ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.08
https://doi.org/10.26493/1855-3974.2947.cd6
(Also available at http://amc-journal.eu)

Quotients of skew morphisms of cyclic groups

Martin Bachratý *
Faculty of Civil Engineering, Slovak University of Technology, Bratislava, Slovakia

Received 25 August 2022, accepted 19 April 2023, published online 4 October 2023

Abstract

A skew morphism of a finite group B is a permutation φ of B that preserves the identity element of B and has the property that for every $a \in B$ there exists a positive integer i_a such that $\varphi(ab) = \varphi(a)\varphi^{i_a}(b)$ for all $b \in B$. The problem of classifying skew morphisms for all finite cyclic groups is notoriously hard, with no such classification available up to date. Each skew morphism φ of $\mathbb{Z}_n$ is closely related to a specific skew morphism of $\mathbb{Z}_{|\langle\varphi\rangle|}$, called the quotient of φ. In this paper, we use this relationship and other observations to prove new theorems about skew morphisms of finite cyclic groups. In particular, we classify skew morphisms for all cyclic groups of order $2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free. We also develop an algorithm for finding skew morphisms of cyclic groups, and implement this algorithm in MAGMA to obtain a census of all skew morphisms for cyclic groups of order up to 161.

During the preparation of this paper we noticed a few flaws in Section 5 of the paper Cyclic complements and skew morphisms of groups from 2016. We propose and prove weaker versions of the problematic original assertions (namely Lemma 5.3(b), Theorem 5.6 and Corollary 5.7), and show that our modifications can be used to fix all consequent proofs (in the aforementioned paper) that use at least one of those problematic assertions.

Keywords: Skew morphism, cyclic group, coset-preserving, quotient, square-free.

Math. Subj. Class. (2020): 20B25, 05C25, 05E18

1 Introduction

A skew morphism of a finite group B is a permutation φ of B that preserves the identity element of B and has the property that for every $a \in B$ there exists a positive integer i_a such that $\varphi(ab) = \varphi(a)\varphi^{i_a}(b)$ for all $b \in B$. The *order* of a skew morphism, denoted by

*The author acknowledges the use of the MAGMA system [7] to find examples of skew morphisms relevant to this paper. The author also acknowledges support from the APVV Research Grants 17-0428 and 19-0308, and the VEGA Research Grants 1/0206/20 and 1/0567/22.

E-mail address: martin.bachraty@stuba.sk (Martin Bachratý)

$\mathrm{ord}(\varphi)$, is defined as the order of the cyclic group $\langle\varphi\rangle$. Note that for each $a \in B$ there is a unique choice for i_a such that $i_a \in \{1, 2, \ldots, \mathrm{ord}(\varphi) - 1\}$ (unless φ is the identity permutation). The function π that maps each element $a \in B$ to this integer i_a is called the *power function* of φ, and it satisfies $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in B$. In the case when φ is the identity permutation of B, we define $\pi(a) = 1$ for all $a \in B$.

Skew morphisms were first introduced by Jajcay and Širáň in [18], with primary interest in their connection to the regular Cayley maps. Skew morphisms are also intriguing from a purely group-theoretical point of view, mainly due to their close relationship with group automorphisms, with which they share a number of important features. The problem of classifying all skew morphisms for given families of finite groups has gained much attention in the last two decades; see [8, 10, 23, 24] for example. Recently, in [4], skew morphisms were classified for all finite simple groups, and we understand that a classification for dihedral groups is imminent; see [19]. On the other hand, the problem of finding all skew morphisms for finite cyclic groups remains open, despite recent positive progress, which we discuss next.

Automorphisms of a finite group B are special cases of skew morphisms (with $\pi(a) = 1$ for all $a \in B$), and as such can be viewed as an important family of skew morphisms. There are also other intriguing families of skew morphisms, for example, *coset-preserving* (sometimes also called *smooth*) skew morphisms, which are defined as skew morphisms satisfying $\pi(a) = \pi(\varphi(a))$ for all $a \in B$. Coset-preserving skew morphisms have been fully classified for all finite cyclic groups in [6]. Another interesting family of skew morphisms that is fully understood for finite cyclic groups consists of all skew morphisms φ such that φ^2 is an automorphism of the same group; see [16].

While there is no classification of skew morphisms of finite cyclic groups available to date, skew morphisms have been fully classified for some specific (infinite) families of finite cyclic groups. Most notably, this was done for cases where the order of a cyclic group is a prime [18] (in this case, all skew morphisms are automorphisms), a product of two distinct primes [20], and any power of an odd prime [21]. Some partial progress for cyclic 2-groups can be found in [14].

Another approach for studying skew morphisms of finite cyclic groups is to find a connection between skew morphisms of a given cyclic group B and skew morphisms of cyclic groups of smaller orders. Presumably the strongest finding to date made in this direction is the observation of Kovács and Nedela proved in [20] which states that if $\gcd(m, n) = \gcd(m, \phi(n)) = \gcd(\phi(m), n) = 1$, then the skew morphisms of $\mathbb{Z}_{mn}$ are exactly the direct products of skew morphisms of $\mathbb{Z}_m$ and $\mathbb{Z}_n$. There is also a useful connection between general skew morphisms and coset-preserving skew morphisms for finite cyclic groups. Namely, for each skew morphism φ of a finite cyclic group B there exists an exponent e such that φ^e is a non-trivial coset-preserving skew morphism of B; see [5].

In this paper, we combine a number of known facts about skew morphisms (which we summarise in Sections 2 and 3) with new observations presented in Section 4, to prove a number of theorems about skew morphisms of cyclic groups. Namely, in Section 5 we develop a new method for finding skew morphisms of cyclic groups, and implement it to obtain a census of all skew morphisms of cyclic groups of order up to 161. (Up to the time of writing this paper, and apart from some specific orders, skew morphisms of cyclic groups were known only up to order 60; see [9].) Further, in Section 6 we show that all skew morphisms of $\mathbb{Z}_n$ are coset-preserving if and only if $n = 2^e m$ for some $e \in \{0, 1, 2, 3, 4\}$

and m odd and square-free. As a consequence, we obtain a complete classification of skew morphisms for all cyclic groups of order expressible in this form, significantly expanding the list of finite cyclic groups for which such classification is available. During the review process, it was communicated to us that Kan Hu, István Kovács and Young Soo Kwon has recently submitted a paper devoted to similar ideas to those we investigated in Section 6 of this paper.

2 Preliminaries

In this section, we recall some definitions from group theory and provide some background from the theory of skew morphisms. All groups considered in this paper are assumed to be finite. For the cyclic group of order n we use the additive notation $\mathbb{Z}_n$, and so the elements of $\mathbb{Z}_n$ may be viewed as integers in the interval $[0, n-1]$. We also let $\mathrm{Sym}(G)$ denote the symmetric group on (the underlying set of) a group G.

The *core* of a subgroup H in a group G is the largest normal subgroup of H contained in G. We say that H is *core-free* in G if the core of H in G is trivial. A *complement* for H in G is a subgroup K of G such that $G = HK$ and $H \cap K = \{1\}$. The following theorem proved by Lucchini in [22] will be helpful.

Theorem 2.1 ([22])**.** *Let C be a cyclic proper subgroup of a group G. If C is core-free in G, then $|C| < |G : C|$.*

Next, let φ be a skew morphism of a group B, and identify B with the subgroup of $\mathrm{Sym}(B)$ which acts by left multiplication. Then it can be easily checked that $B\langle\varphi\rangle$ is a subgroup of $\mathrm{Sym}(B)$ (see [20] for example). Moreover, $B\langle\varphi\rangle$ is a complementary factorisation and $\langle\varphi\rangle$ is core-free in $B\langle\varphi\rangle$ (see [12, Lemma 4.1]). A group G containing B which has a cyclic core-free complement C for B is called a *skew product group* for a group B, and we say that C is a *skew complement* (for B in G). The skew product group $B\langle\varphi\rangle$ (for B) with skew complement $\langle\varphi\rangle$ described in this paragraph is said to be *induced* by φ.

Conversely, let G be a skew product group for a group B, and let c be a generator of a skew complement for B in G. Note that every element $g \in G$ is uniquely expressible in a form $g = ac'$ with $a \in B$ and $c' \in C$. Then for every $a \in B$ there exists a unique $a' \in B$ and a unique exponent $j \in \{1, 2, \ldots, |C| - 1\}$ such that $ca = a'c^j$, and this induces a bijection $\varphi\colon B \to B$ and a function $\pi\colon B \to \mathbb{N}$, defined by $\varphi(a) = a'$ and $\pi(a) = j$. It can be easily checked that φ is a skew morphism of B with power function π. We say that φ is *induced* by the pair (B, c).

Recall that if φ is a skew morphism of B with power function π, then we have $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in B$. (Hence, if $B = \mathbb{Z}_n$, then $\varphi(a+b) = \varphi(a) + \varphi^{\pi(a)}(b)$ for all $a, b \in \mathbb{Z}_n$.) Also recall that an automorphism of B is a skew morphism with $\pi(a) = 1$ for all $a \in B$. In what follows, it will be often convenient to distinguish between general skew morphisms and skew morphisms that are not automorphisms, and so we will refer to the latter as *proper* skew morphisms. We say that φ is *trivial* if it is the identity permutation of B. The *kernel* of φ, denoted by $\ker\varphi$, is the subset $\{a \in B \mid \pi(a) = 1\}$ of B. By definition, φ is an automorphism of B if and only if $\ker\varphi = B$. In the case of proper skew morphisms $\ker\varphi$ is not equal to B, but it is always a subgroup of B; see [18, Lemma 4].

