Group presentations for a class of radical rings of matrices

Noelle Antony, Clare Coleman and David Easdown

November 16, 2001

Abstract

In this paper we assemble some facts about radical rings which arise by sandwich multiplication using a Jacobson radical element. We find a group presentation for the Munn ring consisting of $n \times n$ matrices over $\mathbb{Z}_{p^k}$, where p is prime, which employs a scalar sandwich matrix where the scalar is from $p\mathbb{Z}_{p^k}$, regarded as a group with respect to the circle operation.

1 Introduction and preliminaries

Groups of units of rings with identity are well studied. However many rings arise naturally without an identity. For example, nontrivial rings which coincide with their Jacobson radical never have an identity, and one does not typically expect a semigroup ring or algebra to have an identity. Nevertheless, all rings possess groups of *quasi-units*, that is, elements which are invertible with respect to the circle operation $\circ$ defined by

$$x \circ y \quad = \quad x + y - xy \; .$$

Consider a ring S, not necessarily with 1, with multiplication denoted by $\cdot$ or juxtaposition. We refer to $(S, \circ)$ as the *circle monoid* of S. Denote by

S^1 the result of adjoining 1 to S, which may be done in such a way that the characteristic n of the ring is preserved, so that the prime subring of S^1 is a copy of $\mathbb{Z}_n$ (where we take $\mathbb{Z}_0$ to be $\mathbb{Z}$) (see, for example, [11, Theorem 2.26] or [1]). Then the mapping

$$\widehat{\ } \ : \ (S, \circ) \ \to \ (S^1, \cdot) \ , \ \ x \ \mapsto \ \widehat{x} \ = \ 1 - x \qquad (x \in S)$$

is a monoid embedding, which is an isomorphism when $S = S^1$. An element $x \in S$ is called *quasi-invertible* if there is an element y such that

$$x \circ y \ = \ y \circ x \ = \ 0 \ ,$$

in which case we call y the *quasi-inverse* of x and write $x' = y$. Put

$$\mathcal{G}(S) \ = \ \{ \, x \in S \mid x \text{ is quasi-invertible} \, \} \ ,$$

called the *group of quasi-units* or the *circle group* of S. When $S = S^1$, denote by $G(S)$ the group of units of $(S, \cdot)$, in which case $\widehat{\ } \ : \ \mathcal{G}(S) \ \to \ G(S)$ is a group isomorphism. It is straightforward to check that if $S \neq S^1$ then $\mathcal{G}(S^1) \cong G(\mathbb{Z}_n) \times \mathcal{G}(S)$, where n is the characteristic of S .

The Jacobson radical of S, denoted by $\mathcal{J}(S)$, may be defined to be the largest ideal of S consisting of quasi-invertible elements. It is easy to see that any ideal of S contained in $\mathcal{J}(S)$ forms a normal subgroup of $(\mathcal{G}(S), \circ)$. The existence of complements of $\mathcal{J}(S)$ and the nilradical in $\mathcal{G}(S)$ appears to be a delicate issue and is discussed in [1]. For example if S is a finite ring with identity of prime characteristic, then the Jacobson radical is always complemented [17]. However finite rings exist in non-prime characteristic where complementation fails [8].

Call S *radical* if $S = \mathcal{J}(S)$. The circle group of a radical ring has also been called the *adjoint group* [23]. Chick [3] [4] investigates, also with Gardner [5], interesting examples of commutative radical rings S in which $(S, \circ)$ and $(S, +)$ are isomorphic. The question of when an abstract group arises as the circle group of a ring, and the interplay between finite generation, nilpotency of the ring and nilpotency of its circle group have been investigated by a number of authors including Ault, Watters, Kruse, Tahara, Hosomi and Sandling [2] [23] [13] [14] [22] [21]. Membership criteria for the circle groups of band graded rings have been investigated by Kelarev [12].

It should be remarked that many authors use as circle operation $\circ^+$ defined by $x \circ^+ y = x + y + xy$. (We prefer our definition because the quasi-inverse of a nilpotent element is then the negative sum of powers of the element, rather than an alternating sum.) This does not matter in our context, however, because negation is an isomorphism between the monoids $(S, \circ)$ and $(S, \circ^+)$, an instance of a phenomenon remarked upon below. Both $\circ = \circ^{(1)}$ and $\circ^+ = \circ^{(-1)}$ are special cases of the associative derived operation $\circ^{(k)}$, where k is an integer, defined by

$$x \circ^{(k)} y \;=\; x + y - kxy \; .$$

Derived operations are binary operations formed by combinations of the ring operations as polynomial expressions in two noncommuting variables with integer coefficients, and, by a theorem of McConnell and Stokes [16], are associative if and only if they have one of the following forms:

$$x * y \quad = \quad \begin{cases} x + y - kxy & (1) \\ x + y - kyx & (2) \\ kxy & (3) \\ kyx & (4) \\ x & (5) \\ y & (6) \\ 0 & (7) \end{cases}$$

where k is an integer. Observe that (5), (6) and (7) do not produce interesting semigroups, being left-zero, right-zero and null respectively, whilst (2) is dual to (1) and (4) dual to (3). If (3) is regarded as defining a new ring multiplication then all instances of (1) arise as circle monoids. We put this in a more general setting as follows:

Let $(S,+)$ be an abelian group, T a set containing S, and $z \in T$. Suppose that T has an associative partial binary operation, denoted by juxtaposition, satisfying the following conditions:

(1) $\quad (\forall x, y \in S) \qquad xzy \in S$;

(2) $\quad (\forall u, v, w \in S) \quad (u+v)zw = uzw+vzw \quad$ and $\quad uz(v+w) = uzv+uzw$.

Then it is routine to verify that $(S, +, *^{(z)})$ is a ring where

$$x *^{(z)} y \;=\; xzy \; .$$

We refer to $*^{(z)}$ as *sandwich* multiplication. This construction includes for example the Munn ring

$$(\mathsf{Mat}_{m,n}(R), +, *^{(z)})$$

formed by taking T to be the set of all matrices over R^1 for a given ring R, under the partial binary operation of matrix multiplication, $S = \mathsf{Mat}_{m,n}(R)$ to be the subset of $m{\times}n$ matrices over R, and z an $n{\times}m$ sandwich matrix. The terminology *Munn ring* is due to McAlister [15], which in turn derives from the notion of *Munn algebra* (see [18], [6, Section 5.2] and [20, Chapter 5]), though in our definition above we allow an unrestricted sandwich matrix P (see also [19]). More generally, one could take T to be the set of all homomorphisms between abelian groups, under the partial binary operation of composition, S to be the set of all homomorphisms from an abelian group A to an abelian group B, regarded itself as an abelian group under pointwise addition, and z some fixed homomorphism from B to A.

A further class of examples is obtained by taking T to be any ring and S an ideal of T. For each $z \in T$ we obtain the ring $(S, +, *^{(z)})$. Denote the circle operation for this ring by $\circ^{(z)}$, so that

$$x \circ^{(z)} y \;=\; x + y - xzy \; .$$

In the special case that $T = S^1$ then, in the McConnell-Stokes classification, each instance of (3) becomes sandwich multiplication $*^{(k)}$ where k may be taken to lie in the prime subring of T, and then each instance of (1) becomes a circle operation.

