Decomposition of rings under the circle operation

Clare Coleman and David Easdown

August 31, 1999

Abstract

We consider rings S, not necessarily with 1, and develop a decomposition theory for submonoids and subgroups of $(S, \circ)$ where the circle operation $\circ$ is defined by $x \circ y = x + y - xy$. Decompositions are expressed in terms of internal semidirect, reverse semidirect and general products, which may be realised externally in terms of naturally occurring representations and antirepresentations. The theory is applied to matrix rings over S when S is radical, obtaining group presentations in terms of $(S, +)$ and $(S, \circ)$. Further details are worked out in special cases when $S = p\mathbb{Z}_{p^t}$ for p prime and $t \geq 3$.

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. 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 different ways depending on the characteristic (see, for example, [10, Theorem 2.26]). Then the mapping

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

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

$$x' \ = \ y \qquad \text{and} \qquad \overline{x} \ = \ 1 - x' \ ,$$

so that, in S^1,

$$\overline{x}\,\widehat{x} \ = \ \widehat{x}\,\overline{x} \ = \ 1 \ .$$

Put

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

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 $\widehat{\ } \ : \ \mathcal{G}(S) \ \rightarrow \ G(S)$ is a group isomorphism.

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, investigated in [7].

Call S *radical* if $S = \mathcal{J}(S)$. The circle group of a radical ring has also been called the *adjoint group* [40]. 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 [1] [40] [12] [13] [39] [37]. Membership criteria for the circle groups of band graded rings have been investigated by Kelarev [11].

It should be remarked that many authors use as circle operation $\circ^+$ defined by $x \circ^+ y = x + y + xy$. This does not matter in our context, however, because negation is an isomorphism between the monoids $(S, \circ)$ and $(S, \circ^+)$. Both $\circ = \circ^{(-1)}$ and $\circ^+ = \circ^{(1)}$ are special cases of the derived associative operation $\circ^{(k)}$, where k is an element of the prime subring of S, defined by

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

Derived associative operations are characterized by McConnell and Stokes[21]. If k is invertible then it is easy to see that $(S, \circ) \cong (S, \circ^{(k)})$ under the map $x \mapsto k^{-1}x$ for $x \in S$.

In this paper we develop a general decomposition theory (Section 5) for submonoids and subgroups of rings under $\circ$, in terms of *semidirect*, *reverse semidirect* and *general products*, defined later in this section. Details of the mappings involved in the case of semidirect and reverse semidirect products can best be understood in terms of naturally occurring representations and antirepresentations (Section 4). This theory is applied to obtain decompositions of the circle group of the ring of matrices with entries from a radical ring S (Section 6), yielding a group presentation (Section 7) in terms of $(S, +)$ and $(S, \circ)$, further details of which are worked out (Section 8) when $S = p\mathbb{Z}_{p^t}$ for p prime and $t \geq 3$.

We establish here some notational conventions used throughout the paper. If M is a monoid then its identity element is denoted by 1 or 1_M, and the *dual* of M is the monoid $M^* = \{x^* \mid x \in M\}$ with multiplication

$$x^* y^* \;=\; (yx)^* \qquad (x, y \in M) \;.$$

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

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

and if H is a subgroup of G then we write $H \leq G$. The use of angular brackets varies slightly according to context. If X is a subset of a monoid or group then $\langle X \rangle$ denotes the submonoid or subgroup, respectively, generated by X. The difference in meaning never causes confusion here. If X is a subset of a ring S then $\langle X \rangle_+$ denotes the additive subgroup generated by X, and if $X \subseteq \mathcal{G}(S)$ then $\langle X \rangle_\circ$ denotes the subgroup generated by X under $\circ$. If Σ is an alphabet and $\mathcal{R}$ a collection of relations then $\langle \Sigma \mid \mathcal{R} \rangle$ denotes a group presentation. Manipulations of group presentations in the final sections use Tietze transformations, a good reference for which is [23]. In some examples, monoid presentations appear (which are not groups), for which we adopt the notation $\langle \Sigma \mid \mathcal{R} \rangle_{\text{monoid}}$.

Let S be a ring, $x \in \mathcal{G}(S)$ and $k \in \mathbb{Z}$. Denote the kth power of x in $(S, \circ)$ by $x^{\circ k}$, and note that, since $\widehat{\ }$ is a monoid homomorphism, $(1-x)^k = 1 - x^{\circ k}$. It is well-known (see, for example [22, Theorem XVI.9]), for p prime and $n \geq 1$, that the group of units of $\mathbb{Z}_{p^n}$ is isomorphic to $C_{p-1} \times C_{p^{n-1}}$, if p is odd, or $p = 2$ and $n \leq 2$, and $C_2 \times C_{2^{n-2}}$, if $p = 2$ and $n > 2$. It is easy to see that

$$(p\mathbb{Z}_{p^n}, \circ) \;=\; \begin{cases} \langle p \rangle_\circ & \text{if } p \text{ is odd, or } p = 2 \text{ and } n \leq 2 \;; \\[2ex] \langle 2, 4 \rangle_\circ & \text{if } p = 2 \text{ and } n > 2 \;. \end{cases}$$

If $n \geq 1$ then we denote by $M_n(S)$ the ring of $n \times n$ matrices with entries from S. Note that $\mathcal{J}(M_n(S)) = M_n(\mathcal{J}(S))$. If S is radical then so also is $M_n(S)$, whence $M_n(S) = \mathcal{G}(M_n(S))$ is a group under $\circ$.

Our development begins by recalling a well-known construction. Let M and N be monoids. Given a monoid antihomomorphism $\varphi : M \longrightarrow \mathrm{End}\,(N)$

then we may form the *(external) semidirect product*

$$N \rtimes_\varphi M = \{\, (n,m) \mid n \in N \,, m \in M \,\}$$

with multiplication

$$(n_1, m_1)(n_2, m_2) = (n_1[n_2(m_1\varphi)], m_1 m_2)$$

which is easily seen to be a monoid with identity $(1,1)$. Dually, given a monoid homomorphism $\varphi : M \longrightarrow \mathrm{End}\,(N)$ then we may form the *(external) reverse semidirect product*

$$M \ltimes_\varphi N = \{\, (m,n) \mid m \in M \,, n \in N \,\}$$

with multiplication

$$(m_1, n_1)(m_2, n_2) = (m_1 m_2, [n_1(m_2\varphi)]n_2)\,,$$

which is a monoid, and one may verify that

$$(M \ltimes_\varphi N)^* \cong N^* \rtimes_{\varphi^*} M^* \tag{1.1}$$

under the map $(m,n)^* \mapsto (n^*, m^*)$ for $m \in M$, $n \in N$, where $\varphi^* : M^* \longrightarrow \mathrm{End}\,(N^*)$ is the antihomomorphism

$$m^*\varphi^* \;:\; n^* \mapsto (n(m\varphi))^* \quad (m \in M \,, n \in N)\,.$$

In both cases above one can easily verify that if M is a group then $\varphi : M \longrightarrow \mathrm{Aut}\,(N)$. If M and N are both groups and $\varphi : M \longrightarrow \mathrm{Aut}\,(N)$ is an antihomomorphism then one verifies that $N \rtimes_\varphi M$ is a group (see also (1.5) below) and

$$N \rtimes_\varphi M \cong M \ltimes_\psi N \tag{1.2}$$

under the map $(n,m) \mapsto (m^{-1}, n^{-1})^{-1}$ for $m \in M$, $n \in N$, where $\psi : M \longrightarrow \mathrm{Aut}\,(N)$ is the homomorphism defined by $m\psi = m^{-1}\phi$ for $m \in M$. This accords with (and can be deduced from) isomorphism (1.1) because every group is isomorphic to its dual under the inversion mapping.

For the development of the theory of semidirect products of semigroups, though not needed in this paper, and for historical background, the interested reader is referred to the work of Nico [27] and Preston [28] [29] [30] [31].

We now describe a construction which encompasses both semidirect and reverse semidirect products, and which arises naturally in the decomposition theory we develop later for circle subgroups and submonoids of rings. The notation is due to Rosenmai [36]. Suppose that we have monoids M and N and maps

$$\lhd : M \times N \longrightarrow M\,, \quad (m,n) \mapsto m \lhd n$$

$$\rhd : M \times N \longrightarrow N\,, \quad (m,n) \mapsto m \rhd n$$

which satisfy the following conditions, known as the *general product axioms*:

(P1) $(\forall m \in M)(\forall n_1\,, n_2 \in N) \quad m \lhd (n_1 n_2) = (m \lhd n_1) \lhd n_2$

(P2) $(\forall m_1\,, m_2 \in M)(\forall n \in N) \quad (m_1 m_2) \rhd n = m_1 \rhd (m_2 \rhd n)$

(P3) $(\forall m_1\,, m_2 \in M)(\forall n \in N) \quad (m_1 m_2) \lhd n = (m_1 \lhd (m_2 \rhd n))(m_2 \lhd n)$

(P4) $(\forall m \in M)(\forall n_1\,, n_2 \in N) \quad m \rhd (n_1 n_2) = (m \rhd n_1)((m \lhd n_1) \rhd n_2)$

(P5) $(\forall m \in M) \quad m \lhd 1_N = m$

(P6) $(\forall n \in N) \quad 1_M \rhd n = n$

(P7) $(\forall n \in N) \quad 1_M \lhd n = 1_M$

(P8) $(\forall m \in M) \quad m \rhd 1_N = 1_N$

Now form the *(external) general product*

$$N \circledast M = \{\, (n,m) \mid n \in N\,, m \in M \,\}$$

with multiplication

$$(n_1, m_1)(n_2, m_2) = (n_1(m_1 \triangleright n_2), (m_1 \triangleleft n_2)m_2)$$

which may be routinely seen to form a monoid with identity element $(1, 1)$.

If $m \triangleleft n = m$ for all $m \in M$, $n \in N$ then one may check that this reduces to the semidirect product

$$N \circledast M = N \rtimes_{\varphi} M \tag{1.3}$$

where $m\varphi : n \mapsto m \triangleright n$ for $m \in M$, $n \in N$. If $m \triangleright n = n$ for all $m \in M$, $n \in N$ then this reduces to the reverse semidirect product

$$N \circledast M = N \ltimes_{\psi} M \tag{1.4}$$

where $n\psi : m \mapsto m \triangleleft n$ for $m \in M$, $n \in N$. If M and N are groups then one may check that $N \circledast M$ is also a group and, for $m \in M$, $n \in N$,

$$(n, m)^{-1} = (m^{-1} \triangleright n^{-1}, m^{-1} \triangleleft n^{-1}). \tag{1.5}$$

The concept of a general product was first studied for groups by B.H. Neumann [26], and subsequently by Zappa [41] and Casadio [2]. For further development in the theory of groups the reader is referred also to the work of Rédei and Szép [32] [33] [34] [35] [38], who introduce the term *skew product*. The concept for semigroups and monoids has been developed by Kunze [14] [15] [16] [17], who refers to them as *bilateral semidirect products*, focusing attention on transformation semigroups and applications to automata theory. The terminology that we use has been popularized by Lavers [18] [19] who finds applications in the theory of vine monoids and monoid presentations. We remark that axioms (P1), (P2), (P3), (P4) define a *semigroup general product*, though we have no use for this wider notion in this paper.

One may ask whether there is a simple criterion for recognizing when a monoid is isomorphic to the general product of two of its submonoids. Call a monoid M an *internal general product* of submonoids N_1 and N_2 if $M = N_1 N_2$ (monoid product of sets) and factorizations are unique, that is

$$(\forall m \in M)(\exists!\, n_1 \in N_1)(\exists!\, n_2 \in N_2) \quad m = n_1 n_2 \,.$$

It is straightforward to verify the following result, first noted by Kunze [14].

Proposition 1.1. *If a monoid M is the internal general product of submonoids N_1 and N_2 then*

$$M \cong N_1 \circledast N_2$$

under the map $n_1 n_2 \mapsto (n_1\,, n_2)$ for $n_1 \in N_1\,, n_2 \in N_2\,,$ with respect to the mappings $\lhd$ and $\rhd$ defined by the equation

$$n_2 n_1 = (n_2 \rhd n_1)(n_2 \lhd n_1)$$

for unique $n_2 \rhd n_1 \in N_1$ and $n_2 \lhd n_1 \in N_2\,.$

Call a monoid M with submonoids N_1, N_2 an *internal semidirect* [*reverse semidirect*] *product of* N_1 *by* N_2 if M is an internal general product of N_1 and N_2 [N_2 and N_1] and

$$(\forall n_1 \in N_1)(\forall n_2 \in N_2)(\exists n_1^* \in N_1) \quad n_2 n_1 \;=\; n_1^* n_2 \quad [\; n_1 n_2 \;=\; n_2 n_1^* \;]\,.$$

We deduce easily the following.

