CYCLIC COMPLEMENTS AND SKEW MORPHISMS OF GROUPS

MARSTON D.E. CONDER, ROBERT JAJCAY, AND THOMAS W. TUCKER

Abstract. A skew morphism of a group is a generalisation of an automorphism, which arose from the study of regular Cayley maps, but occurs more generally in the context of any group expressible as a product AB of subgroups A and B with B cyclic and $A \cap B = \{1\}$. Specifically, a skew morphism of a group A is a bijection $\varphi : A \to A$ fixing the identity element of A and having the property that $\varphi(xy) = \varphi(x)\varphi^{\pi(x)}(y)$ for all $x, y \in A$, where $\pi(x)$ depends only on x. The kernel of φ is the subgroup of all $x \in A$ for which $\pi(x) = 1$.

In this paper, we present a number of previously unknown properties of skew morphisms, one being that if A is any finite group, then the order of every skew morphism of A is less than $|A|$, and another being that the kernel of every skew morphism of a non-trivial finite group is non-trivial.

We also prove a number of theorems about skew morphisms of finite abelian groups, some of which either simplify or extend recent theorems of Kovács and Nedela (2011). For example, we determine all skew morphisms of the finite abelian groups whose order is prime, or the square of a prime, or the product of two distinct primes. In addition, we completely determine the finite abelian groups for which every skew morphism is an automorphism; these are precisely the cyclic groups C_n with $n = 4$ or $\gcd(n, \phi(n)) = 1$, and the elementary abelian 2-groups $C_2 \times \cdots \times C_2$.

1. Introduction

In the mid-1900s a number of papers were written about groups expressible as the product of subgroups of various kinds. Perhaps the most famous is a paper by Itô [8], who proved that if $G = AB$ where the subgroups A and B are abelian, then G is metabelian (that is, the commutator subgroup of G is abelian). Also Huppert proved that if $G = AB$ where A is dihedral and B is abelian or dihedral or a p-group, then G is soluble [6]. Other contributions to this topic were made by Douglas, Ore, Rédei and Szép, for example.

Decades later, the concept of a skew morphism of a group was introduced, in the context of regular Cayley maps, which are embeddings of graphs on surfaces that admit a group of automorphisms acting regularly on the vertices of the embedded graph [11]. Skew morphisms generalise the notion of an automorphism of a group, and have properties that make them interesting in their own right.

In this paper we exploit a connection between these two topics, and develop the theory of both of them further. Our initial motivation was to prove that the 'kernel' of a non-trivial skew morphism is always non-trivial, but this work grew into something larger, involving a systematic study of skew morphisms and their properties, both in general and

for some specific kinds of groups, and the results have implications for the structure of groups expressible as a product AB of complementary subgroups A and B where B is cyclic. Every such product gives rise to a skew morphism of A, and vice versa, and the language and theory of skew morphisms make it possible to say much more about such group factorisations than appears to have been possible in the past.

Given a group A, a permutation $\varphi\colon A \to A$ of the elements of A that fixes the identity of A is said to be a *skew morphism* of A with associated *power function* $\pi\colon A \to \mathbb{Z}$ if

$$\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b) \quad \text{for all } a, b \in A.$$

Note that φ is an automorphism of A if the power function π takes constant value 1. More generally, the *kernel* of φ is defined as the subset $\{a \in A \mid \pi(a) = 1\}$ of A, and denoted by $\ker\varphi$. In the case when A is finite, every skew morphism φ is necessarily of finite order, say m, and then the power function π may be regarded as a function from A to $\mathbb{Z}_m$. It is easy to show that $K = \ker\varphi$ is a subgroup of A, and the values of π on two elements of A coincide if and only if they lie in the same right coset of K, but until now, not much more could be said about the order or the kernel of skew morphisms in general.

Next, let G be a group that is expressible as a product AY of two subgroups A and Y with $A \cap Y = \{1\}$. We may call such a group G a *complementary product* of A and Y. In the case where Y is cyclic, let y be any generator of Y. Then left multiplication of elements of A by y gives rise to a skew morphism φ of A, given by $ya = \varphi(a)y^{\pi(a)}$ for all $a \in A$. Details are given in the next section, but here we note that the fundamental property $ya = \varphi(a)y^{\pi(a)}$ that provides the connection between complementary products and skew morphisms was observed as early as 1938, by Ore [16, p. 805].

The importance of skew morphisms in the study of regular maps is now well-established, but relatively little has been written on the general theory of skew morphisms. In this paper, we exploit the connection with complementary products and take things much further, proving a number of new theorems — some about skew morphisms of finite groups in general, and some for the special cases of abelian and dihedral groups. For example, we generalise a theorem of Horoševskiĭ [7] which says the order of every automorphism of a finite group of order $n > 1$ is less than n, by proving the same thing for skew morphisms in Theorem 4.2. Then as a corollary, we prove that the kernel of every skew morphism of a non-trivial finite group is non-trivial, in Theorem 4.3. We recognised the latter as a possibility after computing the skew morphisms of small finite groups (with the help of the Magma system [1]), and this paper grew out of our attempts to prove it.

This paper also builds on another recent one by Kovács and Nedela [13], in which the theory of Schur rings was used to prove various theorems about skew morphisms of cyclic groups. We generalise some of the theorems of [13] and simplify the proofs of others, by taking a different approach, and making use of our theorem about non-trivial kernel. In particular, we prove a number of new theorems about skew morphisms of abelian groups. A key to our approach comes from the fact (which we proved in [3]) that the kernel K of every skew morphism φ of a finite abelian group A is preserved by φ. (That does not happen

for other finite groups.) In the abelian case, if a subgroup N of $K = \ker\varphi$ is preserved by φ, then φ induces a skew morphism on A/N and restricts to an automorphism of N. These observations prove very useful, and culminate in Theorem 7.5, where we completely determine all finite abelian groups for which every skew morphism is an automorphism.

We begin by giving some further background on skew morphisms in Section 2, including their relationship with regular Cayley maps. In Section 3 we explain the connection with complementary subgroup factorisations $G = AY$ (including the special case where Y has trivial core in G, which we call a 'skew product'), and also make some observations about powers of a skew morphism. We prove our main general theorems about the order and kernel of a skew morphism in Section 4. Then Sections 5 to 8 are devoted to skew morphisms of abelian groups, cyclic groups, and dihedral groups; in particular, in Section 7 we consider the question of which (abelian) groups admit skew morphisms that are not automorphisms. Finally, in Section 9 we make some observations about the group generated by all skew morphisms of a given group A.

2. Further background on skew morphisms

Although introduced for finite groups, the concept of skew morphisms can be easily extended to the case of infinite groups, and so some of the theory we present can be stated in the context of both finite and infinite groups. Most of the properties in which we are interested, however, depend on the order of the skew morphisms (or the order of the groups) being finite, and hence we state the finiteness of the order of the groups involved whenever that becomes an issue.

Even though the definition of a skew morphism seems to be quite a departure from that of a group automorphism, there is still a strong interaction with group multiplication, and so skew morphisms share many of the algebraic properties of group automorphisms. For example, the following gives properties of skew morphisms that are well known to be true, and were proved in [11]:

Lemma 2.1. *Let A be a group, and let φ be a skew morphism of A with associated power function π. Then*:

(a) $\varphi^j(ab) = \varphi^j(a)\varphi^{\sigma(j,a)}(b)$ *where* $\sigma(j,a) = \sum_{0\le i<j} \pi(\varphi^i(a))$, *for all* $a, b \in A$ *and all* $j \in \mathbb{N}$,

(b) *the kernel* $K = \ker\varphi$ *is a subgroup of* A,

(c) $\pi(a) = \pi(b)$ *if and only if* a *and* b *lie in the same right coset of* K *in* A,

(d) *the set* $\mathrm{Fix}(\varphi) = \{a \in A \mid \varphi(a) = a\}$ *is a subgroup of* A,

(e) *the intersection* $\ker\varphi \cap \mathrm{Fix}(\varphi)$ *is a normal subgroup of* A, *and*

(f) *if* A *is finite, and* φ *has order* m, *then*

$$\pi(ab) \equiv \sum_{0\le i<\pi(a)} \pi(\varphi^i(b)) \equiv \sigma(\pi(a), b) \bmod m, \quad \text{for all } a, b \in A.$$

Here we note that if the skew morphism φ has finite order m, then m is the least common multiple (LCM) of the lengths of the cycles of φ on the group A. We also note that the cycles of a skew morphism φ are often referred to as its *orbits* instead.

Next, we give the following general fact, which will be useful later:

Proposition 2.2. *Let φ be any skew morphism of a group A, and let N be a subgroup of $K = \ker\varphi$ that is normal in A and is preserved by φ (so $\varphi(N) = N$). Then the mapping $\varphi^*\colon A/N \to A/N$ given by $\varphi^*(Nx) = N\varphi(x)$ is a well-defined skew morphism of A/N.*

Proof. First, if $a \in N$ and $x \in A$ then $\varphi(ax) = \varphi(a)\varphi(x) \in N\varphi(x)$, since φ preserves N, and so the mapping φ^* is well-defined. Next, let π be the power function of φ. Then we have $\varphi^*((Nx)(Ny)) = \varphi^*(Nxy) = N\varphi(xy) = N\varphi(x)\varphi^{\pi(x)}(y) = N\varphi(x)N\varphi^{\pi(x)}(y) = \varphi^*(Nx)(\varphi^*)^{\pi(x)}(Ny)$ for all $x, y \in A$, and it follows that φ^* is a skew morphism of A/N. □

Finally in this section, we explain some of the connections between skew morphisms and regular Cayley maps.

A *map* is a 2-cell embedding of a connected graph or multigraph Γ on some closed surface, where '2-cell embedding' means that when Γ is removed from surface, it breaks it up into regions which are simply-connected (and are called the *faces* of the map). Each edge of Γ is associated with two opposite *arcs* or *darts* of the corresponding map M, which are the incident vertex-edge pairs (v, e). An *automorphism* of a map M is any permutation of its darts that preserves incidence with the vertices and faces. By connectedness, every automorphism of M is uniquely determined by its effect on any incident vertex-edge-face triple (v, e, f), and so the number of automorphisms of M is bounded above by the number of such triples (which are sometimes called 'flags'). A general map M is called *regular* if this upper bound is attained, however, in the context of orientable maps (embeddings into orientable surfaces), an *orientable map is called regular* if the group of all orientation-preserving automorphisms of M is transitive on the darts of M.

If the underlying graph Γ of the regular map M is simple, and the automorphism group of M contains a subgroup A that acts regularly (or in other words, sharply-transitively) on the vertices of Γ, then Γ is a Cayley graph for A, and M is a regular Cayley map for A. In that case, the subgroup A is complementary to the stabiliser G_v in the automorphism group $G = \mathrm{Aut}\, M$ of any vertex v. In the orientable situation, we can take G as the group of all orientation-preserving automorphisms of M, and then G has a complementary factorisation $G = AG_v$, with G_v cyclic (generated by a 'rotation' of the darts of Γ emanating from v), and left multiplication of A by a generator of G_v gives a skew morphism of A.

Another way to define regular Cayley maps is to start with the more general notion of a *Cayley map.*

Let A be a group, let X be a generating set for A such that X is closed under inverses and does not contain the identity element of A, and let ρ be a cyclic permutation of the elements of X. Then the Cayley map $M = \mathrm{CM}(A, X, \rho)$ is a 2-cell embedding of the Cayley graph $\mathrm{Cay}(A, X)$ on an orientable surface, with the property that the local counter-clockwise

orientation of the set $\{(a, ax) : x \in X\}$ of the darts emanating from every vertex a agree with the cyclic order induced on X by ρ, namely $((a, ax), (a, ax^\rho), (a, ax^{\rho^2}), \ldots, (a, ax^{\rho^{-1}}))$.

