dMFA
ARS MATHEMATICA CONTEMPORANEA
Also available at http://amc.imfm.si
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 4 (2011) 329–349

Decomposition of skew-morphisms of cyclic groups

István Kovács *
FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia
Roman Nedela †
Institute of Mathematics, Slovak Academy of Science, Ďumbierska 1, 975 49 Banská Bystrica, Slovakia

Received 10 December 2009, accepted 16 July 2011, published online 1 October 2011

Abstract

A skew-morphism of a group H is a permutation σ of its elements fixing the identity such that for every $x, y \in H$ there exists an integer k such that $\sigma(xy) = \sigma(x)\sigma^k(y)$. It follows that group automorphisms are particular skew-morphisms. Skew-morphisms appear naturally in investigations of maps on surfaces with high degree of symmetry, namely, they are closely related to regular Cayley maps and to regular embeddings of the complete bipartite graphs. The aim of this paper is to investigate skew-morphisms of cyclic groups in the context of the associated Schur rings. We prove the following decomposition theorem about skew-morphisms of cyclic groups $\mathbb{Z}_n$: if $n = n_1n_2$ such that $(n_1, n_2) = 1$, and $(n_1, \phi(n_2)) = (\phi(n_1), n_2) = 1$ (ϕ denotes Euler's function) then all skew-morphisms σ of $\mathbb{Z}_n$ are obtained as $\sigma = \sigma_1 \times \sigma_2$, where σ_i are skew-morphisms of $\mathbb{Z}_{n_i}$, $i = 1, 2$. As a consequence we obtain the following result: All skew-morphisms of $\mathbb{Z}_n$ are automorphisms of $\mathbb{Z}_n$ if and only if $n = 4$ or $(n, \phi(n)) = 1$.

Keywords: Cyclic group, permutation group, skew-morphism, Schur ring.

Math. Subj. Class.: 05C25, 05E18

1 Introduction

Let G be a group with identity element e. A nonidentity permutation σ of G with finite order $\mathrm{ord}(\sigma) = m$ is said to be a *skew-morphism* of G if there exists a function π from G to $\{1, \ldots, m\}$ such that

*Supported in part by "ARRS – Agencija za raziskovanje Republike Slovenije", program no. P1-0285.
†Suported by the Slovak Ministry of Education, grant VEGA 2/5132/26.
E-mail addresses: istvan.kovacs@upr.si (István Kovács), nedela@savbb.sk (Roman Nedela)

1. $\sigma(e) = e$, and
2. $\sigma(xy) = \sigma(x)\sigma^{\pi(x)}(y)$ for all $x, y \in G$.

The function π is called the *power function* of σ. For example, all automorphisms of G are skew-morphisms, and these can be characterised as those having power function $\pi(x) = 1$ for all $x \in G$. One can prove that the above definition of skew-morphism is equivalent to the one given in the abstract. We adopt the terminology *pure skew-morphism* for a skew-morphism which is not an automorphism of G. Following [7], we denote by $\mathrm{Skew}(G)$ the set of all skew-morphisms of G.

The notion of a skew-morphism was introduced by Jajcay and Širáň in [7] in the context of regular Cayley maps. Let G be a finite group and ρ be a cyclic permutation of a set of generators X of G closed under taking inverses. The pair (G, ρ) determines a 2-cell embedding of the (right) Cayley graph $Cay(G; X)$ into an orientable surface, where the cyclic permutation of arcs based at a vertex is induced by ρ and G. The corresponding map is called the Cayley map $CM(G; \rho)$. By definition, the group of left translations G_L acts as a group of map automorphisms of $CM(G; \rho)$. It follows that Cayley maps are vertex-transitive. Jajcay and Širáň proved that the map automorphism group of $CM(G; \rho)$ is regular on arcs if and only if ρ extends to a skew-morphism σ of G. Moreover, the map automorphism group of the regular Cayley map $CM(G; \rho)$ is a product $G_L\langle\sigma\rangle$. For more details we refer the reader to the papers [3, 4, 7]. In particular, an ongoing project of Conder and Tucker is aimed towards a classification of all regular Cayley maps coming from cyclic groups, equivalently, this requires to understand skew-morphisms of $\mathbb{Z}_n$ admitting an orbit T for which $T = T^{-1}$ and T generates $\mathbb{Z}_n$. Note that there are skew-morphisms of $\mathbb{Z}_n$ with no such orbit. Skew-morphisms of cyclic groups appear in the study of regular embeddings of complete bipartite graphs as well. More precisely, a classification of regular embeddings of $K_{n,n}$ is equivalent to the description of the set of all skew-morphisms σ of $\mathbb{Z}_n$ whose order divides n, and whose power function π satisfies $\pi(x) = -\sigma^{-x}(-1)$ for all $x \in \mathbb{Z}_n$ (see [14, 12]). Skew-morphisms of $\mathbb{Z}_n$ posessing these properties are called *n-admissible* in [12]. A classification of regular embeddings of $K_{n,n}$ was completed recently by Jones [8]; this result was preceeded by several papers treating partial cases (see [5, 6, 9, 10]). In particular, a formula enumerating all n-admissible skew-morphisms in $\mathrm{Skew}(\mathbb{Z}_n)$ can be found in [8].

In this paper we consider skew-morphisms of $\mathbb{Z}_n$ with no restriction. The set of all skew-morphisms of $\mathbb{Z}_n$ will be denoted by $\mathrm{Skew}(\mathbb{Z}_n)$. For $i = 1, 2$, let σ_i be a permutation of $\mathbb{Z}_{n_i}$. The *direct product* $\sigma_1 \times \sigma_2$ is the permutation of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ defined as $(\sigma_1 \times \sigma_2)\colon (x_1, x_2) \mapsto (\sigma_1(x_1), \sigma_2(x_2))$ for all $(x_1, x_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Notice that if σ_i is a skew-morphism of $\mathbb{Z}_{n_i}$ for both $i = 1, 2$, $\sigma_1 \times \sigma_2$ is not necessarily a skew-morphism of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. In what follows ϕ denotes Euler's function.

In this paper we prove the following decomposition theorem.

Theorem 1.1. *Let n be a natural number which admits a decomposition $n = n_1n_2$, where $(n_1, n_2) = 1$ and $(n_1, \phi(n_2)) = (\phi(n_1), n_2) = 1$. Then $\sigma \in \mathrm{Skew}(\mathbb{Z}_n)$ if and only if $\sigma = \sigma_1 \times \sigma_2$, and $\sigma_i \in \mathrm{Skew}(\mathbb{Z}_{n_i})$ for $i = 1, 2$.*

In proving Theorem 1.1 our main tool is to study the permutation group $G = \langle(\mathbb{Z}_n)_L, \sigma\rangle \leq \mathrm{Sym}(\mathbb{Z}_n)$, where $(\mathbb{Z}_n)_L$ is the left regular representation of $\mathbb{Z}_n$. In particular, we study the transitivity module over $\mathbb{Z}_n$ induced by $\langle\sigma\rangle$, to which we shall also refer as the *S-ring*

generated by σ, and denote it by $V(\sigma)$. At this point we remark that, the transitivity modules over $\mathbb{Z}_n$ which are induced by cyclic permutation groups with a faithful orbit are, in general, not known. To give a description of these S-rings seems to be an interesting problem in the theory of S-rings over cyclic groups.

An outline of the paper is as follows. Section 2 contains definitions and facts on skew-morphisms and S-rings needed for further use. In Sections 3-5 we consider the S-rings $V(\sigma)$, $\sigma \in \mathrm{Skew}(\mathbb{Z}_n)$. In Section 3 we apply the structure theorems of Evdokimov and Ponomarenko to the S-rings $V(\sigma)$ and discuss some consequences for the skew-morphisms σ. In Sections 4 and 5 we restrict to special orders n. In Section 4 we set $n = p^e$, p is an odd prime, and prove that the S-rings $V(\sigma)$ in this case coincide with those generated by group automorphisms (see Theorem 4.1). This result is used to construct the whole set $\mathrm{Skew}(\mathbb{Z}_{p^2})$. In Section 5 we set $n = pq$, where p, q are distinct primes. We first determine all S-rings $V(\sigma)$, and using this result we construct the whole set $\mathrm{Skew}(\mathbb{Z}_{pq})$. Theorem 1.1 is proved in Section 6.

2 Preliminaries

1. Skew-morphisms

First we summarize some properties of skew-morphisms proved in [7].

Proposition 2.1. *Let σ be a skew-morphism of a group H and let π be the power function of σ. Then the following hold.*

(i) For all $k \geq 1$, and all $x, y \in H$, $\sigma^k(xy) = \sigma^k(x)\sigma^{\sum_{i=0}^{k-1} \pi(\sigma^i(x))}(y)$.

(ii) The set $\ker \pi = \{x \in H : \pi(x) = 1\}$ is a subgroup of H.

(iii) For all $x, y \in G$, $\pi(x) = \pi(y)$ if and only if x and y belong to the same right coset of the subgroup $\ker \pi$ in H.

For an arbitrary group H and $h \in H$, let h_L be the permutation in $\mathrm{Sym}(H)$ defined by $h_L(x) = hx, x \in H$. Thus $H_L = \{h_L \mid h \in H\}$ is the *left regular representation* of H. Throughout the paper a permutation group $G \leq \mathrm{Sym}(H)$ with $H_L \leq G$ will be referred to as an *overgroup* of H_L in $\mathrm{Sym}(H)$. Skew-morphisms of H appear naturally in the investigation of *overgroups* of H_L in $\mathrm{Sym}(H)$ with cyclic point stabilizers. The following proposition relates skew-morphisms of groups and products of groups, where one of the factors is cyclic.

Proposition 2.2. *Let G be an overgroup of H_L in $\mathrm{Sym}(H)$, and G_e be the stabilizer of e in G. If G_e is a cyclic group, then any generator σ of G_e is a skew-morphism of H. Conversely, if σ is a skew-morphism of a group H, then the permutation group $G = \langle H_L, \sigma \rangle$ has point stabilizer $G_e = \langle \sigma \rangle$.*

Proof. Let $G_e = \langle \sigma \rangle$. By the assumptions G is a product $G = G_e H_L = H_L G_e$. It follows that for every $x \in G$ there exists a unique integer k, $1 \leq k < \mathrm{ord}(\sigma)$, and a unique $y \in H$ such that $\sigma x_L = y_L \sigma^k$. Setting $y = \sigma(x)$ and $k = \pi(x)$ we get the identity

$$\sigma x_L = \sigma(x)_L \sigma^{\pi(x)}. \tag{2.1}$$

Let us fix x and apply the above permutations to an arbitrary element $y \in H$. Then we obtain that

$$\sigma(xy) = (\sigma x_L)(y) = \left(\sigma(x)_L \sigma^{\pi(x)}\right)(y) = \sigma(x)\sigma^{\pi(x)}(y).$$

Thus σ is a skew-morphism of H.

Vice-versa, if σ is a skew-morphism then the equation (2.1) holds proving $G = \langle\sigma\rangle H_L = H_L\langle\sigma\rangle$. It follows that $H_L \leq \langle\sigma\rangle H_L \leq Sym(H_L)$. Hence, $G = \langle\sigma\rangle H_L$ is an overgroup of H_L with the point stabilizer $G_e = \langle\sigma\rangle$. □

Following [4], we shall refer to the group $\langle H_L, \sigma\rangle$ in (ii) as the *skew product group* induced by σ.

Corollary 2.3. *Let σ be a skew-morphism of a group H, and T be an orbit of $\langle\sigma\rangle$ such that $\langle T\rangle = H$. Then $\langle\sigma\rangle$ acts faithfully on T. In particular,* $\mathrm{ord}(\sigma) = |T|$.

