J. Group Theory **20** (2017), 1135–1154
DOI 10.1515/jgth-2017-0015

Skew-morphisms of cyclic p-groups

István Kovács and Roman Nedela

Communicated by Andrea Lucchini

Abstract. Let G be a finite group having a factorisation $G = AB$ into subgroups A and B with B cyclic and $A \cap B = 1$, and let b be a generator of B. The associated skew-morphism is the bijective mapping $f : A \to A$ well-defined by the equality $baB = f(a)B$, where $a \in A$. In this paper, we shall classify all skew-morphisms of cyclic p-groups, where p is an odd prime.

1 Introduction

Following Jajcay and Širáň [9], a *skew-morphism* of a finite group A is a bijective mapping $f : A \to A$ fixing the identity element of A and having the property that $f(xy) = f(x)f^{\pi(x)}(y)$ for all $x, y \in A$, where the integer $\pi(x)$ depends only on x. We also refer to the mapping $\pi : A \to \mathbb{Z}$ as a *power function* corresponding to f. The original motivation to investigate skew-morphisms of groups come from the characterisation of regular Cayley maps proved by Jajcay and Širáň [9]: "A Cayley map $CM(G;\rho)$, where G is a group and ρ is a cyclic permutation of the generators is regular if and only if ρ extends to a skew-morphism of G". Note that the orbit of ρ is by definition closed under taking inverses and the existence of at least one generating orbit closed under taking inverses is a characteristic feature of skew-morphisms related to Cayley regular maps. Recall that to define a 2-cell embedding of a connected graph into an orientable surface combinatorially one needs to determine a cyclic permutation of arcs based at v for each vertex v. A Cayley map is an embedding of a Cayley graph into an orientable surface such that a chosen global orientation induces at each vertex the same cyclic permutation of generators. Cayley maps are vertex-transitive, since each Cayley automorphism of the graph extends to an automorphism of the map. If the group of map automorphisms is regular on arcs, the map itself is called regular. Another geometric

The first author was supported in part by the Slovenian Research Agency (research program P1-0285, and research projects N1-0032, N1-0038, J1-5433 and J1-6720). The second author was supported by the grant APVV-15-0220, by the project LO1506 of the Czech Ministry of Education, Youth and Sports, and Project P202/12/G061 of Czech Science Foundation.

motivation for investigation of skew-morphisms can be found in papers [8, 13], where skew-morphisms are studied in connection with highly symmetrical hypermaps and with regular embeddings of complete bipartite graphs.

Although the concept of a skew-morphism was introduced and investigated in the context of regular Cayley maps and hypermaps, see [3, 5, 8, 9], Conder, Jajcay and Tucker [4] pointed out that it appeared already in the context of factorisation of groups. Namely, let G be a finite group having a factorisation $G = AB$ into subgroups A and B with B cyclic and $A \cap B = 1$, and let b be a generator of B. Then there exists a bijective mapping $f : A \to A$ well-defined by the equality $baB = f(a)B$, where $a \in A$. It is not hard to show that f is a skew-morphism of A. Moreover, all skew-morphisms of A arise in this way. Every automorphism of A is a skew-morphism with the power function $\pi(x) = 1$ for all $x \in A$; the converse, however, does not hold in general. In particular, the normality of A in $G = AB$, is a necessary and sufficient condition for a skew-morphism defined by this factorisation to be an automorphism. There are plenty of factorisations AB, where A is not normal and B is cyclic, and there are many skew-morphisms that are not automorphisms, even in the case when A is cyclic. Particular examples of skew-morphisms which are not group automorphisms were given in [1, 4, 12] for abelian groups and in [4, 14] for dihedral groups. The problem of determining all skew-morphisms for a given group arises. Since every automorphism is a skew-morphism, this problem is at least as hard as the problem of determining $\mathrm{Aut}(G)$ for a given group G, which is not an easy task in general. One of the problems one needs to overcome consists in the fact that the composition of two skew-morphisms of G may not be a skew-morphism. Even to determine the skew-morphisms of cyclic groups seems to be a difficult problem.

Problem. Determine the skew-morphisms of cyclic groups.

In this paper, we make a step towards its solution by determining all skew-morphisms for cyclic p-groups, where $p > 2$ is an odd prime. The next natural step to accomplish is a determination of skew-morphisms of cyclic 2-groups. A partial solution of the above problem appears in [5], where skew-morphisms containing a generating orbit closed under taking inverses are classified.

In [12], we investigated skew-morphisms of cyclic groups in connection with Schur rings of cyclic groups. Among others we proved the following decomposition theorem. In what follows we denote by $\mathrm{Skew}(\mathbb{Z}_n)$ the set of skew-morphisms of the cyclic additive group $\mathbb{Z}_n$, and by ϕ Euler's totient function.

Theorem 1.1 (cf. [12, Theorem 1.1]). *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, and $\gcd(n_1, \phi(n_2)) = \gcd(\phi(n_1), n_2) = 1$. Then $\sigma \in \mathrm{Skew}(\mathbb{Z}_n)$ if and only if σ is of the form $\sigma = \sigma_1 \times \sigma_2$, where $\sigma_1 \in \mathrm{Skew}(\mathbb{Z}_{n_1})$ and $\sigma_2 \in \mathrm{Skew}(\mathbb{Z}_{n_2})$.*

It was shown in [12, Corollary 4.10] (and reproved in [4, Theorem 6.4]) that the cyclic group $\mathbb{Z}_{p^2}$ has exactly $(p-1)(p^2-2p+2)$ skew-morphisms, where p is an odd prime. In this paper, we generalise this result to the cyclic group $\mathbb{Z}_{p^e}$ of order p^e with arbitrary $e \geq 2$ by proving

Theorem 1.2. *If $e \geq 2$ and p is an odd prime, then the cyclic group $\mathbb{Z}_{p^e}$ has exactly $(p-1)(p^{2e-1}-p^{2e-2}+2)/(p+1)$ skew-morphisms.*

Detailed description of the set $\text{Skew}(\mathbb{Z}_{p^e})$ of skew-morphisms can be found in Theorems 5.4 and 5.5, which are the main results of the paper.

The paper is organised as follows. In the next section we recall some known facts for further use. Among others we state in Lemma 2.1 that the order of a skew-morphism of a cyclic group $\mathbb{Z}_n$ divides $n\phi(n)$. In particular, if $n = p^e$ for a prime p, the skew-morphisms split into two classes: the first class contains those skew-morphisms whose order is a power of p, the others form the complement of the first class. In Section 3 we define a two-parametrised family of skew-morphisms $s_{i,j}$ and investigate its properties. Although the skew-morphisms of a group do not form a group in general, in the investigated case of cyclic p-groups, the skew-morphism $s_{i,j}$ all "live" in a split metacyclic group $G = CY$ of order p^{2e-1}, where C is a normal cyclic subgroup of order p^e and Y is cyclic of order p^{e-1}, see Remark 3.2. In Section 4 the above family is generalised to a family of skew-morphisms $s_{i,j,k,l}$ given by four integer parameters i, j, k, l. Finally, in the last section we prove that every skew-morphism in $\text{Skew}(\mathbb{Z}_{p^e})$ is one of $s_{i,j,k,l}$, and that the skew-morphisms of the first class are exactly the skew-morphisms $s_{i,j} = s_{i,j,0,0}$, see Theorems 5.4 and 5.5. For the purpose of enumeration we clarify in Proposition 4.4 which 4-tuples of parameters determine the same skew-morphism.

A key role in our investigation is played by Huppert's theorem [7, III.11.5] establishing the structure of the skew product group in case the order of the skew-morphism is a power of p, and also by a result of King [11] on presentations of metacyclic p-groups. In the proof that the parametrised family of skew-morphisms $s_{i,j,k,l}$ equals $\text{Skew}(\mathbb{Z}_{p^e})$, we use some essential information on automorphisms of split metacyclic p-groups obtained by Bidwell and Curran [2].