If $M = \mathrm{CM}(A, X, \rho)$ is regular (as an oriented map), then it is a *regular Cayley map* for A. Moreover, in that case X is an orbit of the skew morphism φ described above, and ρ is the cyclic order induced on X by φ; see [17]. Conversely, if φ is a skew morphism of A, and X is an orbit of φ that is closed under inverses and generates A, then a regular Cayley map $M = \mathrm{CM}(A, X, \rho)$ can be constructed for A in which ρ is the restriction of φ to X.

For more information on regular Cayley maps, see [2, 4, 11] and other references given there.

It has been recently observed (in [10]) that every skew morphism φ preserves the subgroups generated by its orbits. If an orbit X is closed under inverses, then X gives rise to a regular Cayley map for the subgroup generated by X. On the other hand, if the orbit X is not closed under inverses, then X is paired with another orbit X^* consisting entirely of the inverses of the elements of X, and then their union $X \cup X^*$ gives rise to a Cayley map M for the subgroup generated by $X \cup X^*$, admitting an automorphism group that acts transitively on vertices and edges of M but has exactly two orbits of equal size on the darts. Such a Cayley map is called *half-regular* in [10].

It is important to emphasise here that all of the new theorems in this paper concern skew morphisms in general, and not just those associated with regular Cayley maps. The class of all skew morphisms is much larger than that of 'map' skew morphisms, and even contains automorphisms that are not associated with maps. Also there are some facts that are easy to prove for 'map' skew morphisms, or only for automorphisms, but are much more challenging for arbitrary skew morphisms.

3. Skew product groups

In this section we describe the relationship between skew morphisms of finite groups, and finite groups that have a factorisation of the form AY where A and Y are subgroups such that Y is cyclic and $A \cap Y = \{1\}$, and then give some applications. The initial part of our approach (leading up to Proposition 3.1) is similar to a small piece of the approach taken by Kovács and Nedela in [13].

First let G be any finite group that has such a complementary subgroup factorisation (with Y cyclic). Note that $YA = AY$ $(= G)$, since AY is a subgroup of G. Also let y be a generator of Y. Then for any $a \in A$, we know that $ya \in YA = AY$, so $ya = a'y^j$ for some $a' \in A$ and some $j \in \mathbb{Z}$, both of which are uniquely determined by a. We can now define functions $\varphi\colon A \to A$ and $\pi\colon A \to \mathbb{Z}$ by setting

$$\varphi(a) = a' \quad \text{and} \quad \pi(a) = j \quad \text{whenever } ya = a'y^j \quad \text{where } a' \in A \text{ and } j \in \mathbb{Z}.$$

Under this definition, $ya = \varphi(a)y^{\pi(a)}$ for all $a \in A$, and it follows that φ is a bijection (for if $\varphi(a) = \varphi(b)$ then $yay^{-\pi(a)} = \varphi(a) = \varphi(b) = yby^{-\pi(b)}$, so $a^{-1}b = (ya)^{-1}yb = y^{\pi(b)-\pi(a)} \in Y$

and therefore $a^{-1}b = 1$). Also it is easy to see from the identity $ya = \varphi(a)y^{\pi(a)}$ that

$$y(ab) = (ya)b = \varphi(a)y^{\pi(a)}b = \varphi(a)\varphi^{\pi(a)}(b)y^j$$

for some j, which implies that $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$, so that φ is a skew morphism of A.

Conversely, let φ be any skew morphism of a finite group A, with power function π. Then φ is a bijection, and as such, generates a cyclic subgroup Y of $\mathrm{Sym}(A)$. We may consider A as a group of permutations of A, in its action by left multiplication. On the other hand, for clarity we will let y be the generator of Y induced by φ. Note that A is a regular subgroup of $\mathrm{Sym}(A)$, while Y fixes the identity element, and so $A \cap Y = \{1\}$ in $\mathrm{Sym}(A)$. Hence in particular, $|AY| = |A||Y| = |YA|$. Now from the definition of skew morphism, for each $a \in A$ we have $ya = \varphi(a)y^{\pi(a)} \in AY$, and it follows that $YA \subseteq AY$ in $\mathrm{Sym}(A)$. Then by finiteness (and the fact that $|AY| = |YA|$), this gives $AY = YA$, and so $G = AY$ is a subgroup of $\mathrm{Sym}(A)$, and hence a group, with a complementary subgroup factorisation of the type considered earlier.

Note also that in both cases above, the element a lies in $K = \ker\varphi$ if and only if $ya = \varphi(a)y$, or equivalently, $yay^{-1} \in A$. Hence K is the largest subgroup B of A for which $yBy^{-1} \subseteq A$, namely the intersection $A \cap y^{-1}Ay$. Thus we obtain the following:

Proposition 3.1. *Let A be any finite group. Then*
(a) *if G is any finite group with a complementary subgroup factorisation $G = AY$ where Y is cyclic, and y is a generator of Y, then the rule $ya = \varphi(a)y^{\pi(a)}$ (for $a \in A$) defines a skew morphism φ of A with power function π; and conversely*
(b) *if φ is any skew morphism of A of order m, with power function π, then there exists a finite group G with a complementary subgroup factorisation $G = AY$, where $Y = \langle y\rangle$ has order m, and in this group $ya = \varphi(a)y^{\pi(a)}$ for all $a \in A$.*
Furthermore, in either case, $\ker\varphi = A \cap y^{-1}Ay$, and in particular, A is normal in G if and only if φ is an automorphism of A.

In case (b), where the group G is constructed from the skew morphism φ, we call $G = AY$ a *skew product* group. An alternative construction for it was fore-shadowed in [9].

Here we note that in case (a), the order of the skew morphism φ coming from the factorisation $G = AY$ can be less than $|Y|$, and in that case G is not a skew product group. For example, if y^k is central in G then φ^k is trivial and so the order of φ divides k. More generally, the order of φ is equal to the index in Y of its core in G, as we show in Lemma 4.1 below. On the other hand, the skew morphism φ of A given by case (a) above is the skew morphism associated with a regular Cayley map for A if and only if φ has an orbit on A that generates A and is closed under inverses.

Also we note that more than one skew morphism of A can be associated with a complementary subgroup factorisation AY for G, depending on the choice of generator for Y. Specifically, if φ is the skew morphism associated with the generator y of Y, then for each $i \in \mathbb{N}$ we have $y^ia = \varphi^i(a)y^{\sigma(i,a)}$, and in this sense y^i is associated with φ^i. It is important to note that φ^i need not be a skew morphism. We do, however, have the following:

Lemma 3.2. *If φ is a skew morphism of the finite group A, then so is φ^i whenever i is coprime to the order $|\varphi|$ of φ. Hence in particular, the inverse of every skew morphism is a skew morphism.*

Proof. If i is coprime to the order of φ, then y^i generates Y, and so gives rise to a skew morphism of A, which must be φ^i. □

Lemma 3.3. *Let φ be a skew morphism of the finite group A, with power function π. Then φ^i is a skew morphism of A if and only if for every $a \in A$ there is some $k_{i,a} \in \mathbb{Z}_{|\varphi|}$ such that $\sigma(i,a) = \pi(\varphi^{i-1}(a)) + \cdots + \pi(\varphi(a)) + \pi(a) \equiv ik_{i,a}$ mod $|\varphi|$. Moreover, when this happens, the power function of φ^i takes a to $k_{i,a}$ for all $a \in A$, and if $\ker\varphi$ is preserved by φ, then $\ker(\varphi^i)$ contains $\ker\varphi$.*

Proof. Most of this follows easily from the fact that $\varphi^i(ab) = \varphi^i(a)\varphi^{\sigma(i,a)}(b)$ for all $a, b \in A$. For the last part, note that if $a \in \ker\varphi$ and $\ker\varphi$ is preserved by φ, then $\varphi^j(a) \in \ker\varphi$ and so $\pi(\varphi^j(a)) = 1$ for all j, giving $\sigma(i,a) = 1 + 1 + \cdots + 1 = i$, and then $k_{i,a} = 1$, which implies that $a \in \ker(\varphi^i)$. □

Finally in this section, we give an example of a skew morphism of the finite non-abelian simple group A_5, obtainable from another simple group $\mathrm{PSL}(2,11)$.

Example 3.4. *The group $\mathrm{PSL}(2,11)$, of order 660, has a subgroup A of order 60 which is isomorphic to A_5, and complementary to a cyclic Sylow 11-subgroup Y. Also if y is any generator of Y then $A \cap y^{-1}Ay$ is dihedral of order 6. Thus A_5 has a skew morphism φ of order 11, with kernel K of index 10, and power function values $1, 2, \ldots, 10$.*

4. Main theorems

The automorphism group of a simple regular Cayley map $M = \mathrm{CM}(A, X, \rho)$ for a group A is a skew product group, obtainable from A and a skew morphism φ whose restriction to X is equal to the rotation ρ; see [11]. In particular, the order of φ is $|X|$, and the automorphism group has order $|A| \cdot |X|$. In this case $|X| < |A|$ because X is a set of non-trivial elements of A, and therefore the skew morphism φ has order less than $|A|$.

We now generalise this result to all skew morphisms of finite groups, by proving that the order of every skew morphism of a finite group of order $n > 1$ is less than n. This also generalises a theorem of Horoševskiĭ [7] which says the same thing for automorphisms. To prove it, we use this observation:

Lemma 4.1. *If G is any finite group with a complementary subgroup factorisation $G = AY$ with Y cyclic, then for any generator y of Y, the order of the skew morphism φ of A is the index in Y of its core in G, or equivalently, the smallest index in Y of a normal subgroup of G. Moreover, in this case the quotient $\overline{G} = G/\mathrm{Core}_G(Y)$ is the skew product group associated with the skew morphism φ, with complementary subgroup factorisation $\overline{G} = \overline{A}\,\overline{Y}$ where $\overline{A} = AY/Y \cong A/(A \cap Y) \cong A$ and $\overline{Y} = Y/\mathrm{Core}_G(Y)$.*

Proof. Suppose φ^i is trivial. Then $y^i a = \varphi^i(a) y^{\sigma(i,a)} = a y^{\sigma(i,a)}$ and so $a^{-1} y^i a = y^{\sigma(i,a)} \in Y$ for all $a \in A$, and by finiteness it follows that $a^{-1}\langle y^i \rangle a = \langle y^i \rangle$ for all $a \in A$. Thus $\langle y^i \rangle$ is normalised by A, as well as by $\langle y \rangle = Y$, and hence by $AY = G$. Conversely, suppose $\langle y^i \rangle$ is normal in G. Then for all $a \in A$ we have $a^{-1} y^i a \in Y$, so $\varphi^i(a) y^{\sigma(i,a)} = y^i a \in aY$, and it follows from the fact that $A \cap Y = \{1\}$ that $\varphi^i(a) = a$ (for all $a \in A$). Thus φ^i is trivial. Hence the order of φ is the smallest positive integer i for which $\langle y^i \rangle$ is normal in G, or in other words, the index in Y of $\mathrm{Core}_G(Y)$. The rest follows easily. □

This observation also sheds light on the case of a regular Cayley map $M = \mathrm{CM}(A, X, \rho)$ whose underlying graph is not simple. It is known that such a map M has multiple edges if and only if the stabiliser Y of the identity vertex in the full automorphism group of M has non-trivial core; see [2]. In that case, the full automorphism group of the regular Cayley map is not a skew product, and the order of the automorphism group of the map M can exceed $|A|^2$. The order of the associated skew morphism φ of A is equal to the number of distinct neighbours of the identity vertex in the underlying Cayley graph (and is therefore smaller than $|A|$), rather than the number of edges incident with the identity vertex.