Remark. In the case where H is an abelian group we will consider the right action of permutations of H, that is, the product $\pi_1\pi_2$ of two permutations evaluated from the left to the right; in this case we write $x\,\pi_i$ (or ocasionally x^{π_i}) for the image $\pi_i(x), x \in H$, and we have $x\,(\pi_1\pi_2) = (x\pi_1)\pi_2$. In this context we obtain the *right permutation group* $\langle H_R, \sigma\rangle$ acting on H, where H_R is the right representation of H consisting of permutations h_R (that is $x\,h_R = xh, x \in H$) and where σ acts on the right (that is $x\sigma = \sigma(x), x \in H$). Since H is abelian, we have $H_L = H_R$, and from (i) in Proposition 2.1 we get $y\,(x_R\,\sigma^k) = \sigma^k(yx) = \sigma^k(xy) = \sigma^k(x)\sigma^{\sum_{i=0}^{k-1}\pi(\sigma^i(x))}(y)$ for all $x, y \in H$. The latter equals $y\,(\sigma^{\sum_{i=0}^{k-1}\pi(\sigma^i(x))}\,\sigma^k(x)_R)$, hence giving us the commuting rule in the right permutation group $\langle H_R, \sigma\rangle$,

$$x_R\,\sigma^k = \sigma^{\sum_{i=0}^{k-1}\pi(\sigma^i(x))}\,\sigma^k(x)_R \quad \text{for all } x \in H. \tag{2.2}$$

Conversely, if G is a right permutation group of H such that $H_R \leq G$ and the stabilizer G_e is a cyclic group, then any generator of G_e is a skew-morphism of H.

Let $G \leq \mathrm{Sym}(H)$ be a transitive permutation group, and let $\mathcal{B}$ be an *imprimitivity block system* (or *block system* for short) of G. Then denote by $G_{\mathcal{B}}$ the corresponding kernel, that is, $G_{\mathcal{B}} = \{g \in G \mid g(B) = B \text{ for all } B \in \mathcal{B}\}$. Furthermore, denote the permutation of $\mathcal{B}$ induced by the action of $g \in G$ on $\mathcal{B}$ by $g^{\mathcal{B}}$, and set $G^{\mathcal{B}} = \{g^{\mathcal{B}} \mid g \in G\}$. For a block B, denote by $G_{\{B\}}$ the set-wise stabilizer of B in G, and for a subgroup $H \leq G_{\{B\}}$, denote the restriction of H to B by H^B. Note that in the case where $H_L \leq G \leq \mathrm{Sym}(H)$ and H is abelian, any block system $\mathcal{B}$ is formed by the K-cosets of a subgroup $K \leq H$. In this case we identify $\mathcal{B}$ by the factor group H/K, and it follows readily that $(H_L)^{\mathcal{B}} = (H/K)_L$ and $(H/K)_L \leq G^{\mathcal{B}} \leq \mathrm{Sym}(H/K)$.

Skew-morphisms of abelian groups satisfy the following properties (see also [3]).

Proposition 2.4. *Let σ be a skew-morphism of an abelian group H with power function π, and let $\mathcal{B}$ be a block system of the skew product group $G = \langle H_L, \sigma\rangle$ formed by the K-cosets of a subgroup $K \leq H$. Then the following hold.*

(i) The restriction σ^K is a skew-morphism of K. If there is a block system of G formed by the K'-cosets of a subgroup $K' \leq H$ such that $H = K \times K'$, then σ^K is an automorphism of K if and only if $K_L \triangleleft G$.

(ii) The permutation $\sigma^{\mathcal{B}}$ is a skew-morphism of H/K; moreover, its power function $\overline{\pi}$ satisfies $\overline{\pi}(Kx) \equiv \pi(x) \pmod{\mathrm{ord}(\sigma^{\mathcal{B}})}$ for all $x \in H$.

Proof. (i): We have σ^K is an automorphism of K if and only if $\pi(x) \equiv 1 \pmod{\mathrm{ord}(\sigma^K)}$ for all $x \in K$. If $K_L \triangleleft G$, then $\sigma x_L \sigma^{-1} = \sigma(x)_L \in K_L$ for all $x \in K$ and by the previous remark, σ^K is an automorphism of K. Suppose next that σ^K is an automorphism of K. Then G is a subgroup of $G^K_{\{K\}} \times G^{K'}_{\{K'\}}$. As $G^K_{\{K\}} = \langle \sigma^K, K^K_L \rangle$, it follows that $K^K_L \triangleleft G^K_{\{K\}}$, hence $K_L \triangleleft G$.

(ii): $G^{\mathcal{B}}$ is an overgroup of $(H/K)_L$ in $\mathrm{Sym}(H/K)$. The group $G^{\mathcal{B}}$ has cyclic stabilizer $\langle \sigma^{\mathcal{B}} \rangle$, giving that $\sigma^{\mathcal{B}}$ is a skew-morphism, see Proposition 2.2. Since σ is a skew-morphism, we have $\sigma x_L = \sigma(x)_L \sigma^{\pi(x)}$ in G. This implies in $G^{\mathcal{B}}$ that $\sigma^{\mathcal{B}}\ (Kx)_L = \sigma^{\mathcal{B}}(Kx)_L\ (\sigma^{\mathcal{B}})^{\pi(x)}$. However $\sigma^{\mathcal{B}}\ (Kx)_L = \sigma^{\mathcal{B}}(Kx)_L\ (\sigma^{\mathcal{B}})^{\overline{\pi}(Kx)}$, so the result follows. □

2. Schur rings

Let H be a group written in multiplicative notation and denote the identity element by e. Denote by $\mathbb{Z}(H)$ the *group ring* of H over the ring $\mathbb{Z}$. The group ring $\mathbb{Z}(H)$ is also a $\mathbb{Z}$-module with scalar multiplication $a(\sum_{h\in H} a_h h) = \sum_{h\in H}(aa_h)h, \quad a \in \mathbb{Z}$. The $\mathbb{Z}$-submodule of $\mathbb{Z}(H)$ spanned by the elements $\eta_1, \ldots, \eta_r \in \mathbb{Z}(H)$ will be denoted by $\langle \eta_1, \ldots, \eta_r \rangle$. Given a subset $S \subseteq H$, we write $\underline{S}$ for the $\mathbb{Z}(H)$-element $\sum_{h\in H} a_h h$ defined by $a_h = 1$ if $h \in S$, and $a_h = 0$ otherwise. Such elements in $\mathbb{Z}(H)$ will be called *simple quantities*.

By a *Schur ring* (for short *S-ring*) $\mathcal{A}$ over H of *rank* r we mean a subring of the group ring $\mathbb{Z}(H)$ such that there exist subsets $T_1, \ldots, T_r$ of H satisfying the following axioms:

1. $\mathcal{A}$ has a $\mathbb{Z}$-module basis of simple quantities: $\mathcal{A} = \langle \underline{T_1}, \ldots, \underline{T_r} \rangle$.
2. $T_1 = \{e\}$, and $\sum_{i=1}^r \underline{T_i} = \underline{H}$.
3. For every $i \in \{1, \ldots, r\}$ there exists $j \in \{1, \ldots, r\}$ such that $T_i^{-1} = \{x^{-1} \mid x \in T_i\} = T_j$.

The subsets $T_1, \ldots, T_r$ are the *basic sets* of $\mathcal{A}$, and we use the notation $\mathsf{Bsets}(\mathcal{A}) = \{T_1, \ldots, T_r\}$. A subgroup $K \leq H$ is an *$\mathcal{A}$-subgroup* if $\underline{K} \in \mathcal{A}$. In this case $\mathcal{A}_K = \mathcal{A} \cap \mathbb{Z}(K)$ is an S-ring over K, also called an *induced S-subring* of $\mathcal{A}$.

It is trivial that the whole group ring $\mathbb{Z}(H)$ and the $\mathbb{Z}$-submodule $\langle \underline{e}, \underline{H \setminus \{e\}} \rangle$ are S-rings over H. The latter one is the *trivial S-ring* over H. Further examples can be obtained from an overgroup G of H_L in $\mathrm{Sym}(H)$ as follows. Let G_e denote the stabilizer of e in G, and let $T_1 = \{e\}, T_2, \ldots, T_r$ be the orbits of G_e. Then due to a result of Schur, the $\mathbb{Z}$-submodule $\langle \underline{T_1}, \ldots, \underline{T_r} \rangle$ is an S-ring over H (see [17, Theorem 24.1]). This is also called the *transitivity module* over H induced by G_e, denoted by $V(H, G_e)$. Thus

$$V(H, G_e) = \langle\, \underline{T} \mid T \in \mathrm{Orb}(G_e) \,\rangle.$$

It is interesting to note that not all S-rings over H arise in this way, and an S-ring $\mathcal{A}$ is called *Schurian* if $\mathcal{A} = V(H, G_e)$ for some overgroup G of H_L in $\mathrm{Sym}(H)$. Note that, if a subgroup $K \leq H$ satisfies $\underline{K} \in V(H, G_e)$, then K is a block of the permutation group G.

We conclude this section with two structure theorems of Evdokimov and Ponomarenko about S-rings over cyclic groups. This requires some more general notation. Let $\mathcal{A}$ be an S-ring of a group H, and let E and F be two $\mathcal{A}$-subgroups of H such that $E \lhd H$, $F \lhd H$, $E \cap F = 1$, and $EF = H$. The S-ring $\mathcal{A}$ is the *tensor product* of the induced S-subrings $\mathcal{A}_E$ and $\mathcal{A}_F$, denoted by $\mathcal{A} = \mathcal{A}_E \otimes \mathcal{A}_F$, if for any basic set T_i of $\mathcal{A}$ we have $T_i = T_j T_k$ for some basic sets $T_j \subset E$ and $T_k \subset F$.

For an arbitrary subset $X \subseteq H$ its *radical* is defined as $\mathrm{rad}(X) = \{y \in H \colon Xy = yX = X\}$. Equivalently, $\mathrm{rad}\, X$ is the largest subgroup K of H such that X is the union of both right and left cosets of K.

An S-ring $\mathcal{A}$ of a group H is said to satisfy the *U/L-condition* ([11, Definition 5.2]) if the following hold:

1. $L \le U \le H$, and $L \lhd H$,
2. L and U are $\mathcal{A}$-subgroups,
3. $L \le \mathrm{rad}(T_i)$ for any basic set $T_i \in \mathsf{Bsets}(\mathcal{A})$ such that $T_i \subseteq H \setminus U$.

If, moreover, $L \ne 1$, $U \ne H$, then we say $\mathcal{A}$ satisfies the U/L-condition *nontrivially*. In [16], the S-ring $\mathcal{A}$ satisfying the above conditions was introduced as the *wedge product* of S-rings $\mathcal{A}_U$ and the *quotient S-ring* $\mathcal{A}/L$. The latter S-ring is defined over the factor group H/L by having basic sets $T_i/L = \{Lt \mid t \in T_i\}$, $i \in \{1, \dots, r\}$ (see [15, Proposition 3.5]). If in addition $U = L$, then we say that $\mathcal{A}$ is the *wreath product* of the quotient S-ring $\mathcal{A}/L$ with the induced S-subring $\mathcal{A}_L$, and shall write $\mathcal{A} = \mathcal{A}/L \wr \mathcal{A}_L$.

Now, suppose that H is an abelian group and let T_i be a basic set of an arbitrary S-ring $\mathcal{A}$ over H. Then it follows for any number m coprime with $|H|$ that (see [17, Theorem 23.9 (a)]),

$$T_i^{(m)} := \{\, x^m \mid x \in T_i \,\} \text{ is a basic set of } \mathcal{A}. \tag{2.3}$$

Let $H = \mathbb{Z}_n$. Then (2.3) implies that $\mathrm{rad}(T_i)$ is the same for all basic sets T_i of $\mathcal{A}$ that contain a generator of $\mathbb{Z}_n$. This radical is the *radical of* $\mathcal{A}$ and denoted by $\mathrm{rad}\, \mathcal{A}$.

The first theorem describes S-rings with trivial radical (see [11, Corollary 6.4]).

