

# Recognition and Computations of Matrix Rings

T. Y. Lam<sup>1</sup>, University of California, Berkeley, Ca 94720

André Leroy, Université d'Artois, 62307 Lens Cedex, France

## Abstract

An eigenring formula for computing a base ring for an  $n \times n$  matrix ring is given in the context of the Agnarsson-Amitsur-Robson characterization of such matrix rings. Various other recognition criteria and computations of "hidden" matrix rings are also given.

## §1. Introduction

In the last few years there has been a resurgence of interest in the recognition and characterization of matrix rings. P. R. Fuchs [Fu], J. C. Robson [R], and more recently Agnarsson-Amitsur-Robson [AAR] have obtained several new interesting criteria for a given ring  $R$  to be an  $n \times n$  matrix ring  $\mathbf{M}_n(A)$ , and Chatters [Ch<sub>1</sub>, Ch<sub>2</sub>, Ch<sub>3</sub>], Levy-Robson-Stafford [LRS] have given numerous fascinating examples of non-obvious (or "hidden") matrix rings. In the present paper, we shall develop these themes some more, and contribute a number of new results to this ongoing study.

It is well-known that, if a ring  $R$  is an  $n \times n$  matrix ring, there may exist more than one ring  $A$  for which  $R \cong \mathbf{M}_n(A)$ . In a beginning section (§2) of this paper, we consider the Agnarsson-Amitsur-Robson characterization (2.1) of an  $n \times n$  matrix ring  $R$ , and give in that context a formula for computing a specific base ring  $A$  for  $R$  (Theorem 2.2). This formula expresses  $A$  as an eigenring of a certain nilpotent element in  $R$ , and is explicit enough to permit various direct computations of matrix rings. An illustration for this is given in Example (2.7) in terms of Morita rings. Another application of (2.1) and (2.2) is to the study of Ore extension rings. Let  $S = R[t, \sigma, \delta]$  be an Ore extension (a.k.a. skew polynomial ring), where  $\sigma$  is an endomorphism of the base ring  $R$ , and  $\delta$  is a  $\sigma$ -derivation on  $R$ . Certain quotients of  $S$  may be  $k \times k$  matrix rings, and sometimes  $S$  itself may be an  $k \times k$  matrix ring (for some  $k \geq 2$ ). In §3, we give instances of these by using the Agnarsson-Amitsur-Robson Theorem (2.1). In each case, (2.2) is applied to make an *explicit* computation of a base ring for the matrix ring in question: see, for instance, Thms. (3.1) and (3.14). A result which is

---

<sup>1</sup>Supported in part by NSF

particularly easy to state is Theorem (3.5): *If  $R$  is nonzero, and contains an element  $b$  such that  $b^{m+n} = 0$  and  $\delta(b^m), \delta(b^n)$  are both units, then necessarily  $m = n$ , and  $S$  is isomorphic to the  $(2n) \times (2n)$  matrix ring over the eigenring of  $b$  in  $S$ .*

In §4, we study various new characterizations (Th. 4.1) for an  $n \times n$  matrix ring  $R$ , in terms of equations involving units and nilpotent elements in  $R$ , as well as in terms of  $n$ th root properties of certain nilpotent matrices over  $R$ . For simplicity, we shall only state a special case of this result below, where the  $E_{i,j}$ 's denote the standard matrix units throughout this paper.

**Theorem.** *For a given integer  $n \geq 2$ , a ring  $R$  is an  $n \times n$  matrix ring iff for some (resp. for all)  $r \geq 2$ , the  $r \times r$  matrix  $F_0 := E_{2,1} + E_{3,2} + \cdots + E_{r,r-1}$  over  $R$  has an  $n$ th root in  $\mathbf{M}_r(R)$ .*

This implies, in particular, that if  $R$  admits a (unital) homomorphism into a nonzero ring which is commutative, or reduced, or without nontrivial idempotents, then  $F_0$  can never have an  $n$ th root in  $\mathbf{M}_r(R)$  for any  $r, n \geq 2$ .

The last section (§5) concludes with an example of a hidden matrix ring with quaternionic entries which generalizes an earlier example of Levy, Robson and Stafford in [LRS].

*Acknowledgment.* We thank the referee for detailed comments on this paper which led to its present shorter version.

## §2. A Formula for the Base Ring

For the reader's convenience, we first recall the following recognition theorem for matrix rings, due to Agnarsson, Amitsur and Robson:

**Theorem 2.1.** [AAR] *Let  $m, n$  be positive integers. A ring  $R$  is an  $(m+n) \times (m+n)$  matrix ring (over some other ring  $A$ ) iff there exist elements  $a, f, b \in R$  such that  $f^{m+n} = 0$ , and  $af^m + f^n b = 1$ .*

As we have observed in the Introduction, under the conditions of the theorem, the base ring  $A$  may not be unique, even up to isomorphism; see, for instance, [Ch<sub>2</sub>], [Ch<sub>3</sub>], [La<sub>3</sub>], [La<sub>4</sub>]. Thus, all we can realistically hope for is an explicit construction of *some* base ring  $A$ . The following result, also based on [AAR], provides such a construction.

**Theorem 2.2.** *Under the conditions of Theorem 2.1, we have  $R \cong \mathbf{M}_{m+n}(A)$  where  $A = \mathbf{I}_R(fR)/fR$ . (Here,  $\mathbf{I}_R(fR)$  denotes the idealizer of the right ideal  $fR$  in  $R$ .)*

**Proof.** Assume that the elements  $a, f, b$  exist (as in Theorem 2.1). By the proof of this theorem in [AAR], there exist two other elements  $c, d \in R$  such that  $cf^{m+n-1} + fd = 1$ .

Furthermore, it was shown that a complete set of  $(m+n) \times (m+n)$  matrix units in  $R$  is given by

$$(2.3) \quad E_{ij} = f^{i-1} c f^{m+n-1} d^{j-1}.$$

Therefore, for  $e := E_{11} = c f^{m+n-1}$ , the work in [AAR] gives  $R \cong \mathbf{M}_{m+n}(A)$ , with the base ring  $A := \text{End}_R(eR)$ . We shall now compute this endomorphism ring more explicitly. Consider the sequence of right  $R$ -modules:

$$(2.4) \quad 0 \longrightarrow fR \longrightarrow R \longrightarrow eR \longrightarrow 0,$$

where the second map is an inclusion, and the third map is left multiplication by  $e$ . This is a zero-sequence since  $e \cdot fR = c f^{m+n-1} fR = c f^{m+n} R = 0$ . We claim that this sequence is exact. Indeed, if  $r \in R$  is such that  $er = 0$ , then in view of the equation  $e + fd = 1$  we have  $r = (1 - e)r = fdr \in fR$ . Therefore,

$$A = \text{End}_R(eR) \cong \text{End}_R(R/fR) \cong \mathbf{I}_R(fR)/fR,$$

where the last isomorphism follows from [Co<sub>2</sub>: (0.7.1)].

**QED**

The quotient ring  $\mathbf{I}_R(fR)/fR$  above is known as the *eigenring* of  $f$ ; we shall henceforth denote it by  $\mathbf{E}_R(f)$ . The advantages in choosing  $\mathbf{E}_R(f)$  to be the base ring are two-fold. First, this ring depends only on a single element  $f \in R$ , and not on the other elements  $a, b, c, d, e$ . Secondly, *the eigenring  $\mathbf{E}_R(f)$  is a ring which we can often compute explicitly*. In concrete situations, we have usually much better control over the nilpotent element  $f$  than over the idempotent  $e = c f^{m+n-1}$ .