Theorem 4.2. *If φ is a skew morphism of the non-trivial finite group A, then the order of φ is less than $|A|$.*

Proof. Let $G = AY$ be the skew product associated with φ. By the above Lemma, the core of Y in G is trivial. We can can use a theorem of Lucchini [15] or similar theorem by Herzog and Kaplan [5] to prove that $|Y| < |A|$, and the assertion follows.

Lucchini's theorem states that if P is a transitive permutation group of degree $n > 1$ with cyclic point-stabilisers, then $|P| \leq n(n-1)$. To apply this, we take P to be the permutation group induced by our group G on right cosets of the subgroup Y, by right multiplication. The degree is $n = |G:Y| = |A|$, and since the core of Y in G is trivial, P is isomorphic to G, and hence Lucchini's theorem gives $|G| \leq n(n-1) \leq |A|(|A|-1)$. On the other hand, $|G| = |AY| = |A||Y|$, so this implies $|Y| \leq |A| - 1 < |A|$.

Similarly, the theorem of Herzog and Kaplan states that if G is a non-trivial finite group with a cyclic subgroup B of order $\sqrt{|G|}$ or more, then B has non-trivial core in G. Applying this to our group $G = AY$ with $B = Y$ (which we know is core-free in G), we find that $|Y| < \sqrt{|G|}$, so $|Y|^2 < |G| = |A||Y|$, and again this gives $|Y| < |A|$. □

Our next main theorem is a consequence of the above:

Theorem 4.3. *Every skew morphism of a non-trivial finite group has non-trivial kernel.*

Proof. Let φ be a skew morphism of the finite group A, with kernel K and power function $\pi : A \to \mathbb{Z}_m$, where m is the order of φ. By Lemma 2.1, the number of distinct values taken by π is equal to the index $|A:K|$, and therefore $|A:K| \leq m$. But also Theorem 4.2 gives $m < |A|$, and so $|A:K| \leq m < |A|$, which implies $|K| > 1$. □

As an immediate further consequence, we have the following, which extends an observation made in [11] for skew morphisms associated with regular Cayley maps:

Corollary 4.4. *Every skew morphism of a cyclic group of prime order is an automorphism.*

5. Skew morphisms of abelian groups

We begin with some observations made by us in [3, Lemma 5.1], and we include a copy of the proof for completeness.

Lemma 5.1. *Let A be a finite abelian group, and φ be a skew morphism of A, with power function π and kernel K. Then*:

(a) *φ preserves K setwise*;
(b) *the restriction of φ to K is a group automorphism of K*; *and*
(c) *for each $b \in A$, the difference $\pi(b)-1$ is divisible by the length of every non-trivial orbit of φ on K.*

Proof. Let $a \in K$ and $b \in A$. Then since A is abelian,

$$\varphi(b)\varphi(a) = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi^{\pi(b)}(a),$$

for all $b \in A$, and so $\varphi^{\pi(b)}(a) = \varphi(a)$. It follows that either $\varphi(a) = a$, or $\pi(b)$ is congruent to 1 modulo the length of the orbit of a. This proves part (c). Next, we note that the elements a and $\varphi(a)$ lie in the same orbit $\mathcal{O}$ of φ, and then since $\pi(b) \equiv 1 \bmod |\mathcal{O}|$ it follows that $\varphi^{\pi(b)}(\varphi(a)) = \varphi(\varphi(a)) = \varphi^2(a)$. In turn we find

$$\varphi(\varphi(a)b) = \varphi(b\varphi(a)) = \varphi(b)\varphi^{\pi(b)}(\varphi(a)) = \varphi(b)\varphi^2(a) = \varphi^2(a)\varphi(b),$$

and therefore $\varphi(b) = \varphi^{\pi(\varphi(a))}(b)$. As this holds for all $b \in A$, we conclude that $\pi(\varphi(a)) = 1$, and therefore $\varphi(a) \in \ker\varphi = K$, proving part (a). Finally, since $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in K$, we obtain (b), namely that the restriction $\varphi\restriction_K$ is an automorphism of K. □

The above lemma and the resulting fact that every skew morphism φ of a finite abelian group induces a skew morphism φ^* of the quotient group A/K (see Proposition 2.2) can be used to recursively determine all skew morphisms of small abelian groups.

For example, a short computation using Magma [1] shows the following:

- C_2 has only one skew morphism (namely the identity);
- C_3 has two skew morphisms, namely the two automorphisms of C_3;
- C_4 has two skew morphisms, namely the two automorphisms of C_4;
- $C_2 \times C_2$ ($\cong V_4$) has six skew morphisms, namely the six automorphisms;
- C_5 has four skew morphisms, namely the four automorphisms of C_5;
- C_6 has four skew morphisms: two automorphisms and two others with kernel C_3;
- C_7 has six skew morphisms, namely the six automorphisms of C_7;
- C_8 has six skew morphisms: four automorphisms and two others with kernel C_4;
- $C_4 \times C_2$ has 16 skew morphisms: eight automorphisms and eight others with kernel C_4;
- $C_2 \times C_2 \times C_2$ has 168 skew morphisms, all of which are automorphisms.

We can use this to obtain a stronger version of Theorem 4.3:

Theorem 5.2. *If A is a finite abelian group of order greater than 2, then the kernel of every skew morphism of A has order greater than 2. Equivalently, if the finite group G is a complementary product AB where A is abelian and $|A| > 2$, and B is cyclic and core-free in G, then A contains a normal subgroup K of G with $|K| > 2$.*

Proof. We use induction on $|A|$. For $2 < |A| < 6$, we know that every skew morphism of A is an automorphism, so the kernel always has order $|A|$.

For the inductive step, we suppose $|A| \geq 6$, and to prove the theorem, we suppose that the kernel of some skew morphism φ of A has order 2. Let π be the power function, and let v be the non-trivial element of K. Then $\varphi(v) = v$, since φ preserves K. Next let φ^* be the skew morphism of A/K induced by φ, with $\varphi^*(Kx) = K\varphi(x)$ for all $x \in A$, and let L/K be its kernel. By induction, we can suppose that $|L/K| > 2$ (since $|A/K| \geq 3$).

Now if $\mathcal{O}^*$ is any orbit of φ^*, then the length of the corresponding orbit $\mathcal{O}$ of φ is either the same as the length of $\mathcal{O}^*$, or twice the length of $\mathcal{O}^*$, depending on whether or not $\mathcal{O}$ contains two elements of the form x and vx (where v is the non-trivial element of K). Noting the way in which power functions are determined by the orbits of the skew morphism, we deduce that the number of values of the power function π is either the same as the number of values of the power function of φ^*, or twice as many. Hence the index $|A:K|$ is at most twice the index in A/K of the kernel L/K of φ^*. But that implies $|A:K| \leq 2|A:L|$, which is impossible since $|L:K| > 2$. Thus no such counterexample φ exists. □

This can be used to speed up and hence extend the computation mentioned earlier. Again with the help of MAGMA [1], we have completely determined the skew morphisms of all cyclic groups of order up to 60, and all abelian groups of order up to 32. Details are available from the first author on request.

Next we prove a highly technical lemma that is key to many subsequent theorems.

Lemma 5.3. *Let φ be a skew morphism of the finite abelian group A, and suppose φ has order m and power function π. Also suppose N is any non-trivial subgroup of $K = \ker\varphi$ preserved by φ, and let e be the exponent of N, and let φ^* be the the skew morphism of the quotient group $\overline{A} = A/N$ induced by φ. Then*:

(a) *if b is any element of A for which $\overline{b} = Nb$ lies in the kernel of φ^*, then $e\pi(b) \equiv e \bmod m$, and in particular, if $\gcd(e, m) = 1$ then $b \in K$;*

(b) *if $K \neq A$ (so that φ is not an automorphism of A), then m has a non-trivial divisor in common with e; and*

(c) *if $\mu = \varphi^k$, where k is the order of φ^*, then μ is a skew morphism of A, with $K = \ker\varphi \subseteq \ker\mu$.*

Furthermore, if N is cyclic of prime order p, then:

(d) $\mu\restriction_N$ *is exponentiation by some unit* r *mod* p,
(e) *if* r *has order* $j > 1$, *then* μ *has order* j, *while*
(f) *if* $r \equiv 1$ *mod* p, *then* μ *has order* 1 *or* p, *and*
(g) *if also* A/K *is cyclic, and* μ *is trivial on* N *but non-trivial on* A, *then* μ *has order* p, *and the power function* π_μ *of* μ *is a homomorphism from* A *to* $\mathbb{Z}_p^*$, *with* $N \subseteq K = \ker\varphi \subseteq \ker\mu = \ker\pi_\mu$.

Proof. First let c be any element of A. Then since $\overline{b}$ lies in the kernel of φ^*, we have

$$N\varphi(bc) = \varphi^*(Nbc) = \varphi^*(\overline{bc}) = \varphi^*(\overline{b})\varphi^*(\overline{c}) = \varphi^*(Nb)\varphi^*(Nc) = N\varphi(b)N\varphi(c) = N\varphi(b)\varphi(c).$$

It follows that $\varphi(b)\varphi^{\pi(b)}(c) = \varphi(bc) = w\varphi(b)\varphi(c)$ for some $w \in N$, and so $\varphi^{\pi(b)}(c) = v\varphi(c)$ for some $v \in N$. Then letting $u = \varphi^{-1}(v)$, which lies in N (since φ preserves N) and hence in $\ker\varphi$, we find $\varphi^{\pi(b)}(c) = \varphi(u)\varphi(c) = \varphi(uc)$, and so $\varphi^{\pi(b)-1}(c) = uc$.

Also since A is abelian, we have

$$\varphi(b)\varphi(u) = \varphi(u)\varphi(b) = \varphi(ub) = \varphi(bu) = \varphi(b)\varphi^{\pi(b)}(u),$$

and therefore $\varphi^{\pi(b)-1}(u) = u$. It follows that

$$\varphi^{2(\pi(b)-1)}(c) = \varphi^{\pi(b)-1}(\varphi^{\pi(b)-1}(c)) = \varphi^{\pi(b)-1}(uc) = \varphi^{\pi(b)-1}(u)\varphi^{\pi(b)-1}(c) = u(uc) = u^2c,$$

and by induction $\varphi^{e\pi(b)-e}(c) = \varphi^{e(\pi(b)-1)}(c) = u^ec$.

But N has exponent e, so $u^e = 1$, and thus we obtain $\varphi^{e\pi(b)-e}(c) = c$, which proves that $e\pi(b)-e$ is divisible by the length of the orbit of c.

It follows that $e(\pi(b)-1) = e\pi(b)-e$ is divisible by the LCM of the lengths of the orbits of φ, which is its order m. Finally, if e is coprime to m, then from $e\pi(b) \equiv e \bmod m$ it follows that $\pi(b) \equiv 1 \bmod m$, so that $b \in K$. This proves part (a), and hence also part (b).

Next, let $b, c \in A$. Then $\mu(bc) = \varphi^k(bc) = \varphi^k(b)\varphi^{\sigma(k,b)}(c) = \mu(b)\varphi^{\sigma(k,b)}(c)$ where $\sigma(k,b)$ is independent of c; see Lemma 2.1. This gives $\varphi^{\sigma(k,b)}(c) = \mu(b)^{-1}\mu(bc)$, which must lie in the same coset of N as $b^{-1}bc = c$, since μ is the identity on A/N. Thus we have $N\varphi^{\sigma(k,b)}(c) = Nc$ for all $c \in A$, so $\varphi^{\sigma(k,b)}$ acts trivially on A/N. Hence $\sigma(k,b)$ is divisible by k, for all $b \in A$, and so Lemma 3.3 tells us that μ is a skew morphism of A, with $\ker\varphi \subseteq \ker\mu$ (by Lemmas 5.1 and 3.3). This proves part (c).