One may ask what relationship, if any, exists between the monoids $(S, \circ^{(z)})$ and $(S, \circ^{(w)})$ as z and w vary over T. For example, if $S = T = \mathbb{Z}_4$ then one may easily verify that $(S, \circ^{(1)}) \cong (S, \circ^{(3)}) \cong (S, \cdot)$ is not a group (in fact, an ideal extension of a two-element null semigroup by a two element group), $(S, \circ^{(2)})$ is a product of two cyclic groups of order 2, and $(S, \circ^{(0)}) = (S, +)$ is a cyclic group of order 4.

It is easy to check that if S is an ideal of a ring T with identity, $z, w \in T$, and u is a unit of T which commutes with w such that $z = uw$, then

$$x \mapsto u^{-1}x \qquad \text{for} \qquad x \in S$$

yields a ring isomorphism: $(S, +, *^{(z)}) \to (S, +, *^{(w)})$, which in turn induces a monoid isomorphism: $(S, \circ^{(z)}) \to (S, \circ^{(w)})$. In particular, for any ring S, $(S, \circ) \cong (S, \circ^{+}) \cong (S, \circ^{(k)})$ for any integer k which is invertible modulo the characteristic.

We establish here some notational conventions used throughout the paper. The kth power of an element x with respect to a binary operation $\odot$ is denoted by $x^{\odot k}$. The cyclic group of order n is denoted by C_n, written multiplicatively. If G is a group and $x, y \in G$ then we write

$$x^y \;=\; y^{-1}xy \qquad \text{and} \qquad [x, y] \;=\; x^{-1}y^{-1}xy \;.$$

If Σ is an alphabet and $\mathcal{R}$ a collection of relations then $\langle \Sigma \mid \mathcal{R} \rangle$ denotes a group presentation.

Let S be a ring. Abbreviate to

$$\mathsf{Mat}_n(S) = \mathsf{Mat}_{n,n}(S, +, \cdot) \;,$$

the usual ring of $n \times n$ matrices with entries from a ring $(S, +, \cdot)$. Note that $\mathcal{J}(\mathsf{Mat}_n(S)) = \mathsf{Mat}_n(\mathcal{J}(S))$. Thus if S is radical then so also is $\mathsf{Mat}_n(S)$, whence $\mathsf{Mat}_n(S) = \mathcal{G}(\mathsf{Mat}_n(S))$ is a group under $\circ$. Observe further that for $z \in \mathbb{Z}$,

$$\mathsf{Mat}_n(S, +, *^{(z)}) \;=\; (\mathsf{Mat}_n(S), +, *^{(z)}) \;=\; (\mathsf{Mat}_n(S), +, *^{(zI)}) \,,$$

where I denotes the $n \times n$ identity matrix, the latter being a Munn ring with respect to the scalar sandwich matrix zI. Membership of the Jacobson radical of Munn rings in general is characterised by Munn:

Theorem 1.1. *[19] If S is any ring then a matrix α lies in the Jacobson radical of the Munn ring $(\mathsf{Mat}_{m,n}(S), +, *^{(P)})$ where P is a sandwich matrix over S^1 if and only if all entries of $P\alpha P$ lie in $\mathcal{J}(S)$.*

Using $n = m = 1$ and noting that $\mathcal{J}(S) = S \cap \mathcal{J}(S^1)$, we immediately deduce the following:

Corollary 1.2. *If S is any ring and $z \in \mathcal{J}(S^1)$ then $(S, +, *^{(z)})$ is radical, so that $(S, \circ^{(z)})$ is a group. In particular, $\mathsf{Mat}_n(\mathbb{Z}_{p^n}, \circ^{(q)})$ is a group for any prime p and $q = p^\ell$ for $\ell \geq 1$.*

The remainder of this paper is devoted to finding a group presentation for $\mathsf{Mat}_n(\mathbb{Z}_{p^n}, \circ^{(q)})$.

2 Circle monoids of integers modulo a power of a prime

This section provides detailed analysis of circle monoids of $\mathbb{Z}_{p^n}$ with respect to sandwich multiplication by powers of a prime p, which is interesting in its own right, but aspects of which are needed later in developing certain group presentations. We begin by noting the following, the proof of which is routine:

Lemma 2.1. *If m, n are positive integers such that m divides n, then the mapping $z \mapsto mz$, for $z \in \mathbb{Z}$, induces a ring isomorphism: $(\mathbb{Z}_{n/m}, +, *^{(m)}) \to (m\mathbb{Z}_n, +, \cdot)$.*

Corollary 2.2. *If m, n are positive integers such that m divides n, then the monoids $(\mathbb{Z}_{n/m}, \circ^{(m)})$ and $(m\mathbb{Z}_n, \circ)$ are isomorphic.*

The following is well-known (see, for example [17, Theorem XVI.9]):

Lemma 2.3. *If p is prime and $n \geq 1$ then*

$$G(\mathbb{Z}_{p^n}) \;\cong\; \mathcal{G}(\mathbb{Z}_{p^n}) \;\cong\; \begin{cases} C_{p-1} \times C_{p^{n-1}} & \text{if } p \text{ is odd or } p = 2 \text{ and } n \leq 2\,; \\ \\ C_2 \times C_{2^{n-2}} & \text{if } p = 2 \text{ and } n > 2\,. \end{cases}$$

Observe that $\mathcal{J}(\mathbb{Z}_{p^n}) = p\mathbb{Z}_{p^n}$ is the Sylow p-subgroup of $\mathcal{G}(\mathbb{Z}_{p^n})$, yielding the following:

Corollary 2.4. *If p is prime and $n \geq 1$ then*

$$(p\mathbb{Z}_{p^n}, \circ) \;\cong\; \begin{cases} C_{p^{n-1}} & \text{if } p \text{ is odd or } p = 2 \text{ and } n \leq 2\,; \\ \\ C_2 \times C_{2^{n-2}} & \text{if } p = 2 \text{ and } n > 2\,. \end{cases}$$

Note that 2 has order 2 in the group $(\mathbb{Z}_{2^n}, \circ)$, yet 2 is not a multiple of 2^ℓ if $\ell > 1$. From this, and the fact that subgroups of cyclic groups are cyclic, Corollaries 2.2 and 2.4 yield the following:

Corollary 2.5. *If p is prime, $1 \leq \ell \leq n$, and $\ell > 1$ if $p = 2$, then*

$$(\mathbb{Z}_{p^n}, \circ^{(p^\ell)}) \;\cong\; (p^\ell\mathbb{Z}_{p^{n+\ell}}, \circ) \;\cong\; (1 + p^\ell\mathbb{Z}_{p^{n+\ell}}, \cdot) \;\cong\; C_{p^n}\,.$$

To get more detailed information concerning generators and orders of elements, we first note the following facts about binomial coefficients (proofs of which the reader can supply, or can be found in [8]):

Lemma 2.6. *If p is prime, $t \geq 1$ and $0 \leq i \leq p^{t-1}$ then*

$$\binom{p^t}{pi} \;\equiv\; \binom{p^{t-1}}{i} \quad \bmod p^t\,.$$

Lemma 2.7. *If p is prime, $t \geq 1$, $0 \leq i < p^{t-1}$ and $1 \leq k \leq p-1$ then*

$$\binom{p^t}{pi+k} \equiv 0 \mod p^t .$$

Some aspects of the following theorem are remarked upon, without proof, in [10].