Theorem 2.5. *Let $\mathcal{A}$ be an S-ring over $\mathbb{Z}_n$. Then $\mathrm{rad}\, \mathcal{A} = 1$ if and only if $\mathbb{Z}_n$ is decomposed into a direct product $\mathbb{Z}_n = E_1 \times \cdots \times E_k$ of $\mathcal{A}$-subgroups $E_1, \dots, E_k$, and $\mathcal{A}$ is decomposed into the tensor product $\mathcal{A} = \mathcal{A}_{E_1} \otimes \cdots \otimes \mathcal{A}_{E_k}$ of induced S-subrings $\mathcal{A}_{E_1}, \dots, \mathcal{A}_{E_k}$, where $\mathcal{A}_{E_1}$ is normal with trivial radical, and $\mathcal{A}_{E_i}$ is trivial for all $i \in \{2, \dots, k\}$.*

In general, an S-ring $\mathcal{A}$ over H is *normal* if $H_L \trianglelefteq \mathrm{Aut}(\mathcal{A})$, where $\mathrm{Aut}(\mathcal{A})$ is the subgroup in $\mathrm{Sym}(H)$ formed by all permutations preserving the relations (see [13])

$$R_i = \Big\{(h, ht) \mid h \in H, t \in T_i\Big\}, \quad T_i \in \mathsf{Bsets}(\mathcal{A}).$$

Note that if $\mathcal{A} = V(H, G_e)$ for some $H_L \le G \le \mathrm{Sym}(H)$, then $G \le \mathrm{Aut}(\mathcal{A})$.

For the case of nontrivial radical the following statement holds true (see [11, Corollary 5.5]).

Theorem 2.6. *An S-ring $\mathcal{A}$ over $\mathbb{Z}_n$ satisfies some U/L-condition nontrivially if and only if* $\mathrm{rad}\, \mathcal{A} > 1$.

3 S-rings and skew-morphisms of $\mathbb{Z}_n$

Let σ be a skew-morphism of a group H. Then the skew product group $G = \langle H_L, \sigma\rangle$ is an overgroup of H_L in $\mathrm{Sym}(H)$ with stabilizer $G_e = \langle\sigma\rangle$. Thus σ induces the transitivity module $V(H, \langle\sigma\rangle)$, which we call the *S-ring generated by* σ, and for short denote it also by $V(\sigma)$. In this section we study these S-rings in the case when H is a cyclic group.

First we set some notation. For the rest of the paper the cyclic group of order n is the additive group $\mathbb{Z}_n$, written also as $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, and will also denote the ring of integers modulo n. As usual, we denote by $\mathbb{Z}_n^*$ the multiplicative group of invertible elements in $\mathbb{Z}_n$. For $x \in \mathbb{Z}_n$ we write $\mathrm{ord}(x)$ for the order of x as an element in $\mathbb{Z}_n$, and $\mathrm{ord}^*(x)$ for the order of x as an element in $\mathbb{Z}_n^*$ whenever $x \in \mathbb{Z}_n^*$. For $a \in \mathbb{Z}_n$ we write α_a for the homomorphism from the cyclic group $\mathbb{Z}_n$ onto the cyclic group $\mathbb{Z}_{n/(n,a)}$ defined by

$$\alpha_a(x) = ax,\ x \in \mathbb{Z}_n.$$

The mapping α_a is an automorphism if and only if $a \in \mathbb{Z}_n^*$. For a divisor d of n let C_d denote the unique additive subgroup of $\mathbb{Z}_n$ of order d. Thus we have $C_d = \{\, x(n/d) \mid x \in \{0, \ldots, d-1\}\,\}$. Let τ be the permutation in $\mathrm{Sym}(\mathbb{Z}_n)$ acting as follows

$$\tau(x) = x + 1,\ x \in \mathbb{Z}_n.$$

By Proposition 2.2 a skew-morphism σ of $\mathbb{Z}_n$ with a power function π induces the skew product group $G = \langle\tau, \sigma\rangle$.

By (i) in Proposition 2.1, for a fixed $x \in \mathbb{Z}_m$, $m = \mathrm{ord}(\sigma)$, and $y \in \mathbb{Z}_n$ we have

$$\sigma^x(y + z) = \sigma^x(y)\sigma^{\pi(y)+\pi(\sigma(y))+\cdots+\pi(\sigma^{x-1}(y))}(z) \text{ for all } z \in \mathbb{Z}_n.$$

Thus the following commuting rule holds in G,

$$\sigma^x\tau^y = \tau^{\sigma^x(y)}\sigma^{\pi(y)+\pi(\sigma(y))+\cdots+\pi(\sigma^{x-1}(y))} \text{ for all } x \in \mathbb{Z}_m, y \in \mathbb{Z}_n, \tag{3.1}$$

where $m = \mathrm{ord}(\sigma)$. In particular, the characteristic identity of a skew-morphism σ of $\mathbb{Z}_n$ can be expressed as

$$\sigma\tau^y = \tau^{\sigma(y)}\sigma^{\pi(y)} \text{ for all } y \in \mathbb{Z}_n.$$

Suppose that $\mathcal{B}$ is a block system of $G = \langle\tau, \sigma\rangle$, and $\mathcal{B}$ is formed by the C_d -cosets for some subgroup $C_d \le \mathbb{Z}_n$. Then we write $\sigma|_d$ for the skew-morphism σ^{C_d}, see (i) in Proposition 2.4. Also, we write $\sigma|^{n/d}$ for the skew-morphism $\sigma^{\mathcal{B}}$ of the factor group $\mathbb{Z}_n/C_d \cong \mathbb{Z}_{n/d}$, see (ii) in Proposition 2.4.

In our first result we describe skew-morphisms inducing S-rings with trivial radical.

Proposition 3.1. *Let σ be a skew-morphism of $\mathbb{Z}_n$ with $\mathrm{rad}\, V(\sigma) = 1$. Then σ is an automorphism of $\mathbb{Z}_n$.*

Proof. We set $G = \langle\tau, \sigma\rangle$ and $\mathcal{A} = V(\sigma)$. Assume first that $\mathrm{rad}\, V(\sigma) = 1$. By Theorem 2.5, the group $\mathbb{Z}_n$ decomposes into a direct product $\mathbb{Z}_n = C_{n_1} \times \cdots \times C_{n_k}$ of $\mathcal{A}$-subgroups $C_{n_1}, \ldots, C_{n_k}$ so that

$$\mathcal{A} = \mathcal{A}_{C_{n_1}} \otimes \cdots \otimes \mathcal{A}_{C_{n_k}},$$

where the induced S-subring $\mathcal{A}_{C_{n_1}}$ is normal, and $\mathcal{A}_{C_{n_i}}$ is trivial for all $i \in \{2,\dots,k\}$. It is obvious that $\mathcal{A}_{C_{n_i}} = V(\sigma|_{n_i})$ for all $i \in \{1,\dots,k\}$. In particular, the skew product group $G_i = \langle (C_{n_i})_L, \sigma|_{n_i}\rangle \le \mathrm{Aut}(\mathcal{A}_{C_{n_i}})$ for all $i \in \{1,\dots,k\}$.

For $i = 1$ the subring $\mathcal{A}_{C_{n_1}}$ is normal, hence $(C_{n_1})_L \trianglelefteq \mathrm{Aut}(\mathcal{A}_{C_{n_1}})$. Therefore $(C_{n_1})_L \trianglelefteq \langle (C_{n_1})_L, \sigma|_{n_1}\rangle$, so $\sigma|_{n_1}$ is an automorphism of C_{n_1}. By (i) in Proposition 2.4, $(C_{n_1})_L \triangleleft G$.

Let $i > 1$. Then $\mathcal{A}_{C_{n_i}} = V(\sigma|_{n_i})$ is trivial. Thus the subring $\mathcal{A}_{C_{n_i}}$ is generated by $\underline{0}$ and $\underline{C_{n_i} \setminus \{0\}}$, and so $C_{n_i} \setminus \{0\}$ is an orbit of $\sigma|_{n_i}$. It follows that $\mathrm{ord}(\sigma|_{n_i}) = |C_{n_i} \setminus \{0\}|$, and we obtain that G_i is a sharply 2-transitive Frobenius group. Therefore G_i must have a regular elementary abelian normal subgroup, say E_i. Furthermore, $|G_i| = |E_i|(|E_i| - 1)$, hence E_i is a Sylow p-subgroup of G_i. We conclude that $n_i = |E_i|$, $(C_{n_i})_L = E_i \triangleleft G_i$. Hence $\sigma|_{n_i}$ is an automorphism of C_{n_i}, and $(C_{n_i})_L \triangleleft G$ by (i) in Proposition 2.4.

To summarize, $(C_{n_i})_L \triangleleft G$ for all $i \in \{1,\dots,k\}$. Therefore, $(\mathbb{Z}_n)_L \triangleleft G$, equivalently, σ is an automorphism of $\mathbb{Z}_n$. □

It follows from Theorem 2.6 that a generating orbit of a pure skew-morphism σ of $\mathbb{Z}_n$ is a union of cosets of a nontrivial subgroup $L \le \mathbb{Z}_n$.

We give next three corollaries which seem to be of independent interest.

Corollary 3.2. *All skew-morphisms of $\mathbb{Z}_n$ have power functions with nontrivial kernel.*

Proof. Let σ be a skew-morphism of $\mathbb{Z}_n$ with power function π. To simplify notation we put $H = \mathbb{Z}_n$. The skew product group $G = \langle H_L, \sigma\rangle = H_L\langle\sigma\rangle$. Let $m = \mathrm{ord}(\sigma)$. By Corollary 2.3, $m < n$. Consider G acting on the right cosets of H_L in G. Denote by $\widetilde{G}$ the induced permutation group. Then $\widetilde{G}$ is of degree m, in particular, $\widetilde{\langle\sigma\rangle}$ is a regular cyclic subgroup. The point stabilizer of the coset H_L in $\widetilde{G}$ is $\widetilde{H_L}$, hence it is cyclic. Also, $\widetilde{H_L} \cong H_L/\mathrm{core}_G(H_L)$, where $\mathrm{core}_G(H_L) = \bigcap_{g\in G} g^{-1}H_L g$, or in other words, the largest normal subgroup of G contained in H_L. Any generator of $\widetilde{H_L}$ becomes a skew-morphism of $\widetilde{\langle\sigma\rangle}$, hence $|\widetilde{H_L}| < m < n = |H_L|$. Therefore, there exists a nontrivial subgroup $K \le H = \mathbb{Z}_n$ such that $K_L \triangleleft G$. It is obvious that $K \le \ker\pi$ (see the proof of (i) in Proposition 2.4). □

The next fact was important in the study of regular cyclic maps (see [2]).

Corollary 3.3. *Let σ be a skew-morphism σ of $\mathbb{Z}_n$, and T be an orbit of σ such that $\langle T\rangle = \mathbb{Z}_n$. Then there exists $t \in T$ such that $\langle t\rangle = \mathbb{Z}_n$.*

Proof. We prove the statement by induction on n. The statement is trivially true if n is a prime. Thus we assume that n is a composite number, and that the statement is true for all groups $\mathbb{Z}_{n'}$ such that $n' < n$.

If $\mathrm{rad}\, V(\sigma) = 1$ then by Proposition 3.1 σ is an automorphism of $\mathbb{Z}_n$, and we are done. Let $\mathrm{rad}\, V(\sigma) \ne 1$. Then $V(\sigma)$ satisfies the C_u/C_l-condition for subgroups $1 < C_l \le C_u < \mathbb{Z}_n$. Since $\langle T\rangle$ generates $\mathbb{Z}_n$, the set $T/C_l = \{x + C_l |\ x \in T\}$ forms a generating orbit of $\mathbb{Z}_n/C_l$ in the quotient skew-morphism. By the induction hypothesis there exists $t \in T$ such that $\langle t + C_l\rangle = \mathbb{Z}_n/C_l$. If $\langle C_l + t\rangle < \mathbb{Z}_n$, then $\langle C_l + t\rangle/C_l < \mathbb{Z}_n/C_l$, and $C_l + t$ is a nongenerating element of $\mathbb{Z}_n/C_l$, a contradiction. It follows that $\mathbb{Z}_n = \langle t + C_l\rangle = \langle t\rangle + C_l$. Let $m = \mathrm{ord}(t)$. Then $n = lm/(l,m)$. Set $t' = \frac{n}{l} + t$. Then $\mathrm{ord}(t') = lm/(l,m) = n$, so $\langle t'\rangle = \mathbb{Z}_n$. Now, by the C_u/C_l condition we find $C_l + t \subseteq T$, hence $t' \in T$, proving the result. □

Corollary 3.4. *Let σ be a skew-morphism of $\mathbb{Z}_n$. Then $\mathrm{ord}(\sigma)$ is a divisor of $n\phi(n)$. Moreover, if $(\mathrm{ord}(\sigma), n) = 1$, then σ is an automorphism of $\mathbb{Z}_n$.*

Proof. We prove the statement by induction on n. If n is a prime, then by Corollary 3.2 $\ker \pi = \mathbb{Z}_n$, hence σ is an automorphism of $\mathbb{Z}_n$ and $\mathrm{ord}(\sigma) \mid \phi(n)$. Thus we assume that n is a composite number, and that the statement is true for all groups $\mathbb{Z}_{n'}$ such that $n' < n$.

