J. Aust. Math. Soc. **101** (2016), 310–334
doi:10.1017/S1446788716000112

INTERCHANGE RINGS

CHARLES C. EDMUNDS

(Received 19 February 2015; accepted 29 September 2015; first published online 12 May 2016)

Communicated by L. Batten

Abstract

An *interchange ring,* $(R, +, \bullet)$, is an abelian group with a second binary operation defined so that the *interchange law* $(w + x) \bullet (y + z) = (w \bullet y) + (x \bullet z)$ holds. An *interchange near ring* is the same structure based on a group which may not be abelian. It is shown that each interchange (near) ring based on a group G is formed from a pair of endomorphisms of G whose images commute, and that all interchange (near) rings based on G can be characterized in this manner. To obtain an associative interchange ring, the endomorphisms must be commuting idempotents in the endomorphism semigroup of G. For G a finite abelian group, we develop a group-theoretic analogue of the simultaneous diagonalization of idempotent linear operators and show that pairs of endomorphisms which yield associative interchange rings can be diagonalized and then put into a canonical form. A best possible upper bound of 4^r can be given for the number of distinct isomorphism classes of associative interchange rings based on a finite abelian group A which is a direct sum of r cyclic groups of prime power order. If A is a direct sum of r copies of the same cyclic group of prime power order, we show that there are exactly $\frac{1}{6}(r + 1)(r + 2)(r + 3)$ distinct isomorphism classes of associative interchange rings based on A. Several examples are given and further comments are made about the general theory of interchange rings.

2010 *Mathematics subject classification*: primary 16Y99; secondary 17A99, 17D99.

Keywords and phrases: double magma, interchange rings.

1. Introduction

Kock [5] introduced the notion of a double semigroup in his study of two-fold monoidal categories. A double semigroup is a nonempty set with two associative binary operations which satisfy the interchange law (see Equation (1.1) below). As early as 1961 Eckmann and Hilton [2] introduced the interchange law in their well-known argument demonstrating commutativity of the higher homotopy groups. Studies in double categories also make fruitful use of this law. Recently DeWolf [1] added to the study begun by Kock showing that all double inverse semigroups are commutative with both operations identical. In [3] the author discussed the construction of various double semigroups using commutation operations on a group. The purpose of this note is to study the implications of the interchange law in a

universal algebraic context. Primarily, we will consider double magmas whose first operation is a group and develop the obvious analogies with near rings and rings.

We will begin in the most general context and add further axioms as the theory develops. A *magma* $(M, *)$ is a pair consisting of a nonempty set and a binary operation on that set. A *double magma* $(M, *, \bullet)$ is a triple consisting of a nonempty set with two binary operations satisfying the interchange law,

$$(w * x) \bullet (y * z) = (w \bullet y) * (x \bullet z) \tag{1.1}$$

for each $w, x, y, z \in M$. We call a double magma *commutative, associative*, or *unital* provided both magmas, $(M, *)$ and $(M, \bullet)$, are commutative, associative, or unital, respectively. An associative double magma is called a *double semigroup*. Expressed in this terminology, the Eckmann–Hilton argument proves that if a double magma is unital, then it is commutative, associative, the two identity elements for the operations coincide and, in fact, the two binary operations are the same. A double magma, $(M, *, *)$, with two identical operations is a double magma in name only; it coincides, essentially, with a magma, $(M, *)$, satisfying the *medial law,* $(w * x) * (y * z) = (w * y) * (x * z)$. If this magma is a semigroup, the medial law has a strong impact on its structure. For example if $(M, *)$ is finite or uniformly periodic, then it is commutative. In what follows we will try to avoid the situation where the two operations coincide; thus, as the Eckmann–Hilton theorem implies, we must not let a double magma be unitary. Henceforth we will allow at most one of the operations to have an identity element. With this point in mind, we define a double magma to be *proper* if its operations do not coincide and *improper* otherwise.

The specific focus of this study is an investigation of the analogy between a double magma $(M, *, \bullet)$ and a ring $(R, +, \cdot)$. A *ring* is an additive abelian group with an associative multiplication and distributive laws serving to connect the two operations algebraically. We will not consider rings with identity, since the analogous double magma is then forced to be improper. A double magma has no algebraic structure on its two binary operations, but, as with the distributive laws in a ring, the interchange law connects the two operations. A *near ring* is a generalization of a ring in which the additive structure may not be abelian. Also only one of the distributive laws, usually the right distributive law, is imposed for a near ring. We begin our study with an arbitrary group $(G, +)$ written additively using the usual conventions that the identity element is denoted 0 and the inverse of $x \in G$ is written $-x$. We will form a double magma $(G, +, \bullet)$ where the magma $(G, \bullet)$ has no algebraic structure beyond the closure of its binary operation on G. Thus, with the distributive laws replaced by the interchange law, we have something like a near ring, but with the associative law not necessarily holding on the multiplication.

Definition 1.1. An *interchange near ring* is a triple, $(G, +, \bullet)$, with $(G, +)$ a group and $(G, +, \bullet)$ a double magma.

If the additive structure is an abelian group, we specialize the definition.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

DEFINITION 1.2. An *interchange ring*[1] is an interchange near ring $(G, +, \bullet)$ for which $(G, +)$ is abelian.

The use of the term 'ring' in this definition is an abuse of language since a ring must be both associative and distributive. However there are nonassociative rings (for example, Lie rings and Jordan rings) and I think of an interchange ring as a 'nonassociative', 'nondistributive' ring. From the beginning, my goal has been to see what ringlike behaviour, and what nonringlike behaviour, these algebraic structures exhibit. I feel that the results in Section 7 show that the analogy with rings is at least somewhat useful in this study.

Interchange rings may seem like exotic objects, but it is interesting to note that the familiar structures $(\mathbb{Z}, +, -)$ and $(\mathbb{Q} - \{0\}, \times, \div)$ are interchange rings. In fact, if $(A, +)$ is any abelian group, $(A, +, -)$ is an interchange ring. It is a well-known algebraic problem to determine which abelian groups admit a nonzero ring structure. For example, the Prufer group, or quasicyclic group $\mathbb{Z}_{p^\infty}$, can be seen to admit only the zero ring structure. In Section 3 we show that every nontrivial group G admits at least three nonzero interchange (near) ring structures and there is a clearly defined process for constructing each such structure from the group. The construction starts with a pair, (ε, η), of endomorphisms of G with commuting images and then defines a product by $x \bullet y = \varepsilon(x) + \eta(y)$. It is shown that each product constructed in this way yields an interchange near ring (Theorem 3.3), and that each interchange near ring based on G arises in this manner (Theorem 3.4). It is then observed that the equivalence relation of similarity of pairs, that is, the existence of $\alpha \in \mathrm{Aut}(G, +)$ for which $\alpha^{-1}(\varepsilon_1, \eta_1)\alpha = (\varepsilon_2, \eta_2)$, corresponds exactly to isomorphism of the associated interchange (near) rings (Theorem 3.7).

In Section 4 we show that an interchange (near) ring is associative if and only if it is generated by a pair of commuting, idempotent endomorphisms of its additive group (Theorem 4.3). In Section 5 we restrict our attention to interchange rings based on finite abelian groups. We apply techniques familiar in operator theory to characterize all finite associative interchange rings by showing how to diagonalize pairs of their generating endomorphisms (Theorem 5.9). We obtain a best possible upper bound of 4^r for the number of distinct isomorphism classes of associative interchange rings based on a finite abelian group, A, which is a direct sum of r cyclic groups of prime power order (Theorem 5.10). In Section 6 we further restrict A to a direct sum of r isomorphic copies of a cyclic group of prime power order and develop a unique canonical form for pairs of endomorphism generating the interchange rings based on A (Corollary 6.9). Using this result, we obtain the exact number, $\frac{1}{6}(r+1)(r+2)(r+3)$, of distinct isomorphism classes of associative interchange rings based on A (Theorem 6.10). In Section 7 we make some comments about the extent to which interchange ring theory might be developed by analogy with standard ring theory. One would hope, someday, to see a structure theory of interchange rings.

[1] As pointed out by the referee, this is not to be confused with an interchange algebra as defined in [6].

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

2. Preliminaries

We begin with some fundamental statements about interchange near rings. Note the algebraic importance of the zero element.

LEMMA 2.1. *If $(G, +, \bullet)$ is an interchange near ring, then the following statements are true.*

(i) *Zero is idempotent multiplicatively;* $0 \bullet 0 = 0$.
(ii) *Zero distributes multiplicatively over addition; for each* $x, y \in G$, $0 \bullet (x + y) = (0 \bullet x) + (0 \bullet y)$ *and* $(x + y) \bullet 0 = (x \bullet 0) + (y \bullet 0)$.
(iii) *For each* $x, y \in G$, $x \bullet y = x \bullet 0 + 0 \bullet y$.
(iv) *For each* $x, y \in G$, $(-x) \bullet (-y) = -(x \bullet y)$.

PROOF. (i) We use the identity property of 0 and then apply the interchange law to obtain $0 \bullet 0 = (0 + 0) \bullet (0 + 0) = (0 \bullet 0) + (0 \bullet 0)$. Adding the inverse of $0 \bullet 0$ to both sides, we obtain our result.

(ii) $0 \bullet (x + y) = (0 + 0) \bullet (x + y) = (0 \bullet x) + (0 \bullet y)$. The second equality follows by the interchange law. The right-hand law follows similarly.

(iii) $x \bullet y = (x + 0) \bullet (0 + y) = x \bullet 0 + 0 \bullet y$.

(iv) $(x \bullet y) + (-x \bullet -y) = (x + (-x)) \bullet (y + (-y)) = 0 \bullet 0 = 0$. The result follows. □

LEMMA 2.2. *If $(G, +, \bullet)$ is an interchange near ring then $(G, \bullet)$ is associative if and only if, for each $x \in G$, (i) $(x \bullet 0) \bullet 0 = x \bullet 0$, (ii) $(0 \bullet x) \bullet 0 = 0 \bullet (x \bullet 0)$, and (iii) $0 \bullet (0 \bullet x) = 0 \bullet x$.*

PROOF. Note first that if $(G, \bullet)$ is associative then (ii) follows immediately. Conditions (i) and (ii) follow from associativity and Lemma 2.1(i). Conversely, assuming that (i)–(iii) hold and applying Lemma 2.1, $(x \bullet y) \bullet z = (x \bullet 0 + 0 \bullet y) \bullet 0 + 0 \bullet z = (x \bullet 0) \bullet 0 + (0 \bullet y) \bullet 0 + 0 \bullet z = x \bullet 0 + 0 \bullet (y \bullet 0) + 0 \bullet (0 \bullet z) = x \bullet 0 + 0 \bullet ((y \bullet 0) + (0 \bullet z)) = x \bullet (y \bullet z)$. □

In rings the additive identity is an annihilator (that is, $x \cdot 0 = 0 \cdot x = 0$, for each x); however, the existence of an annihilator in an interchange near ring destroys its structure. We define an element $a \in G$ to be an *annihilator* in an interchange near ring, $(G, +, \bullet)$, if $a \bullet x = x \bullet a = a$ for every $x \in G$. A *zero semigroup* is a semigroup $(S, \cdot)$ satisfying the identity $w \cdot x = y \cdot z$. This implies that all entries in the Cayley table are equal; thus zero semigroups are considered trivial for most purposes.

PROPOSITION 2.3. *If $(G, +, \bullet)$ is an interchange near ring containing an annihilator, then $(G, \bullet)$ is a zero semigroup.*

PROOF. Suppose that a is an annihilator. Thus, for each $x \in G$, we have $a = a \bullet x = a \bullet 0 + 0 \bullet x = a + 0 \bullet x$. Therefore $0 \bullet x = 0$, for each $x \in G$. Similarly, we can show that $x \bullet 0 = 0$, for each $x \in G$. Thus, by Lemmas 2.1(i) and 2.1(iii), we have $x \bullet y = x \bullet 0 + 0 \bullet y = 0 + 0 = 0$, for each $x, y \in G$. Hence $(G, \bullet)$ is a zero semigroup. □

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

3. Constructing interchange near rings from groups

In this section we will show that any nontrivial group admits a number of distinct interchange (near) ring structures. For $(G,+)$ a group, we denote the sets of endomorphisms and automorphisms of G by $\mathrm{End}(G,+)$ and $\mathrm{Aut}(G,+)$, respectively.

DEFINITION 3.1. If $(G,+)$ is a group with $\varepsilon,\eta \in \mathrm{End}(G,+)$, we say that the pair (ε,η) is *image-commuting* when $\varepsilon(x)+\eta(y)=\eta(y)+\varepsilon(x)$, for every $x,y\in G$.

If $(G,+)$ is abelian, then each pair of endomorphisms is image commutating. If $(G,+)$ is nonabelian and the image of G under either map is contained in the centre of G, then the maps are also image-commuting. We give an example to illustrate that image-commuting endomorphisms need not have abelian images.