Proposition 1.2. *If a monoid M is the internal semidirect* [*reverse semidirect*] *product of N_1 by N_2 then*

$$M \;\cong\; N_1 \rtimes_\phi N_2 \qquad [\; N_2 \ltimes_\phi N_1 \;]$$

where $\;\phi : N_2 \to \mathrm{End}\,(N_1)\;$ *is defined by the equation*

$$n_2 n_1 \;=\; (n_1(n_2\phi))n_2 \qquad [\; n_1 n_2 \;=\; n_2(n_1(n_2\phi)) \;]$$

for $n_1 \in N_1$, $n_2 \in N_2$.

2 Examples

We give some contrasting examples using groups and monoids illustrating general, semidirect and reverse semidirect products. The group examples will be revisited, from a different direction, in Section 8, as an application of the theory of presentations which we develop in Section 7.

Example 2.1. We give a simple example of a general product which is neither semidirect nor reverse semidirect. Let $M = \{\, x^i \mid i \in \mathbb{Z}^+ \cup \{0\} \,\}$ be the infinite monogenic monoid and define, for $i\,, j \in \mathbb{Z}^+ \cup \{0\}$,

$$x^i \lhd x^j = \begin{cases} 1 & \text{if } j \geq i \\ x^{i-j} & \text{if } i > j \end{cases} \quad , \qquad x^i \rhd x^j = \begin{cases} 1 & \text{if } i \geq j \\ x^{j-i} & \text{if } j > i\,. \end{cases}$$

Then it is routine to check that the general product axioms are satisfied, so we may form the general product $M \circledast M$, and further that

$$M \circledast M \cong \langle\, a\,, b \mid ab = 1 \,\rangle_{\text{monoid}}\,,$$

the bicyclic monoid [9, Example V.4.6][6, Section 1.12].

We give two examples of general products of groups which we will see later arise as the circle groups of the ring of 2×2 matrices over $p\mathbb{Z}_{p^3}$ where p is an odd and even prime respectively.

Example 2.2. Let p be any prime and

$$G = \langle\, x\,, y \mid x^{p^2} = y^{p^2} = 1\,,\ x^y = x^{1-p} \,\rangle\,.$$

Observe that $z \mapsto z^{1-p}$ is an automorphism of C_{p^2} of order p, with respect to which we may form the semidirect product $C_{p^2} \rtimes C_{p^2}$, and this is isomorphic to G. Thus we may write

$$G = \{\, x^i y^j \mid i\,, j \in \mathbb{Z}_{p^2} \,\}$$

with multiplication

$$x^{i_1} y^{j_1} x^{i_2} y^{j_2} = x^{i_1 + i_2 (1-p)^{j_1}} y^{j_1 + j_2}\,.$$

Now define $\triangleleft\,,\triangleright : G\times G \longrightarrow G$ by the rules

$$x^iy^j \triangleleft x^ky^l \;=\; x^{i(1-p)^{-l}}y^{j-ikp}\,, \qquad x^iy^j \triangleright x^ky^l \;=\; x^{k(1-p)^j}y^{l+ikp}\,,$$

interpreting the expressions in the exponents always as elements of $\mathbb{Z}_{p^2}$. The verification of axioms (P5), (P6), (P7), (P8) is trivial and (P1), (P2) straightforward. To check (P3) note that, for $z\in C_{p^2}$,

$$z^{(1-p)^p} = z\,, \quad (z^p)^{(1-p)} = z^p\,.$$

Then $\quad [x^{i_1}y^{j_1} \triangleleft (x^{i_2}y^{j_2} \triangleright x^ky^l)](x^{i_2}y^{j_2} \triangleleft x^ky^l)$

$$\begin{aligned}
&= x^{i_1(1-p)^{-l-i_2kp}+i_2(1-p)^{-l}(1-p)^{j_1-i_1k(1-p)^{j_2}p}}y^{j_1-i_1k(1-p)^{j_2}p+j_2-i_2kp}\\
&= x^{i_1(1-p)^{-l}+i_2(1-p)^{-l}(1-p)^{j_1}}y^{j_1-i_1kp+j_2-i_2kp}\\
&= x^{(i_1+i_2(1-p)^{j_1})(1-p)^{-l}}y^{j_1+j_2-(i_1+i_2(1-p)^{j_1})kp}\\
&= (x^{i_1}y^{j_1}x^{i_2}y^{j_2}) \triangleleft x^ky^l\,,
\end{aligned}$$

which verifies (P3). The verification of (P4) is similar. Thus we may form the general product $G \circledast G$. Observe that

$$y^{-1} \triangleright x \;=\; x^{1+p} \;\;,\quad y^{-1} \triangleleft\, x \;=\; y \;\;,\quad x \,\triangleright y \;=\; y \;\;,\quad x \triangleleft\, y = x^{1+p}\;,$$

$$y\, \triangleright y \;=\; y \triangleleft\, y \;=\; y \;\;,\quad x\, \triangleright x \;=\; xy^p \;\;,\quad x \triangleleft\, x \;=\; xy^{-p}\;.$$

It follows, by an obvious identification of generators and a straightforward counting argument (using the previous observations to check satisfiability of the relations below), that $G \circledast G$ is isomorphic to the group

$$\begin{aligned}\langle\, x_1,y_1,x_2,y_2 \mid {x_i}^{p^2} = {y_i}^{p^2} = 1\,,\ {x_i}^{y_j} = x_i^{1-p}\,,\ i,j=1,2\,,&\\ [y_1\,,y_2]=1\,,[x_1\,,x_2] = y_1^{-p}{y_2}^{p}\,\rangle\,.&\end{aligned}$$

Example 2.3. Consider

$$H = \langle\, x,y,z \,|\, x^4 = y^2 = z^2 = 1\,,\ [x,y] = [y,z] = 1\,, x^z = x^{-1}\,\rangle$$

which may be viewed as a semidirect product, in at least two ways, isomorphic to

$$C_4 \rtimes (C_2 \times C_2) \quad \text{or} \quad (C_4 \times C_2) \rtimes C_2$$

where the copy of C_4 and the second copy of C_2 form a dihedral subgroup of order 8. We may write

$$H = \{\, x^i y^j z^k \mid i \in \mathbb{Z}_4 \,, j, k \in \mathbb{Z}_2 \,\}$$

with multiplication

$$x^{i_1} y^{j_1} z^{k_1} x^{i_2} y^{j_2} z^{k_2} = x^{i_1 + i_2 (-1)^{k_1}} y^{j_1 + j_2} z^{k_1 + k_2} \,.$$

Now define $\lhd \,, \rhd : H \times H \longrightarrow H$ by the rules

$$x^i y^j z^k \lhd x^l y^m z^n \;=\; x^{(-1)^n i} y^{j+il} z^k \,, \qquad x^i y^j z^k \rhd x^l y^m z^n \;=\; x^{(-1)^k l} y^{m+il} z^n \,.$$

It is straightforward to verify the general product axioms (relying on the fact that $y = y^{-1}$ for (P3)). Thus we may form the general product $H \circledast H$ which, by a straightforward counting argument, is isomorphic to

$$\begin{aligned} \langle\, x_1 \,, y_1 \,, z_1 \,, x_2 \,, y_2 \,, z_2 \mid {x_i}^4 = {y_i}^2 = {z_i}^2 = 1 \,, [x_i \,, y_j] = [y_i \,, z_j] = 1 \,, \\ {x_i}^{z_j} = x_i^{-1} \,,\; i, j = 1, 2 \,,\; [y_1 \,, y_2] = [z_1 \,, z_2] = 1 \,, [x_1 \,, x_2] = y_1 y_2 \,\rangle \,. \end{aligned}$$

The differences between semidirect and reverse semidirect products become apparent when one moves beyond the class of groups. We combine both in the example below. A *Munn ring* $\mathcal{M}(S; P)$, where S is a ring and P is an $m \times n$ matrix over S^1, consists of $n \times m$ matrices over S with usual addition of matrices and multiplication $\cdot$ defined by

$$\alpha \cdot \beta \;=\; \alpha P \beta$$

for $\alpha, \beta \in \mathcal{M}(S; P)$, where juxtaposition denotes normal matrix multiplication. For a detailed analysis of the circle monoids of Munn rings the interested reader is referred to another paper [8] of the authors. The terminology *Munn ring* is due to McAlister [20], which in turn derives from the notion of *Munn algebra* (see [24] and [6, Section 5.2]), though in our definition above we allow an unrestricted sandwich matrix P (see also [25]).

Example 2.4. Consider the commutative monoid

$$M_1 = \langle\, x\,, y \,|\, x^2 = 1\,, y^3 = y^2\,, y = xy = yx \,\rangle_{\text{monoid}}$$

which is an ideal extension (in the sense of [6, Section 4.4]) of a two element null semigroup by a copy of C_2 with zero adjoined, and we may write

$$M_1 = \{\, 1\,, x\,, y\,, y^2 = 0 \,\}\,.$$

Then $M_1 \;\cong\; (\mathbb{Z}_4\,, \cdot) \;\cong\; (\mathbb{Z}_4\,, \circ)$. We write $C_4 = \langle z \rangle$ and induce endomorphisms $x\varphi$, $y\varphi$ of C_4 by the rules

$$x\varphi \,:\, z \mapsto z^{-1}\,, \quad y\varphi \,:\, z \mapsto z^2\,.$$

The relations of M_1 are satisfied in $\operatorname{End}(C_4)$ when x , y are replaced by $x\varphi$, $y\varphi$ respectively, so we induce a homomorphism (= antihomomorphism, since M_1 is commutative) $\varphi \,:\, M_1 \longrightarrow \operatorname{End}(C_4)$ with respect to which we may form the semidirect product

$$M_2 = C_4 \rtimes_\varphi M_1\,.$$

Clearly

$$M_2 \;\cong\; \langle\, x\,, y\,, z \,|\, \text{relations of } M_1\,,\ z^4 = 1\,,\ xz = z^3x\,,\ yz = z^2y \,\rangle_{\text{monoid}}$$

and we may write, without causing confusion,

$$M_2 = \{\, z^i x^j\,, z^i y^k \,|\, i \in \mathbb{Z}_4\,, j \in \mathbb{Z}_2\,, k \in \{1\,,2\} \,\}\,.$$

It is not difficult to see, by a simple counting argument, that M_2 is isomorphic to the circle monoid of the Munn ring $\mathcal{M}(\mathbb{Z}_4\,;\, (\begin{smallmatrix}1\\0\end{smallmatrix}))$. Now put

$$K = \langle\, u\,, v \,|\, u^4 = v^4 = [u\,, v] = 1 \,\rangle \;\cong\; C_4 \times C_4$$

and induce endomorphisms $x\psi$, $y\psi$, $z\psi$ of K by the rules

$$\begin{aligned} x\psi &: u \mapsto u^{-1}\,, && v \mapsto v \\ y\psi &: u \mapsto u^2\,, && v \mapsto v \\ z\psi &: u \mapsto uv^{-1}\,, && v \mapsto v\,. \end{aligned}$$

The relations of M_2 are satisfied in $\mathrm{End}\,(K)$ where x , y , z are replaced by $x\psi$, $y\psi$, $z\psi$ respectively, so we induce a homomorphism $\psi\,:\,M_2 \longrightarrow \mathrm{End}\,(K)$ with respect to which we may form the reverse semidirect product

$$M_3 = M_2 \ltimes_\psi K\,.$$

It is not difficult to verify that M_3 is isomorphic to the circle monoid of the Munn ring $\mathcal{M}(\mathbb{Z}_4\,;\,(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}))$, and further that

$$\begin{aligned} M_3 \;\cong\; \langle\, x\,,y\,,z\,,u\,,v\,|\; &\text{relations of } M_2 \text{ and } K\,,\;\; ux = xu^3\,,\;\; uy = yu^2\,, \\ & uz = zuv^3\,,\;\; vx = xv\,,\;\; vy = yv\,,\;\; vz = zv\,\rangle_{\text{monoid}}\,. \end{aligned}$$

3 Some technical lemmas

In this section we collect together some observations of a technical nature which will be useful later in applying Tietze transformations. The proofs of Lemmas 3.1 and 3.2 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. *Suppose that G is a group and $x, y, z \in G$ such that $[x, z] = z^\alpha$ for some $\alpha \in \mathbb{Z}$, $[y, z] = z^2$ and $[x, y] = 1$. Then*