Let σ be an arbitrary skew-morphism of $\mathbb{Z}_n$ with power function π. In the case where $\mathrm{rad}\, V(\sigma) = 1$, by Proposition 3.1 the skew-morphism σ is an automorphism of $\mathbb{Z}_n$. It follows that $\mathrm{ord}(\sigma) \mid \phi(n)$.

Let $\mathrm{rad}\, V(\sigma) \neq 1$. Then $V(\sigma)$ satisfies the C_u/C_l-condition for subgroups $1 < C_l \leq C_u < \mathbb{Z}_n$. Consider the skew-morphism $\sigma|^{n/l}$ of the factor group $\mathbb{Z}_n/C_l \cong \mathbb{Z}_{n/l}$. Let T be an orbit of σ such that $\langle T\rangle = \mathbb{Z}_n$. By Corollary 2.3, $\mathrm{ord}(\sigma) = |T|$. Then T/C_l is an orbit of $\sigma|^{n/l}$ such that $\langle T/C_l\rangle = \mathbb{Z}_n/C_l$, and hence $\mathrm{ord}(\sigma|^{n/l}) = |T/C_l|$. As $V(\sigma)$ satisfies the C_u/C_l-condition, $|T/C_l| = |T|/l$, and we obtain that $\mathrm{ord}(\sigma|^{n/l}) = \mathrm{ord}(\sigma)/l$. Induction gives

$$\mathrm{ord}(\sigma)/l = \mathrm{ord}(\sigma|^{n/l}) \mid (n/l)\,\phi(n/l).$$

This implies that $\mathrm{ord}(\sigma) \mid n\phi(n/l)$, hence $\mathrm{ord}(\sigma) \mid n\phi(n)$.

As noted after Proposition 3.1, if σ is a pure skew-morphism of $\mathbb{Z}_n$, then a generating orbit T of σ must be a union of L-cosets for a subgroup $1 < L \leq \mathbb{Z}_n$. By Corollary 2.3, $\mathrm{ord}(\sigma) = |T|$ is divisible by $|L|$, in particular $|L| \mid (\mathrm{ord}(\sigma), n)$. Now, it is clear that if $(\mathrm{ord}(\sigma), n) = 1$, then σ must be an automorphism of $\mathbb{Z}_n$. □

If n is a square-free integer and σ is a skew-morphism of $\mathbb{Z}_n$, then the fact that σ is an automorphism of $\mathbb{Z}_n$ can be read off quickly from the generated S-ring $V(\sigma)$.

Proposition 3.5. *Let n be a square-free number and σ be a skew-morphism of $\mathbb{Z}_n$. Then σ is an automorphism of $\mathbb{Z}_n$ if and only if $\underline{C_d} \in V(\sigma)$ for all subgroups $C_d \leq \mathbb{Z}_n$.*

Proof. The implication $\Rightarrow$ is obvious.

The converse implication $\Leftarrow$ follows by an easy induction on the order n. We get that all subgroups of $(\mathbb{Z}_n)_L$ of prime index are normal in $G = \langle \tau, \sigma\rangle$. Since n is square-free, this implies $(\mathbb{Z}_n)_L \trianglelefteq G$, equivalently, σ is an automorphism of $\mathbb{Z}_n$. □

There is yet another S-ring which can be associated with a skew-morphism σ of an arbitrary group H. Consider the skew product group $G = \langle H_L, \sigma\rangle = H_L\langle\sigma\rangle$. The group G has a well-known right action on the set G/H_L of right H_L-cosets in G as for $x, y \in G$, $(H_L x)^y = H_L xy$. As $G = H_L\,\langle\sigma\rangle$ and $|H_L \cap \langle\sigma\rangle| = 1$, the elements σ^i form a complete set of coset representatives of H_L in G. Thus the set G/H_L can be identified with $\langle\sigma\rangle$, and the group G admits a corresponding right action on $\langle\sigma\rangle$. (We remark that the only property we are using here is that $|H_L \cap G_e| = 1$, hence the same right action can be defined on arbitrary point stabilizer G_e, and G_e need not be generated by one element.) Formally, for $\sigma^i \in \langle\sigma\rangle$ and $g \in G$ we set $(\sigma^i)^g = \sigma^j$, where the integer j satisfies

$$H_L(\sigma^i)^g = H_L\,\sigma^i g = H_L\sigma^j.$$

For $g \in G$, denote by $\widetilde{g}$ the permutation of $\langle\sigma\rangle$ induced by g. The subgroup $\langle\sigma\rangle \leq G$ is faithful, and $\widetilde{\langle\sigma\rangle} = \langle\sigma\rangle_R$. The group H_L is not always faithful, in fact $\widetilde{H_L} \cong$

$H_L/\operatorname{core}_G(H_L)$, where $\operatorname{core}_G(H_L) = \bigcap_{g\in G} g^{-1}H_L g$, or in other words, the largest normal subgroup of G contained in H_L. The stabilizer of $\mathrm{id} \in \langle\sigma\rangle$ equals $\widetilde{H_L}$, hence we obtain the S-ring $V(\langle\sigma\rangle, \widetilde{H_L})$ over $\langle\sigma\rangle$. Notice that $\operatorname{core}_G(H_L) \le K_L$, where $K = \ker\pi$, π is the power function of σ, and that the conjugate subgroup $\sigma K_L \sigma^{-1} \le H_L$. If $H \cong \mathbb{Z}_n$ is a cyclic group, then every subgroup of H_L is uniquely determined by its order, in particular, $|\sigma K_L\sigma^{-1}| = |K_L|$ yields that $\sigma K_L\sigma^{-1} = K_L$. This implies, in turn, that K_L is a normal subgroup in G, $K_L \le \operatorname{core}_G(H_L)$, and so $\operatorname{core}_G(H_L) = \ker\pi$. Then $\widetilde{H_L}$ is cyclic, and thus any of its generators is a skew-morphism of $\langle\sigma\rangle$ (see the remark following Corollary 2.3). Recall that $H_L = \langle\tau\rangle$, where τ is the permutation $x \mapsto x+1$, $x \in \mathbb{Z}_n$. Let $\operatorname{ord}(\sigma) = m$, and let ψ be the isomorphism from $\langle\sigma\rangle$ to $\mathbb{Z}_m$ sending σ^x to $x \in \mathbb{Z}_m$. Then the function

$$\sigma_* = \psi^{-1}\,\widetilde{\tau}\,\psi$$

is a skew-morphism of $\mathbb{Z}_m$. We shall call σ_* the *skew-morphism derived from* σ. The skew-morphism σ is related to its derived skew-morphism σ_* as follows.

Proposition 3.6. *Let σ be a skew-morphism of $\mathbb{Z}_n$ with $\operatorname{ord}(\sigma) = m$, and π be the power function of σ. Then the derived skew-morphism σ_* of $\mathbb{Z}_m$ and its power function π_* are given by*

$$(\sigma_*)^y(x) = \pi(y) + \pi(\sigma(y)) + \cdots + \pi(\sigma^{x-1}(y)), \tag{3.2}$$

$$\pi_*(x) \equiv \sigma^x(1) \pmod{n/|\ker\pi|}. \tag{3.3}$$

Proof. Using commuting rule (3.1) in the skew product group $G = \langle\tau,\sigma\rangle$ we conclude that

$$\langle\tau\rangle\,\sigma^x\tau^y = \langle\tau\rangle\,\sigma^{\pi(y)+\pi(\sigma(y))+\cdots+\pi(\sigma^{x-1}(y))}.$$

This shows that $\widetilde{\tau}^{\,y}\colon \sigma^x \mapsto \sigma^{\pi(y)+\pi(\sigma(y))+\cdots+\pi(\sigma^{x-1}(y))}$, and (3.2) follows.

Notice that $\langle\widetilde{\sigma},\widetilde{\tau}\rangle = \langle\langle\sigma\rangle_R,\widetilde{\tau}\rangle$ is a right permutation group with skew-morphism $\widetilde{\tau}$. Thus by the commuting rule (2.2),

$$\widetilde{\sigma}^{\,x}\,\widetilde{\tau} = \widetilde{\tau}^{\,\pi_*(x)}\,\widetilde{\sigma}^{\,\sigma_*(x)} \text{ for all } x \in \mathbb{Z}_m.$$

Combining this with (3.1) gives us $\pi_*(x) \equiv \sigma^x(1) \pmod{\operatorname{ord}(\widetilde{\tau})}$. Now, $\operatorname{ord}(\widetilde{\tau}) = [(\mathbb{Z}_n)_L\colon \operatorname{core}_G((\mathbb{Z}_n)_L)]$, and (3.3) follows as $\operatorname{core}_G((\mathbb{Z}_n)_L) \cong \ker\pi$. □

Note that the derived skew-morphism σ_* is the identity if and only if σ is an automorphism.

4 S-rings $V(\sigma)$ over $\mathbb{Z}_{p^e}$

In this section our goal is to prove the following theorem about S-rings $V(\sigma)$ where $\sigma \in \operatorname{Skew}(\mathbb{Z}_{p^e})$, p is an odd prime.

Theorem 4.1. *If $\sigma \in \operatorname{Skew}(\mathbb{Z}_{p^e})$, where p is an odd prime, then $V(\sigma) = V(\alpha)$ for some $\alpha \in \operatorname{Aut}(\mathbb{Z}_{p^e})$.*

Theorem 4.1 suggests the following definition.

Definition 4.2. A permutation σ of a finite group H is a near automorphism if σ is a skew-morphism of H, and the orbits of σ are equal to the orbits of an automorphism $\alpha \in \mathrm{Aut}(H)$ (or equivalently, $V(\sigma) = V(\alpha)$ holds).

In this context Theorem 4.1 can be rephrased as every skew-morphism of $\mathbb{Z}_{p^e}, p$ is an odd prime, is a near automorphism.

We first prove several properties of skew-morphisms of $\mathbb{Z}_{p^e}$, p is an odd prime.

Lemma 4.3. *Let $\sigma \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ be a skew-morphism with power function π. Then all subgroups $C_{p^i}, i \in \{0, 1, \ldots, e\}$ are blocks of $\langle \tau, \sigma \rangle$.*

Proof. We prove the lemma by induction on the exponent e. The case $e = 1$ is trivially true. By Corollary 3.2, the power function π of σ has nontrivial kernel, say K. Therefore K is normal in the group $G = \langle \tau, \sigma \rangle$, in particular, C_p is a block of G. Now, applying induction to $\sigma|^{p^{e-1}}$ if $e > 1$ yields the result. □

In the next lemma we consider skew-morphisms of p-power order.

Lemma 4.4. *Let $\sigma \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ of order p^f with power function π. Then the following hold:*

(i) The orbit T generated by 1 is the coset $T = 1 + C_{p^f}$, in particular $\sigma^i(1) \equiv 1 \pmod{p^{e-f}}$ for $i = 0, 1, \ldots, p^f - 1$;

(ii) For all $x \in \mathbb{Z}_{p^e}$, $\pi(x) \equiv 1 \pmod{p}$; in particular, if the order of σ is p then σ is an automorphism;

(iii) For every $i \in \mathbb{N}$, σ^i is a skew-morphism of $\mathbb{Z}_{p^e}$, moreover $\mathrm{ord}(\sigma^i(1)) = p^f/(p^f, i)$.

Proof. We put $G = \langle \tau, \sigma \rangle$. Observe that $f < e$.