Now suppose N is cyclic of prime order p. Then $\varphi\restriction_N$ is an automorphism, and hence is exponentiation by some unit r mod p. For any $c \in A$, since μ is trivial on A/N we know that $\mu(c) = ac$ for some $a \in N$, and then an easy induction gives

$$\mu^i(c) = \mu^{i-1}(a)\mu^{i-2}(a)\dots\mu(a)ac = a^{r^{i-1}+r^{i-2}+\cdots+r+1}c \text{ for all } i.$$

If c is not fixed by μ, then $a \neq 1$, so the length of the μ-orbit of c is the smallest i for which $r^{i-1}+\cdots+r+1 \equiv 0 \bmod p$. When $r = 1$, the smallest i (and hence the orbit length) is p, while if $r \not\equiv 1 \bmod p$, then since $r^i - 1 = (r-1)(r^{i-1}+\cdots+r+1) \equiv 0 \bmod p$, the smallest i is the order j of r as a unit mod p. This proves (d), (e) and (f).

Finally, for (g) we suppose $r = 1$ but μ is non-trivial, and also suppose that A/K is cyclic. Let c be any element of A for which the coset Kc generates A/K, and again suppose $\mu(c) = ac$ where $a \in N$. Then $\mu^i(c) = a^i c$ for all i (since μ fixes $a \in N$). Next, let $s = \pi_\mu(c)$, where π_μ is the power function of μ. Then $\mu(c^2) = \mu(cc) = \mu(c)\mu^s(c) = aca^s c = a^{s+1}c^2$. More generally, if $\mu(c^j) = a^{s^{j-1}+\cdots+s+1}c^j$, then $\mu^s(c^j) = a^{s(s^{j-1}+\cdots+s+1)}c^j$, and so

$$\mu(c^{j+1}) = \mu(cc^j) = \mu(c)\mu^{\pi_\mu(c)}(c^j) = ac\mu^s(c^j) = aca^{s(s^{j-1}+\cdots+s+1)}c^j = a^{s^j+\cdots+s^2+s+1}c^{j+1},$$

and hence by induction this holds for all j. On the other hand, also

$$\mu(c^{j+1}) = \mu(c^j)\mu^{\pi_\mu(c^j)}(c) = a^{s^{j-1}+\cdots+s+1}c^j a^{\pi_\mu(c^j)}c = a^{\pi_\mu(c^j)+s^{j-1}+\cdots+s+1}c^{j+1},$$

and therefore $a^{\pi_\mu(c^j)} = a^{s^j}$, so $\pi_\mu(c^j) \equiv s^j \bmod p$, for all j. But Kc generates A/K, so every element of A is of the form bc^j for some $b \in K$, and then since $K \subseteq \ker\mu$, we find that $\pi_\mu(bc^j) \equiv \pi_\mu(c^j) \equiv s^j \bmod p$ as well. Thus π_μ is a homomorphism from A to $\mathbb{Z}_p^*$ (with $N \subseteq K = \ker\varphi \subseteq \ker\mu = \ker\pi_\mu$). □

As an immediate application we have the following:

Theorem 5.4. *Let A be a finite abelian p-group, and let φ be a skew morphism of A that is not an automorphism of A. Then the order of φ is divisible by p.*

Proof. Let m be the order of φ. By Lemma 5.1, the kernel K of φ is preserved by φ, so we can take $N = K$ in Lemma 5.3. Since $K \neq A$ and the exponent e of K is a power of p, we find $\gcd(e, m) \neq 1$ and therefore $\gcd(p, m) \neq 1$. □

Corollary 5.5. *If the finite group G is a complementary product AB where A is an abelian p-group, and B is cyclic and core-free in G, then either A is normal in G (so G is a semi-direct product $A \rtimes B$), or p divides $|B|$.*

A corollary of the next application gives a stronger form of Theorem 5.2.

Theorem 5.6. *Let φ be a skew morphism of the finite abelian group A, with kernel K, and let L/K be the kernel of the skew morphism φ^* of A/K induced by φ. If p is a prime that divides $|L|$ but not $|K|$, then $p < q$ for every prime divisor q of $|K|$.*

Proof. Suppose that such a prime p exists, and let q be any prime divisor of $|K|$. We know that φ induces an automorphism of K, and as K is abelian, it follows that φ preserves the subgroup N consisting of the identity and all elements of order q. In particular, N is a subgroup of K of exponent q that is invariant under φ.

Next let b be any element of order p in L, and let m and π be the order and power function of φ. Since L/K is the kernel of φ^*, we know by Lemma 5.3 that $q(\pi(b) - 1) \equiv 0 \bmod m$. If q is coprime to m, then $\pi(b) \equiv 1 \bmod m$ and so $b \in K$, which is impossible since K has no element of order p. Thus q divides m, and $\pi(b) - 1 \equiv 0 \bmod m/q$. In particular, $\pi(b) = 1 + i(m/q)$ where $1 \leq i \leq q-1$, so there are at most $q-1$ possibilities for $\pi(b)$.

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

Corollary 5.7. *Let A be a non-trivial finite abelian group. If K is the kernel of any skew morphism of A, then every prime divisor of $|K|$ is larger than every prime that divides $|A|$ but not $|K|$. In particular if q is the largest prime divisor of $|A|$, then the order of the kernel of every skew morphism of A is divisible by q when q is odd, or by 4 when $q = 2$.*

Proof. We use induction on $|A|$ to prove the first part. Let φ be any skew morphism of A, with kernel K, and suppose that p is any prime divisor of $|A|$ that does not divide $|K|$. Also let L/K be the kernel of the skew morphism φ^* of A/K induced by φ. If p divides $|L/K|$, then by Theorem 5.6, we know that p is smaller than every prime divisor of $|K|$. On the other hand, if p does not divide $|L/K|$, then by induction p is smaller than every prime divisor of $|L/K|$, and hence smaller than every prime divisor of $|K|$.

For the second part, we observe that if $q = 2$, then A is a 2-group, and then by Theorem 5.2 we know that $|K| > 2$, and hence that $|K|$ is divisible by 4. □

A consequence of Corollary 5.7 is that if φ is a skew morphism of an abelian group A, and φ has an orbit $\mathcal{O}$ on A that is larger than $|A| - q$ where q is the largest prime divisor of $|A|$, then φ must be an automorphism of A. To see this, note that the kernel K of φ is preserved by φ but now also q divides $|K|$, and so the given orbit $\mathcal{O}$ is contained in K, and therefore $A = \langle \mathcal{O} \rangle \subseteq K$. This is an improvement over Corollary 5.3 in [3], which showed the same thing holds for the *smallest* prime dividing $|A|$.

Note also that Corollary 5.7 does not always hold when A is non-abelian. For example, the dihedral group D_3 of order 6 has skew morphisms of order 4 with kernel of order 2, and in Example 3.4 we saw that A_5 (of order 60) has a skew morphism with kernel of order 6, which is not divisible by 5.

Another application of Lemma 5.3 is the following:

Theorem 5.8. *Every skew morphism of an elementary abelian 2-group is an automorphism. Hence if the finite group G is a complementary product of an elementary abelian 2-subgroup A and a cyclic subgroup B, then either A is normal in G (so that G is a semi-direct product $A \rtimes B$), or B has non-trivial core in G, say J, and then AJ/J ($\cong A$) is normal in G/J (so that G/J is isomorphic to semi-direct product $A \rtimes B/J$).*

Proof. Let A be the elementary abelian 2-group C_2^n, of order 2^n, and let φ be a skew morphism of A, of order m, with kernel K. We use induction on n to prove that φ is an automorphism, or equivalently, $K = A$. This is easily seen to be true when $|A| = 2$ or 4, so for the inductive step, we can assume that $n \geq 3$.

We know that K is preserved by φ, and that φ induces a skew morphism φ^* of A/K, which by induction is an automorphism. Now the kernel of φ^* on A/K is A/K itself, and so we can take $N = K$ (and $e = 2$) in Lemma 5.3, and find that $2\pi(b) \equiv 2 \bmod m$ for all $b \in A$.

If m is odd then $\pi(b) \equiv 1 \bmod m$ for all $b \in A$, so every element of A lies in K, as required.

On the other hand, suppose m is even. Then the congruence $2\pi(b) \equiv 2 \bmod m$ implies that $\pi(b) \equiv 1$ or $\frac{m}{2}+1 \bmod m$, for all $b \in A$. Thus π has at most two values in $\mathbb{Z}_m$, so $|A : K| = 1$

or 2. If $|A:K| = 1$ then $K = A$, so we will now assume $|A:K| = 2$. If x is any element of $A \setminus K$, then φ is completely determined by the automorphism $\xi = \varphi\restriction_K$ of K and the element $y = \varphi(x)$, since $\varphi(ax) = \varphi(a)\varphi(x) = \xi(a)y$ for every element $ax \in Kx = A \setminus K$. But A is elementary abelian (and so is like a vector space of rank n over $\mathbb{Z}_2$), and hence there is a unique automorphism θ of A restricting to ξ on K and taking x to y. Then θ takes the same values as φ, so $\varphi = \theta$, and therefore φ is an automorphism.

The rest follows easily. □

There is no analogue of this theorem for skew morphisms of elementary abelian groups of odd order; even the smallest such group (namely $C_3 \times C_3$) has skew morphisms that are not automorphisms. In fact, it is easy to show that for every odd prime p, the group $C_p \times C_p$ has a skew morphism with kernel of order (and index) p:

Example 5.9. *Let $V = C_p \times C_p$, and let $\{u, v\}$ be generating pair for V. Also let r be a primitive element in $\mathbb{Z}_p^*$, of order $p-1$, and let α be the automorphism of V of order $p(p-1)$ associated with the matrix $\begin{pmatrix} r & 1 \\ 0 & r \end{pmatrix}$, taking u to u^r, and v to uv^r. Next let G be the semi-direct product $V \rtimes_\alpha Y$, where Y is a cyclic group of order $p(p-1)$ generated by y, and $ywy^{-1} = w^\alpha$ for each $w \in V$. Then G has complementary factorisation $G = VY$, with V normal in G, corresponding to the automorphism α of $V = C_p \times C_p$. Now let A be the subgroup generated by u and vy^{p-1}. It is an easy exercise to verify that vy^{p-1} has order p and commutes with u, so that $A \cong C_p \times C_p$, but also $y(vy^{p-1})y^{-1} \notin A$, so that A is not normal in G. Also $A \cap Y = \{1\}$, and therefore $G = AY$ is another complementary subgroup factorisation for G, giving a skew morphism for $A \cong C_p \times C_p$ with kernel $K = A \cap y^{-1}Ay = \langle u \rangle$ of order p.*

With a little more work, however, we can prove something much stronger:

Theorem 5.10. *Let A be the elementary abelian p group $C_p \times C_p$ (of order p^2), where p is an odd prime, and let K be any cyclic subgroup of order p, and let a be a generator for K and let x be any element of $A \setminus K$. Then for any given triple (d, n, r) with $d, n \in \{1, 2, \ldots, p-1\}$ and $r \in \{2, \ldots, p-1\}$, if k is the order of r as a unit mod p, then there exists a unique element $b \in K$ such that the mapping $\varphi\colon A \to A$ given by $\varphi(a^i x^j) = a^{ri + \frac{dj(j-1)rn}{2}}(bx^r)^j$ is a skew morphism of A with $\varphi^k(x) = a^d x$. This skew morphism has order pk (where k is the order of r as a unit mod p), and the power function π of φ is given by $\pi(a^i x^j) = 1 + jnk$ mod pk for all i and j. Conversely, every skew morphism of $C_p \times C_p$ that is not an automorphism arises this way. In particular, there are $(p-1)^2(p-2)$ such skew morphisms for each K, and the total number of skew morphisms of $C_p \times C_p$ is $2(p+1)(p-1)^3$.*

Proof. First, let φ be any skew morphism of A such that φ is not an automorphism, and suppose φ has order m and power function π. Then the kernel K of φ must be one of the $p+1$ subgroups of order p in A, and φ induces a skew morphism φ^* of A/K.