**Remarks 2.5.** (A) In the situation of (2.2), we have in fact the following two equations giving explicitly the idealizer ring  $\mathbf{I}_R(fR)$ :

$$(2.6) \quad eRe \oplus fR = \mathbf{I}_R(fR) = Rf^{m+n-1} + fR.$$

The proof of these equations will be left to the reader.

(B) Strictly speaking,  $\mathbf{E}_R(f)$  should be called the *right eigenring* of  $f$ . But fortuitously, in the situation of (2.2), this right eigenring turns out to be isomorphic to the left eigenring  $\mathbf{I}_R(Rf)/Rf$ . This fact will not be needed in the rest of the paper, so its proof will also be left to the reader.

**Example 2.7.** Consider a Morita ring of the form  $T = \begin{pmatrix} R & V \\ W & S \end{pmatrix}$ , as in [Ro: p.35, p.471]. Here  $R, S$  are rings,  $V$  is an  $(R, S)$ -bimodule,  $W$  is an  $(S, R)$ -bimodule, etc. Suppose  $R, S$  are both  $k \times k$  matrix rings, with matrix units  $\{e_{ij}\}$  and  $\{e'_{ij}\}$ . Then  $E_{ij} := \begin{pmatrix} e_{ij} & 0 \\ 0 & e'_{ij} \end{pmatrix}$  are clearly matrix units for  $T$ , so  $T$  is a  $k \times k$  matrix ring over  $C := E_{11} T E_{11}$ . An easy

calculation shows that  $C$  is the Morita ring  $\begin{pmatrix} eRe & eVe' \\ e'We & e'Se' \end{pmatrix}$ , where  $e = e_{11}$ ,  $e' = e'_{11}$ . If  $R$  (resp.  $S$ ) comes with elements  $a, f, b$  (resp.  $a', f', b'$ ) as in (2.1) which give rise to the matrix units  $\{e_{ij}\}$  (resp.  $\{e'_{ij}\}$ ), one can apply (2.2) above to express the base ring  $C$  in terms of  $f$  and  $f'$  alone, namely:  $C \cong \begin{pmatrix} \mathbf{E}_R(f) & \mathbf{E}_V \\ \mathbf{E}_W & \mathbf{E}_S(f') \end{pmatrix}$ , where

$$\mathbf{E}_V := \{v \in V : vf' \in fV\}/fV, \quad \text{and} \quad \mathbf{E}_W := \{w \in W : wf \in f'W\}/f'W.$$

Details of the verifications will be left to the reader.

### §3. Matrix Rings Arising from Ore Extensions

In this section, we give a few applications of Theorems (2.1) and (2.2) to the study of Ore extensions. For the reader's convenience, we first recall some notational conventions. By an Ore extension, we mean a skew polynomial ring  $S := R[t, \sigma, \delta]$ , where  $\sigma$  is an endomorphism of the ring  $R$ , and  $\delta$  is a  $\sigma$ -derivation on  $R$  (an additive map satisfying  $\delta(rr') = \sigma(r)\delta(r') + \delta(r)r'$  for all  $r, r' \in R$ ). Elements of  $S$  are of the form  $\sum r_i t^i$  (with  $r_i \in R$ ), and are multiplied according to the rule  $tr = \sigma(r)t + \delta(r)$  (for all  $r \in R$ ). In the classical case when  $R$  is a division ring, proper quotient rings of  $S$  are all artinian, so the simple quotient rings of  $S$  are always matrix rings (over division rings) by Wedderburn's Theorem. For explicit examples of this nature, see, for instance, [JS: (1.3.15), (1.3.27)], [Ch<sub>3</sub>: (4.5)]. If  $R$  is not a division ring, the chance is not as good, but under suitable assumptions, certain quotients of  $S$  may still be matrix rings; see, for instance, [GW: Ex. 2ZG]. The first theorem in this section completes a result in [AAR]. In the latter, the Ore extension quotient  $T$  studied below was shown to be a  $p^n \times p^n$  matrix ring; using Theorem 2.2, we identify a natural base ring for  $T$ .

**Theorem 3.1.** *Let  $R$  be a ring of prime characteristic  $p > 0$ , and let  $\delta$  be a derivation on  $R$  such that  $\delta^{p^n} = 0$  and  $1 \in \delta^{p^n-1}(R)$ , where  $n \geq 1$  is a fixed integer. Consider the Ore extension  $R[t, \delta]$ , and let  $T = R[t, \delta]/(t^{p^n})$ . Then  $T \cong \mathbf{M}_{p^n}(R_\delta)$ , where  $R_\delta := \ker(\delta)$  is the ring of constants of  $R$  under the derivation  $\delta$ .*

**Proof.** Let  $f$  be the image of  $t$  in  $T$ . In [AAR], it is shown that there is an equation

$$af^{p^{n-1}} + f^{p^n-p^{n-1}}b = 1 \in T$$

for suitable  $a, b \in T$ . Since we also have  $f^{p^n} = 0$ , (2.2) implies that  $T \cong \mathbf{M}_{p^n}(A)$ , where  $A = \mathbf{E}_T(f)$ . We finish by showing that this eigenring is isomorphic to  $R_\delta$ . For convenience, we identify  $R_\delta$  with its image in  $T$ . If we can show that

$$(3.2) \quad \mathbf{I}_T(fT) = fT \oplus R_\delta,$$

then clearly  $\mathbf{E}_T(f) = \mathbf{I}_T(fT)/fT \cong R_\delta$ . To prove (3.2), first note that any  $r \in R_\delta$  commutes with  $f$ , so in particular  $r \in \mathbf{I}_T(fT)$ . Secondly, if  $r \in R_\delta \cap fT$ , then, in  $R[t, \delta]$ , we have  $r \in tR + (t^{p^n}) = tR$ , which implies that  $r = 0$ . Finally, let  $g \in R[t, \delta]$  be the preimage of an arbitrary element in  $\mathbf{I}_T(fT)$ , and write  $g$  in the form  $\sum_i t^i a_i$ . (For the argument below, it is somehow more convenient to express  $g$  as a polynomial with coefficients on the right.) Since  $fT \subseteq \mathbf{I}_T(fT)$ , it follows that  $a_0 = \bar{g} - \sum_{i \geq 1} f^i a_i \in \mathbf{I}_T(fT)$ , so that  $a_0 t \in tR + (t^{p^n}) = tR$ . On the other hand,  $a_0 t = ta_0 - \delta(a_0)$ , so we must have  $\delta(a_0) = 0$ , i.e.  $a_0 \in R_\delta$ . This implies that  $\bar{g} \in fT + R_\delta$ , so the equation (3.2) follows. **QED**

**Remark 3.3.** It is of interest to point out that the assumption  $1 \in \delta^{p^n-1}(R)$  is crucial for the validity of the above theorem. To see this, consider the case when  $R$  is a polynomial ring  $k[x, y]$  over a field  $k$  of characteristic 2, and  $\delta$  is the  $k$ -derivation on  $R$  with  $\delta(x) = 0$  and  $\delta(y) = x$ . In this example, we have  $\delta^2 = 0$  but  $1 \notin \delta(R)$ . (Here we are dealing with  $p = 2$

and  $n = 1$ .) We claim that  $T = R[t, \delta]/(t^2)$  has no nontrivial idempotents; in particular,  $T$  cannot be a  $2 \times 2$  matrix ring. Indeed, if  $e = a + bt + (t^2) \in T$  is an idempotent (where  $a, b \in R$ ), then

$$a + bt \equiv (a + bt)(a + bt) \equiv (a^2 + b \cdot \delta(a)) + b \cdot \delta(b)t \pmod{(t^2)}$$

implies that  $b = b \cdot \delta(b)$  and  $a^2 + b \cdot \delta(a) = a$ . Since  $\delta(b) \neq 1$  (as we have already observed), we must have  $b = 0$  and  $a = a^2$ , so  $e$  can only be a trivial idempotent.