(i): By Corollary 2.3, $|T| = \mathrm{ord}(\sigma) = p^f$. By Lemma 4.3 $C_{p^{e-1}} = \langle p \rangle$ is fixed by σ and hence $T \subseteq \mathbb{Z}^*_{p^e}$. Let c be a generator of $\mathbb{Z}^*_{p^e}$. By (2.3) $T, cT, c^2T, \ldots, c^{p^{e-1}(p-1)-1}T$ are basic sets in $V(\sigma)$ and the union of these sets forms $\mathbb{Z}^*_{p^e}$. It follows that the least power of c fixing T is $d = c^{(p-1)p^{e-f-1}}$ of multiplicative order p^f. In particular $T = \{1, d, d^2, \ldots, d^{p^f-1}\}$. Since $\mathbb{Z}^*_{p^e}$ is cyclic, it contains a unique subgroup of order p^f, namely $1 + C_{p^f}$. It follows that $T = 1 + C_{p^f}$.

(ii): Consider the skew-morphism σ_* derived from σ. Then σ_* is a skew-morphism of $\mathbb{Z}_{p^f}$ of p-power order. Because of (3.2), $\sigma_*^y(1) = \pi(y)$ for all $y \in \mathbb{Z}_{p^e}$. Now, the result follows by (i).

(iii): If i is coprime to p then σ^i is a generator of the stabilizer of 0 in G and the result follows by Proposition 2.2. For $i = p^\ell$ for some $\ell > 0$ by (i) in Proposition 2.1 σ^i is a skew-morphism if and only if p^ℓ divides $\sum_{j=0}^{p^\ell-1} \pi(\sigma^j(x))$ which holds true by (ii). Clearly, the orbit of σ^{p^ℓ} generated by 1 consists of the elements of the multiplicative subgroup of $\mathbb{Z}^*_{p^e}$ generated by d^{p^ℓ}, and we are done. □

Next we determine the skew-morphisms $\sigma \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ of order p^2. Denote by $\mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$ the set of all functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. For $f, g \in \mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$, let fg and $f + g$ be the functions in $\mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$ defined as $(fg)(x) = f(g(x))$ and $(f + g)(x) =$

$f(x)+g(x)$, respectively, for all $x \in \mathbb{Z}_n$. Further, if $c \in \mathbb{Z}_n$, then let cf be the function in $\mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$ defined as $(cf)(x) = cf(x)$ for all $x \in \mathbb{Z}_n$.

Let $f \in \mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$. We introduce the *sum operator* ∇ as the function in $\mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$ defined as

$$\begin{aligned}(\nabla f)(0) &= 0, \text{ and}\\ (\nabla f)(x) &= f(0)+f(1)+\cdots+f(x-1) \text{ if } x \in \mathbb{Z}_n, x \neq 0.\end{aligned}$$

Note that ∇ satisfies $\nabla(f+g) = \nabla f + \nabla g$ for all $f, g \in \mathrm{Fun}(\mathbb{Z}_n, \mathbb{Z}_n)$.

Let us put $n = p^e$ for the rest of the section, where p is an odd prime. For $a \in \mathbb{Z}_{p^e}^*$ and $b \in \mathbb{Z}_{p^e}, b \in C_p$ define the function

$$\sigma_{a,b} = \alpha_a + \nabla\alpha_b.$$

Let $\mathcal{G}_e = \{\sigma_{a,b} \mid a \in \mathbb{Z}_{p^e}^*, \mathrm{ord}^*(a) = p^i, i \in \{0,1,\ldots,e-1\}, b \in C_p\}$.

Lemma 4.5. *With the above notation $\mathcal{G}_e$ is a subgroup of $\mathrm{Sym}(\mathbb{Z}_{p^e})$, $\mathcal{G}_e \cong \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_p$ with the composition rule $\sigma_{a,b}\sigma_{c,d} = \sigma_{ac,b+d}$. In particular, $\mathrm{ord}(\sigma_{a,b}) = \mathrm{ord}^*(a)$ if $a \neq 1$ and $\mathrm{ord}(\sigma_{a,b}) = \mathrm{ord}(b)$ if $a = 1$.*

Proof. Clearly, the identity permutation $\mathrm{id} = \sigma_{1,0}$, hence $\mathrm{id} \in \mathcal{G}_e$. Now, it is enough to prove that $\sigma_{a_1,b_1}\sigma_{a_2,b_2} = \sigma_{a_1a_2,b_1+b_2}$ for all $\sigma_{a_1,b_1}, \sigma_{a_2,b_2} \in \mathcal{G}$. Since $b \in C_p$, we have

$$(\nabla\alpha_b)(x) = (\nabla\alpha_b)(x') \text{ if } x \equiv x' \pmod p.$$

Since $a_2 \in 1 + C_{p^i}$ for some $i \in \{0,1,\ldots,e-1\}$ we have $\sigma_{a_2,b_2} \equiv \mathrm{id} \pmod p$. It follows that $(\nabla\alpha_{b_1})\,\sigma_{a_2,b_2} = \nabla\alpha_{b_1}$. Thus

$$\sigma_{a_1,b_1}\sigma_{a_2,b_2} = (\alpha_{a_1} + \nabla\alpha_{b_1})\,\sigma_{a_2,b_2} = \alpha_{a_1}\sigma_{a_2,b_2} + \nabla\alpha_{b_1}.$$

Since $a_1b_2 = b_2$ in $\mathbb{Z}_{p^e}$,

$$\alpha_{a_1}\sigma_{a_2,b_2} = \alpha_{a_1a_2} + \nabla\alpha_{a_1b_2} = \alpha_{a_1a_2} + \nabla\alpha_{b_2}.$$

These yield $\sigma_{a_1,b_1}\sigma_{a_2,b_2} = \alpha_{a_1a_2} + \nabla\alpha_{b_2} + \nabla\alpha_{b_1} = \alpha_{a_1a_2} + \nabla\alpha_{b_1+b_2}$. It follows that $\mathcal{G}_e$ is a group generated by the automorphisms $\sigma_{a,0}$ and elements $\sigma_{1,b}$. □

Lemma 4.6. *The permutations $\sigma_{a,b}$ in $\mathcal{G}_e$ are pure skew-morphisms of $\mathbb{Z}_{p^e}$ if and only if $a \in 1 + C_{p^f}$, where $f > 1$ and $b \neq 0$.*

Proof. Let $b \neq 0$ and $a \in 1 + C_{p^f}$, where $f > 1$. To simplify notation we set $\sigma = \sigma_{a,b}$. Let $a' = b + 1$. Notice that $a' \in \mathbb{Z}_{p^e}^*$ and $\mathrm{ord}^*(a') = p$. By Lemma 4.5, $\sigma^p = \alpha_{a^p} + \nabla\alpha_{pb} = \alpha_{a^p}$. Thus $\sigma^\ell = \alpha_{a'}$ for a suitable $\ell \in \mathbb{N}$. Since the order of σ is p^f for some $f \in \{2,\ldots,e-1\}$, we get that p^{f-1} divides ℓ.

It follows that $(xb+1) = a'^x$ for all $x \in \mathbb{Z}_{p^e}$. We want to show that $\sigma(x+1) = a(1 + a' + a'^2 + \cdots + a'^x)$ for all $x \in \mathbb{Z}_{p^e}$. We have

$$\begin{aligned}a(1 + a' + a'^2 + \cdots + a'^x) &= a(1 + (b+1) + (b+1)^2 + \cdots + (b+1)^x)\\ &= a(x+1) + a(b + 2b + 3b + \cdots + xb)\\ &= a(x+1) + ab(1 + 2 + 3 + \cdots + x)\\ &= a(x+1) + b(1 + 2 + 3 + \cdots + x)\end{aligned}$$

If $x \neq p^e - 1$ the last term is equal $\sigma(x+1)$ by definition. For $x = p^e - 1$ we get $a((p^e-1)+1) + b(1+2+3+\cdots+(p^e-1)) = 0 = \sigma(0)$.

Now we are ready to prove the commuting rule $\sigma\tau = \tau^a\sigma^{\ell+1}$. This is equivalent to the identity $\sigma(x+1) = a + a'\sigma(x)$. Inserting $\sigma(x+1) = a(1 + a' + a'^2 + \cdots + a'^x)$ and $\sigma(x) = a(1 + a' + a'^2 + \cdots + a'^{x-1})$ we get the result.

Taking this to the ith power, $i \in \mathbb{N}$ we find $\sigma\langle\tau\rangle \subseteq \langle\tau\rangle\langle\sigma\rangle$. A simple induction argument gives $\sigma^i\langle\tau\rangle \subseteq \langle\tau\rangle\langle\sigma\rangle$ for all $i \in \mathbb{N}$. We conclude that $\langle\sigma\rangle\langle\tau\rangle = \langle\tau\rangle\langle\sigma\rangle$, hence σ is a skew-morphism of $\mathbb{Z}_{p^e}$. Furthermore, σ takes $1 \mapsto a$ and $2 \mapsto 2a + b$. Therefore, it cannot be an automorphism for $b \neq 0$.

Clearly $\sigma_{a,0}$ is an automorphism. It remains to show that $\sigma_{a,b}$, where $b \neq 0$ and $a \in 1 + C_p$ is not a pure skew-morphism. By Lemma 4.5 the order of σ is p. By Lemma 4.4(iii) $\sigma_{a,b}$ is an automorphism, a contradiction. □

Lemma 4.7. *The skew-morphisms of $\mathbb{Z}_{p^e}$ of order p^2 are exactly the elements $\sigma_{a,b}$ in $\mathcal{G}_e$ of order p^2.*

Proof. Let $\sigma(1) = a$. By (ii) in Lemma 4.4, $a \in \mathbb{Z}_{p^e}^*$ with $\mathrm{ord}^*(a) = p^2$. Let $\sigma' = \sigma^{\pi(1)-1}$. Because of (iii) in Lemma 4.4 we have σ' is a skew-morphism of $\mathbb{Z}_{p^e}$ of order at most p. Therefore σ' is an automorphism of $\mathbb{Z}_{p^e}$, and we may write $\sigma' = \alpha_{a'}$ for some $a' \in \mathbb{Z}_{p^e}^*, \mathrm{ord}^*(a') = p^i, i \leq 1$.

By (3.1), σ satisfies $\sigma\tau = \tau^{\sigma(1)}\sigma^{\pi(1)}$. Therefore,

$$\sigma\tau = \tau^a\sigma^{\pi(1)-1}\sigma = \tau^a\alpha_{a'}\sigma = \tau^a(\alpha_{a'} + \sigma) = \sigma + \kappa_a + \alpha_b, \tag{4.1}$$

where $b = a' - 1$, and κ_a is the constant function $\kappa_a(x) = a$ for all $x \in \mathbb{Z}_{p^e}$. Notice that $b \in C_p$, and hence we have $\alpha_{a'}\sigma = \alpha_{a'}$ as $\sigma(x) \equiv x \pmod p$ for all $x \in \mathbb{Z}_{p^e}$. It is not difficult to see that the functional equation in (4.1) with σ as variable and initial value $\sigma(0) = 0$ has a unique solution, and this is

$$\sigma = \nabla(\kappa_a + \alpha_b) = \nabla\kappa_a + \nabla\alpha_b = \alpha_a + \nabla\alpha_b.$$

We obtain that $\sigma \in \mathcal{G}_e$ and this completes the proof. □

Proof of Theorem 4.1. We put $G = \langle\tau, \sigma\rangle$, and let P be the Sylow-p-subgroup of G. By Corollary 3.4, $\mathrm{ord}(\sigma) = p^f d$, where $d \mid (p-1)$. The group P contains $(\mathbb{Z}_{p^e})_L$ and has stabilizer $P_0 = \langle\sigma^d\rangle$. It follows from Proposition 2.2 that σ^d is a skew-morphism of $\mathbb{Z}_{p^e}$ of order p^f. If $f = 0$, then σ is an automorphism of $\mathbb{Z}_{p^e}$, see Corollary 3.4. Thus we assume that $f \geq 1$.

We prove the theorem by induction on e. If $e = 1$, then σ is an automorphism of $\mathbb{Z}_p$, and the proposition is trivially true. Let $e > 1$ and assume that the proposition holds for any group $\mathbb{Z}_{p^{e'}}$ for which $e' < e$. We put $\mathcal{A} = V(\sigma)$. By Lemma 4.3, all subgroups C_{p^i} are blocks of G, equivalently, $C_{p^i} \in \mathcal{A}$ for all $i \in \{0, 1, \ldots, e\}$.

