Journal of Algebra **231**, 691–704 (2000)
doi:10.1006/jabr.2000.8350, available online at http://www.idealibrary.com on IDEAL

# Rings of Order $p^5$
# Part II. Local Rings

B. Corbas and G. D. Williams



E-mail: {b.corbas, g.d.williams}@reading.ac.uk

*Communicated by Peter M. Neumann*

Received February 2, 1999

The structure and classification up to isomorphism of all *local* rings of order $p^5$ are given here. This completes the determination of all rings of this order, which was begun in the companion to this paper. © 2000 Academic Press
*Key Words:* finite rings; local rings.

## INTRODUCTION

The present paper is a sequel to [1] and concludes our determination of all rings of order $p^5$, where $p$ is prime. In Part I we classified all except the local rings, and it is to the latter case that we now address ourselves.

Throughout $R$ will denote a *local* ring of order $p^5$ having prime subring $A$, Jacobson radical $J$, and residue field $R/J = \mathbf{F}_{p^r}$. The notations introduced in Section 2 of [1] will remain in force. In particular $K$ denotes $\mathbf{F}_p$, $\Sigma_m$ is a set of coset representatives of $K^{*m}$ in $K^*$, $\Sigma_m^0 = \Sigma_m \cup \{0\}$, and $d_i$ is the dimension of $J^i/J^{i+1}$ over $R/J$. As in the lower orders, we shall use the decimal numbering $k.d_1.d_2$ to distinguish the cases, $p^k$ being the characteristic of $R$, suppressing the $d_i$ when they are irrelevant. In what follows we shall make frequent use of the preliminary results obtained in [1]. Recall in particular that, with the single exception of $R = \mathbf{F}_{p^5}$, we have $r = 1$, so that $R/J = K$ and $|J| = p^4$. For convenience we divide our account into sections, one for each of the characteristics $p, \dots, p^5$.



0021-8693/00 $35.00

## 1. CHARACTERISTIC $p$

In this case $A = K = \mathbf{F}_p$. The rings are as follows.

**1.0.** $\mathbf{F}_{p^5}$.

**1.1.** $K[X]/(X^5)$ [1, Lemma 2.2].

**1.2.1.** Choose $x, y, z, t \in J$ such that $J = Kx \oplus Ky \oplus J^2$, $J^2 = Kz \oplus J^3$, and $J^3 = Kt$. Then $x^2 = \alpha_1 z + \alpha_2 t$, $xy = \beta_1 z + \beta_2 t$, $yx = \gamma_1 z + \gamma_2 t$, $y^2 = \delta_1 z + \delta_2 t$, with coefficients in $K$. Now $J^3 = Jz = Kxz + Kyz$, so we may assume that $Kyz \subset Kxz$, say $yz = \lambda xz$. Replacing $y$ by $y - \lambda x$ allows us to assume that $yz = 0$, and, multiplying $x$ by a scalar, we may take $xz = t$. Similarly $J^3 = Kzx + Kzy$, and so $zx, zy$ are not both zero. If $a, b, c \in R$, write $A(abc)$ for the associativity condition $(ab)c = a(bc)$. From $A(yx^2)$ and $A(yxy)$ we derive $\gamma_1 = 0$. In the same way $A(y^2x)$, $A(y^3)$ lead to $\delta_1 = 0$, and $A(xyx), A(xy^2)$ to $\beta_1 = 0$. Then $\alpha_1 \neq 0$, else $J^2 = J^3$. Now $A(x^3), A(x^2y)$ give $zx = t, zy = 0$. Replacing $y$ by $y - \beta_2 z$ and $z$ by $z + \alpha_2 \alpha_1^{-1} t$ allows us to assume that $\beta_2 = \alpha_2 = 0$. If we now replace $z, t$ by $\alpha_1 z, \alpha_1 t$, the multiplication in $J$ is given by the table

| | $x$ | $y$ | $z$ | $t$ |
|---|---|---|---|---|
| $x$ | $z$ | 0 | $t$ | 0 |
| $y$ | $\gamma t$ | $\delta t$ | 0 | 0 |
| $z$ | $t$ | 0 | 0 | 0 |
| $t$ | 0 | 0 | 0 | 0 |

where we have written $\gamma = \gamma_2$, $\delta = \delta_2$. One checks, conversely, that such a table does indeed define a ring $R$ with basis $(1, x, y, z, t)$, and in particular that associativity holds. Moreover the ideal $J$ spanned by $(x, y, z, t)$ is such that $J^4 = 0$, whence $J \subset \operatorname{rad} R$, and it follows that $R$ is a local ring of the type under discussion, with radical $J$. If $\gamma, \delta$ are both non-zero, replace $x, y, z, t$ by $\gamma^2\delta^{-1}x, \gamma^3\delta^{-2}y, \gamma^4\delta^{-2}z, \gamma^6\delta^{-3}t$, respectively, and then $\gamma = \delta = 1$. If $\gamma \neq 0$, $\delta = 0$, replace $y$ by $\gamma^{-1}y$, so that $\gamma = 1$. If $\gamma = 0$, $\delta \neq 0$, replace $x, y, z, t$ by $\delta x, \delta y, \delta^2 z, \delta^3 t$, and then $\delta = 1$. In summary, *there are* 4 *rings in this case, given by the table above with*: (i) $\gamma = \delta = 1$; (ii) $\gamma = 1, \delta = 0$; (iii) $\gamma = 0, \delta = 1$, *and* (iv) $\gamma = \delta = 0$.

These are not isomorphic. The first two are not commutative, whereas the last two are. Indeed, (iii) is $K[X,Y]/(X^4, XY, Y^2 - X^3)$ and (iv) is $K[X,Y]/(X^4, XY, Y^2)$. Moreover from the table one calculates that the right annihilator $\operatorname{Ann}_r(J) = Kt$ $(\delta \neq 0)$, $Ky \oplus Kt$ $(\delta = 0)$. The dimension of this distinguishes the other cases.