Since $\ker\varphi$ is a subgroup of B and also $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in \ker\varphi$, it follows that φ restricts to a group isomorphism from the kernel to its image. In particular, if $\ker\varphi$ is preserved by φ set-wise, then φ restricts to an automorphism of $\ker\varphi$. In [11] this was shown to always be true for abelian groups. We also have the following.

Lemma 2.2 ([18]). *Let φ be a skew morphism of a group B with power function π. Then two elements $a, b \in B$ belong to the same right coset of the subgroup $\ker\varphi$ in B if and only if $\pi(a) = \pi(b)$.*

Theorem 2.3 ([12]). *Every skew morphism of a non-trivial group has non-trivial kernel.*

An immediate consequence of Theorem 2.3 is that every skew morphism of a group of prime order is an automorphism. The following facts about kernels of skew morphisms will be useful, too.

Lemma 2.4 ([12]). *Let G be a skew product group for a group B with skew complement C, and let c be a generator of C. If φ is the skew morphism induced by (B, c), then $\ker\varphi$ is the largest subgroup H of B for which $cHc^{-1} \subseteq B$. In particular, φ is an automorphism of B if and only if B is normal in G.*

Proposition 2.5 ([12]). *Let φ be a skew morphism of a group B, and let N be a subgroup of $\ker\varphi$ that is normal in B and preserved by φ. Then the mapping $\varphi_N^* : B/N \to B/N$ given by $\varphi_N^*(x) = N\varphi(x)$ is a well-defined skew morphism of B/N.*

Lemma 2.6 ([12]). *Let φ be a skew morphism of a finite abelian group A with power function π. Also suppose that N is any non-trivial subgroup of $\ker\varphi$ preserved by φ, let i be the exponent of N, and let φ_N^* be the skew morphism of A/N induced by φ. If a is an element of A such that Na lies in the kernel of φ_N^*, then $i\pi(a) \equiv i \pmod{\mathrm{ord}(\varphi)}$ and, in particular, if $\gcd(i, \mathrm{ord}(\varphi)) = 1$, then $a \in \ker\varphi$.*

Note that if φ is a skew morphism of $\mathbb{Z}_n$, then $\ker\varphi$ is normal in $\mathbb{Z}_n$ and φ restricts to an automorphism of $\ker\varphi$. Moreover, since $\mathbb{Z}_n$ is cyclic, so is (its subgroup) $\ker\varphi$. Noting that every automorphism of a cyclic group preserves all of its subgroups, we deduce that φ preserves all subgroups of $\ker\varphi$. Hence it follows from Proposition 2.5 that φ_N^* is a well defined skew morphism of $\mathbb{Z}_n/N$ for each subgroup N of $\ker\varphi$. In the case when $N = \ker\varphi$, we will write simply φ^* instead of φ_N^*.

We proceed with some useful facts about orders of skew morphisms.

Proposition 2.7 ([20]). *Let φ be a skew morphism of a group B, and let T be an orbit of $\langle\varphi\rangle$. If $\langle T\rangle = B$, then $\mathrm{ord}(\varphi) = |T|$.*

Theorem 2.8 ([12]). *The order of a skew morphism of a non-trivial group B is less than the order of B.*

Theorem 2.9 ([20]). *If φ is a skew morphism of a group $\mathbb{Z}_n$, then $\mathrm{ord}(\varphi)$ is a divisor of $n\phi(n)$. Moreover, if $\gcd(\mathrm{ord}(\varphi), n) = 1$, then φ is an automorphism of $\mathbb{Z}_n$.*

The *periodicity* of a skew morphism φ of a group B, denoted by p_φ, is the smallest positive integer such that $\pi(a) = \pi(\varphi^{p_\varphi}(a))$ for all $a \in B$. Similarly, the *periodicity* of $a \in B$ (with respect to φ) is the smallest positive integer p_a such that $\pi(a) = \pi(\varphi^{p_a}(a))$. Note that if $\ker\varphi$ is preserved by φ (which is always true if B is abelian), then the periodicity of φ can be defined equivalently as the order of φ^*.

Recall that φ is coset-preserving if $\pi(a) = \pi(\varphi(a))$ for all $a \in B$. Equivalently, coset-preserving skew morphisms can be viewed as skew morphism that preserves all right cosets of $\ker\varphi$ in B, or as skew morphisms with the periodicity equal to 1. The following theorem about periodicities underlines the importance of coset-preserving skew morphisms in the study of skew morphisms of abelian (and, in particular, cyclic) groups.

Theorem 2.10 ([5]). *If φ is a skew morphism of an abelian group A, then φ^{p_φ} is a coset-preserving skew morphism of A. Moreover, if A is cyclic, b is a generator of A, and φ is non-trivial, then $p_\varphi = p_b$ and $p_\varphi < \mathrm{ord}(\varphi)$.*

The following fact will be helpful too.

Lemma 2.11 ([12]). *Let φ be any skew morphism of a finite group G, and let H be any finite group. Then φ can be extended to a skew morphism θ of $G \times H$, such that $\theta \restriction_G = \varphi$ and $\ker\theta = \ker\varphi \times H$.*

We conclude this section with two well-known facts about skew morphisms that are easy exercises, but we include their proofs for completeness.

Lemma 2.12. *Let φ be a skew morphism of an abelian group A. If $\varphi(a) = a$ for some $a \in A$, then $a \in \ker\varphi$.*

Proof. Let a' be any element of A. Since a is fixed by φ, we have $\varphi(aa') = a\varphi^{\pi(a)}(a')$. On the other hand, we have $\varphi(aa') = \varphi(a'a) = \varphi(a')\varphi^{\pi(a')}(a) = \varphi(a')a$, and hence $\varphi(a') = \varphi^{\pi(a)}(a')$ for all $a' \in A$. It follows that $\pi(a) = 1$, and therefore $a \in \ker\varphi$. □

Lemma 2.13. *Let φ be a skew morphism of a group B with power function π, and let $a \in B$. Then:*

$$\varphi(a^i) = \varphi(a)\varphi^{\pi(a)}(a)\varphi^{\pi(a^2)}(a)\dots\varphi^{\pi(a^{i-1})}(a) \text{ for all } i \in \mathbb{N}.$$

Proof. The assertion is trivially true for $i = 1$. Next, if it holds for some positive integer j, then $\varphi(a^{j+1}) = \varphi(a^j a) = \varphi(a^j)\varphi^{\pi(a^j)}(a) = \varphi(a)\varphi^{\pi(a)}(a)\dots\varphi^{\pi(a^{j-1})}(a)\varphi^{\pi(a^j)}(a)$, and so it is also true for $j+1$. Hence the proof follows by induction. □

3 Skew morphisms of abelian groups

Several useful facts about skew morphisms of abelian groups (which we also apply in this paper) were proved in [12]. During the preparation of this paper, however, we noticed that three assertions in [12] do not hold. In this section, we list the incorrect findings and provide a counterexample for each of them. We also propose and prove weaker versions of the original statements. Finally, we discuss all proofs in [12] that use at least one of the flawed statements, and show that in all cases it is sufficient to replace the flawed statements by our modifications. For the rest of the section, we let φ be a skew morphism of an abelian group A with power function π. Also, to distinguish between references to this paper and references to [12], we put an asterisk after each numbered reference in the latter case.

The first flawed assertion in [12] is part (b) of Lemma 5.3*. It states that if N is a non-trivial subgroup of $\ker\varphi$ preserved by φ, and φ is not an automorphism of A, then $\mathrm{ord}(\varphi)$ has a non-trivial divisor in common with the exponent of N. To show that this is not true, note that according to [9] the cyclic group of order 12 admits a proper skew morphism ψ of order 3 with kernel (which is preserved by ψ) of order 6. Since $\ker\psi$ is cyclic and preserved by ψ, so is its unique subgroup of order 2. But the exponent of this subgroup, which is 2, does not have a non-trivial divisor in common with $\mathrm{ord}(\psi)$. We propose the following modification:

Lemma 3.1. *If φ is a proper skew morphism of an abelian group A, then $\mathrm{ord}(\varphi)$ has a non-trivial divisor in common with the exponent of $\ker\varphi$.*

Proof. Let $K = \ker\varphi$, let e be the exponent of K, and let L/K be the kernel of the skew morphism φ^* of A/K induced by φ. Since φ is proper we know that A/K is a non-trivial group, and by Theorem 2.3 it follows that L/K is non-trivial. In particular, there exists an element a of A such that $a \notin K$ and $a \in L$. It follows that $\pi(a) \not\equiv 1 \pmod{\mathrm{ord}(\varphi)}$, by Lemma 2.6 we have $e\pi(a) \equiv e \pmod{\mathrm{ord}(\varphi)}$, and the rest follows. □

Part (b) of Lemma 5.3* is used in the proofs of six theorems presented in [12]. Proofs of Theorem 5.4*, Theorem 5.10*, Theorem 6.2* and Theorem 6.4* are all easily fixable, since in each case Lemma 5.3(b)* is applied for $N = K$, and hence it is sufficient to replace it with Lemma 3.1. The proof of Theorem 6.1* can also be corrected. Here Lemma 5.3(b)* is used to show that if φ is proper and $A \cong \mathbb{Z}_n$, then $\gcd(\mathrm{ord}(\varphi), n) \neq 1$. Since A is cyclic, the exponent of $\ker\varphi$ is equal to the order of $\ker\varphi$ (which necessarily divides n), so this is an easy consequence of Lemma 3.1. Finally, since Theorem 7.3* was already proved previously in [20], there is no need to fix its alternative proof presented in [12]; although we believe that it is possible.