EXAMPLE 3.2. We present the symmetric group on three letters additively as

$$S_3=\langle a,b;3a=0,2b=0,b+a=2a+b\rangle.$$

Each element of S_3 can be written uniquely as $ia+jb$ with $i\in\mathbb{Z}_3$ and $j\in\mathbb{Z}_2$. Let $(G,+)$ be the direct product of two copies of S_3 and define two endomorphisms of $(G,+)$ as follows: for each $(ia+jb,ka+lb)\in G$, let $\varepsilon(ia+jb,ka+lb)=(0,ia+jb)$ and let $\eta(ia+jb,ka+lb)=(ka+lb,0)$. Note that the images of both ε and η are isomorphic to S_3, and hence are nonabelian. However, since the images of these endomorphisms are in different direct factors, they commute; thus (ε,η) is an image-commuting pair.

We are now in a position to state the main results of this section.

THEOREM 3.3. *If $(G,+)$ is a group, (ε,η) is an image-commuting pair of endomorphisms of $(G,+)$, and a binary operation $\bullet$ is defined on G by $x\bullet y=\varepsilon(x)+\eta(y)$, for each $x,y\in G$, then $(G,+,\bullet)$ is an interchange near ring.*

The converse also holds.

THEOREM 3.4. *If $(G,+,\bullet)$ is an interchange near ring, then the pair (ε,η) of mappings from G to G defined by $\varepsilon(x)=x\bullet 0$ and $\eta(x)=0\bullet x$, for each $x\in G$, is a pair of image-commutating endomorphisms of G.*

We will denote the set of all image-commuting pairs of endomorphisms of $(G,+)$ by $\mathrm{ICE}(G,+)$, and the set of all interchange near rings based on $(G,+)$ by $\mathrm{INR}(G,+)$. Given a pair $(\varepsilon,\eta)\in\mathrm{ICE}(G,+)$, we denote the binary operation constructed from this pair in Theorem 3.3 by $\bullet_{(\varepsilon,\eta)}$. Given an interchange near ring, $(G,+,\bullet)$, we denote the pair of image-commuting mappings defined in Theorem 3.4 by $(\varepsilon_\bullet,\eta_\bullet)$.

THEOREM 3.5. *The mapping $\Psi:\mathrm{ICE}(G)\to\mathrm{INR}(G)$ defined by $\Psi(\varepsilon,\eta)=(G,+,\bullet_{(\varepsilon,\eta)})$ is a bijection.*

We will leave the task of determining structural parallels between these two classes to category theorists.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Proof of Theorem 3.3. It is sufficient to show that the interchange law holds. Letting $w, x, y, z \in G$, we have $(w \bullet x) + (y \bullet z) = \varepsilon(w) + \eta(x) + \varepsilon(y) + \eta(z)$. Since ε and η are image-commuting, we can interchange the two middle terms, and obtain $(w \bullet x) + (y \bullet z) = \varepsilon(w) + \varepsilon(y) + \eta(x) + \eta(z) = \varepsilon(w + y) + \eta(x + z) = (w + y) \bullet (x + z)$. □

Proof of Theorem 3.4. Clearly $\varepsilon(x) = x \bullet 0$ maps from G into G. To show that ε is a homomorphism, we let $x, y \in G$ and consider $\varepsilon(x + y)$ and $\varepsilon(-x)$. Applying Lemma 2.1, we have $\varepsilon(x + y) = (x + y) \bullet 0 = x \bullet 0 + y \bullet 0 = \varepsilon(x) + \varepsilon(y)$ and $\varepsilon(-x) = (-x) \bullet 0 = -(x \bullet 0) = -\varepsilon(x)$. Thus ε is a homomorphism of G. The proof that η is a homomorphism of G is similar. Lastly, we must see that the pair is image-commuting. Let $x, y \in G$ and consider the sum $\varepsilon(x) + \eta(y)$. By Lemma 2.1 and the interchange law, we have $\varepsilon(x) + \eta(y) = x \bullet 0 + 0 \bullet y = x \bullet y = (0 + x) \bullet (y + 0) = (0 \bullet y) + (x \bullet 0) = \eta(y) + \varepsilon(x)$. □

Proof of Theorem 3.5. First we will show that Ψ maps $\mathrm{ICE}(G)$ into $\mathrm{INR}(G)$. It suffices to show that the image of any $(\varepsilon, \eta) \in \mathrm{ICE}(G, +)$ under Ψ, namely $(G, +, \bullet_{(\varepsilon,\eta)})$, satisfies the interchange law. Supposing that $w, x, y, z \in G$, we have $(w \bullet_{(\varepsilon,\eta)} x) + (y \bullet_{(\varepsilon,\eta)} z) = (\varepsilon(w) + \eta(x)) + (\varepsilon(y) + \eta(z))$. Since (ε, η) is an image-commuting pair, we can rearrange the second sum as

$$(\varepsilon(w) + \eta(x)) + (\varepsilon(y) + \eta(z)) = (\varepsilon(w) + \varepsilon(y)) + (\eta(x) + \eta(z)).$$

Since ε and η are endomorphisms of G, we can apply the definition of $\bullet_{(\varepsilon,\eta)}$ in reverse, to conclude that

$$(\varepsilon(w) + \varepsilon(y)) + (\eta(x) + \eta(z)) = \varepsilon(w + y) + \eta(x + z) = (w + y) \bullet_{(\varepsilon,\eta)} (x + z).$$

To prove that Ψ is injective, we suppose that (ε_1, η_1) and (ε_2, η_2) are image-commuting pairs for which $\Psi(\varepsilon_1, \eta_1) = \Psi(\varepsilon_2, \eta_2)$, that is, $(G, +, \bullet_{(\varepsilon_1,\eta_1)}) = (G, +, \bullet_{(\varepsilon_2,\eta_2)})$, and therefore $\bullet_{(\varepsilon_1,\eta_1)} = \bullet_{(\varepsilon_2,\eta_2)}$. To keep our calculations more readable, we will use $\bullet_i$ as shorthand notation for $\bullet_{(\varepsilon_i,\eta_i)}$. Since each η_i is a homomorphism of G, it follows that $\eta_i(0) = 0$. Thus, for any $x \in G$, $\varepsilon_1(x) = \varepsilon_1(x) + \eta_1(0) = x \bullet_1 0 = x \bullet_2 0 = \varepsilon_2(x) + \eta_2(0) = \varepsilon_2(x)$. Thus $\varepsilon_1 = \varepsilon_2$, and a similar calculation shows that $\eta_1 = \eta_2$. Therefore $(\varepsilon_1, \eta_1) = (\varepsilon_2, \eta_2)$ and Ψ is injective. To see that Ψ is surjective, we let $(G, +, \bullet)$ be any element of $\mathrm{INR}(G, +)$. Theorem 3.4 shows how to construct the pair, $(\varepsilon_\bullet, \eta_\bullet)$, of image-commuting endomorphisms of $(G, +)$ from $(G, +, \bullet)$. Applying Ψ to this pair, we obtain the interchange near ring $\Psi(\varepsilon_\bullet, \eta_\bullet)$ based on $(G, +)$. For now, let us denote the second operation of the interchange near ring thus produced by $\odot$, writing $\Psi(\varepsilon_\bullet, \eta_\bullet) = (G, +, \odot)$. Note that $\odot$ is constructed from the pair $(\varepsilon_\bullet, \eta_\bullet)$ as in Theorem 3.3. That is, for each $x, y \in G$, $x \odot y = \varepsilon_\bullet(x) + \eta_\bullet(y) = x \bullet 0 + 0 \bullet y = x \bullet y$. Therefore $\odot = \bullet$, and as a result, $(G, +, \odot) = (G, +, \bullet)$. It follows that $\Psi(\varepsilon_\bullet, \eta_\bullet) = (G, +, \bullet)$, and hence that Ψ is surjective. □

At this point we have shown that distinct pairs of image-commuting endomorphisms yield unequal interchange near rings, but they could be isomorphic. If $(G_1, +_1, \bullet_1)$ and $(G_2, +_2, \bullet_2)$ are interchange near rings, a mapping $\varphi : (G_1, +_1, \bullet_1) \to (G_2, +_2, \bullet_2)$,

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

is an *interchange near ring homomorphism* if $\varphi : (G_1, +_1) \to (G_2, +_2)$ is a group homomorphism and, for each $x, y \in G_1$, $\varphi(x \bullet_1 y) = \varphi(x) \bullet_2 \varphi(y)$. This homomorphism is an *interchange near ring isomorphism* exactly when it is a bijection. We will denote isomorphism of interchange near rings by $\cong$. It is routine to check that both relations defined below are equivalence relations.

DEFINITION 3.6. If $\varepsilon, \eta \in \mathrm{End}(G, +)$ and $\alpha \in \mathrm{Aut}(G, +)$ so that $\alpha^{-1}\varepsilon\alpha = \eta$, we say that ε *is similar to* η (under α) and write $\varepsilon \sim \eta(\alpha)$ or, more simply, $\varepsilon \sim \eta$. For pairs of endomorphisms of G, (ε_1, η_1) *is similar to* (ε_2, η_2), denoted $(\varepsilon_1, \eta_1) \sim (\varepsilon_2, \eta_2)(\alpha)$ or $(\varepsilon_1, \eta_1) \sim (\varepsilon_2, \eta_2)$, whenever there is an automorphism $\alpha \in \mathrm{Aut}(G, +)$ such that $\alpha^{-1}(\varepsilon_1, \eta_1)\alpha = (\alpha^{-1}\varepsilon_1\alpha, \alpha^{-1}\eta_1\alpha) = (\varepsilon_2, \eta_2)$.

THEOREM 3.7. *If $(G, +)$ is a group and $(G, +, *)$ and $(G, +, \odot)$ are interchange near rings based on $(G, +)$, then $(G, +, *) \cong (G, +, \odot)$ if and only $(\varepsilon_*, \eta_*) \sim (\varepsilon_\odot, \eta_\odot)$.*

PROOF. ($\Rightarrow$) Suppose that there is an isomorphism $\varphi : (G, +, *) \to (G, +, \odot)$. First consider ε_* applied to any $x \in G$, $\varepsilon_*(x) = x * 0$. Applying the isomorphism φ, we obtain $\varphi(\varepsilon_*(x)) = \varphi(x * 0) = \varphi(x) \odot \varphi(0) = \varphi(x) \odot 0 = \varepsilon_\odot(\varphi(x))$. Therefore, $(\varphi\varepsilon_* - \varepsilon_\odot\varphi)(x) = 0$, for each $x \in G$. It follows that $\varphi\varepsilon_* = \varepsilon_\odot\varphi$, and by a similar argument that $\varphi\eta_* = \eta_\odot\varphi$. Thus we have $(\varepsilon_*, \eta_*) \sim (\varepsilon_\odot, \eta_\odot)$.

($\Leftarrow$) Now suppose that $(\varepsilon_*, \eta_*) \sim (\varepsilon_\odot, \eta_\odot)$. Thus there is an automorphism ϕ of $(G, +)$ such that $\phi\varepsilon_* = \varepsilon_\odot\phi$ and $\phi\eta_* = \eta_\odot\phi$. We claim that ϕ is an isomorphism mapping $(G, +, *)$ onto $(G, +, \odot)$. Since ϕ is an automorphism of $(G, +)$ we know that it is a bijection from G to G and that it is a group homomorphism with respect to addition. To prove that $(G, +, *)$ and $(G, +, \odot)$ are isomorphic under ϕ, it remains to show that, for each $x, y \in G$, $\phi(x * y) = \phi(x) \odot \phi(y)$: $\phi(x * y) = \phi(x * 0 + 0 * y) = \phi(x * 0) + \phi(0 * y) = \phi\varepsilon_*(x) + \phi\eta_*(y) = \varepsilon_\odot\phi(x) + \eta_\odot\phi(y) = \phi(x) \odot \phi(y)$. □

THEOREM 3.8. *If $(G, +)$ is a nontrivial group, there are at least three distinct isomorphism classes of proper interchange near rings based on G.*

PROOF. Let ι and ζ be the identity map and the zero map, respectively, from G to G. Note that ζ is image-commuting with all endomorphisms of G. Since both of these mappings commute with every automorphism of G, their similarity classes are singletons. Thus, by Theorems 3.2 and 3.5, the pairs $(\zeta, \zeta), (\zeta, \iota)$ and (ι, ζ) generate three nonisomorphic proper interchange near rings based on G. □

Note first that we have dispensed with the pair (ι, ι) since it generates an improper interchange near ring. The pair (ζ, ζ) generates the product $x \bullet y = 0$, yielding the *zero interchange ring,* the pair (ζ, ι) generates the product $x \bullet y = x$, the *right zero semigroup,* and (ι, ζ) generates the product $x \bullet y = y$, the *left zero semigroup.* We will refer to these three isomorphism classes of proper interchange near rings as the *essential interchange rings based on G.* We will find these relatively uninteresting and refer to proper interchange near rings based on G which are not of these three types as *inessential*. The question, in ring theory, of whether or not there exists a nonzero ring based on a particular abelian group is parallel to the question, in interchange (near)

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

ring theory, of whether or not there is an inessential interchange (near) ring based on a group. For instance, there are no inessential interchange near rings based on the cyclic group of order two.

With this much structure involved, the discussion calls for an example of how our theorems can be applied in some specific cases.