2 Preliminary results

Throughout the paper $\mathbb{Z}_{p^e}$ represents the cyclic group of order p^e, where p is an odd prime. Let $\text{Sym}(\mathbb{Z}_{p^e})$, $\text{Aut}(\mathbb{Z}_{p^e})$ and $\text{Skew}(\mathbb{Z}_{p^e})$ denote the set (group) of all permutations, automorphisms, and skew-morphisms of $\mathbb{Z}_{p^e}$, respectively. In this paper we multiply permutations from the right to the left, that is, if f and g

are in $\mathrm{Sym}(\mathbb{Z}_{p^e})$ and $x \in \mathbb{Z}_{p^e}$, then $(fg)(x) = f(g(x))$. We set t to denote the translation of $\mathbb{Z}_{p^e}$ defined by $t(x) = x + 1$.

Let $s \in \mathrm{Skew}(\mathbb{Z}_{p^n})$ be a skew-morphism with power function π. The *skew product group* of $\mathbb{Z}_{p^e}$ induced by s is the group $\langle t, s\rangle$. Notice that the skew product group factorises as $\langle t, s\rangle = \langle t\rangle\langle s\rangle$, and for every $i \in \mathbb{Z}_{p^e}$,

$$st^i = t^{s(i)} s^{\pi(i)}. \tag{2.1}$$

Also, $|\langle t, s\rangle| = p^e \cdot |s|$, where $|s|$ is the order of the permutation s. The following converse also holds (see [12, Proposition 2.2]): if $f \in \mathrm{Sym}(\mathbb{Z}_{p^e})$, then

$$f(0) = 0 \text{ and } |\langle t, f\rangle| = p^e \cdot |f| \implies f \in \mathrm{Skew}(\mathbb{Z}_{p^e}). \tag{2.2}$$

The next result is in [12, Corollary 3.4], see [4, Theorem 6.1], as well.

Lemma 2.1. *Let $s \in \mathrm{Skew}(\mathbb{Z}_n)$. Then the order $|s|$ of s divides $n\phi(n)$. Moreover, if* $\gcd(|s|, n) = 1$ *or* $\gcd(\phi(n), n) = 1$*, then s is an automorphism of $\mathbb{Z}_n$.*

In the next lemma we collect a number of properties of skew-morphisms of $\mathbb{Z}_{p^e}$ proved in [12]. In fact, part (i) is [12, Lemma 4.4 (iii)], (ii) is [12, Lemma 4.4 (ii)], and (iii) is [12, Theorem 4.1].

Lemma 2.2. *Let $s \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ be a skew-morphism of order p^i with power function π.*

(i) *The power s^p is also in* $\mathrm{Skew}(\mathbb{Z}_{p^e})$.

(ii) *For all $x \in \mathbb{Z}_{p^e}$, $\pi(x) \equiv 1 \pmod p$. In particular, if s has order p, then s is in* $\mathrm{Aut}(\mathbb{Z}_{p^e})$.

(iii) *There exists an automorphism $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^e})$ of order p^i such that the $\langle\alpha\rangle$-orbits coincide with the $\langle s\rangle$-orbits.*

It is well known that $\mathrm{Aut}(\mathbb{Z}_{p^e}) \cong \mathbb{Z}_{(p-1)p^{e-1}}$, and the automorphisms of order p^i $(1 \le i \le e-1)$ are given as

$$x \mapsto (kp^{e-i} + 1)x, \tag{2.3}$$

where $k \in \{1, \dots, p^i - 1\}$ and $p \nmid k$ (see, e.g., [10]). This implies that, for any $k \in \{0, \dots, p^n - 1\}$,

$$\gcd((p+1)^k - 1, p^e) = p \cdot \gcd(k, p^{e-1}). \tag{2.4}$$

Lemma 2.3. *Let $s \in \mathrm{Skew}(\mathbb{Z}_{p^e})$ be a skew-morphism of order p^i. Then*

$$\gcd(s(1) - 1, p^e) = p^{e-i}.$$

Proof. The statement is clear if $i = 0$, let $i \geq 1$. According to Lemma 2.2 (iii), the orbit of 1 under $\langle s \rangle$ is equal to the orbit of 1 under $\langle \alpha \rangle$ for some automorphism α of order p^i. By (2.3), this orbit is $\Omega := \{xp^{e-i} + 1 : x \in \{0, \dots, p^i - 1\}\}$. This in turn implies that $\langle s \rangle$ is regular on Ω, and thus $s(1)$ is not in the orbit of 1 under $\langle s^p \rangle$. Since s^p is a skew-morphism, see Lemma 2.2 (i), it follows that $s(1) \notin \{xp^{e-i+1} + 1 : x \in \{0, \dots, p^{i+1} - 1\}\}$. The lemma is proved. □

We end the section with a property of metacyclic p-groups.

Lemma 2.4. *Let G be a metacyclic p-group given by the presentation*

$$G = \left\langle x, y \mid x^{p^m} = y^{p^n} = 1,\ x^y = x^{1+p^{m-n}} \right\rangle,$$

where $m > n \geq 1$. Then the order of the element $x^i y^j$ is equal to $\max\{|x^i|, |y^j|\}$, *where $|x^i|$ and $|y^j|$ denote the order of x^i and y^j, respectively.*

Proof. We prove the lemma by induction on m. If $m = 2$, then G is the unique non-abelian group of order p^3 and of exponent p^2. In this case the lemma follows by a straightforward computation.

Let $m \geq 3$ and $N = \langle x^{p^{m-1}}, y^{p^{n-1}} \rangle$. We claim that $N \cong \mathbb{Z}_p^2$, N is normal in G. Indeed, setting $z = y^{p^{n-1}}$ and $w = x^{p^{m-1}}$, we have $z^{-1}xz = x^1 w^k$, for some k. It follows that $x^{-1}z^{-1}x = w^k z^{-1} \in N$, and so conjugation by both x and y fixes $N = \langle z, w \rangle$. The factor group G/N admits the presentation

$$G/N = \left\langle \bar{x}, \bar{y} \mid \bar{x}^{p^{m-1}} = \bar{y}^{p^{n-1}} = 1,\ \bar{x}^{\bar{y}} = \bar{x}^{1+p^{m-n}} \right\rangle,$$

where for $g \in G$, $\bar{g}$ denotes the image of g under the natural homomorphism $G \to G/N$. The lemma holds trivially if either $x^i = 1$ or $y^j = 1$, hence we assume below that $x^i \neq 1$ and $y^j \neq 1$. Then we find, using the induction hypothesis, that the order of $\bar{x}^i \bar{y}^j$ is equal to $\max\{|\bar{x}^i|, |\bar{y}^j|\} = \frac{1}{p} \max\{|x^i|, |y^j|\}$. Therefore, we are done if we show that $\bar{x}^i \bar{y}^j$ has order $\frac{1}{p}|x^i y^j|$, where $|x^i y^j|$ denotes the order of $x^i y^j$. Obviously, $x^i y^j \neq 1$. Let z be an element in $\langle x^i y^j \rangle$ of order p. If $z \notin N$, then $\langle N, z \rangle$ is isomorphic to a group of order p^3 and of exponent p. This implies that $\langle N, z \rangle$ is not metacyclic, contradicting the fact that every subgroup of G is metacyclic (cf. [7, III.11.1]). Therefore, $z \in N$, and thus $\bar{x}^i \bar{y}^j$ has order $\frac{1}{p}|x^i y^j|$, as it is required. □

3 The skew-morphisms $s_{i,j}$

For the rest of the paper let $a \in \mathrm{Aut}(\mathbb{Z}_{p^e})$ be the automorphism defined by

$$a(x) = (p + 1)x.$$

By (2.3), a has order p^{e-1}. Consider the permutation $ta^j \in \mathrm{Sym}(\mathbb{Z}_{p^e})$ for some $j \in \{0, 1, \dots, p^{e-1} - 1\}$. Recall that t is the translation $t(x) = x + 1$. By Lemma 2.4, ta^j has order p^e, and thus it is a full cycle. Therefore, there exists a unique permutation $b_j \in \mathrm{Sym}(\mathbb{Z}_{p^e})$ such that $b_j(0) = 0$ and the conjugate

$$t^{b_j} := b_j t b_j^{-1} = ta^j. \tag{3.1}$$

In fact, for $x \in \mathbb{Z}_{p^e}$ with $x \neq 0$, the permutation b_j can be expressed as

$$b_j(x) = 1 + (p+1)^j + \cdots + (p+1)^{(x-1)j}. \tag{3.2}$$

Define the permutations

$$s_{i,j} = b_j^{-1} a^i b_j, \quad i, j \in \{0, 1, \dots, p^{e-1} - 1\}. \tag{3.3}$$