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

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

Proof. Observe that $z^y = z^{-1}$, so, by Lemma 3.2,

$$[x^\lambda y, z^\mu] \;=\; [x^\lambda, z^\mu]^y\,[y, z^\mu] \;=\; z^{-\mu(1-(1-\alpha)^\lambda)}z^{2\mu} \;=\; z^{\mu(1+(1-\alpha)^\lambda)}\,.$$

$\square$

Lemma 3.4. *Let p be a prime, $t \geq 3$, and put*

$$q = \begin{cases} p & \text{if } \; p \neq 2 \\ 4 & \text{if } \; p = 2\,. \end{cases}$$

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

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

(all quasi-inversion taking place in $\mathbb{Z}_{p^t}$), and for each $m = 0\,, \ldots\,, p^{t-3} - 1\,,$

$$x^{1-(-mp^2)'}y = z^{-\alpha}yx^{1-(-mp^2)'}w^\alpha$$

where α is the least positive integer such that

$$(1-q)^\alpha = 1 + (1-(-mp^2)')p^2$$

in $\mathbb{Z}_{p^t}$ (which exists because $q\mathbb{Z}_{p^t} = \langle q \rangle_\circ$). 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 positive integer such that

$$(1-q)^\nu = 1 + \lambda\mu p^2$$

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

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^t, we may interpret exponents as elements of $\mathbb{Z}_{p^t}$. Let $\lambda > 1$. By an inductive hypothesis, choosing α so that $(1-q)^\alpha = 1+(\lambda-1)p^2$,

$$\begin{aligned}
x^\lambda y &= xx^{\lambda-1}y \;=\; xz^{-\alpha}yx^{\lambda-1}w^\alpha \\
&= z^{-\alpha}x^{z^{-\alpha}}yx^{\lambda-1}w^\alpha \\
&= z^{-\alpha}x^{(1-q)^{-\alpha}}yx^{\lambda-1}w^\alpha \\
&= z^{-\alpha}z^{-\beta}yx^{(1-q)^{-\alpha}}w^\beta x^{\lambda-1}w^\alpha\,,
\end{aligned}$$

choosing β such that $(1-q)^\beta = 1+(1-q)^{-\alpha}p^2$ by the hypothesis, since $(1-q)^{-\alpha} = 1-(-(\lambda-1)p^2)'$, so that

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

where $\delta = \alpha+\beta$, after observing that (performing arithmetic in $\mathbb{Z}_{p^t}$)

$$\begin{aligned}
(1-q)^{-\alpha}+(1-q')^{-\beta}(\lambda-1) &= (1-q)^{-\alpha}+(1-q)^\beta(\lambda-1) \\
&= (1-q)^{-\alpha}+(1+(1-q)^{-\alpha}p^2)(\lambda-1) \\
&= \lambda-1+(1-q)^{-\alpha}(1+(\lambda-1)p^2) \\
&= \lambda-1+1 \;=\; \lambda\,.
\end{aligned}$$

Further we have that

$$\begin{aligned}
(1-q)^\delta &= (1-q)^\alpha(1-q)^\beta \\
&= (1-q)^\alpha(1+(1-q)^{-\alpha}p^2) \\
&= (1-q)^\alpha+p^2 = 1+\lambda p^2\,.
\end{aligned}$$

Now let $\mu > 1$, $\lambda \geq 1$. By an inductive hypothesis, we have, choosing γ such that $(1-q)^\gamma = 1+\lambda(\mu-1)p^2$,

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

choosing ϵ such that $(1-q)^\epsilon = 1+(1-q')^\gamma\lambda p^2$ by the first half, so that, since $[z\,,w]=1$,

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

where $\sigma=\epsilon+\gamma$, after observing that

$$\begin{aligned}
(1-q')^{-\epsilon}(\mu-1)+(1-q)^{-\gamma} &= (1-q)^\epsilon(\mu-1)+(1-q)^{-\gamma} \\
&= (1+(1-q')^\gamma\lambda p^2)(\mu-1)+(1-q)^{-\gamma} \\
&= \mu-1+(1-q)^{-\gamma}(\lambda(\mu-1)p^2+1) \\
&= \mu-1+1=\mu\,.
\end{aligned}$$

Further we have that

$$\begin{aligned}
(1-q)^\sigma &= (1-q)^\epsilon(1-q)^\gamma \\
&= (1+(1-q')^\gamma\lambda p^2)(1-q)^\gamma \\
&= (1-q)^\gamma+\lambda p^2 \\
&= 1+\lambda(\mu-1)p^2+\lambda p^2 \\
&= 1+\lambda\mu p^2\,.
\end{aligned}$$

$\square$

The next result is used in developing the presentation in Section 6 for circle groups of rings of matrices over radical rings. Though we only apply it in this paper in a group-theoretic context, it is no harder to state and prove for monoids, and it is useful in studying the circle monoids of Munn rings (see [8]). Note that the angular brackets refer to *submonoid* generation for the remainder of this section.

Lemma 3.5. *Let M be a monoid and n a positive integer. For each $i\,,j \in \{\,1, \ldots, n\,\}$, let $X_{ij} \subseteq M$ and put $Y_{ij} = \langle\, X_{ij}\,\rangle$. Suppose that*

(1) $\quad M = \langle \bigcup_{i,j} X_{ij} \rangle$.

(2) $\quad (\forall i \neq l\,, j \neq k\,)(\,\forall x \in X_{ij}\,)(\,\forall y \in X_{kl}\,) \qquad xy \;=\; yx$

(3) $\quad (\forall i, j\,, k \neq i\,)(\,\forall x \in X_{ij}\,)(\,\forall y \in X_{jk}\,)(\,\exists z_1, z_2, w_1, w_2 \in Y_{ik})$

$$xy \;=\; z_1yx \;=\; yxz_2\;, \quad yx \;=\; xyw_1 \;=\; w_2xy\;;$$

(4) $\quad (\forall i > j\,)(\,\forall x \in Y_{ij}\,)(\,\forall y \in Y_{ji}\,)(\,\exists z \in Y_{jj}\,)(\,\exists w \in Y_{ii}\,) \qquad xy = zyxw\,.$

Then $M = \prod_{i=1}^{n}\prod_{j=1}^{n} Y_{ij}$ *, so, in particular, if M is finite,* $|M| \leq \prod_{i=1}^{n}\prod_{j=1}^{n} |Y_{ij}|$.

We prove Lemma 3.5 by first developing a sequence of lemmas, each of which is assumed to have the hypotheses of Lemma 3.5.

Lemma 3.6. $(\forall j \neq i\,)(\,\forall x \in Y_{ii}\,)(\forall y \in Y_{ij}\,[\,Y_{ji}\,]\,)(\,\exists z\,, w \in Y_{ij}\,[\,Y_{ji}\,]\,)$

$$yx = xz \qquad \textit{and} \qquad xy = wx\;.$$

Proof. This follows by (3) and a simple induction on the number of generators. ☐

Lemma 3.7. $(\forall i \neq j \neq k \neq i\,)(\,\forall x \in Y_{jk}\,)(\,\forall y \in Y_{ij}\,)(\,\exists z_1, z_2 \in Y_{ik}\,)$

$$yx = xyz_1 \qquad \textit{and} \qquad xy = yxz_2\;.$$

Proof. Suppose $i \neq j \neq k \neq i$. By (2), elements of Y_{ik} commute with elements of $Y_{ij} \cup Y_{jk}$, so, by a simple induction on the number of generators, it suffices to suppose $x \in X_{jk}$, $y \in X_{ij}$, and then the result follows immediately by (3). ☐

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

$$R_i \;=\; Y_{i1} \ldots Y_{in}\,.$$

Lemma 3.8. *For each* $i \in \{1, \ldots, n\}$,

$$R_i = \langle \bigcup_{j=1}^{n} X_{ij} \rangle ,$$

so, in particular, $R_i R_i = R_i$.

Proof. Clearly $\bigcup_{j=1}^{n} X_{ij} \subseteq R_i \subseteq \langle \bigcup_{j=1}^{n} X_{ij} \rangle$, so to prove the Lemma it suffices to show R_i is closed under multiplication on the right by elements of $\bigcup_{j=1}^{n} X_{ij}$. Let $g = y_1 \ldots y_n \in R_i$ where $y_j \in Y_{ij}$ for $j = 1, \ldots, n$. Let $k \in \{1, \ldots, n\}$ and choose $x \in X_{ik}$. We show $gx \in R_i$. If $k > i$ then, by (2),

$$gx \;=\; y_1 \ldots y_{k-1}(y_k x) y_{k+1} \ldots y_n \;\in\; R_i .$$

If $k = i$ then, by Lemma 3.6, for each $j > i$, $y_j x = x z_j$ for some $z_j \in Y_{ij}$, so

$$gx \;=\; y_1 \ldots y_{i-1}(y_i x) z_{i+1} \ldots z_n \;\in\; R_i .$$

If $k < i$ then, by (2) and Lemma 3.6, there exists $z \in Y_{ik}$ such that

$$\begin{aligned} gx &= y_1 \ldots y_i \, x \, y_{i+1} \ldots y_n \;=\; y_1 \ldots y_{i-1} \, z \, y_i \, y_{i+1} \ldots y_n \\ &= y_1 \ldots y_{k-1}(y_k z) y_{k+1} \ldots y_n \;\in\; R_i . \end{aligned}$$

□

Lemma 3.9. $(\forall i > j)(\forall k) \quad R_i Y_{jk} \subseteq R_j R_i$.

Proof. Suppose $i, j, k \in \{1, , \ldots, n\}$ and $j < i$. Let $g \in R_i$, $x \in X_{jk}$, so $g = y_1 \ldots y_n$ for some $y_1 \in Y_{i1}, \ldots, y_n \in Y_{in}$. If $i \neq k$ then, by (2),

$$gx \;=\; y_1 \ldots y_j \, x \, y_{j+1} \ldots y_n \;=\; y_1 \ldots y_{j-1} \, x \, w \, y_{j+1} \ldots y_n$$

for some $w \in Y_{ij}$, by Lemma 3.6, if $k = j$, and for $w = y_j z$ for some $z \in Y_{ik}$, by Lemma 3.7, if $k \neq j$, so that, by (2) and Lemma 3.8,

$$\begin{aligned} gx &= x(y_1 \ldots y_{j-1} \, w \, y_{j+1} \ldots y_n) \\ &\in X_{jk} \langle \bigcup_{l=1}^{n} X_{il} \rangle \;=\; X_{jk} R_i \;\subseteq\; R_j R_i . \end{aligned}$$

If $i = k$ then, making free use of (2) throughout,

$$
\begin{aligned}
gx &= y_1 \dots y_i\, x(\, y_{i+1}\, z_{i+1}\,) \dots (\, y_n\, z_n\,) \\
&\qquad\qquad (\,\exists z_{i+1} \in Y_{j,i+1}\,) \dots (\,\exists z_n \in Y_{jn}\,) \text{ by Lemma 3.7} \\
&= y_1 \dots y_{i-1}\, w\, y_i\, y_{i+1}\, \dots y_n\, z_{i+1} \dots z_n \\
&\qquad\qquad (\,\exists w \in Y_{ji}\,) \text{ by Lemma 3.6} \\
&= y_1 \dots y_j\, w\, (\, y_{j+1}\, z_{j+1}\,) \dots (\, y_{i-1}\, z_{i-1}\,) y_i \dots y_n\, z_{i+1} \dots z_n \\
&\qquad\qquad (\,\exists z_{j+1} \in Y_{j,j+1}\,) \dots (\,\exists z_{i-1} \in Y_{j,i-1}\,) \text{ by Lemma 3.7} \\
&= y_1 \dots y_j\, w\, y_{j+1} \dots y_n\, z_{j+1} \dots z_{i-1}\, z_{i+1} \dots z_n \\
&= y_1 \dots y_{j-1}\, (\, u\, w\, y_j\, v\,)\, y_{j+1} \dots y_n\, z_{j+1} \dots z_{i-1}\, z_{i+1} \dots z_n \\
&\qquad\qquad (\,\exists u \in Y_{jj}\,)(\,\exists v \in Y_{ii}\,) \text{ by (4)} \\
&= u\, y_1 \dots y_{j-1}\, w\, y_j\, v\, y_{j+1} \dots y_n\, z_{j+1} \dots z_{i-1}\, z_{i+1} \dots z_n \\
&= u\, w\, (\, y_1\, z_1\,) \dots (\, y_{j-1}\, z_{j-1}\,)\, y_j\, v\, y_{j+1} \dots y_n\, z_{j+1} \dots z_{i-1}\, z_{i+1} \dots z_n \\
&\qquad\qquad (\,\exists z_1 \in Y_{j1}\,) \dots (\,\exists z_{j-1} \in Y_{j,j-1}\,) \text{ by Lemma 3.7} \\
&= (\, u\, w\, z_1 \dots z_{j-1}\,)(\, y_1 \dots y_j\, v\, y_{j+1} \dots y_n\,)(\, z_{j+1} \dots z_{i-1}\, z_{i+1} \dots z_n\,) \\
&\in R_j R_i (\, z_{j+1} \dots z_{i-1}\, z_{i+1} \dots z_n\,) \;\subseteq\; R_j R_j R_i \;=\; R_j R_i\,,
\end{aligned}
$$

in the last line, by iterating the previous case (when $i \neq k$), and also by Lemma 3.8. This proves $R_i X_{jk} \subseteq R_j R_i$. It follows immediately that $R_i Y_{jk} \subseteq R_j R_i$. ☐

Lemma 3.10. $(\,\forall i > j\,)\;\; R_i R_j \subseteq R_j R_i$.