Another flawed assertion in [12] is Theorem 5.6*. It states that if $L/(\ker\varphi)$ is the kernel of the skew morphism φ^* of $A/(\ker\varphi)$ induced by φ, and p is a prime that divides $|L|$ but not $|\ker\varphi|$, then $p < q$ for every prime divisor q of $|\ker\varphi|$. Again, we provide a counterexample that shows that this is not true. According to [9] the cyclic group of order 42 admits a proper skew morphism ρ of order 7 with kernel of order 14. Since $\mathbb{Z}_{42}/(\ker\rho)$ is isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_3$ does not admit any proper skew morphism, it follows that the kernel $L/(\ker\rho)$ (of the skew morphism of $\mathbb{Z}_{42}/(\ker\rho)$ induced by ρ) is equal to $\mathbb{Z}_{42}/(\ker\rho)$. Therefore, $|L| = |\mathbb{Z}_{42}|$ and, in particular, 3 divides $|L|$. But 3 is greater than 2, and 2 is a prime divisor of $|\ker\rho|$. We propose the following modification:

Theorem 3.2. *Let φ be a skew morphism of the finite abelian group A, let $K = \ker\varphi$, and let q be any prime divisor of $|K|$. Also let N be a subgroup of K consisting of the identity and all elements of order q, and let L/N be the kernel of the skew morphism φ_N^* of A/N induced by φ. If p is a prime that divides $|L|$ but not $|K|$, then $p < q$.*

Proof. Suppose that such a prime p exists. Since K is abelian, we know that N is a subgroup of K of exponent q that is invariant under φ. Next, let a be any element of order p in L, let $m = \mathrm{ord}(\varphi)$, and let π be the power function of φ. Since L/N is the kernel of φ_N^*, we know by Lemma 2.6 that $q(\pi(a) - 1) \equiv 0 \pmod{m}$. If q is relatively prime to m, then $\pi(a) \equiv 1 \pmod{m}$ and so $a \in K$, which is impossible since K has no element of order p. Thus q divides m and $\pi(a) - 1 \equiv 0 \pmod{m/q}$. In particular, $\pi(a) = 1 + i(m/q)$ where $1 \leq i \leq q - 1$, so there are at most $q - 1$ possibilities for $\pi(a)$.

The same holds for every non-trivial power of a. So now if $p > q$, then by the pigeonhole principle two different powers of a will have the same value under π, in which case they lie in the same coset of N. But that cannot happen since $K \cap \langle a\rangle$ is trivial. Thus $p < q$. □

The only application of the flawed original version of Theorem 5.6* is Corollary 5.7*. This final problematic assertion in [12] states that every prime divisor of $|\ker\varphi|$ is greater than every prime that divides $|A|$ but not $|\ker\varphi|$. To see that this is not true, take the skew morphism ρ of $\mathbb{Z}_{42}$ with kernel of order 14 discussed earlier. Since 2 divides $|\ker\rho|$ and 3 divides $|\mathbb{Z}_{42}|$ but not $|\ker\rho|$, the statement is clearly not true. The following, however, still holds.

Corollary 3.3. *Let A be a non-trivial finite abelian group, and let p be the largest prime divisor of $|A|$. Then the order of the kernel of every skew morphism of A is divisible by p when p is odd, or by 4 when $p = 2$.*

Proof. Let φ be any skew morphism of A, let $K = \ker\varphi$, and suppose to the contrary that p does not divide $|K|$. Also let q be any prime divisor of $|K|$, let N be a subgroup of K consisting of the identity and all elements of order q, and let L/N be the kernel of the skew morphism φ_N^* of A/N induced by φ. If p divides $|L/N|$, then by Theorem 3.2 we know that p is smaller than q, so this cannot happen. It follows that p does not divide $|L/N|$, so we can repeat the same argument for the skew morphism φ_N^* of A/N with kernel L/N. (Note that p divides $|A/N|$.) Since A is finite, this will eventually terminate for some groups A', N' and L' with $|L'/N'| = 1$. Then since the kernel L'/N' is trivial, it follows by Theorem 2.3 that A'/N' is a trivial group, and hence $|A'| = |N'|$. But this is impossible, since p divides $|A'|$ but not $|N'|$. The second part for $p = 2$ follows from the original proof of [12, Corollary 5.7]. □

Both applications of Corollary 5.7*, namely the proofs of Theorem 6.2* and Theorem 9.1*, only use the fact that the order of $\ker\varphi$ is divisible by the largest prime divisor of $|A|$. Since this follows by Corollary 3.3, both theorems still hold, and their proofs can be corrected by minor changes in their wording.

4 Quotients and their properties

In this section, we will show that if BC is a complementary product of two cyclic groups with C core-free in BC, then not only C corresponds to some skew morphism of B (of order $|C|$), but also B corresponds to some skew morphism of C (of order smaller than $|B|$). Let φ be a skew morphism of a cyclic group B, let $G = B\langle\varphi\rangle$, and let $C = \langle\varphi\rangle$. Also let b be a generator of B. To distinguish between φ as a permutation of B and φ as a generator of the cyclic group C, we use c in the latter case. Since C is core-free in G, by Theorem 2.1 we have

$$|G : B| = |C| < |G : C| = |B|\,,$$

so (again by Theorem 2.1) we find that B has a non-trivial core in G. Let K denote the core of B in G, and for every $X \leq G$ let $\overline{X}$ denote XK/K ($\cong X/(X \cap K)$). Next, let H be a subgroup of B such that $cHc^{-1} \subseteq B$. Then, since B is cyclic, H is the unique subgroup of B of order $|H|$, and so $cHc^{-1} = H$. It follows that H is normal in G, and so it is contained in K. Moreover, since K is the core of B in G, we have $cKc^{-1} = K \subseteq B$, and hence by Lemma 2.4 we find that $K = \ker\varphi$.

Now we look closely at the product $\overline{G} = \overline{B}\,\overline{C}$. First, noting that $K \cap C = \{1\}$ we have $C \cong \overline{C}$ (and so $\overline{C}$ is cyclic, and hence abelian) and $\overline{B} \cap \overline{C} = \{1\}$. Since B is cyclic, so is its quotient $\overline{B}$, and by the definition of K we deduce that $\overline{B}$ is core-free in $\overline{G}$. Now it is straightforward to check that the bijection that maps every element $\overline{d} \in \overline{C}$ to the unique element $\overline{d'} \in \overline{C}$ such that $\overline{d}\,\overline{b} = \overline{b}^j\overline{d'}$ defines a skew morphism of $\overline{C}$, with power function $\overline{\pi}$ given by $\overline{\pi}(\overline{d}) = j$. (We choose $\overline{b}$ to be the image of $b \in B$ under the natural homomorphism from B to $\overline{B}$; since b is a generator of B, it follows that $\overline{b}$ is a generator of $\overline{B}$.)

A skew morphism of C ($\cong \overline{C}$) constructed in the way described in the previous paragraph is called the *quotient* of φ (with respect to b), and will be denoted by $\overline{\varphi}$. Since a cyclic group $\overline{B}$ can be generated by different elements, φ can have more than one quotient.

(In fact, by [4, Remark 5.1] this is always true unless B has a unique generator.) In the case of additive notation $B = \mathbb{Z}_n$, and unless otherwise specified, by the quotient of φ we understand the quotient with respect to 1.

The above construction (proposed in the author's PhD thesis [3]) was also introduced independently in [15], where it was noted that if φ is a skew morphism of $\mathbb{Z}_n$ and $\overline{\varphi}$ is a quotient of φ, then $(\varphi, \overline{\varphi})$ is an $(\mathrm{ord}(\varphi), n)$-reciprocal pair of skew morphisms. A pair (φ, ρ) of skew morphisms of $\mathbb{Z}_n$ and $\mathbb{Z}_m$ with power functions π and τ is called (m, n)-*reciprocal* if $\mathrm{ord}(\varphi)$ divides m, $\mathrm{ord}(\rho)$ divides n, and the congruences $\pi(i) \equiv \rho^i(1) \pmod{\mathrm{ord}(\varphi)}$ and $\tau(j) \equiv \varphi^j(1) \pmod{\mathrm{ord}(\rho)}$ hold for each $i \in \mathbb{Z}_n$ and $j \in \mathbb{Z}_m$. We note that while every pair $(\varphi, \overline{\varphi})$ gives an $(\mathrm{ord}(\varphi), n)$-reciprocal pair of skew morphisms, not every reciprocal pair arises in this way. For example, there exist (m, n)-reciprocal pairs of skew morphisms with $m = n$, but by Theorem 2.8 we know that $\mathrm{ord}(\varphi)$ is always strictly smaller than n.

The following observation is an easy consequence of the fact that a skew morphism (of a cyclic group) and its quotient always give a reciprocal pair of skew morphisms.

Lemma 4.1. *Let φ be a skew morphism of $\mathbb{Z}_n$ with power function π, and let $\overline{\varphi}$ be the quotient of φ with power function $\overline{\pi}$. Then for every $i \in \mathbb{N}$:*

(a) $\pi(i) = \overline{\varphi}^i(1)$, *so in particular* $\mathrm{ord}(\overline{\varphi}) = n/|\ker\varphi|$; *and*

(b) $\varphi^i(1) \equiv \overline{\pi}(i) \pmod{n/|\ker\varphi|}$.

Proof. First, since $(\varphi, \overline{\varphi})$ is an $(\mathrm{ord}(\varphi), n)$-reciprocal pair of skew morphisms, we have $\pi(i) \equiv \overline{\varphi}^i(1) \pmod{\mathrm{ord}(\varphi)}$. Hence, since both π and $\overline{\varphi}$ are mappings into $\mathbb{Z}_{\mathrm{ord}(\varphi)}$, it follows that $\pi(i) = \overline{\varphi}^i(1)$. The second part of (a) follows from the fact that $n/|\ker\varphi|$ is the smallest non-zero integer in $\ker\varphi$. Finally, (b) follows easily as $\overline{\pi}(i) \equiv \varphi^i(1) \pmod{\mathrm{ord}(\overline{\varphi})}$ and $\mathrm{ord}(\overline{\varphi}) = n/|\ker\varphi|$. □

Next we provide a lemma which shows that quotients can be used to check whether a skew morphism of a cyclic group is an automorphism or a coset-preserving skew morphism.