**Example 3.4.** Let  $R = k[x]$ , where  $k$  is a field of characteristic  $p > 0$ , and let  $\delta$  be the  $k$ -derivation  $\frac{d}{dx}$  on  $R$ , so that  $1 = \delta(x) \in \delta(R)$ . It is easy to see that  $\delta^p = 0$ , and that the ring of  $\delta$ -constants in  $R$  is  $R_\delta = k[x^p]$ . For the Weyl algebra  $R[t, \delta]$ , (3.1) (for  $n = 1$ ) gives then an isomorphism

$$R[t, \delta]/(t^p) \cong \mathbf{M}_p(R_\delta) = \mathbf{M}_p(k[x^p]) \cong \mathbf{M}_p(R).$$

As is pointed out in [AAR], this isomorphism can be obtained from (a transformation of) [GW: Ex. 2ZF].

In the rest of this section, we shall study the Ore extension  $S = R[t, \sigma, \delta]$  *itself*, instead of its quotient rings. Goodearl has shown (*c.f.* [Go: (4.6), (7.5), (7.7)]) that  $S$  can sometimes be an  $n \times n$  matrix ring (for some  $n > 1$ ); we shall try to develop this theme further. The following somewhat surprising result shows that, assuming only the existence of an element  $b$  with certain mild properties in  $R$ ,  $S$  will already be a matrix ring (of even size). The argument we use demonstrates a curious connection between the Agnarsson-Amitsur-Robson equations in (2.1) and the formation of an Ore extension.

**Theorem 3.5.** *Let  $S = R[t, \sigma, \delta]$  where  $R \neq 0$ , and let  $m, n$  be positive integers. Suppose  $R$  contains an element  $b$  such that  $b^{m+n} = 0$ , and  $u := \delta(b^m)$ ,  $v := \delta(b^n)$  are in  $U(R)$  (the group of units of  $R$ ). Then  $m = n$ , and  $S \cong \mathbf{M}_{2n}(A)$ , where  $A = \mathbf{E}_S(b)$ . If, moreover,  $b \in \text{rad}(R)$  (the Jacobson radical of  $R$ ), then  $m = n = 1$ , and  $S \cong \mathbf{M}_2(A)$ .*

**Proof.** From  $b^{m+n} = 0$ , we get

$$0 = \delta(b^m b^n) = \sigma(b^m)\delta(b^n) + \delta(b^m)b^n = \sigma(b^m)v + ub^n.$$

Since  $u, v \in U(R)$ , this gives

$$(3.6) \quad u^{-1}\sigma(b^m) = -b^n v^{-1}.$$

On the other hand, we have  $tb^m = \sigma(b^m)t + \delta(b^m)$ . Left-multiplying this by  $u^{-1}$  and using (3.6), we get

$$(u^{-1}t)b^m = u^{-1}\sigma(b^m)t + 1 = -b^n(v^{-1}t) + 1$$

in  $S$ . By (2.2), it follows that  $S \cong \mathbf{M}_{m+n}(A)$ , where  $A = \mathbf{E}_S(b)$ .

Next, we shall prove that, under the hypotheses of the theorem, we must have  $m = n$  (and therefore  $S \cong \mathbf{M}_{2n}(A)$ ). Assume, on the contrary, that  $n \neq m$ ; say,  $n > m$ . From  $v = \delta(b^{n-m}b^m) = \sigma(b^{n-m})u + \delta(b^{n-m})b^m$ , we get

$$(3.7) \quad \sigma(b^{n-m}) = vu^{-1} - \delta(b^{n-m})b^m u^{-1}.$$

On the other hand, left-multiplying (3.6) by  $b^m$ , we get  $b^m u^{-1} \sigma(b^m) = 0$ . Using this with (3.7) above, we see that

$$(3.8) \quad \sigma(b^n) = \sigma(b^{n-m})\sigma(b^m) = [vu^{-1} - \delta(b^{n-m})b^m u^{-1}]\sigma(b^m) = vu^{-1}\sigma(b^m).$$

By induction on  $r \geq 1$ , we shall now show that

$$(3.9) \quad \sigma(b^m) = (uv^{-1})^r \sigma(b^{m+r(n-m)}).$$

For  $r = 1$ , this follows from (3.8) above. Inductively, if (3.9) holds for some  $r$ , then

$$\begin{aligned} \sigma(b^m) &= (uv^{-1})^r \sigma(b^m) \sigma(b^{r(n-m)}) \\ &= (uv^{-1})^r (uv^{-1}) \sigma(b^n) \sigma(b^{r(n-m)}) \\ &= (uv^{-1})^{r+1} \sigma(b^{m+(r+1)(n-m)}). \end{aligned}$$

Now, for a sufficiently large integer  $r$ , we'll have  $r(n-m) \geq n$ , so (3.9) implies that  $\sigma(b^m) = 0$  (since  $b^{n+m} = 0$ ). Going back to (3.6), we have then  $b^n = 0$ , so  $v = \delta(b^n) = 0$ . This is a contradiction, since  $R$  is a nonzero ring.

To prove the last part of the theorem, we shall proceed independently of the arguments above. Assume now that  $b \in \text{rad}(R)$ . By symmetry, it suffices to prove that  $m = 1$ . Suppose, instead, that  $m \geq 2$ . Then

$$u = \delta(b^{m-1}b) = \sigma(b^{m-1})\delta(b) + \delta(b^{m-1})b$$

implies that

$$\sigma(b^{m-1})\delta(b) = u - \delta(b^{m-1})b \in U(R) + \text{rad}(R) \subseteq U(R).$$

Thus,  $R$  has a unit which has a nilpotent left factor (namely,  $\sigma(b^{m-1})$ ). This is impossible in a nonzero ring. **QED**

**Examples 3.10.** (A) An example for the case  $b \in \text{rad}(R)$  is provided by  $(R, \sigma, \delta)$  where  $R$  is the ring of dual numbers  $k[b]$  over a field  $k$  (with  $b^2 = 0$ ),  $\sigma$  is the  $k$ -automorphism of  $R$  defined by  $\sigma(b) = -b$ , and  $\delta$  is the  $\sigma$ -derivation defined by  $\delta(k) = 0$  and  $\delta(b) = 1$ . By (3.5),  $S = R[t, \sigma, \delta] \cong \mathbf{M}_2(\mathbf{E}_S(b))$ . We leave it to the reader to show that the eigenring  $\mathbf{E}_S(b)$  here is isomorphic to the (ordinary) polynomial ring  $k[t]$ .