Theorem 2.8. *Let p be prime and k, ℓ be positive integers such that $\ell \leq k$. Suppose that $\ell > 1$ if $p = 2$. Put $q = p^\ell$. Then $(\mathbb{Z}_{p^k}, \circ^{(q)})$ is a cyclic group and, for each integer x and $n \geq 0$,*

$$x^{\circ^{(q)} n} \equiv \frac{1-(1-xq)^n}{q} \mod p^k .$$

If $0 < x < p^k$, then, regarded as an element of the group $(\mathbb{Z}_{p^k}, \circ^{(q)})$, the order of x is p^{k-j} where p^j is the highest power of p dividing x. In particular $(\mathbb{Z}_{p^k}, \circ^{(q)})$ is generated by 1, and for all $n \geq 0$,

$$q 1^{\circ^{(q)} n} \equiv 1-(1-q)^n \mod p^{k+\ell}$$

and

$$q(1^{\circ^{(q)} n})^\dagger \equiv 1-(1-q')^n \mod p^{k+\ell} ,$$

where $\dagger$ denotes quasi-inversion in $(\mathbb{Z}_{p^k}, \circ^{(q)})$ and $'$ denotes usual quasi-inversion in $\mathbb{Z}_{p^k}$.

Proof. By Corollary 2.5, $(\mathbb{Z}_{p^k}, \circ^{(q)})$ is a cyclic group. If x is any integer and $n \geq 0$ then, by Lemma 2.1,

$$q x^{\circ^{(q)} n} \equiv (qx)^{\circ n} \mod p^k q = p^{k+\ell} ,$$

so that

$$1 - q x^{\circ^{(q)} n} \equiv 1-(qx)^{\circ n} = (1-qx)^n \mod p^{k+\ell} ,$$

yielding

$$x^{\circ^{(q)} n} \equiv \frac{1-(1-qx)^n}{q} \mod p^k .$$

Now suppose $0 < x < p^k$ and write $x = p^j y$ where y is not divisible by p. Note that $0 \leq j \leq k-1$.

Consider s such that $1 \leq s \leq p^{k-j}$. Suppose first that s is not divisible by p. By Lemma 2.7,

$$\binom{p^{k-j}}{s} \quad \equiv \quad 0 \qquad \bmod \ p^{k-j} \ ,$$

so that

$$\binom{p^{k-j}}{s} x^s q^{s-1} \quad = \quad \binom{p^{k-j}}{s} y^s p^{js+\ell(s-1)} \quad \equiv \quad 0 \qquad \bmod \ p^k$$

since $js + \ell(s-1) \geq j$. If, further, $1 < s \leq p^{k-j-1}$ then, by Lemma 2.7,

$$\binom{p^{k-j-1}}{s} \quad \equiv \quad 0 \qquad \bmod \ p^{k-j-1} \ ,$$

yielding

$$\binom{p^{k-j-1}}{s} x^s q^{s-1} \quad = \quad \binom{p^{k-j-1}}{s} y^s p^{js+\ell(s-1)} \quad \equiv \quad 0 \qquad \bmod \ p^k$$

since now $js + \ell(s-1) \geq j+1$.

Suppose secondly that s is divisible by p, say $s = p^m t$ where t is not divisible by p and $m \geq 1$. Note that

$$js + \ell(s-1) \ \geq \ j + \ell(p^m - 1) \ \geq \ j + m + 1 \ .$$

By Lemmas 2.7 and 2.6,

$$\binom{p^{k-j}}{s} \quad \equiv \quad \binom{p^{k-j-m}}{t} \quad \equiv \quad 0 \qquad \bmod \ p^{k-j-m} \ ,$$

so that

$$\binom{p^{k-j}}{s} x^s q^{s-1} \quad \equiv \quad \binom{p^{k-j-m}}{t} y^s p^{js+\ell(s-1)} \quad \equiv \quad 0 \qquad \bmod \ p^k \ ,$$

since $js + \ell(s-1) \geq j + m$. In the case that $s \leq p^{k-j-1}$ then, again by Lemmas 2.7 and 2.6,

$$\binom{p^{k-j-1}}{s} \quad \equiv \quad \binom{p^{k-j-m-1}}{t} \quad \equiv \quad 0 \qquad \bmod \ p^{k-j-m-1} ,$$

yielding

$$\binom{p^{k-j-1}}{s} x^s q^{s-1} \quad \equiv \quad \binom{p^{k-j-m-1}}{t} y^s p^{js+\ell(s-1)} \quad \equiv \quad 0 \qquad \bmod \ p^k ,$$

now since $js + \ell(s-1) \geq j + m + 1$.

These congruences tell us, firstly, that

$$x^{\circ(q)p^{k-j}} \quad \equiv \quad \frac{1-(1-qx)^{p^{k-j}}}{q} \quad = \quad \sum_{s=1}^{p^{k-j}} (-1)^{s-1} \binom{p^{k-j}}{s} x^s q^{s-1} \ \equiv \ 0 \quad \bmod \ p^k ,$$

so that the order of x divides p^{k-j}, and, secondly, that

$$\begin{aligned} x^{\circ(q)p^{k-j-1}} \quad &\equiv \quad \frac{1-(1-qx)^{p^{k-j-1}}}{q} \quad = \quad \sum_{s=1}^{p^{k-j-1}} (-1)^{s-1} \binom{p^{k-j-1}}{s} x^s q^{s-1} \\ &\equiv \ p^{k-j-1}x \ = \ yp^{k-1} \ \not\equiv \ 0 \quad \bmod \ p^k , \end{aligned}$$

so that the order of x is precisely p^{k-j}. The very last assertion of the theorem follows by noting that $1^\dagger = -(1 + q + q^2 + \ldots)$, so that $1^\dagger q = q'$.

□

3 Some technical lemmas

In this section we collect together some observations of a technical nature which will be useful later in deriving group presentations. The proofs of Lemmas 3.1 and 3.2, also noted in [9], are straightforward inductions and left to the reader.

Lemma 3.1. *If G is a group and $x, y, z \in G$ such that $[x\,, y] = z$ and $[x\,, z] = [y\,, z] = 1$ then $[x^\lambda\,, y^\mu] = z^{\lambda\mu}$ for all $\lambda\,, \mu \in \mathbb{Z}^+$.*

Lemma 3.2. *If G is a group and $x, y \in G$ such that $[x\,, y] = y^{\alpha}$ for some $\alpha \in \mathbb{Z}$ then*

$$[x^{\lambda}\,, y^{\mu}] = y^{\mu(1-(1-\alpha)^{\lambda})}$$

for all $\lambda\,, \mu \in \mathbb{Z}^{+}$.