Proof. This follows immediately by Lemmas 3.8 and 3.9. ☐

Proof of Lemma 3.4. We have to show $M = R_1 \dots R_n$. Clearly $\bigcup_{i,j} X_{ij} \subseteq R_1 \dots R_n$, so it suffices to show $R_1 \dots R_n$ is closed under multiplication on the right by elements of $\bigcup_{i,j} X_{ij}$. For any j,

$$R_n X_{nj} \quad \subseteq \quad \langle \overset{n}{\underset{k=1}{\cup}} X_{nk} \rangle \quad = \quad R_n \ ,$$

by Lemma 3.8, so that

$$R_1 \dots R_n X_{nj} \quad \subseteq \quad R_1 \dots R_n \ ,$$

and, for any $i < n$,

$$R_1 \dots R_n X_{ij} \quad \subseteq \quad R_1 \dots R_n R_i \quad \subseteq \quad (\, R_1 \dots R_i \,)(\, R_i \dots R_n \,) \quad = \quad R_1 \dots R_n \ ,$$

since $(\, R_{i+1} \dots R_n \,) R_i \ \subseteq \ R_i \dots R_n$, by Lemma 3.10, and since $R_i R_i = R_i$, by Lemma 3.8. This completes the proof of Lemma 3.5. $\square$

4 Representations and antirepresentations

Consider a ring S. In what follows we develop a sequence of steps leading to naturally occurring representations and antirepresentations of circle submonoids of S by endomorphisms (or automorphisms if the submonoid is a subgroup) of additive subgroups of $(S\,,+)$. From these we may form external semidirect and reverse semidirect products. In the next section we will find conditions under which these become internal, leading to a decomposition theory for a large class of circle monoids and groups.

(1) Define

$$\rho_S \ , \ \lambda_S \, : \, S \longrightarrow \mathrm{End}\,(S\,,+)$$

by, for $x, y \in S$,

$$x\rho_S \ : \ y \mapsto yx \ , \quad x\lambda_S \ : \ y \mapsto xy \ .$$

It is well known (and easily checked) that ρ_S and λ_S are a representation and antirepresentation respectively of S, and faithful if S has 1.

(2) Let M be a multiplicatively closed subset of S^1 and $T\,,U$ be additive subgroups of S^1 closed under multiplication by elements of M on the right, left respectively. Define

$$\rho_{M,T}\ :\ M \longrightarrow \mathrm{End}\,(T\,,+) \quad \text{by} \quad m\rho_{M,T}\ :\ t \mapsto tm \quad (m \in M\,, t \in T)$$

and

$$\lambda_{M,U}\ :\ M \longrightarrow \mathrm{End}\,(U\,,+) \quad \text{by} \quad m\lambda_{M,U}\ :\ u \mapsto mu \quad (m \in M\,, u \in U)\,.$$

Then $\rho_{M,T}$ and $\lambda_{M,U}$ are a representation and antirepresentation respectively, resulting from ρ_{S^1} and λ_{S^1} by restriction. Further, it is easy to see that if $M \leq G(S^1)$, then

$$(4.1) \qquad \rho_{M,T}\ :\ M \longrightarrow \mathrm{Aut}\,(T\,,+) \quad \text{and} \quad \lambda_{M,U}\ :\ M \longrightarrow \mathrm{Aut}\,(U\,,+)\,.$$

(3) Let $\mathcal{M}$ be a subset of S closed under $\circ$, and $T\,,U$ be additive subgroups of S^1 closed under ordinary ring multiplication by elements of $\mathcal{M}$ (and hence also by elements of $\widehat{\mathcal{M}}$) on the right, left respectively. Define the composites

$$\widehat{\rho}_{\mathcal{M},T} \;=\; \widehat{\ }\circ\rho_{\mathcal{M},T} \qquad \text{and} \qquad \widehat{\lambda}_{\mathcal{M},U} \;=\; \widehat{\ }\circ\lambda_{\mathcal{M},U}\,,$$

so

$$m\widehat{\rho}_{\mathcal{M},T}\ :\ t \;\mapsto\; t\widehat{m} \;=\; t - tm \qquad (m \in \mathcal{M}\,, t \in T)$$

and

$$m\widehat{\lambda}_{\mathcal{M},U}\ :\ u \;\mapsto\; \widehat{m}u \;=\; u - mu \quad (m \in \mathcal{M}\,, u \in U)\,.$$

Because they are composites with a monoid homomorphism, we have that $\widehat{\rho}_{\mathcal{M},T}$ and $\widehat{\lambda}_{\mathcal{M},U}$ are a representation and antirepresentation respectively. Further, by (4.1), if $\mathcal{M} \leq (\mathcal{G}(S)\,,\circ)$ then

$$(4.2) \qquad \widehat{\rho}_{\mathcal{M},T}\ :\ \mathcal{M} \longrightarrow \mathrm{Aut}\,(T\,,+) \quad \text{and} \quad \widehat{\lambda}_{\mathcal{M},U}\ :\ \mathcal{M} \longrightarrow \mathrm{Aut}\,(U\,,+)\,.$$

(4) Suppose, in addition to the hypothesis of (3), that there is an anti-isomorphism $^\dagger : \mathcal{M} \longrightarrow \mathcal{M}$ (for example † might be quasi-inversion if $\mathcal{M} \leq (\mathcal{G}(S)\,,\circ))$. Define the composites

$$\widehat{\rho}^{\,\dagger}_{\mathcal{M},T} = {}^\dagger \circ \widehat{\rho}_{\mathcal{M},T} \qquad \text{and} \qquad \widehat{\lambda}^{\,\dagger}_{\mathcal{M},U} = {}^\dagger \circ \widehat{\lambda}_{\mathcal{M},U}$$

so

$$m\widehat{\rho}^{\,\dagger}_{\mathcal{M},T} \;:\; t \mapsto t - tm^\dagger \quad (m \in \mathcal{M}\,, t \in T)$$

and

$$m\widehat{\lambda}^{\,\dagger}_{\mathcal{M},U} \;:\; u \mapsto u - m^\dagger u \quad (m \in \mathcal{M}\,, u \in U)\,.$$

Because they are composites with an anti-isomorphism, $\widehat{\rho}^{\,\dagger}_{\mathcal{M},T}$ and $\widehat{\lambda}^{\,\dagger}_{\mathcal{M},U}$ are an antirepresentation and representation respectively. Further, by (4.2), if $\mathcal{M} \leq (\mathcal{G}(S)\,,\circ)$ then

$$\widehat{\rho}^{\,\dagger}_{\mathcal{M},T} \;:\; \mathcal{M} \longrightarrow \mathrm{Aut}\,(T\,,+) \quad \text{and} \quad \widehat{\lambda}^{\,\dagger}_{\mathcal{M},U} \;:\; \mathcal{M} \longrightarrow \mathrm{Aut}\,(U\,,+)\,.$$

As a result of these four steps, we may, under the appropriate hypotheses, form the external semidirect products

$$U \rtimes_{\widehat{\lambda}_{\mathcal{M},U}} \mathcal{M} \qquad \text{and} \qquad T \rtimes_{\widehat{\rho}^{\,\dagger}_{\mathcal{M},T}} \mathcal{M}\,,$$

and the external reverse semidirect products

$$\mathcal{M} \ltimes_{\widehat{\rho}_{\mathcal{M},T}} T \qquad \text{and} \qquad \mathcal{M} \ltimes_{\widehat{\lambda}^{\,\dagger}_{\mathcal{M},U}} U\,.$$

In the case that $\mathcal{M} \leq (\mathcal{G}(S), \circ)$, and † is quasi-inversion, then all of these are groups and, by (1.2),

$$\mathcal{M} \ltimes_{\widehat{\rho}_{\mathcal{M},T}} T \;\cong\; T \rtimes_{\widehat{\rho}^{\,\dagger}_{\mathcal{M},T}} \mathcal{M}$$

and

$$U \rtimes_{\widehat{\lambda}_{\mathcal{M},U}} \mathcal{M} \;\cong\; \mathcal{M} \ltimes_{\widehat{\lambda}^{\,\dagger}_{\mathcal{M},U}} U\,.$$

5 Circle Decompositions

In this section we find decompositions of circle monoids and groups using internal general, semidirect and reverse semidirect products, and, in particular, look for conditions under which the external constructions of the previous section can be realized up to isomorphism. We begin with general conditions under which additive and circle decompositions coincide and the circle factorization is unique.

Lemma 5.1. *Suppose* $(I\,,+) \le (S\,,+)$, $(\mathcal{H}\,,\circ) \le (\mathcal{G}(S)\,,\circ)$ *and* $I \cap \langle\,\mathcal{H}\rangle_+ = \{0\}$. *If* I *absorbs multiplication on the right* [*left*] *by elements of* $\mathcal{H}$ *then*

$$I + \mathcal{H} = I \circ \mathcal{H} \quad [\,\mathcal{H} \circ I\,]$$

and circle factorizations are unique.

Proof. Suppose I absorbs multiplication on the right by elements of $\mathcal{H}$. If $x \in I$ and $h \in \mathcal{H}$ then $x\widehat{h}\,, x\overline{h} \in I$,

$$x \circ h \;=\; x + h - xh \;=\; x\widehat{h} + h \;\in\; I + \mathcal{H}$$

and

$$x + h \;=\; x\overline{h} + h - x\overline{h}h \;=\; (x\overline{h}) \circ h \;\in\; I \circ \mathcal{H}\,.$$

This proves $I + \mathcal{H} \;=\; I \circ \mathcal{H}$. If $x_1\,, x_2 \in I$, $h_1\,, h_2 \in \mathcal{H}$ and $x_1 \circ h_1 = x_2 \circ h_2$ then

$$h_1 - h_2 \;=\; x_2 - x_1 + x_1h_1 - x_2h_2 \;\in\; I \cap \langle\,\mathcal{H}\rangle_+ \;=\; \{0\}\,,$$

so $h_1 = h_2$ and $x_1 = x_1 \circ h_1 \circ h_1{}' = x_2 \circ h_1 \circ h_1{}' = x_2$. This proves circle factorizations are unique. The other half of the lemma is dual. $\square$

Theorem 5.2. *Suppose that I is a subring of S, $(\mathcal{H}, \circ) \leq (\mathcal{G}(S), \circ)$, $I \cap \langle \mathcal{H} \rangle_+ = \{0\}$ and I absorbs multiplication by elements of $\mathcal{H}$ on both the right and left. Then*

$$I + \mathcal{H} = I \circ \mathcal{H} = \mathcal{H} \circ I$$

and $I + \mathcal{H}$ is the internal semidirect product of $(I, \circ)$ by $(\mathcal{H}, \circ)$. Furthermore

$$I + \mathcal{H} \cong (I, \circ) \rtimes_\theta (\mathcal{H}, \circ)$$

where θ is defined by

$$h\theta : x \mapsto \widehat{h}x\overline{h} \qquad (x \in I, h \in \mathcal{H}) .$$