(B) An example for the case  $m = n = 2$  (with necessarily  $b \notin \text{rad}(R)$ ) can be constructed as follows. Let  $W = k\langle x, y \rangle$  be the Weyl algebra (with relation  $yx - xy = 1$ ) over a field  $k$  of characteristic 2, and let  $\delta$  be the (ordinary)  $k$ -derivation on  $W$  with  $\delta(x) = 1$  and  $\delta(y) = x$ . (Note that  $\delta$  "respects" the relation  $yx - xy = 1$ , which is essentially why it exists.) From

$\delta(y^2) = \delta(y)y + y\delta(y) = xy + yx = 1$ , we get  $\delta(y^4) = \delta(y^2)y^2 + y^2\delta(y^2) = y^2 + y^2 = 0$ . Noting that  $y^2$  (and hence  $y^4$ ) is in the center of  $W$ , we can form the quotient ring  $R := W/y^4W$ . Since  $\delta(y^4) = 0$ ,  $\delta$  induces a derivation on  $R$ , which we again denote by  $\delta$ . For the element  $b := y + y^4W \in R$ , we have therefore  $b^4 = 0$  and  $\delta(b^2) = \delta(y^2) = 1$ . It follows from Theorem 3.5 that the Ore extension  $S = R[t, \delta]$  is isomorphic to  $\mathbf{M}_4(\mathbf{E}_S(b))$ .

**Remark.** In connection with Theorem 3.5, the notion of a ‘‘c.v. polynomial’’ introduced in [LL<sub>2</sub>] can be brought to bear. By definition, a c.v. (‘‘change-of-variable’’) polynomial is a polynomial  $p(t) \in S$  such that  $p(t)b = \sigma'(b)p(t) + \delta'(b)$  for every  $b \in R$ , where  $\sigma'$  is some endomorphism of  $R$ , and  $\delta'$  is some  $\sigma'$ -derivation. Using such a c.v. polynomial  $p(t)$  (if it exists) in lieu of  $t$ , we see by the same argument as in the proof of (3.5) that, if  $R$  is nonzero and contains an element  $b$  such that  $b^{m+n} = 0$  and  $\delta'(b^m), \delta'(b^n) \in U(R)$ , then necessarily  $m = n$ , and  $S = R[t, \sigma, \delta] \cong \mathbf{M}_{2n}(\mathbf{E}_S(b))$ .

Now, even if we don't have a c.v. polynomial at our disposal, the idea of trying to ‘‘commute’’ a skew polynomial with a scalar can be used to find more instances where an Ore extension  $S$  is a full matrix ring. This time, we shall choose the skew polynomial to be  $t^{n-1}$  and the scalar to be  $b^{n-1}$ , where  $n$  is a fixed integer such that  $b^n = 0$ . In order to make the necessary computations, we shall need some more notations in working with an Ore extension  $S = R[t, \sigma, \delta]$ . As in [LL<sub>1</sub>: p.310], we define  $f_j^i \in \text{End}(R, +)$  to be the sum of all possible  $i$ -fold products with  $j$  factors of  $\sigma$  and  $i - j$  factors of  $\delta$ . (For instance,  $f_0^i = \delta^i$ ,  $f_i^i = \sigma^i$ ,  $f_1^i = \delta^{i-1}\sigma + \delta^{i-2}\sigma\delta + \cdots + \delta\sigma\delta^{i-2} + \sigma\delta^{i-1}$ , etc.) The operators  $f_j^i$  arise naturally in connection with the commutation rule

$$(3.11) \quad t^i r = \sum_{j=0}^i f_j^i(r) t^j \quad (\forall r \in R),$$

which is easily verified by induction. We first prove the following preliminary result.

**Lemma 3.12.** *Let  $S = R[t, \sigma, \delta]$  be as above, where  $R$  is any ring. Let  $b \in R$  be such that  $b\delta(b) = \delta(b)b$  and  $\sigma(b) = qb = bq$ , where  $q \in R$ . Then, for any  $i \geq j \geq 0$  and any  $k \geq i - j$ , we have  $f_j^i(b^k) \in b^{k+j-i}R$ .*

**Proof.** We proceed by induction on  $i$ . First consider the case  $i = 1$ . If  $j = 1$  also, we have

$$f_1^1(b^k) = \sigma(b^k) = \sigma(b)^k = (bq)^k = b^k q^k,$$

which lies in  $b^k R = b^{k+1-1}R$ . If  $j = 0$ , we have  $f_0^1(b^k) = \delta(b^k)$ , so it suffices to show that  $\delta(b^k) \in b^{k-1}R$ . Now, by a straightforward computation (see [Go: Lemma 1.1]), we have (for any  $b$ ):

$$\delta(b^k) = \sum_{j=0}^{k-1} \sigma(b)^j \delta(b) b^{k-1-j}.$$



Since  $\sigma(b) = bq$  and  $b$  commutes with  $q$  and  $\delta(b)$ , this yields

$$(3.13) \quad \delta(b^k) = b^{k-1}(1 + q + q^2 + \cdots + q^{k-1})\delta(b) \in b^{k-1}R.$$

Therefore, we are done in the case  $i = 1$ . Now suppose the lemma is true for some  $i$ . To get the case  $i + 1$ , we use the (obvious) operator equation  $f_j^{i+1} = \sigma f_{j-1}^i + \delta f_j^i$ . Applying this to  $b^k$  ( $k \geq i + 1 - j$ ) and using the inductive hypothesis, we have

$$\begin{aligned} f_j^{i+1}(b^k) &= \sigma f_{j-1}^i(b^k) + \delta f_j^i(b^k) \\ &= \sigma(b^{k+j-1-i}r_1) + \delta(b^{k+j-i}r_2) \quad (\text{for suitable } r_1, r_2 \in R) \\ &= b^{k+j-1-i}q^{k+j-1-i}\sigma(r_1) + b^{k+j-i}q^{k+j-i}\delta(r_2) + \delta(b^{k+j-i})r_2. \end{aligned}$$

By (3.13),  $\delta(b^{k+j-i}) = b^{k+j-1-i}r_3$  for some  $r_3 \in R$ . This, together with the above equations, clearly shows that  $f_j^{i+1}(b^k) \in b^{k+j-(i+1)}R$ , as desired. **QED**

We can now state our next main result in this section, which is inspired by an earlier result of Goodearl [Go: (7.5)].

**Theorem 3.14.** *Let  $S = R[t, \sigma, \delta]$ , and let  $b \in R$  be such that  $b^n = 0$ ,  $b\delta(b) = \delta(b)b$  and  $\sigma(b) = qb = bq$  for some  $q \in R$ . If  $u := \delta^{n-1}(b^{n-1})$  is a unit of  $R$  commuting with  $b$ , then  $S$  is an  $n \times n$  matrix ring; in fact,  $S \cong \mathbf{M}_n(A)$  where  $A$  is the eigenring  $\mathbf{E}_S(b)$ .*

**Proof.** Using (3.11) and (3.12), we have

$$\begin{aligned} t^{n-1}b^{n-1} &= \sum_{j=0}^{n-1} f_j^{n-1}(b^{n-1}) t^j \\ &= \sum_{j=1}^{n-1} f_j^{n-1}(b^{n-1}) t^j + f_0^{n-1}(b^{n-1}) \\ &= \sum_{j=1}^{n-1} b^j s_j + \delta^{n-1}(b^{n-1}), \end{aligned}$$

for suitable  $s_j \in S$ . Therefore, we have

$$(3.15) \quad t^{n-1}b^{n-1} = bs + u \quad \text{for some } s \in S.$$

Since  $b$  commutes with  $u$  (and hence also with  $u^{-1}$ ), left-multiplication of (3.15) by  $u^{-1}$  yields

$$(u^{-1}t^{n-1})b^{n-1} = u^{-1}(bs + u) = b(u^{-1}s) + 1.$$

Thus, we have  $ab^{n-1} + bc = 1$  for suitable  $a, c \in S$ , and Theorem 2.2 implies that  $S \cong \mathbf{M}_n(A)$  for  $A = \mathbf{E}_S(b)$ . **QED**

Note that, in the case  $n = 2$ , (3.5) would have given a better result, with only the hypotheses  $b^2 = 0$ ,  $\delta(b) \in U(R)$ , and nothing else. Thus, one should use (3.10) only when  $n \geq 3$ . A similar remark applies to (3.16) below.