Lemma 3.3. *Let p be prime and k, ℓ be positive integers such that $\ell \leq k$. If $p = 2$ we assume that $\ell > 1$. Put*

$$q = p^{\ell} \qquad \text{and} \qquad L = \begin{cases} 0 & \text{if } k - 2\ell \leq 0 \\ p^{k-2\ell} - 1 & \text{if } k - 2\ell > 0\,. \end{cases}$$

Suppose G is a group, $x, y, z, w \in G$ such that x, y, z, w each have order dividing p^{k},

$$x^{z} = x^{1-q}\,,\ x^{w} = x^{1-q'}\,,\ y^{z} = y^{1-q'}\,,\ y^{w} = y^{1-q}\,,\ [z\,, w] = 1$$

(all quasi-inversion taking place in $\mathbb{Z}_{p^k}$), and for each $m = 0\,, \ldots\,, L\,,$

$$x^{\alpha} y = z^{-\beta} y x^{\alpha} w^{\beta}$$

where $\alpha = (1-q)^{mq}$ and β is the least nonnegative integer such that

$$1^{\circ^{(q)}\beta} = -\alpha q$$

in $\mathbb{Z}_{p^k}$ (which exists because $(\mathbb{Z}_{p^k}, \circ^{(q)})$ is generated by 1). Then, for all $\lambda\,, \mu \in \mathbb{Z}^{+}$,

$$x^{\lambda} y^{\mu} = z^{-\nu} y^{\mu} x^{\lambda} w^{\nu}$$

where ν is the least nonnegative integer such that

$$1^{\circ^{(q)}\nu} = -\lambda\mu q$$

in $\mathbb{Z}_{p^k}$.

Proof. The case $\lambda = \mu = 1$ is covered by the hypothesis (when $m = 0$), which starts an induction. In the following, since orders divide p^k, we may interpret exponents as elements of $\mathbb{Z}_{p^k}$. Let $\lambda > 1$. By an inductive hypothesis, choosing β so that $1^{\circ(q)\beta} = -(\lambda - 1)q$,

$$\begin{aligned} x^\lambda y &= x x^{\lambda-1} y = x z^{-\beta} y x^{\lambda-1} w^\beta = z^{-\beta} x^{z^{-\beta}} y x^{\lambda-1} w^\beta \\ &= z^{-\beta} x^{(1-q)^{-\beta}} y x^{\lambda-1} w^\beta . \end{aligned}$$

But β is a multiple of q, since, by Theorem 2.8, $-(\lambda-1)q$ has order dividing $p^{k-\ell}$ and 1 has order p^k in the group $(\mathbb{Z}_{p^k}, \circ^{(q)})$. Note also, by Theorem 2.8 and Corollary 2.3, that $1-q$ has order $p^{k-\ell}$ in $G(\mathbb{Z}_{p^k})$. Write $-\beta = Kq$ for some integer K. If $L = 0$ then

$$(1-q)^{-\beta} = ((1-q)^q)^K = 1^K = 1 ,$$

since $p^{k-\ell}$ divides q, yielding, by the hypothesis when $m = 0$,

$$x^{(1-q)^{-\beta}} y = xy = z^{-\gamma} y x w^\gamma = z^{-\gamma} y x^{(1-q)^{-\beta}} w^\gamma$$

where $1^{\circ(q)\gamma} = -q = -(1-q)^{-\beta} q$. If $L > 0$ then write

$$K = m p^{k-2\ell} + n \qquad \text{where} \qquad 0 \leq n \leq L$$

so that

$$(1-q)^{-\beta} = ((1-q)^{p^{k-\ell}})^m (1-q)^{nq} = (1-q)^{nq} ,$$

yielding

$$x^{(1-q)^{-\beta}} y = z^{-\gamma} y x^{(1-q)^{-\beta}} w^\gamma$$

by the hypothesis where $1^{\circ(q)\gamma} = -(1-q)^{-\beta} q$. In both cases,

$$\begin{aligned} x^\lambda y &= z^{-\beta} z^{-\gamma} y x^{(1-q)^{-\beta}} w^\gamma x^{\lambda-1} w^\beta = z^{-(\beta+\gamma)} y x^{(1-q)^{-\beta}} (x^{\lambda-1})^{w^{-\gamma}} w^\gamma w^\beta \\ &= z^{-(\beta+\gamma)} y x^{(1-q)^{-\beta}} x^{(1-q')^{-\gamma}(\lambda-1)} w^{\gamma+\beta} = z^{-\delta} y x^\lambda w^\delta \end{aligned}$$

where $\delta = \alpha + \beta$, after observing that, in $\mathbb{Z}_{p^k}$, using the formulae of Theorem 2.8,

$$\begin{aligned}
(1-q)^{-\beta} + (1-q')^{-\gamma}(\lambda-1) &= (1-q)^{-\beta} + (1-q)^{\gamma}(\lambda-1) \\
= (1-q)^{-\beta} + (1-q1^{\circ(q)\gamma})(\lambda-1) &= \lambda - 1 + (1-q)^{-\beta}(1+(\lambda-1)q^2) \\
= \lambda - 1 + (1-q)^{-\beta}(1-q1^{\circ(q)\beta}) &= \lambda - 1 + (1-q)^{-\beta}(1-q)^{\beta} = \lambda .
\end{aligned}$$

Further, by Theorem 2.8,

$$\begin{aligned}
1^{\circ(q)\delta} &= 1^{\circ(q)\beta} \circ^{(q)} 1^{\circ(q)\gamma} = -(\lambda-1)q - (1-q)^{-\beta}q(1-q1^{\circ(q)\beta}) \\
&= -\lambda q + q - q(1-q)^{-\beta}(1-q)^{\beta} = -\lambda q .
\end{aligned}$$

Now let $\mu > 1$, $\lambda \geq 1$. By an inductive hypothesis, we have, choosing δ such that $1^{\circ(q)\delta} = -\lambda(\mu-1)q$,

$$\begin{aligned}
x^{\lambda}y^{\mu} &= x^{\lambda}y^{\mu-1}y = z^{-\delta}y^{\mu-1}x^{\lambda}w^{\delta}y = z^{-\delta}y^{\mu-1}w^{\delta}(x^{\lambda})^{w^{\delta}}y \\
&= z^{-\delta}y^{\mu-1}w^{\delta}x^{(1-q')^{\delta}\lambda}y = z^{-\delta}y^{\mu-1}w^{\delta}z^{-\epsilon}yx^{(1-q')^{\delta}\lambda}w^{\epsilon} ,
\end{aligned}$$

choosing ϵ such that $1^{\circ(q)\epsilon} = -(1-q')^{\delta}\lambda q$ by the first half, so that, since $[z, w] = 1$,