Since $A/K \cong C_p$, we know that φ^* is an automorphism, and it follows from part (b) of Lemma 5.3 that m is divisible by p (since $\ker\varphi \neq A$). On the other hand, φ^* must be exponentiation by r for some unit r mod p. If k is the multiplicative order of r mod p, then k is coprime to p, and so by parts (e) and (f) of Lemma 5.3, we find that μ has order p, and $\mu = \varphi^k$ acts trivially on K. Hence in particular, $m = kp$. Also by part (g) of Lemma 5.3, the power function π_μ of μ is a homomorphism from A to $\mathbb{Z}_p^*$, with $K \subseteq \ker\mu = \ker\pi_\mu$. But $|A:K| = p$ is coprime to $p-1 = |\mathbb{Z}_p^*|$, and it follows that $|A:\ker\mu| = 1$, so μ is an automorphism of A. In particular, $\mu \neq \varphi$, so $k \neq 1$ and therefore $r \in \{2, 3, \ldots, p-1\}$.

Moreover, since $\varphi^k = \mu$ has order p and acts trivially on both K and A/K, it must fix a and take x to cx for some non-trivial $c \in K$, and then $\mu(x^i) = (cx)^i = c^i x^i$ for all i, and by induction, $\mu^j(x^i) = c^{ij}x^i$ for all $j > 0$. Also we know that $\varphi(x) = bx^r$ for some $b \in K$, and then since $\mu = \varphi^k$ commutes with φ, we find that

$$\varphi(c)bx^r = \varphi(c)\varphi(x) = \varphi(cx) = \varphi(\mu(x)) = \mu(\varphi(x)) = \mu(bx^r) = \mu(b)\mu(x^r) = bc^r x^r,$$

and so $\varphi(c) = c^r$. Then since c is non-trivial, it follows that φ induces exponentiation by r on K (the same as it does on on A/K).

Next, by Lemma 5.3 we know that $p(\pi(x)-1) \equiv 0 \bmod kp$, and therefore $\pi(x) \equiv 1 \bmod k$, say $\pi(x) = 1 + nk$ where $1 \leq n < p$. Hence for all $i > 0$ we have

$$\varphi^{\pi(x)}(x^i) = \varphi^{1+nk}(x^i) = \varphi(\varphi^{nk}(x^i)) = \varphi(\mu^n(x^i)) = \varphi(c^{in}x^i) = \varphi(c^{in})\varphi(x^i) = c^{irn}\varphi(x^i).$$

In particular, $\varphi(x^2) = \varphi(x)\varphi^{\pi(x)}(x) = \varphi(x)c^{rn}\varphi(x) = c^{rn}\varphi(x)^2$, and then by induction,

$$\begin{aligned}\varphi(x^j) &= \varphi(x)\varphi^{\pi(x)}(x^{j-1}) = \varphi(x)c^{(j-1)rn}\varphi(x^{j-1}) = \varphi(x)c^{(j-1)rn}c^{\frac{(j-1)(j-2)rn}{2}}\varphi(x)^{j-1} \\ &= c^{(j-1)rn+\frac{(j-1)(j-2)rn}{2}}\varphi(x)^j = c^{\frac{j(j-1)rn}{2}}\varphi(x)^j \quad \text{for all } j \geq 0.\end{aligned}$$

Note that if $c = a^d$ and $\varphi(x) = bx^r$, then this gives $\varphi(x^j) = a^{\frac{dj(j-1)rn}{2}}(bx^r)^j$ for all j, and it follows that φ is as given in the statement of the theorem.

Also by Lemma 5.3 we know that $\pi(x^j)-1$ is divisible by k, so $\pi(x^j) = 1+qk$ for some q, and therefore

$$\varphi(x^{j+1}) = \varphi(x^j)\varphi^{\pi(x^j)}(x) = \varphi(x^j)\varphi^{qk+1}(x) = \varphi(x^j)\mu^q(\varphi(x)) = \varphi(x^j)\mu^q(bx^r) = \varphi(x^j)bc^{rq}x^r.$$

Substituting $c^{\frac{j(j-1)rn}{2}}\varphi(x)^j$ for $\varphi(x^j)$ and the analogous expression for $\varphi(x^{j+1})$, we find

$$c^{\frac{(j+1)jrn}{2}}\varphi(x)^{j+1} = bc^{rq}c^{\frac{j(j-1)rn}{2}}\varphi(x)^j x^r = c^{rq}c^{\frac{j(j-1)rn}{2}}\varphi(x)^{j+1},$$

and therefore $rq \equiv \frac{(j+1)jrn}{2} - \frac{j(j-1)rn}{2} \equiv jrn \bmod p$, which gives $q \equiv jn \bmod p$. Thus $\pi(x^j) = 1 + jnk$, and hence $\pi(ux^j) = 1 + jnk$, for all $u \in K$ and all j.

For uniqueness of b (for given values of d, r and n), we show that for each i there exists an integer q_i independent of b for which $\varphi^i(x) = b^{ir^{i-1}}a^{q_i}x^{r^i}$. This is clearly true for $i = 1$ (with $q_1 = 0$), and we can prove it for all $i > 1$ by induction, since

$$\varphi^{i+1}(x) = \varphi(\varphi^i(x)) = \varphi(b^{ir^{i-1}}a^{q_i}x^{r^i}) = b^{ir^i}a^{q_i r}a^{\frac{dr^i(r^i-1)rn}{2}}\varphi(x)^{r^i} = b^{ir^i}a^{q_i r}a^{\frac{dr^i(r^i-1)rn}{2}}(bx^r)^{r^i},$$

which implies that we can take $q_{i+1} = q_i r + \frac{dr^i(r^i-1)rn}{2}$.

In particular, we find that $cx = \varphi^k(x) = b^{kr^{k-1}} a^{q_k} x^{r^k} = b^{kr^{k-1}} a^{q_k} x$, so $b^{kr^{k-1}} a^{q_k} = c$, and then since k and r are units mod p and b is non-trivial, it follows that there is just just one possibility for b.

Finally, we show that given any triple (d, n, r) of the required form, there exists a skew morphism φ of A with the required properties.

To do this, again we let k be the order of r as a unit mod p, and let $c = a^d$, and then let b be the unique element of K for which $b^{kr^{k-1}} a^{q_k} = c$.
(Note that q_k can be found recursively from $q_{i+1} = q_i r + \frac{dr^i(r^i-1)rn}{2}$, starting with $q_1 = 0$.)
Then we can define φ by $\varphi(a^i x^j) = a^{ir} c^{\frac{j(j-1)rn}{2}} (bx^r)^j$ for all i and j, and by using some of the above arguments it is an easy exercise to verify that φ is a skew morphism of A of order pk with $\varphi^k(x) = cx = a^d x$, and with power function π given by $\pi(a^i x^j) = 1 + jnk$ mod pk for all i and j.

Thus for each of the $p+1$ possibilities for K, the number of skew morphisms with kernel K is equal to the number of triples (d, n, r), namely $(p-1)^2(p-2)$. Also the number of automorphisms is $(p^2-1)(p^2-p)$, and so the total number of skew morphisms of $C_p \times C_p$ is $(p^2-1)(p^2-p) + (p+1)(p-1)^2(p-2) = (p+1)(p-1)^2(2p-2) = 2(p+1)(p-1)^3$. □

6. Skew morphisms of cyclic groups

We begin this section with two theorems, parts of which were proved by Kovács and Nedela, but we take a different approach. The first is a stronger version of Corollary 3.4 in [13].

Theorem 6.1. *Let φ be a skew morphism of C_n. Then the order m of φ divides $n\phi(n)$. Moreover, if $\gcd(m, n) = 1$ or $\gcd(\phi(n), n) = 1$, then φ is an automorphism of C_n.*

Proof. We will use induction on n. We know that for all $n \leq 5$, every skew morphism of C_n is an automorphism, and of course if φ is an automorphism of C_n (for any n), then its order divides $|\mathrm{Aut}(C_n)| = \phi(n)$; hence the claims are true for all $n \leq 5$. From now on we let $A = C_n$, and suppose that φ is not an automorphism of A.

The kernel K of φ is non-trivial (by Theorem 4.3), and since A is abelian we know that K is preserved by φ; indeed the restriction $\varphi\restriction_K$ is an automorphism of K (by Theorem 5.1). Then because K is cyclic, K has a subgroup N of prime order p, invariant under φ. By induction, the order k of the skew morphism φ^* induced by φ on G/N divides $(n/p)\,\phi(n/p)$. The latter divides $n\phi(n)$, but if we define $d = \gcd(k, \phi(p))$, then we can divide by $\phi(p)/d$ and find that k divides $nd\phi(n)/\phi(p)$.

Also by parts (e) and (f) of Lemma 5.3, we know that $\mu = \varphi^k$ has order $1, p$ or j, where j divides $\phi(p)$ and is the order of $\mu\restriction_N$ if μ acts non-trivially on N. If μ has order 1 or p, then φ has order k or kp, both of which divide $n\phi(n/p)$ and hence divide $n\phi(n)$. On the other hand, if μ has order j, so that φ has order jk, let us suppose that $\varphi\restriction_N$ is exponentiation by

r. Then r^k has the same multiplicative order in $\mathbb{Z}_p^*$ as r^d, and hence $\varphi\restriction_N$ must have order jd. But of course $\varphi\restriction_N$ is an automorphism of $N \cong C_p$, so jd divides $\phi(p)$, and therefore j divides $\phi(p)/d$. It follows that jk divides $(\phi(p)/d)(nd\phi(n)/\phi(p)) = n\phi(n)$, as required.

Next, $K \neq A$ since φ is not an automorphism, so by Lemma 5.3, we know that p divides m, and therefore $\gcd(n, m) \neq 1$. Equivalently, this proves that if $\gcd(m, n) = 1$ then φ is an automorphism of A.

Finally, suppose $\gcd(\phi(n), n) = 1$ but $\gcd(m, n) \neq 1$. Then $\gcd(\phi(n/p), n/p) = 1$, so by induction φ^* is an automorphism of A/N, which in turn implies that its order k divides $\phi(n/p)$ and hence is coprime to n. On the other hand, since we have assumed that $\gcd(m, n) \neq 1$, the order of $\mu = \varphi^k$ must have a prime divisor in common with n. By Lemma 5.3 the order of $\mu = \varphi^k$ must be equal to p or j, but j is the order of $\mu\restriction_N$, so j divides $\phi(p)$ and hence is coprime to n, and therefore the order of $\mu = \varphi^k$ must be p. In particular, $r \equiv 1 \bmod p$, and μ is trivial on N. Moreover, by part (g) of Lemma 5.3, the power function π_μ of μ is a homomorphism from A to $\mathbb{Z}_p^*$. This implies that $|A : \ker\mu|$ divides $\phi(p)$, and since $\gcd(n, \phi(p)) = 1$, it follows that $\ker\mu = A$ and therefore μ is an automorphism of A. Hence its order p divides $\phi(n)$, so $\gcd(\phi(n), n) \neq 1$, a contradiction. Equivalently, this proves that if $\gcd(\phi(n), n) = 1$ then φ is an automorphism of A. □

Theorem 6.2. *Let p and q be primes with $p < q$, let A be the cyclic group C_{pq}, and let x be a generator of A. Then*:

(a) *if $\gcd(p, q-1) = 1$, then every skew morphism of A is an automorphism, while*

(b) *if $\gcd(p, q-1) \neq 1$, then if φ is a skew morphism of A that is not an automorphism, then $K = \ker\varphi \cong C_q$, and φ acts trivially on both K and A/K, and there exists a unit $s \in \mathbb{Z}_q^*$ of order p and some $a \in K \setminus \{1\}$ such that $\varphi(x) = ax$ and $\pi(x) = s$, and conversely, for any unit $s \in \mathbb{Z}_q^*$ of order p and any element $a \in K$ of order q, there is a unique skew morphism φ of A such that $\varphi(x) = ax$ and $\pi(x) = s$.*

Hence in particular, the number of skew morphisms of C_{pq} is

$$\begin{cases} (p-1)(q-1) & \text{if } \gcd(p, q-1) = 1 \\ 2(p-1)(q-1) & \text{if } \gcd(p, q-1) \neq 1. \end{cases}$$

Proof. First let $A = C_{pq}$, and suppose φ is a skew morphism of A that is not an automorphism. Then $K = \ker\varphi$ is a non-trivial proper subgroup of A, and $|K|$ is divisible by q (by Corollary 5.7), so $|K| = q$ and $|A/K| = p$. Also φ preserves K, and $\varphi\restriction_K$ is an automorphism of K, and the skew morphism φ^* induced by φ on A/K is an automorphism.