Proof. Observe that $I + \mathcal{H}$ is a submonoid of $(S, \circ)$, by the formula

$$(x_1 + h_1) \circ (x_2 + h_2) = (x_1 \circ x_2) + (h_1 \circ h_2) - x_1 h_2 - h_1 x_2 \tag{5.1}$$

and the fact that I absorbs multiplication by elements of $\mathcal{H}$ on both the right and the left, and, by Lemma 5.1, that $I + \mathcal{H} = I \circ \mathcal{H} = \mathcal{H} \circ I$ and circle factorizations are unique. If $x \in I, h \in \mathcal{H}$ then $h' \circ x \circ h = x - h'x - xh + h'xh \in I$ so that I is closed under conjugation by elements of $\mathcal{H}$. It follows immediately that $I + \mathcal{H}$ is the internal semidirect product of $(I, \circ)$ by $(\mathcal{H}, \circ)$. The last claim follows easily by observing, for $x \in I, h \in \mathcal{H}$, that

$$h \circ x = h + x - hx = \widehat{h}x + h = (\widehat{h}x\overline{h}) \circ h .$$

□

Corollary 5.3. *If I is a subring of S, $(\mathcal{H}, \circ) \leq (\mathcal{G}(S), \circ)$, $I \cap \langle \mathcal{H} \rangle_+ = \{0\}$, I absorbs multiplication by elements of $\mathcal{H}$ on the right [left] and $\mathcal{H}$ annihilates I by multiplication on the left [right], then*

$$I + \mathcal{H} \;=\; I \circ \mathcal{H} \;=\; \mathcal{H} \circ I ,$$

$I + \mathcal{H}$ is the internal semidirect product of $(I, \circ)$ by $(\mathcal{H}, \circ)$, and

$$I + \mathcal{H} \;\cong\; (I, \circ) \rtimes_{\widehat{\rho}'_{\mathcal{H},I}} (\mathcal{H}, \circ) \quad [(I, \circ) \rtimes_{\widehat{\lambda}_{\mathcal{H},I}} (\mathcal{H}, \circ)] .$$

Proof. This is immediate from Theorem 5.2, noting that for $x \in I\,, h \in \mathcal{H}\,,$

$$\widehat{h}x\overline{h} = \begin{cases} x\overline{h} & \text{if } hx = 0 \\ \widehat{h}x & \text{if } x\overline{h} = 0\,. \end{cases}$$

□

Theorem 5.4. *Suppose that I is a subring of $S\,,$ $(\mathcal{H}\,,+) \leq (S\,,+)\,,$ $I \cap \mathcal{H} = \{0\}\,,$ $(\mathcal{H}\,,\circ) \leq (\mathcal{G}(S)\,,\circ)$ and I and $\mathcal{H}$ absorb each other by multiplication on the right [left]. Then*

$$I + \mathcal{H} = I \circ \mathcal{H} \quad [\,\mathcal{H} \circ I\,]$$

and $I + \mathcal{H}$ is the internal general product of $(I\,,\circ)$ with $(\mathcal{H}\,,\circ)$ [$(\mathcal{H}\,,\circ)$ with $(I\,,\circ)$]. Furthermore

$$I + \mathcal{H} \quad \cong \quad (I\,,\circ) \circledast (\mathcal{H}\,,\circ) \quad [\,(\mathcal{H}\,,\circ) \circledast (I\,,\circ)\,]$$

where the mappings $\lhd$ and $\rhd$ are defined by, for $x \in I$, $h \in \mathcal{H}$,

$$h \lhd x = h\widehat{x}\,,\ h \rhd x = x\overline{h\widehat{x}} \qquad [\,x \lhd h = \overline{\widehat{x}h}x\,,\ x \rhd h = \widehat{x}h\,]$$

Proof. We prove the "right" half, the other being dual. Observe that $I + \mathcal{H}$ is a submonoid of $(S\,,\circ)$ (again by equation (5.1)) so, by Lemma 5.1, $I + \mathcal{H} = I \circ \mathcal{H}$ is the internal general product of $(I\,,\circ)$ with $(\mathcal{H}\,,\circ)$. The last claim follows by observing that, for $x \in I\,, h \in \mathcal{H}\,,$

$$h \circ x = x + h\widehat{x} = (x\overline{h\widehat{x}}) \circ (h\widehat{x})\,.$$

□

Corollary 5.5. *If I is a subring of $S\,,$ $(\mathcal{H}\,,+) \leq (S\,,+)\,,$ $I \cap \mathcal{H} = \{0\}\,,$ $(\mathcal{H}\,,\circ) \leq (\mathcal{G}(S)\,,\circ)\,,$ $\mathcal{H}$ absorbs elements of I by multiplication on the left [right] and I annihilates $\mathcal{H}$ by multiplication on the right [left], then*

$$I + \mathcal{H} \quad = \quad \mathcal{H} \circ I \quad [\,I \circ \mathcal{H}\,]\,,$$

$I+\mathcal{H}$ is the internal semidirect [reverse semidirect] product of $(\mathcal{H}\,,\circ)$ by $(I\,,\circ)$ and

$$I+\mathcal{H} \;\cong\; (\mathcal{H}\,,\circ) \rtimes_{\widehat{\lambda}_{I,\mathcal{H}}} (I\,,\circ) \quad [\,(I\,,\circ) \ltimes_{\widehat{\rho}_{I,\mathcal{H}}} (\mathcal{H}\,,\circ)\,]$$

Proof. This is immediate from Theorem 5.4, noting that, for $x \in I\,, h \in \mathcal{H}\,,$

$$x = \begin{cases} \overline{\widehat{x}h}x & \text{if } (\widehat{x}h)x = 0 \\ x\overline{h\widehat{x}} & \text{if } x(h\widehat{x}) = 0\,. \end{cases}$$

□

In the applications that now follow, all of the submonoids are subgroups, and the conclusions of Corollaries 5.4 and 5.5 carry the same information (in accordance with (1.2)). In [8] the authors consider monoids which are not groups (see Example 2.4 above) and Theorems 5.2 and 5.4 and their corollaries play markedly different roles.

6 Matrices over a radical ring

Let S be a radical ring and $n \geq 1$. Then S is an abelian group under addition and a (not necessarily abelian) group under circle. (Even when both groups are abelian they need not be isomorphic; for example $(2\mathbb{Z}_8\,,+)$ is cyclic of order 4, whilst $(2\mathbb{Z}_8\,,\circ)$ is isomorphic to the Klein 4 group.) Then $M_n(S) = \mathcal{J}(M_n(S)) = \mathcal{G}(M_n(S))$ is a group under $\circ$ and has many possible decompositions. In this section we give a decomposition involving rows (which dualizes to columns) and then a contrasting decomposition involving both rows and columns leading to a recursive formula. In both cases $(M_n(S)\,,\circ)$ is built from $(S\,,+)$ and $(S\,,\circ)$ using direct, semidirect and general products. All of the anti-representations involved in the use of semidirect products are described explicitly using the theory and notation of Section 5. The $\lhd\,,\rhd$ mappings involved in forming general products, whilst not explicitly described here, can be gleaned from results in Section 5.

Put $M = M_n(S)$ and for $i, j \in \{1, \ldots, n\}$,

$$\begin{aligned}
X_{ij} &= \{\alpha \in M \mid \alpha_{kl} = 0 \text{ if } k \neq i \text{ or } l \neq j\}, \\
R_i &= X_{i1} + \ldots + X_{in}, \\
\widetilde{R_i} &= X_{i1} + \ldots + X_{i,i-1} + X_{i,i+1} + \ldots + X_{in}, \\
C_i &= X_{1i} + \ldots + X_{ni}, \\
\widetilde{C_i} &= X_{1i} + \ldots + X_{i-1,i} + X_{i+1,i} + \ldots + X_{ni}, \\
T_i &= R_1 + \ldots + R_i, \\
M_i &= \{\alpha \in M \mid \alpha_{kl} = 0 \text{ if } k > i \text{ or } l > i\}.
\end{aligned}$$

All of these are subrings and hence circle subgroups of M. We develop our understanding of $(M, \circ)$ through the following sequence of steps.

(1) If $i \neq j$ then X_{ij} is both an ideal and a normal subgroup of R_i, and X_{ij} is a null ring (so circle coincides with addition) which annihilates elements of R_i, and X_{ii} in particular, by multiplication on the left. Clearly then, for each i,

$$\widetilde{R_i} = X_{i1} \circ \ldots \circ X_{i,i-1} \circ X_{i,i+1} \circ \ldots \circ X_{in}$$

and, for $j \neq i$,

$$X_{ij} \cap \Big(\sum_{\substack{k \neq j \\ k \neq i}} X_{ik}\Big) = \{0\},$$

yielding an internal direct product decomposition of $\widetilde{R_i}$, whence

$$(6.1) \qquad (\widetilde{R_i}, \circ) \cong (S, +)^{n-1}.$$

(2) For each i, $(X_{ii}, \circ) \cong (S, \circ)$ and X_{ii} is a left ideal of R_i. Further, $\widetilde{R_i}$ absorbs multiplication by elements of X_{ii} on the left and is annihilated by X_{ii} by multiplication on the right. Also $\widetilde{R_i} \cap X_{ii} = \{0\}$. Hence, by

Corollary 5.3 or 5.5 and isomorphism (6.1)

$$\begin{aligned} R_i &= \widetilde{R_i} + X_{ii} = \widetilde{R_i} \circ X_{ii} \\ &\cong \widetilde{R_i} \rtimes_{\hat{\lambda}_{X_{ii},\widetilde{R_i}}} X_{ii} \\ &\cong (S\,,+)^{n-1} \rtimes (S\,,\circ)\,. \end{aligned} \tag{6.2}$$

Observe also that, for $j \neq i$, X_{ij} is normalized by R_i, and X_{ii} in particular, so the factors may be placed in any order, yielding, for example,

$$R_i = \widetilde{R_i} \circ X_{ii} = X_{i1} \circ \ldots \circ X_{in} \tag{6.3}$$

(3) Dual formulae and the use of equation (1.2) yield, for each i,

$$\begin{aligned} C_i &= \widetilde{C_i} + X_{ii} = \widetilde{C_i} \circ X_{ii} = C_{1i} \circ \ldots \circ C_{ni} \\ &\cong \widetilde{C_i} \rtimes_{\hat{\rho}'_{X_{ii},\widetilde{C_i}}} X_{ii} \\ &\cong (S\,,+)^{n-1} \rtimes (S\,,\circ)\,. \end{aligned}$$

(4) For each $i < n$, T_i and R_{i+1} are right ideals of M, $T_{i+1} = T_i + R_{i+1}$ and $T_i \cap R_{i+1} = \{0\}$, so that, by Theorem 5.4, T_{i+1} is the general product

$$T_{i+1} = T_i \circ R_{i+1} \cong (T_i\,,\circ) \circledast (R_{i+1}\,,\circ)\,. \tag{6.4}$$

(and the general product mappings, though not explicitly described here, may also be deduced from Theorem 5.4). For each i, we have, by a simple induction,

$$T_i = R_1 \circ \ldots \circ R_i \cong (\ldots(R_1 \circledast R_2) \circledast \ldots) \circledast R_i\,.$$

Steps (1) to (4) culminate, by equation (6.3) and its dual, in the following result.

Theorem 6.1. *If S is a radical ring and $n \geq 1$ then*

$$\begin{aligned} M_n(S) &= R_1 \circ \ldots \circ R_n \;=\; C_1 \circ \ldots \circ C_n \\ &= (X_{11} \circ \ldots \circ X_{1n}) \circ \ldots \circ (X_{n1} \circ \ldots \circ X_{nn}) \\ &= (X_{11} \circ \ldots \circ X_{n1}) \circ \ldots \circ (X_{1n} \circ \ldots \circ X_{nn}) \\ &\cong (\ldots (R_1 \circledast R_2) \circledast \ldots) \circledast R_n \;\cong\; (\ldots (C_1 \circledast C_2) \circledast \ldots) \circledast C_n \,. \end{aligned}$$

We describe an alternative recursive decomposition of $M = M_n$, which uses a mixture of general and semidirect products. By equation (6.4) we have the internal general product

$$M \;=\; T_n \;=\; T_{n-1} \circ R_n \,. \tag{6.5}$$

But M_{n-1} and $\widetilde{C_n}$ are left ideals of T_{n-1}, M_{n-1} annihilates $\widetilde{C_n}$ by multiplication on the right, $T_{n-1} = M_{n-1} + \widetilde{C_n}$ and $M_{n-1} \cap \widetilde{C_n} = \{0\}$, so, by Corollary 5.3 or 5.5 and the dual of isomorphism (6.1),

$$\begin{aligned} T_{n-1} &= \widetilde{C_n} \circ M_{n-1} \\ &\cong (\widetilde{C_n}\,, \circ) \rtimes_{\hat{\lambda}_{M_{n-1},\widetilde{C_n}}} (M_{n-1}\,, \circ) \\ &\cong (S\,, +)^{n-1} \rtimes (M_{n-1}\,, \circ)\,. \end{aligned}$$

Thus by equation (6.5) and isomorphism (6.2) we get the following recursive formula.