Proposition 3.1. *Every permutation $s_{i,j}$ defined in* (3.3) *is a skew-morphism of $\mathbb{Z}_{p^e}$.*

Proof. By definition, the order $|s_{i,j}| = |a^i|$. Assume at first that $p \nmid i$, or equivalently, $s_{i,j}$ has order p^{e-1}. It is clear that $s_{i,j}(0) = 0$. Thus by (2.2), it is enough to show that $|\langle t, s_{i,j}\rangle| = p^{2e-1}$. We have

$$|\langle t, s_{i,j}\rangle| = |\langle t, s_{i,j}\rangle^{b_j}| = |\langle t^{b_j}, s_{i,j}^{b_j}\rangle| = |\langle ta^j, a^i\rangle| = p^{2e-1},$$

therefore $s_{i,j}$ is a skew-morphism. The last equality comes from the following observation: assuming $\langle ta^j\rangle \cap \langle a^i\rangle \neq 1$ we get that some power of a centralises t, a contradiction with the definition of a and t.

Now, suppose that $i = p^k i'$, $p \nmid i'$. As $s_{i',j}$ is a skew-morphism of $\mathbb{Z}_{p^e}$, and

$$s_{i,j} = s_{i',j}^{p^k},$$

it follows from Lemma 2.2 (i) that $s_{i,j}$ is a skew-morphism too. □

Remark 3.2. The reader might observe that in case a skew-morphism of the cyclic group of order p^e has order p^{e-1}, then the skew product G has the following canonical presentation:

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

In the above notation $t = x$ and conjugation by y is the automorphism a. Besides the canonical factorisation $G = \langle x\rangle\langle y\rangle$, we have a factorisation $G = \langle xy^j\rangle\langle y\rangle$, for any j. By Lemma 2.4, $\langle xy^j\rangle$ has order p^e, so y gives another skew-morphism of the cyclic group of order p^e (generated by different element of order p^e).

Given two factorisations $G = BY = CY$, where $Y = \langle y \rangle$, $|B| = |C| = p^e$ for any $c \in C$ there is a unique $b \in B$ such that $c = by^i$. Thus there is a bijection $\sigma : C \to B$ that provides a "change of coordinates". Let ϕ and ψ be the two skew-morphisms determined by y with respect to the two factorisations CY and BY. Then $ycY = \phi(c)Y$ and $ycY = y\sigma(c)Y = \psi(\sigma(c))Y$. The last term is by the factorisation BY. To convert back to CY, we use σ^{-1}, thus $\phi = \sigma^{-1}\psi\sigma$. The skew-morphisms $s_{i,j}$ all live in the split metacyclic p-group G and are obtained by left multiplication on $\langle x^j y \rangle$, to be precise, they are conjugate to y^i by the permutation b_j.

Notice that the skew-morphism $s_{i,j}$ is not uniquely determined by the parameters i and j. For instance, $s_{0,j}$ is the identity mapping for every j. The rest of the section is devoted to the proof of following theorem.

Theorem 3.3. *Let $e \geq 2$, and $i, i', j, j' \in \{0, 1, \ldots, p^{e-1} - 1\}$. Then*

$$s_{i,j} = s_{i',j'} \iff i = i' \text{ and } j \equiv j' \pmod{p^{e-2}/\gcd(i, p^{e-2})}.$$

The theorem will be derived in a sequence of lemmas.

Lemma 3.4. *Let $e \geq 2$, and $j, j' \in \{0, 1, \ldots, p^{e-1}-1\}$ such that $j \equiv j' \pmod{p^u}$ for some $u \in \{0, 1, \ldots, e-1\}$. Then for all $x, x' \in \mathbb{Z}_{p^e}$ with $x \equiv x' \pmod{p^{e-1-u}}$,*

$$b_{j'}(x) - b_j(x') = b_{j'}(x) - b_j(x).$$

Proof. We divide the proof into four steps.

Claim 1. *We have $b_j(p^{e-1-u}) = b_{j'}(p^{e-1-u})$.*

We start by the observation that if $x, y, z \in \mathbb{Z}_{p^e}$, then

$$(t^x a^y)^z = t^{x b_y(z)} a^{yz}. \tag{3.4}$$

It follows that

$$(ta^j)^{p^{e-1-u}} = t^{b_j(p^{e-1-u})} a^{jp^{e-1-u}},$$
$$(ta^{j'})^{p^{e-1-u}} = t^{b_{j'}(p^{e-1-u})} a^{j'p^{e-1-u}}.$$

Since $a^{jp^{e-1-u}} = a^{j'p^{e-1-u}}$, Claim 1 is equivalent to

$$(ta^j)^{p^{e-1-u}} = (ta^{j'})^{p^{e-1-u}}.$$

Recall that an arbitrary p-group G is *regular* if for all $x, y \in G$,

$$(xy)^p = x^p y^p c_1 \cdots c_r,$$

where all c_i belong to the commutator $\langle x, y\rangle'$. In the case when $p > 2$, a sufficient condition for G to be regular is that its commutator subgroup G' is cyclic (see [7, III.10.2)]). In particular, it follows that $\langle t, a\rangle$ is a regular p-group. Thus by [7, III.10.6],

$$(ta^j)^{p^{e-1-u}} = (ta^{j'})^{p^{e-1-u}}$$

is equivalent to

$$((ta^j)^{-1}ta^{j'})^{p^{e-1-u}} = 1.$$

Putting $j' - j = j_0 p^u$, for some j_0, we get

$$((ta^j)^{-1}ta^{j'})^{p^{e-1-u}} = (a^{j_0 p^u})^{p^{e-1-u}} = 1.$$

Claim 2. *We have* $b_j(xp^{e-1-u}) = b_{j'}(xp^{e-1-u})$ *for all* $x \in \{0, 1, \dots, p^{u+1}-1\}$.

Let $x \in \{0, 1, \dots, p^{u+1} - 1\}$. Recall that $t^{b_j} = ta^j$. By this and (3.4),

$$(t^{xp^{e-1-u}})^{b_j} = (ta^j)^{xp^{e-1-u}} = t^{b_j(xp^{e-1-u})}a^{xp^{e-1-u}j},$$

$$(t^{xp^{e-1-u}})^{b_{j'}} = (ta^{j'})^{xp^{e-1-u}} = t^{b_{j'}(xp^{e-1-u})}a^{xp^{e-1-u}j'}.$$

Thus Claim 2 is equivalent to $(t^{xp^{e-1-u}})^{b_j} = (t^{xp^{e-1-u}})^{b_{j'}}$. Since this holds for $x = 1$ by Claim 1, it also holds for all $x > 1$.

Claim 3. *We have* $p^{e-1-u} \mid b_j(xp^{e-1-u})$ *for all* $x \in \{0, 1, \dots, p^{u+1} - 1\}$.

The order of ta^j is p^e. This implies that $(ta_j)^{xp^{e-u-1}} = t^{b_j(xp^{e-1})}a^{jxp^{e-u-1}}$ has order at most p^{u+1}. As $a^{jxp^{e-u-1}}$ has order at most p^u, it follows from Lemma 2.4 that $t^{b_j(xp^{e-u-1})}$ has order at most p^{u+1}. This yields Claim 3.

Claim 4. *We have* $b_{j'}(x') - b_j(x') = b_{j'}(x) - b_j(x)$ *for all* $x, x' \in \mathbb{Z}_{p^n}$ *with* $x \equiv x' \pmod{p^{e-1-u}}$.