EXAMPLE 3.9. Interchange near rings based on S_3. For economy, we will rename the elements of $(S_3, +)$ as given in Example 3.2, $0, a, 2a, b, a+b, 2a+b$, as $0, 1, 2, 3, 4, 5$, respectively. We denote an endomorphism ε mapping $0 \mapsto 0$, $1 \mapsto v$, $2 \mapsto w$, $3 \mapsto x$, $4 \mapsto y$ and $5 \mapsto z$ by $\varepsilon = (0vwxyz)$. There are six automorphisms of $(S_3, +)$,

$$\alpha_0 = (012345), \quad \alpha_1 = (012453), \quad \alpha_2 = (012534),$$
$$\alpha_3 = (021354), \quad \alpha_4 = (021435) \quad \text{and} \quad \alpha_5 = (021543),$$

and four proper endomorphisms,

$$\varepsilon_0 = (000000), \quad \varepsilon_1 = (000333), \quad \varepsilon_2 = (000444) \quad \text{and} \quad \varepsilon_3 = (000555).$$

The images of S_3 under these maps are

$$\alpha_i(S_3) = S_3, \quad \varepsilon_0(S_3) = \{0\}, \quad \varepsilon_1(S_3) = \{0, 3\}, \quad \varepsilon_2(S_3) = \{0, 4\} \quad \text{and} \quad \varepsilon_3(S_3) = \{0, 5\}.$$

To form an interchange near ring, the pairs we select must be image-commuting, thus the only candidates are pairs of the form $(\varepsilon_0, \varepsilon)$ and $(\varepsilon, \varepsilon_0)$ for $\varepsilon \in \mathrm{End}(S_3, +)$, and the pairs $(\varepsilon_1, \varepsilon_1), (\varepsilon_2, \varepsilon_2)$ and $(\varepsilon_3, \varepsilon_3)$. Since $\alpha_1^{-1}\varepsilon_1\alpha_1 = \varepsilon_2$ and $\alpha_3^{-1}\varepsilon_2\alpha_3 = \varepsilon_3$, we have $(\varepsilon_1, \varepsilon_1) \sim (\varepsilon_2, \varepsilon_2) \sim (\varepsilon_3, \varepsilon_3)$; therefore, these last three pairs will yield isomorphic interchange rings. We express $\mathrm{End}(S_3)$ as a disjoint union of similarity classes:

$$\mathrm{End}(S_3) = \{\alpha_0\} \dot\cup \{\alpha_1, \alpha_2\} \dot\cup \{\alpha_3, \alpha_4, \alpha_5\} \dot\cup \{\varepsilon_0\} \dot\cup \{\varepsilon_1, \varepsilon_2, \varepsilon_3\}.$$

Thus the nonsimilar, image-commuting pairs are $(\varepsilon_1, \varepsilon_1)$, $(\varepsilon_0, \varepsilon)$ where $\varepsilon \in \{\alpha_0, \alpha_1, \alpha_3, \varepsilon_0, \varepsilon_1\}$, and $(\varepsilon, \varepsilon_0)$ where $\varepsilon \in \{\alpha_0, \alpha_1, \alpha_3, \varepsilon_1\}$. Hence there are nine distinct isomorphism classes of interchange near rings based on S_3; the three essential interchange near rings generated by the pairs $(\varepsilon_0, \varepsilon_0), (\varepsilon_0, \alpha_0)$ and $(\alpha_0, \varepsilon_0)$ plus six additional inessential interchange near rings.

4. Commutativity, idempotence, and associativity of $(G, \bullet)$

PROPOSITION 4.1. *If $(G, +, \bullet)$ is an interchange near ring constructed from a pair (ε, η) of image-commuting endomorphisms of $(G, +)$, then $(G, \bullet)$ is commutative if and only if $\varepsilon = \eta$.*

PROOF. Note first that if $(G, \bullet)$ is commutative, we have $\varepsilon(x) + \eta(y) = x \bullet y = y \bullet x = \varepsilon(y) + \eta(x)$. Our conclusion follows letting $y = 0$. Conversely, if we suppose that $\varepsilon = \eta$, then, recalling that ε and η are image-commuting, we have $x \bullet y = \varepsilon(x) + \eta(y) = \eta(y) + \varepsilon(x) = \varepsilon(y) + \eta(x) = y \bullet x$. □

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Note that when $(G, \bullet)$ is commutative, to be image-commuting $\varepsilon(G)(= \eta(G))$ must be abelian. We denote the identity mapping of $\mathrm{End}(G, +)$ by ι.

PROPOSITION 4.2. *If $(G, +, \bullet)$ is an interchange near ring constructed from a pair (ε, η) of image-commuting endomorphisms of $(G, +)$, then $(G, \bullet)$ is idempotent if and only if $\varepsilon + \eta = \iota$.*

PROOF. Note that for each $x \in G$, $x \bullet x = \varepsilon(x) + \eta(x) = (\varepsilon + \eta)(x)$. It follows that idempotence of $(G, \bullet)$ is equivalent to $\varepsilon + \eta = \iota$. □

The following theorem characterizes those interchange near rings which have an associative multiplication.

THEOREM 4.3. *If $(G, +, \bullet)$ is an interchange near ring constructed from a pair (ε, η) of image-commuting endomorphisms of $(G, +)$, then $(G, \bullet)$ is associative if and only if ε and η are commuting idempotents in the semigroup* $\mathrm{End}(G, +)$.

PROOF. By Lemma 2.2, $(G, \bullet)$ is associative if and only if, for each $x \in G$, (i) $(x \bullet 0) \bullet 0 = x \bullet 0$, (ii) $(0 \bullet x) \bullet 0 = 0 \bullet (x \bullet 0)$, and (iii) $0 \bullet (0 \bullet x) = 0 \bullet x$. Since $\varepsilon(x) = x \bullet 0$, we have $\varepsilon^2(x) = \varepsilon(\varepsilon(x)) = \varepsilon(x) \bullet 0 = (x \bullet 0) \bullet 0$. Therefore condition (i) is equivalent to the idempotence of ε. Similarly, condition (iii) is equivalent to the idempotence of η. Finally, note that $(0 \bullet x) \bullet 0 = \varepsilon(0 \bullet x) = \varepsilon(\varepsilon(0) + \eta(x)) = \varepsilon\eta(x)$, while $0 \bullet (x \bullet 0) = \varepsilon(0) + \eta(x \bullet 0) = \eta(\varepsilon(x) + \eta(0)) = \eta\varepsilon(x)$. Thus condition (ii) is equivalent to the commutativity of ε and η. □

EXAMPLE 4.4. Associative interchange near rings of order six. The two groups of order six are the cyclic group of order six, which we will present as $C_6 = \langle a; 6a = 0 \rangle$, and the symmetric group on three letters, S_3, which was discussed in Example 3.9. We will find 16 isomorphism classes of associative interchange rings based on C_6 and six isomorphism classes of associative interchange near rings with additive structure $(S_3, +)$. Thus we have a total of 22 distinct isomorphism classes of associative interchange near rings of order six. Any endomorphism of C_6 can be written as $\varepsilon_i : x \mapsto ix$ for $i \in \mathbb{Z}_6$. The mappings ε_1 and ε_5 are automorphisms, and the other mappings are proper endomorphisms. Since C_6 is abelian, all pairs of endomorphisms are image-commuting. It is easy to see that $(\mathrm{End}(C_6, +), \circ)$ is a commutative semigroup with idempotents $E = \{\varepsilon_0, \varepsilon_1, \varepsilon_3, \varepsilon_4\}$. Thus for each $\alpha \in \mathrm{Aut}(C_6, +)$ and for each $\varepsilon \in \mathrm{End}(C_6, +)$, $\alpha^{-1}\varepsilon\alpha = \varepsilon$. It follows that each similarity class in $\mathrm{End}(C_6, +)$ is a singleton, and hence each of the 16 pairs of elements from E generates a distinct isomorphism class of associative interchange rings. By Proposition 4.1, we see that the four pairs $(\varepsilon_i, \varepsilon_i)(1 \le i \le 4)$ yield commutative multiplications. And by Proposition 4.2, the pairs $(\varepsilon_0, \varepsilon_1)$, $(\varepsilon_1, \varepsilon_0)$, $(\varepsilon_3, \varepsilon_4)$, and $(\varepsilon_4, \varepsilon_3)$ yield idempotent multiplications. Turning to S_3, we see from Example 3.9 that among the nine pairs which yield interchange near rings, there are six which are pairs of commuting idempotents: $(\varepsilon_0, \varepsilon_0), (\varepsilon_0, \alpha_0), (\alpha_0, \varepsilon_0), (\varepsilon_0, \varepsilon_1), (\varepsilon_1, \varepsilon_0), (\varepsilon_1, \varepsilon_1)$. These generate six distinct isomorphism classes. By Proposition 4.1, we see that only the pairs $(\varepsilon_0, \varepsilon_0)$ and $(\varepsilon_1, \varepsilon_1)$ yield commutative multiplications. And by Proposition 4.2, the pairs $(\varepsilon_0, \alpha_0)$ and $(\alpha_0, \varepsilon_0)$ yield idempotent multiplications.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

5. Finite associative interchange rings

In this section we direct the reader to McCoy [7, Ch. 8] for reference to results on abelian groups and to Hoffman and Kunze [4, Ch. 6] for reference to linear algebra. We begin by proving some facts about endomorphisms of finite abelian groups which are analogous to familiar results in linear algebra, and facilitated by the fact that an abelian group is a $\mathbb{Z}$-module. The goal of this section (Theorem 5.9) is to apply the theory thus developed to give a characterization of all finite associative interchange rings. Given a finite abelian group $(A, +)$, we will show that an associative interchange ring based on A is defined by a pair of diagonalizable endomorphisms, and that, when all such pairs are made diagonal, up to similarity, they yield all isomorphism classes of associative interchange rings based on A. This will be accomplished by characterizing the commuting, idempotent elements of $\mathrm{End}(A, +)$ and then appealing to Theorem 4.3. We will decompose A as a direct sum in a way that allows us to take advantage of an analogy with linear algebra. Luckily, it turns out, the theorem of linear algebra which we will need, that commuting, idempotent linear operators are simultaneously diagonalizable, survives in the context of finite abelian groups (Theorem 5.9). This diagonalization will allows us to give a tight upper bound on the number of associative interchange rings based on a finite abelian group A (Theorem 5.10).

For the remainder of this section $(A, +)$ will denote a finite additive abelian group with identity element 0. By the fundamental structure theorem, we know that A can be decomposed as a direct sum of prime power order cyclic groups. We will refer to any such decomposition as a *ppc-decomposition*. Furthermore, if A is decomposed in this manner as both $A = A_1 \oplus A_2 \oplus \cdots \oplus A_s$ and $A = B_1 \oplus B_2 \oplus \cdots \oplus B_t$, then $s = t$ and there is bijection between the sets of summands so that each A_i is isomorphic to the corresponding B_j. Since the number of these prime power order cyclic summands is invariant for A, we call this number the *prime power cyclic rank* of A, denoted ppc-rank(A). The true invariant here is the multiset of prime power order cyclic summands which form A as a direct sum. Routine use of the fundamental structure theory for finite abelian groups shows that (i) ppc-rank is invariant under isomorphism, and (ii) if A is a finite abelian group and $S \leq A$, then ppc-rank$(S) \leq$ ppc-rank(A).

For each i $(1 \leq i \leq r)$, let $a_i \in A$ so that $A = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_r \rangle$ with each summand a cyclic group of prime power order, and let $\bar{a} = \{a_1, \ldots, a_r\}$. Any $a \in A$ can be written uniquely as $a = c_1 a_1 + \cdots + c_r a_r$ with each $c_i \in \mathbb{Z}_{|a_i|}$, where $|a_i|$ denotes the order of a_i. It is reasonable to think of $\bar{a}$ as a basis for A, analogous to the standard concept for finite dimensional vector spaces. We will call any such set $\bar{a}$ a *prime power cyclic basis* of A, and abbreviate this term as ppc-basis. The trivial group has no ppc-basis and has ppc-rank zero. We comment that the ppc-rank is not the usual rank of the abelian group. In fact the cyclic group of order 6 has rank 1 and ppc-rank 2.

If $\bar{x} = \{x_1, \ldots, x_r\}$ is a ppc-basis for A and $\phi^* : \bar{x} \to A$ is a mapping for which each $|\phi^*(x_i)|$ divides $|x_i|$, then we can extend ϕ^* uniquely to an endomorphism $\phi \in \mathrm{End}(A, +)$ linearly; that is, if $a \in A$ is written $a = c_1 x_1 + \cdots + c_r x_r$ with each $c_i \in \mathbb{Z}_{|x_i|}$, we let $\phi(a) = c_1 \phi^*(x_1) + \cdots + c_r \phi^*(x_r)$. The fact that this is a homomorphism can be seen by appealing to the presentation of A implied by the ppc-basis $\bar{x}$. If we denote the

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

order of each x_i in A as n_i, then A can be presented as $A = \langle G; R\rangle$ where the generating set is $G = \bar{x}$ and the set of relations is $R = \{n_i x_i = 0 : 1 \le i \le r\} \cup \{x_i + x_j = x_j + x_i : 1 \le i, j \le r\}$. Any mapping of G into A extends to a unique homomorphism exactly when the mapping preserves these relations. Since we are mapping into an abelian group, the second set of relations holds under ϕ. And the first set holds, that is, $\phi(n_i x_i) = n_i \phi^*(x_i) = 0$, since we have made the hypothesis that each $|\phi^*(x_i)|$ divides $|x_i|$.