Let m and k be the orders of φ and φ^* respectively. By Lemma 5.3, we find that m has a prime divisor in common with the exponent q of K, and as q is prime, it follows that q divides m. Also k divides $\phi(p) = p-1$ and so is coprime to q (because $p < q$). On the other hand, since q divides m, we find that q divides the order of $\mu = \varphi^k$. By Lemma 5.3, we find that μ is trivial on K, and the power function π_μ is a homomorphism from A to $\mathbb{Z}_q^*$, with kernel containing K. If the kernel is A, then μ is an automorphism of A and so its

order divides $|\mathrm{Aut}(A)| = |\mathrm{Aut}(C_{pq})| = \phi(p)\phi(q) = (p-1)(q-1)$, but in that case it cannot be divisible by q, contradiction. Hence the kernel of μ (and of π_μ) must be K itself, and from this we find that the homomorphism π_μ gives an isomorphism from $A/K \cong C_p$ to a subgroup of $\mathbb{Z}_q^*$. Hence in particular, p divides $q-1$. This proves (a).

Continuing, we know that p divides $q-1$, and the order of $\mu = \varphi^k$ is divisible by q, so μ is trivial on K. In fact, by Lemma 5.3, we find that μ has order q exactly, so φ has order kq. Letting $\tau = \pi_\mu$ for simplification, on one hand we have

$$\varphi^{k+1}(bc) = \mu(\varphi(bc)) = \mu(\varphi(b)\varphi^{\pi(b)}(c)) = \mu(\varphi(b))\mu^{\tau(\varphi(b))}(\varphi^{\pi(b)}(c)) = \varphi^{k+1}(b)\varphi^{k\tau(\varphi(b))+\pi(b)}(c),$$

while on the other hand,

$$\varphi^{k+1}(bc) = \varphi(\mu(bc)) = \varphi(\mu(b)\mu^{\tau(b)}(c)) = \varphi(\mu(b))\varphi^{\pi(\mu(b))}(\mu^{\tau(b)}(c)) = \varphi^{k+1}(b)\varphi^{\pi(\mu(b))+k\tau(b)}(c),$$

for all $b, c \in A$. It follows that $k\tau(\varphi(b)) + \pi(b) \equiv \pi(\mu(b)) + k\tau(b) \bmod kq$ for all $b \in A$. But also $\pi(\mu(b)) \equiv \pi(b) \bmod kq$, since b and $\mu(b) = \varphi^k(b)$ always lie in the same coset of $K = \ker\varphi$, and so we find that $k\tau(\varphi(b)) \equiv k\tau(b) \bmod kq$ for all $b \in A$. Hence we have $\tau(\varphi(b)) \equiv \tau(b) \bmod q$, or equivalently, $\pi_\mu(\varphi(b)) \equiv \pi_\mu(b) \bmod q$ for all $b \in A$. This implies that $\varphi(b)$ and b lie in the same coset of $\ker\mu = K$, for all $b \in A$. Thus every coset of K is preserved by φ, or in other words, φ is trivial on A/K. In turn, this gives $k = 1$, so $\mu = \varphi$, and φ is trivial on K as well.

Now $\varphi(x)$ lies in Kx and so $\varphi(x) = ax$ for some $a \in K$. Also $\varphi(x) \neq x$, for otherwise $\varphi(x^2) = \varphi(x)\varphi^{\pi(x)}(x) = xx = x^2$ and by induction $\varphi(x^i) = x^i$ for all i, so φ is the identity automorphism on A, contradiction. Hence a is non-trivial, and so has order q. Similarly, in the last part of the proof of Lemma 5.3 we can take $c = x$, and then $s = \pi_\mu(c) = \pi(c) = \pi(x)$ generates the image of the multiplicative power function π, so s has order p in $\mathbb{Z}_q^*$. This proves the first part of (b).

Note that $\varphi^i(x) = a^i x$ for all i, and then $\varphi(x^2) = \varphi(x)\varphi^s(x) = axa^s x = a^{1+s}x^2$, so $\varphi^i(x^2) = a^{(1+s)i}x^2$ for all i, and an easy induction gives $\varphi(x^j) = a^{1+s+s^2+\cdots+s^{j-1}}x^j$ for all j.

Conversely, suppose s is any unit in $\mathbb{Z}_q^*$ of order p, and a is any element in K of order q. Then it is a straightforward exercise to show that defining $\varphi(x^j) = a^{1+s+s^2+\cdots+s^{j-1}}x^j$ for all j gives a skew morphism of A with $\varphi(x) = ax$ and $\pi(x) = s$. This proves the second part of (b). Finally, there are $(p-1)(q-1)$ skew morphisms that are not automorphisms in case (b), and $(p-1)(q-1)$ automorphisms in both cases, so the total number of skew morphisms of C_{pq} is as given. □

A similar theorem holds when $q = p$ (or in other words, for C_{p^2}), for every odd prime p. This was also proved in [13, Proposition 4.9], but here we take a quite different approach, similar to the one in our proof of Theorem 5.10.

We will use the following, which gives properties of certain sums of ascending powers of an integer mod p or p^2 when p is an odd prime.

Lemma 6.3. *Let $t_0^n = 0$ and $t_i^n = 1 + t^n + t^{2n} + \ldots + t^{(i-1)n}$ for positive integers t, i and n. Then $t_{i+j}^n = t_i^n + t_j^n t^{in}$ for all i and j. Also if p is an odd prime, and $t \equiv 1 + dp \bmod p^2$ for some non-negative integer d, then*

(a) $t_i^n \equiv i \bmod p$, (b) $t_i^n \equiv i + \frac{i(i-1)}{2}dnp \bmod p^2$,

(c) $t_{ip}^n \equiv ip \bmod p^2$, (d) $t_i^n \equiv t_j^n \bmod p^2$ *if and only if* $i \equiv j \bmod p^2$.

Proof. First, $t_{i+j}^n = 1 + t^n + \ldots + t^{(i-1)n} + t^{in}(1 + t^n + \ldots + t^{(j-1)n}) = t_i^n + t^{in}t_j^n$ if $i, j > 0$, and it is easy to see that the same thing holds if i or j is 0. Also part (a) is easy, since $t \equiv 1 \bmod p$. For part (b), a binomial expansion gives $t^{jn} \equiv (1 + dp)^{jn} \equiv 1 + jdnp \bmod p^2$ for all j, and so

$$t_i^n \equiv 1 + (1+dnp) + (1+2dnp) + (1+3dnp) + \ldots + (1+(i-1)dnp) \equiv i + \tfrac{i(i-1)}{2}dnp \bmod p^2$$

for all $i > 0$, and part (c) follows from this. For part (d), we note that by part (b) we have

$$2(t_i^n - t_j^n) \equiv 2i + i(i-1)dnp - (2j + j(j-1)dnp) \equiv (i-j)(2 + (i+j-1)dnp) \bmod p^2.$$

Then since 2 and $2 + (i+j-1)dnp$ are coprime to p^2, it follows that $t_i^n - t_j^n \equiv 0 \bmod p^2$ if and only if $i - j \equiv 0 \bmod p^2$. □

Theorem 6.4. *Let A be the cyclic group of order p^2, where p is an odd prime, and let x be a generator for A, and let N be the subgroup generated by x^p. Then for any given triple (d, n, r) with $d, n \in \{1, 2, \ldots, p-1\}$ and $r \in \{2, \ldots, p-1\}$, if we let k be the order of r as a unit mod p, and let $t = 1 + dp$ and define t_i^n for all i as in Lemma 6.3, then there exists a unique element $a \in N$ such that the mapping $\varphi\colon A \to A$ given by $\varphi(x^i) = (ax^r)^{t_i^n}$ for $0 \le i < p^2$ is a skew morphism of A with $\varphi^k(x) = x^t$. This skew morphism has order pk, where k is the order of r as a unit mod p, and the power function π of φ is given by $\pi(x^i) = 1 + ink \bmod pk$ for all i. Conversely, every skew morphism of C_{p^2} that is not an automorphism arises this way. In particular, there are exactly $(p-1)^2(p-2)$ such skew morphisms, and the total number of skew morphisms of C_{p^2} is $(p-1)(p^2-2p+2)$.*

Proof. First, suppose φ is any skew morphism of A such that φ is not an automorphism, and suppose φ has order m and power function π. Then the kernel of φ must be N, of order p, and φ induces a skew morphism φ^* of A/N.

Since $A/N \cong C_p$, we know that φ^* is an automorphism, and it follows from Lemma 5.3 that m is divisible by p (since $\ker\varphi \ne A$). On the other hand, φ^* must be exponentiation by r for some unit $r \bmod p$, and if k is the multiplicative order of $r \bmod p$, then k is coprime to p, and so by parts (e) and (f) of Lemma 5.3, we find that μ has order p, and $\mu = \varphi^k$ acts trivially on N. Hence in particular, $m = kp$. Also by part (g) of Lemma 5.3, the power function π_μ of μ is a homomorphism from A to $\mathbb{Z}_p^*$, with $N \subseteq \ker\mu = \ker\pi_\mu$. But $|A : N| = p$ is coprime to $p-1 = |\mathbb{Z}_p^*|$, and it follows that $|A : \ker\mu| = 1$, so μ is an automorphism of A. In particular, $\mu \ne \varphi$, so $k \ne 1$ and therefore $r \in \{2, 3, \ldots, p-1\}$. Moreover, since μ has order p, it must be exponentiation by t for some $t \equiv 1 \bmod p$, say $t = 1 + dp$ where $1 \le d < p$.

Now let x be any generator of A. Then by Lemma 5.3 we have $p(\pi(x)-1) \equiv 0 \bmod kp$, and so $\pi(x) \equiv 1 \bmod k$, say $\pi(x) = 1 + nk$ where $1 \leq n < p$. Also since $\mu = \varphi^k$ commutes with φ, we find that $\varphi(x^{it}) = \varphi(\mu(x^i)) = \mu\varphi(x^i) = (\varphi(x^i))^t$ for all i, and therefore

$$\varphi^{\pi(x)}(x^i) = \varphi^{1+nk}(x^i) = \varphi(\varphi^{nk}(x^i)) = \varphi((x^i)^{t^n}) = \varphi(x^i)^{t^n} \text{ for all } i > 0.$$

We now find that $\varphi(x^2) = \varphi(x)\varphi^{\pi(x)}(x) = \varphi(x)\varphi(x)^{t^n} = \varphi(x)^{1+t^n} = \varphi(x)^{t_2^n}$, and indeed by induction, we have $\varphi(x^i) = \varphi(x)^{t_i^n}$ for all i:

$$\varphi(x^i) = \varphi(x)\varphi^{\pi(x)}(x^{i-1}) = \varphi(x)\varphi(x^{i-1})^{t^n} = \varphi(x)(\varphi(x)^{t_{i-1}^n})^{t^n} = \varphi(x)^{1+t^n t_{i-1}^n} = \varphi(x)^{t_i^n},$$

since $1 + (t_{i-1}^n)t^n = t_i^n$ (as in the first assertion of Lemma 6.3).

