If D does not admit any nontrivial decompositions, D is said to be indecomposable.

Given a division algebra D with center F , the index of D ($\text{ind}(D)$) is defined to be the square root of $\dim_F(D)$, and the exponent of D ($\text{exp}(D)$) is defined to be the least integer k such that $D \otimes_F \cdots \otimes_F D$ (k times) is isomorphic to a matrix ring over F . It is well known that D is indecomposable only if $\text{ind}(D)$ is a power of a prime. Further, if D has index and exponent p^n for some prime p , then D is necessarily indecomposable.

A natural question, then, is the following: Given an arbitrary prime p , do there exist indecomposable division algebras of all indices p^n and exponents p^m , $n > m \geq 1$? This question (in its full generality) was first addressed by Saltman [S, Theorem 2.6], who showed that for $m \geq \{n/2\} + 1$ (where $\{n/2\}$ is the least integer $\geq n/2$), the universal division algebras $UD(p^n, p^m)$ of index p^n and exponent p^m are indecomposable. Recently, using results derived from the geometry of Brauer-Severi varieties, Schofield and van den Bergh [SvdB, Theorem 2.2] showed that the algebras $UD(p^n, p^m)$ are indeed indecomposable for all n and m such that $n \geq m \geq 2$.

In this paper we show that indecomposable division algebra of all indices p^n and exponents p^m ($n \geq m \geq 2$) can be constructed directly from cyclic algebras. Our construction requires the ground field to contain enough roots of unity, but it does not rely on difficult generic methods. We then use this technique to obtain a concrete family of indecomposable division algebras whose centers are rational function fields.

Received by the editors October 12, 1990.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 16A39.

Key words and phrases. Division algebras, indecomposability, cyclic algebras, symbol algebras.

This work constitutes a part of the author's doctoral dissertation, and was supported in part by the N.S.F.

It is worth remarking that other special cases of indecomposable division algebras exist in the literature, for instance, Amitsur, Rowen, and Tignol [ART, Theorem 5.1], index 8 and exponent 2, Tignol [T, Theorem 2], index p^2 and exponent p for odd primes p , and Jacob and Wadsworth [JW1, Remark 5.6], index p^n and exponent p^m ($n > m \geq \{n/2\} + 1$). Also, Rowen [R, Theorem 5] describes a family of indecomposable algebras; however, his results depend on an absence of roots of unity. Finally, Jacob [J, Theorem 3.3] describes indecomposable algebras of index p^n ($n \geq 2$, $n \geq 3$ if $p = 2$) and exponent p ; his examples remain the only known nongeneric examples of exponent p (and index an arbitrary power of p).

2. THE CONSTRUCTION

First, some notation. Let F be a field containing all primitive p^j th roots of unity ($j = 1, 2, \dots$), and for each j , choose a primitive p^j th root of unity ω_j such that $\omega_j^p = \omega_{j-1}$ ($j = 1, 2, \dots$, and where ω_0 is understood to be 1). Given a, b in $F - \{0\}$, we write $(a, b)_{p^n}$ for the algebra generated by two symbols i, j subject to $i^{p^n} = a$, $j^{p^n} = b$, $ij = \omega_n ji$, and refer to such an algebra as a symbol algebra. It is well known that such an algebra is central simple over F , of dimension p^{2n} . Thus, if A denotes this algebra, then A is isomorphic to a matrix ring over some division ring D . We define the index of A ($\text{ind}(A)$) to be the index of D . Also, we define $A^{1/p}$ to be the algebra $(a, b)_{p^{n+1}}$. By a standard identity (e.g. [D, Chapter 11, Lemma 6]), $(A^{1/p})^p \sim A$ in the Brauer group of F (where $(A^{1/p})^p$ is the tensor product of $A^{1/p}$ with itself p times).