For the remainder of this section and the next we will let A be a finite abelian group of ppc-rank$(A) = r$ and fix a particular pcc-basis $\bar{e} = \{e_1, \ldots, e_r\}$ for A, which we will refer to as the *standard pcc-basis* for A. We say that an endomorphism $\delta \in \mathrm{End}(A, +)$ is *diagonal* when, for each element e_i of the standard basis, there exists $d_i \in \mathbb{Z}_{|e_i|}$ such that $\delta(e_i) = d_i e_i$. If $\varepsilon \in \mathrm{End}(A, +)$, a nonzero element $a \in A$ is called a *characteristic element* of ε if there exists a $\lambda \in \mathbb{Z}_{|a|}$ such that $\varepsilon(a) = \lambda a$. In this case we call λ the *characteristic value* of ε associated with a. We say that an endomorphism $\varepsilon \in \mathrm{End}(A, +)$ is *diagonalizable* if A has a ppc-basis consisting of characteristic elements of ε. The following result is analogous to a familiar one in linear algebra.

Proposition 5.1. *If A is a finite abelian group and $\varepsilon \in \mathrm{End}(A, +)$ is diagonalizable, then ε is similar to a diagonal endomorphism.*

Proof. Let us suppose that $\bar{x} = \{x_1, x_2, \ldots, x_r\}$ is a ppc-basis of A with each x_i a characteristic element of ε. Thus for each x_i there is a $\lambda_i \in \mathbb{Z}_{|x_i|}$ such that $\varepsilon(x_i) = \lambda_i x_i$. First, we wish to define an automorphism $\alpha \in \mathrm{Aut}(A, +)$ sending the standard basis $\bar{e}$ to this basis $\bar{x}$. Since $\bar{e}$ and $\bar{x}$ are both ppc-bases for A, then $A = \langle e_1\rangle \oplus \cdots \oplus \langle e_r\rangle = \langle x_1\rangle \oplus \cdots \oplus \langle x_r\rangle$ are decompositions of A into direct sums of cyclic groups of prime power order and, as mentioned earlier, there is a bijection of these summands pairing each $\langle e_i\rangle$ with a unique isomorphic $\langle x_j\rangle$. Thus there is a permutation π of $\{1, 2, \ldots, r\}$ so that $\langle e_i\rangle \cong \langle x_{\pi(i)}\rangle$, for each i. In particular, $|x_{\pi(i)}|$ equals, and hence divides, $|e_i|$. Thus the mapping $\alpha^* : \bar{e} \to \bar{x}$ defined by $\alpha^*(e_i) = x_{\pi(i)}$ can be extended to an endomorphism, α, of A. And since it is a bijection of the two ppc-bases of A, α is an automorphism of A. Next, we define a mapping $\delta^* : \bar{e} \to A$ by $\delta^*(e_i) = \lambda_{\pi(i)} e_i$. Since $\lambda_{\pi(i)} \in \mathbb{Z}_{|x_{\pi(i)}|}$ and $|x_{\pi(i)}| = |e_i|$, it follows that $\lambda_{\pi(i)} \in \mathbb{Z}_{|e_i|}$, and hence that the extension of this map, δ, is a diagonal endomorphism of A. Note now that $\varepsilon\alpha(e_i) = \varepsilon(x_{\pi(i)}) = \lambda_{\pi(i)} x_{\pi(i)}$, while $\alpha\delta(e_i) = \alpha(\lambda_{\pi(i)} e_i) = \lambda_{\pi(i)}\alpha(e_i) = \lambda_{\pi(i)} x_{\pi(i)}$. Thus $\alpha\delta = \varepsilon\alpha$ and it follows that $\alpha^{-1}\varepsilon\alpha = \delta$, and thus that ε is similar to δ. □

Lemma 5.2. *If $(A, +)$ is a finite abelian group, $(\varepsilon_1, \varepsilon_2)$ is a pair of commuting endomorphisms of A, and (η_1, η_2) is a pair of endomorphisms of A which is similar to $(\varepsilon_1, \varepsilon_2)$, then (η_1, η_2) is a commuting pair.*

Proof. Since $(\varepsilon_1, \varepsilon_2) \sim (\eta_1, \eta_2)$, there is an $\alpha \in \mathrm{Aut}(A, +)$ for which $\eta_1 = \alpha^{-1}\varepsilon_1\alpha$ and $\eta_2 = \alpha^{-1}\varepsilon_2\alpha$. Therefore,

$$\eta_1\eta_2 = \alpha^{-1}\varepsilon_1\alpha\alpha^{-1}\varepsilon_2\alpha = \alpha^{-1}\varepsilon_1\varepsilon_2\alpha = \alpha^{-1}\varepsilon_2\varepsilon_1\alpha = \alpha^{-1}\varepsilon_2\alpha\alpha^{-1}\varepsilon_1\alpha = \eta_2\eta_1. \qquad \square$$

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

LEMMA 5.3. *If A is a finite abelian group, $\varepsilon \in \mathrm{End}(A,+)$ is idempotent, and $0 \neq a \in A$ is a prime power order characteristic element of ε with characteristic value λ, then $\lambda \in \{0,1\} \subseteq \mathbb{Z}_{|a|}$.*

PROOF. Suppose that p is a prime and n is a positive integer such that $|a| = p^n$. Since there is a $\lambda \in \mathbb{Z}_{p^n}$ such that $\varepsilon(a) = \lambda a$, we have $\lambda a = \varepsilon(a) = \varepsilon^2(a) = \varepsilon(\varepsilon(a)) = \varepsilon(\lambda a) = \lambda\varepsilon(a) = \lambda^2 a$. It follows that $(\lambda^2 - \lambda)a = 0$, and therefore that $\lambda^2 \equiv \lambda \bmod p^n$. Now suppose that λ is not congruent to 0 and write $\lambda = p^m s$, where $0 \leq m < n$ and s is coprime to p. We may rewrite $\lambda^2 \equiv \lambda \bmod p^n$ as $p^{2m}s^2 \equiv p^m s \bmod p^n$. Therefore $p^m s \equiv 1 \bmod p^{n-m}$ and, since $n - m \geq 1$, it must be that $m = 0$ and $\lambda \equiv s \equiv 1 \bmod p^n$. The result follows. □

We will need to consider the structure of idempotent endomorphisms of A more carefully. Let A be a finite abelian group, $\varepsilon \in \mathrm{End}(A,+)$, and, for each i $(1 \leq i \leq r)$, $A_i \leq A$ such that $A = A_1 \oplus A_2 \oplus \cdots \oplus A_r$. If $\varepsilon(A_i) \leq A_i$, for each i, we say that each A_i is invariant under ε. For each i, we define $\varepsilon_i \in \mathrm{End}(A_i,+)$ to be the restriction of ε to A_i; thus for each $a_i \in A_i$, we have $\varepsilon_i(a_i) = \varepsilon(a_i)$. Note that, since A_i is invariant under ε, ε_i maps into A_i. We call ε the *direct sum of the endomorphisms* $\varepsilon_1, \ldots, \varepsilon_r$, and write $\varepsilon = \varepsilon_1 + \cdots + \varepsilon_r$. Note that ε_i is not an endomorphism of A. For each $a \in A$, there are unique elements $a_i \in A_i$ so that $a = a_1 + \cdots + a_r$ and, according to our definitions, $\varepsilon(a) = \varepsilon(a_1) + \cdots + \varepsilon(a_r) = \varepsilon_1(a_1) + \cdots + \varepsilon_r(a_r)$.

LEMMA 5.4. *If A is a finite abelian group, $\varepsilon \in \mathrm{End}(A,+)$, and A can be decomposed as $A = A_1 \oplus A_2 \oplus \cdots \oplus A_r$ with each A_i invariant under ε, and ε is written as the direct sum $\varepsilon = \varepsilon_1 + \cdots + \varepsilon_r$, then ε is idempotent if and only if, for each i $(1 \leq i \leq r)$, ε_i is idempotent.*

PROOF. If $a \in A$ and $a = a_1 + \cdots + a_r$, where each $a_i \in A_i$, then $\varepsilon(a) = \varepsilon(a_1) + \cdots + \varepsilon(a_r) = \varepsilon_1(a_1) + \cdots + \varepsilon_r(a_r)$, and $\varepsilon^2(a) = \varepsilon(\varepsilon_1(a_1) + \cdots + \varepsilon_r(a_r)) = \varepsilon_1^2(a_1) + \cdots + \varepsilon_r^2(a_r)$. Therefore, if each ε_i is idempotent, then ε is idempotent. Now suppose that some ε_i were not idempotent. Letting $a' \in A_i$ so that $\varepsilon_i(a') \neq \varepsilon_i^2(a')$, we see that $\varepsilon(a') \neq \varepsilon^2(a')$, and therefore ε is not idempotent. □

LEMMA 5.5. *If A is a finite abelian group of ppc-rank r, and δ is a diagonal endomorphism of A, then δ is idempotent if and only if, for each i $(1 \leq i \leq r)$, $\delta(e_i) \in \{0, e_i\}$.*

PROOF. Since δ is diagonal, there is a $d_i \in \mathbb{Z}_{|e_i|}$, for each i $(1 \leq i \leq r)$, such that $\delta(e_i) = d_i e_i$. Thus each e_i is a characteristic element of δ and each subgroup $\langle e_i \rangle$ is invariant under δ. Writing $A = \langle e_1 \rangle \oplus \cdots \oplus \langle e_r \rangle$ and decomposing δ over this sum as $\delta = \delta_1 + \cdots + \delta_r$, Lemma 5.4 implies that if δ is idempotent then each δ_i is idempotent. Since each e_i is of prime power order, Lemma 5.3 implies that d_i, the characteristic value of δ_i associated with e_i, is either 0 or 1 modulo $|e_i|$. Thus we have $\delta(e_i) \in \{0, e_i\}$, as required. Conversely, suppose that for each i we have $\delta(e_i) \in \{0, e_i\}$. If e_i has characteristic value 1, then $e_i = \delta(e_i) = \delta_i(e_i)$. It follows that $\delta_i^2(e_i) = \delta_i(e_i) = e_i$ and δ_i is idempotent. On the other hand, if e_i has characteristic value 0, then $0 = \delta(e_i) = \delta_i(e_i)$

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

and $\delta_i^2(e_i) = \delta_i(0) = 0$. In either case, we conclude that each δ_i is idempotent and, by Lemma 5.4, that δ is therefore also idempotent. □

LEMMA 5.6. *If A is a finite abelian group, then idempotent diagonal endomorphisms of A commute.*

PROOF. Let A be of ppc-rank r and let δ_1 and δ_2 be idempotent diagonal endomorphisms of A. By Lemma 5.5, for $j = 1, 2$ and for each i $(1 \le i \le r)$, we have $\delta_j(e_i) \in \{0, e_i\}$. We claim that $\delta_1\delta_2(e_i) = \delta_2\delta_1(e_i)$ for each i. There are four cases to consider: (i) $\delta_1(e_i) = \delta_2(e_i) = 0$; (ii) $\delta_1(e_i) = 0, \delta_2(e_i) = e_i$; (iii) $\delta_1(e_i) = e_i, \delta_2(e_i) = 0$; (iv) $\delta_1(e_i) = \delta_2(e_i) = e_i$. In each case it is routine to check that δ_1 and δ_2 commute when applied to any e_i. Writing $a \in A$ as $a = m_1e_1 + \cdots + m_re_r$, we see that $\delta_1\delta_2(a) = \sum_{i=1}^r m_i\delta_1\delta_2(e_i) = \sum_{i=1}^r m_i\delta_2\delta_1(e_i) = \delta_1\delta_2(a)$. □

LEMMA 5.7. *If A is a finite abelian group, ε and η are similar endomorphisms of A, and ε is idempotent, then η is idempotent.*

PROOF. Let $\alpha \in \mathrm{Aut}(A, +)$ so that $\alpha^{-1}\varepsilon\alpha = \eta$. Then $\eta^2 = (\alpha^{-1}\varepsilon\alpha)^2 = \alpha^{-1}\varepsilon^2\alpha = \alpha^{-1}\varepsilon\alpha = \eta$. □

LEMMA 5.8. *If $(A, +)$ is an abelian group, and $\varepsilon \in \mathrm{End}(A, +)$ is idempotent, then $A = \varepsilon(A) \oplus \ker(\varepsilon)$. Furthermore, $\varepsilon(A)$ and $\ker(\varepsilon)$ are invariant under ε, with ε acting as the identity mapping on $\varepsilon(A)$ and as the zero mapping on $\ker(\varepsilon)$.*