$$\begin{aligned}
x^{\lambda}y^{\mu} &= z^{-\delta}y^{\mu-1}z^{-\epsilon}w^{\delta}yx^{(1-q')^{\delta}\lambda}w^{\epsilon} \\
&= z^{-\delta}z^{-\epsilon}(y^{\mu-1})^{z^{-\epsilon}}y^{w^{-\delta}}w^{\delta}x^{(1-q')^{\delta}\lambda}w^{\epsilon} \\
&= z^{-(\delta+\epsilon)}y^{(1-q')^{-\epsilon}(\mu-1)}y^{(1-q)^{-\delta}}(x^{(1-q')^{\delta}\lambda})^{w^{-\delta}}w^{\delta}w^{\epsilon} \\
&= z^{-\sigma}y^{(1-q')^{-\epsilon}(\mu-1)+(1-q)^{-\delta}}x^{(1-q')^{-\delta}(1-q')^{\delta}\lambda}w^{\sigma} \\
&= z^{-\sigma}y^{\mu}x^{\lambda}w^{\sigma}
\end{aligned}$$

where $\sigma = \epsilon + \gamma$, after observing that, again by Theorem 2.8,

$$\begin{aligned}
(1-q')^{-\epsilon}(\mu-1) + (1-q)^{-\delta} &= (1-q)^{\epsilon}(\mu-1) + (1-q)^{-\delta} \\
&= (1-q1^{\circ(q)\epsilon})(\mu-1) + (1-q)^{-\delta} \\
&= \mu - 1 + q(\mu-1)(1-q')^{\delta}\lambda q + (1-q)^{-\delta} \\
&= \mu - 1 + (1-q)^{-\delta}(1-q1^{\circ(q)\delta}) \\
&= \mu - 1 + (1-q)^{-\delta}(1-q)^{\delta} = \mu .
\end{aligned}$$

Finally we observe that

$$\begin{aligned} 1^{\circ^{(q)}\sigma} &= 1^{\circ^{(q)}\delta} \circ^{(q)} 1^{\circ^{(q)}\epsilon} \\ &= -\lambda(\mu-1)q - (1-q')^{\delta}\lambda q(1-q1^{\circ^{(q)}\delta}) \\ &= -\lambda\mu q + \lambda q(1-(1-q)^{-\delta}(1-q)^{\delta}) \;=\; -\lambda\mu q\,. \end{aligned}$$

□

4 A group presentation

Throughout p denotes a prime and k a positive integer. Our aim is to exhibit a group presentation for any Munn ring over $\mathbb{Z}_{p^k}$ with respect to a scalar sandwich matrix where the scalar is a multiple of p, regarded as a group with respect to the circle operation. Multiplying through by a unit, as explained in the first section, it suffices to assume the scalar is a power of p. Up to isomorphism then, the problem is to find a presentation for the group

$$(\mathsf{Mat}_n(\mathbb{Z}_{p^k}), \circ^{(q)})$$

where $q = p^\ell$ for some $\ell \leq k$. It is hoped that this will be a stepping stone towards a complete understanding of the circle monoids of all finite Munn rings over $\mathbb{Z}_{p^k}$, since, in the general case, up to isomorphism, one may take the sandwich matrix to be a direct sum of scalar matrices augmented possibly by extra rows or columns of zeros (see Chapters 3 and 6 of [7]).

We begin by reviewing the general theory of group presentations of radical matrix rings initiated by Coleman and Easdown [9], and apply one of their main results in our context. Let S be any radical ring and suppose

$$(\,S\,,+\,) \cong \langle\,\Gamma^{(+)}\,|\,\mathcal{R}^{(+)}\,\rangle\,,\;(\,S\,,\circ\,) \cong \langle\,\Gamma^{(\circ)}\,|\,\mathcal{R}^{(\circ)}\,\rangle$$

for some alphabet $\Gamma^{(+)}$, $\Gamma^{(\circ)}$ and collections of relations $\mathcal{R}^{(+)}$, $\mathcal{R}^{(\circ)}$ over $\Gamma^{(+)}$, $\Gamma^{(\circ)}$ respectively. We may suppose no generator is redundant, so that there are collections $W^{(+)}$, $W^{(\circ)}$ of words (normal forms), over $\Gamma^{(+)}$, $\Gamma^{(\circ)}$ respectively such that

$$\Gamma^{(+)} \subseteq W^{(+)} , \quad \Gamma^{(\circ)} \subseteq W^{(\circ)} ,$$

and bijections

$$\varphi \, : \, W^{(+)} \longrightarrow S \, , \quad \psi : W^{(\circ)} \longrightarrow S$$

whose inverses induce the above isomorphisms. We now create a new alphabet

$$\Gamma = \{ \, \sigma_{ij} \mid i \, , j \in \{ \, 1 \, , \ldots \, , n \, \} \, , \;\; \sigma \in \Gamma^{(+)} \text{ if } i \neq j \, , \;\; \text{and} \;\; \sigma \in \Gamma^{(\circ)} \text{ if } i = j \, \} \, .$$

For any $i \, , j \in \{ \, 1 \, , \ldots \, , n \, \}$, put

$$1_{ij} = 1$$

where 1 here denotes the empty word, and if $w = \sigma^{(1)} \ldots \sigma^{(m)}$ is any non-empty word where $\sigma^{(1)} , \ldots , \sigma^{(m)}$ are letters, put

$$w_{ij} = \sigma_{ij}^{(1)} \ldots \sigma_{ij}^{(m)} \, ,$$

so that, if w is over $\Gamma^{(+)}$ and $i \neq j$, or over $\Gamma^{(\circ)}$ and $i = j$, then w_{ij} is over Γ. For any $i \neq j$, let $\mathcal{R}_{ij}^{(+)}$ denote the collection of relations of the form

$$v_{ij} = w_{ij}$$

where $v = w$ is a relation of $\mathcal{R}^{(+)}$. For any i, let $\mathcal{R}_{i}^{(\circ)}$ denote the collection of relations of the form

$$v_{ii} = w_{ii}$$

where $v = w$ is a relation of $\mathcal{R}^{(\circ)}$. Now let $\mathcal{R}$ denote the collection of relations of the following types:

(1) $\bigcup\limits_{i \neq j} \mathcal{R}_{ij}^{(+)} \cup \bigcup\limits_{i} \mathcal{R}_{i}^{(\circ)}$.