Note that the crucial condition in (3.14) is that  $u := \delta^{n-1}(b^{n-1})$  be a *unit* in  $R$  (commuting with  $b$ ). If we assume a couple more mild properties on  $q$  and on  $\delta(b)$ , this condition can be formulated more explicitly, as follows.

**Corollary 3.16.** *Let  $S = R[t, \sigma, \delta]$ . Suppose  $R$  contains an element  $b$  such that  $b^n = 0$ ,  $b\delta(b) = \delta(b)b$  and  $\sigma(b) = qb = bq$ , where  $q \in R$ . If, moreover,  $q, \delta(b) \in R_\delta$ ,  $\delta(b) \in U(R)$ , and  $u_i := 1 + q + \cdots + q^{i-1} \in U(R)$  for all  $i < n$ , then  $S$  is an  $n \times n$  matrix ring; in fact,  $S \cong \mathbf{M}_n(A)$  where  $A$  is the eigenring  $\mathbf{E}_S(b)$ .*

**Proof.** Recall from (3.13) that  $\delta(b^k) = b^{k-1}u_k\delta(b)$ . Since  $q$  and  $\delta(b)$  both belong to  $R_\delta$ , so does the product  $u_k\delta(b)$ . Therefore, another application of  $\delta$  gives

$$\delta^2(b^k) = \delta(b^{k-1})u_k\delta(b) = b^{k-2}u_{k-1}\delta(b)u_k\delta(b).$$

Proceeding in this manner, we get

$$\delta^k(b^k) = u_1\delta(b)u_2\delta(b) \cdots u_k\delta(b).$$

For  $k = n - 1$ , it follows easily from our hypotheses that  $u := \delta^{n-1}(b^{n-1})$  is a unit, and that  $ub = bu$ . Therefore, Theorem 3.14 applies. **QED**

**Remark 3.17.** We may further simplify our hypotheses by assuming that  $\delta(b) = 1$ . In this case, certainly  $\delta(b)$  is a unit commuting with  $b$ , and is of course a  $\delta$ -constant. If we also assume that  $\sigma(b) = b$ , then we can take  $q = 1$ , which certainly commutes with  $b$  and is a  $\delta$ -constant. In this case,  $u_i$  is just  $i \cdot 1$ , so we need only assume that each of  $2, 3, \dots, n - 1$  is a unit in  $R$ . This is true, for instance, if  $R$  is an algebra over a field whose characteristic is either 0 or at least  $n$ . Therefore, there are many concrete situations to which our results (3.14), (3.16) can be applied.

It is of interest to compare our result (3.14) with Goodearl's [Go: (7.5)]. In (3.14), our hypotheses on  $b$  are of a "local" nature, and are considerably weaker than those in [Go: (7.5)]. For instance, we need not assume (as Goodearl did) that  $b, q$  are *central* elements in  $R$ , or that  $1 + q + \cdots + q^{n-1} = 0$  (which would imply that  $q$  is an  $n$ th root of unity). If we work under Goodearl's assumptions in [Go: (7.5)], then in the notations of (3.14) it can be checked that  $\delta^n$  is an ordinary derivation stabilizing  $bR$ . In this case, it is relatively straightforward to compute that the eigenring  $\mathbf{E}_S(b)$  is isomorphic to the differential polynomial ring  $(R/bR)[t', \delta^n]$ . Therefore, (3.10) will give directly Goodearl's conclusion that  $R[t, \sigma, \delta] \cong \mathbf{M}_n((R/bR)[t', \delta^n])$ .

#### §4. Recognition Theorems and $n$ th Root Properties

In this section, we derive a list of new characterizations of an  $n \times n$  matrix ring  $R$  involving  $n$ th roots of nilpotent matrices over  $R$ . The result (4.1) below may be viewed as a multipronged extension of Robson's theorem [R: (2.2)], which is used in the proof (see (1)  $\implies$  (7)). Part of the subtlety of (4.1) lies in the repeated changes of quantifiers from one set of conditions to another.

**Theorem 4.1.** *Let  $R$  be a ring, and  $n \geq 2$  be a fixed integer. Then the following statements are equivalent:*

- (1)  $R$  is an  $n \times n$  matrix ring (over some ring  $A$ ).
- (2) For any  $r \geq 2$ , the matrix

$$(4.2) \quad F_0 := E_{2,1} + E_{3,2} + \cdots + E_{r,r-1} \in \mathbf{M}_r(R)$$

has an  $n$ th root in  $\mathbf{M}_r(R)$ .

- (3) For some  $r \geq 2$ , the matrix  $F_0$  in (4.2) has an  $n$ th root in  $\mathbf{M}_r(R)$ .
- (4) For some  $r \geq 2$ , there exist non right-0-divisors  $d_1, \dots, d_{r-1} \in R$ , at least one of which is a unit, such that the matrix

$$(4.3) \quad F := d_1 E_{2,1} + d_2 E_{3,2} + \cdots + d_{r-1} E_{r,r-1} \in \mathbf{M}_r(R)$$

has an  $n$ th root in  $\mathbf{M}_r(R)$ .

- (5) For any  $r \geq 2$  and any central elements  $d_1, \dots, d_{r-1} \in R$ , the matrix  $F$  in (4.3) has an  $n$ th root in  $\mathbf{M}_r(R)$ .
- (5') For any  $r \geq 2$  and any units  $d_1, \dots, d_{r-1} \in R$ , the matrix  $F$  in (4.3) has an  $n$ th root in  $\mathbf{M}_r(R)$ .
- (6) There exist elements  $b, f, g \in R$  such that  $f^n = g^n = 0$  and  $bf^{n-1} + gbf^{n-2} + g^2bf^{n-3} + \cdots + g^{n-1}b \in U(R)$ .
- (6') There exist elements  $f, g \in R$  such that  $f^n = g^n = 0$  and  $f^{n-1} + gfn^{n-2} + g^2fn^{n-3} + \cdots + g^{n-1} \in U(R)$ .
- (7) There exist elements  $c, g \in R$  such that  $g^n = 0$  and  $cg^{n-1} + gcn^{n-2} + g^2cn^{n-3} + \cdots + g^{n-1}c = 1$ .
- (7') There exist elements  $c, g \in R$  such that  $g^n = 0$  and  $cg^{n-1} + gcn^{n-2} + g^2cn^{n-3} + \cdots + g^{n-1}c \in U(R)$ .
- (8) For any unit  $u \in U(R)$ , there exist elements  $b, f, g \in R$  such that  $f^n = g^n = 0$  and  $u = bf^{n-1} + gbf^{n-2} + g^2bf^{n-3} + \cdots + g^{n-1}b$ .