Put $x' = x + x_0 p^{e-1-u}$ and $j' = j + j_0 p^u$. By (3.2) and Claim 2,

$$\begin{aligned} b_{j'}(x') - b_{j'}(x) &= b_{j'}(x) + (p+1)^{j'x} b_{j'}(x_0 p^{e-1-u}) - b_{j'}(x) \\ &= (p+1)^{jx}(p+1)^{j_0 p^u x} b_{j'}(x_0 p^{e-1-u}) \\ &= (p+1)^{jx}(p+1)^{j_0 p^u x} b_j(x_0 p^{e-1-u}). \end{aligned}$$

By (2.3), $(p+1)^{j_0 p^u x} \equiv 1 \pmod{p^{u+1}}$. Thus we find, using also Claim 3, that

$$(p+1)^{j_0 p^u x} b_j(x_0 p^{e-1-u}) = b_j(x_0 p^{e-1-u}).$$

Therefore,

$$b_{j'}(x') - b_{j'}(x) = (p+1)^{jx} b_j(x_0 p^{e-1-u}) = b_j(x') - b_j(x).$$

This completes the proof. □

Lemma 3.5. *Let $e \geq 2$ and $i \in \{0, \ldots, p^{e-1} - 1\}$. Then for all $x \in \mathbb{Z}_{p^e}$,*

$$s_{i,j}(x) \equiv x \pmod{p \cdot \gcd(i, p^{e-1})}.$$

Proof. By (3.3), the order of $s_{i,j}$ is $p^{e-1}/\gcd(i, p^{e-1})$. By Lemma 2.2 (iii), there exists an automorphism $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^e})$ of the same order such that the $\langle\alpha\rangle$-orbits coincide with the $\langle s_{i,j}\rangle$-orbits. It follows that $\alpha \in \langle a^{\gcd(i,p^{e-1})}\rangle$. Let $x \in \mathbb{Z}_{p^e}$. Then there exists some $l \in \{0, \ldots, p^{e-1} - 1\}$ with $\gcd(i, p^{e-1}) \mid l$ such that

$$s_{i,j}(x) = a^l(x),$$

and hence

$$s_{i,j}(x) \equiv (p + 1)^l x \pmod{p^e}. \tag{3.5}$$

By (2.4), $(p+1)^l \equiv 1 \pmod{p \cdot \gcd(l, p^{e-1})}$. Since $\gcd(i, p^{e-1}) \mid \gcd(l, p^{e-1})$, it follows that $(p + 1)^l \equiv 1 \pmod{p \cdot \gcd(i, p^{e-1})}$. Substituting this in (3.5), the lemma follows. □

Lemma 3.6. *Let $e \geq 2$, and $i, j, j' \in \{0, \ldots, p^{e-1} - 1\}$. Then*

$$s_{i,j} = s_{i,j'} \iff j \equiv j' \pmod{p^{e-2}/\gcd(i, p^{e-2})}. \tag{3.6}$$

Proof. The statement holds if $i = 0$, and hence below we assume that $i > 0$.

($\Rightarrow$) Let $s_{i,j} = s_{i,j'}$, and π be the power function of $s_{i,j}$. By (2.1),

$$s_{i,j}t = t^{s_{i,j}(1)}s_{i,j}^{\pi(1)}$$

holds in $\langle t, s_{i,j}\rangle$. This implies in $\langle t, s_{i,j}\rangle^{b_j} = \langle ta^j, a^i\rangle$,

$$t^{(p+1)^i}a^{i+j} = a^i(ta^j) = (ta^j)^{s_{i,j}(1)}(a^i)^{\pi(1)} = t^{b_j(s_{i,j}(1))}a^{s_{i,j}(1)j+\pi(1)i}.$$

As $b_j(s_{i,j}(1)) = (b_j s_{i,j})(1) = (a^i b_j)(1) = (p + 1)^i$, we get

$$a^{i+j} = a^{s_{i,j}(1)j+\pi(1)i}. \tag{3.7}$$

Since $s_{i,j} = s_{i,j'}$, the same argument yields $a^{i+j'} = a^{s_{i,j'}(1)j'+\pi(1)i}$. Thus

$$a^{(j-j')(s_{i,j}(1)-1)} = 1,$$

and hence

$$j \equiv j' \pmod{p^{e-1}/\gcd(s_{i,j}(1) - 1, p^{e-1})}. \tag{3.8}$$

By (3.3), the order of $s_{i,j}$ is $p^{e-1}/\gcd(i, p^{e-1})$. This and Lemma 2.3 yield $\gcd(s_{i,j}(1)-1, p^e) = p\cdot\gcd(i, p^{e-1})$. Since $i \neq 0$, $\gcd(i, p^{e-1}) = \gcd(i, p^{e-2})$ and $\gcd(s_{i,j}(1) - 1, p^e) = \gcd(s_{i,j}(1) - 1, p^{e-1})$, and thus

$$\gcd(s_{i,j}(1) - 1, p^{e-1}) = p \cdot \gcd(i, p^{e-2}).$$

This and (3.8) yield the right side of (3.6).

($\Leftarrow$) Put $p^u = p^{e-2}/\gcd(i, p^{e-2})$. Then order of a^i is $p^{e-1}/\gcd(i, p^{e-2}) = p^{u+1}$, and hence by (2.3),

$$(p+1)^i = zp^{e-u-1} + 1 \quad \text{for some } z \in \{1, \ldots, p^{u+1} - 1\},\ p \nmid z. \tag{3.9}$$

For two arbitrary mappings $f, g : \mathbb{Z}_{p^e} \to \mathbb{Z}_{p^e}$, their *sum* $f+g$, *difference* $f-g$, and *product* fg are the mappings from $\mathbb{Z}_{p^e}$ to $\mathbb{Z}_{p^e}$ defined in the usual way, that is, for $x \in \mathbb{Z}_{p^e}$,

$$(f+g)(x) = f(x)+g(x), \quad (f-g)(x) = f(x)-g(x), \quad (fg)(x) = f(g(x)).$$

Let $j' = j + j_0 p^u$, for some j_0. For every $x \in \mathbb{Z}_{p^e}$ with $x \neq 0$,

$$((p+1)^{j_0 p^u x} - 1) \mid ((p+1)^{j'x} - (p+1)^{jx}).$$

Therefore, $p^{u+1} \mid ((p+1)^{j'x} - (p+1)^{jx})$. This and (3.2) imply

$$(b_{j'} - b_j)(x) \equiv 0 \pmod{p^{u+1}} \quad \text{for all } x \in \mathbb{Z}_{p^e}.$$

This and (3.9) yield $a^i(b_{j'} - b_j) = b_{j'} - b_j$. Also, by Lemma 3.5,

$$s_{i,j}(x) \equiv x \pmod{p^{e-u-1}} \quad \text{for all } x \in \mathbb{Z}_{p^e}.$$

Therefore, by Lemma 3.4,

$$(b_{j'} - b_j)(s_{i,j}(x)) = (b_{j'} - b_j)(x) \text{ for all } x \in \mathbb{Z}_{p^e}.$$

Consequently, $(b_{j'} - b_j)s_{i,j} = b_{j'} - b_j = a^i(b_{j'} - b_j)$. Thus

$$a^i b_{j'} - a^i b_j = b_{j'} s_{i,j} - b_j s_{i,j} = b_{j'} s_{i,j} - a^i b_j;$$

and we get $s_{i,j} = b_{j'}^{-1} a^i b_{j'} = s_{i,j'}$. □

Theorem 3.3 follows from Lemma 3.6 and the following lemma.