PROOF. For each $a \in A$, $a = \varepsilon(a) + (a - \varepsilon(a))$. Clearly $\varepsilon(a) \in \varepsilon(A)$. To see that $a - \varepsilon(a) \in \ker(\varepsilon)$, note that $\varepsilon(a - \varepsilon(a)) = \varepsilon(a) - \varepsilon^2(a) = 0$. It follows that $A = \varepsilon(A) + \ker(\varepsilon)$. To see that the sum is direct, let $x \in \varepsilon(A) \cap \ker(\varepsilon)$. Since $x \in \varepsilon(A)$, there is an $x' \in A$ with $\varepsilon(x') = x$. Therefore we have $x = \varepsilon(x') = \varepsilon^2(x') = \varepsilon(\varepsilon(x')) = \varepsilon(x)$. Since $x \in \ker(\varepsilon)$, this shows that $x = 0$, and therefore $\varepsilon(A) \cap \ker(\varepsilon) = \{0\}$. Since ε acts as the identity mapping on its image and the zero mapping on its kernel, it follows that both subgroups are invariant under ε. □

THEOREM 5.9. *Let $(A, +)$ be a finite abelian group and let $(\varepsilon_1, \varepsilon_2)$ be a pair of endomorphisms of A. The pair $(\varepsilon_1, \varepsilon_2)$ is a commuting pair of idempotent endomorphisms of A if and only if there exists a pair (δ_1, δ_2) of idempotent diagonal endomorphisms of A similar to $(\varepsilon_1, \varepsilon_2)$.*

PROOF. Suppose first that $(\varepsilon_1, \varepsilon_2)$ is similar to a pair (δ_1, δ_2) of idempotent diagonal endomorphisms of A. Since δ_1 and δ_2 are idempotent and similar to ε_1 and ε_2, respectively, Lemma 5.7 implies that ε_1 and ε_2 are idempotent. Lemma 5.6 implies that the pair (δ_1, δ_2) commutes and, thus, by Lemma 5.2, the pair $(\varepsilon_1, \varepsilon_2)$ commutes.

Conversely, suppose that $(\varepsilon_1, \varepsilon_2)$ is a commuting pair of idempotent endomorphisms of A. We will apply Lemma 5.8 to decompose A as $A = \varepsilon_1(A) \oplus \ker(\varepsilon_1)$. Since ε_1 acts as the identity map on $\varepsilon_1(A)$ and the zero mapping on $\ker(\varepsilon_1)$, each nonzero element, x, of these summands is a characteristic element of ε_1 having characteristic value one if $x \in \varepsilon_1(A)$ and zero if $x \in \ker(\varepsilon_1)$.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Claim. *Both* $\varepsilon_1(A)$ *and* $\ker(\varepsilon_1)$ *are invariant under* ε_2.

Proof of Claim. Since ε_1 acts as the identity mapping on $\varepsilon_1(A)$, we have $x = \varepsilon_1(x)$, for each $x \in \varepsilon_1(A)$. Applying ε_2 and using the commutativity of the two endomorphisms, we have $\varepsilon_2(x) = \varepsilon_2\varepsilon_1(x) = \varepsilon_1\varepsilon_2(x)$. Thus $\varepsilon_2(x) \in \varepsilon_1(A)$ and it follows that ε_2 maps $\varepsilon_1(A)$ into itself. Thus $\varepsilon_1(A)$ is invariant under ε_2. Now let $x \in \ker(\varepsilon_1)$. Since $\varepsilon_1(x) = 0$, it follows that $0 = \varepsilon_2(0) = \varepsilon_2\varepsilon_1(x) = \varepsilon_1\varepsilon_2(x)$. Hence $\varepsilon_2(x) \in \ker(\varepsilon_1)$ and this shows that $\ker(\varepsilon_1)$ is invariant under ε_2, and the claim is established. □

Thus we may decompose the endomorphism ε_2 according to the direct sum decomposition $A = \varepsilon_1(A) \oplus \ker(\varepsilon_1)$ as $\varepsilon_2 = \varepsilon_{2,1} + \varepsilon_{2,2}$, where $\varepsilon_{2,1}$ denotes the restriction of ε_2 to $\varepsilon_1(A)$ and $\varepsilon_{2,2}$ denotes the restriction of ε_2 to $\ker(\varepsilon_1)$. Since ε_2 is idempotent, Lemma 5.4 implies that $\varepsilon_{2,1}$ and $\varepsilon_{2,2}$ are idempotent. Applying Lemma 5.8 to the endomorphisms $\varepsilon_{2,1}$ and $\varepsilon_{2,2}$ acting on $\varepsilon_1(A)$ and $\ker(\varepsilon_1)$ respectively, we obtain decompositions of these as $\varepsilon_1(A) = \varepsilon_{2,1}(\varepsilon_1(A)) \oplus \ker(\varepsilon_{2,1})$ and $\ker(\varepsilon_1) = \varepsilon_{2,2}(\ker \varepsilon_1) \oplus \ker \varepsilon_{2,2}$. We observe that the nonzero elements of $\varepsilon_{2,1}(\varepsilon_1(A))$ and $\ker(\varepsilon_{2,1})$ are characteristic elements of ε_2 with $\lambda = 1$ and $\lambda = 0$, respectively. Also the nonzero elements of $\varepsilon_{2,2}(\ker(\varepsilon_1))$ and $\ker(\varepsilon_{2,2})$ are characteristic elements of ε_2 with $\lambda = 1$ and $\lambda = 0$, respectively. Writing

$$A = \varepsilon_{2,1}(\varepsilon_1(A)) \oplus \ker(\varepsilon_{2,1}) \oplus \varepsilon_{2,2}(\ker(\varepsilon_1) \oplus \ker(\varepsilon_{2,2}), \tag{5.1}$$

we see that the nonzero elements of these four summands are simultaneously characteristic elements of both ε_1 and ε_2. Since each of the four summands is a finite abelian group, each can be given a ppc-decomposition. Let us suppose that the four summands in (5.1) have ppc-bases $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4$, of ranks r_1, r_2, r_3, r_4 respectively, with $r = r_1 + r_2 + r_3 + r_4$. If we let $s_1 = r_1$, $s_2 = s_1 + r_2$, $s_3 = s_2 + r_3$ and $s_4 = s_3 + r_4 (= r)$, we can number these basis elements consecutively as $\bar{x}_1 = \{x_1, x_2, \ldots, x_{s_1}\}$, $\bar{x}_2 = \{x_{s_1+1}, x_{s_1+2}, \ldots, x_{s_2}\}$, $\bar{x}_3 = \{x_{s_2+1}, x_{s_2+2}, \ldots, x_{s_3}\}$, $\bar{x}_4 = \{x_{s_3+1}, x_{s_3+2}, \ldots, x_{s_4}\}$. Consider the standard basis, $\bar{e} = \{e_1, \ldots, e_r\}$, of A. By the fundamental structure theorem, and as in the proof of Proposition 5.1, we know that there is a permutation π of $\{1, 2, \ldots, r\}$ such that $|e_i| = |x_{\pi(i)}|$, for each i $(1 \le i \le r)$. It follows that the mapping $\alpha : A \to A$ defined by extending $\alpha(e_i) = x_{\pi(i)}$, for each i, is an automorphism of A. Since each x_i is a characteristic vector of both ε_1 and ε_2, and since both are idempotent, by Lemma 5.3, there exist $\lambda_i, \mu_i \in \{0, 1\}$ such that $\varepsilon_1(x_i) = \lambda_i x_i$ and $\varepsilon_2(x_i) = \mu_i x_i$. We define two diagonal endomorphisms as follows: $\delta_1(e_i) = \lambda_{\pi(i)} e_i$ and $\delta_2(e_i) = \mu_{\pi(i)} e_i$. It follows then that $\varepsilon_1\alpha(e_i) = \varepsilon_1 x_{\pi(i)} = \lambda_{\pi(i)} x_{\pi(i)}$, $\alpha\delta_1(e_i) = \alpha(\lambda_{\pi(i)} e_i) = \lambda_{\pi(i)}\alpha(e_i) = \lambda_{\pi(i)} x_{\pi(i)}$, $\varepsilon_2\alpha(e_i) = \varepsilon_2 x_{\pi(i)} = \mu_{\pi(i)} x_{\pi(i)}$ and $\alpha\delta_2(e_i) = \alpha(\mu_{\pi(i)} e_i) = \mu_{\pi(i)}\alpha(e_i) = \mu_{\pi(i)} x_{\pi(i)}$. Thus we have $\varepsilon_1\alpha = \alpha\delta_1$ and $\varepsilon_2\alpha = \alpha\delta_2$; hence, $\alpha^{-1}\varepsilon_1\alpha = \delta_1$ and $\alpha^{-1}\varepsilon_2\alpha = \delta_2$, as required. □

Note that the pair (δ_1, δ_2) constructed in this proof commutes by Lemma 5.6.

Theorem 5.10. *If* A *is a finite abelian group of ppc-rank* r*, then there are at most* 4^r *isomorphism classes of associative interchange rings based on* A*. This bound is best possible in the sense that, for each* $r > 0$*, there exists a finite abelian group,* A_r*, of ppc-rank* r *with exactly* 4^r *isomorphism classes of associative interchange rings based on* A_r*.*

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Proof. If A is any finite abelian group, Theorem 4.3 implies that each pair of commuting idempotent endomorphisms of A yields an associative interchange ring and all associative interchange rings based on A arise in this manner. Applying Theorem 5.9, we know that each isomorphism class of these interchange rings contains an interchange ring constructed from a pair (δ_1, δ_2) of idempotent diagonal endomorphisms of A. If δ is an idempotent diagonal endomorphism of A, Lemma 5.5 implies that, for each $i\,(1 \le i \le r)$, $\delta(e_i) \in \{0, e_i\}$. There are 2^r such δs, and thus there are $(2^r)^2$ pairs of these. Many of these pairs may be similar and hence the number of isomorphism classes of associative interchange rings based on A may be less, but 4^r provides an upper bound. To show that this bound is best possible in the sense stated, let p_i denote the ith prime number, let $n(r) = p_1 \cdots p_r$, and let A_r be the group $(\mathbb{Z}_{n(r)}, +)$. Note that $\mathbb{Z}_{n(r)} = \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_r}$ is of ppc-rank r and is generated additively by the multiplicative identity 1 of the ring $(\mathbb{Z}_{n(r)}, +, \cdot)$. If ε is an endomorphism of $\mathbb{Z}_{n(r)}$ and $x \in \mathbb{Z}_{n(r)}$, then $\varepsilon(x) = x\varepsilon(1)$. Thus for each endomorphism there is an element $a \in \mathbb{Z}_{n(r)}$ so that $\varepsilon(x) = ax$, and it follows that, for each i, $\varepsilon(e_i) = ae_i$ when a is reduced modulo $|e_i|(= p_i)$. Therefore each endomorphism, ε, is diagonal and, by Lemma 5.5, ε is idempotent if and only if, for each i, $\varepsilon(e_i) \in \{0, e_i\}$. Since ε is of the form $\varepsilon(x) = ax$ for some $a \in \mathbb{Z}_{n(r)}$, we see that $ae_i \in \{0, e_i\}$. Thus, for each i, either $a \equiv 0 \bmod p_i$ or $a \equiv 1 \bmod p_i$. Writing $a = a_1 + \cdots + a_r$ and $\varepsilon = \varepsilon_1 + \cdots + \varepsilon_r$, we then have each $a_i \in \{0, 1\} \subseteq \mathbb{Z}_{p_i}$. Selecting these in all possible ways, we see there are 2^r elements $a \in \mathbb{Z}_{n(r)}$ produced. Thus there are $(2^r)^2$ distinct pairs of these endomorphisms. Note also, if ε and η are endomorphisms of $\mathbb{Z}_{n(r)}$ with $\varepsilon(x) = ax$ and $\eta(x) = bx$, then $\varepsilon\eta(x) = abx = bax = \eta\varepsilon(x)$; thus composition of mappings is commutative in $\mathrm{End}(\mathbb{Z}_{n(r)}, +)$. It follows that if $\alpha \in \mathrm{Aut}(\mathbb{Z}_{n(r)}, +)$ and $\varepsilon \in \mathrm{End}(\mathbb{Z}_{n(r)}, +)$, we have $\alpha^{-1}\varepsilon\alpha = \varepsilon$. Therefore similarity classes of endomorphisms of $\mathbb{Z}_{n(r)}$ are singletons. Thus the 4^r pairs of endomorphisms we have generated are nonsimilar and, by Theorem 3.7, each such pair generates an associative interchange near ring based on A_r in a distinct isomorphism class. □

Theorem 5.11. *If $(A, +)$ is a finite abelian group of ppc-rank r, then there are at most 2^r isomorphism classes of interchange rings based on A whose multiplicative structure forms a band (that is, an idempotent semigroup). This bound is best possible in the sense that, for each $r > 0$, there exists a finite abelian group, A_r, of ppc-rank r with exactly 2^r isomorphism classes of associative interchange rings based on A_r.*