Proposition 1. *Let F be a field containing a primitive p^{n+1} th root of unity ($n \geq 1$). Let $a, b \in F - \{0\}$, and let $A = (a, b)_{p^n}$. Assume that A is a division algebra (so its index is p^n), and let p^m ($0 < m \leq n$) be its exponent. Then $A^{1/p}$ is an indecomposable division algebra of index p^{n+1} and exponent p^{m+1} .*

Proof. Clearly, $\text{ind}(A^{1/p}) \leq p^{n+1}$. On the other hand, since $\text{ind}(A)$ is a power of p , by [A, p. 76, Lemma 7] we have $\text{ind}(A^{1/p}) \geq p \cdot \text{ind}((A^{1/p})^p) = p \cdot \text{ind}(A) = p^{n+1}$. Thus, $\text{ind}(A^{1/p})$ is exactly p^{n+1} . Since we now have $\text{ind}(A^{1/p}) = p \cdot \text{ind}((A^{1/p})^p)$, $A^{1/p}$ must be indecomposable by Saltman's criterion [S, Lemma 3.2]. Finally, since $\text{exp}(A) = p^m$, $\text{exp}(A^{1/p})$ must be p^{m+1} . \square

The proposition above thus reduces the construction of indecomposable division algebras of index p^n and exponent p^m ($n \geq m \geq 2$) to the construction of symbol algebras of index p^n and exponent p^m ($n \geq m \geq 1$). One family of such algebras are the generic cyclic algebras described in [O, Propositions 2.1 and 2.2] (if one assumes that the ground field there contains enough roots of unity). We describe below a different construction that yields division algebras that are defined over rational function fields and are somewhat easy to compute with. These examples were inspired by the construction in [T, Theorem 1].

Since the problem of indecomposability is trivial if $m = n$, we focus on the case where $m < n$. Let F_0 be a field containing the primitive p^j th roots of unity ω_j ($j = 1, \dots, n+1$) described above. Let $k = n - m$ (so $k \geq 1$ by assumption), and let $F = F_0(x_0, x_1, \dots, x_k, y)$ be the rational function field

in the $k + 2$ indeterminates x_0, x_1, \dots, x_k, y . We define $R_{n,m}$ by

$$R_{n,m} = (x_0, x_0^{p^k} - y)_{p^m} \otimes_F (x_1, x_1^{p^{k-1}} - y)_p \otimes_F (x_2, x_2^{p^{k-2}} - y)_p \otimes_F \dots \otimes_F (x_{k-1}, x_{k-1}^p - y)_p \otimes_F (x_k, x_k - y)_p.$$

Proposition 2. $R_{n,m}$ is a division algebra of index p^n and exponent p^m , and is isomorphic to $(y, a)_{p^n}$ for some a in F .

Proof. For $j = 0, 1, \dots, k$, let E_j be the field $F_0(x_0, x_1, \dots, x_j, y)$, and let A_j be the central simple algebra over E_j defined by

$$A_j = (x_0, x_0^{p^k} - y^{p^{k-j}})_{p^m} \otimes_{E_j} (x_1, x_1^{p^{k-1}} - y^{p^{k-j}})_p \otimes_{E_j} \dots \otimes_{E_j} (x_j, x_j^{p^{k-j}} - y^{p^{k-j}})_p$$

(so that E_k is just F and A_k is just $R_{n,m}$). We will first show inductively that A_j has index p^{m+j} , from which it will follow that $R_{n,m}$ has index p^n . We will use valuation-theoretic results from [JW2] to establish this.