Lemma 3.7. *If $s_{i,j} = s_{i',j'}$, then $i = i'$.*

Proof. Let $s_{i,j} = s_{i',j'}$, and let π be the power function of $s_{i,j}$. We prove the lemma by induction on the order of $s_{i,j}$. The statement holds obviously if $s_{i,j}$ is the identity permutation, that is, if $i = 0$. Thus for the rest of the proof assume that $i \neq 0$. By (3.7),

$$a^{(s_{i,j}(1)-1)j} = a^{i(1-\pi(1))} \quad \text{and} \quad a^{(s_{i,j}(1)-1)j'} = a^{i'(1-\pi(1))}.$$

Then

$$s_{ip,j} = s_{i,j}^p = s_{i',j'}^p = s_{i'p,j'}.$$

Thus by the induction hypothesis, $ip \equiv i'p \pmod{p^{e-1}}$. As $p \mid (\pi(1)-1)$, see Lemma 2.2 (ii), we conclude $i(1-\pi(1)) = i'(1-\pi'(1)) \pmod{p^{e-1}}$. Thus the above equalities reduce to $j \equiv j' \pmod{p^{e-1}/\gcd(p^{e-1}, s_{i,j}(1)-1)}$. Since it has already been shown that $\gcd(s_{i,j}(1)-1, p^{e-1}) = p \cdot \gcd(p^{e-2}, i)$, it follows that $j \equiv j' \pmod{p^{e-2}/\gcd(p^{e-2}, i)}$. Thus by Lemma 3.6, $s_{i',j'} = s_{i',j}$, and we get $s_{i,j} = s_{i',j'} = s_{i',j}$. It is obvious that this implies that $i = i'$. □

4 The skew-morphisms $s_{i,j,k,l}$

For the rest of the paper we set b to be an automorphism of $\mathbb{Z}_{p^e}$ of order $p-1$. Define the permutations

$$s_{i,j,k,l} = b_j^{-1} a^i b^k b_l b_j, \tag{4.1}$$

where the integers i, j, k, l satisfy the following conditions:

(C0) $i, l \in \{0, \dots, p^{e-1}-1\}$, $k \in \{0, \dots, p-2\}$, $j \in \{0, \dots, p^{e-2-c}-1\}$, where $p^c = \gcd(i, p^{e-2})$.

(C1) If $i = 0$ or $k = 0$, then $l = 0$.

(C2) If $i \neq 0$ and $k \neq 0$, then $p^c \mid j$ and $p^{\max\{c, e-2-c\}} \mid l$.

A 4-tuple (i, j, k, l) of integers satisfying conditions (C0), (C1) and (C2) will be called *admissible*.

Note that the permutations $s_{i,j,k,l}$ include all skew-morphisms in the form $s_{i,j}$. Namely, given any skew-morphism $s_{i,j}$, in view of Theorem 3.3 we may assume that $j < p^{e-2-c}$ for $c = \gcd(i, p^{e-2-})$, and thus by (3.3) and (4.1), $s_{i,j} = s_{i,j,0,0}$.

Before we prove that all permutations $s_{i,j,k,l}$ are skew-morphisms, we give two lemmas.

Lemma 4.1. *Let G be a split metacyclic p-group given by the presentation*

$$G = \langle x, y \mid x^{p^m} = y^{p^n} = 1,\ x^y = x^{1+p^{m-n}} \rangle,$$

where $m > n \geq 1$. Then the automorphisms in $\mathrm{Aut}(G)$ *are the mappings $\theta_{u,v,w}$, where $u, v \in \{0, \dots, p^m-1\}$ with $p \nmid u$, $p^{m-n} \mid v$, and $w \in \{0, \dots, p^n-1\}$ with $p^{2n-m} \mid w$ whenever $2n > m$, defined as*

$$\theta_{u,v,w}(x^i y^j) = x^{ui+vj} y^{wi+j} \quad \text{for all } x^i y^j \in G.$$

In particular, $|\mathrm{Aut}(G)| = (p-1)p^{m-1+n+\min\{n,m-n\}}$.

Proof. This is a corollary of the more general result [2, Theorem 3.1]. □

Lemma 4.2. *With the notation of Lemma* 4.1*, let* $u \in \{0, \ldots, p^m - 1\}$*,* $p \nmid u$ *such that* $u \neq 1$*, and as a unit of the ring* $\mathbb{Z}_{p^m}$*,* u *has order* d *with* $p \nmid d$*. Then the automorphism* $\theta_{u,0,w}$ *has order* d*.*

Proof. A straightforward computation gives

$$(\theta_{u,0,w})^k(x^i y^j) = x^{u^k i} y^{wi(1+u+\cdots+u^{k-1})+j}.$$

Therefore, the order $|\theta_{u,0,w}| \geq d$. Also, $p^m \mid (u^d - 1)$. On the other hand, since the order of the unit $u \neq 1$ is not divisible by p, it follows that $p \nmid (u-1)$ as well. We conclude from these that $p^m \mid (1 + u + \cdots + u^{d-1})$. Using also that $n < m$, we find $(\theta_{u,0,w})^d(x^i y^j) = x^i y^j$, and thus $|\theta_{u,0,w}| = d$. □

Theorem 4.3. *Every permutation* $s_{i,j,k,l}$ *defined in* (4.1) *is a skew-morphism of* $\mathbb{Z}_{p^e}$*.*

Proof. Let $s_{i,j,k,l}$ be a permutation defined in (4.1). If $k = 0$, then $s_{i,j,k,l} = s_{i,j}$ and the statement holds. For the rest of the proof it is assumed that $k \neq 0$.

Let $i = 0$. Then $j = 0$ by (C0) and $l = 0$ by (C1). We get $s_{i,j,k,l} = b^k$, which is an automorphism in $\mathrm{Skew}(\mathbb{Z}_{p^e})$. Now, suppose that $i \neq 0$. Since $k \neq 0$, we have $t^{b^k} = t^u$ for some $u \in \{2, \ldots, p^e - 1\}$, $p \nmid u$, and as unit of $\mathbb{Z}_{p^e}$, u has order d with $p \nmid d$. Let $p^c = \gcd(i, p^{e-2})$. Let $G = \langle ta^j, a^i, b^k b_l \rangle$ and $P = \langle ta^j, a^i \rangle$. It follows from (C2) that $P = \langle t, a^i \rangle$ and there exists $a_1 \in \langle a^i \rangle$ such that P admits the presentation

$$P = \big\langle t, a_1 \mid t^{p^e} = (a_1)^{p^{e-1-c}} = 1,\ t^{a_1} = t^{1+p^{c+1}} \big\rangle.$$

Clearly, $a_1 = a^{i'}$ for a some i' satisfying $\gcd(i', p^{e-2}) = p^c$. This and (C2) yield $p^{e-2}/\gcd(i', p^{e-2}) \mid l$, and so $s_{i',l} = s_{i',0} = a^{i'}$ follows from Theorem 3.3. In other words, b_l commutes with $a_1 = a^{i'}$. Now, we can write

$$t^{b^k b_l} = t^u a^l \quad \text{and} \quad (a_1)^{b^k b_l} = a_1. \tag{4.2}$$

The group $\langle a_1 \rangle$ is equal to $\langle a^{p^c} \rangle$. On the other hand, by (C2), $p^c \mid l$, and so $a^l = a_1^w$ for some $w \in \{0, \ldots, p^{e-1-c} - 1\}$. This and (4.2) yield that P is normal in G. We claim that $b^k b_l$ acts on P by conjugation as the automorphism $\theta_{u,0,w}$ described in Lemma 4.1. In fact, we have to show that p^{e-2-2c} divides w whenever $2(e-1-c) > e$. In order to see that this indeed holds, observe that $a^l = a_1^w = a^{i'w}$, $\gcd(i', p^{e-2}) = p^c$, and finally $p^{e-2-c} \mid l$, by (C2).

Since $b^k b_l$ fixes 0 and P is transitive on $\mathbb{Z}_{p^e}$, $Z_{\langle b^k b_l \rangle}(P) = 1$. Equivalently, $b^k b_l$ acts faithfully on P, in particular, $|b^k b_l| = |\theta_{u,0,l}|$. Now, by Lemma 4.2, $|b^k b_l| = d$. Thus $|G| = |P| \cdot d$. This implies that the stabiliser G_0 of 0 in G has order $|G_0| = p^{e-1-c} d$. Also, as a^i commutes with $b^k b_l$, we find

$$|a^i b^k b_l| = p^{e-1-c} d = |G_0|,$$

implying that $G_0 = \langle a^i b^k b_l \rangle$, and G factorises as $G = \langle ta^j \rangle \langle a^i b^k b_l \rangle$. Therefore, the conjugate group $G^{(b_j)^{-1}}$ factorises as $G^{(b_j)^{-1}} = \langle t \rangle \langle s_{i,j,k,l} \rangle$, and hence $s_{i,j,k,l}$ is a skew-morphism by (2.2). □

Proposition 4.4. *Every permutation $s_{i,j,k,l}$ in* (4.1) *is uniquely determined by the admissible* 4*-tuple* (i, j, k, l)*. In particular, there is a bijection between the set of admissible* 4*-tuples of integers and the set of skew-morphisms $s_{i,j,k,l}$.*

Proof. Suppose that $s_{i,j,k,l}$ and $s_{i',j',k',l'}$ are two skew-morphisms defined in (4.1) for which $s_{i,j,k,l} = s_{i',j',k',l'}$. We are going to prove that

$$(i, j, k, l) = (i', j', k', l').$$

It follows that these skew-morphisms have order

$$\frac{p^{e-1}(p-1)}{\gcd(i, p^{e-1}) \gcd(k, p-1)} = \frac{p^{e-1}(p-1)}{\gcd(i', p^{e-1}) \gcd(k', p-1)}.$$

In particular, $\gcd(i, p^{e-1}) = \gcd(i', p^{e-1})$.