**Proof.** We first prove the cyclical equivalence of (1) through (7) (leaving out (5'), (6') and (7') for the moment). To begin with, we have the obvious implications (5)  $\implies$  (2)  $\implies$  (3)  $\implies$  (4).

(4)  $\implies$  (6) Without loss of generality, we may assume that the element  $d_1$  in (4) is a unit. Suppose  $F = X^n$  for some  $X = (x_{ij}) \in \mathbf{M}_r(R)$ . Then,  $X$  commutes with  $X^n = F$ . Writing out the first two rows of the two sides of the equation  $F X = X F$ , we have

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ d_1 x_{11} & d_1 x_{12} & \cdots & d_1 x_{1r} \end{pmatrix} = \begin{pmatrix} x_{12} d_1 & x_{13} d_2 & \cdots & x_{1r} d_{r-1} & 0 \\ x_{22} d_1 & x_{23} d_2 & \cdots & x_{2r} d_{r-1} & 0 \end{pmatrix}.$$

Since the  $d_i$ 's are not right-0-divisors, we must have  $x_{1j} = 0$  for all  $j \geq 2$ , and therefore  $x_{2k} = 0$  for all  $k \geq 3$ . Writing

$$f = x_{11}, \quad g = x_{22}, \quad \text{and} \quad b = x_{21},$$

we can express  $X$  as a block matrix<sup>2</sup>  $\begin{pmatrix} Y & 0 \\ W & Z \end{pmatrix}$ , with  $Y = \begin{pmatrix} f & 0 \\ b & g \end{pmatrix}$ . The  $n$ th power of  $X$  has the form  $X^n = \begin{pmatrix} Y^n & 0 \\ * & Z^n \end{pmatrix}$ , so it follows that  $Y^n = \begin{pmatrix} 0 & 0 \\ d_1 & 0 \end{pmatrix}$ . On the other hand, by an easy induction on  $n$ , we have  $Y^n = \begin{pmatrix} f^n & 0 \\ u & g^n \end{pmatrix}$ , where

$$u := b f^{n-1} + g b f^{n-2} + g^2 b f^{n-3} + \cdots + g^{n-1} b.$$

Thus we must have  $f^n = g^n = 0$  and  $u = d_1 \in U(R)$ .

(6)  $\implies$  (7) Let  $u := b f^{n-1} + g b f^{n-2} + g^2 b f^{n-3} + \cdots + g^{n-1} b \in U(R)$  in (6). Left-multiplying by  $g$  and right-multiplying by  $f$ , we get

$$g u = g b f^{n-1} + g^2 b f^{n-2} + \cdots + g^{n-1} b f = u f.$$

Therefore, for  $v := u^{-1}$ , we have  $f v = v g$ , so by induction on  $i \geq 0$  we get  $f^i v = v g^i$ . Right-multiplying the expression for  $u$  by  $v$ , we get

$$\begin{aligned} 1 &= b f^{n-1} v + g b f^{n-2} v + g^2 b f^{n-3} v + \cdots + g^{n-1} b v \\ &= b v g^{n-1} + g b v g^{n-2} + g^2 b v g^{n-3} + \cdots + g^{n-1} b v \\ &= c g^{n-1} + g c g^{n-2} + g^2 c g^{n-3} + \cdots + g^{n-1} c, \end{aligned}$$

where  $c := b v \in R$ . This proves (7).

(7)  $\implies$  (1) is part of Robson's result, namely, (ii)  $\implies$  (i) in [R: (2.2)]. (Incidentally, we shall not need the other parts of Robson's result.)

(1)  $\implies$  (5) Suppose  $R = \mathbf{M}_n(A)$ , where  $A$  is some ring. Since the elements  $d_i$ 's in (5) are *central* in  $R$ , they must be scalar matrices in  $\mathbf{M}_n(A)$  [La<sub>2</sub>: p.5, Ex.1.9]; say  $d_i = a_i I$ , where

---

<sup>2</sup>The method of comparing entries of  $F X = X F$  actually shows  $X$  to be a *lower triangular* matrix. This information is, however, not needed for the arguments to follow.

$a_i \in A$ , and  $I$  denotes the  $n \times n$  identity matrix over  $A$ . As usual, we identify  $\mathbf{M}_r(R)$  with  $\mathbf{M}_{rn}(A)$ . Under this identification, the matrix  $F \in \mathbf{M}_r(R)$  becomes the matrix

$$(4.4) \quad \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ a_1 I & 0 & 0 & & & \\ 0 & a_2 I & 0 & & & \\ & & & \ddots & & \vdots \\ & & & \ddots & \ddots & \\ 0 & 0 & 0 & \cdots & a_{r-1} I & 0 \end{pmatrix}$$

with  $n \times n$  blocks as its “entries”. We shall construct an explicit  $n$ th root for  $F$  in  $\mathbf{M}_{rn}(A)$ . Consider a matrix

$$C = c_1 E_{2,1} + c_2 E_{3,2} + \cdots + c_{rn-1} E_{rn, rn-1} \in \mathbf{M}_{rn}(A).$$

By direct matrix multiplication, we see that

$$C^2 = c_2 c_1 E_{3,1} + c_3 c_2 E_{4,2} + \cdots + c_{rn-1} c_{rn-2} E_{rn, rn-2},$$

$$C^3 = c_3 c_2 c_1 E_{4,1} + c_4 c_3 c_2 E_{5,2} + \cdots + c_{rn-1} c_{rn-2} c_{rn-3} E_{rn, rn-3},$$

etc. Therefore, if we choose the  $c_i$ 's such that  $c_{jn} = a_j$  for all  $j \leq r-1$ , and  $c_i = 1$  for all  $i$  not divisible by  $n$ , the power  $C^n$  will be precisely the matrix in (4.4), i.e.  $C^n = F \in \mathbf{M}_{rn}(A) = \mathbf{M}_r(R)$ , as desired.

Having proved the equivalence of (1) through (7), it is now easy to extend the equivalence to the other four conditions (5'), (6'), (7') and (8). First, it is clear that any of these conditions implies one of the conditions (1) to (7). (For instance, (5') implies (2), and each of (6'), (7') and (8) implies (6).) Therefore, it suffices to show each of them also *follows* from one of (1) through (7).

(7)  $\implies$  (7') is clear.

(7)  $\implies$  (8) Given  $u \in U(R)$  and the equation in (7), let  $b := cu$ . Then  $c = bu^{-1}$ , and we have  $1 = bu^{-1}g^{n-1} + gbu^{-1}g^{n-2} + \cdots + g^{n-1}bu^{-1}$ . Right-multiplying by  $u$ , we get

$$\begin{aligned} u &= bu^{-1}g^{n-1}u + gbu^{-1}g^{n-2}u + \cdots + g^{n-1}b \\ &= b(u^{-1}gu)^{n-1} + gb(u^{-1}gu)^{n-2} + \cdots + g^{n-1}b. \end{aligned}$$

Therefore, for  $f := u^{-1}gu$ , we have  $f^n = u^{-1}g^nu = 0$  and  $u = bf^{n-1} + gbf^{n-2} + g^2bf^{n-3} + \cdots + g^{n-1}b$ . This checks (8).