(2) $(\forall i \neq l\,, j \neq k\,)\left(\forall a \in \begin{cases}\Gamma^{(+)} & \text{if } i \neq j \\ \Gamma^{(\circ)} & \text{if } i = j\end{cases}\right)\left(\forall b \in \begin{cases}\Gamma^{(+)} & \text{if } k \neq l \\ \Gamma^{(\circ)} & \text{if } k = l\end{cases}\right)$

$$[\, a_{ij}\,, b_{kl}\,] = 1\,.$$

(3) $(\forall i \neq j \neq k \neq i\,)(\forall u\,, v \in W^{(+)}\,)$

$$[\, u_{ij}\,, v_{jk}\,] = \big(\,(\,-(\,u\varphi\,)(\,v\varphi\,)\,)\varphi^{-1}\,\big)_{ik}\ .$$

(4) $(\forall i \neq j\,)(\forall u \in W^{(\circ)}\,, v \in W^{(+)}\,)$

$$[\, u_{ii}\,, v_{ij}\,] = \big(\,(\,(\,u\psi\,)'(\,v\varphi\,)\,)\varphi^{-1}\,\big)_{ij}\ .$$

(5) $(\forall i \neq j\,)(\forall u \in W^{(+)}\,, v \in W^{(\circ)}\,)$

$$[\, u_{ij}\,, v_{jj}\,] = \big(\,(\,-(\,u\varphi\,)(\,v\psi\,)\,)\varphi^{-1}\,\big)_{ij}\ .$$

(6) $(\forall i > j\,)(\forall u\,, v \in W^{(+)}\,)$

$$u_{ij}v_{ji} = \big(\,(\,-(\,v\varphi\,)(\,u\varphi\,)\,)'\psi^{-1}\,\big)_{jj}\, v_{ji}u_{ij}\,\big(\,(\,-(\,u\varphi\,)(\,v\varphi\,)\,)\psi^{-1}\,\big)_{ii}\ .$$

The following is proved in [9]:

Theorem 4.1. *The groups* $(\,\mathsf{Mat}_n(S)\,, \circ\,)$ *and* $\langle\, \Gamma \,|\, \mathcal{R}\,\rangle$ *are isomorphic.*

We now apply this theorem to prove the following:

Theorem 4.2. *Let* p *be prime and* k, ℓ *positive integers such that* $\ell \leq k$. *Suppose* $\ell > 1$ *if* $p = 2$. *Put*

$$q = p^{\ell} \qquad \textit{and} \qquad L = \begin{cases} 0 & \textit{if } k - 2\ell \leq 0 \\ p^{k-2\ell} - 1 & \textit{if } k - 2\ell > 0\,. \end{cases}$$

Then the ring

$$\mathsf{Mat}_n(\mathbb{Z}_{p^k}, +, *^{(q)})$$

is a group with respect to the circle operation $\circ^{(q)}$ *and has the group presentation* $\langle A \mid \mathcal{R} \rangle$ *where*

$$A \;=\; \{\; a_{ij} \mid i,j \in \{1,\dots,n\} \;\}$$

and $\mathcal{R}$ *consists of the following relations:*

(1) $(\forall i\,, j\,)\quad a_{ij}^{p^k} = 1\,;$

(2) $(\forall i \neq l\,, j \neq k\,)\quad [\,a_{ij}\,, a_{kl}\,] = 1\,;$

(3) $(\forall i \neq j \neq k \neq i\,)\quad [\,a_{ij}\,, a_{jk}\,] = a_{ik}^{-q}\,;$

(4) $(\forall i \neq j\,)\quad [\,a_{ii}\,, a_{ij}\,] = a_{ij}^{q'}\,;$

(5) $(\forall i \neq j\,)\quad [\,a_{ij}\,, a_{jj}\,] = a_{ij}^{-q}\,;$

(6) $(\forall i > j\,)(\,\forall m = 0\,,\dots\,,\,L\,)$

$$a_{ij}^{\alpha} a_{ji} = a_{jj}^{-\beta} a_{ji} a_{ij}^{\alpha} a_{ii}^{\beta}$$

where $\alpha = (1-q)^{mq}$ *and* β *is the least nonnegative integer such that*

$$1^{\circ^{(q)}\beta} = -\alpha q$$

in $\mathbb{Z}_{p^k}$ *(which exists because* $(\,p\mathbb{Z}_{p^k}\,, \circ^{(q)}\,)$ *is cyclic generated by* 1 *).*

Note that (3) and (5) could be amalgamated. However in practice it is convenient to keep them separate because when $n = 2$ the collection (3) is empty, and also (5) may easily be reformulated as conjugation relations.

Proof. Put $G = (\mathsf{Mat}_n(\mathbb{Z}_{p^k}), \circ^{(q)})$. If $x \in \mathbb{Z}_{p^k}$ denote the quasi-inverse with respect to $\circ$ by $'$ and with respect to $\circ^{(q)}$ by $\dagger$. By Corollary 2.5,

$$(\mathbb{Z}_{p^k}, +) \;\cong\; (\mathbb{Z}_{p^k}, \circ^{(q)}) \;\cong\; C_{p^\ell} \;\cong\; \langle a \mid a^{p^k} = 1 \rangle.$$

In the preceding theory, then, we take $\Gamma^{(+)} = \Gamma^{(\circ)} = \{a\}$,

$$W^{(+)} = W^{(\circ)} = \{a^i \mid 0 \le i \le p^k - 1\}\;,$$

and $\phi : a^i \mapsto i$, $\psi : a^i \mapsto 1^{\circ(q)i}$ for each i. By Theorem 4.1, and the formulae in Theorem 2.8, a presentation for G uses generators a_{ij} where $i, j \in \{1, \ldots, n\}$ and relations

(1) $(\forall i , j) \quad a_{ij}^{p^k} = 1$;

(2) $(\forall i \neq l , j \neq k) \quad [a_{ij} , a_{kl}] = 1$;

(3) $(\forall i \neq j \neq k \neq i)(\forall \lambda, \mu) \quad [a_{ij}^{\lambda} , a_{jk}^{\mu}] = a_{ik}^{-\lambda\mu q}$;

(4) $(\forall i \neq j)(\forall \lambda, \mu) \quad [a_{ii}^{\lambda} , a_{ij}^{\mu}] = a_{ij}^{(1^{\circ(q)}\lambda)^{\dagger}\mu q} = a_{ij}^{\mu(1-(1-q')^{\lambda})}$;

(5) $(\forall i \neq j)(\forall \lambda, \mu) \quad [a_{ij}^{\lambda} , a_{jj}^{\mu}] = a_{ij}^{-\lambda 1^{\circ(q)}\mu q} = a_{ij}^{-\lambda(1-(1-q)^{\mu})}$;

(6) $(\forall i > j)(\forall \lambda, \mu)$

$$a_{ij}^{\lambda} a_{ji}^{\mu} = a_{jj}^{-\alpha} a_{ji}^{\mu} a_{ij}^{\lambda} a_{ii}^{\alpha}$$

where $1^{\circ(q)\alpha} = -\lambda\mu q$.