Proof. Since a band is a semigroup, we need only consider associative interchange rings. We know that an associative interchange ring based on A is constructed from a pair of commutating, idempotent endomorphisms of A. As seen above, this is similar to a pair (δ_1, δ_2) of idempotent diagonal endomorphisms of A for which each standard basis element is sent to either itself or zero. For the multiplicative structure to be idempotent, Proposition 4.2 tells us that $\alpha + \beta = \iota$, the identity mapping. Thus we know that $\delta_2 = \delta_1 - \iota$, that is, $\delta_2(e_i) = e_i$ if $\delta_1(e_i) = 0$ and $\delta_2(e_i) = 0$ if $\delta_1(e_i) = e_i$. Since there are two choices for the image of each e_i under δ_1, there are 2^r distinct mappings, δ_1. If the pair is to form an idempotent product, δ_2 is determined uniquely by δ_1.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Thus there are 2^r such pairs and, hence, at most 2^r isomorphism classes of interchange rings whose multiplicative structure is a band. To see that the bound is best possible in the sense claimed, for each $r > 0$, we consider the group A_r discussed in the proof of Theorem 5.10. We saw that there were exactly 2^r idempotent diagonal endomorphisms of A_r. Pairing each such δ with $\iota - \delta$ gives a set of 2^r pairs which produce, uniquely, all possible isomorphism classes of interchange rings whose multiplicative structure forms a band. □

6. Interchange rings based on elementary abelian p^n-groups

In the case of an elementary abelian p-group, A, we will calculate an exact number of associative interchange rings based on A. This number is a cubic polynomial in the ppc-rank of A. It turns out that we can carry out this programme for a moderately broader class of groups. Given a prime, p, and a positive integer, n, we call a finite abelian group, A, which is a direct sum of r copies of the cyclic group of order p^n an *elementary abelian p^n-group* of ppc-rank r. Note that when $n = 1$, A is an elementary abelian p-group. If A is an elementary abelian p^n-*group* of ppc-rank r, then, when A is written as a direct sum using the standard basis, $A = \langle e_1 \rangle \oplus \cdots \oplus \langle e_r \rangle$, each e_i has order p^n. In what follows we will maintain the convention that permutations, as well as all other functions, are composed on the left, thus $(\pi_1 \circ \pi_2)(x) = \pi_1(\pi_2(x))$.

Definition 6.1. Let p be a fixed prime, let n and r be fixed positive integers, and let A be an elementary abelian p^n-group of ppc-rank r. An $\alpha \in \mathrm{Aut}(A, +)$ is called a *permutation automorphism* of A whenever there exists a permutation, π, of the set $\{1, \ldots, r\}$ such that $\alpha(e_i) = e_{\pi(i)}$ for each i $(1 \leq i \leq r)$.

Note that for any permutation π, of the set $\{1, \ldots, r\}$, a permutation automorphism exists as given in the definition. Since $|e_{\pi(i)}| = p^n = |e_i|$, defining α as the extension of $\alpha(e_i) = e_{\pi(i)}$ always yields a homomorphism. It is a bijection since it acts by permuting the standard basis. The permutation automorphism associated with π will be denoted α_π. Note also that the permutation automorphisms of A form a subgroup of $\mathrm{Aut}(A, +)$, since $\alpha_\pi^{-1} = \alpha_{\pi^{-1}}$, and if π_1 and π_2 are permutations of $\{1, \ldots, r\}$, $\alpha_{\pi_1} \circ \alpha_{\pi_2} = \alpha_{\pi_1 \circ \pi_2}$.

Lemma 6.2. *If A is an elementary abelian p^n-group of ppc-rank r, $\alpha_\pi \in \mathrm{Aut}(A, +)$ is a permutation automorphism of A, and $\delta, \eta \in \mathrm{End}(A, +)$ with δ a diagonal endomorphism of A and η similar to δ under α_π, then η is a diagonal endomorphism of A.*

Proof. For each i $(1 \leq i \leq r)$, suppose that $\delta(e_i) = d_i e_i$. Since $\eta = \alpha_\alpha^{-1} \delta \alpha_\alpha$, it follows that $\eta(e_i) = \alpha_\pi^{-1} \delta \alpha_\pi(e_i) = \alpha_\pi^{-1} \delta(e_{\pi(i)}) = \alpha_\pi^{-1}(d_{\pi(i)} e_{\pi(i)}) = d_{\pi(i)} \alpha_\pi^{-1}(e_{\pi(i)}) = d_{\pi(i)} e_{\pi^{-1}\pi(i)} = d_{\pi(i)} e_i$. Therefore η is a diagonal endomorphism of A. □

If A is an elementary abelian p^n-group of ppc-rank r, given an integer s $(0 \leq s \leq r)$, we say that an idempotent diagonal endomorphism $\delta \in \mathrm{End}(A, +)$ is in *s-canonical form* if $\delta(e_i) = e_i$ for $0 \leq i \leq s$ and $\delta(e_i) = 0$ for $s < i \leq r$. Note that if δ is of this form and $s = 0$, then δ is the zero map, and if $s = r$, then δ is the identity map.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

If δ is an idempotent diagonal endomorphism of an elementary abelian p^n-group of ppc-rank r, we let $I(\delta) = \{i \in \{1, \dots, r\} : \delta(e_i) = e_i\}$. Note that δ is in s-canonical form if and only if $I(\delta) = \{1, \dots, s\}$.

PROPOSITION 6.3. *If A is an elementary abelian p^n-group of ppc-rank r and δ is an idempotent diagonal endomorphism of A, then there is an idempotent diagonal endomorphism η of A in s-canonical form, for $s = |I(\delta)|$, and a permutation automorphism α_π under which δ is similar to η.*

PROOF. Since δ is diagonal, for each i $(1 \le i \le r)$, there is a $d_i \in \mathbb{Z}_{|e_i|}$ with $\delta(e_i) = d_i e_i$, and since δ is idempotent, Lemma 5.3 implies that each $d_i \in \{0, 1\}$. If δ is the zero mapping or the identity mapping, then it is in s-canonical form for $s = 0$ and $s = r$, respectively. Selecting $\eta = \delta$ and α_π as the identity automorphism, our result follows. Thus we may assume that $I(\delta)$ is a proper, nonempty subset of $\{1, \dots, r\}$. Let π be any permutation of $\{1, \dots, r\}$ such that $\pi(\{1, \dots, s\}) = I(\delta)$. We will establish our result by letting $\eta = \alpha_\pi^{-1}\delta\alpha_\pi$ and showing that η is in s-canonical form. By Lemma 6.2 we know η is diagonal. For any e_i we have $\eta(e_i) = \alpha_\pi^{-1}\delta\alpha_\pi(e_i) = \alpha_\pi^{-1}\delta(e_{\pi(i)})$. It is clear that $\pi(i) \in I(\delta)$ if and only if $1 \le i \le s$. Therefore for $1 \le i \le s$, $\eta(e_i) = \alpha_\pi^{-1}\delta(e_{\pi(i)}) = \alpha_\pi^{-1}(e_{\pi(i)}) = e_{\pi^{-1}(\pi(i))} = e_i$, while for $s + 1 \le i \le r$, we have $\pi(i) \notin I(\delta)$ and, since $d_i \in \{0, 1\}$, it follows that $\delta(e_{\pi(i)}) = 0$. Therefore, $\eta(e_i) = \alpha_\pi^{-1}\delta(e_{\pi(i)}) = \alpha_\pi^{-1}(0) = 0$. This establishes that η is in s-canonical form, and Lemma 5.5 establishes that η is idempotent. □

Next we will show that, up to similarity, s-canonical form is unique.

PROPOSITION 6.4. *If A is an elementary abelian p^n-group, and δ and η are similar idempotent diagonal endomorphisms of A with δ in s-canonical form and η in t-canonical form, then $s = t$ and, hence, $\eta = \delta$.*

PROOF. Note that if $s = 0$ then δ is the zero map, which is similar only to itself. Since $\delta \sim \eta$, it follows that $\eta = \delta$, and therefore that $t = 0$, and our result follows. Similarly, if $t = r$, then δ is the identity mapping, and the result follows again. Assume then that $1 \le s < t < r$. Since δ and η are similar, there is an $\alpha \in \mathrm{Aut}(A, +)$ such that $\alpha\delta = \eta\alpha$. The automorphism α is determined by its action on the standard basis; therefore, for each i there exist $a_{ji} \in \mathbb{Z}_{|e_j|}$ $(1 \le j \le r)$ such that $\alpha(e_i) = \sum_{j=1}^{r} a_{ji}e_j$.

CLAIM. *For each $i > s$, $\alpha(e_i) \in \langle e_{t+1}, \dots, e_r \rangle$.*

PROOF OF CLAIM. Note that for $i > s$, $\alpha\delta(e_i) = \alpha(0) = 0$, while

$$\eta\alpha(e_i) = \eta\Big(\sum_{j=1}^{r} a_{ji}e_j\Big) = \sum_{j=1}^{r} a_{ji}\eta(e_j) = \sum_{j=1}^{t} a_{ji}e_j.$$

The last equality holds since we have assumed η to be in t-canonical form. Since $\alpha\delta = \eta\alpha$, this implies, for $i > s$, that $\sum_{j=1}^{t} a_{ji}e_j = 0$. Since the elements $\{e_1, \dots, e_t\}$

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

form a ppc-basis for A, they form an independent set, and it follows that, for each $i > s$ and $j \leq t$, we have $a_{ji} = 0$. Using this fact, we see that, for $i > s$,

$$\alpha(e_i) = \sum_{j=1}^{r} a_{ji}e_j = \sum_{j=1}^{t} a_{ji}e_j + \sum_{j=t+1}^{r} a_{ji}e_j = \sum_{j=t+1}^{r} a_{ji}e_j.$$

Thus, for $i > s$, $\alpha(e_i) \in \langle e_{t+1}, \ldots, e_r\rangle$ and our claim is established. □

It follows from the claim that the $\alpha\langle e_{s+1}, \ldots, e_r\rangle$ is a subgroup of $\langle e_{t+1}, \ldots, e_r\rangle$. Since α is an automorphism of A, it preserves ppc-rank on subgroups; thus we know that $r - s = \text{ppc-rank}\langle e_{s+1}, \ldots, e_r\rangle \leq \text{ppc-rank}\langle e_{t+1}, \ldots, e_r\rangle = r - t$. It follows that $s \geq t$, providing a contradiction to the original assumption that $s < t$. Therefore we can conclude that $s \geq t$. A symmetrical argument shows that $t \geq s$, and it follows that $s = t$. □

Corollary 6.5. *If A is an elementary abelian p^n-group of ppc-rank r, then there are exactly $r + 1$ distinct isomorphism classes of commutative, associative interchange rings based on A.*

Proof. Suppose that a pair (ε, η) of commuting, idempotent, endomorphisms of A generates a commutative, associative interchange ring. By Proposition 4.1, we have $\varepsilon = \eta$. When we put ε into s-canonical form, η is automatically put into the same form. By Propositions 6.3 and 6.4 we see that this generates a distinct isomorphism class of interchange rings for each value of s. Since s ranges from 0 to r, our result follows. □

If A is an elementary abelian p^n-group of ppc-rank r, δ is an idempotent diagonal endomorphism of A, and s, t_1, t_2 are integers such that $0 \leq t_1 \leq s \leq t_2 \leq r$, we say that δ is in *s, t_1, t_2-canonical form* when $\delta(e_i) = e_i$ if $0 \leq i \leq t_1$ and $s < i \leq t_2$ and when $\delta(e_i) = 0$ if $t_1 < i \leq s$ and $t_2 < i \leq r$. We introduce one further notation; for any integer s $(1 \leq s \leq r)$, let $I_{s,1}(\delta) = \{i \in \{1, \ldots, s\} : \delta(e_i) = e_i\}$ and $I_{s,2}(\delta) = \{i \in \{s + 1, \ldots, r\} : \delta(e_i) = e_i\}$.