Assume $j = 0$. Consider $A_0 = (x_0, x_0^{p^k} - y^{p^k})_{p^m}$. Recall that $(x_0^{p^k} - y^{p^k})$ factors completely into linear factors of the form $(x_0 - \omega_k^i y)$ ($i = 0, 1, \dots, p^k - 1$). With respect to the $(x_0 - y)$ -adic valuation on E_0 (i.e., the discrete valuation obtained by localizing $F_0[x_0, y]$ at the height 1 prime ideal generated by $(x_0 - y)$) the field $E_0(x_0^{1/p^m})$ is unramified over E_0 . In particular, the valuation extends uniquely from E_0 to $E_0(x_0^{1/p^m})$ and the value group does not grow. Hence the value of the norm from $E_0(x_0^{1/p^m})$ to E_0 of any nonzero element in $E_0(x_0^{1/p^m})$ is a multiple of p^m . Since $(x_0^{p^k} - y^{p^k})$ has value 1, it follows that $(x_0^{p^k} - y^{p^k})^l$ cannot be the norm of an element in $E_0(x_0^{1/p^m})$ for $0 < l < p^m$. Hence A_0 has exponent, and consequently index, p^m .

Now assume that $0 < j \leq k$ and that A_{j-1} has been shown to have index p^{m+j-1} . Let $E_{j,h}$ denote the henselization of E_j with respect to the $(x_j - y)$ -adic valuation, and consider $A_{j,h} = A_j \otimes_{E_j} E_{j,h}$. Notice that the factor $(x_j, x_j^{p^{k-j}} - y^{p^{k-j}})_p \otimes_{E_j} E_{j,h}$ ($= N$, say) has the same form as [JW2, Example 4.3]. In particular, it is a nicely semiramified division algebra, in the terminology of [JW2, §4]. (Of course, N can also be seen to be a division algebra by an argument analogous to that used for A_0 .) Recalling that the residues of x_j and y are equal with respect to this valuation, we find that the residue of $E_{j,h}$ (which equals the residue of E_j) is just E_{j-1} and that the residue \bar{N} of N is $E_{j-1}(y^{1/p})$. If we put $z = y^{1/p}$, then \bar{N} is just $F_0(x_0, x_1, \dots, x_{j-1}, z)$, a rational function field in $j + 1$ variables. Now observe that the elements x_i and $x_i^{p^{k-i}} - y^{p^{k-j}}$ ($i = 0, 1, \dots, j-1$) are all units with respect to the $(x_j - y)$ -adic valuation. Let I denote the division algebra similar to $(x_0, x_0^{p^k} - y^{p^{k-j}})_{p^m} \otimes_{E_{j,h}} (x_1, x_1^{p^{k-1}} - y^{p^{k-j}})_p \otimes_{E_{j,h}} \dots \otimes_{E_{j,h}} (x_{j-1}, x_{j-1}^{p^{k-(j-1)}} - y^{p^{k-j}})_p$ in the Brauer group of $E_{j,h}$. The $(x_j - y)$ -adic valuation extends to I since $E_{j,h}$ is henselian. It follows from [JW2, Example 2.4(i) and Proposition 2.5] that I is inertial over $E_{j,h}$, and if \bar{I} denotes the residue of I , that $\bar{I} \otimes_{E_{j-1}} \bar{N}$ is similar to the algebra $(x_0, x_0^{p^k} - z^{p^{k-(j-1)}})_{p^m} \otimes_{\bar{N}} (x_1, x_1^{p^{k-1}} - z^{p^{k-(j-1)}})_p \otimes_{\bar{N}} \dots \otimes_{\bar{N}} (x_{j-1}, x_{j-1}^{p^{k-(j-1)}} - z^{p^{k-(j-1)}})_p$ in the

Brauer group of \overline{N} . This has the same form as A_{j-1} (but defined, instead, over $F_0(x_0, x_1, \dots, x_{j-1}, z)$), so, by induction, it has index p^{m+j-1} . Hence, by [JW2, Theorem 5.15], $\text{ind}(A_{j,h}) = \text{ind}(N) \cdot \text{ind}(\overline{I} \otimes_{E_{j-1}} \overline{N}) = p \cdot p^{m+j-1} = p^{m+j}$. Thus, $\text{ind}(A_j) \geq \text{ind}(A_{j,h}) \geq p^{m+j}$. But $\text{ind}(A_j) \leq \sqrt{\text{dim}_{E_j}(A_j)} = p^{m+j}$. Hence, A_j has index exactly p^{m+j} .