Collections (1) and (2) are the same as in the statement of this theorem. We may replace (3) by the relations

$$(\forall i \neq j \neq k \neq i) \quad [a_{ij} , a_{jk}] = a_{ik}^{-q} ,$$

since the rest are implied by these and Lemma 3.1, in the presence of (2). We may replace (4) by the relations

$$(\forall i \neq j) \quad [a_{ii} , a_{ij}] = a_{ij}^{q'} ,$$

since the rest are implied by these and Lemma 3.2. We may replace (5) by the relations

$$(\forall i \neq j) \quad [a_{ij} , a_{jj}] = a_{ij}^{-q} ,$$

equivalent to

$$(\forall i \neq j) \quad [a_{jj} , a_{ij}] = a_{ij}^{q} ,$$

which, by Lemma 3.2, imply, for each λ, μ,

$$[a_{ij}^{\lambda} , a_{jj}^{\mu}] = [a_{jj}^{\mu} , a_{ij}^{\lambda}]^{-1} == a_{ij}^{-\lambda(1-(1-q)^{\mu})} .$$

Suppose $i \geq j$. Observe that relations above imply

$$a_{ii}^{p^k} \;=\; a_{ij}^{p^k} \;=\; a_{ji}^{p^k} \;=\; a_{jj}^{p^k} \;=\; [a_{jj}, a_{ii}] \;=\; 1 \;,$$

$$a_{ij}^{a_{jj}} \;=\; a_{ij}[a_{ij}, a_{jj}] \;=\; a_{ij}^{1-q} \;, \qquad a_{ij}^{a_{ii}} \;=\; a_{ij}[a_{ii}, a_{ij}]^{-1} \;=\; a_{ij}^{1-q'} \;,$$

and similarly,

$$a_{ji}^{a_{jj}} \;=\; a_{ji}^{1-q'} \;, \qquad a_{ji}^{a_{ii}} \;=\; a_{ji}^{1-q} \;,$$

so that, taking $x = a_{ij}$, $y = a_{ji}$, $z = a_{jj}$ and $w = a_{ii}$, Lemma 3.3 implies all of the relations of (6) may be replaced by the subcollection, for $m = 0, \ldots, L$,

$$a_{ij}^{\alpha} a_{ji} = a_{jj}^{-\beta} a_{ji} a_{ij}^{\alpha} a_{ii}^{\;\beta}$$

where $\alpha = (1-q)^{mq}$ and $1^{\circ^{(q)}\beta} = -\alpha q$. $\square$

The previous proof employs the general machinery of [9]. A direct, though very long, argument can be constructed along the following lines, using some counting to exploit finiteness of the groups. First observe, by calculation, that all of the relations hold if we identify the generator a_{ij} with the $n \times n$ matrix consisting of 1 in the (i,j)th position and 0 elsewhere. For example, for (6), if $\alpha = (1-q)^{mq}$ and $1^{\circ^{(q)}\beta} = -\alpha q$ then $a_{jj}^{-\beta} a_{ji} a_{ij}^{\alpha} a_{ii}^{\beta}$ becomes identified with

$$\begin{array}{cc} & \begin{array}{cc} j & i \end{array} \\ \begin{array}{c} j \\ i \end{array} & \begin{pmatrix} (-\alpha q)^{\dagger} & 0 \\ 0 & 0 \end{pmatrix} \end{array} \circ^{(q)} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \circ^{(q)} \begin{pmatrix} 0 & 0 \\ \alpha & 0 \end{pmatrix} \circ^{(q)} \begin{pmatrix} 0 & 0 \\ 0 & -\alpha q \end{pmatrix}$$

$$= \begin{pmatrix} (-\alpha q)^{\dagger} & 1 - q(-\alpha q)^{\dagger} \\ 0 & 0 \end{pmatrix} \circ^{(q)} \begin{pmatrix} 0 & 0 \\ \alpha & -\alpha q \end{pmatrix}$$

$$= \begin{pmatrix} (-\alpha q)^{\dagger} - q(1 - q(-\alpha q)^{\dagger})\alpha & 1 - q(-\alpha q)^{\dagger} - q(1 - q(-\alpha q)^{\dagger})(-\alpha q) \\ \alpha & -\alpha q \end{pmatrix}$$

$$= \begin{pmatrix} (-\alpha q) \circ^{(q)} (-\alpha q)^{\dagger} & 1 - q\big((-\alpha q) \circ^{(q)} (-\alpha q)^{\dagger}\big) \\ \alpha & -\alpha q \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ \alpha & -\alpha q \end{pmatrix} \;=\; \begin{pmatrix} 0 & 0 \\ \alpha & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \;,$$

which becomes identified with $a_{ij}^{\alpha} a_{ji}$. The next step is to verify that these matrices generate the entire group. For example, when $n = 2$,

$$
\begin{aligned}
\begin{pmatrix} x & y \\ z & w \end{pmatrix} &= \begin{pmatrix} x & 0 \\ z & 0 \end{pmatrix} \circ^{(q)} \begin{pmatrix} 0 & y(1-xq)^{-1} \\ 0 & w + zqy(1-xq)^{-1} \end{pmatrix} \\
&= \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \circ^{(q)} \begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix} \circ^{(q)} \begin{pmatrix} 0 & 0 \\ 0 & w + zqy(1-xq)^{-1} \end{pmatrix} \\
&\qquad\qquad \circ^{(q)} \begin{pmatrix} 0 & y(1-xq)^{-1} \\ 0 & 0 \end{pmatrix} ,
\end{aligned}
$$

which becomes identified with $a_{11}^{\alpha} a_{21}^{z} a_{22}^{\beta} a_{12}^{y(1-xq)^{-1}}$ where $1^{\circ^{(q)}\alpha} = x$ and $1^{\circ^{(q)}\beta} = w + zqy(1-xq)^{-1}$. The previous calculation can be put into a conceptual framework involving semidirect and general products, leading to the following recursive formula for any radical matrix ring S, which is proved in Section 6 of [9]:

$$
(\mathsf{Mat}_n(S)\,,\circ) \cong \big((S\,,+)^{n-1} \rtimes (\mathsf{Mat}_{n-1}(S)\,,\circ)\big) \circledast \big((S\,,+)^{n-1} \rtimes (S\,,\circ)\big) \ ,
$$

where $\rtimes$ and $\circledast$ denote semidirect and general product respectively. Details and background, particularly for general products, can be found in Sections 1 and 6 of [9].

In our sketch of a direct proof of Theorem 4.2 we have reached the stage at least that $\mathsf{Mat}_n(\mathbb{Z}_{p^k}, \circ^{(q)})$ is a homomorphic image of the group defined by the presentation. To see that the homomorphism is an isomorphism it is sufficient to prove that the group contains at most p^{kn^2} elements, the size of $\mathsf{Mat}_n(\mathbb{Z}_{p^k})$. One may do this by proving that if $w \in W$ and a_{kl} is any generator, where

$$
W \;=\; \left\{ \prod_{i=1}^{n} \prod_{j=1}^{n} a_{ij}^{\alpha_{ij}} \;\middle|\; \alpha_{ij} \in \{0, \ldots, p^k - 1\} \right\}
$$

then the relations can be used to transform the word $w a_{kl}$ into another word from W, and noticing that the size of W is p^{kn^2}. The first step towards a word argument would be to apply Lemmas 3.1, 3.2 and 3.3 (as in the formal proof of Theorem 4.2) to amplify the supply of relations and then use an inductive argument to manipulate words. A general argument and technique along these lines is provided in Lemma 3.5 of [9], which is stated and proved for monoids.