Let $i = 0$ or $i' = 0$. Then we get $i = i' = 0$, hence $j = j' = 0$, and $l = l' = 0$, by condition (C1). Thus $b^k = s_{0,0,k,0} = s_{0,0,k',0} = b^{k'}$, implying that $k = k'$, and so

$$(i, j, k, l) = (i', j', k', l').$$

Now, suppose that none of i and i' is equal to 0. Let $\gcd(i, p^{e-2}) = p^c$ (so $\gcd(i', p^{e-2}) = p^c$ as well). By (3.3) and (4.1),

$$s_{i,j} b_j^{-1} b^k b_l b_j = s_{i',j'} b_{j'}^{-1} b^{k'} b_{l'} b_{j'}.$$

Both $s_{i,j}$ and $s_{i',j'}$ have order $p^{e-1-c} \neq 1$, and both $b_j^{-1} b^k b_l b_j$ and $b_{j'}^{-1} b^{k'} b_{l'} b_{j'}$ have the same order not divisible by p. We have proved above that

$$[s_{i,j}, b_j^{-1} b^k b_l b_j] = [s_{i',j'}, b_{j'}^{-1} b^{k'} b_{l'} b_{j'}] = 1$$

also hold, and we deduce from these that $s_{i,j} = s_{i',j'}$ and

$$b_j^{-1} b^k b_l b_j = b_{j'}^{-1} b^{k'} b_{l'} b_{j'}.$$

Since both j and j' are in $\{0, \dots, p^{e-2-c} - 1\}$, it follows by Theorem 3.3 that $i = i'$ and $j = j'$. This implies that $b^k b_l = b^{k'} b_{l'}$. From this by (3.2), we obtain $b^k(1) = (b^k b_l)(1) = (b^{k'} b_{l'})(1) = b^{k'}(1)$. This in turn implies that $k = k'$ and $b_l = b_{l'}$. Then, by (3.2) again, $(p+1)^l = b_l(2) - 1 = b_{l'}(2) - 1 = (p+1)^{l'}$, from which $l = l'$. This completes the proof of the proposition. □

5 Skew-morphisms of $\mathbb{Z}_{p^e}$

In this section we prove that skew-morphisms $s_{i,j,k,l}$ comprise all skew-morphisms of $\mathbb{Z}_{p^e}$. Our argument is divided in two cases depending on whether the order of the skew-morphism is a p-power or not.

5.1 Skew-morphisms of p-power order

Let G be a skew product group of $\mathbb{Z}_{p^e}$ induced by a skew-morphism s of some p-power order. Then G factorises as $\langle t\rangle\langle s\rangle$, hence by a result of Huppert [6] (cf. also [7, III.11.5]) G is metacyclic. Note that this implies that the commutator subgroup G' is cyclic, and therefore, $G' \cap \langle s\rangle = 1$. Indeed, as G' is characteristic in G, any of its subgroups is normal in G, on the other hand, no non-trivial normal subgroup of G is contained in $\langle s\rangle$. Also, since $\langle t\rangle < G$ acts regularly on $\mathbb{Z}_{p^e}$, it follows that the center $Z(G) \le \langle t\rangle$, in particular, $Z(G)$ is a cyclic group. These observations will be used below.

Lemma 5.1. *Let $G = \mathbb{Z}_{p^e}\langle s\rangle$ be a skew product group of $\mathbb{Z}_{p^e}$ of order p^{e+i}, where $1 \le i \le e-1$. If G is a split metacyclic group, then its commutator subgroup G' has order p^i, and the exponent* $\exp(G/G') = p^{\max\{i,e-i\}}$.

Proof. Since G is a split metacyclic and non-abelian group, it has a presentation in the form

$$G = \big\langle x, y \mid x^{p^k} = 1,\ y^{p^l} = 1,\ x^y = x^{1+p^{k-m}}\big\rangle,$$

where $1 \le m \le \min\{l, k-1\}$. The order $|G| = p^{k+l}$, and hence $k + l = e + i$. The elements in G of order p generate the subgroup $\langle x^{p^{k-1}}, y^{p^{l-1}}\rangle \cong \mathbb{Z}_p^2$. On the other hand, $G = \langle t\rangle\langle s\rangle$, where $s \in \mathrm{Skew}(\mathbb{Z}_{p^e})$. We have observed above that the center $Z(G)$ is a cyclic group. Therefore, $Z(G)\cap\langle y\rangle = 1$, from which $l = m < k$. We conclude that $\exp(G) = p^k$, and thus $k = e$, $i = l = m$, $G' = \langle x^{p^{e-i}}\rangle$, and finally, $\exp(G/G') = p^{\max\{i,e-i\}}$. □

Let us consider the skew product groups of $\mathbb{Z}_{p^e}$ induced by the skew-morphisms $s_{i,j}$. Theorem 3.3 implies that these groups can be listed as the groups $G(i, j)$, where $G(0, 0) := \langle t\rangle$; and for $e \ge 2$,

$$G(i, j) := \langle t, s_{p^{e-1-i},j}\rangle, \quad i \in \{1, \dots, e-1\},\ j \in \{0, \dots, p^{i-1}-1\}. \tag{5.1}$$

Notice that $|G(i, j)| = p^{e+i}$.

Lemma 5.2. *Let $e \ge 2$ and let $G(i, j)$ be a group defined in* (5.1). *Then $G(i, j)$ is a split metacyclic group if and only if $p^{e-1-i} \mid j$.*

Proof. We have $G(i,j)^{b_j} = \langle ta^j, a^{p^{e-1-i}}\rangle$, see the proof of Proposition 3.1. Let $G = \langle ta^j, a^{p^{e-1-i}}\rangle$. This shows that, if $p^{e-1-i} \mid j$, then G is a split metacyclic group. It remains to prove that, if G is a split metacyclic group, then $p^{e-1-i} \mid j$. In fact, we prove that $p^{e-1-i} \nmid j$ forces that G is a non-split metacyclic group.

Let $p^m = \gcd(j, p^{e-1})$, and assume that $e-1-i > m$. By (5.1),

$$0 \le m \le i-2. \tag{5.2}$$

The commutator $[x,y]$ of two elements $x, y \in G$ is given by

$$[x,y] := xyx^{-1}y^{-1}.$$

Then $[a^{p^{e-1-i}}, ta^j] = t^{(p+1)^{p^{e-1-i}}-1}$. Let $N = \langle t^{(p+1)^{p^{e-1-i}}-1}\rangle$. Clearly, we have $N \le G'$. Notice that N is normal in G, and G/N is abelian. This implies that $N \ge G'$, and therefore, $G' = N$. By (2.4), $|G'| = p^i$. On the other hand, $|\langle t\rangle \cap \langle ta^j\rangle| = p^{m+1}$. Thus $|G' \cap \langle ta^j\rangle| = p^{\min\{i,m+1\}}$, from which we obtain $|G' \cap \langle ta^j\rangle| = p^{m+1}$ by (5.2). Also, $G' \le \langle t\rangle$, hence $G' \cap \langle a\rangle = 1$ (this follows also from the observation preceding Lemma 5.1), and so

$$\exp(G/G') = p^{\max\{e-1-m,i\}} = p^{e-m-1}$$

because we assumed $e-1-i > m$. Finally, as $e-m-1$ is larger than both i and $e-i$, $\exp(G/G') > p^{\max\{i,e-i\}}$. Now, Lemma 5.1 gives that G is a non-split metacyclic group. □

Lemma 5.3. *Let $e \ge 2$ and $1 \le i \le e-1$. The number of non-isomorphic non-split skew product groups of $\mathbb{Z}_{p^e}$ of order p^{e+i} is at most* $\min\{i-1, e-1-i\}$.