To prove that $R_{n,m}$ has exponent p^m , note that, if $m > 1$, $R_{n,m}^p \sim (x_0, x_0^{p^k} - y)_{p^{m-1}}$. By the same argument used for A_0 above, but applied instead to the $(x_0^{p^k} - y)$ -adic valuation, it can be seen that $R_{n,m}^p$ has exponent p^{m-1} . Hence $R_{n,m}$ must have exponent p^m .

Finally, we establish the required isomorphism. Recall the identity $(a, a - b)_{p^l} \sim (b, (a - b)/a)_{p^l} \otimes_F (a, -1)_{p^l}$, $l = 1, 2, \dots$, valid for any $a, b \in F - \{0\}$ with $a - b \neq 0$ [D, Chapter 11, Lemma 11]. Notice that -1 is a p^l th power for $l = 1, \dots, n$, by the assumption about the roots of unity in F . Using this, along with standard properties of symbol algebras (e.g. [D, Chapter 11, Lemmas 4 and 6]), we get for $j = 1, \dots, k$ that

$$(x_j, x_j^{p^{k-j}} - y)_p \sim (x_j^{p^{k-j}}, x_j^{p^{k-j}} - y)_{p^{k-j+1}} \sim \left(y, \frac{x_j^{p^{k-j}} - y}{x_j^{p^{k-j}}} \right)_{k-j+1} \sim (y, a_j)_{p^n},$$

where we have written a_j for

$$\left(\frac{x_j^{p^{k-j}} - y}{x_j^{p^{k-j}}} \right)^{p^{n-(k-j+1)}}.$$

Similarly, $(x_0, x_0^{p^k} - y)_{p^m} \sim (y, a_0)_{p^n}$, where $a_0 = (x_0^{p^k} - y)/x_0^{p^k}$. Writing a for the product of a_0 and the a_j 's ($j = 1, \dots, k$), and noting that the index of $R_{n,m}$ is p^n , we get that $R_{n,m}$ is indeed isomorphic to $(y, a)_{p^n}$. \square

Theorem. *The algebras $R_{n,m}^{1/p} (= (y, a)_{p^{n+1}})$ are indecomposable division algebras of index p^{n+1} and exponent p^{m+1} ($n > m \geq 1$).*

Proof. This is immediate from Propositions 1 and 2. \square

REFERENCES

[A] A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Pub. vol. 24, Providence, RI, 1961.
 [ART] S. A. Amitsur, L. H. Rowen, and J.-P. Tignol, *Division algebras of degree 4 and 8 with involution*, Israel J. Math. **33** (1979), 133–148.
 [D] P. K. Draxl, *Skew fields*, London Math. Soc. Lecture Note Ser., Vol. 81, Cambridge Univ. Press, Cambridge, 1983.
 [J] B. Jacob, *Indecomposable division algebras of prime exponent*, J. Reine Angew. Math. (to appear).
 [JW1] B. Jacob and A. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc. **293** (1986), 693–721.
 [JW2] ———, *Division algebras over henselian fields*, J. Algebra **128** (1990), 126–179.
 [O] C. Ousmane, *Algèbres cycliques génériques*, Bull. Soc. Math. Belg. Sér. B **40** (1988), 43–59.

- [R] L. H. Rowen, *Cyclic division algebras*, *Israel J. Math.* **41** (1982), 213–234.
- [S] D. Saltman, *Indecomposable division algebras*, *Comm. Algebra* **7** (1979), 791–817.
- [SvdB] A. Schofield and M. van den Bergh, *The index of a Brauer class on a Brauer-Severi variety*, *Trans. Amer. Math. Soc.* (to appear).
- [T] J.-P. Tignol, *Algèbres indécomposables d'exposant premier*, *Adv. in Math.* **65** (1987), 205–228.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT SAN DIEGO, LA JOLLA, CALIFORNIA 92093