**1.2.2.** Choose $x_1, x_2, y_1, y_2 \in J$ such that $J = Kx_1 \oplus Kx_2 \oplus J^2$, $J^2 = Ky_1 \oplus Ky_2$. Then $x_i x_j = \alpha_{ij} y_1 + \beta_{ij} y_2$ ($\alpha_{ij}, \beta_{ij} \in K$) and these four products span $J^2$. The ring structure is determined by the pair of $(2 \times 2)$ matrices $M = (\alpha_{ij})$, $N = (\beta_{ij})$, which are linearly independent over $K$. Conversely, any pair of independent matrices defines such a ring by letting $R$ have basis $(1, x_1, x_2, y_1, y_2)$ and defining $x_i x_j$ as above and all other products of the $x_i$ and $y_j$ to be zero. Then the ideal $J$ spanned by $(x_1, x_2, y_1, y_2)$ is such that $J^3 = 0$, and again it follows that $R$ is local, with radical $J$. The independence of $M, N$ implies that $J^2 = Ky_1 \oplus Ky_2$.

If $(x'_1, x'_2, y'_1, y'_2)$ is a new basis of $J$ with corresponding matrices $M', N'$, then we may write $x'_i = p_{1i} x_1 + p_{2i} x_2 + z_i$ ($z_i \in J^2$), so that $P = (p_{ij})$ is the transition matrix from the basis $(\bar{x}_1, \bar{x}_2)$ of $J/J^2$ to the basis $(\bar{x}'_1, \bar{x}'_2)$. Equally, let $Q = (q_{ij})$ be the transition matrix from the basis $(y_1, y_2)$ of $J^2$ to $(y'_1, y'_2)$. Since $J^3 = 0$, calculating $x'_i x'_j$ and comparing coefficients of $y_i$ leads to equations which, in matrix form, are

$$\begin{cases} P^t M P = q_{11} M' + q_{12} N' \\ P^t N P = q_{21} M' + q_{22} N'. \end{cases}$$

Evidently, the problem of classifying our rings up to isomorphism amounts to that of classifying pairs of linearly independent matrices $(M, N)$ under the above relation of *equivalence*, $P$ and $Q$ being arbitrary invertible matrices. This linear algebra problem has been solved over any field $K$ in [2, 3] and we extract the results, where $K = \mathbf{F}_p$. If $p \neq 2$, let $\varepsilon$ be a fixed non-square of $K$. If $\delta = 1$ (resp. $\varepsilon$), then for each $\xi \in K$ (resp. $K^*$) choose a non-zero solution $(\alpha, \beta)$ of the equation $\alpha^2 - \delta\beta^2 = \xi$, and let $\Pi_\delta$ be the set of these. Then, *the isomorphism classes of rings are given by the pairs of matrices*

(i) $p \neq 2$,

$$\begin{pmatrix} 1 & \\ & \delta \end{pmatrix}, \begin{pmatrix} & 1 \\ \sigma & \end{pmatrix} \ (\delta = 0, 1, \varepsilon;\ \sigma = \pm 1), \qquad \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} & 1+\beta \\ 1-\beta & \end{pmatrix} \ (\beta \in K^*), \qquad \begin{pmatrix} 1 & \alpha \\ -\alpha & \delta \end{pmatrix}, \begin{pmatrix} & 1+\beta \\ 1-\beta & \end{pmatrix}$$

$(\delta = 1, \varepsilon;\ (\alpha, \beta) \in \Pi_\delta)$.

*Hence there are* $3p + 5$ *distinct rings in this case*, *with* 3 *commutative*.

(ii) $p = 2$,

$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \quad \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} & 1 \\ 0 & \end{pmatrix}, \quad \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} & 0 \\ 1 & \end{pmatrix},$$
$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ & \delta \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix},$$
$$\begin{pmatrix} \delta & 1 \\ & 0 \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix} (\delta = 0, 1).$$

*There are* 10 *such rings*, 3 *being commutative*.

**1.3.** Let $J = Kx_1 \oplus Kx_2 \oplus Kx_3 \oplus J^2$, $J^2 = Ky$. Then $x_i x_j = \alpha_{ij} y$ ($\alpha_{ij} \in K$) and these nine products span $J^2$. The ring structure is determined by the $(3 \times 3)$ matrix $M = (\alpha_{ij})$, which is non-zero, and any non-zero matrix defines such a ring. If $(x'_1, x'_2, x'_3, y')$ is a new basis of $J$ with corresponding matrix $M'$, then as above we have $x'_i = \sum_j p_{ji} x_j + r_i y$ and $y' = qy$. Calculating $x'_i x'_j$ and comparing coefficients leads to the matrix condition $P^t M P = qM'$, where $P$ is invertible and $q \neq 0$. If $M, M'$ are so related, we call them *projectively congruent*. This reduces to ordinary congruence when $q = 1$. The rings in the present case are evidently classified by the non-zero matrix $M$ up to projective congruence. This matrix classification problem has been dealt with in [4, 5]. If, as before, $\varepsilon$ denotes a non-square in $K$ ($p$ odd), the results are that *the isomorphism classes of rings are given by the matrices*

(i) $p \neq 2$,

$$\begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & \varepsilon & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} \mu & & \\ & & 1 \\ & -1 & \end{pmatrix},$$
$$\begin{pmatrix} \mu & & \\ & 1 & 1 \\ & & \delta \end{pmatrix}, \begin{pmatrix} \varepsilon & & \\ & 1 & 2 \\ & & 1 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 1 \\ & & 1 \\ & 1 & \end{pmatrix}, \qquad \textit{where } \mu = 0, 1 \textit{ and } \delta \in K.$$

*There are* $2p + 9$ *such rings*, *with* 4 *commutative*.