Proposition 6.6. *If A is a finite elementary abelian p^n-group of ppc-rank r, δ is an idempotent diagonal endomorphism of A, and s $(0 \leq s \leq r)$ is an integer, then there exist an idempotent diagonal endomorphism η of A in s, t_1, t_2-canonical form for $t_1 = |I_{s,1}(\delta)|t_2 = s + |I_{s,2}(\delta)|$, and a permutation automorphism α_π such that δ is similar to η under α_π and, for $0 < s < r$, the subgroups $A_s = \langle e_1, \ldots, e_s\rangle$ and $B_s = \langle e_{s+1}, \ldots, e_r\rangle$ are invariant under α_π.*

Proof. If $s = 0$ then $I_{s,1}(\delta) = \varnothing$ and $I_{s,2}(\delta) = I(\delta)$, and our result follows immediately from Proposition 6.3. If $s = r$, then $I_{s,1}(\delta) = I(\delta)$ and $I_{s,2}(\delta) = \varnothing$, and the result again follows from Proposition 6.3. Thus we may assume that $0 < s < r$. Note that, by Lemma 5.5, since δ is idempotent, for each i we have $\delta(e_i) \in \{0, e_i\}$; therefore, A_s and B_s are both invariant under δ. Since $A = A_s \oplus B_s$ we can then write δ as the direct sum $\delta = \delta_1 + \delta_2$, where δ_1 and δ_2 are the restrictions of δ to A_s and B_s, respectively. Note that by Lemma 5.4, δ_1 and δ_2 are idempotent. Since $\delta(e_i) \in \{0, e_i\}$

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

the same is true of δ_1 and δ_2, thus they are diagonal as well. We then apply Proposition 6.3 to both $\delta_1 \in \mathrm{End}(A_s, +)$ and $\delta_2 \in \mathrm{End}(B_s, +)$. We then have idempotent diagonal endomorphisms $\eta_1 \in \mathrm{End}(A_s, +)$ in t_1-canonical form and $\eta_2 \in \mathrm{End}(B_s, +)$ in t_2'-canonical form, for $t_2' = t_2 - s(= |I_{s,2}(\delta)|)$, and permutation automorphisms $\alpha_{\pi_1} \in \mathrm{Aut}(A_s, +)$ and $\alpha_{\pi_2} \in \mathrm{Aut}(B_s, +)$ so that δ_1 is similar to η_1 under α_{π_1} and δ_2 is similar to η_2 under α_{π_2}. Let $\eta = \eta_1 + \eta_2 (\in \mathrm{End}(A, +))$ and $\alpha = \alpha_{\pi_1} + \alpha_{\pi_2}$ $(\in \mathrm{Aut}(A, +))$, and note that since α is defined as a direct product, the subgroups A_s and B_s are invariant under α. To complete the proof we need to establish that (i) η is in s, t_1, t_2-canonical form, (ii) δ is similar to η under α, and (iii) α is a permutation automorphism. To prove (i) we first calculate $\eta(e_i)$ for $1 \le i \le s$. Since $e_i \in A_s$, $\eta(e_i) = \eta_1(e_i)$. Since η_1 is in t_1-canonical form, we have $\eta(e_i) = e_i$ for $1 \le i \le t_1$ and $\eta(e_i) = 0$ for $t_1 < i \le s$. Now considering $\eta(e_i)$ for $s < i \le r$, we have $\eta(e_i) = \eta_2(e_i)$. Since η_2 is in t_2'-canonical form, we obtain $\eta(e_i) = e_i$ for $s < i \le t_2$ and $\eta(e_i) = 0$ for $t_2 < i \le r$. Thus η is in s, t_1, t_2-canonical form and (i) is established. To prove (ii) we note that $\alpha^{-1}\delta\alpha = (\alpha_1 + \alpha_2)^{-1}(\delta_1 + \delta_2)(\alpha_1 + \alpha_2) = {\alpha_1}^{-1}\delta_1\alpha_1 + {\alpha_2}^{-1}\delta_2\alpha_2 = \eta_1 + \eta_2 = \eta$. To establish (iii) let π be the permutation of $\{1, \ldots, r\}$ which acts as π_1 on $\{1, \ldots, s\}$ and as π_2 on $\{s+1, \ldots, r\}$. Thus we have $\alpha = \alpha_{\pi_1} + \alpha_{\pi_2} = \alpha_\pi$, a permutation automorphism of A. □

If (δ_1, δ_2) is a pair of idempotent diagonal endomorphisms of A, s, t_1, and t_2 are integers with $1 \le t_1 \le s \le t_2 \le r$ such that δ_1 is in s-canonical form and δ_2 in s, t_1, t_2-canonical form, then we say that the pair (δ_1, δ_2) is in *canonical form*.

Proposition 6.7. *If A is an elementary abelian p^n-group of ppc-rank r, and (δ_1, δ_2) is a pair of idempotent diagonal endomorphisms of A, then for $s = |I(\delta_1)|$, $t_1 = |I_{s,1}(\delta_2)|$ and $t_2 = |I_{s,2}(\delta_2)|$, there exists a pair of idempotent diagonal endomorphisms of A, (η_1, η_2), such that $(\delta_1, \delta_2) \sim (\eta_1, \eta_2)$, η_1 is in s-canonical form, and η_2 is in s, t_1, t_2-canonical form. In other words, any pair of idempotent diagonal endomorphism of A can be put into canonical form.*

Proof. Focusing first on δ_1, by Proposition 6.3, we know that there is an idempotent diagonal endomorphism η_1 of A in s-canonical form with δ_1 similar to η_1 under a permutation automorphism α. Letting $\delta_2' = \alpha^{-1}\delta_2\alpha$ we see, by Lemma 6.2, that δ_2' is diagonal and, by Lemma 5.7, δ_2' is idempotent. Thus we have (δ_1, δ_2) similar under a permutation automorphism to an idempotent diagonal pair (η_1, δ'_2) with η_1 in s-canonical form. Applying Proposition 6.6 to δ_2' with $s = |I(\delta_1)|$, we have the existence of an idempotent diagonal endomorphism η_2 of A in s, t_1, t_2-canonical form and a permutation automorphism α_π such that δ_2' is similar to η_2 under α_π with the subgroups $A_s = \langle e_1, \ldots, e_s \rangle$ and $B_s = \langle e_{s+1}, \ldots, e_r \rangle$ invariant under α_π.

Claim. *α_π commutes with η_1.*

Proof of Claim. Note that since A_s is invariant under α_π, for $1 \le i \le s$, we have $e_{\pi(i)} = \alpha_\pi(e_i) \in A_s$. It follows that $\eta_1(e_{\pi(i)}) = e_{\pi(i)}$. Therefore $\eta_1\alpha_\pi(e_i) = \eta_1(e_{\pi(i)}) = e_{\pi(i)}$, while $\alpha_\pi\eta_1(e_i) = \alpha_\pi(e_i) = e_{\pi(i)}$. Thus α_π commutes with η_1 on A_s. Since B_s is invariant

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

under α_π, for $s < i \le r$, we have $e_{\pi(i)} = \alpha_\pi(e_i) \in B_s$. Thus $\eta_1(e_{\pi(i)}) = 0$. Thus we have $\eta_1\alpha_\pi(e_i) = \eta_1(e_{\pi(i)}) = 0$, while $\alpha_\pi\eta_1(e_i) = \alpha_\pi(0) = 0$. Thus we see that α_π commutes with η_1 on B_s and the claim follows. □

Since $(\delta_1, \delta_2) \sim (\eta_1, \delta'_2)$, to complete the proof we must show that (η_1, δ'_2) is similar to (η_1, η_2). Since α_π commutes with η_1, we have $\alpha_\pi^{-1}(\eta_1, \delta'_2)\alpha_\pi = (\alpha_\pi^{-1}\eta_1\alpha_\pi, \alpha_\pi^{-1}\delta'_2\alpha_\pi) = (\eta_1, \eta_2)$. □

Proposition 6.8. *If A is an elementary abelian p^n-group of ppc-rank r, (δ_1, δ_2) and (η_1, η_2) are pairs of idempotent diagonal endomorphisms of A, s, t_1, t_2, s', t'_1, and t'_2 are integers with $1 \le t_1 \le s \le t_2 \le r$ and $1 \le t'_1 \le s' \le t'_2 \le r$, with δ_1 in s-canonical form, δ_2 in s, t_1, t_2-canonical form, η_1 in s'-canonical form, and η_2 in s', t'_1, t'_2-canonical form, and $(\delta_1, \delta_2) \sim (\eta_1, \eta_2)$, then $s = s', t_1 = t'_1$, and $t_2 = t'_2$. Thus if both pairs are in canonical form and similar, they are equal.*

Proof. Let $\alpha \in \mathrm{Aut}(A, +)$ so that $\alpha^{-1}(\delta_1, \delta_2)\alpha = (\eta_1, \eta_2)$. Since δ_1 is similar to η_1, Proposition 6.4 implies that $s = s'$ and $\delta_1 = \eta_1$. Since $\alpha^{-1}\delta_1\alpha = \eta_1 = \delta_1$, it follows that α commutes with δ_1. Henceforth we will write s' as s and η_1 as δ_1. For each i and j $(1 \le i, j \le r)$, let $a_{ji} \in \mathbb{Z}_{|e_i|}$ so that $\alpha(e_i) = \sum_{j=1}^{r} a_{ji}e_j$.

Claim. *α is invariant on A_s and B_s.*

Proof of Claim. Note that $\delta_1(e_i) = e_i$ for $1 \le i \le s$. Since α commutes with δ_1, we have

$$\begin{aligned}
\alpha(e_i) = \alpha\delta_1(e_i) &= \delta_1\alpha(e_i) \\
&= \delta_1\Big(\sum_{i=1}^{r} a_{ji}e_j\Big) \\
&= \sum_{i=1}^{r} a_{ji}\delta_1(e_j) \\
&= \sum_{i=1}^{s} a_{ji}\delta_1(e_j) + \sum_{i=s+1}^{r} a_{ji}\delta_1(e_j) \\
&= \sum_{i=1}^{s} a_{ji}e_j + \sum_{i=s+1}^{r} a_{ji}(0) \\
&= \sum_{j=1}^{s} a_{ji}e_j \in A_s.
\end{aligned}$$

For each $a \in A_s$, there exist $c_i \in \mathbb{Z}_{|e_i|}$ such that $a = \sum_{i=1}^{s} c_ie_i$. Therefore $\alpha(a) = \alpha(\sum_{i=1}^{s} c_ie_i) = \sum_{i=1}^{s} c_i\alpha(e_i) \in A_s$. Next suppose that $s < i \le r$. We then have $\delta_1(e_i) = 0$.

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Since α commutes with δ_1, we obtain

$$\begin{aligned} 0 = \alpha(0) &= \alpha\delta_1(e_i) = \delta_1\alpha(e_i) \\ &= \delta_1\Big(\sum_{j=1}^{r} a_{ji}e_j\Big) \\ &= \sum_{j=1}^{r} a_{ji}\delta_1(e_j) = \sum_{j=1}^{s} a_{ji}\delta_1(e_j) + \sum_{j=s+1}^{r} a_{ji}\delta_1(e_j) \\ &= \sum_{j=1}^{s} a_{ji}e_j + \sum_{j=s+1}^{r} a_{ji}(0) = \sum_{j=1}^{s} a_{ji}e_j. \end{aligned}$$

Since $\sum_{j=1}^{s} a_{ji}e_j = 0$, we conclude that for $s < i \le r$ and $1 \le j \le s$, we have $a_{ji} = 0$. Thus for $s < i \le r$,

$$\alpha(e_i) = \sum_{j=1}^{s} a_{ji}e_j + \sum_{j=s+1}^{r} a_{ji}e_j = \sum_{j=1}^{s}(0)e_j + \sum_{j=s+1}^{r} a_{ji}e_j = \sum_{j=s+1}^{r} a_{ji}e_j \in B_s.$$

Thus the claim is established. □

Note that any diagonal endomorphism is invariant on both A_s and B_s since it sends e_i to some d_ie_i. Thus we may decompose α, δ_2 and η_2 over the direct sum $A = A_s \oplus B_s$ as $\alpha = \alpha_1 + \alpha_2$, $\delta_2 = \delta_{2,1} + \delta_{2,2}$ and $\eta_2 = \eta_{2,1} + \eta_{2,2}$. Since $\alpha^{-1}\delta_2\alpha = \eta_2$, we can rewrite this as $(\alpha_1 + \alpha_2)^{-1}(\delta_{2,1} + \delta_{2,2})(\alpha_1 + \alpha_2) = \eta_{2,1} + \eta_{2,2}$. Thus we conclude that $\alpha_1^{-1}\delta_{2,1}\alpha_1 = \eta_{2,1}$ and $\alpha_1^{-1}\delta_{2,2}\alpha_1 = \eta_{2,2}$. Note that $\delta_{2,1}$ and $\eta_{2,1}$ are idempotent diagonal endomorphisms of A_s, an elementary abelian p^n-group of ppc-rank s, which are similar under $\alpha_1 \in \mathrm{Aut}(A_s, +)$. Note also that $\delta_{2,1}$ is in t_1-canonical form and $\eta_{2,1}$ is in t_1'-canonical form. Applying Proposition 6.4 to $\delta_{2,1}$ and $\eta_{2,1}$, we see that $t_1 = t_1'$ and, in fact, $\delta_{2,1} = \eta_{2,1}$. Applying a similar argument to $\delta_{2,2}$ and $\eta_{2,2}$, which are idempotent diagonal endomorphisms of B_s in t_2- and t_2'-canonical form, respectively, we see that $t_2 = t_2'$ and $\delta_{2,2} = \eta_{2,2}$. It follows that $\delta_2 = \delta_{2,1} + \delta_{2,2} = \eta_{2,1} + \eta_{2,2} = \eta_2$ as required. □

Corollary 6.9. *If $(A, +)$ is an elementary abelian p^n-group of ppc-rank r and $(\varepsilon_1, \varepsilon_2)$ is a pair of commuting, idempotent endomorphisms of A, then there exists a unique pair (δ_1, δ_2) of commuting, idempotent diagonal endomorphisms which is similar to $(\varepsilon_1, \varepsilon_2)$ and in canonical form.*