Lemma 4.2. *A skew morphism φ of $\mathbb{Z}_n$ is coset-preserving if and only if the quotient $\overline{\varphi}$ of φ is an automorphism. Moreover, φ is proper if and only if $\overline{\varphi}$ is non-trivial.*

Proof. Let φ be a coset-preserving skew morphism of $\mathbb{Z}_n$. This is equivalent with $\varphi(1) \equiv 1 \pmod{n/|\ker\varphi|}$, which by Lemma 4.1(b) happens if and only if $\overline{\pi}(1) = 1$. This proves the first part. The second part follows easily by Lemma 4.1(a) as $\varphi \in \mathrm{Aut}(\mathbb{Z}_n)$ if and only if $\pi(1) = 1$, and $\overline{\varphi}$ is trivial if and only if $\overline{\varphi}(1) = 1$. □

We note that a part of the Lemma 4.2 was proved in [17], where it was shown that if $\overline{\varphi}$ is an automorphism, then φ is coset-preserving, but not the other way around. Also note that since the only skew morphism of $\mathbb{Z}_2$ is the identity mapping, it follows immediately from Lemma 4.2 that if a skew morphism of a cyclic group has order 2, then it must be an automorphism. (This is also an easy consequence of Lemma 2.4.) Another consequence of Lemma 4.2 is the fact that a proper skew morphism of $\mathbb{Z}_n$ is coset-preserving if and only if the quotient of its quotient is the identity mapping. Somewhat interestingly, Lemma 4.2 also implies that by taking quotients every skew morphism of a cyclic group can be reduced to a non-trivial automorphism of the same group.

5 Using quotients to generate skew morphisms

In this section, we describe an algorithm for finding recursively skew morphisms of cyclic groups based on various observations about the quotients of skew morphisms.

5.1 Skew morphisms with a given quotient

First, we explain how to find all skew morphisms of a cyclic group with a given quotient. The following observation about quotients of skew morphisms of cyclic groups will be useful.

Proposition 5.1. *Let φ be a skew morphism of $\mathbb{Z}_n$ with power function π, and let $\overline{\varphi}$ be the quotient of φ with power function $\overline{\pi}$. Then:*

(a) *the periodicity p_φ of φ is the smallest generator of $\ker\overline{\varphi}$;*

(b) $\operatorname{ord}(\varphi) = |\ker\overline{\varphi}|p_\varphi$*; and*

(c) *the orbit T of $\langle\varphi\rangle$ that contains 1 is expressible in the form*

$$T = (x_1, \ldots, x_{p_\varphi}, \psi(x_1), \ldots, \psi(x_{p_\varphi}), \ldots, \psi^{\operatorname{ord}(\psi)-1}(x_1), \ldots, \psi^{\operatorname{ord}(\psi)-1}(x_{p_\varphi})), \tag{5.1}$$

for some coset-preserving skew morphism ψ of $\mathbb{Z}_n$ such that $\operatorname{ord}(\psi) = \operatorname{ord}(\varphi)/p_\varphi$ and $\psi(1) \equiv 1 \pmod{n/|\ker\varphi|}$, and with $x_1 = 1$ and $x_i \equiv \overline{\pi}(i-1) \pmod{n/|\ker\varphi|}$ for each $i \in \{2, \ldots, p_\varphi\}$.

Proof. First, by Theorem 2.10 we have $p_\varphi = p_1$. Then, since the values taken by π at any two elements of $\mathbb{Z}_n$ are equal if and only if they belong to the same right coset of $\ker\varphi$ in $\mathbb{Z}_n$, it follows that p_1 is the smallest positive integer such that $1 \equiv \varphi^{p_1}(1) \pmod{n/|\ker\varphi|}$, which by Lemma 4.1(b) is equivalent with $1 \equiv \overline{\pi}(p_1) \pmod{n/|\ker\varphi|}$. Noting that $n/|\ker\varphi| = \operatorname{ord}(\overline{\varphi})$, we deduce that p_1 is the smallest positive integer such that $\overline{\pi}(p_1) = 1$, and (a) follows. Moreover, since p_φ is the smallest non-trivial element of $\ker\overline{\varphi}$, which is a subgroup of $\mathbb{Z}_{\operatorname{ord}(\varphi)}$, it follows that $\operatorname{ord}(\varphi) = |\ker\overline{\varphi}|p_\varphi$, which proves (b).

To prove the final assertion, let T denote the orbit of $\langle\varphi\rangle$ that contains 1, and let $\psi = \varphi^{p_1}$. By Theorem 2.10 we know that ψ is a coset-preserving skew morphism of $\mathbb{Z}_n$, and by the definition of the periodicity we have $\psi(1) \equiv 1 \pmod{n/|\ker\varphi|}$. By Proposition 2.7 we know that the size of T is equal to $\operatorname{ord}(\varphi)$. Moreover, p_1 divides $|T|$ (see [6, Lemma 3.1]), and hence $\operatorname{ord}(\psi) = \operatorname{ord}(\varphi^{p_1}) = \operatorname{ord}(\varphi)/p_1$, and the effect of ψ on T induces p_1 cycles, each of length $\operatorname{ord}(\varphi)/p_1$. Finally, by Lemma 4.1(b) we have $x_i = \varphi^{i-1}(1) \equiv \overline{\pi}(i-1) \pmod{n/|\ker\varphi|}$ and the rest follows. □

Let ρ be a skew morphism of a cyclic group $\mathbb{Z}_m$. We will provide a detail explanation of the method for finding all skew morphisms φ of $\mathbb{Z}_n$ with quotient ρ.[1]

First, we find the smallest positive integer j such that $j \in \ker\rho$. Then by Proposition 5.1(a) we have $p_1 = p_\varphi = j$. Next, since ρ is a quotient of φ, it follows by

[1] It is important to emphasise here that this method finds all skew morphisms with a particular quotient only for a given cyclic group. If we do not restrict ourselves to a specific group, then in some cases we can find infinitely many skew morphisms with a given quotient. For example, using the classification of skew morphisms for cyclic p-groups of odd order (presented in [21]) it can be shown that each cyclic 3-group of order at least 9 admits a skew morphism whose quotient is the skew morphism $(1, 3, 5)$ of $\mathbb{Z}_6$.

Lemma 4.1(a) that $\mathrm{ord}(\rho) = n/|\ker\varphi|$, and hence $\ker\varphi$ is the unique subgroup of $\mathbb{Z}_n$ of order $n/\mathrm{ord}(\rho)$. As a next step we find all coset-preserving skew morphisms ψ of $\mathbb{Z}_n$ satisfying $\mathrm{ord}(\psi) = m/p_\varphi$ and $\psi(1) \equiv 1 \pmod{n/|\ker\varphi|}$ (note here that $m = |\mathbb{Z}_m| = \mathrm{ord}(\varphi)$). This allows us to identify all possible candidates for the orbit T of $\langle\varphi\rangle$ that contains 1, using (5.1). (For each choice of ψ, we have at most $|\ker\varphi|^{p_1-1} = (n/\mathrm{ord}(\rho))^{p_1-1}$ candidates; the number of candidates could be smaller since sometimes (5.1) does not define a cycle on B.)

Next, suppose that φ is a skew morphism, and let φ_1 be the cyclic permutation of T induced by φ. Then by Lemma 4.1(a) we have $\pi(i) = \rho^i(1)$, and hence by Lemma 2.13 we find that

$$\varphi(i) = \varphi_1(1) + \varphi_1^{\rho(1)}(1) + \varphi_1^{\rho^2(1)}(1) + \cdots + \varphi_1^{\rho^{i-1}(1)}(1) \text{ for all } i \in \mathbb{N}. \tag{5.2}$$

As a final step, for each candidate for φ_1 we use (5.2) to define a function $\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_n$, and then check whether φ is a skew morphism of $\mathbb{Z}_n$, and T an orbit of $\langle\varphi\rangle$. It can be easily verified that if this is true, then ρ is the quotient of φ.

Remark 5.2. Note that to use (5.2), we do not need to know the complete orbit T, but only the elements $\varphi_1^{\rho^i(1)}(1)$ for each $i \in \{0, 1, \ldots, \mathrm{ord}(\rho)\}$. In fact, since for every positive integer j we have $\varphi_1^{j+p_1}(1) = \psi(\varphi_1^j(1))$, only elements of the form $\varphi_1^e(1)$ with $e \equiv \rho^i(1) \pmod{p_1}$ are needed to define φ. In some cases, this significantly reduces the number of possible candidates for φ_1.

5.2 Algorithm for finding all skew morphisms of a cyclic group

We are ready to describe our algorithm for finding all skew morphisms of cyclic groups up to any order. This algorithm is recursive in the sense that it takes the sets of all skew morphisms of the groups $\mathbb{Z}_m$ for $m \in \{2, 3, \ldots, n-1\}$ as input and outputs all skew morphisms of $\mathbb{Z}_n$. Since the only skew morphism of $\mathbb{Z}_2$ is the identity permutation, the algorithm can be easily initialised.