(ii) $p = 2$,

$$\begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 0 & & \\ & & 1 \\ & 1 & \end{pmatrix}, \begin{pmatrix} \mu & & \\ & 1 & 1 \\ & & \delta \end{pmatrix},$$
$$\begin{pmatrix} \mu & 0 & 1 \\ & & 1 \\ & 1 & \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ & & 1 \\ & 1 & 1 \end{pmatrix}, \qquad \textit{where } \mu = 0, 1 \textit{ and } \delta = 0, 1.$$

*There are* 11 *such rings*, *with* 4 *commutative*.

**1.4.** Choose a basis $(x, y, z, t)$ of $J$. All products of these are zero and we obtain just *one commutative ring*: $R = K[X, Y, Z, T]/(X, Y, Z, T)^2$.

This completes the classification in characteristic $p$.

## 2. CHARACTERISTIC $p^2$

Throughout this section the prime ring $A = \mathbf{Z}_{p^2}$. We go through the cases again:

**2.1.** Choose $x \in J - J^2$, so that $R = A[x]$ and the other conclusions of [1, Lemma 2.2] hold, in particular $p \in J^2$. In fact $p \in J^3$, for otherwise $J^2 = Rp + J^3$ and squaring gives the contradiction $J^4 = 0$. We split into two subcases, according to whether $p$ belongs to $J^4$ or not.

**2.1.a.** $p \in J^4$. Then $px = 0$ and $x^4 = ap$, where $a$ belongs to $A^*$, the group of units of $A$. It follows that $R = A[X]/(pX, X^4 - ap)$. As for existence, one checks easily that the latter ring is indeed local of order $p^5$ and of the type under consideration. To classify these up to isomorphism, suppose also that $R = A[x']$, with $px' = 0$, $x'^4 = a'p$. Then $x' = bx + y$ $(b \in A^*,\ y \in J^2)$, and so $x'^4 = b^4x^4$. Thus $a'p = b^4ap$, whence $a' \equiv b^4a$ (mod $p$). If, conversely, this last condition holds, replace $x$ by $x' = bx$, and then $x'^4 = a'p$. This is similar to Case **2.1.1.a** in order $p^4$ [1], and our rings are classified by $a \in \Sigma_4$, or more precisely by the image of $a$ under the epimorphism $A^* \to K^* \to K^*/K^{*4}$, the first map being reduction mod $p$. To summarize, *the distinct rings are given by* $R = A[X]/(pX, X^4 - ap)$, *with* $a \in \Sigma_4$. *The number of rings is* 4, 2, *or* 1 *according to whether* $p \equiv 1(4)$, $p \equiv 3(4)$, *or* $p = 2$.

**2.1.b.** $p \notin J^4$. Here there is a parallel with Case **2.1.1.b** in order $p^4$. We have $J^3 = Ap \oplus J^4$, $J = Ax + J^2$, and multiplying gives $J^4 = Apx$, so that $J^3 = Ap \oplus Apx$. Let $x^3 = ap + bpx$ $(a, b \in A)$. Then $a \in A^*$, else $x^4 = bpx^2 = 0$. If $p \neq 3$, we may replace $x$ by $x - bx^2/3a$ and so assume that $b = 0$. Hence $R = A[X]/(pX^2, X^3 - ap)$, where once again one checks without difficulty that the latter ring really does have the right properties. To classify these, suppose also that $R = A[x']$, with $px'^2 = 0$, $x'^3 = a'p$. Then $x' = cx + y$ $(c \in A^*,\ y \in J^2)$, and so $x'^3 = c^3x^3 + 3c^2x^2y$. But $x'^3 - c^3x^3 \in Ap$, $3c^2x^2y \in J^4$ and the sum in $J^3$ is direct. So in fact $x'^3 = c^3x^3$. As above, our rings are classified by $a \in \Sigma_3$. If $p = 3$, then $a \equiv \pm 1(3)$, and replacing $x$ by $ax$ allows us to assume that $a = 1$, so that $x^3 = 3 + 3bx$. If, as before, $x' = cx + y$ is a new generator, with $x'^3 = 3 + 3b'x'$, then $x'^3 = c^3x^3 = cx^3$. But $3 \in J^3$, so that $3y = 0$ and $3 + 3b'cx = 3c + 3bcx$. Since the sum in $J^3$ is direct, it follows that $b' \equiv b(3)$. We have proved that *for* $p \neq 3$ *the rings are given by* $R = A[X]/(pX^2, X^3 - ap)$, $a \in \Sigma_3$. *The number of rings is* 3 *or* 1 *according to whether* $p \equiv 1(3)$ *or not.*

*For* $p = 3$ *there are* 3 *rings*: $R = A[X]/(3X^2, X^3 - 3 - 3bX)$ *with* $b = 0, \pm 1$.

**2.2.** We observe first that $pJ^2 = 0$. If not, then $pxy \neq 0$ for some $x, y \in J$, and so $J^2 = Axy$. Then $px$ has order $p$ in $J^2$, so that $px = apxy$. This gives the contradiction $pxy = apxy^2 = 0$, since $J^4 = 0$. We now split into five subcases, in the first three of which $p \in J^2$ and we consider the possibilities for the chain $J^2 \supset J^3 \supset pJ \supset 0$.