Next, by Lemma 5.3 we know that $\pi(x^i)-1$ is divisible by k, so $\pi(x^i) = 1+qk$ for some q, and therefore

$$\varphi(x)^{t_{i+1}^n} = \varphi(x^{i+1}) = \varphi(x^i)\varphi^{\pi(x^i)}(x) = \varphi(x)^{t_i^n}\varphi^{qk+1}(x) = \varphi(x)^{t_i^n}\mu^q(\varphi(x)) = \varphi(x)^{t_i^n+t^q}.$$

Hence $t^q \equiv t_{i+1}^n - t_i^n \equiv t^{in} \bmod p^2$, again by the first assertion of Lemma 6.3, and so we can take $q = in$, and find that $\pi(x^i) = 1 + ink$, for all i.

Also we note that since φ^* induces exponentiation by r on A/N, we have $\varphi(x) \in (Nx)^r$ and therefore $\varphi(x) = ax^r$ for some $a \in N$, and thus every such skew morphism of $A \cong C_{p^2}$ has the required form.

For uniqueness of a, we suppose that $a = x^{jp}$ and then $\varphi(x) = ax^r = x^{jp+r} = x^s$, say, and show that for all $i > 0$ there is some integer q_i independent of j such that $\varphi^i(x) = x^{s^i+q_ip}$.

The latter is true for $i = 1$ with $q_1 = 0$, and we can prove it for all $i > 1$ by induction: we have $\varphi^{i+1}(x) = \varphi(\varphi^i(x)) = \varphi(x^{s^i+q_ip}) = (x^s)^{t_{s^i+q_ip}^n} = x^{s\,t_{s^i+q_ip}^n}$, and then by part (b) of Lemma 6.3 and the fact that $s \equiv r \bmod p$ we find that

$$s\,t_{s^i+q_ip}^n \;\equiv\; s(s^i + q_ip + \tfrac{s^i(s^i-1)}{2}dnp) \;\equiv\; s^{i+1} + r(q_i + \tfrac{r^i(r^i-1)}{2}dn)p \bmod p^2.$$

Thus we can take $q_{i+1} = rq_i + \frac{r^{i+1}(r^i-1)}{2}dn$, which is again independent of j.

In particular, we find $x^t = \varphi^k(x) = x^{s^k+q_kp}$. But $s^k = (r + jp)^k \equiv r^k + kr^{k-1}jp \bmod p^2$, and so there is just one value of j for which this can occur. Hence a is unique.

Finally, we show that given any triple (d, n, r) of the required form, there exists a skew morphism φ of A with the required properties.

To do this, again we let k be the order of r as a unit mod p, and let $t = 1 + dp$ and define t_i^n for all i as in Lemma 6.3, then take $a = x^{jp}$ where j satisfies $(jp+r)^k + q_kp \equiv t \bmod p^2$. (Note that q_k can be found recursively from $q_{i+1} = rq_i + \frac{r^{i+1}(r^i-1)}{2}dn$, starting with $q_1 = 0$.) Then we can define φ by $\varphi(x^i) = (ax^r)^{t_i^n}$ for all i, and by using some of the above arguments it is an easy exercise to verify that φ is a skew morphism of A of order pk with $\varphi^k(x) = x^t$, and with power function π given by $\pi(x^i) = 1 + ink \bmod pk$ for all i.

Hence the number of skew morphisms that are not automorphisms is equal to the number of triples (d, n, r), namely $(p-1)^2(p-2)$, and the total number of skew morphisms of C_{p^2} is $\phi(p^2) + (p-1)^2(p-2) = p(p-1) + (p-1)^2(p-2) = (p-1)(p^2-2p+2)$. □

We now give two more theorems about skew morphisms of cyclic groups, which will be useful later.

Theorem 6.5. *For every even integer $n > 4$, the cyclic group C_n has a skew morphism with kernel of index 2.*

Proof. This follows from a construction given by the authors in their classification of all anti-balanced regular Cayley maps for finite abelian groups in [3, §7]. (A regular Cayley map of a group A is *anti-balanced* if the power function of the associated skew morphism takes the two values ± 1.) It is also easy to give a direct construction, as follows:

Let $A = C_n$, let x be any generator of A, and let B be the index 2 subgroup generated by x^2. Now define $\varphi\colon A \to A$ by setting

$$\varphi(x^j) = \begin{cases} x^j & \text{if } j \text{ is even} \\ x^{j+2} & \text{if } j \text{ is odd.} \end{cases}$$

Then clearly φ is a bijection, and it is an easy exercise to verify that it is a skew morphism, with power function values 1 on B and -1 on Bx. In particular, B is the kernel of φ. □

Theorem 6.6. *For every odd prime-power $q = p^e$ with $e > 1$, the cyclic group C_q has a skew morphism with kernel of index p.*

Proof. Let $V = C_q$, and let v be any generator of V. Also let $r = p^{e-1} - 1$, which is a unit of order $2p$ in $\mathbb{Z}_q^*$ (with $r^p \equiv -1 \bmod q$) and a unit of order $2p^2$ in $\mathbb{Z}_{pq}^* = \mathbb{Z}_{p^{e+1}}^*$. Now let G be the semi-direct product $V \rtimes_r Y$, where Y is a cyclic group of order $2p$ generated by y, and $yvy^{-1} = v^r$. Then G has complementary subgroup factorisation $G = VY$, with V normal in G, corresponding to the automorphism of $V = C_q = \langle v \rangle$ determined by $v \mapsto v^r$.

Next let $t = r^2$, which is congruent to 1 mod p^{e-1} and has order p in $\mathbb{Z}_q^*$, and let a be the element vy^2 in G. Then

$$a^p = (vy^2)^p = v^{1+t+\cdots+t^{p-1}} y^{2p} = v^s,$$

where $s = 1 + t + \cdots + t^{p-1}$ in $\mathbb{Z}_q$. Since $(1-t)s = (1-t)(1+t+\cdots+t^{p-1}) = 1-t^p$, which is congruent to 0 mod p^e but not mod p^{e+1}, we find that $s \equiv 0 \bmod p$ but $s \not\equiv 0 \bmod p^2$. Thus $a^p = v^s$ has order $p^{e-1} = q/p$, so $A = \langle a \rangle$ has order q. Also $A \cap Y = \{1\}$, because the largest cyclic subgroup of $A \cong C_q$ of order dividing $2p$ is $\langle v^{q/p} \rangle$. Hence G has another complementary subgroup factorisation $G = AY$. In this one, however, the subgroup A is not normal, because if it were, than it would contain $yay^{-1} = yvy^{2-1} = v^r y^2$ and hence contain $yay^{-1}a^{-1} = v^{r-1}$, which is impossible since v^{r-1} generates V. On the other hand, the subgroup of order q/p generated by $a^p = v^s$ is normal in G, and so must be $A \cap y^{-1}Ay$.

Also the core of Y in G is trivial, and so the factorisation $G = AY$ gives rise to a skew morphism φ of $A \cong C_q$ with kernel $K = A \cap y^{-1}Ay$ of index p. □

Note: In the terminology of [4], the pair (q, r) in the above proof is 'admissible', and gives a regular Cayley map for C_q with a balanced representation with regard to $V = \langle v \rangle$, and a non-balanced representation with regard to $A = \langle vy^2 \rangle$.

7. Skew morphisms that are not automorphisms

Every group automorphism is a skew morphism, but the converse is not true. A skew morphism of a finite group A is an automorphism of A if and only if its power function takes constant value 1, or equivalently, its kernel is A. Hence for example, we have Corollary 4.4, stating that every skew morphism of a cyclic group of prime order is an automorphism.

In [13, Theorem 6.3] it was shown that the same holds for the cyclic group of order n if and only if $n = 4$ or $\gcd(n, \phi(n)) = 1$, where ϕ is Euler's function. We will generalise this to the case of all finite abelian groups in Theorem 7.5.

Before doing that, we need to introduce and prove some other things.

Definition 7.1. *If $\varphi : A \to A$ and $\nu : B \to B$ are permutations on the sets A and B, then their* direct product *$\varphi \times \nu$ is the permutation of the Cartesian product $A \times B$ given by $(\varphi \times \nu)(a, b) = (\varphi(a), \nu(b))$ for all $(a, b) \in A \times B$.*

If φ and ν are skew morphisms of the groups A and B, then it is not always the case that $\varphi \times \nu$ is a skew morphism of $A \times B$, but there are some important and helpful situations where it is.

Lemma 7.2. *Let φ be any skew morphism of a finite group A, and let B be any finite group. Then φ can be extended to a skew morphism θ of the direct product $A \times B$, such that $\theta{\restriction_A} = \varphi$ and $\ker\theta = \ker\varphi \times B$. In particular, if φ is not an automorphism of A, then θ is not an automorphism of $A \times B$.*

Proof. Take $\theta = \varphi \times \iota$, where ι is the identity permutation on B, and let π be the power function associated with φ. Then for any $a, a' \in A$ and any $b, b' \in B$ we have

$$\theta((a,b)(a',b')) = \theta(aa', bb') = (\varphi(aa'), bb') = (\varphi(a)\varphi^{\pi(a)}(a'), bb')$$
$$= (\varphi(a), b)(\varphi^{\pi(a)}(a'), b') = \theta(a,b)\theta^{\pi(a)}(a', b'),$$

and it follows that θ is a skew morphism of $A \times B$, with power function ψ given by $\psi(a, b) = \pi(a)$ for all (a, b). Clearly $\ker\theta = \ker\varphi \times B$, and so in particular, $\ker\theta \neq A \times B$ if and only if $\ker\varphi \neq A$. □

In the other direction, we have the following generalisation of an easily-proved property of automorphisms of direct products of groups of coprime orders. This is originally due to Kovács and Nedela [13, Theorem 1.1], but we give a different (and much shorter) proof.

Theorem 7.3. *Let m and n be positive integers such that $\gcd(m,n) = \gcd(m,\phi(n)) = \gcd(\phi(m),n) = 1$. Then every skew morphism of the direct product group $C_m \times C_n$ ($\cong C_{mn}$) is of the form $\varphi \times \nu$, where φ and ν are skew morphisms of C_m and C_n.*

Proof. We use induction on mn. If $m = 1$ or $n = 1$ the claim is trivial, so now suppose $m, n > 1$. Let θ be any skew morphism of $A \times B$, where $A = C_m$ and $B = C_n$, which we will identify with the subgroups $A \times \{1\}$ and $\{1\} \times B$. Then the kernel K of θ is non-trivial (by Theorem 4.3), and since $A \times B$ is abelian we know that K is preserved by θ; indeed the restriction $\theta\restriction_K$ is an automorphism of K (by Theorem 5.1). Also K is cyclic, since $A \times B \cong C_{mn}$, and so K contains a subgroup N of prime order p that is preserved by θ. Moreover, since $\gcd(m,n) = 1$, we can assume without loss of generality that $N \subseteq A$.

By induction, the skew morphism θ^* induced by θ on $G/N \cong A/N \times B$ is of the form $\xi \times \nu$ where ξ and ν are skew morphisms of A/N and B, and in particular, θ^* preserves A/N and B. It follows that θ preserves A and $C = N \times B$.