The further argument is divided into four steps.

(a) $\mathcal{A}_{C_{p^{e-1}}} = V(\beta)$ for some automorphism β in $\mathrm{Aut}(C_{p^{e-1}})$.

We have $\mathcal{A}_{C_{p^{e-1}}} = V(C_{p^{e-1}}, \sigma|_{p^{e-1}})$. Thus (a) follows by induction.

(b) $\mathcal{A}/C_p = V(\gamma)$ for some automorphism γ in $\mathrm{Aut}(\mathbb{Z}_{p^e}/C_p)$.

We have $\mathcal{A}/C_p = V(\mathbb{Z}_{p^e}/C_p, \sigma|^{p^{e-1}})$. Thus (b) follows by induction.

(c) There exists a unique automorphism α in $\mathrm{Aut}(\mathbb{Z}_{p^e})$ such that $\alpha|_{p^{e-1}} = \beta$ and $\alpha|^{p^{e-1}} = \gamma$.

First, there exists a unique automorphism α in $\mathrm{Aut}(\mathbb{Z}_{p^e})$ such that

$$p \mid \mathrm{ord}(\alpha) \text{ and } \alpha|^{p^{e-1}} = \gamma.$$

Then

$$\beta|^{p^{e-2}} = \big(\sigma|_{p^{e-1}}\big)|^{p^{e-2}} = \big(\sigma|^{p^{e-1}}\big)|_{p^{e-2}} = \gamma|_{p^{e-2}}.$$

The latter can be written as

$$\big(\alpha|^{p^{e-1}}\big)|_{p^{e-2}} = \big(\alpha|_{p^{e-1}}\big)|^{p^{e-2}}.$$

Thus we have $\beta|^{p^{e-2}} = \big(\alpha|_{p^{e-1}}\big)|^{p^{e-2}}$. This forces $\beta = \alpha|_{p^{e-1}}$ if $p^2 \mid \mathrm{ord}(\alpha|_{p^{e-1}})$, or $(\alpha|_{p^{e-1}}, p^{e-2}) = (\beta, p^{e-2})$.

Assume that $f \geq 3$. Then $p^3 \mid \mathrm{ord}(\sigma)$, hence $p^3 \mid \mathrm{ord}(\alpha)$, and we are done as $p^2 \mid \mathrm{ord}(\alpha|_{p^{e-1}})$.

Let $f = 2$. Then $(\alpha|_{p^{e-1}}, p^{e-2}) = p$. But σ^d is a skew-morphism of $\mathbb{Z}_{p^e}$ of order p^2. Applying Lemma 4.7 we find that $\mathrm{ord}(\sigma|_{p^{e-1}}, p^{e-2}) = p$ also.

Let $f = 1$. Then $(\alpha|_{p^{e-1}}, p^{e-2}) = 1$. But σ^d is a skew-morphism of $\mathbb{Z}_{p^e}$ of order p. Thus σ^d is an automorphism of $\mathbb{Z}_{p^e}$, and we find that $\mathrm{ord}(\sigma|_{p^{e-1}}, p^{e-2}) = 1$. This completes (c).

(d) $\mathcal{A} = V(\alpha)$.

This follows directly from (c) and the fact that every basic set $T \in \mathsf{Bsets}(\mathcal{A})$ where $\langle T \rangle = \mathbb{Z}_{p^e}$ is a union of C_p-cosets. □

Remark. Theorem 4.1 does not hold for powers of 2. Take the permutation $\sigma \in \mathrm{Sym}(\mathbb{Z}_{2^e})$ defined as

$$\sigma(x) = \begin{cases} x+2 & \text{if } x \notin C_{2^{e-1}}, \\ x & \text{if } x \in C_{2^{e-1}}. \end{cases}$$

It is easy to check that σ is a skew-morphism of $\mathbb{Z}_{2^e}$, and its power function π satisfies $\pi(x) = 1$ for all $x \in C_{2^{e-1}}$, and $\pi(x) = -1$ for all $x \notin C_{2^{e-1}}$. Clearly, if $e \geq 3$, then $V(\sigma) \neq V(\alpha)$ for all $\alpha \in \mathrm{Aut}(\mathbb{Z}_{2^e})$.

As a small application of Theorem 4.1 we determine the whole set $\mathrm{Skew}(\mathbb{Z}_{p^2})$. We need to consider the automorphisms of the group

$$\mathcal{M}_e = \big\langle x, y \mid x^{p^e} = y^p = 1, x^y = x^{p^{e-1}+1} \big\rangle.$$

The next lemma is a special case of [1, Lemma 2.1].

Lemma 4.8. *The automorphisms in* $\mathrm{Aut}(\mathcal{M}_e)$ *are given as the permutations* $\theta_{a,b,c}$, $a \in \mathbb{Z}_{p^e}^*, b \in C_p$ *and* $c \in \mathbb{Z}_p$ *defined as*

$$\theta_{a,b,c}(x^i y^j) = x^{ai+bj}\, y^{ci+j} \quad \text{for all } i \in \mathbb{Z}_{p^e},\ j \in \mathbb{Z}_p.$$

Therefore, $|\mathrm{Aut}(\mathcal{M}_e)| = (p-1)p^{e+1}$.

Proposition 4.9. *If* p *is an odd prime, then*

$$\mathrm{Skew}(\mathbb{Z}_{p^2}) = \mathrm{Aut}(\mathbb{Z}_{p^2}) \cup \Big\{ \alpha_a + a\nabla\alpha_b \mid a \in \mathbb{Z}_{p^2}^*, \mathrm{ord}^*(a) = pd, d > 1, b \in C_p, b \neq 0 \Big\}.$$

Proof. Let $\sigma \in \mathrm{Skew}(\mathbb{Z}_{p^2})$. We are going to show that σ is a permutation described in the statement. We put $G = \langle \tau, \sigma \rangle$ and let P be the Sylow p-subgroup of G. By Corollary 3.4, $\mathrm{ord}(\sigma) \mid p(p-1)$. Let $\mathrm{ord}(\sigma) = p^f d$ for a divisor d of $p-1$. Because of Sylow's Theorem $P \lhd G$, and thus $\mu = \sigma^p$ acts on P by conjugation as an automorphism; denote by $\overline{\mu}$ the induced automorphism. If $f = 0$, then $P = (\mathbb{Z}_{p^2})_L$, and $\sigma = \mu$ is an automorphism of $\mathbb{Z}_{p^2}$ of order d.

Let $f > 0$. Then with a suitable choice $\sigma_0 \in \langle \sigma^d \rangle$ we have

$$P = \big\langle \tau, \sigma_0 \mid \tau^{p^2} = \sigma_0^{\,p} = 1, \tau^{\sigma_0} = \tau^{p+1} \big\rangle \cong \mathcal{M}_2.$$

By Lemma 4.8, $\overline{\mu} = \theta_{u,v,w}$ for some $u \in \mathbb{Z}_{p^2}^*$, $v \in C_p$ and $w \in \mathbb{Z}_p$. Now, $\mathrm{ord}(\overline{\mu}) = \mathrm{ord}(\mu) = d$, and $\overline{\mu}$ fixes σ_0. These imply that $u \in \mathbb{Z}_{p^e}^*$ has $\mathrm{ord}^*(u) = d$, and $v = 0$. If $u = 1$, then $\overline{\mu} = \theta_{1,0,1}$ is the identity, and in this case σ is an automorphism of $\mathbb{Z}_{p^2}$ of order p. Let $u > 1$. Then $\overline{\mu} = \theta_{u,0,w}$ for some $w \in \mathbb{Z}_p$. Then

$$\mu\tau\mu^{-1} = \overline{\mu}(\tau) = \theta_{u,0,w}(\tau) = \tau^u\, \alpha_{p+1}^w. \tag{4.2}$$

Using the fact that $\mu(0) = 0$, μ is determined by (4.2). We obtain that $\mu(x) = u(1 + (p+1)^w + \cdots + (p+1)^{w(x-1)})$ for all $x \in \mathbb{Z}_{p^2}, x \neq 0$. Because $(p+1)^y = yp + 1$ in $\mathbb{Z}_{p^2}$ for all $y \in \mathbb{Z}_{p^2}$, we may write $\mu = \alpha_u + u\nabla\alpha_b$, where $b = wp$ is in C_p. This gives $\sigma = \alpha_{a'}\mu$ for $a' \in \mathbb{Z}_{p^2}^*, \mathrm{ord}^*(a') = p$. Therefore $\sigma = \alpha_a + a\nabla\alpha_b$, where $a = a'u$. Now, σ is a pure skew-morphism if and only if $b \neq 0$.

Conversely, let $\sigma = \alpha_a + a\nabla\alpha_b$, $a \in \mathbb{Z}_{p^2}^*$, $\mathrm{ord}^*(a) = pd, d > 1, b \in C_p, b \neq 0$. Then $a = a'a''$ for $a', a'' \in \mathbb{Z}_{p^2}^*$ with $\mathrm{ord}(a') = p$ and $\mathrm{ord}^*(a'') = d$. From this $\sigma = \alpha_{a'}\sigma'$ for $\sigma' = \alpha_{a''} + a''\nabla\alpha_b$. From the above discussion it follows that σ' normalizes $P = \langle \tau, \alpha_{p+1} \rangle$. This implies $\langle \tau, \sigma \rangle = \langle P, \sigma' \rangle = P\langle \sigma' \rangle = \langle \tau \rangle \langle \sigma \rangle$, so that σ is a skew-morphism of $\mathbb{Z}_{p^2}$. □

The formula for the number $|\mathrm{Skew}(\mathbb{Z}_{p^2})|$ of all skew-morphisms of $\mathbb{Z}_{p^2}$ follows directly from Proposition 4.9.

Corollary 4.10. *If* p *is an odd prime, then* $|\mathrm{Skew}(\mathbb{Z}_{p^2})| = (p-1)(p^2 - 2p + 2)$.

5 S-rings $V(\sigma)$ over $\mathbb{Z}_{pq}$

We recall that the wreath product $\mathbb{Z}(\mathbb{Z}_q) \wr \mathbb{Z}(\mathbb{Z}_p)$ of S-rings $\mathbb{Z}(\mathbb{Z}_q)$ and $\mathbb{Z}(\mathbb{Z}_p)$ is the S-ring over $\mathbb{Z}_{pq}$ that has basic sets $\{x\}, x \in C_p$ and the cosets $C_p + y, y \in \mathbb{Z}_{pq} \setminus C_p$. Similarly the wreath product $\mathbb{Z}(\mathbb{Z}_p) \wr \mathbb{Z}(\mathbb{Z}_q)$ is the S-ring over $\mathbb{Z}_{pq}$ that has basic sets $\{x\}, x \in C_q$ and the cosets $C_q + y, y \in \mathbb{Z}_{pq} \setminus C_q$. Two distinct primes p, q will be called *disjoint* if neither $q \mid (p-1)$, nor $p \mid (q-1)$.

Theorem 5.1. *Let $q < p$ be distinct primes and σ be a skew-morphism of $\mathbb{Z}_{pq}$. Then $V(\sigma) = V(\alpha)$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_{pq})$, unless $q \mid (p-1)$ and $V(\sigma) = \mathbb{Z}(\mathbb{Z}_q) \wr \mathbb{Z}(\mathbb{Z}_p)$.*

Proof. Let σ be a pure skew-morphism of $\mathbb{Z}_{pq}$ of order $\mathrm{ord}(\sigma) = m$. By Proposition 3.5, not all subgroups of $\mathbb{Z}_{pq}$ are $V(\sigma)$-subgroups. The S-ring $V(\sigma)$ is neither trivial, hence either $\underline{C_p} \in V(\sigma)$ and $\underline{C_q} \notin V(\sigma)$, or $\underline{C_p} \notin V(\sigma)$ and $\underline{C_q} \in V(\sigma)$. We show that in the first case $q \mid (p-1)$ and $\overline{V(\sigma)} = \mathbb{Z}(\mathbb{Z}_q) \wr \mathbb{Z}(\mathbb{Z}_p)$ as described above. Then by the symmetry, the second case implies $p \mid (q-1)$, a contradiction.