Proof. By [11, Theorem 3.2], every metacyclic non-split p-group G has up to isomorphism a presentation in the form:

$$G = \left\langle x, y \mid x^{p^m} = 1,\ y^{p^n} = x^{p^{m-u}},\ x^y = x^{1+p^{m-c}}\right\rangle, \tag{5.3}$$

where

$$\max\{1, m-n+1\} \le u < \min\{c, m-c+1\}. \tag{5.4}$$

Now, suppose that G is a non-split skew product group of $\mathbb{Z}_{p^e}$ of order p^{e+i} induced by some $s \in \mathrm{Skew}(\mathbb{Z}_{p^e})$. Consider the presentation of G described in (5.3). Since G is non-split, $m < e$. The exponent $\exp(G) = p^e$. On the other hand, (5.3) shows that $\exp(G) = p^{\max\{m,n+u\}}$, and it follows that $e = n+u$. Thus the order $|y| = p^{n+u} = p^e$, and we obtain $|Z(G) \cap \langle y\rangle| = p^{e-c}$.

We compute next $|Z(G) \cap \langle y\rangle|$ in another way. Since y has order p^e, it acts on $\mathbb{Z}_{p^e}$ as a full cycle. In particular, $G = \langle y, s\rangle$. Suppose that s centralises $y_1 \in \langle y\rangle$. Then $s(y_1(0)) = y_1(s(0)) = y_1(0)$, and so $y_1(0)$ is fixed by s. Conversely, suppose that $s(t) = t$ for some $t \in \mathbb{Z}_{p^e}$. Then $t = y_2(0)$ for a unique $y_2 \in \langle y\rangle$, and we find $[s, y_2^{-1}]$ fixes 0. As G' is normal and cyclic, it is semi-regular on $\mathbb{Z}_{p^e}$. We conclude that $[s, y_2^{-1}] = 1$, and y_2 is centralised by s. By these we have shown

$$|Z(G) \cap \langle y \rangle| = |\{t \in \mathbb{Z}_{p^e} : s(t) = t\}|.$$

Lemma 2.2 (iii) implies

$$|\{t \in \mathbb{Z}_{p^e} : s(t) = t\}| = p^{e-i},$$

and so $|Z(G) \cap \langle y \rangle| = p^{e-i}$ also holds; and therefore, $c = i$. From (5.3), we have $|G| = p^{m+n}$. As $|G| = p^{e+i}$ and $|y| = p^{n+u} = p^e$, we get $n = e - u$ and $m = i + u$. In view of (5.4), the number of possible groups in (5.3) is bounded above by the number of solutions of the inequalities

$$\max\{1, i - e + 2u + 1\} \le u < \min\{i, u + 1\}$$

with variable u. This number is $\min\{i - 1, e - 1 - i\}$, and the lemma follows. □

We are ready to prove the main result of the subsection.

Theorem 5.4. *The skew-morphisms of $\mathbb{Z}_{p^e}$ of p-power order are exactly the skew-morphisms $s_{i,j}$ defined in* (3.3).

Proof. Let s be a skew-morphism of order p^i, and let $G = \langle t, s \rangle$. We show below that G is isomorphic to one of the groups $G(i, j)$ defined in (5.1).

Suppose that G is a split metacyclic group. We have proved in Lemma 5.1 that $\exp(G) = p^e$, and this implies that $G \cong G(i, 0)$.

Suppose that G is non-split. Then by Lemma 5.3, $2 \le i \le e-2-i$. Furthermore, by Lemma 5.2, each of the groups $G(i, p^j)$, $j \in \{0, \dots, \min\{i - 2, e - 2 - i\}\}$ is a non-split metacyclic group. Also, we have computed in the proof of Lemma 5.2 that $\exp(G(i, p^j)/G(i, p^j)') = p^{e-1-j}$, and therefore, the above groups are pairwise non-isomorphic. This and Lemma 5.3 yield that G is isomorphic to one of the above groups $G(i, p^j)$.

Now, we may assume without loss of generality that G is a subgroup of $\langle t, a \rangle$. Then the skew-morphism s and its power function π can be described as follows: there exists a factorisation $G = \langle x \rangle \langle y \rangle$ such that $|x| = p^e$, $|y| = p^i$ (thus $\langle x \rangle \cap \langle y \rangle = 1$), $Z(G) \cap \langle y \rangle = 1$, and for every $k \in \mathbb{Z}_{p^e}$,

$$yx^k = x^{s(k)} y^{\pi(k)}. \tag{5.5}$$

Now, $x = t^u a^v$ and $y = t^w a^z$ for some $u, v, w, z \in \{0, \dots, p^{e-1} - 1\}$. Since $|x| = p^e$, it follows that $p \nmid u$, see Lemma 2.4. Suppose that y is fixed-point free. This gives $((p + 1)^z - 1)X = -w$ has no solution for $X \in \mathbb{Z}_{p^e}$, or equivalently, $\gcd(w, p^e) < \gcd((p + 1)^z - 1, p^e)$. This in turn implies that $|t^w| > |a^z|$, and $t^{p^{e-1}} \in \langle t^w a^z \rangle = \langle y \rangle$. As $t^{p^{e-1}} \in Z(\langle t, a \rangle)$, $Z(G) \cap \langle y \rangle \neq 1$, a contradiction. Therefore, y has a fixed point. It follows from this that y can be mapped into $\langle a \rangle$ under conjugation by some element $x_1 \in \langle x \rangle$. Thus $y^{x_1} = a^m$ for some $m \in \{0, \dots, p^{e-1} - 1\}$, and after conjugation by x_1, equation (5.5) becomes

$$a^m x^k = x^{s(k)} (a^m)^{\pi(k)},$$

and hence

$$a^m (t^u a^v)^k = (t^u a^v)^{s(k)} (a^m)^{\pi(k)}.$$

This and (3.4) yield $t^{u a^m (b_v(k)))} = t^{u b_v (s(k))}$. Since $p \nmid u$, this implies

$$(a^m b_v)(k) = (b_v s)(k)$$

for all $k \in \mathbb{Z}_{p^e}$, and so $a^m b_v = b_v s$, from which $s = b_v^{-1} a^m b_v = s_{m,v}$. This completes the proof of the theorem. □

5.2 Skew-morphisms whose order is not a p-power

We complete the classification of all skew-morphisms of $\mathbb{Z}_{p^e}$ by proving the following theorem.

Theorem 5.5. *The skew-morphisms of $\mathbb{Z}_{p^e}$ whose order is not a p-power are exactly the skew-morphisms $s_{i,j,k,l}$, $k \neq 0$, defined in* (4.1).

Proof. Let s be a skew-morphism of order $p^c d$, $p \nmid d$ and $d > 1$. Notice that $c \in \{0, \dots, e-1\}$ and $d \mid (p-1)$ because of Lemma 2.1.

Let $c = 0$. Then by Lemma 2.1, s is in $\mathrm{Aut}(\mathbb{Z}_{p^e})$ and it has order d. Thus $s = b^k$ for some $k \in \{2, \dots, p-2\}$, and so $s = s_{0,0,k,0}$.