**2.2.a.** $p \in J^2$, $J^3 = 0$. Since $pJ = 0$ we may regard $J$ as a $K$-algebra (without identity) and choose $x_1, x_2, y \in J$ such that $J = Kx_1 \oplus Kx_2 \oplus J^2$, $J^2 = Ky \oplus Kp$. For $\lambda \in K$, one must be careful not to confuse $\lambda p$ in $A$ with $p\lambda = 0$ in $K$. As in Case **1.2.2** we have $x_i x_j = \alpha_{ij} y + \beta_{ij} p$ $(\alpha_{ij}, \beta_{ij} \in K)$ and these products span $J^2$. Note also a parallel with Case **2.2.a** in order $p^4$. The matrices $M = (\alpha_{ij})$, $N = (\beta_{ij})$ are linearly independent, and one verifies as before that any such pair of matrices gives rise to a ring of the present type. If we change to new generators $x'_1, x'_2, y'$ with corresponding matrices $M', N'$, then $x'_i = p_{1i} x_1 + p_{2i} x_2 + z_i$ $(z_i \in J^2)$ and we put $P = (p_{ij})$. If $Q = (q_{ij})$ is the transition matrix from the basis $(y, p)$ of $J^2$ to $(y', p)$, we obtain as before the conditions

$$\begin{cases} P^t M P = q_{11} M' + q_{12} N' \\ P^t N P = q_{21} M' + q_{22} N'. \end{cases}$$

Our problem now boils down to that of classifying pairs of matrices over $K$ under an equivalence relation similar to that of Case **1.2.2**, but with the crucial difference that $Q$ is restricted to be of the form $\begin{pmatrix} * & \\ * & 1 \end{pmatrix}$, since here $q_{12} = 0$, $q_{22} = 1$. This linear algebra problem has a quite different solution. The list of normal forms for the pairs $(M, N)$ turns out to be rather extensive and is given in full in [6]. For brevity we do not repeat it here, but confine ourselves to stating the number of isomorphism classes. *The numbers of distinct rings of this type are given as follows*:

(i) $p \neq 2$. *There are* $2p^2 + 10p + 15$ *rings*, *of which* 10 *are commutative*.

(ii) $p = 2$. *There are* 23 *rings*, *of which* 6 *are commutative*.

**2.2.b.** $p \in J^2$, $J^3 \neq 0$, $pJ = 0$. Note first that $p \in J^3$, for otherwise $J^2 = Ap + J^3$ and then $J^3 = pJ = 0$. Once again we regard $J$ as a $K$-algebra and write $J = Kx \oplus Ky \oplus J^2$, $J^2 = Kz \oplus J^3$ and $J^3 = Kp$. This is similar to Case **1.2.1**. The argument of the first paragraph there applies, and we may take the multiplication to be given by

| | $x$ | $y$ | $z$ | $p$ |
|---|---|---|---|---|
| $x$ | $\alpha z$ | $0$ | $p$ | $0$ |
| $y$ | $\gamma p$ | $\delta p$ | $0$ | $0$ |
| $z$ | $p$ | $0$ | $0$ | $0$ |
| $p$ | $0$ | $0$ | $0$ | $0$ |

where $\alpha \neq 0$. We may not, of course, renormalize $p$ this time to take $\alpha = 1$. Conversely, any such table gives rise to a ring of the present class. Note that $R$ is commutative if and only if $\gamma = 0$, and that if $R$ is not commutative we may scale $y$ and take $\gamma = 1$. If $x', y', z'$ are new generators with structure constants $\alpha', \gamma', \delta'$, we have $x' = ax + cy + ez + u$, $y' = bx + dy + fz + v$, $z' = gz + w$ with $a, \dots, g \in K$ and $u, v, w \in J^3$. Then $x'z' = agxz$ and $y'z' = bgxz$, giving $a \neq 0$, $b = 0$ and hence $d \neq 0$, else $y' \in J^2$. Computing $x'^2, x'y', y'x'$ and $y'^2$ and comparing coefficients leads to the equations

$$\alpha' = a^3\alpha, \qquad \gamma' = ad\gamma, \qquad \delta' = d^2\delta \text{ (some } a, d \neq 0). \tag{1}$$

These conditions are also sufficient for the rings with structure constants $(\alpha, \gamma, \delta)$ and $(\alpha', \gamma', \delta')$ to be isomorphic, as follows by setting $x' = ax$, $y' = dy$, $z' = a^{-1}z$. We now analyze the conditions (1). If $R$ is commutative, so that $\gamma = \gamma' = 0$, then $R$ is classified by the cube-class of $\alpha$ and the square-class of $\delta$. But if $R$ is noncommutative ($\gamma = \gamma' = 1$), then $ad = 1$ and (1) becomes $\alpha' = a^3\alpha$, $\delta' = a^{-2}\delta$ ($a \neq 0$). In particular, if we fix $\delta = \delta' \neq 0$, then $a = \pm 1$, and $\alpha' = \pm\alpha$. We have proved that *the distinct rings of this type are determined by the table above*.

*For $R$* commutative, *we take $\gamma = 0$, $\alpha \in \Sigma_3$, and $\delta \in \Sigma_2^0$.*

*For $R$* noncommutative, *we take $\gamma = 1$ and*

$$\begin{cases} \textit{either} & \alpha \in \Sigma_3, \delta = 0 \\ \textit{or} & \alpha \in K^*/\{\pm 1\}, \delta \in \Sigma_2. \end{cases}$$

*The numbers of rings are*

| | $p \equiv 1(3)$ | $p \not\equiv 1(3)$, *p odd* | $p = 2$ |
|---|---|---|---|
| *Commutative* | 9 | 3 | 2 |
| *Noncommutative* | $p + 2$ | $p$ | 2 |

**2.2.c.** $p \in J^2$, $J^3 = pJ \neq 0$. Here $p \notin J^3$, else $pJ = 0$. Thus $J^2 = Ap \oplus J^3$. By [1, Lemma 2.1] we have $J = Ax + Ay + J^2$, and we may assume that $px \neq 0$. Then $J^3 = Apx$ and $py = rpx$ ($r \in A$). Replacing $y$ by $y - rx$ allows us to take $py = 0$. Hence $R = A \oplus Ax \oplus Ay$, $J = Ap \oplus Ax$