We put $G = \langle \tau, \sigma \rangle$, and let $\mathcal{B}$ be the block system of G formed by the C_p-cosets. Thus $m = pd$, for some $d \mid (q-1)$. Let $G_{\mathcal{B}}$ denote the kernel of G acting on $\mathcal{B}$. It is obvious that τ^q is in $G_{\mathcal{B}}$. By Proposition 2.4.(ii), $\sigma^{\mathcal{B}}$ is a skew-morphism of $\mathbb{Z}_{pq}/C_P \cong \mathbb{Z}_q$. It follows from the classification of S-rings over $\mathbb{Z}_{pq}$ that any basic set of $V(\sigma)$, which is not contained in C_p, is a union of C_p-cosets (e.g. [13]). Let T be an orbit of σ such that $\langle T \rangle = \mathbb{Z}_{pq}$. By Corollary 2.3, $|\sigma| = |T|$ and $|\sigma^{\mathcal{B}}| = |T/C_p| = |T|/p$. This implies that $|G/G_{\mathcal{B}}| = |G|/p^2$ and $|\langle \sigma \rangle \cap G_{\mathcal{B}}| = |\langle \sigma \rangle : \langle \sigma^B \rangle| = p$, and thus σ^d is in $G_{\mathcal{B}}$. We conclude that

$$G_{\mathcal{B}} = \langle \tau^q, \sigma^d \rangle = \langle \tau^q \rangle \times \langle \sigma^d \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Consider the group $N = \langle \tau \rangle G_{\mathcal{B}}$. Then $N = \langle \tau \rangle \langle \sigma^d \rangle$, and σ^d is a pure skew-morphism of $\mathbb{Z}_{pq}$ of order p. Clearly, $V(\sigma^d) = \mathbb{Z}(\mathbb{Z}_q) \wr \mathbb{Z}(\mathbb{Z}_p)$.

Since $N = G_{\mathcal{B}} \rtimes \langle \tau^p \rangle$, the element τ^p acts on $G_{\mathcal{B}}$ by conjugation as a group automorphism. We may identify τ^p with a matrix $A(\tau^p)$ in $\mathrm{GL}(2,p)$ such that for all $(i,j) \in \mathbb{Z}_p \times \mathbb{Z}_p$,

$$\left(\tau^{qi}\sigma^{dj}\right)^{\tau^p} = \tau^{qi'}\sigma^{dj'} \text{ if } \begin{pmatrix} i' \\ j' \end{pmatrix} = A(\tau^p) \begin{pmatrix} i \\ j \end{pmatrix}.$$

Now, τ^q is fixed by τ^p and $\langle \sigma^d \rangle$ is not normalized by τ^p. Also, $\mathrm{ord}(A(\tau^p)) = \mathrm{ord}(\tau^p) = q$. These conditions imply that

$$A(\tau^p) = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, a, b \in \mathbb{Z}_p^*,\ b^q = 1, b \neq 1.$$

It also follows that $q \mid (p-1)$.

Let $A = A(\tau^p)$. The group $N = \langle \tau^q, \sigma^d \rangle \rtimes \langle \tau^p \rangle$, and we may identify N with the group of all pairs (x, A^i), where $x = (x_1, x_2)^\top$ is in the vector space $V = \mathbb{Z}_p^2$, and $i \in \{0, 1, \ldots, q-1\}$. The group operation $*$ is defined as

$$(x, A^i) * (y, A^j) = (x + A^i y, A^{i+j}).$$

Note that $e_1 = (1,0)$ and $e_2 = (0,1)$ in V correspond to τ^q and σ^d, respectively. Denote $\mu = \sigma^p$.

Since $N \lhd G$, $G = N \rtimes \langle \mu \rangle$, and hence μ acts on N as a group automorphism. Denote this automorphism by $\overline{\mu}$. Then $\overline{\mu}$ satisfies the following conditions:

1. $\mathrm{ord}(\overline{\mu}) = d$,
2. $\overline{\mu}$ normalizes $\langle (e_1, I) \rangle$,
3. $\overline{\mu}$ fixes (e_2, I),

To see 1. observe that if $\mathrm{ord}(\overline{\mu}) < d$, then a subgroup $1 < M < \langle\mu\rangle$ centralizes N. In particular, M centralizes τ, hence M is semiregular, which is impossible. Condition 2. follows from the fact that $\langle\tau^q\rangle \triangleleft G$. Finally, Condition 3. follows from $\mu\sigma^d = \sigma^d\mu$. The above conditions imply

$$\overline{\mu}\colon \begin{cases} (x,I) \mapsto (Bx, I), \text{ where } B = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}, \text{ for some } c \in \mathbb{Z}_p^*. \\ (0,A) \mapsto (v, A^k) \text{ for some } v \in V, k \in \{1,\dots,q-1\} \end{cases}.$$

Since $\overline{\mu}$ is an automorphism, it is defined by the above images, and we have

$$\overline{\mu}\colon (x, A^i) \mapsto (Bx + (I + A^k + \cdots + A^{k(i-1)})v, A^{ki}).$$

In particular, $(I + A^k + \cdots + A^{k(q-1)})v = 0$. Then

$$\overline{\mu}\big((x,A)\big) * \overline{\mu}\big((y,I)\big) = \overline{\mu}\big((x,A) * (y,I)\big) = \overline{\mu}\big((x + Ay, A)\big).$$

Therefore $(Bx + v, A^k) * (By, I) = (Bx + A^kBy + v, A^k) = (Bx + BAy + v, A^k)$. From this $BAB^{-1} = A^k$, and thus

$$\begin{aligned} ac &\equiv a(1 + b + \ldots, b^{k-1}) \pmod p, \\ b^k &\equiv b \pmod p. \end{aligned}$$

Now $b \neq 1$ and $b^q = 1$ in $\mathbb{Z}_p^*$. As $k < q$, $b^k = b \pmod p$ implies $k = 1$. It follows that $c = 1$. We have $\overline{\mu}^d : (0,A) \mapsto (dv, A)$. Since $\overline{\mu}^d = id$, $dv = 0$ and so $v = 0$. Thus $\overline{\mu}$ is the identity, and $d = \mathrm{ord}(\mu) = 1$. We obtain $V(\sigma) = V(\sigma^d) = \mathbb{Z}(\mathbb{Z}_q) \wr \mathbb{Z}(\mathbb{Z}_p)$, as claimed. □

Let σ be a pure skew-morphism of $\mathbb{Z}_{pq}$. The order of σ equals $|T|$, where T is an orbit of σ such that $\langle T\rangle = \mathbb{Z}_{pq}$ (see Corollary 2.3). By Theorem 5.1 we obtain that a pure skew-morphism of $\mathbb{Z}_{pq}$ must have order either p or q. We conclude the section with describing the pure skew-morphisms of prime order in an arbitrary cyclic group $\mathbb{Z}_n$.

Let $n = mp$, where p is a prime. Then every element in $\mathbb{Z}_n$ is written as $xm + y$ for uniquely defined $x \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_m$. For $b \in \mathbb{Z}_p^*$ denote by π_b the function in $\mathrm{Fun}(\mathbb{Z}_m, \mathbb{Z}_p)$ defined as $\pi_b(x) = b^x$.

Proposition 5.2. *Let σ be a pure skew-morphism of $\mathbb{Z}_n$ of order p, p is a prime, and π be the power function of σ. Then $n = pm$, $(n, p-1) > 1$, and there exist $a, b \in \mathbb{Z}_p^*$, $b \neq 1$, $b^{(n,p-1)} = 1$ so that*

$$\begin{aligned} \sigma(z) &= z + ma(\nabla\pi_b)(y) \\ \pi(z) &= b^z \end{aligned}$$

for all $z \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_m$, $y \equiv z$ mod (m).

Moreover, every mapping $\sigma : \mathbb{Z}_{pm} \to \mathbb{Z}_{pm}$ given by the above formula is a pure skew-morphism of order p and a different choice of the parameters $a, b \in \mathbb{Z}_p^*$ gives different skew-morphisms.

Proof. We set $G = \langle \tau, \sigma \rangle$. Since σ is pure, by Proposition 3.1 $\operatorname{rad} V(\sigma) = C_p$, $\underline{C_p} \in V(\sigma)$ and $n = pm$ for some m. Then $\sigma|^m$ is the identity. The subgroup $(C_p)_L$ is centralized by σ. Therefore σ maps a $\mathbb{Z}_n$-element written in the form $xm + y$, $x \in \mathbb{Z}_p$, $y \in \mathbb{Z}_m$ as

$$\sigma(xm + y) = (x + c)m + y \text{ for some } c \in \mathbb{Z}_p.$$

The value c is the same for $x'm + y'$ whenever $y' = y$, and thus there is a function $\varphi\colon \mathbb{Z}_m \to \mathbb{Z}_p$ which associates $c = \varphi(y)$ with $y \in \mathbb{Z}_m$. As $\sigma(0) = 0$, we have $\varphi(0) = 0$. Let $\sigma(1) = am + 1 \in C_p + 1$ (see (ii) in Lemma 4.4). Then $a \neq 0$, and $\varphi(1) = a$.

By (3.1), $\sigma\tau = \tau^{am+1}\sigma^{\pi(1)}$. For $mx + y \in \mathbb{Z}_n$,

$$(\sigma\tau)(xm + y) = \big(x + \varphi(y + 1)\big)m + y + 1,$$

and also

$$\tau^{am+1}\sigma^{\pi(1)}(xm + y) = \big(x + \pi(1)\varphi(y) + a\big)m + y + 1.$$

Combining these equations we find

$$\varphi(y + 1) = \pi(1)\varphi(y) + a \text{ for all } y \in \mathbb{Z}_m. \tag{5.1}$$

Applying (5.1) repeatedly leads to

$$a(1 + \pi(1) + \pi(1)^2 + \cdots + \pi(1)^{m-1}) \equiv 0 \,(\mathrm{mod}\, p). \tag{5.2}$$

Since $\sigma \notin \operatorname{Aut}(\mathbb{Z}_n)$, $\pi(1) \in \{2, \ldots, p - 1\}$. Thus (5.2) is equivalent to $\pi(1)^m = 1$ in $\mathbb{Z}_p$. This means $(n, p - 1) > 1$, and $\pi(1)^{(n,p-1)} = 1$ holds. Inserting $b = \pi(1)$ into (5.1) and solving, we get $\varphi = a(\nabla\pi_b)$. Thus σ has the form as claimed.

It remains to prove that σ is indeed a skew-morphism and to determine its power function π. It is clear that $\sigma\tau^m = \tau\sigma^m$. We claim that,

$$\sigma\tau^z = \tau^{\sigma(z)}\sigma^{b^z} \text{ for all } z \in \mathbb{Z}_n. \tag{5.3}$$

We prove (5.3) by induction on z. The equality is clear if $z = 0$ or $z = 1$. The induction hypothesis gives

$$\sigma\tau^{z+1} = \sigma\tau^z\tau = \tau^{\sigma(z)}\sigma^{b^z}\tau = \tau^{\sigma(z)}\sigma^{b^z-1}\tau^{am+1}\sigma^b.$$

Using $\sigma\tau^{am} = \tau^{am}\sigma$ and $b^z = b^y$ if $z = mx + y$ we conclude

$$\begin{aligned} \sigma\tau^{z+1} &= \tau^{\sigma(z)+am}\sigma^{b^z-1}\tau\sigma^b \\ &= \tau^{\sigma(z)+2am}\sigma^{b^z-2}\tau\sigma^{2b} \\ &\cdots \\ &= \tau^{\sigma(z)+b^z am+1}\sigma^{b^{z+1}} = \tau^{\sigma(z+1)}\sigma^{b^{z+1}}. \end{aligned}$$

Comparing (5.3) with (3.1) we see that σ is a skew-morphism of $\mathbb{Z}_n$ and that the power function π is given by $\pi(z) = b^z$, $z \in \mathbb{Z}_n$. □

The formula for $|\operatorname{Skew}(\mathbb{Z}_{pq})|$ follows directly from Theorem 5.1 and Proposition 5.2.