(1)  $\implies$  (6') Say  $R = \mathbf{M}_n(A)$ . Let

$$f = E_{1,2} + E_{2,3} + \cdots + E_{n-1,n} \quad \text{and} \quad g = E_{2,1} + E_{3,2} + \cdots + E_{n,n-1} \quad \text{in } R,$$

which, of course, satisfy  $f^n = g^n = 0$ . A direct calculation shows that

$$f^{n-1} + gf^{n-2} + g^2f^{n-3} + \dots + g^{n-1}$$

is a matrix with 1's on the "opposite diagonal" (the  $(1, n)$ ,  $(2, n-1)$ ,  $\dots$ ,  $(n, 1)$  entries), 0's above and integers below this opposite diagonal. Such a matrix is obviously invertible in  $\mathbf{M}_n(\mathbf{Z})$ , and therefore also invertible in  $R = \mathbf{M}_n(A)$ . This checks (6').

(2)  $\implies$  (5') The trick here is that, in any  $\mathbf{M}_r(R)$  ( $r \geq 2$ ), we can construct an  $n$ th root of  $F$  from an  $n$ th root of  $F_0$  (if the  $d_i$ 's are units in  $R$ ). In fact, let  $X_0$  be an  $n$ th root of  $F_0$  in  $\mathbf{M}_r(R)$ . Consider the invertible diagonal matrix

$$D := \text{diag}(1, d_1, d_2d_1, d_3d_2d_1, \dots, d_{r-1} \cdots d_2d_1) \in \mathbf{M}_r(R),$$

and let  $X := DX_0D^{-1}$ . Then  $X^n = DX_0^nD^{-1} = DF_0D^{-1}$ . The matrix on the RHS is computed by left-multiplying the rows of  $F_0$  by  $1, d_1, d_2d_1, d_3d_2d_1, \dots$ , and then right-multiplying the columns of the resulting matrix by  $1, d_1^{-1}, d_1^{-1}d_2^{-1}, d_1^{-1}d_2^{-1}d_3^{-1}, \dots$ . A moment's reflection shows that this yields the matrix  $F$ . Therefore,  $X^n = DF_0D^{-1} = F$ , as desired. **QED**

**Remarks 4.5.** (A) For the proof of (1)  $\implies$  (5) above, it might seem to a casual reader that we were only using the fact that  $\mathbf{M}_r(R)$  is an  $rn \times rn$  matrix ring (instead of the stronger fact that  $R$  itself is an  $n \times n$  matrix ring). However, this is not the case. For the argument above to work, we need to have  $R = \mathbf{M}_n(A)$  in order to identify  $F$  with the matrix in (4.4); this is *not* guaranteed by an arbitrary isomorphism from  $\mathbf{M}_r(R)$  to  $\mathbf{M}_{rn}(A)$ . In general, if we are only given that  $\mathbf{M}_r(R)$  is an  $rn \times rn$  matrix ring, the condition (5) (or equivalently, any of the other conditions) in the Theorem will *not* follow. To see this, look at the case when  $n = 2$ , and use the known fact that there exist (noncommutative) domains  $R$  such that  $\mathbf{M}_2(R) \cong \mathbf{M}_4(R)$  (see [Co<sub>1</sub>], or [La<sub>4</sub>: (8.3)]). For such a ring  $R$ ,  $\mathbf{M}_2(R)$  is a  $4 \times 4$  matrix ring, but the fact that  $R$  is a domain clearly precludes  $R$  from being a ring of  $2 \times 2$  matrices. Therefore, none of the conditions (2) through (8) can hold.

(B) In the condition (4) above, it is also essential to assume that at least one of the non-0-divisors  $d_1, \dots, d_{r-1}$  be actually a *unit* in  $R$ . For instance, let  $R$  be the ring  $\begin{pmatrix} \mathbf{Z} & 2\mathbf{Z} \\ 2\mathbf{Z} & \mathbf{Z} \end{pmatrix}$ , and let  $f = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ , and  $g = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$  in  $R$ . Then  $d_1 := f + g = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$  is a non-0-divisor but not a unit in  $R$ . Since  $f^2 = g^2 = 0$ , the matrix  $\begin{pmatrix} 0 & 0 \\ d_1 & 0 \end{pmatrix}$  has a square root  $\begin{pmatrix} f & 0 \\ 1 & g \end{pmatrix}$  in  $\mathbf{M}_2(R)$ . However,  $R$  is *not* a  $2 \times 2$  matrix ring since it admits a homomorphism into  $\mathbf{Z}_2 \times \mathbf{Z}_2$  sending  $(a_{ij})$  into  $(a_{11}, a_{22}) \pmod{2}$ . The same example shows that, in the conditions (6), (6') and (7'), it is essential to assume that the sums there be *units*, instead of just non-0-divisors.

(C) In case the conditions of Theorem 4.1 hold, a base ring for the  $n \times n$  matrix ring  $R$  can be easily computed, by our earlier result (2.2). In fact, if  $R$  contains elements  $c, g$  such

that  $g^n = 0$  and  $cg^{n-1} + gcg^{n-2} + g^2cg^{n-3} + \cdots + g^{n-1}c = 1$  (as in (7')), then we have  $cg^{n-1} + gd = 1$  for  $d := cg^{n-2} + gcg^{n-3} + \cdots + g^{n-2}c$ . From (2.2) and the proof of (4.1), it follows immediately that, under *any* of the conditions (6), (6'), (7), (7'), or (8), a base ring for the  $n \times n$  matrix ring  $R$  can be taken to be the eigenring  $\mathbf{E}_R(g)$ .

It is also worth pointing out that, in the case  $n = 2$ , (1)  $\iff$  (6') in Theorem 4.1 recaptures the result of Fuchs, Maxson and Pilz ([FMP, Th. III.2], [Fu: Cor. 4]) on the characterization of  $2 \times 2$  matrix rings, namely:  *$R$  is a  $2 \times 2$  matrix ring iff it contains elements  $f, g$  such that  $f^2 = g^2 = 0$  and  $f + g \in U(R)$ .* The general equivalence (1)  $\iff$  (6') in Theorem 4.1 is thus a generalization of the Fuchs-Maxson-Pilz result to the  $n \times n$  case. Note that our generalization is different from that of Fuchs in [Fu: Th. 1]. Fuchs' generalization involves the use of annihilators in  $R$ , but our generalization involves only an existential equation with nilpotent elements in  $R$ , in the same spirit as in the  $2 \times 2$  case.

For a concrete and explicit conclusion deducible from Theorem 4.1, we record the following:

**Corollary 4.6.** *Let  $d_i \in R$  be as in (4) in (4.1), and assume that  $R$  admits a (unital) homomorphism into a nonzero ring  $S$  which is either commutative, or reduced, or without nontrivial idempotents. Then the matrix*

$$F = d_1E_{2,1} + d_2E_{3,2} + \cdots + d_{r-1}E_{r,r-1} \in \mathbf{M}_r(R)$$

*cannot have an  $n$ th root in  $\mathbf{M}_r(R)$  for any  $r, n \geq 2$ .*

**Proof.** Assume that  $F$  has an  $n$ th root in  $\mathbf{M}_r(R)$ . Then, by the Theorem,  $R$  is an  $n \times n$  matrix ring. But then  $S$  is also an  $n \times n$  matrix ring (by [Ro: (1.1.22)]), which is impossible. **QED**

## §5. A Result on Hidden Matrices

We conclude this paper with a generalization of an arithmetic result of Levy, Robson and Stafford on  $2 \times 2$  matrices over the integer quaternions  $\mathbf{H} = \mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}k$ . In [LRS: (6.8)], it is shown that, for any odd prime  $p$ , the subring  $T(p) = \mathbf{H} + \mathbf{M}_2(p\mathbf{H})$  of  $\mathbf{M}_2(\mathbf{H})$  is a  $2 \times 2$  matrix ring iff  $p \equiv 1 \pmod{4}$ . The proof of this result in [LRS] involves the notion of genus class groups. We shall improve this result below by considering  $T(c)$  for any positive integer  $c$ , using (for the sufficiency part) entirely elementary arguments.