As the first step, we use the method presented in [6] to find all coset-preserving skew morphisms of $\mathbb{Z}_n$. Further details on this method are available in Section 6.3. Next, let φ be a skew morphism of $\mathbb{Z}_n$ that is not coset-preserving, and let $\overline{\varphi}$ be the quotient of φ. Then by Lemma 4.2 we know that $\overline{\varphi}$ is a proper skew morphism of $\mathbb{Z}_{\mathrm{ord}(\varphi)}$. Moreover, by Theorem 2.8 and Theorem 2.9 we find that $\mathrm{ord}(\varphi) < n$, and that $\mathrm{ord}(\varphi)$ divides $n\phi(n)$, and $\gcd(\mathrm{ord}(\varphi), n) \neq 1$. Since we know all skew morphisms of $\mathbb{Z}_m$ for each $m < n$, and we also know all coset-preserving skew morphisms of $\mathbb{Z}_n$, it follows that we can simply apply the method explained in the previous subsection to find all skew morphisms of $\mathbb{Z}_n$ that are not coset-preserving. Together with the coset-preserving skew morphisms of $\mathbb{Z}_n$ (which include all automorphisms and were found earlier), this gives all skew morphisms of $\mathbb{Z}_n$.

A MAGMA [7] implementation of the described algorithm succeeded in finding all skew morphisms of cyclic groups of order up to 161. (The file listing all of these skew morphisms is available at [2].) This significantly improves the previous largest complete list [9] which goes up to the order 60. In Table 1 we summarise the information obtained about skew morphisms of cyclic groups $\mathbb{Z}_n$ for $n \leq 161$. We include a group in the table if and only if it admits a proper skew morphism. Moreover, if a listed group admits a proper skew morphism that is not coset-preserving, then the order of the group is preceded by

n	Skew	Classes	n	Skew	Classes	n	Skew	Classes
6	**2** + 2	**1**	58	**28** + 28	**1**	114	**148** + 36	**7**
8	**2** + 4	**1**	60	**80** + 16	**17**	116	**112** + 56	**3**
*9	**4** + 6	**2**	62	**30** + 30	**1**	*117	**88** + 72	**11**
10	**4** + 4	**1**	*63	**44** + 36	**7**	118	**58** + 58	**1**
12	**4** + 4	**2**	*64	**268** + 32	**42**	120	**208** + 32	**43**
14	**6** + 6	**1**	66	**60** + 20	**13**	*121	**900** + 110	**90**
16	**12** + 8	**4**	68	**64** + 32	**3**	122	**60** + 60	**1**
*18	**24** + 6	**6**	70	**72** + 24	**11**	124	**60** + 60	**2**
20	**16** + 8	**3**	*72	**156** + 24	**36**	*125	**1568** + 100	**152**
21	**12** + 12	**1**	74	**36** + 36	**1**	*126	**348** + 36	**34**
22	**10** + 10	**1**	*75	**96** + 40	**24**	*128	**1132** + 64	**114**
24	**16** + 8	**7**	76	**36** + 36	**2**	129	**84** + 84	**1**
*25	**48** + 20	**12**	78	**104** + 24	**9**	130	**144** + 48	**17**
26	**12** + 12	**1**	80	**152** + 32	**26**	132	**120** + 40	**26**
*27	**64** + 18	**20**	*81	**676** + 54	**110**	134	**66** + 66	**1**
28	**12** + 12	**2**	82	**40** + 40	**1**	*135	**256** + 72	**80**
30	**24** + 8	**7**	84	**104** + 24	**14**	136	**228** + 64	**10**
*32	**60** + 16	**14**	86	**42** + 42	**1**	138	**132** + 44	**25**
34	**16** + 16	**1**	88	**80** + 40	**15**	140	**240** + 48	**29**
*36	**48** + 12	**12**	*90	**216** + 24	**36**	142	**70** + 70	**1**
38	**18** + 18	**1**	92	**44** + 44	**2**	*144	**552** + 48	**96**
39	**24** + 24	**1**	93	**60** + 60	**1**	146	**72** + 72	**1**
40	**44** + 16	**9**	94	**46** + 46	**1**	*147	**960** + 84	**68**
42	**52** + 12	**7**	*96	**272** + 32	**58**	148	**144** + 72	**3**
44	**20** + 20	**2**	*98	**480** + 42	**38**	*150	**648** + 40	**74**
*45	**16** + 24	**8**	*99	**40** + 60	**20**	152	**144** + 72	**23**
46	**22** + 22	**1**	*100	**512** + 40	**42**	*153	**64** + 96	**32**
48	**64** + 16	**20**	102	**96** + 32	**19**	154	**180** + 60	**17**
*49	**180** + 42	**30**	104	**132** + 48	**13**	155	**120** + 120	**1**
*50	**152** + 20	**18**	105	**48** + 48	**4**	156	**352** + 48	**22**
52	**48** + 24	**3**	106	**52** + 52	**1**	158	**78** + 78	**1**
*54	**246** + 18	**33**	*108	**492** + 36	**66**	*160	**616** + 64	**84**
55	**40** + 40	**1**	110	**168** + 40	**9**			
56	**48** + 24	**11**	111	**72** + 72	**1**			
57	**36** + 36	**1**	112	**192** + 48	**36**			

Table 1: Skew morphisms of cyclic groups of order n.

the asterisk character (*). All included groups are listed by their orders, and for each of them we provide the total number of skew morphisms (written as the sum of the numbers of proper skew morphisms and automorphisms), and the number of conjugacy classes of proper skew morphisms in $\mathrm{Aut}(\mathbb{Z}_n)$. Note that the automorphism group of a cyclic group $\mathbb{Z}_n$ is always abelian, and hence the conjugation action of $\mathrm{Aut}(\mathbb{Z}_n)$ on itself is trivial. It follows that the number of conjugacy classes of $\mathrm{Aut}(\mathbb{Z}_n)$ is equal to $|\mathrm{Aut}(\mathbb{Z}_n)|$. For this reason, we list the number of conjugacy classes only for proper skew morphisms. We also note that the numbers of skew morphisms in Table 1 for $n \leq 60$ coincide with the numbers of skew morphisms in [9].

5.3 Remarks concerning Table 1

An inspection of Table 1 suggests various interesting questions regarding skew morphisms of cyclic groups. Possibly the most natural question to ask here is which values n actually appear in Table 1 or, equivalently, which cyclic groups admit a proper skew morphism.

This was answered in [20] for cyclic groups, and later in [12] for all other abelian groups. Specifically, if an abelian group A does not admit any proper skew morphism, then A is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or A is an elementary abelian 2-group.

Next, we look at values n such that $\mathbb{Z}_n$ admits (up to conjugacy in $\mathrm{Aut}(\mathbb{Z}_n)$) only one proper skew morphism. In [20] this was shown to be true for all cases where n is a product of two distinct primes and $\gcd(n, \phi(n)) > 1$. The only other value n that appears in Table 1 and has this property is $n = 8$. An interesting question raised in this context is whether this covers all such values n, or if there are others.

We are also interested in those cyclic groups that admit only coset-preserving skew morphisms. Unlike general skew morphisms, coset-preserving skew morphisms are well understood for cyclic groups, and, in particular, we can list all coset-preserving skew morphisms of $\mathbb{Z}_n$ in polynomial time; see [6]. Thus, if for some n we can show that all skew morphisms of $\mathbb{Z}_n$ are coset-preserving, then we can find all skew morphisms of $\mathbb{Z}_n$ much faster than by using the algorithm explained in Section 5.2. In the following section we completely solve this problem by characterising all cyclic groups that admit only coset-preserving skew morphisms.

6 Cyclic groups that admit only coset-preserving skew morphisms

In this section we focus on cyclic groups admitting only coset-preserving skew morphisms. Our main theorem is the following:

Theorem 6.1. *All skew morphisms of $\mathbb{Z}_n$ are coset-preserving if and only if $n = 2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free.*

Note that Theorem 6.1 include all groups $\mathbb{Z}_n$ that does not admit any proper skew morphism, as in that case either $n = 4$, or $(n, \phi(n)) = 1$, which forces n to be square-free (for if some prime square p^2 divides n, then p is a common factor of n and $\phi(n)$). In what follows, we will say that the positive integer n is *resolvable* if it is expressible in the form $n = 2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free. The proof of Theorem 6.1 is split into two parts; in Section 6.1 we show that if n is not resolvable, then $\mathbb{Z}_n$ admits a non-coset-preserving skew morphism, and in Section 6.2 we show that if n is resolvable, then $\mathbb{Z}_n$ does not admit a non-coset-preserving skew morphism. Then in Section 6.3 we use Theorem 6.1 (and further facts about coset-preserving skew morphisms of cyclic groups) to enumerate all skew morphisms for many finite cyclic groups for which no such enumeration was available to date. Finally, in Section 6.4 we give an example that demonstrates how Theorem 6.1 can be applied to find a precise formula for the number of skew morphisms of $\mathbb{Z}_n$ in the case when n is resolvable and has a relatively small number of prime factors.

6.1 Cyclic groups admitting non-coset-preserving skew morphisms

Here we show that if the order of a cyclic group is divisible by 32 or by the square of an odd prime, then this group admits a skew morphism that does not preserve the cosets of its kernel. To do this, we will use some facts about skew morphisms of $\mathbb{Z}_n$ that give rise to a regular Cayley map. First, we have the following:

Proposition 6.2 ([18])**.** *A skew morphism φ of a finite group B gives rise to a regular Cayley map for B if and only if the set of elements of some orbit of $\langle\varphi\rangle$ is closed under taking inverses and generates B.*

We say that a skew morphism φ of a group B is *t-balanced* if its kernel has index 2 in B. The value t is given by $t = \pi(a)$, where a is any element of B not contained in $\ker\varphi$. In the special case when $t = \mathrm{ord}(\varphi) - 1$ we say that φ is anti-balanced. For further information on t-balanced skew morphisms we refer the reader to [11]. The following observation shows that every coset-preserving skew morphism of $\mathbb{Z}_n$ that gives rise to a regular Cayley map is either an automorphism of $\mathbb{Z}_n$, or a t-balanced skew morphism of $\mathbb{Z}_n$.