Proof. Theorem 5.9 and Proposition 6.6 show that $(\varepsilon_1, \varepsilon_2)$ is similar to a pair (δ_1, δ_2) of idempotent diagonal endomorphisms in canonical form. Lemma 5.6 shows that δ_1 and δ_2 commute. Proposition 6.7 shows that the pair is unique. □

Theorem 6.10. *If $(A, +)$ is an elementary abelian p^n-group of ppc-rank r, then there are exactly $\frac{1}{6}(r+1)(r+2)(r+3)$ isomorphism classes of associative interchange rings based on A.*

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

Proof. Theorem 4.3 says that each associative, interchange ring based on A is formed from a pair, $(\varepsilon_1, \varepsilon_2)$, of commuting idempotent endomorphisms of A. These pairs may yield isomorphic interchange rings; however, Theorem 3.5 shows that isomorphism of these interchange rings is determined exactly up to similarity of these pairs. Corollary 6.9 implies that there is exactly one pair, (δ_1, δ_2), of diagonal endomorphisms in canonical form which is similar to $(\varepsilon_1, \varepsilon_2)$. Thus the isomorphism class of the associative interchange ring generated from $(\varepsilon_1, \varepsilon_2)$ is the same as that for (δ_1, δ_2), and (δ_1, δ_2) is the only pair in canonical form which generates an element of that isomorphism class. Note that Lemma 5.6 implies that (δ_1, δ_2) is a commuting pair. Thus we can count the distinct isomorphism classes of associative interchange rings based on A by counting the number of distinct pairs (δ_1, δ_2) of diagonal endomorphism in canonical form. Since δ_1 is in s-canonical form for some $s\,(1 \le s \le r)$, we see there are $r + 1$ possibilities for δ_1. For each of these the δ_2 is in s, t_1, t_2-canonical form with $1 \le t_1 \le s \le t_2 \le r$. With s fixed we can vary t_1 from 0 to s and, independently, vary t_2 from s to r. Thus for each choice of δ_1 there are $(s + 1)(r - s + 1)$ choices for δ_2. Thus we have exactly $\sum_{s=0}^{r} (s + 1)(r - s + 1)$ distinct pairs (δ_1, δ_2), and this corresponds to the number of distinct isomorphism classes of associative interchange rings based on A. Induction on r shows that this bound has the lovely closed form $\frac{1}{6}(r + 1)(r + 2)(r + 3)$. □

There are eight isomorphism classes of rings based on the Klein 4-group, V. In the next example we will find that there are exactly ten isomorphism classes of associative interchange rings based on V.

Example 6.11. Interchange rings based on the Klein 4-group. The Klein 4-group is $V = \{0, 1, 2, 3\}$ with Cayley table

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

We denote the endomorphism $\varepsilon : V \to V$ sending $0 \mapsto 0, 1 \mapsto x, 2 \mapsto y$, and $3 \mapsto z$ by $\varepsilon = (0xyz)$. $\mathrm{End}(V, +)$ has order 16 with six automorphisms and ten proper endomorphisms: $\mathrm{End}(V, +) = \{\alpha_0 = (0123), \alpha_1 = (0132), \alpha_2 = (0213), \alpha_3 = (0231), \alpha_4 = (0312), \alpha_5 = (0321), \varepsilon_0 = (0000), \varepsilon_1 = (0011), \varepsilon_2 = (0022), \varepsilon_3 = (0033), \varepsilon_4 = (0101), \varepsilon_5 = (0110), \varepsilon_6 = (0202), \varepsilon_7 = (0220), \varepsilon_8 = (0303), \varepsilon_9 = (0330)\}$. Since $(V, +)$ is abelian, each pair of endomorphisms is image-commuting. The set of idempotents in $\mathrm{End}(V, +)$ is $E = \{\alpha_0, \varepsilon_0, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_7, \varepsilon_8\}$. We wish to list a complete set of nonsimilar pairs of commuting idempotents to exhaust the isomorphism classes of associative interchange rings based on V. We may begin with ε_0 and α_0, each of which commutes with every endomorphism and has a singleton similarity class. Thus we will include the commuting pairs $(\varepsilon_0, \varepsilon_0)$, (α_0, α_0), $(\alpha_0, \varepsilon_0)$, $(\varepsilon_0, \alpha_0)$ in our list. A straightforward calculation shows that the endomorphisms $E' = \{\varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_7, \varepsilon_8\}$

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

are similar to each other. Thus, under similarity, the pairs of the form $(\gamma_0, \varepsilon_i)$ with $\gamma_0 \in \{\alpha_0, \varepsilon_0\}$ reduce to $(\alpha_0, \varepsilon_2), (\varepsilon_2, \alpha_0), (\varepsilon_0, \varepsilon_2), (\varepsilon_2, \varepsilon_0)$. Thus we will include these four pairs as well.

We find that $\varepsilon_2\varepsilon_4 = \varepsilon_4\varepsilon_2$, $\varepsilon_3\varepsilon_5 = \varepsilon_5\varepsilon_3$ and $\varepsilon_7\varepsilon_8 = \varepsilon_8\varepsilon_7$ are the only pairs from E' which commute. Furthermore, we have $\alpha_1^{-1}(\varepsilon_2, \varepsilon_4)\alpha_1 = (\varepsilon_3, \varepsilon_5)$ and $\alpha_5^{-1}(\varepsilon_2, \varepsilon_4)\alpha_5 = (\varepsilon_7, \varepsilon_8)$. Thus the only candidates for nonsimilar pairs here are $(\varepsilon_2, \varepsilon_4)$ and $(\varepsilon_4, \varepsilon_2)$. Thus we have found a complete set of ten pairs of commuting idempotent endomorphisms of $(V, +)$ which are nonsimilar and represent each isomorphism class of associative interchange rings based on the Klein 4-group. Among the ten semigroups produced, $(\varepsilon_0, \varepsilon_0)$ generates the zero semigroup, (α_0, α_0) produces an improper interchange ring with the product identical to the sum, and $(\alpha_0, \varepsilon_0)$ and $(\varepsilon_0, \alpha_0)$ generate the left- and right-zero semigroups. The remaining six pairs produce more interesting products. For example, selection of the pair $(\varepsilon_7, \varepsilon_7)$ yields the interchange ring $(V, +, \bullet)$ with multiplication having the Cayley table

$\bullet$	0	1	2	3
0	0	2	2	0
1	2	0	0	2
2	2	0	0	2
3	0	2	2	0

Note that for $p = 2$ and $n = 1$, V is a p^n-group of ppc-rank $r = 2$; thus Theorem 6.10 predicts exactly $\frac{1}{6}(2 + 1)(2 + 2)(3 + 2) = 10$ isomorphism classes of associative interchange rings, and this is what we have found.

7. Interchange ring theory

Since interchange rings are as yet uninvestigated, it would seem natural to ask how much of standard ring theory would transfer over to interchange rings. In this section we will make some elementary first steps in this direction. For full generality we will allow the additive group to be nonabelian, thus we state our theorems for interchange near rings and they will hold for interchange rings as well. As in universal algebra, it is natural to identify subobjects as follows.

Definition 7.1. If $(R, +, \bullet)$ is an interchange near ring and R' is a nonempty subset of R, we say that R' is an *interchange near subring* of R, denoted $R' \leq R$, when $(R', +)$ is a subgroup of $(R, +)$ and $(R', \bullet)$ is a submagma of $(R, \bullet)$.

As with rings, the trivial interchange ring $\{0\}$ and the whole of R are interchange near subrings of R. To see a nontrivial example, we may take $(R, +, \bullet)$ to be one of the associative interchange rings found in Example 6.11. Here the additive structure is the Klein 4-group and the multiplication is defined as $x \bullet y = \varepsilon_7(x + y)$. Letting $R' = \{0, 2\}$, it is easy to see that $R' \leq R$. Note that this interchange subring is improper. To see an example of a proper interchange near subring, we refer to Example 3.9, where the

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

additive structure is $(S_3, +)$ and the product is defined as $x \bullet y = \alpha_3(x) + \varepsilon_0(y) = \alpha_3(x)$. Note that $\{0, 1, 2\}$ is a proper, nonzero interchange near subring of $(S_3, +)$.

In groups and rings congruences correspond to special subobjects, namely normal subgroups and ideals, while for semigroups and lattices this is not the case. It is interesting to notice that for interchange rings congruences correspond to special subobjects. Thus we can form quotient interchange rings using these.

DEFINITION 7.2. If $(R, +, \bullet)$ is an interchange near ring, a subset I of R is an *ideal* of R, denoted $I \triangleleft R$, if and only if $(I, +, \bullet)$ is an interchange near subring of $(R, +, \bullet)$ and $(I, +)$ is a normal subgroup of $(R, +)$.

We form a congruence relation, C, on $(R, +)$ using the ideal, I, in the standard way: for each $x, y \in I$, $(x, y) \in C$ if and only if $x - y \in I$.

THEOREM 7.3. *Let $(R, +, \bullet)$ be an interchange near ring, and $I \triangleleft R$. Then the relation, C, is a congruence relation on $(R, +, \bullet)$.*

PROOF. Since we have selected N as a normal subgroup of R, it follows that C is an equivalence relation on R and that it acts as a congruence on $(R, +)$. It remains to show that it is a congruence on $(R, \bullet)$. So let $x_1, x_2, y_1, y_2 \in R$ so that $x_1 - x_2, y_1 - y_2 \in I$. Therefore there exist $i, i' \in I$ such that $x_1 = x_2 + i$ and $y_1 = y_2 + i'$. Therefore, by the interchange law, $x_1 \bullet y_1 = (x_2 + i) \bullet (y_2 + i') = (x_2 \bullet y_2) + (i \bullet i')$. By hypothesis $i \bullet i' \in I$, thus we have $x_1 \bullet y_1 - x_2 \bullet y_2 \in I$, as required. □

Universal algebraic results imply that we can form a unique quotient interchange near ring, R/I. It is routine to check that the fundamental homomorphism theorem and the three isomorphism theorems hold in this case. It is also possible to prove, by a straightforward analogy with ring theory, that an ideal I is maximal if and only if R/I is simple.

Further points of departure are the investigation of structures like polynomial rings and group rings using interchange rings. It is interesting to note that when one forms $n \times n$ matrices over an interchange (near) ring, $M_n(R)$, a natural definition of matrix addition and multiplication makes this into an interchange (near) ring as well.

DEFINITION 7.4. If $(R, +, \bullet)$ is an interchange (near) ring and $M_n(R)$ is the set of $n \times n$ matrices over R, we define the *sum* and *product* of matrices $A = (a_{ij})$ and $B = (b_{ij})$ in $M_n(R)$, respectively, as $A + B = (a_{ij} + b_{ij})$ and $A \bullet B = (\sum_{k=1}^{n} a_{ik} \bullet b_{kj})$.

It follows by a simple induction on n that $x_1 \bullet y_1 + x_2 \bullet y_2 + \cdots + x_n \bullet y_n = (x_1 + x_2 + \cdots + x_n) \bullet (y_1 + y_2 + \cdots + y_n)$.

THEOREM 7.5. *If $(R, +, \bullet)$ is an interchange (near) ring, then $(M_n(R), +, \bullet)$ is an interchange (near) ring.*

PROOF. Clearly $(M_n(R), +)$ is a group and is abelian if $(R, +)$ is abelian. It remains to verify the interchange law: $A \bullet B + C \bullet D = (\sum_{k=1}^{n} a_{ik} \bullet b_{kj}) + (\sum_{k=1}^{n} c_{ik} \bullet d_{kj}) = \sum_{k=1}^{n} (a_{ik} \bullet b_{kj} + c_{ik} \bullet d_{kj}) \underset{IL}{=} \sum_{k=1}^{n} ((a_{ik} + c_{kj}) \bullet (b_{ik} + d_{kj})) = (A + C) \bullet (B + D)$. □

Thus there are many avenues open to explore ...

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press

References

[1] D. DeWolf, 'On double inverse semigroups', Master's Thesis, Dalhousie University, Halifax, Nova Scotia, 2013, page 95.
[2] B. Eckmann and P. Hilton, 'Group-like structures in general categories. I. Multiplications and comultiplications', *Math. Ann.* **145** (1961), 227–255.
[3] C. C. Edmunds, 'Constructing double magma on groups using commutation operations', *Canad. Math. Bull.* (to appear) arXiv:1308.2691.
[4] K. Hoffman and R. Kunze, *Linear Algebra* (Prentice-Hall, Inc., Englewood Cliffs, NJ, 1961).
[5] J. Kock, 'Note on commutativity of double semigroups and two-fold monodial categories', *J. Homotopy Relat. Struct.* **2**(2) (2007), 217–228.
[6] J.-L. Loday and B. Vallette, *Algebraic Operands*, Grundlehren der Mathematischen Wissenschaften, 346 (Springer, Heidelberg, 2012).
[7] N. H. McCoy, *Introduction to Modern Algebra* (Allyn and Bacon, Boston, 1975).

CHARLES C. EDMUNDS, Mount Saint Vincent University,
Mathematics, 166 Bedford Highway, Halifax, Nova Scotia, Canada B3M 2J6
e-mail: cedmunds6868@gmail.com

https://doi.org/10.1017/S1446788716000112 Published online by Cambridge University Press