$\oplus Ay$, and $J^2 = Ap \oplus Apx$. The argument is now rather similar to the previous case. Let $x^2 = \alpha_1 p + \alpha_2 px$, $xy = \beta_1 p + \beta_2 px$, $yx = \gamma_1 p + \gamma_2 px$, $y^2 = \delta_1 p + \delta_2 px$, where the coefficients may be taken in $K$. The associativity conditions $A(x^2 y)$, $A(yx^2)$, $A(xy^2)$ give $\beta_1 = \gamma_1 = \delta_1 = 0$ and replacing $y$ by $y - \beta_2 p$ allows us to assume that $\beta_2 = 0$. We now consider the characteristic.

Suppose that $p \neq 2$. Replace $x$ by $x - \frac{1}{2}\alpha_2 p$, and then $\alpha_2 = 0$. The multiplication in $R$ is now determined by the table

| | $x$ | $y$ | $p$ |
|---|---|---|---|
| $x$ | $\alpha p$ | 0 | $px$ |
| $y$ | $\gamma px$ | $\delta px$ | 0 |
| $p$ | $px$ | 0 | 0 |

where we have dropped the remaining subscripts and $\alpha \neq 0$. As usual, one checks that any such table defines a ring of the present type. If $x', y'$ are new generators with structure constants $\alpha', \gamma', \delta'$, write $x' = ax + cy + ep$, $y' = bx + dy + fp$. Although this time $px \neq 0$, there is no harm in regarding $a, \dots, f$ as being in $K$, since the new multiplication table depends only on their images mod $p$. From $px' = apx$, $py' = bpx$ we deduce $a \neq 0$, $b = 0$ and then $d \neq 0$, else $y' \in J^2$. Computing $x'^2, x'y', y'x', y'^2$ and comparing coefficients leads to the equations

$$\alpha' = a^2\alpha, \qquad \gamma' = d\gamma, \qquad \delta' = a^{-1} d^2\delta \ (\text{some } a, d \neq 0). \tag{2}$$

Again these conditions are also sufficient for the rings with structure constants $(\alpha, \gamma, \delta)$ and $(\alpha', \gamma', \delta')$ to be isomorphic: set $x' = ax$, $y' = dy$. By choice of $a, d$ we may take $\gamma, \delta$ to be 0 or 1 and it follows from (2) that *for $p \neq 2$ the distinct rings are given by the table above.*

*For $R$* commutative, *we take $\gamma = 0$ and*

$$\begin{cases} \textit{either} & \alpha \in \Sigma_2,\ \delta = 0 \\ \textit{or} & \alpha \in \Sigma_4,\ \delta = 1. \end{cases}$$

*For $R$* noncommutative, *we take $\gamma = 1$ and*

$$\begin{cases} \textit{either} & \alpha \in \Sigma_2,\ \delta = 0 \\ \textit{or} & \alpha \in K^*,\ \delta = 1. \end{cases}$$

*The numbers of rings are*

| | $p \equiv 1(4)$ | $p \equiv 3(4)$ |
|---|---|---|
| *Commutative* | 6 | 4 |
| *Noncommutative* | $p + 1$ | $p + 1$ |

Now consider $p = 2$. Then $\alpha_1 = 1$ and the multiplication table has the form

| | $x$ | $y$ | $2$ |
|---|---|---|---|
| $x$ | $2 + \alpha 2x$ | $0$ | $2x$ |
| $y$ | $\gamma 2x$ | $\delta 2x$ | $0$ |
| $2$ | $2x$ | $0$ | $0$ |

Changing to $x', y'$ as before, we have here $b = 0$, $a = d = 1$ and we obtain the equations

$$\alpha' = \alpha + c(\gamma + \delta), \qquad \gamma' = \gamma, \qquad \delta' = \delta. \tag{3}$$

Once more, setting $x' = x + cy$, $y' = y + c\delta 2$ shows (3) also to be sufficient for isomorphism. If $\gamma = \delta$, then $\alpha' = \alpha$. But if $\gamma \neq \delta$, we may then take $\alpha = 0$. Thus *for $p = 2$ the rings are given by the previous table, where $(\alpha, \gamma, \delta)$ is any triple of elements of K except for* $(1, 0, 1)$ *and* $(1, 1, 0)$. *There are* 3 *commutative rings and* 3 *noncommutative*.

In the remaining cases we have $p \notin J^2$. As in [1, Lemma 2.1] we may write $J = Ap + Ax + J^2$. Hence $pJ = Apx$, $J^2 = Apx + Ax^2 + J^3$, and $J^3 = Ax^3$. Thus $J = Ap + Ax + Ax^2 + Ax^3$, $R = A + Ax + Ax^2 + Ax^3 = A[x]$, and $R$ is commutative.

**2.2.d.** $p \notin J^2$, $pJ = 0$. There is clearly *one such ring*: $R = A[X]/(pX, X^4)$.

**2.2.e.** $p \notin J^2$, $pJ \neq 0$. The order of $R$ shows that $x^2 \neq 0$, and so both $x^2$ and $px$ have order $p$. Certainly $Ax^2 \neq Apx$, else $J^3 = Ax^3 = Apx^2 = 0$ and then $J^2 = Apx$ would have order $p$. Hence $J^2 = Apx \oplus Ax^2$ and we may write $x^3 = apx + bx^2$ $(a, b \in A)$. So $0 = x^4 = bx^3 = abpx + b^2x^2$, and hence $b^2x^2 = 0$, the sum being direct. Thus $p \mid b$ and $x^3 = apx$, and so $R = A[X]/(pX^2, X^3 - apX)$, where as usual one verifies that this last ring has the right properties. If $x' = cx + dp + y$ $(c \in A^*, d \in A, y \in J^2)$ is a new generator with $x'^3 = a'px'$, one deduces easily that $a' \equiv c^2 a(p)$, and our rings are classified by $a \in \Sigma_2^0$. In summary, *the rings are given by $R = A[X]/(pX^2, X^3 - apX)$ with $a \in \Sigma_2^0$. There are* 3 *rings* $(p \neq 2)$ *and* 2 $(p = 2)$.