Lemma 6.3. *If φ is a coset-preserving skew morphism of $\mathbb{Z}_n$ that gives rise to a regular Cayley map, then the index of $\ker\varphi$ in $\mathbb{Z}_n$ is at most two. In particular, if n is odd, then $\ker\varphi = \mathbb{Z}_n$ and φ is an automorphism of $\mathbb{Z}_n$.*

Proof. Since φ gives rise to a regular Cayley map, by Proposition 6.2 there exists some orbit T of $\langle\varphi\rangle$ that is closed under taking inverses and generates $\mathbb{Z}_n$. Further, by [20, Corollary 3.3] we know that T contains some element t such that $\langle t\rangle = \mathbb{Z}_n$, and since $T = -T$, we also have $-t \in T$. Next, from the fact that φ is coset-preserving we deduce that t and $-t$ are both in the same coset of $\ker\varphi$ in $\mathbb{Z}_n$. It follows that $2t \in \ker\varphi$, and noting that t is a generator of $\mathbb{Z}_n$, we also have $\gcd(n, t) = 1$. Hence $2 \in \ker\varphi$, and the rest follows. □

Throughout the proof of the following proposition we repeatedly refer to the classification of regular Cayley maps for cyclic groups given in [13].

Proposition 6.4. *If a positive integer n is divisible by 32 or p^2 for some odd prime p, then $\mathbb{Z}_n$ admits a skew morphism that is not coset-preserving.*

Proof. First, assume that n is odd and divisible by p^2 for some odd prime p. Then there exists a regular Cayley map for $\mathbb{Z}_n$ with non-balanced representation (see [13, Section 8]), and hence there exists a proper skew morphism φ of $\mathbb{Z}_n$ that gives rise to this Cayley map. Since φ is proper and n is odd, by Lemma 6.3 we deduce that φ is not coset-preserving.

Next, if n is even and divisible by p^2 for some odd prime p, then we have $\mathbb{Z}_n = \mathbb{Z}_\ell \times \mathbb{Z}_{2^e}$ with ℓ odd. Since ℓ is clearly divisible by p^2, from the previous paragraph we know that $\mathbb{Z}_\ell$ admits a skew morphism φ that is not coset-preserving. By Lemma 2.11 there exists a skew morphism θ of $\mathbb{Z}_n$ such that $\theta\restriction_{\mathbb{Z}_\ell} = \varphi$ and $\ker\theta = \ker\varphi \times \mathbb{Z}_{2^e}$. Now it can be easily seen that since φ does not preserve the cosets of $\ker\varphi$ in $\mathbb{Z}_\ell$, the same is true for θ and cosets of $\ker\theta$ in $\mathbb{Z}_n$.

Finally, let n be even and divisible by 32, and consider the factorisation $\mathbb{Z}_n = \mathbb{Z}_{2^e} \times \mathbb{Z}_\ell$ with ℓ odd. Note that to show that $\mathbb{Z}_n$ admits a non-coset-preserving skew morphism, it is sufficient to prove this for $\mathbb{Z}_{2^e}$ (and the rest will follow by Lemma 2.11). Let $M(2m, r)$ be the regular Cayley map for $\mathbb{Z}_{2m}$ given by [13, Definition 3.6]. This map is defined for every unit r modulo m such that if b is the largest divisor of m that is relatively prime to $r - 1$, then either $b = 1$, or r is a root of -1 modulo b of multiplicative order $2k$ where k is relatively prime to m/b. Let $m = 2^{e-1}$, $r = 2^{e-3} + 1$, and $M = M(2m, r)$. Note that the largest divisor of m relatively prime to $r - 1$ is 1, and hence $b = 1$. Also note that r is not a root of -1 modulo m, and since $e \geq 5$ we have $r^2 \not\equiv 1 \pmod m$. It follows that M has no balanced, no t-balanced, and no anti-balanced representation; see [13, Section 8]. Since every automorphism of $\mathbb{Z}_{2^e}$ gives rise to a skew morphism with a balanced representation, and every skew morphism of $\mathbb{Z}_{2^e}$ with kernel of index 2 in $\mathbb{Z}_{2^e}$ gives rise to a skew morphism with either t-balanced or anti-balanced representation, we

deduce that a skew morphism φ of $\mathbb{Z}_{2^e}$ that gives rise to M has kernel of index greater than two in $\mathbb{Z}_{2^e}$. Hence by Lemma 6.3 we find that φ is not coset-preserving. □

6.2 Cyclic groups admitting only coset-preserving skew morphisms

Next we show that if the positive integer n is resolvable, then all skew morphisms of $\mathbb{Z}_n$ are coset-preserving. We start with the following technical lemma.

Lemma 6.5. *Let φ be a skew morphism of a cyclic group $\mathbb{Z}_n$, let N be any non-trivial subgroup of $\ker\varphi$, let φ_N^* be the skew morphism of $\mathbb{Z}_n/N$ induced by φ, and let L/N be the kernel of φ_N^*. Also let s be a prime factor of $n/|\ker\varphi|$, let k_s denote the largest power of s that divides $|(\ker\varphi)/N|$, and let $a = n/(s|\ker\varphi|)$ be an element of $\mathbb{Z}_n$. If sk_s divides $|L/N|$, then $a \notin \ker\varphi$ and $a \in L$.*

Proof. First, since $a|\ker\varphi| = n/s < n$, we have $a \notin \ker\varphi$. (Note that this part is true regardless of whether sk_s divides $|L/N|$.) Next, let $K = \ker\varphi$, and let m be an integer such that $|K/N| = mk_s$. (Observe that m and k_s are relatively prime.) Then since K/N is a subgroup of L/N, we know that mk_s divides $|L/N|$. But $|L/N|$ is also divisible by sk_s, and since $\gcd(m, k_s) = 1$, it follows that $|L/N|$ must be divisible by msk_s. Hence $|L|$ is divisible by $s|K|$, and therefore $a \in L$. □

We are now ready to prove the key part of the proof of Theorem 6.1.

Proposition 6.6. *Let $n = 2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free. Then every skew morphism of $\mathbb{Z}_n$ is coset-preserving.*

Proof. Suppose to the contrary that the assertion is not true, and let n be the smallest resolvable integer such that $\mathbb{Z}_n$ admits a skew morphism φ that is not coset-preserving. Also let $K = \ker\varphi$, let φ^* denote the skew morphism of $\mathbb{Z}_n/K$ induced by φ, and let $\overline{\varphi}$ be a quotient of φ. Since the only skew morphism of the trivial group is clearly coset-preserving, we have $n > 1$. Recalling that every skew morphism of a non-trivial group has a non-trivial kernel, it follows that $|K| \geq 2$. In particular, it follows that $|K|$ has at least one prime factor. We proceed by considering the two following cases:

Case (a): $|K|$ is a prime power

Let p be the largest prime divisor of n. Then by Corollary 3.3 we know that p divides $|K|$. If $p = 2$, then $n = 2$, 4, 8, or 16, in which case $\mathbb{Z}_n$ does not admit a skew morphism that is not coset-preserving; see [9]. Hence p is odd and $|K| = p$, and thus $|\mathbb{Z}_n/K| = n/p$. Then since p is the largest prime divisor of n, we know that p does not divide $|\mathbb{Z}_n/K|\phi(|\mathbb{Z}_n/K|)$, and it follows from Theorem 2.9 that p does not divide the order of φ^*. Further, by Lemma 3.1 we know that p divides $\mathrm{ord}(\varphi)$, and since $\mathrm{ord}(\varphi^*) = p_\varphi$, we deduce that p divides $\mathrm{ord}(\varphi^{p_\varphi})$. On the other hand, noting that φ^{p_φ} preserves the cosets of K in $\mathbb{Z}_n$, we have $\mathrm{ord}(\varphi^{p_\varphi}) \leq |K| = p$, and hence $\mathrm{ord}(\varphi^{p_\varphi}) = p$. Therefore $\mathrm{ord}(\varphi) = pp_\varphi$, and then by Proposition 5.1(b) we have $|\ker\overline{\varphi}| = p$. But p does not divide (n/p), which (by Lemma 4.1(a)) is the order of $\overline{\varphi}$, and so by Lemma 3.1 we find that $\overline{\varphi}$ is a group automorphism. Hence by Lemma 4.2 we deduce that φ is coset-preserving, contradiction.

Case (b): $|K|$ has at least two distinct prime factors

Let $k = |K|$, and let d denote the integer satisfying $n = kd$. (Note that the elements of K are exactly the multiples of d modulo n.) Also let $d = r_1 \dots r_\ell$ be a factorisation such that each factor is either an odd prime or the maximum possible power of two. Since φ does not preserve the cosets of K in $\mathbb{Z}_n$, we know that $\varphi(1) \not\equiv 1 \pmod{d}$. Hence, noting that all factors r_i for $i \in \{1, \dots, \ell\}$ are pairwise relatively prime, it follows from the Chinese Remainder Theorem that there exists $r \in \{r_1, \dots, r_\ell\}$ such that $\varphi(1) \not\equiv 1 \pmod{r}$. We will show that this cannot happen.