Theorem 6.2. *If S is a radical ring and $n \geq 1$ then*

$$(M_n(S)\,, \circ) \cong \big((S\,, +)^{n-1} \rtimes (M_{n-1}(S)\,, \circ)\big) \circledast \big((S\,, +)^{n-1} \rtimes (S\,, \circ)\big)\,.$$

7 A group presentation

Let S be any radical ring and n any positive integer. In this section we first find a presentation for $(M_n(S), \circ)$ in terms of the addition and circle multiplication tables of S. We then modify it to yield a presentation in terms of presentations and sets of normal forms for the groups $(S, +)$ and $(S, \circ)$. In Section 8 we illustrate how this result can be used to find explicit, concise presentations in important special cases.

Form the alphabet

$$\Sigma_S = \{ x_{ij} \mid x \in S, \; i, j \in \{1, \dots n\} \} .$$

Let $\mathcal{R}_S$ be the collection of relations of the following types:

(1) $(\forall i, j)(\forall x, y \in S)$

$$x_{ij} y_{ij} = \begin{cases} (x + y)_{ij} & \text{if } j \neq i, \\ (x \circ y)_{ij} & \text{if } j = i . \end{cases}$$

(2) $(\forall i \neq l, j \neq k)(\forall x, y \in S) \quad [x_{ij}, y_{kl}] = 1 .$

(3) $(\forall i \neq j \neq k \neq i)(\forall x, y \in S)$

$$[x_{ij}, y_{jk}] = (-xy)_{ik} .$$

(4) $(\forall i \neq j)(\forall x, y \in S)$

$$[x_{ii}, y_{ij}] = (x'y)_{ij} .$$

(5) $(\forall i \neq j)(\forall x, y \in S)$

$$[x_{ij}, y_{jj}] = (-xy)_{ij} .$$

(6) $(\forall i > j)(\forall x, y \in S)$

$$x_{ij} y_{ji} = \big((-yx)'_{jj} \big) \, y_{ji} x_{ij} (-xy)_{ii} .$$

The reader might observe that (3) and (5) could be amalgamated. However it is convenient to keep them separate for the purposes of the proofs below.

Theorem 7.1. $(\, M_n(S)\, , \circ\,) \;\cong\; \langle\, \Sigma_S \,|\, \mathcal{R}_S \,\rangle$.

Proof. Put $G = \langle\, \Sigma_S \,|\, \mathcal{R}_S \,\rangle$. We identify elements of G with words over Σ_S without causing confusion. Observe that

$$\Sigma_S = \bigcup_{i\,,j} X_{ij}$$

where, for each $i\,,j$,

$$X_{ij} = \{\, x_{ij} \,|\, x \in S \,\}\,,$$

so that, by (1) of $\mathcal{R}_S$, $X_{ij} \;=\; \langle\, X_{ij} \,\rangle$ (where the angular brackets may be interpreted both as subgroup and submonoid generation). By rearranging the commutators it is easy to see that the relations in $\mathcal{R}_S$ imply that the hypotheses of Lemma 3.5 are satisfied with G in place of M, so

$$G = \prod_{i=1}^{n}\prod_{j=1}^{n} X_{ij}\,. \tag{7.1}$$

For each $x \in S$ and $i\,,j$, let ${x_{ij}}^{\dagger}$ denote the $n \times n$ matrix consisting of zeros everywhere except for x in the $(\,i\,,j\,)$th place. It is routine to check that all of the relations of $\mathcal{R}_S$ become equations in $M_n(S)$ when each x_{ij} is replaced by ${x_{ij}}^{\dagger}$. As an example of the nature of the calculations involved, the following suffices to verify (6):

$$\begin{array}{cc} & \begin{array}{cc} j & i \end{array} \\ \begin{array}{c} j \\ i \end{array} & \begin{pmatrix} -(\,yx\,)' & 0 \\ 0 & 0 \end{pmatrix} \end{array} \circ \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ 0 & -xy \end{pmatrix}$$

$$= \begin{pmatrix} (-yx)' & y - (yx)'y \\ 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ x & -xy \end{pmatrix}$$
$$= \begin{pmatrix} (-yx)' - (y - (yx)'y)x & y - (yx)'y + (y - (yx)'y)xy \\ x & -xy \end{pmatrix}$$
$$= \begin{pmatrix} 0 & y \\ x & -xy \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}$$

Thus the mapping $x_{ij} \mapsto {x_{ij}}^\dagger \quad (x \in S, i, j \in \{1, \ldots, n\})$ induces a well-defined homomorphism $\varphi : G \longrightarrow M_n(S)$. Now put, for i, j,

$$ {X_{ij}}^\dagger = \{ {x_{ij}}^\dagger \mid x \in S \} $$

and observe, by Theorem 6.1, that

$$M_n(S) \;=\; ({X_{11}}^\dagger \circ \ldots \circ {X_{1n}}^\dagger) \circ \ldots \circ ({X_{n1}}^\dagger \circ \ldots \circ {X_{nn}}^\dagger) \;=\; \langle \bigcup_{i,j} {X_{ij}}^\dagger \rangle_\circ ,$$

which proves φ is onto. To complete the proof it suffices to show φ is one-one, and for that it is sufficient, by equation (7.1), to check the induced map, also denoted by φ, on the *set of words*

$$W \;=\; \prod_{i=1}^{n} \prod_{j=1}^{n} X_{ij}$$

is one-one.

Let $u, v \in W$ and suppose $u\varphi = v\varphi$. There are elements $x(i,j), y(i,j) \in S$ for $i, j \in \{1, \ldots, n\}$ such that

$$u \;=\; \prod_{i=1}^{n} \prod_{j=1}^{n} (x(i,j))_{ij} \quad \text{and} \quad v \;=\; \prod_{i=1}^{n} \prod_{j=1}^{n} (y(i,j))_{ij} .$$

For each $k \in \{1, \ldots, n\}$, put

$$r_k \;=\; \prod_{j=1}^{n} (x(k,j))_{kj} \quad \text{and} \quad s_k \;=\; \prod_{j=1}^{k} (y(k,j))_{kj} ,$$

so $u = r_1 \dots r_n$ and $v = s_1 \dots s_n$. We will prove

$$(7.2) \qquad (\forall k = 1, \dots, n) \quad r_k\varphi \;=\; s_k\varphi\,.$$

Suppose that $r_l\varphi = s_l\varphi$ for all $l > k$ (which is vacuously true if $k = n$). Then, since $M_n(S)$ is radical,

$$\begin{aligned}
(r_1 \dots r_k)\varphi &= (r_1 \dots r_k)\varphi \circ (r_{k+1} \dots r_n)\varphi \circ ((r_{k+1} \dots r_n)\varphi)' \\
&= (r_1 \dots r_n)\varphi \circ (r_n\varphi)' \circ \dots \circ (r_{k+1}\varphi)' \\
&= (s_1 \dots s_n)\varphi \circ (s_n\varphi)' \circ \dots \circ (s_{k+1}\varphi)' \\
&= (s_1 \dots s_k)\varphi\,.
\end{aligned}$$

But, by a simple matrix calculation, we see that the kth rows of $(r_1 \dots r_k)\varphi$ and $(s_1 \dots s_k)\varphi$ are $r_k\varphi$ and $s_k\varphi$ respectively, whence $r_k\varphi = s_k\varphi$, and equation (7.2) follows by induction.

By another simple matrix calculation, $r_k\varphi$ and $s_k\varphi$ are matrices with zeros everywhere except for the kth rows which are

$$\big(\, x(k,1) \quad \dots \quad x(k,k) \quad \widehat{z}\,x(k,k+1) \quad \dots \quad \widehat{z}\,x(k,n) \,\big)$$

and

$$\big(\, y(k,1) \quad \dots \quad y(k,k) \quad \widehat{w}\,y(k,k+1) \quad \dots \quad \widehat{w}\,y(k,n) \,\big)$$

respectively, where $z = x(k,k)$ and $w = y(k,k)$. But $r_k\varphi = s_k\varphi$, so, for $j = 1, \dots, k$, $\quad x(k,j) = y(k,j)$, and in particular $z = w$. Hence, also, for $j = k+1, \dots, n$,

$$x(k,j) \;=\; \overline{z}\,\widehat{z}\,x(k,j) \;=\; \overline{z}\,\widehat{z}\,y(k,j) \;=\; y(k,j)\,.$$

This proves $u = v$, proving φ is one-one, completing the proof of Theorem 7.1. $\square$

The reader might note that if S is finite then it is not necessary to argue that ϕ is one-one on W, since this follows immediately from the fact that ϕ is onto and, by Lemma 3.5, $|G| \le \Pi_{i=1}^{n}\Pi_{j=1}^{n}\,|X_{ij}|$.

The presentation of Theorem 7.1 uses the entire addition and circle multiplication tables of S, leading to superfluity in practice. For example, the generators 0_{ij} may be deleted and replaced by 1 throughout, for all $i\,,j$. In Theorem 7.2 below we give a presentation for $(\,M_n(S)\,,\circ\,)$ in terms of presentations for $(\,S\,,+\,)$ and $(\,S\,,\circ\,)$. 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, which we may refer to as *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

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

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

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

Theorem 7.2. $(\, M_n(S) \,, \circ\,) \cong \langle\, \Gamma \,|\, \mathcal{R} \,\rangle$.

Proof. Put $H = \langle\, \Gamma \,|\, \mathcal{R} \,\rangle$. By Theorem 7.1 it is sufficient to prove $H \cong G = \langle\, \Sigma_S \,|\, \mathcal{R}_S \,\rangle$. We do this by applying Tietze transformations to G .

Step 1: Add to Σ_S the alphabet Γ, which we may assume to be disjoint from Σ_S, and to $\mathcal{R}_S$ relations of the form

$$\sigma_{ij} = s_{ij}$$

where $\sigma \in \begin{cases} \Gamma^{(+)} & \text{if } i \neq j \\ \Gamma^{(\circ)} & \text{if } i = j \end{cases}$ and $s = \begin{cases} \sigma\varphi & \text{if } i \neq j \\ \sigma\psi & \text{if } i = j\,. \end{cases}$

Step 2: Add relations

$$x_{ij} = w_{ij}$$

where $x \in S$ and $w = \begin{cases} x\varphi^{-1} & \text{if } i \neq j \\ x\psi^{-1} & \text{if } i = j\,. \end{cases}$ This is justified for $i \neq j$ ($i = j$ being similar) as follows:

Suppose $x \in S$ and $x\varphi^{-1} = w = \sigma^{(1)} \ldots \sigma^{(t)}$ for some $\sigma^{(1)}, \ldots, \sigma^{(t)} \in \Gamma^{(+)}$. Then, in S,

$$x \ = \ \sigma^{(1)}\varphi + \ldots + \sigma^{(t)}\varphi$$

so, by type (1) relations in G, followed by Step 1 relations,

$$x_{ij} \ = \ (\,\sigma^{(1)}\varphi\,)_{ij} \ldots (\,\sigma^{(t)}\varphi\,)_{ij} \ = \ {\sigma^{(1)}}_{ij} \ldots {\sigma^{(t)}}_{ij} = w_{ij}\,.$$

Step 3: Add all relations in

$$\bigcup_{i \neq j} \mathcal{R}_{ij}^{(+)} \cup \bigcup_{i} \mathcal{R}_{i}^{(\circ)}\,.$$

This is justified for $\mathcal{R}^{(+)}$ ($\mathcal{R}^{(\circ)}$ is similar) as follows:

Suppose $v = w$ is a relation of $\mathcal{R}^{(+)}$. Write $v = \sigma^{(1)} \ldots \sigma^{(t)}$, $w = \tau^{(1)} \ldots \tau^{(u)}$ where $\sigma^{(1)}, \ldots, \sigma^{(t)}$, $\tau^{(1)}, \ldots, \tau^{(u)} \in \Gamma^{(+)}$.