We split Case **2.3** into three subcases:

**2.3.a.** $p \in J^2$. Let $J = Kx_1 \oplus Kx_2 \oplus Kx_3 \oplus J^2$, $J^2 = Kp$, and put $x_i x_j = \alpha_{ij} p$ $(\alpha_{ij} \in K)$. Just as in Case **1.3** the ring structure is given by the non-zero matrix $M = (\alpha_{ij})$, but this time up to *congruence*, since no change of basis in $J^2$ is involved. From [4, 5] we thus have that *the* *isomorphism classes of rings are given by the matrices*

(i) $p \neq 2$,

$$\begin{pmatrix} \nu & & \\ & 0 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & \nu & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & \nu \end{pmatrix}, \begin{pmatrix} \mu & & \\ & & 1 \\ & -1 & \end{pmatrix}, \begin{pmatrix} \mu & & \\ & 1 & 1 \\ & & \delta \end{pmatrix},$$
$$\begin{pmatrix} \mu & & \\ & \varepsilon & 2\varepsilon \\ & & \varepsilon \end{pmatrix}, \begin{pmatrix} \mu & 0 & 1 \\ & & 1 \\ & 1 & \end{pmatrix}, \qquad \textit{where } \mu = 0, 1, \varepsilon;\ \nu = 1, \varepsilon \textit{ and } \delta \in K.$$

*There are* $3p + 15$ *such rings, with* 6 *commutative.*

(ii) $p = 2$,

$$\begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 0 & & \\ & & 1 \\ & 1 & \end{pmatrix}, \begin{pmatrix} \mu & & \\ & 1 & 1 \\ & & \delta \end{pmatrix},$$
$$\begin{pmatrix} \mu & 0 & 1 \\ & & 1 \\ & 1 & \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ & & 1 \\ & 1 & 1 \end{pmatrix}, \qquad \textit{where } \mu = 0, 1 \textit{ and } \delta = 0, 1.$$

*There are* 11 *such rings, with* 4 *commutative.*

**2.3.b.** $p \notin J^2$, $pJ = 0$. Write $J = Kp \oplus Kx_1 \oplus Kx_2 \oplus J^2$, $J^2 = Ky$, and let $x_i x_j = \alpha_{ij} y$ ($\alpha_{ij} \in K$). There is some similarity this time with both Cases **2.2.a** and **1.3**. The ring structure is determined by the non-zero matrix $M = (\alpha_{ij})$, and any such matrix gives a ring of this type. As before, the rings are classified by the projective congruence class of $M$, and we use the representatives for these classes given in [7]. Thus, *the distinct rings of this type are given by the matrices*

$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & \\ & \xi \end{pmatrix} (\xi \in \Sigma_2), \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & \delta \end{pmatrix} (\delta \in K).$$

*The number of rings is* $p + 4$ $(p \neq 2)$, 5 $(p = 2)$. *In either case* 3 *are commutative.*

**2.3.c.** $p \notin J^2$, $pJ \neq 0$. This is very like Case **2.2.c** and we have $R = A \oplus Ax \oplus Ay$, $J = Ap \oplus Ax \oplus Ay$, $J^2 = Apx$, with $py = 0$. Write $x^2 = \alpha px$, $xy = \beta px$, $yx = \gamma px$, $y^2 = \delta px$, with coefficients in $K$. As before, we may take $\beta = 0$, and we now consider the characteristic.

Let $p \neq 2$. Replace $x$ by $x - \frac{1}{2}\alpha p$, and then $\alpha = 0$. The multiplication table is

| | $x$ | $y$ | $p$ |
|---|---|---|---|
| $x$ | 0 | 0 | $px$ |
| $y$ | $\gamma px$ | $\delta px$ | 0 |
| $p$ | $px$ | 0 | 0 |

The same discussion as before shows that the rings with structure constants $(\gamma, \delta)$ and $(\gamma', \delta')$ are isomorphic if and only if

$$\gamma' = d\gamma, \qquad \delta' = a^{-1} d^2\delta \text{ (some } a, d \neq 0). \tag{4}$$

We may thus take $\gamma, \delta$ to be 0 or 1, and hence, *for $p \neq 2$ the distinct rings are given by the table above, with $\gamma, \delta \in \{0, 1\}$. Two are commutative, two not.*

For $p = 2$ the table is

| | $x$ | $y$ | 2 |
|---|---|---|---|
| $x$ | $\alpha 2x$ | 0 | $2x$ |
| $y$ | $\gamma 2x$ | $\delta 2x$ | 0 |
| 2 | $2x$ | 0 | 0 |

The conditions for isomorphism of two such rings are again given by (3) and thus, *for $p = 2$ the rings are given by the previous table, where $(\alpha, \gamma, \delta)$ is any triple of elements of $K$ except for $(1,0,1)$ and $(1,1,0)$. There are 3 commutative rings and 3 noncommutative.*

**2.4.** Choose a basis $(p, x, y, z)$ of $J$. All products of these are zero and we obtain just *one commutative ring*: $R = A[X,Y,Z]/(p,X,Y,Z)^2$.

We have now dealt with characteristic $p^2$.