First, assume that r is odd. It follows that r is a prime, and also that n is not divisible by r^2. (And so, in particular, r does not divide $|K|$.) Let p be any prime factor of $|K|$, let N be the unique subgroup of K of order p, and let φ_N^* be the skew morphism of $\mathbb{Z}_n/N$ induced by φ. Also let L/N be the kernel of φ_N^*, and suppose that $|L/N|$ is not divisible by r. Since the order of the cyclic group $\mathbb{Z}_n/N$ is clearly resolvable, by the assumption of minimality of n we know that φ_N^* is coset-preserving. Then since r divides $\mathbb{Z}_n/N$ but not L/N, we have $\varphi(1) \equiv \varphi_N^*(1) \equiv 1 \pmod{r}$. But this contradicts the fact that $\varphi(1) \not\equiv 1 \pmod{r}$, and hence we deduce that r divides $|L/N|$. Now, since r does not divide $|K|$, it follows that r does not divide $|K/N|$, and thus we may use Lemma 6.5 (with $s = r$ and $k_s = 1$). Hence we deduce that the element $a = d/r$ of $\mathbb{Z}_n$ is not contained in K, but also $a \in L$, and by Lemma 2.6 it follows that $p\pi(a) \equiv p \pmod{\operatorname{ord}(\varphi)}$. Since p was an arbitrary prime factor of $|K|$, the same is true also for some other prime factor q of $|K|$. (Here we use the assumption that the order of K has at least two distinct prime factors.) Hence we have

$$\begin{aligned} p\pi(a) &\equiv p \pmod{\operatorname{ord}(\varphi)}, \\ q\pi(a) &\equiv q \pmod{\operatorname{ord}(\varphi)}, \end{aligned}$$

for a pair of distinct primes p and q. Then since $\gcd(p, q) = 1$, we deduce that $\pi(a) \equiv 1 \pmod{\operatorname{ord}(\varphi)}$, and consequently $a \in K$, contradiction.

Next, assume that r is even. Again let p denote a prime factor of $|K|$, and define N, φ_N^*, and L/N same as in the case when r was odd. Also let k_2 denote the largest power of 2 that divides $|K/N|$, and suppose that $|L/N|$ is not divisible by $2k_2$. Noting that K/N is a subgroup of L/N, it follows that the largest power of 2 that divides $|L/N|$ must be k_2. Then since φ_N^* must be coset-preserving (due to the minimality of n) and the largest power of 2 that divides $|\mathbb{Z}_n/N|$ is equal to rk_2, we deduce that $\varphi(1) \equiv \varphi_N^*(1) \equiv 1 \pmod{r}$, contradicting the fact that $\varphi(1) \not\equiv 1 \pmod{r}$. Hence it follows that $2k_2$ divides $|L/N|$, and Lemma 6.5 (in this case we take $s = 2$ and $k_s = k_2$) implies that the element $a = d/2$ of $\mathbb{Z}_n$ satisfies $a \notin K$ and $a \in L$. Using the same argument as for r odd this again leads to a contradiction. □

Theorem 6.1 now follows directly from Propositions 6.4 and 6.6.

6.3 Enumeration

In [6] it was shown that each coset-preserving skew morphism φ of $\mathbb{Z}_n$ is uniquely determined by the following four parameters: the smallest non-zero element d of $\ker\varphi$; the element h of $\mathbb{Z}_n$ such that $\varphi(1) = 1+h$; the smallest positive integer s such that $\varphi(d) = sd$; and the positive integer $e = \pi(1)$. (Note that s always exists since $d \in \ker\varphi$ and φ restricts to an automorphism of $\ker\varphi$.) Using various properties of coset-preserving skew morphisms it can be checked that if φ is non-trivial, then the parameters d, h, s and e must satisfy the following properties (see [6, Section 4] for details):

(i) all four parameters are positive integers;

(ii) d is a proper divisor of n;

(iii) $s < n/d$ and $\gcd(s, n/d) = 1$;

(iv) h is a multiple of d strictly smaller than n;

(v) if r is the smallest positive integer such that $h\sum_{i=0}^{r-1} s^i \equiv 0 \pmod{n}$, then e is a (multiplicative) unit modulo r of order d and $e < r$;

(vi) $sd \equiv \sum_{j=0}^{d-1}(1 + h\sum_{i=0}^{\ell_j} s^i) \pmod{n}$, where $\ell_j = e^j - 1 \bmod r$; and

(vii) $s^{e-1} \equiv 1 \pmod{n/d}$.

On the other hand, for each set of parameters (d, h, s, e) satisfying all of the above properties there exists a unique non-trivial coset-preserving skew morphism of $\mathbb{Z}_n$ (which can be constructed in a straightforward way) with this parameter set; see [6, Section 5]. This gives a one-to-one correspondence between non-trivial coset-preserving skew morphisms of $\mathbb{Z}_n$ and the sets of parameters (d, h, s, e), and this correspondence can be used to find all coset-preserving skew morphisms of a given cyclic group in a polynomial time (in the cardinality of the group). Hence, by Theorem 6.1 we can quickly find all skew morphisms of $\mathbb{Z}_n$, where n is resolvable. Using the above observations, we developed an algorithm that can enumerate all skew morphisms for any given cyclic group of any resolvable order. A C++ implementation of this algorithm succeeded in enumerating all skew morphisms for cyclic groups of resolvable orders smaller than 10000 within a second, even without parallelisation. In comparison, the best available method to date for finding all skew morphisms for cyclic groups of general order (described in Section 5.2) is computationally feasible only up to order 161. In our enumeration, which is available at [1], we provide the total number of skew morphisms of $\mathbb{Z}_n$, and also the total number of automorphisms and their proportion among all skew morphisms.

6.4 Skew morphisms of $\mathbb{Z}_{4p}$

Although coset-preserving skew morphisms can be generated efficiently, there is no known explicit formula for the number of coset-preserving skew morphisms of $\mathbb{Z}_n$ for general n. Such a formula would be useful, and in the case when n is resolvable it would give the number of all skew morphisms of $\mathbb{Z}_n$. Resolvable integers n with the simplest structure (with respect to their prime factorisation) are primes, in which case all skew morphisms of $\mathbb{Z}_n$ are automorphisms of $\mathbb{Z}_n$. The situation is also completely understood in the case when n is a product of two distinct primes p and q, in which case the number of skew morphisms of $\mathbb{Z}_{pq}$ is $(p-1)(q-1)$ if $\gcd(p, q-1) = \gcd(p-1, q) = 1$, and $2(p-1)(q-1)$ otherwise; see [20] for example. Here we go one step further and find a formula for the number of skew morphisms of $\mathbb{Z}_{4p}$, where p is an odd prime. We will use the following fact:

Proposition 6.7. *Let p be an odd prime. If φ is a proper skew morphism of $\mathbb{Z}_{4p}$, then the action of φ on its kernel is trivial.*

Proof. Let π and K denote the power function and the kernel of φ, and let φ^* be the skew morphism of $\mathbb{Z}_n/K$ induced by φ. Note that by Theorem 6.1 we know that φ is coset-preserving, and so φ^* must be trivial. Further, by Corollary 3.3 we know that p divides $|K|$, and since φ is proper it follows that the order of K is either p or $2p$. We proceed by considering these two cases. In each case, we let T be the orbit of $\langle\varphi\rangle$ that contains 1. Note that by Proposition 2.7 we have $|T| = \mathrm{ord}(\varphi)$.

Case (a): $|K| = p$

Since φ is coset-preserving, we know that the cosets of K in $\mathbb{Z}_n$ are preserved set-wise by φ. Note that only one element of the coset $1 + K$ does not generate $\mathbb{Z}_n$ (either p or $3p$, depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$), and since by Lemma 2.12 no elements outside of K are fixed by φ, it follows that each orbit of $\langle\varphi\rangle$ on $1 + K$ generates $\mathbb{Z}_n$. Hence by Proposition 2.7 we know that all of these orbits have size $\mathrm{ord}(\varphi)$, and since $|1 + K| = |K| = p$, we see that $\mathrm{ord}(\varphi) = p$. Since φ restricts to an automorphism of K, and $\mathrm{ord}(\varphi) = |K| = p$, we deduce that the action of φ on K is trivial.

Case (b): $|K| = 2p$

In this case, since φ is proper, by Theorem 2.9 we have $\gcd(\mathrm{ord}(\varphi), 4p) > 1$. If the order of φ is odd, then we have $\mathrm{ord}(\varphi) = p$ or $\mathrm{ord}(\varphi) = 3p$, but the latter case can be easily excluded since φ must preserve both cosets of K in $\mathbb{Z}_n$ of size $2p$.

Next we deal with the case when $\mathrm{ord}(\varphi)$ is even. Note that by Lemma 4.1(a) we have $\pi(1) = \overline{\varphi}(1)$, and since $\overline{\varphi}$ is an automorphism of the cyclic group $\mathbb{Z}_{\mathrm{ord}(\varphi)}$ of even order, we deduce that $\pi(1)$ is odd. We will use this observation to show that both p and $3p$ are contained in some orbits of $\langle\varphi\rangle$ that generate $\mathbb{Z}_n$. Suppose to the contrary that this is not true. Since every element of $1 + K$ other than p and $3p$ generates $\mathbb{Z}_n$ and no element of $1 + K$ is fixed by φ, we must have $\varphi(p) = 3p$ and $\varphi(3p) = p$. Then since $\pi(1)$ is odd, we have $\varphi^{\pi(1)}(p) = 3p$, and therefore $\varphi(1+p) = \varphi(1) + \varphi^{\pi(1)}(p) = \varphi(1) + 3p$. On the other hand, we have $\varphi(p + 1) = \varphi(p) + \varphi^{\pi(p)}(1) = 3p + \varphi^{\pi(p)}(1)$. But then $\varphi(1) = \varphi^{\pi(p)}(1)$, and since $|T| = \mathrm{ord}(\varphi)$ we find that $\pi(p) = 1$. This forces $p \in K$, contradicting the fact that the order of K is $2p$. Hence we deduce that all orbits of $\langle\varphi\rangle$ on $1 + K$ generate $\mathbb{Z}_n$. In particular, $\mathrm{ord}(\varphi)$ divides $2p$, and it follows that $\mathrm{ord}(\varphi) = 2p$.