For the rest of the proof it will be assumed that $c \neq 0$. Write $s = s_1 s_2$, where s_1 has order p^c and s_2 has order d. Let $G = \langle t, s \rangle$ and let P be a Sylow p-subgroup of G containing t. The group P factorises as $P = \langle t \rangle \langle s_1 \rangle$. Now, (2.2) yields that s_1 is a skew-morphism of $\mathbb{Z}_{p^e}$ of order p^c. By Theorem 5.4, $s_1 = s_{i,j}$ for some $i \in \{0, \dots, p^e - 1\}$ and $j \in \{0, \dots, p^{c-1} - 1\}$. In particular, $P = G(c, j)$. Since $|G : P| = d$ and $d \mid (p-1)$, by the Sylow Theorems, P is normal in G. The permutation s_2 fixes 0 and P is transitive on $\mathbb{Z}_{p^e}$. These yield that $Z_{\langle s_2 \rangle}(P) = 1$, and thus s_2 acts by conjugation on P as an automorphism of order d. We conclude, using the known fact (cf. [2]) that the automorphism group of a non-split metacyclic group is also a p-group, that $P = G(c, j)$ is a split metacyclic group. By Lemma 5.2, this is equivalent to the condition

$$\gcd(i, p^{e-2}) = p^{e-1-c} \mid j. \tag{5.6}$$

Let us consider the conjugate group G^{b_j}. Then $G^{b_j} = \langle ta^j, a^i, s_3\rangle$, where $s_3 = s_2^{b_j}$, $P^{b_j} = \langle ta^j, a^i\rangle$ is normal in G^{b_j}, and s_3 acts on P^{b_j} as an automorphism of order d. There exists $a_1 \in \langle a^i\rangle$ such that P^{b_j} admits the presentation

$$P^{b_j} = \big\langle t, a_1 \mid t^{p^e} = (a_1)^{p^c} = 1,\ t^{a_1} = t^{1+p^{e-c}}\big\rangle.$$

Clearly, $a_1 = a^{i'}$ for a some i' satisfying

$$\gcd(i', p^{e-1}) = \gcd(i, p^{e-1}) = p^{e-1-c}.$$

According to Lemma 4.1 the element s_3 acts on P^{b_j} by conjugation as an automorphism $\theta_{u,v,w}$, where u is a unit of $\mathbb{Z}_{p^e}$, $v \in \{0, \dots, p^e-1\}$, and $w \in \{0, \dots, p^c-1\}$ such that $p^{2c-e} \mid w$ if $2c > e$. As s_3 commutes with a_1, we find

$$a_1 = a_1^{s_3} = \theta_{u,v,w}(a_1) = t^v a_1,$$

hence $v = 0$. Also,

$$t^{s_3} = \theta_{u,0,w}(t) = t^u a_1^w = t^u a^{i'w}.$$

This implies that $s_3 = b^k b_{i'w}$, where $k \in \{0, \dots, p-2\}$ and $k \neq 0$. Then

$$s^{b_j} = (s_1 s_2)^{b_j} = (s_{i,j} s_2)^{b_j} = a^i s_3 = a^i b^k b_{i'w},$$

and thus $s = b_j^{-1} a^i b^k b_{i'w} b_j = s_{i,j,k,l}$, where $l = i'w$.

To finish the proof of the theorem it remains to verify that the 4-tuple (i, j, k, l) is admissible. We have $i, l \in \{0, \dots, p^e - 1\}$ with $i \neq 0$, $j \in \{0, \dots, p^{c-1} - 1\}$, and $k \in \{0, \dots, p-2\}$ with $k \neq 0$. Now, j belongs to the required interval because $\gcd(i, p^{e-2}) = p^{e-c-1}$, and we obtain that (C0) holds.

Since both $i \neq 0$ and $k \neq 0$, we need to check whether (C2) holds. The first part follows from (5.6). The second part is equivalent to $p^{\max\{e-1-c,c-1\}} \mid l$. Since $l = i'w$ and $\gcd(i', p^{e-1}) = \gcd(i, p^{e-1}) = p^{e-1-c}$, the divisibility $p^{e-1-c} \mid l$ follows. We are done if $e - 1 - c \geq c - 1$, thus suppose that $e - 1 - c < c - 1$. In this case $2c > e$, hence $p^{2c-e} \mid w$, and we get $p^{c-1} \mid i'w = l$, as claimed. This completes the proof of the theorem. □

5.3 Enumeration

Finally, we are ready to count the number of skew-morphisms. In view of Proposition 4.4 and Theorems 5.4 and 5.5, this is equivalent to counting the number of admissible 4-tuples (i, j, k, l). Theorem 1.2 follows from the following theorem.

Theorem 5.6. *If $e \geq 2$ and p is an odd prime, then the number of admissible 4-tuples (i, j, k, l) is equal to $(p-1)(p^{2e-1} - p^{2e-2} + 2)/(p+1)$.*

Proof. Let $\mathcal{N}_1$ denote the number admissible 4-tuples (i, j, k, l) with $k = 0$, and let $\mathcal{N}_2$ denote the number of those with $k \neq 0$. By (C1), $\mathcal{N}_1$ is equal to the number of admissible 4-tuples $(i, j, 0, 0)$. Therefore,

$$\begin{aligned}\mathcal{N}_1 &= 1 + \sum_{c=0}^{e-2} \sum_{\substack{i \in \{1,\dots,p^{e-1}-1\} \\ \gcd(i,p^{e-2})=p^c}} p^{e-2-c} \\ &= 1 + \sum_{c=0}^{e-2} (p^{e-1-c} - p^{e-2-c}) p^{e-2-c} \\ &= \frac{p(p^{2e-3}+1)}{p+1}.\end{aligned}$$

Furthermore, using (C0) and (C2), we find

$$\begin{aligned}\frac{\mathcal{N}_2}{p-2} &= 1 + \sum_{c=0}^{e-2} \sum_{\substack{i \in \{1,\dots,p^{e-1}-1\} \\ \gcd(i,p^{e-2})=p^c}} p^{\max\{0,e-2-2c\}+e-1-\max\{c,e-2-c\}} \\ &= 1 + \sum_{c=0}^{e-2} (p^{e-1-c} - p^{e-2-c}) p^{e-1-c} \\ &= \frac{p^{2e-1}+1}{p+1}.\end{aligned}$$

Therefore, $(p+1)(\mathcal{N}_1 + \mathcal{N}_2) = p(p^{2e-3}+1) + (p-2)(p^{2e-1}+1)$, and hence $\mathcal{N}_1 + \mathcal{N}_2 = (p-1)(p^{2e-1} - p^{2e-2} + 2)/(p+1)$. □

Acknowledgments. We would like to thank the referee for the valuable comments.

Bibliography

[1] M. Bachratý and R. Jajcay, Powers of skew-morphisms, in: *Symmetries in Graphs, Maps, and Polytopes. 5th SIGMAP Workshop* (West Malvern 2014), Springer Proc. Math. Stat. 159, Springer, Cham (2016), 1–25.

[2] J. N. S. Bidwell and M. J. Curran, The automorphism group of a split metacyclic p-group, *Arch. Math.* **87** (2006), 488–497.

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

[4] M. Conder, R. Jajcay and T. Tucker, Cyclic complements and skew morphisms of groups, *J. Algebra* **453** (2016), 68–100.

[5] M. Conder and T. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.* **336** (2014), 3585–3609.

[6] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Z.* **58** (1953), 243–264.

[7] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[8] R. Jajcay and R. Nedela, Half-regular Cayley maps, *Graphs Combin.* **31** (2015), 1003–1018.

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

[10] G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer, New York, 1998.

[11] B. W. King, Presentations of metacyclic groups, *Bull. Aust. Math. Soc.* **8** (1973), 105–131.

[12] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars Math. Contemp.* **4** (2011), 291–311.

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

[14] J.-Y. Zhang and S.-F. Du, On the skew-morphisms of dihedral groups, *J. Group Theory* **19** (2016), 993–1016.

Received November 11, 2015; revised March 22, 2017.

Author information

István Kovács, IAM and FAMNIT, University of Primorska,
Glagoljaška 8, 6000 Koper, Slovenia.
E-mail: `istvan.kovacs@upr.si`

Roman Nedela, NTIS – New Technologies for the Information Society,
Faculty of Applied Sciences, University of West Bohemia, Technická 8,
306 14 Plzeň, Czech Republic; and Institute of Mathematics, Slovak Academy of Sciences, Ďumbierska 1, 974 11 Banská Bystrica, Slovakia.
E-mail: `nedela@ntis.zcu.cz`