## 3. CHARACTERISTIC $p^3$

This time the prime ring $A = \mathbf{Z}_{p^3}$, and once more we consider the cases. Note that here we cannot have $d_1 = 4$, else $J^2 = 0$ and then $p^2 = 0$.

**3.1.** Choose $x \in J - J^2$, so that $R = A[x]$ and the other conclusions of [1, Lemma 2.2] hold. Thus $J = Ax + J^2$ and $J^2 = Ap + J^3$, since $p^2 \neq 0$ and hence $p \notin J^3$. Multiplying gives $J^3 = Apx + J^4$, $J^4 = Ap^2$ and so $J = Ap + Ax$. But $p^2 x \in J^5 = 0$, so $x$ has order $p^2$, and it follows that $R = A \oplus Ax$, $J = Ap \oplus Ax$, $J^2 = Ap \oplus Apx$. Let $x^2 = ap + bpx$ $(a, b \in A)$. Then $a \in A^*$, else $x^2 \in J^3$. If $p \neq 2$, we may complete the square and take $b = 0$. Hence $R = A[X]/(p^2X, X^2 - ap)$, where one checks as usual that the quotient is indeed a ring of the right type. If also $R = A[x']$, with $p^2x' = 0$, $x'^2 = a'p$, then putting $x' = cx + dp$ $(c \in A^*)$ leads to the condition $a' \equiv c^2 a(p^2)$. Conversely, if this holds for some $c$, then putting $x' = cx$ gives $x'^2 = a'p$. Thus our rings are classified by the image of $a$ under reduction in $\mathbf{Z}_{p^2}^*/\mathbf{Z}_{p^2}^{*2}$, itself isomorphic to $K^*/K^{*2}$ via reduction mod $p$. Put another way, the congruence condition above may be replaced by congruence mod $p$. As usual, we say that the rings are classified by $a \in \Sigma_2$.

Now let $p = 2$, so that $x^2 = 2a + 2bx$ with $4x = 0$, and we may take $a = \pm 1$, $b = 0, 1$. Changing to a new generator $x' = cx + 2d$ as above leads to the conditions

$$b' = b, \qquad a' \equiv a + 2bd + 2d^2(4) \text{ (some } d). \tag{5}$$

The cases $(a, b) = (1, 0)$ and $(-1, 0)$ are equivalent, as follows by putting $x' = x + 2$. But if $b = 1$, then (5) gives $a' \equiv a(4)$ and the other cases are inequivalent. In all, *for* $p \neq 2$ *there are* 2 *rings*: $R = A[X]/(p^2X, X^2 - ap)$, $a \in \Sigma_2$.

*For* $p = 2$ *there are* 3 *rings*: $R = A[X]/(4X, X^2 - 2a - 2bX)$ *with* $(a, b) = (1, 0), (1, 1),$ *or* $(-1, 1)$.

We divide Case **3.2** into two, noting first that $p \notin J^2$, else $p^2 = 0$.

**3.2.1.** $J^3 \neq 0$. We show first that $p^2J = pJ^2 = 0$. Suppose that $p^2J \neq 0$. Then $p^2z \neq 0$ for some $z \in J$, and so $J^2 = Apz$. But $p^2$ has order $p$ in $J^2$, so that $p^2 = ap^2z$, leading to the contradiction $p^2z = ap^2z^2 = 0$. Hence $p^2J = 0$ and the argument at start of Case **2.2** now applies to show that $pJ^2 = 0$.

Let $J = Ap + Ax + J^2$, so that $J^2 = Ap^2 + Apx + Ax^2 + J^3$ and $J^3 = Ax^3$ from above. Suppose $px \notin A$. Then $J^2 = Ap^2 \oplus Apx$, giving the contradiction $J^3 = JJ^2 = 0$. So $px \in A$ and we have $px = bp^2$ $(b \in A)$. Replacing $x$ by $x - bp$ allows us to take $px = 0$. Equally $x^3 \in A$, else $J^2 = Ap^2 \oplus Ax^3$ and again $J^3 = 0$. Thus $x^3 = ap^2$ $(a \in A^*)$. We now have $R = A \oplus Ax \oplus Ax^2 = A[X]/(pX, X^3 - ap^2)$. One classifies these rings as usual and finds that *the rings are given by* $R = A[X]/(pX, X^3 - ap^2)$, *with* $a \in \Sigma_3$. *The number of rings is* 3 *or* 1 *according to whether* $p \equiv 1(3)$ *or not*.

**3.2.2.** $J^3 = 0$. Let $J = Ap + Ax + J^2$, so that $J^2 = Ap^2 + Apx + Ax^2$ and $pJ = Ap^2 + Apx$. Now $Ap^2 \subset pJ \subset J^2$ and we split into two cases.

**3.2.2.a.** $pJ \neq J^2$. Here $pJ = Ap^2$ and we put $px = ap^2$. Replacing $x$ by $x - ap$ allows us to assume that $px = 0$. Then $J = Ap \oplus Ax \oplus Ax^2$, $R = A \oplus Ax \oplus Ax^2$, and there is thus *one ring*: $R = A[X]/(pX, X^3)$.

**3.2.2.b.** $pJ = J^2$. This time $J^2 = pJ = Ap^2 \oplus Apx$ and hence $J = Ap \oplus Ax$, $R = A \oplus Ax$. Let $x^2 = ap^2 + bpx$ $(a, b \in A)$. If $p \neq 2$, we may complete the square and take $b = 0$. Thus $R = A[X]/(p^2X, X^2 - ap^2)$ and the usual checks show that $R$ is classified by the square-class of $a$

(mod $p$). If $p = 2$, then $x^2 = 4a + 2bx$, $4x = 0$, and we may take $a, b = 0$ or 1. Changing to $x' = cx + 2d$ this time leads to the conditions

$$b' = b, \qquad a' \equiv a + bd + d\ (2)\ (\text{some } d), \tag{6}$$

and it follows that there are three distinct rings. In summary, *for $p \neq 2$ there are 3 rings*: $R = A[X]/(p^2X, X^2 - ap^2)$, $a \in \Sigma_2^0$.