**Proposition 5.1.** *For any positive integer  $c$ , the ring  $T(c) = \mathbf{H} + \mathbf{M}_2(c\mathbf{H})$  is a  $2 \times 2$  matrix ring iff any prime divisor  $p|c$  satisfies  $p \equiv 1 \pmod{4}$ .*

**Proof.** For any prime  $p|c$ , we have  $T(c) \subseteq T(p)$ . If  $p \equiv 3 \pmod{4}$ ,  $T(p)$  is not a  $2 \times 2$  matrix ring by [LRS: (6.8)], so neither is  $T(c)$ . Now assume  $p = 2$  (so  $c$  is even). There is a ring homomorphism  $\phi : T(2) \rightarrow \mathbf{H}/2\mathbf{H}$  sending a matrix  $\begin{pmatrix} t & u \\ v & w \end{pmatrix} \in T(2)$  to  $t \pmod{2\mathbf{H}}$ .

Since  $\mathbf{H}/2\mathbf{H}$  is commutative,  $T(2)$  is not a  $2 \times 2$  matrix ring, so neither is  $T(c)$ . This proves the “necessity” part of the Proposition. To prove the “sufficiency” part, assume now that any prime dividing  $c$  is congruent to 1 (mod 4). Then the same property holds for  $c^2$ . By a standard result in number theory [NZ: p.151], there is a *primitive* expression of  $c^2$  as a sum of two squares, i.e. an expression  $c^2 = a^2 + b^2$  where  $(a, b) = 1$ . It follows that  $(c^2, 2a) = 1$ , so there is an equation

$$c^2d - 2ad' = 1 \quad (\text{where } d, d' \in \mathbf{Z}).$$

To prove that  $T := T(c)$  is a  $2 \times 2$  matrix ring, it suffices (by (7)  $\implies$  (1) in (5.1)) to construct two matrices  $A, F \in T$  such that  $F^2 = 0$  and  $AF + FA = 1$ . Let  $x = ai + bj \in \mathbf{H}$ , and  $w = ck \in c\mathbf{H}$ . Since  $x, w$  anticommute, with  $x^2 = -(a^2 + b^2) = -c^2 = w^2$ , the matrix  $F = \begin{pmatrix} x & -w \\ w & x \end{pmatrix} \in T$  has square zero. Letting  $A$  be the matrix  $\begin{pmatrix} d'i & 0 \\ cdk & d'i \end{pmatrix} \in T$ , we check easily that  $AF + FA = 1$ . **QED**

In the process of writing up this paper for publication, we received a research report of Chatters [Ch<sub>4</sub>] from which we learned that he has also given similar constructions of the matrices  $A$  and  $F$  in the “sufficiency” proof above. However, our explicit description of the integers  $c$  in the Proposition seems new, and this description led directly to the complete “iff” formulation in (5.1).

## References

- [AAR] G. Agnarsson, S. A. Amitsur and J. C. Robson: *Recognition of matrix rings*, II, this memorial issue, pp.
- [Ch<sub>1</sub>] A. W. Chatters: *Representation of tiled matrix rings as full matrix rings*, Math. Proc. Camb. Phil. Soc. **105**(1989), 67-72.
- [Ch<sub>2</sub>] A. W. Chatters: *Matrices, idealisers, and integer quaternions*, J. Algebra **150**(1992), 45-56.
- [Ch<sub>3</sub>] A. W. Chatters: *Nonisomorphic rings with isomorphic matrix rings*, Proc. Edinburgh Math. Soc. **36**(1993), 339-348.
- [Ch<sub>4</sub>] A. W. Chatters: *How to find hidden matrix units*, University of Bristol Mathematical Research Report No. PM-93-04, 1993.
- [Co<sub>1</sub>] P. M. Cohn: *Some remarks on the invariant basis property*, Topology **5**(1966), 215-228.
- [Co<sub>2</sub>] P. M. Cohn: *Free Rings and Their Relations*, Second Edition, London Math. Soc. Monographs, Vol. **19**, Academic Press, London-New York, 1985.



- [Fu] P. R. Fuchs: *A characterisation result for matrix rings*, Bull. Austral. Math. Soc. **43**(1991), 265-267.
- [FMP] P. R. Fuchs, C. J. Maxson and G. F. Pilz: *On rings for which homogeneous maps are linear*, Proc. Amer. Math. Soc. **112**(1991), 1-7.
- [Go] K. R. Goodearl: *Prime ideals in skew polynomial rings and quantized Weyl algebras*, J. Algebra **150**(1992), 324-377.
- [GW] K. R. Goodearl and R. B. Warfield: *An Introduction to Noncommutative Noetherian Rings*, London Math. Soc. Student Text Series, Vol. 16, Cambridge University Press, Cambridge, 1989.
- [JS] N. Jacobson and D. Saltman: *Finite Dimensional Division Algebras*, Springer-Verlag, to appear.
- [La<sub>1</sub>] T. Y. Lam: *A First Course in Noncommutative Rings*, Graduate Texts in Math., Vol. **131**, Springer-Verlag, Berlin-Heidelberg-New York, 1991.
- [La<sub>2</sub>] T. Y. Lam: *Exercises in Classical Ring Theory*, Problem Books in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 1995.
- [La<sub>3</sub>] T. Y. Lam: *A lifting theorem, and rings with isomorphic matrix rings*, in "Five Decades as a Mathematician and Educator: On the 80th Birthday of Professor Y. C. Wong," (eds. K. Y. Chan and M. C. Liu), pp.169-186, World Scientific Publ. Co., Singapore-London-Hong Kong, 1995.
- [La<sub>4</sub>] T. Y. Lam: *Modules with isomorphic multiples, and rings with isomorphic matrix rings, a survey*, preprint, University of California, Berkeley, 1996.
- [LL<sub>1</sub>] T. Y. Lam and A. Leroy: *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119**(1988), 308-336.
- [LL<sub>2</sub>] T. Y. Lam and A. Leroy: *Homomorphisms between Ore extensions*, Azumaya Algebras, Actions and Modules (D. Haile and J. Osterburg, eds.), Contemporary Math., vol. 124, pp. 83-110, Amer. Math. Soc., Providence, R.I., 1992.
- [LRS] L. S. Levy, J. C. Robson and J. T. Stafford: *Hidden matrices*, Proc. London Math. Soc. **69**(1994), 277-308.
- [NZ] I. Niven and H. S. Zuckerman: *An Introduction to the Theory of Numbers*, 4th edition, J. Wiley and Sons, New York, 1980.
- [R] J. C. Robson: *Recognition of matrix rings*, Comm. Algebra **19**(1991), 2113-2124.
- [Ro] L. Rowen: *Ring Theory, I*, Academic Press, Boston-New York-London, 1988.