Then, in S,

$$\sigma^{(1)}\varphi + \ldots + \sigma^{(t)}\varphi = \tau^{(1)}\varphi + \ldots + \tau^{(u)}\varphi\,,$$

so, in G, using type (1) relations,

$$\begin{aligned}(\sigma^{(1)}\varphi)_{ij}\ \dots\ (\sigma^{(t)}\varphi)_{ij} &= (\sigma^{(1)}\varphi + \dots + \sigma^{(t)}\varphi)_{ij}\\ &= (\tau^{(1)}\varphi + \dots + \tau^{(u)}\varphi)_{ij}\\ &= (\tau^{(1)}\varphi)_{ij} \dots (\tau^{(u)}\varphi)_{ij}\,,\end{aligned}$$

so, by Step 1 relations, we deduce that

$$\begin{aligned} v_{ij} &= \sigma_{ij}^{(1)} \dots \sigma_{ij}^{(t)} = (\sigma^{(1)}\varphi)_{ij} \dots (\sigma^{(t)}\varphi)_{ij}\\ &= (\tau^{(1)}\varphi)_{ij} \dots (\tau^{(t)}\varphi)_{ij} = \tau_{ij}^{(1)} \dots \tau_{ij}^{(u)} = w_{ij}\,.\end{aligned}$$

Step 4: Remove all of G's type (1) relations. This is justified for $i \neq j$ ($i = j$ being similar) as follows:

Suppose $x, y \in S$. Then $x + y \in S$ and, in $\langle\, \Gamma^{(+)} \mid \mathcal{R}^{+} \,\rangle$,

$$(x\varphi^{-1})(y\varphi^{-1}) = (x+y)\varphi^{-1}\,,$$

so, as a consequence of relations in $\mathcal{R}_{ij}^{(+)}$, we have

$$(x\varphi^{-1})_{ij}(y\varphi^{-1})_{ij} = ((x+y)\varphi^{-1})_{ij}\,,$$

from which we derive, using relations from Step 2, the relation

$$x_{ij}y_{ij} = (x+y)_{ij}\,.$$

Step 5: Remove all letters from Σ_S, replacing any letter s_{ij} ($s \in S, i, j \in \{1, \dots, n\}$) which appears in any relation by the word $(s\varphi^{-1})_{ij}$ if $i \neq j$, and $(s\psi^{-1})_{ij}$ if $i = j$. The Step 1, 2 relations now become equality of the same letter, word respectively, so are redundant and may be deleted.

The effect of Steps 1 to 5 is to replace Σ_S by Γ, type (1) relations of $\mathcal{R}_S$ by type (1) relations of $\mathcal{R}$ and each relation of types (2) to (6) of $\mathcal{R}_S$ by a relation in which any letter s_{ij} has been replaced by the word $(s\varphi^{-1})_{ij}$ or $(s\psi^{-1})_{ij}$ if $i \neq j$ or $i = j$ respectively.

Step 6: Consider $i \neq l\,, j \neq k$. The transformed type (2) relations have the form

$$[\,v_{ij}\,, w_{kl}\,] = 1$$

where $v \in \begin{cases} W^{(+)} & \text{if } i \neq j \\ W^{(\circ)} & \text{if } i = j \end{cases}$, $w \in \begin{cases} W^{(+)} & \text{if } k \neq l \\ W^{(\circ)} & \text{if } k = l\,, \end{cases}$.

Delete all such relations where $v \notin \begin{cases} \Gamma^{(+)} & \text{if } i \neq j \\ \Gamma^{(\circ)} & \text{if } i = j \end{cases}$

or $w \notin \begin{cases} \Gamma^{(+)} & \text{if } k \neq l \\ \Gamma^{(\circ)} & \text{if } k = l \end{cases}$, since these are implied by the remaining

relations of the form $[\,\sigma_{ij}\,, \tau_{kl}\,] = 1$ where $\sigma \in \begin{cases} \Gamma^{(+)} & \text{if } i \neq j \\ \Gamma^{(\circ)} & \text{if } i = j \end{cases}$ and

$\tau \in \begin{cases} \Gamma^{(+)} & \text{if } k \neq l \\ \Gamma^{(\circ)} & \text{if } k = l\,. \end{cases}$

The relations that remain are precisely those catalogued by $\mathcal{R}$, and Theorem 7.2 is proved. $\square$

8 Examples

We apply the results of the previous section section to determine $(\,M_n(\,S\,)\,, \circ\,)$ when $S = p\mathbb{Z}_{p^t}$, the radical of the ring $\mathbb{Z}_{p^t}$, where p is a prime and $t \geq 3$ (the cases $t = 1\,, 2$ yielding trivial, elementary abelian groups respectively). The cases p odd and even are treated separately because $(\,p\mathbb{Z}_{p^t}\,, \circ\,)$ is cyclic, in fact isomorphic to $(\,p\mathbb{Z}_{p^t}\,, +\,)$, when p is odd, but noncyclic when $p = 2$.

Theorem 8.1. *Let p be odd. Then*

$$(\,M_n(\,p\mathbb{Z}_{p^t}\,)\,, \circ\,) \;\;\cong\;\; \langle\, \Gamma \,|\, \mathcal{R} \,\rangle$$

over the alphabet

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

and where $\mathcal{R}$ comprises relations of the following types

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

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

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

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

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

(6) $(\forall i > j)(\forall m = 0 , \dots , p^{t-3} - 1)$

$$a_{ij}^{1-(-mp^2)'} a_{ji} = a_{jj}^{-\alpha} a_{ji} a_{ij}^{1-(-mp^2)'} a_{ii}^{\alpha}$$

where α is the least positive integer such that

$$(1 - p)^{\alpha} = 1 + (1 - (-mp^2)')p^2$$

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

Proof. Observe that, for $S = p\mathbb{Z}_{p^t}$,

$$(S , +) \;=\; \langle p \rangle_+ \;\cong\; \langle a \mid a^{p^{t-1}} = 1 \rangle \;\cong\; \langle p \rangle_\circ \;=\; (S , \circ) .$$

In the framework leading up to Theorem 7.2 we take

$$W^{(+)} \;=\; W^{(\circ)} \;=\; \{ a^m \mid m \in \{ 0 , \dots , p^{t-1} - 1 \} \}$$

and choose bijections

$$\varphi : W^{(+)} \longrightarrow (S , +) , \quad a^m \mapsto mp$$

and

$$\psi \,:\, W^{(\circ)} \longrightarrow (\,S\,,\circ\,)\,, \quad a^m \mapsto p^{\circ m}\,.$$

Then relations of type $(\,1\,)$, $(\,2\,)$ are identical in Theorems 7.2 and 8.1.

Consider relations of type $(\,3\,)$ in Theorem 7.2. Suppose $i \neq j \neq k \neq i$. The relations have the form

$$[\,a_{ij}^{\;\lambda}\,, a_{jk}^{\;\mu}\,] = a_{ik}^{-\lambda\mu p}$$

for $\lambda\,, \mu \in \{\,0\,, \ldots\,, p^{t-1}\,\}$. The cases $\lambda = 0$ or $\mu = 0$ are redundant, and the cases $\lambda > 0$ and $\mu > 0$ follow from the relation $[\,a_{ij}\,, a_{jk}\,] = a_{ik}^{\;-p}$, by Lemma 3.1, so may be deleted, leaving type $(\,3\,)$ relations of Theorem 8.1.

Suppose $i \neq j$. Relations of type $(\,4\,)$ of Theorem 7.2 have the form

$$[\,a_{ii}^{\;\lambda}\,, a_{ij}^{\;\mu}\,] = (\,(\,(\,p^{\circ\lambda}\,)'(\,\mu p\,)\,)\varphi^{-1}\,)_{ij} = a_{ij}^{(\,1-(\,1-p'\,)^{\lambda}\,)\mu}$$

and of type $(\,5\,)$ the form

$$[\,a_{ij}^{\;\lambda}\,, a_{jj}^{\;\mu}\,] = (\,(\,-(\,\lambda p\,)(\,p^{\circ\mu}\,)\,)\varphi^{-1}\,)_{ij} = a_{ij}^{-(\,1-(\,1-p\,)^{\mu}\,)\lambda}\,.$$

The cases $\lambda = 0$ or $\mu = 0$ are redundant, and the cases $\lambda > 0$ and $\mu > 0$ follow from the relations

$$[\,a_{ii}\,, a_{ij}\,] \;=\; a_{ij}^{\,p'} \qquad \text{and} \qquad [\,a_{ij}\,, a_{jj}\,] \;=\; a_{ij}^{-p}\,,$$

by Lemma 3.2, noting that the latter is equivalent to

$$[\,a_{jj}\,, a_{ij}\,] = [\,a_{ij}\,, a_{jj}\,]^{-1} = a_{ij}^{\,p}\,,$$

whilst the type $(\,5\,)$ relation is equivalent to

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

Deleting all but the cases $\lambda = \mu = 1$ yields type $(\,4\,)$ and $(\,5\,)$ relations of Theorem 8.1.

Suppose $i > j$. Relations of type (6) of Theorem 7.2 have the form

$$\begin{aligned} a_{ij}^{\lambda} a_{ji}^{\mu} &= ((-(\mu p)(\lambda p))'\psi^{-1})_{jj} a_{ji}^{\mu} a_{ij}^{\lambda} ((-(\lambda p)(\mu p))\psi^{-1})_{ii} \\ &= a_{jj}^{-\nu} a_{ji}^{\mu} a_{ij}^{\lambda} a_{ii}^{\nu} \end{aligned}$$

where ν is the least nonnegative integer such that

$$(1-p)^{\nu} = 1 + \lambda\mu p^2 ,$$

for $\lambda, \mu \geq 0$. We delete all such relations except for the cases $\mu = 1, \lambda = 1 - (-mp^2)'$ for $m = 0, \ldots, p^{t-3} - 1$, since those to be deleted are either redundant (when $\lambda = 0$ or $\mu = 0$), or follow from the ones to be retained and the relations $[a_{jj}, a_{ii}] = 1$ (type 2) and

$$a_{ij}^{a_{jj}} = a_{ij}^{1-p}, \quad a_{ij}^{a_{ii}} = a_{ij}^{1-p'}, \quad a_{ji}^{a_{jj}} = a_{ji}^{1-p'}, \quad a_{ji}^{a_{ii}} = a_{ji}^{1-p}$$

(the result of rearranging type (4) and (5) relations of Theorem 8.1) by Lemma 3.4. This completes the proof of Theorem 8.1. □

This presentation simplifies further when $t = 3$.

Theorem 8.2. *Let p be odd. Then*

$$(M_n(p\mathbb{Z}_{p^3}), \circ) \;\cong\; \langle \Gamma \mid \mathcal{R} \rangle$$

over the alphabet

$$\Gamma = \{ a_{ij} \mid i, j \in \{1, \ldots, n\} \}$$

where $\mathcal{R}$ consists of relations

(1) $(\forall i, j)\quad a_{ij}^{p^2} = 1$;

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

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

(4) $(\forall i > j)\quad [a_{ij}, a_{ji}] = a_{jj}^{p} a_{ii}^{-p}$.

Proof. Relations (1), (2) are the same as those of Theorem 8.1. Note that in $\mathbb{Z}_{p^3}$, $p' = -p - p^2$, so that relations (4) of Theorem 8.1 become

$$[\, a_{ii} \, , a_{ij} \,] = a_{ij}^{-p-p^2} = a_{ij}^{-p} \, ,$$

by (1). This can be amalgamated with (3) and (5) of Theorem 8.1 to yield (3) of Theorem 8.2. There is only one relation in (6) of Theorem 8.1 when $t = 3$:

$$a_{ij} a_{ji} = a_{jj}^{-(\, p^2 - p \,)} a_{ji} a_{ii} a_{ii}^{p^2 - p}$$

since $(\, 1 - p \,)^{p^2 - p} = 1 + p^2$ in $\mathbb{Z}_{p^3}$, which becomes, by (1),

$$a_{ij} a_{ji} = a_{jj}^{p} a_{ji} a_{ii} a_{ii}^{-p} \, .$$

Tracing through the isomorphism with $M_n(\, \mathbb{Z}_{p^3} \,)$ (induced by the map $a_{kl} \mapsto a_{kl}^{\dagger}$ in the notation of Theorem 7.1) we see that a_{jj}^{p} and a_{ii}^{-p} are central (since they correspond with matrices with one nonzero entry equal to p^2 and $-p^2$ respectively), so the above relation, in conjunction with commutativity relations, is equivalent to

$$[\, a_{ij} \, , a_{ji} \,] = a_{jj}^{p} a_{ii}^{-p} \, .$$

$\square$

Example 8.3. Further simplification takes place when $n = 2$ in Theorem 8.2: one relation suffices in each of (2) and (4), and relations of type (3) may be rearranged to give four conjugation relations, yielding the following presentation for $(\, M_2(\, p\mathbb{Z}_{p^3} \,) \, , \circ \,)$, for any odd prime p :

$$\begin{aligned} \langle\, a_{11} \, , a_{12} \, , a_{21} \, , a_{22} \;\mid\; a_{ij}^{p^2} = 1 \; (\forall i \, , j \,) \, , \, [\, a_{11} \, , a_{22} \,] = 1 \, , \; [\, a_{21} \, , a_{12} \,] = a_{11}^{p} a_{22}^{-p} \, , \\ a_{ij}^{a_{ii}} = a_{ij}^{1+p} \, , \; a_{ij}^{a_{jj}} = a_{ij}^{1-p} \; (\forall i \neq j \,) \,\rangle \end{aligned}$$

which the reader will recognize as being the presentation of the general product $G \circledast G$ of Example 2.2 , after renaming generators.