*For $p = 2$ there are 3 rings*: $R = A[X]/(4X, X^2 - 4a - 2bX)$ *with* $(a, b) = (0,0), (0,1),$ *or* $(1,1)$.

**3.3.** Again $p \notin J^2$ and we write $J = Ap + Ax_1 + Ax_2 + J^2$, where $J^2 = Kp^2$. We may as usual modify the $x_i$ so that $px_i = 0$. Then $R = A \oplus Kx_1 \oplus Kx_2$, $J = Ap \oplus Kx_1 \oplus Kx_2$. The situation is now similar to several previous cases, such as Cases **2.3.a** and **2.3.b**. If $x_i x_j = \alpha_{ij} p^2$ $(\alpha_{ij} \in K)$, then the ring structure is determined by $M = (\alpha_{ij})$, which may here be any matrix, including zero, and the rings are classified by $M$ up to *congruence*. From [7] we therefore have that *the distinct rings of this type are given by the matrices*

(i) $p \neq 2$,

$$\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} \varepsilon & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & \varepsilon \end{pmatrix}, \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \begin{pmatrix} \varepsilon & 2\varepsilon \\ & \varepsilon \end{pmatrix}, \textit{and}$$
$$\begin{pmatrix} 1 & 1 \\ & \delta \end{pmatrix} \qquad (\delta \in K).$$

*There are $p + 7$ rings, with 5 commutative.*

(ii) $p = 2$, *the same but omitting the representatives involving $\varepsilon$. There are 6 rings, with 4 commutative.*

## 4. CHARACTERISTICS $p^4, p^5$, AND CONCLUSION

In characteristic $p^4$, [1, Proposition 2.3] applies and the rings are as follows:

**4.** $A[X]/(pX, X^2 - ap^3)$ *with* $a \in \Sigma_2^0$. *There are 3 rings* $(p \neq 2)$ *and* 2 $(p = 2)$.

In characteristic $p^5$ there is, of course, just one ring:

**5.** $\mathbf{Z}_{p^5}$.

This completes the classification of all local rings of order $p^5$, and hence of all rings of order $p^n$ $(n \leq 5)$, when taken in conjunction with Part I.

TABLE I
The Numbers of Indecomposable Rings of Order $p^n$ ($n \le 5$)

| Order | Char $p$ | | Char $p^2$ | | Char $p^3$ | | Char $p^4$ | Char $p^5$ |
|---|---|---|---|---|---|---|---|---|
| $p$ | 1 | | | | | | | |
| $p^2$ | 2 | | 1 | | | | | |
| $p^3$ | 3 | 1 | $\begin{cases} 3 \\ 2 \end{cases}$ | | 1 | | | |
| $p^4$ | 7 | $\begin{cases} p+7 \\ 8 \end{cases}$ | $\left[\begin{matrix} 13 \\ 11 \end{matrix}\right.$ | $\begin{cases} p+4 \\ 4 \end{cases}$ | $\begin{cases} 3 \\ 2 \end{cases}$ | | 1 | |
| $p^5$ | 12 | $\begin{cases} 5p+27 \\ 34 \end{cases}$ | $\left(\begin{matrix} 48 \\ 40 \\ 44 \\ 36 \\ 27 \\ 38 \end{matrix}\right.$ | $2p^2+16p+\left(\begin{matrix} 33 \\ 31 \\ 33 \\ 31 \\ 5 \\ 31 \end{matrix}\right.$ | $\left[\begin{matrix} 14 \\ 12 \end{matrix}\right.$ | $\begin{cases} p+4 \\ 4 \end{cases}$ | $\begin{cases} 3 \\ 2 \end{cases}$ | 1 |

For reference, we conclude with Table I giving the total number of indecomposable rings in each of the orders $p, \dots, p^5$. Table I is divided into columns according to the characteristic. The columns for characteristics $p, p^2, p^3$ are further divided into two, the left giving commutative rings and the right noncommutative. In characteristics $p^4$ and $p^5$ the rings are all commutative. To save space, we use the notation $\{^a_b$ to represent the value $a$ ($p \neq 2$), $b$ ($p = 2$). Similarly $[^a_b$ represents $a$ ($p \equiv 1(3)$), $b$ ($p \not\equiv 1(3)$) and a vertical sextuplet preceded by a parenthesis distinguishes, respectively, the cases $p \equiv 1, 5, 7, 11(12)$, $p = 2$, and $p = 3$.

## REFERENCES

1. B. Corbas and G. D. Williams, Rings of order $p^5$. Part I. Nonlocal rings, *J. Algebra*
2. B. Corbas and G. D. Williams, Congruence of two-dimensional subspaces in $M_2(K)$ (characteristic $\neq 2$), *Pacific J. Math.* **188** (1999), 225–235.
3. B. Corbas and G. D. Williams, Congruence of two-dimensional subspaces in $M_2(K)$ (characteristic 2), *Pacific J. Math.* **188** (1999), 237–249.
4. B. Corbas and G. D. Williams, Matrix representatives for three-dimensional bilinear forms over finite fields, *Discrete Math.* **185** (1998), 51–61.
5. G. D. Williams, Projective congruence in $M_3(\mathbf{F}_q)$, preprint, University of Reading, 1997.
6. G. D. Williams, On a class of finite rings of characteristic $p^2$, preprint, University of Reading, 1998.
7. G. D. Williams, Congruence of $(2 \times 2)$ matrices, *Discrete Math.* (2000), in press.