We have shown that if $|K| = 2p$, then $\mathrm{ord}(\varphi)$ is equal to p or $2p$. Hence by order considerations it can be easily seen that φ acts on K either trivially, or by the inversion. To exclude the latter, first note that 1 and $\varphi(1)$ are in the same coset of K in $\mathbb{Z}_{4p}$, and hence $\varphi(1) - 1 \in K$. If we let $h = \varphi(1) - 1$, then we have $\varphi^2(1) = \varphi(h + 1) = \varphi(h) + \varphi(1) = -h + h + 1 = 1$, but then by Proposition 2.7 we have $\mathrm{ord}(\varphi) = 2$, which is impossible. Hence we again conclude that the action of φ on K is trivial. □

Using Theorem 6.1 and Proposition 6.7 we can now easily enumerate all proper skew morphisms of $\mathbb{Z}_{4p}$.

Theorem 6.8. *If p is an odd prime, then the number of skew morphisms of $\mathbb{Z}_{4p}$ is*

$$\begin{cases} 6p - 6 & \text{if } p \equiv 1 \pmod 4 \\ 4p - 4 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Throughout this proof we refer to the properties (i) to (vii) and the parameters d, h, s and e of coset-preserving skew morphisms for cyclic groups explained in Section 6.3.

We know that $|\mathrm{Aut}(\mathbb{Z}_{4p})| = 2p-2$, so we proceed by counting proper skew morphisms of $\mathbb{Z}_{4p}$. Let φ be a proper skew morphism of $\mathbb{Z}_{4p}$, and recall that by Theorem 6.1 it is coset-preserving. Let d, h, s and e be the four defining parameters of φ, and note that by Proposition 6.7 we have $s = 1$. Since p is the largest prime divisor of $4p$, by Corollary 3.3 we know that p divides $|\ker\varphi|$, and it follows that $d = 2$ or $d = 4$. (The case $d = 1$ can be excluded as φ is proper.)

First let $d = 2$, and let h be any positive multiple of 2 strictly smaller than $4p$. If 4 divides h, then by (v) we find that $r = p$ and $e = p-1$. Since $s = 1$, both (iii) and (vii) are trivially true, and (vi) holds as $(1+h)+(1+h(p-1)) \equiv 2+hp \equiv 2 \pmod{4p}$. If 4 does not divide h and $h \neq 2p$, then by (v) we have $r = 2p$ and $e = 2p-1$. Again both (iii) and (vii) hold trivially, and (vi) is also true since $(1+h)+(1+h(2p-1) \equiv 2+2hp \equiv 2 \pmod{4p}$. If $h = 2p$, then it can be easily verified that $\mathrm{ord}(\varphi) = r = 2$, contradicting the fact that φ is proper. Since for all but one choice of h we obtain exactly one coset-preserving skew morphism, it follows that in this case we have exactly $2p-2$ skew morphism of $\mathbb{Z}_{4p}$.

Next let $d = 4$, and let h be any positive multiple of 4 strictly smaller than $4p$. Then by (v) we deduce that $r = p$, and e must be a fourth root of unity modulo p. It follows that necessarily $p \equiv 1 \pmod 4$, in which case there are two possible candidates for e. Note that for either candidate we have $e^2 \equiv -1 \pmod p$ and $e^3 \equiv -e \pmod p$. Again (iii) and (vii) hold trivially, and (vi) holds as well since $(1+h)+(1+he)+(1+h(p-1))+(1+h(p-e)) \equiv 4+2hp \equiv 4 \pmod{4p}$. Hence, if $p \equiv 1 \pmod 4$, then every choice of h gives two coset-preserving skew morphisms (one for each choice of e), which gives a total of $2p-2$ skew morphisms of $\mathbb{Z}_{4p}$. □

ORCID iDs

Martin Bachratý https://orcid.org/0000-0002-4300-7507

References

[1] M. Bachratý, Enumeration of skew morphisms of cyclic groups admitting only coset-preserving skew morphisms up to order 100000, https://drive.google.com/file/d/1HpumLCS-hJW-LCdWbYsUJ-PCj3pVes4g.

[2] M. Bachratý, List of skew-morphisms of cyclic groups up to order 161, https://drive.google.com/file/d/1rpFTIa961JkxHY5yuyN2gm2fUovQSuar.

[3] M. Bachratý, *Skew morphisms and skew product groups of finite groups*, Ph.D. thesis, University of Auckland, 2020, https://researchspace.auckland.ac.nz/bitstream/handle/2292/53164/Bachraty-2020-thesis.pdf.

[4] M. Bachratý, M. Conder and G. Verret, Skew product groups for monolithic groups, *Algebr. Comb.* **5** (2022), 785–802, doi:10.5802/alco.206, https://doi.org/10.5802/alco.206.

[5] M. Bachratý and R. Jajcay, Powers of skew-morphisms, *Symmetries in Graphs, Maps, and Polytopes* (2016), 1–25, doi:10.1007/978-3-319-30451-9_1, https://doi.org/10.1007/978-3-319-30451-9_1.

[6] M. Bachratý and R. Jajcay, Classification of coset-preserving skew-morphisms of finite cyclic groups, *Australas. J. Comb.* **67** (2017), 259–280, https://ajc.maths.uq.edu.au/pdf/67/ajc_v67_p259.pdf.

[7] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265, doi:10.1006/jsco.1996.0125, https://doi.org/10.1006/jsco.1996.0125.

[8] J. Chen, S. Du and C. H. Li, Skew-morphisms of nonabelian characteristically simple groups, *J. Comb. Theory Ser. A* **185** (2022), 105539, doi:10.1016/j.jcta.2021.105539, https://doi.org/10.1016/j.jcta.2021.105539.

[9] M. Conder, List of skew-morphisms for small cyclic groups, https://www.math.auckland.ac.nz/~conder/SkewMorphisms-SmallCyclicGroups-60.txt.

[10] M. Conder, R. Jajcay and T. W. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebr. Comb.* **25** (2007), 343–364, doi:10.1007/s10801-006-0037-0, https://doi.org/10.1007/s10801-006-0037-0.

[11] M. Conder, R. Jajcay and T. W. Tucker, Regular t-balanced Cayley maps, *J. Comb. Theory Ser. B* **97** (2007), 453–473, doi:10.1016/j.jctb.2006.07.008, https://doi.org/10.1016/j.jctb.2006.07.008.

[12] M. Conder, R. Jajcay and T. W. Tucker, Cyclic complements and skew morphisms of groups, *J. Algebra* **453** (2016), 68–100, doi:10.1016/j.jalgebra.2015.12.024, https://doi.org/10.1016/j.jalgebra.2015.12.024.

[13] M. Conder and T. W. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.* **336** (2014), 3585–3609, doi:10.1090/s0002-9947-2014-05933-3, https://doi.org/10.1090/s0002-9947-2014-05933-3.

[14] S. Du, K. Hu. and A. Lucchini, Skew-morphisms of cyclic 2-groups, *J. Group Theory* **22** (2019), 617–635, doi:10.1515/jgth-2019-2046, https://doi.org/10.1515/jgth-2019-2046.

[15] Y.-Q. Feng, K. Hu, R. Nedela, M. Škoviera and N.-E. Wang, Complete regular dessins and skew-morphisms of cyclic groups, *Ars Math. Contemp.* **18** (2020), 289–307, doi:10.26493/1855-3974.1748.ebd, https://doi.org/10.26493/1855-3974.1748.ebd.

[16] K. Hu, Y. S. Kwon and J.-Y. Zhang, Classification of skew morphisms of cyclic groups which are square roots of automorphisms, *Ars Math. Contemp.* **21** (2021), 2–01, 23 pp., doi:10.26493/1855-3974.2129.ac1, https://doi.org/10.26493/1855-3974.2129.ac1.

[17] K. Hu, R. Nedela, N.-E. Wang and K. Yuan, Reciprocal skew morphisms of cyclic groups, *Acta Math. Univ. Comenian.* **88** (2019), 305–318, http://www.iam.fmph.uniba.sk/amuc/ojs/index.php/amuc/article/view/1006.

[18] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179, doi:10.1016/S0012-365X(01)00081-4, https://doi.org/10.1016/S0012-365X(01)00081-4.

[19] I. Kovács and Y. S. Kwon, Regular Cayley maps for dihedral groups, *J. Comb. Theory Ser. B* **148** (2021), 84–124, doi:10.1016/j.jctb.2020.12.002, https://doi.org/10.1016/j.jctb.2020.12.002.

[20] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars Math. Contemp.* **4** (2011), 329–349, doi:10.26493/1855-3974.157.fc1, https://doi.org/10.26493/1855-3974.157.fc1.

[21] I. Kovács and R. Nedela, Skew-morphisms of cyclic p-groups, *J. Group Theory* **20** (2017), 1135–1154, doi:10.1515/jgth-2017-0015, https://doi.org/10.1515/jgth-2017-0015.

[22] A. Lucchini, On the order of transitive permutation groups with cyclic point-stabilizer, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **9** (1998), 241–243.

[23] N.-E. Wang, K. Hu, K. Yuan and J.-Y. Zhang, Smooth skew morphisms of the dihedral groups, *Ars Math. Contemp.* **16** (2019), 527–547, doi:10.26493/1855-3974.1475.3d3, https://doi.org/10.26493/1855-3974.1475.3d3.

[24] J.-Y. Zhang and S. Du, On the skew-morphisms of dihedral groups, *J. Group Theory* **19** (2016), 993–1016, doi:10.1515/jgth-2016-0027, https://doi.org/10.1515/jgth-2016-0027.