Finally we consider the case when $p = 2$.

Theorem 8.4.

$$(M_n(2\mathbb{Z}_{2^t}), \circ) \cong \langle \Gamma \,|\, \mathcal{R} \rangle$$

over the alphabet

$$\Gamma = \{ a_{ij} \,|\, i, j \in \{1, \ldots, n\}, i \neq j \} \cup \{ b_i, c_i \,|\, i \in \{1, \ldots, n\} \}$$

where $\mathcal{R}$ comprises relations

(1) $(\forall i \neq j)$ $a_{ij}^{2^{t-1}} = 1$;

(1)$'$ $(\forall i)$ $b_i^{2^{t-2}} = c_i^{2} = 1$, $[b_i, c_i] = 1$;

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

(2)$'$ $(\forall i \neq j)$ $[b_i, b_j] = [b_i, c_j] = [c_i, c_j] = 1$;

(2)$''$ $(\forall k \neq i \neq l \neq k)$ $[b_i, a_{kl}] = [c_i, a_{kl}] = 1$;

(3) $(\forall i \neq j \neq k \neq i)$ $[a_{ij}, a_{jk}] = a_{ik}^{-2}$;

(4) $(\forall i \neq j)$ $[b_i, a_{ij}] = a_{ij}^{4'}$, $[c_i, a_{ij}] = a_{ij}^{2}$;

(5) $(\forall i \neq j)$ $[a_{ij}, b_j] = a_{ij}^{-4}$, $[a_{ij}, c_j] = a_{ij}^{-2}$;

(6) $(\forall i > j)(\forall m = 0, \ldots, 2^{t-3} - 1)$

$$a_{ij}^{1-(-4m)'} a_{ji} = b_j^{-\alpha} a_{ji} a_{ij}^{1-(-4m)'} b_i^{\alpha}$$

where α is the least positive integer such that

$$(-3)^{\alpha} = 1 + 4(1 - (-4m)')$$

in $\mathbb{Z}_{2^t}$ (which exists because all multiples of 4 comprise the cyclic subgroup of $(2\mathbb{Z}_{2^t}, \circ)$ generated by 4).

Proof. Observe that, for $S = 2\mathbb{Z}_{2^t}$,

$$(S , +) \;=\; \langle 2 \rangle_+ \;\cong\; \langle a \,|\, a^{2^{t-1}} = 1 \rangle \; ;$$

$$(S , \circ) \;=\; \langle 2 , 4 \rangle_\circ \;\cong\; \langle b , c \,|\, b^{2^{t-2}} = c^2 = 1 , [b , c] = 1 \rangle \; .$$

In the framework leading up to Theorem 7.2 we take

$$W^{(+)} \;=\; \{ a^\lambda \,|\, \lambda \in \{ 0 , \ldots , 2^{t-1} - 1 \} \} \, ,$$

$$W^{(\circ)} \;=\; \{ b^\lambda c^\mu \,|\, \lambda \in \{ 0 , \ldots , 2^{t-2} - 1 \} , \mu \in \{ 0 , 1 \} \} \, ,$$

$$\varphi \,:\, W^{(+)} \longrightarrow S \, , \quad a^\lambda \mapsto 2\lambda \, ,$$

$$\psi \,:\, W^{(\circ)} \longrightarrow S \, , \quad b^\lambda c^\mu \mapsto 2^{\circ\mu} \circ 4^{\circ\lambda} \, .$$

We apply Theorem 7.2 and also, to decongest notation slightly, identify b_{ii}, c_{ii} with new letters b_i, c_i respectively. Then relations of types (1), (1)$'$, (2), (2)$'$ and (2)$''$ here are identical with relations of types (1) and (2) which feature in Theorem 7.2. The reduction of relations of types (3) and (6) is identical to that in the proof of Theorem 8.1, relying on Lemma 3.1 and Lemma 3.4 (with $q = 4$) respectively.

Suppose $i \neq j$. Relations of type (4) of Theorem 7.2 have the form

$$[b_i^\lambda, a_{ij}^\mu] \;=\; (((4^{\circ\lambda})'(2\mu))\phi^{-1})_{ij} \;=\; a_{ij}^{(1-(1-4')^\lambda)\mu}$$

or

$$[b_i^\lambda c_i, a_{ij}^\mu] \;=\; (((2 \circ 4^{\circ\lambda})'(2\mu))\phi^{-1})_{ij} \;=\; a_{ij}^{(1+(1-4')^\lambda)\mu} \, ,$$

and of type (5) the form

$$[a_{ij}^{\lambda}, b_j^{\mu}] \;=\; ((-(2\lambda)(4^{\circ\mu})\phi^{-1})_{ij} \;=\; a_{ij}^{-(1-(-3)^{\mu})\lambda}$$

or

$$[a_{ij}^{\lambda}, b_j^{\mu}c_j] \;=\; ((-(2\lambda)(2\circ 4^{\circ\mu})\phi^{-1})_{ij} \;=\; a_{ij}^{-(1+(-3)^{\mu})\lambda} \;.$$

The nonredundant cases follow from the relations

$$[b_i, a_{ij}] \;=\; a_{ij}^{4'} \;, \quad [c_i, a_{ij}] \;=\; a_{ij}^{2} \;, \quad [b_i, c_i] = 1 \;,$$

$$[a_{ij}, b_j] \;=\; a_{ij}^{-4} \;, \quad [a_{ij}, c_j] \;=\; a_{ij}^{-2} \;, \quad [b_j, c_j] = 1 \;,$$

by Lemmas 3.2 and 3.3. Deleting all but the cases $\lambda = \mu = 1$ yields type (4) and (5) relations of Theorem 8.4, and the proof is complete. $\square$

Again, the presentation simplifies when $t = 3$.

Theorem 8.5.

$$(\, M_n(\, 2\mathbb{Z}_8\,)\,, \circ\,) \;\cong\; \langle\, \Gamma \,|\, \mathcal{R}\,\rangle$$

over the alphabet

$$\Gamma = \{\, a_{ij} \,|\, i\,, j \in \{\,1\,, \ldots\,, n\,\}\,, i \neq j\,\} \cup \{\, b_i\,, c_i \,|\, i \in \{\,1\,, \ldots\,, n\,\}\,\}$$

where $\mathcal{R}$ comprises relations

$(\,1\,)$ $\quad (\forall i\,, j \neq i\,)$ $\quad a_{ij}^{\,4} = b_i^{\,2} = c_i^{\,2} = 1\,;$

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

$(\,3\,)$ $\quad (\forall i\,, j \neq k \neq l \neq j\,)$ $\quad [\, b_i\,, c_j\,] = [\, b_k\,, b_l\,] = [\, b_i\,, a_{kl}\,]$
$\qquad = [\, c_k\,, c_l\,] = [\, c_j\,, a_{kl}\,] = 1\,;$

(4) $(\forall i \neq j \neq k \neq i)$ $[\,a_{ij}\,,a_{jk}\,] = [\,c_i\,,a_{ik}\,] = [\,a_{ik}\,,c_k\,] = a_{ik}^{\;2}\,;$

(5) $(\forall i > j)$ $[\,a_{ij}\,,a_{ji}\,] = b_j b_i\,.$

Proof. This follows by making economies to relations appearing in Theorem 8.4, noting that $4' = 4$ in $\mathbb{Z}_8$, exploiting relation (1), and rearranging (6) into a commutator relation, noting that b_i commutes with a_{ij} and a_{ji} for $i \neq j$ by (4) and (5). ☐

Example 8.6. Yet further simplification takes place when $n = 2$ in Theorem 8.5, yielding the following presentation for $(\,M_2(\,2\mathbb{Z}_8\,)\,,\circ\,)$:

$$\langle\, a_{12}\,,a_{21}\,,b_1\,,b_2\,,c_1\,,\,c_2 \mid a_{12}^{\;4} = a_{21}^{\;4} = b_i^{\;2} = c_i^{\;2} = 1\,,\; a_{12}^{\;c_i} = a_{12}^{-1}\,,\; a_{21}^{\;c_i} = a_{21}^{-1}\,, \\ [\,b_i\,,\,x\,] = [\,c_1\,,c_2\,] = 1\,,\; [\,a_{12}\,,a_{21}\,] = b_1 b_2 \quad (\forall i)(\forall x \neq b_i)\,\rangle$$

which the reader will recognize as the presentation of the general product $H \circledast H$ of Example 2.3, after renaming generators.

References

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

[2] Casadio, “Construzione dei gruppi come prodotto di sottogruppi permutabili,” *Rendiconti di Mat. Univ. Roma* **2** (1941), 348-360.

[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 and D. Easdown, "Complementation in the group of units of a ring," School of Mathematics and Statistics Research Report 99-18, University of Sydney, 1999.

[8] C. Coleman and D. Easdown, "Circle subgroups and submonoids of Munn rings," in preparation.

[9] J.M. Howie, *An Introduction to Semigroup Theory*, Academic Press, London, 1976.

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

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

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

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

[14] M. Kunze, "Zappa products," *Acta Math. Hungar.* **41** (1983), 225-239.

[15] M. Kunze, "Semidirect decompositions of semigroups, transformation semigroups, and automata," *Words, Languages and Combinatorics* (Kyoto, 1990), 309-325, World Sci. Publishing, River Edge, NJ, 1992.

[16] M. Kunze, "Bilateral semidirect products of transformation semigroups," *Semigroup Forum* **45** (1992), 166-182.

[17] M. Kunze, “Standard automata and semidirect products of transformation semigroups,” *Theoret. Comput. Sci.* **108** (1993), 151-171.

[18] T.G. Lavers, “The theory of vines,” *Comm. Algebra* **25** (1997), 1257-1284.

[19] T.G. Lavers, “Presentations of general products of monoids,” *J. Algebra* **204** (1998), 733-741.

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

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

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

[23] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory: Presentations in Terms of Generators and Relations*, Dover, New York 1976.

[24] W.D. Munn, “On semigroup algebra,” *Proc. Camb. Phil. Soc.* **51** (1955), 1-15.

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

[26] B.H. Neumann, “Decompositions of groups,” *J. London Math. Soc.* **10** (1935), 3-6.

[27] W.R. Nico, “On the regularity of semidirect products,” *J. Algebra* **80** (1983), 29-36.

[28] G.B. Preston, “Semidirect products of semigroups,” *Proc. Roy. Soc. Edinburgh Sect. A* **102** (1986), 91-102.

[29] G.B. Preston, "The semidirect product of an inverse semigroup and a group," *Bull Austral. Math. Soc.* **33** (1986), 261-172.

[30] G.B. Preston, "Semidirect products of semigroups," *Words, languages and combinatorics, II (Kyoto, 1992)*, 320-327, World Sci. Publishing, River Edge, NJ 1994.

[31] G.B. Preston, "Products of inverse semigroups," *Collect. Math.* **46** (1995), 151-157.

[32] L. Rédei, "Das schiefe Produkt in der Gruppentheorie," *Comm. Math. Helv.* **20** (1947), 225-264.

[33] L. Rédei, "Die Anwendung des schiefen Produktes in der Gruppentheorie," *J. Reine Angew. Math.* **188** (1950), 201-227.

[34] L. Rédei, "Eine Ergänzung zu meiner Arbeit über gruppentheoretische schiefe Produkte," *J. Reine Angew. Math.* **208** (1961), 144.

[35] L. Rédei and J. Szép, "Die Verallgemeinerung der Theorie des Gruppenproduktes von Zappa-Casadio," *Acta Sci. Math. Szeged* **16** (1955), 165-170.

[36] P. Rosenmai, *General Products, Vines and Transformation Monoids*, Honours Thesis, School of Mathematics and Statistics, University of Sydney, 1997.

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

[38] J. Szép, "On the structure of groups represented as the product of two subgroups," *Acta Sci. Math. Szeged* **12A** (1950), 57-61.

[39] 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.

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

[41] G. Zappa, "Sulla construzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro," *Atti Secondo Congresso Un. Mat. Ital. Bologna* **19** (1940), 119-125, Perrella, Rome, 1942.

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