Corollary 5.3. *If p, q are distinct primes, then*

$$|\operatorname{Skew}(\mathbb{Z}_{pq})| = \begin{cases} (p-1)(q-1) & \text{if } p \not| (q-1) \text{ and } q \not| (p-1) \\ 2(p-1)(q-1) & \text{if } q \mid (p-1) \text{ or } p \mid (q-1). \end{cases}$$

6 Decomposing skew-morphism of cyclic groups

We are now in a position to prove our decomposition theorem.

Proof of Theorem 1.1. Let $\sigma \in \mathrm{Skew}(\mathbb{Z}_n)$. First, we prove that σ decomposes as $\sigma = \sigma_1 \times \sigma_2$, where $\sigma_i \in \mathrm{Skew}(\mathbb{Z}_{n_i})$ for $i = 1, 2$. Let $\mathcal{A} = V(\sigma)$. We claim that $\underline{C_{n_i}} \in \mathcal{A}$ for $i = 1, 2$. This we prove by induction on n. If both n_1 and n_2 are primes, then we are done by Theorem 5.1.

Let π be the power function of σ. By Corollary 3.2 $\ker \pi \neq 1$. Choose $C_p \leq \ker \pi$, where p is a prime. Thus $\underline{C_p} \in \mathcal{A}$, and C_p is contained either in C_{n_1} or in C_{n_2}, say $C_p \leq C_{n_1}$. Consider the quotient S-ring $\mathcal{A}/C_p = V(\sigma|^{n/p})$. By the induction hypothesis we get that $\underline{C_{n_1}/C_p}$ and $\underline{C_{n_2p}/C_p}$ are in $\mathcal{A}/C_p$. It follows that $\underline{C_{n_1}} \in \mathcal{A}$. Next C_{n_2p}/C_p contains a subgroup of prime order q ($p \neq q$) which is contained in $\mathcal{A}/C_p$. Consequently, $\underline{C_{pq}} \in \mathcal{A}$. By the assumptions p, q are disjoint primes, hence $\underline{C_q} \in \mathcal{A}$, see Theorem 5.1. Repeating the previous argument with $C_q \leq C_{n_2}$ we deduce that also $\underline{C_{n_2}} \in \mathcal{A}$.

Let us write $\mathbb{Z}_n = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Since $\underline{C_{n_i}} \in \mathcal{A}$ for $i = 1, 2$, the quotient skew-morphisms $\sigma|^{n_i}$, $i = 1, 2$ are well defined and we have

$$\sigma((x_1, x_2)) = \big(\sigma|^{n_1}(x_1), \sigma|^{n_2}(x_2)\big) \text{ for all } (x_1, x_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}.$$

Therefore $\sigma = \sigma|^{n_1} \times \sigma|^{n_2}$.

Second, we prove that for all $\sigma_i \in \mathrm{Skew}(\mathbb{Z}_{n_i})$, $i = 1, 2$, $\sigma_1 \times \sigma_2 \in \mathrm{Skew}(\mathbb{Z}_n)$. Let $G_i = \langle \tau_i, \sigma_i \rangle$ for $i = 1, 2$, where τ_i is the permutation $x \mapsto x + 1$ of $\mathbb{Z}_{n_i}$. Let $\widehat{G}$ be the permutation direct product $\widehat{G} = G_1 \times G_2$. Clearly, $\sigma \in \widehat{G}$. If both σ_1 and σ_2 are automorphisms, then we are done. Assume that σ_1 is a pure skew-morphism. Thus there exists a prime divisor p of n_1 such that $\mathrm{ord}(\sigma|^{n_1/p}) = \mathrm{ord}(\sigma_1)/p$ and $\underline{C_p} \in V(\sigma_1) \otimes V(\sigma_2)$. Let $\mathcal{B}$ be the block system of $\widehat{G}$ formed by the C_p-cosets. Then

$$\widehat{G}_{\mathcal{B}} = \langle (C_p)_L, (\sigma_1^{n_1/p}, 1) \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Corollary 3.4 gives $\mathrm{ord}(\sigma_2) \mid n_2\phi(n_2)$, and thus $p \nmid \mathrm{ord}(\sigma_2)$. We conclude that $\langle (\sigma_1^{n_1/p}, 1) \rangle$ is the only subgroup of order p in $\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle$. We put $\sigma = \sigma_1 \times \sigma_2$, $\tau = \tau_1 \times \tau_2$ and $G = \langle \tau, \sigma \rangle$. Then $(\sigma_1^{n_1/p}, 1) \in \langle \sigma \rangle$ and $\widehat{G}_{\mathcal{B}} \leq G$.

$$|G|/|\widehat{G}_{\mathcal{B}}| = |(\widehat{G}_{\mathcal{B}} G)/\widehat{G}_{\mathcal{B}}| = |G^{\mathcal{B}}| = \Big|\langle (\tau_1 \times \tau_2)^{\mathcal{B}}, \sigma^{\mathcal{B}} \rangle\Big|.$$

We have $(\tau_1 \times \tau_2)^{\mathcal{B}} = \tau_1^{\mathcal{B}} \times \tau_2 \cong \mathbb{Z}_{n_1/p} \times \mathbb{Z}_{n_2}$, and $\sigma^{\mathcal{B}} = \sigma_1^{\mathcal{B}} \times \sigma_2 = \sigma_1|^{n_1/p} \times \sigma_2$. Induction gives $\sigma_1|^{n_1/p} \times \sigma_2 \in \mathrm{Skew}(\mathbb{Z}_{n/p})$, hence

$$\Big|\langle (\tau_1 \times \tau_2)^{\mathcal{B}}, \sigma^{\mathcal{B}} \rangle\Big| = n/p \times \mathrm{ord}(\sigma_1|^{n_1/p} \times \sigma_2) = n/p \times \frac{\mathrm{ord}(\sigma_1|^{n_1/p})\,\mathrm{ord}(\sigma_2)}{\big(\,\mathrm{ord}(\sigma_1|^{n_1/p}), \mathrm{ord}(\sigma_2)\,\big)}$$

As $\mathrm{ord}(\sigma_1|^{n_1/p}) = \mathrm{ord}(\sigma_1)/p$ and $p \nmid \mathrm{ord}(\sigma_2)$, we can further write

$$|G| = |\widehat{G}_{\mathcal{B}}||G^{\mathcal{B}}| = p^2 \times \Big|\langle (\tau_1 \times \tau_2)^{\mathcal{B}}, \sigma^{\mathcal{B}} \rangle\Big| = n \frac{\mathrm{ord}(\sigma_1)\,\mathrm{ord}(\sigma_2)}{\big(\,\mathrm{ord}(\sigma_1), \mathrm{ord}(\sigma_2)\,\big)}.$$

It follows that $G = \langle \tau \rangle \langle \sigma \rangle$ and $\sigma = \sigma_1 \times \sigma_2$ is a skew-morphism of $\mathbb{Z}_n = \langle \tau \rangle$. □

A simple induction leads to the following corollary on the number $|\operatorname{Skew}(\mathbb{Z}_n)|$ of all skew-morphisms of $\mathbb{Z}_n$.

Corollary 6.1. *Let n be an odd integer which decomposes into a product of powers of mutually disjoint primes $n = \prod_{i=1}^{k} p_i^{e_i}$. Then every skew-morphism of $\mathbb{Z}_n$ is a near automorphism and*

$$|\operatorname{Skew}(\mathbb{Z}_n)| = \prod_{i=1}^{k} |\operatorname{Skew}(\mathbb{Z}_{n_i})|.$$

A number $n \geq 1$ is *singular* if $(n, \phi(n)) = 1$. The following result was proved by Jones, Nedela and Škoviera in [10].

Theorem 6.2. *There is one unique orientably regular embedding of $K_{n,n}$ if and only if n is singular.*

We conclude the paper with a similar result about arbitrary skew-morphisms of $\mathbb{Z}_n$.

Theorem 6.3. *All skew-morphisms of $\mathbb{Z}_n$ are automorphisms of $\mathbb{Z}_n$ if and only if $n = 4$ or n is singular.*

Proof. Let n have decomposition $n = n_1 n_2 \dots n_k$ such that for all distinct $i, j \in \{1, 2, \dots, k\}$, $(n_i, n_j) = 1$, and $(n_i, \varphi(n_j)) = (n_j, \varphi(n_i)) = 1$. Now, all skew-morphisms of $\mathbb{Z}_n$ are automorphisms of $\mathbb{Z}_n$ if and only if $|\operatorname{Skew}(\mathbb{Z}_n)| = \phi(n)$. Because of Cororllary 6.1 this is equivalent to $|\operatorname{Skew}(\mathbb{Z}_{n_i})| = \phi(n_i)$ for all $i \in \{1, \dots, k\}$. Proposition 5.2 shows that $|\operatorname{Skew}(\mathbb{Z}_{n_i})| > \phi(n_i)$ if $n_i \neq p_i^e$ for some prime p_i. Thus if n is even, then we must have $n = 2^e$. It follows readily that $|\operatorname{Skew}(\mathbb{Z}_{2^e})| = \phi(2^e)$ if and only if $n \leq 4$ (see also the remark following the proof of Theorem 4.1).

Let n be odd. Then by Proposition 4.9, $|\operatorname{Skew}(\mathbb{Z}_{n_i})| = \phi(n_i)$ if and only if n_i is an odd prime for all $i \in \{1, \dots, k\}$, and this means exactly that n is singular. □

Theorem 6.2 now becomes an easy corollary of Theorem 6.3.

Acknowledgements

A visit of the first author to the Institute of Mathematics, Slovak Academy of Science in Banská Bystrica in September 2008 helped us to write the paper. The first author thanks the Institute of Mathematics for supporting his trip. We would like to thank one of the anonymous referees for helpful suggestions that have improved both the content and the presentation of the paper.

References

[1] J. M. S. Bidwell and M. J. Curran, The automorphism group of a split metacyclic p-group, *Archiv der Mathematik* **87** (2006), 488–497.

[2] M. Conder, private communication.

[3] M. Conder, R. Jajcay and T. Tucker, Regular t-balanced Cayley maps, *J. Combin. Theory B* **97** (2007), 453–473.

[4] M. Conder, R. Jajcay and T. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebraic Combin.* **25** (2007), 259–283.

[5] S-F. Du, G. A. Jones, J. H. Kwak, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2 I: Metacyclic case, *European J. Combin.* **28** (2007), 1595–1609.

[6] S-F. Du, G. A. Jones, J. H. Kwak, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2 II: Non-metacyclic case, accepted for publication in *European J. Combin.*

[7] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179.

[8] G. A. Jones, Complete bipartite maps, factorisable groups and generalized Fermat curves, in: Koolen, Kwak and Xu (eds.), *Applications of Group Theory to Combinatorics*, Taylor and Francis Group, London 2008, 43–58.

[9] G. A. Jones, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is an odd prime power, *European J. Combin.* **28** (2007), 1863–1875.

[10] G. A. Jones, R. Nedela and M. Škoviera, Complete bipartite graphs with a unique regular embedding, *J. Combin. Theory B* **98** (2008), 241–248.

[11] S. A. Evdokimov and I. N. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, *St. Petersburg Math. J.* **14** (2002), No. 2, 189-221.

[12] J-Q. Feng, J. H. Kwak and R. Nedela, Regular embeddings of complete bipartite graphs and skew-morphisms of cyclic groups, preprint.

[13] M. Klin and R. Pöschel, The König Problem, the isomorphism problem for cyclic graphs and the method of Schur rings, in: *Algebraic Methods in Graph Theory, Szeged, 1978*, *Colloq. Math. Soc. János Bolyai*, Vol. 25, North-Holland, Amsterdam (1981), 405-434.

[14] J. H. Kwak and Y. S. Kwon, Regular orientable embeddings of complete bipartite graphs, J. Graph Theory **50** (2005), 105–122.

[15] M. E. Muzychuk, M. H. Klin and R. Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, *DIMACS Series in Discrete Math. and Theoretical Comp. Sci.* **56** (2001), 241–264.

[16] K. H. Leung and S. L. Man, On Schur rings over cyclic groups II, *J. Algebra* **186** (1996), 273–285.

[17] H. Wielandt, *Finite Permutation Groups*, Academic Press, Berlin 1964.