5 Examples

Example 5.1. The group $(\mathsf{Mat}_2(\mathbb{Z}_9), \circ^{(3)})$ has the following presentation:

$$\begin{aligned}\langle\, a, b, c, d \mid\ & a^9 = b^9 = c^9 = d^9 = 1\,,\quad ad = da\,, \\ & b^a = b^{-d} = b^4\,,\ c^d = c^{-a} = c^4\,,\ bc = cba^{-3}d^3\,\rangle\end{aligned}$$

This follows from Theorem 4.2, putting

$$a = a_{11}\,,\ b = a_{12}\,,\ c = a_{21}\,,\ d = a_{22}\,,$$

rearranging commutator relations as conjugation relations, noting that $3' = 3$ in $\mathbb{Z}_9$, $L = 0$ (so (6) only provides one relation), and observing that a^3 and d^3 are central. By Corollary 2.5, this is also a presentation for $(3\mathsf{Mat}_2(\mathbb{Z}_{27}), \circ)$, and appears as Example 8.3 in [9] when $p = 3$. This group has a decomposition

$$(C_9 \rtimes C_9) \circledast (C_9 \rtimes C_9)$$

with appropriate semidirect and general product actions.

Example 5.2. Applying Theorem 4.2, as in the previous example, but noting $L = 2$ so (6) provides 3 relations, the group $\mathsf{Mat}_2(\mathbb{Z}_{27}), \circ^{(3)})$ has the following presentation:

$$\begin{aligned}\langle\, a, b, c, d \mid\ & a^{27} = b^{27} = c^{27} = d^{27} = 1\,,\quad ad = da\,,\ b^a = b^{-d} = b^{-2}\,, \\ & c^d = c^{-a} = c^{-2}\,,\ bc = d^3cba^{-3}\,,\ b^{10}c = d^3cb^{10}a^{-3}\,,\ b^{19}c = d^3cb^{19}a^{-3}\,\rangle\end{aligned}$$

But the matrix $\begin{pmatrix} 0 & 9 \\ 0 & 0 \end{pmatrix}$ clearly commutes under $\circ^{(3)}$ with all matrices, so that b^9 must be central. In particular we may add the relation $b^9c = cb^9$ and use it to deduce the last two relations in the above presentation, which may then be deleted. Thus we get the more succinct presentation:

$$\langle\, a, b, c, d \;\mid\; a^{27} = b^{27} = c^{27} = d^{27} = 1\,,\;\; ad = da\,,\; b^a = b^{-d} = b^{-2}\,,$$
$$c^d = c^{-a} = c^{-2}\,,\; b^9 c = cb^9\,,\; bc = d^3 cba^{-3}\,\rangle$$

(The relation $b^9 c = cb^9$ also follows, of course, by Lemma 3.3, taking $x = b$, $\lambda = 9$, $y = c$, $\mu = 1$, $z = d$, $w = a$ and $\nu = 0$, the least nonnegative integer such that $1^{\circ^{(3)}\nu} = -27 = 0$ in $\mathbb{Z}_{27}$.)

Example 5.3. In the development of the main results of this paper we have been careful to avoid the case $p = 2$, $\ell = 1$. This case is also accounted for, in fact, by observing that, by Corollary 2.2,

$$(\mathbb{Z}_{2^k}, \circ^{(2)}) \;\cong\; (2\mathbb{Z}_{2^{k+1}}, \circ)\,,$$

so that

$$(\mathsf{Mat}_n(\mathbb{Z}_{2^k}), \circ^{(2)}) \;\cong\; (\mathsf{Mat}_n(2\mathbb{Z}_{2^{k+1}}), \circ)\,,$$

a presentation for which is furnished by Theorem 8.4 of [9].

References

[1] N. Antony, "Radicals of rings and the circle operation," Honours thesis, University of Sydney, 2000.

[2] J.C. Ault and J.F. Watters, "Circle groups of nilpotent rings," *American Math. Monthly* **80** (1973), 48-52.

[3] H.L. Chick, "The properties of some rings having isomorphic additive and circle composition groups," *Austral. Math. Soc. Gaz.* **23** (1996), 112-117.

[4] H.L. Chick, "Rings with isomorphic additive and circle composition groups," *Rings and Radicals* (Shijiazhuang, 1994), Pitman Res. Notes. Ser., 346, Longman, Harlow (1996), 160-169.

[5] H.L. Chick and B.J. Gardner, "Commutative quasiregular rings with isomorphic additive and circle composition groups. II. Rational algebras," *Comm. Algebra* **26** (1998), 657-670.

[6] A.H. Clifford and G.B. Preston, *The Algebraic Theory of Semigroups*, Vol. 1, Math. Surveys of the American Math. Soc. 7, Providence, RI, 1961.

[7] C. Coleman, "Circle decompositions of rings, in particular, Munn rings", Doctoral thesis, University of Sydney, 1999.

[8] C. Coleman and D. Easdown, "Complementation in the group of units of a ring," *Bull. Austral. Math. Soc.* **62** (2000), 183-192.

[9] C. Coleman and D. Easdown, "Decompositions of rings under the circle operation," *Beiträge zur algebra und geometrie*, to appear.

[10] I. Fischer and K.E. Eldridge, "Artinian rings with a cyclic quasi-regular group", *Duke Math. J.* **36** (1969), 43-47.

[11] N. Jacobson, *Basic Algebra I*, Freeman, New York, 1985.

[12] A.V. Kelarev, "The groups of units of a commutative semigroup ring," *J. Algebra* **169** (1994), 902-912.

[13] R.L. Kruse, "A note on the adjoint group of a finitely generated radical ring," *J. London Math. Soc.* **1** (1969), 743-744.

[14] R.L. Kruse, "On the circle group of a nilpotent ring," *American Math. Monthly* **77** (1970), 168-170.

204 (1998), 733-741.

[15] D.B. McAlister, "Rings related to completely 0-simple semigroups," *J. Austral. Math. Soc.* **12** (1971), 193-210.

[16] N.R. McConnell and T. Stokes, "Generalising quasiregularity for rings," *Austral. Math. Soc. Gaz.* **25** (1998), 250-252.

[17] B. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[18] W.D. Munn, "On semigroup algebras," *Proc. Camb. Phil. Soc.* **51** (1955), 1-15.

[19] W.D. Munn, "Semigroup rings of completely regular semigroups," *Lattices, Semigroups and Universal Algebras*, Lisbon (1988), 191-210, Plenum, New York, 1990.

[20] J. Okninski, *Semigroup Algebras*, Marcel Dekker, New York, 1991.

102 (1986), 91-102.

[21] R. Sandling, "Group rings of circle and unit groups," *Math. Z.* **140** (1974), 195-202.

[22] K.I. Tahara and A. Hosomi, "On the circle group of finite nilpotent rings," *Groups – Korea 1983*, Eds. A.C. Kim and B.H. Neumann, Springer Lecture Notes in Mathematics 1098 (1984), 161-179.

[23] J.F. Watters, "Radicals of semigroup rings," *Glasgow Math. J.* **10** (1969), 85-93.

School of Mathematics and Statistics
University of Sydney, NSW 2006, Australia
noellea@maths.usyd.edu.au
cec@maths.usyd.edu.au
de@maths.usyd.edu.au