We can now apply Lemma 5.3 to C and its θ-invariant subgroup N. If the kernel of $\theta\restriction_C$ is not C itself, then the order of $\theta\restriction_C$ is divisible by $p = |N|$. On the other hand, since p divides $|A| = m$, we know that p is coprime to $n\phi(n)$ and hence to the order of every skew morphism of B, by Theorem 6.1. In particular, p is coprime to the order k of the skew morphism of C/N induced by θ, and therefore p must divide the order of $(\theta\restriction_C)^k$, which means that $(\theta\restriction_N)^k = ((\theta\restriction_C)^k)\restriction_N$ is trivial. By part (g) of Theorem 5.3, we find that the power function of the skew morphism $(\theta\restriction_C)^k$ is a non-trivial homomorphism from C to $\mathbb{Z}_p^*$, the kernel of which contains N. But that is impossible, since $|C\!:\!N| = |B| = n$ is coprime to $\phi(m)$ and hence to $\phi(p)$. Thus $\ker(\theta\restriction_C) = C$, so $\theta\restriction_C$ is an automorphism of C. In particular, θ preserves all subgroups of C (since C is cyclic), and therefore preserves B.

We can now define $\varphi = \theta\restriction_A$ and $\nu = \theta\restriction_B$. If π is the power function of θ, then for each element $(a,b) \in A \times B$ we have

$$\theta(a,b) = \theta((a,1)(1,b)) = \theta(a,1)\theta^{\pi(a,1)}(1,b) = (\varphi(a),1)(1,\nu^{\pi(a,1)}(b)) = (\varphi(a),\nu^{\pi(a,1)}(b))$$

while on the other hand,

$$\theta(a,b) = \theta((1,b)(a,1)) = \theta(1,b)\theta^{\pi(1,b)}(a,1) = (1,\nu(b))(\varphi^{\pi(1,b)}(a),1) = (\varphi^{\pi(1,b)}(a),\nu(b)).$$

Hence $\nu^{\pi(a,1)}(b) = \nu(b)$ and $\varphi(a) = \varphi^{\pi(1,b)}(a)$, and more importantly, $\theta(a,b) = (\varphi(a),\nu(b))$ for all (a,b). Thus we have $\theta = \varphi \times \nu$, as claimed. □

Next, we consider two specific cases, before giving our main theorem on abelian groups.

Lemma 7.4. *The groups $C_2 \times C_4$ and $C_4 \times C_4$ both have a skew morphism with kernel of index 2.*

Proof. Again we note that such skew morphisms can be found using constructions given by the authors in [3], but we can give examples directly, as follows:

Let $\{a, b\}$ be generating pair for $V = C_2 \times C_4$, with a of order 2 and b of order 4, and let φ be the permutation (a, ab, ab^2, ab^3). Then φ is a skew morphism of order 4, with power function values 1 on $K = \langle b \rangle$, and 3 on Ka; in particular, $K = \ker \varphi$ has order 4.

Similarly, let $\{u, v\}$ be generating pair for $V = C_4 \times C_4$, and take φ to be the permutation $(v, uv, u^2v, u^3v)(v^3, uv^3, u^2v^3, u^3v^3)$. Then φ is a skew morphism of order 4, with power function values 1 on $K = \langle u, v^2 \rangle$, and 3 on Kv; in particular, $K = \ker \varphi$ has order 8. □

We complete this section with a generalisation of [13, Theorem 6.3], from finite cyclic groups to all finite abelian groups.

Theorem 7.5. *Let A be any finite abelian group. Then every skew morphism of A is an automorphism of A if and only if A is is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or A is an elementary abelian 2-group.*

Proof. First, for notational convenience, we will say that a finite group has property $\mathcal{N}$ if all of its skew morphisms are automorphisms, or (otherwise) property $\mathcal{S}$ if it has a skew morphism that is not an automorphism.

We now confirm that the abelian groups mentioned have property $\mathcal{N}$.

The group C_4 has just two skew morphisms, both of which are automorphisms, and we proved in Theorem 5.8 that every elementary abelian 2-group has property $\mathcal{N}$. Next suppose $\gcd(n, \phi(n)) = 1$. Then n is square-free, with prime factorisation $n = p_1 p_2 \dots p_k$ where the p_i are distinct primes such that $\gcd(p_i, \phi(p_j)) = 1$ whenever $i \neq j$. By Theorem 7.3 (and induction on k), every skew morphism of C_n is a direct product of skew morphisms of the cyclic groups $C_{p_1}, C_{p_2}, \dots, C_{p_k}$. Each C_{p_i} has property $\mathcal{N}$, so all these skew morphisms are automorphisms, and hence their direct product is too. Thus C_n has property $\mathcal{N}$.

To prove the converse, namely that these are the only such groups, suppose A is a direct product $C_{q_1} \times C_{q_2} \times \cdots \times C_{q_s}$ of cyclic groups of prime-power order, and let $n = |A|$.

If any one of the cyclic factors C_{q_i} has a skew morphism that is not an automorphism, then the construction in Lemma 7.2 will give a skew morphism of A that is not an automorphism, so we may suppose that none of the C_{q_i} has property $\mathcal{S}$. Then by Theorems 6.5 and 6.6, we know that each q_i is 2 or 4 or an odd prime.

Similarly, we may suppose the same holds for the direct product of each subset of the C_{q_i}.

If n is divisible by an odd prime p, then since $C_2 \times C_p \cong C_{2p}$ and $C_4 \times C_p \cong C_{4p}$ both have property $\mathcal{S}$ (by Theorem 6.5), we may suppose n is odd, and the q_i are odd primes. Similarly, because $C_p \times C_p$ has property $\mathcal{S}$ when p is an odd prime (by Theorem 5.10), we may suppose that no two of the q_i can be the same odd prime. Also by Theorem 6.2 we know that $C_p \times C_q \cong C_{pq}$ has property $\mathcal{S}$ whenever p and q are primes with $p < q$ and $\gcd(p, q-1) \neq 1$, and hence we may suppose $\gcd(q_i, \phi(q_j)) = \gcd(q_i, q_j - 1) = 1$ whenever i and j are distinct. Thus $\gcd(n, \phi(n)) = 1$ in this case.

The only remaining possibility is that each q_i is 2 or 4. Since $C_2 \times C_4$ and $C_4 \times C_4$ both have property $\mathcal{S}$ (by Lemma 7.4), we conclude that $A \cong C_4$ or $(C_2)^s$ in this case. □

Corollary 7.6. *Let G be any finite group expressible as a complementary product AB where A is abelian, and B is cyclic and core-free in G. If A is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or if A is an elementary abelian 2-group, then A is normal in G. Moreover, if A is any other finite abelian group, then there exists at least one such complementary product $G = AB$ in which A is not normal in G.*

8. Skew morphisms of dihedral groups

In this section, we consider the properties of a skew morphism φ of a dihedral group D_n (of order $2n$), with kernel $K = \ker \varphi$. Here we will take u and v as generators of D_n satisfying $u^2 = v^n = (uv)^2 = 1$, and use C_n to denote the maximal cyclic subgroup of order n and index 2, generated by v.

The first observation we make (below) grew out of some work in 2009 by the first author with Young Soo Kwon, motivated by the results of some early computations on skew morphisms of dihedral groups, which showed it is true for D_n for small n. It has also been observed more recently (but with a longer proof) by Zhang and Du [18].

Theorem 8.1. *If φ is a skew morphism of the dihedral group D_n, where $n \geq 3$, and $K = \ker \varphi$ is contained in C_n, then φ preserves K.*

Proof. First, we will assume that $n > 9$, because it can easily be shown with the help of Magma [1] that the theorem holds for $3 \leq n \leq 9$.

Next, we note that the restriction $\varphi\restriction_K$ of φ to K is an isomorphism from K to $\varphi(K)$. Also if $|K| > 2$, then K is the unique cyclic subgroup of its order in D_n, and so must be preserved by $\varphi\restriction_K$, and thus φ preserves K.

Hence from now on we may suppose $|K| = 2$, but that K is not preserved by φ. Then n is even, and K is generated by $z = v^{n/2}$, but $\varphi(z) \neq z$. Also $z' = \varphi(z)$ is an involution (since $\varphi\restriction_K$ is an isomorphism from K to $\varphi(K)$), and therefore $z' = \varphi(z) = v^j u$ for some j.

Let $\mathcal{O}$ be the orbit of z under φ. For any $g \in D_n$ we have $\varphi(zg) = \varphi(z)\varphi(g) = z'\varphi(g)$, while on the other hand, since z is central, $\varphi(zg) = \varphi(gz) = \varphi(g)\varphi^{\pi(g)}(z)$, and therefore $\varphi^{\pi(g)}(z) = \varphi(g)^{-1} z' \varphi(g)$. As g runs through the elements of D_n, so does $\varphi(g)$, and accordingly, the right hand side of the last equation runs through all conjugates of the non-central involution z' in D_n. It follows that the φ-orbit $\mathcal{O}$ of z contains all involutions of the form $v^i u$ where $i \equiv j \bmod 2$, and in particular, $|\mathcal{O}| \geq 1 + n/2$. Also the order m of φ is a multiple of $|\mathcal{O}|$, and must be less than $|D_n| = 2n$. Since $4|\mathcal{O}| \geq 4(1 + n/2) > 2n$, we conclude that $m = |\mathcal{O}|, 2|\mathcal{O}|$ or $3|\mathcal{O}|$.

Next, let x be any involution in the orbit $\mathcal{O}$ for which $\varphi(x)$ is also an involution. Then $1 = \varphi(x^2) = \varphi(x)\varphi^{\pi(x)}(x)$, so $\varphi^{\pi(x)}(x) = \varphi(x)^{-1} = \varphi(x)$, and therefore $\pi(x) \equiv 1 \bmod |\mathcal{O}|$. Moreover, since $m \leq 3|\mathcal{O}|$ it follows that $\pi(x) = r|\mathcal{O}| + 1$ where $r \in \{0, 1, 2\}$, and so x lies in one of at most three cosets of $K = \ker \varphi$. One of those cosets is K itself, containing 1 and z, while the others contain at most two possibilities for x, and so there are at most 5 possibilities for x. The φ-image of every other involution y in $\mathcal{O}$ must be a non-involution.

Now suppose $\mathcal{O}$ contains s possibilities for x, and t other involutions, so that $s \leq 5$ and $s+t \geq 1+n/2$. Then $\mathcal{O}$ contains at least t non-involutions (the φ-images of the possibilities for y above), and so $|\mathcal{O}| \geq s + 2t = 2(s+t) - s \geq 2 + n - s \geq n - 3$. Hence if $m = 3|\mathcal{O}|$, we have $m \geq 3(n-3) = 2n + n - 9 > 2n = |D_n|$, which is impossible, so $m = |\mathcal{O}|$ or $2|\mathcal{O}|$.

On the other hand, if $m = |\mathcal{O}|$, then the only possibility for x is z itself, in which case the φ-image of each of the $n/2$ conjugates of $z' = \varphi(z)$ is a non-involution, and we find that $|\mathcal{O}| \geq 1 + 2(n/2) = n + 1$. Moreover, if y is a conjugate of z' then zy is also an involution, but $\varphi(y)$ is not, so $\varphi(zy) = \varphi(z)\varphi(y) = z'\varphi(y)$ is an involution, and therefore zy cannot lie in $\mathcal{O}$. Hence $v^{n/2}y = zy$ is not conjugate to y, so $n/2$ is odd. Also $z'\varphi(y) = \varphi(zy)$ cannot lie in $\mathcal{O}$, so $\varphi(y) = v^t$ where t is odd, but $t \neq n/2$ (for otherwise $\varphi(y) = v^{n/2} = z \in \mathcal{O}$). It follows that there are only $n/2 - 1$ possibilities for $v^t = \varphi(y)$, but $n/2$ possibilities for y, contradiction.

Thus $m = 2|\mathcal{O}|$, and $s \leq 3$. Accordingly, we have $m = 2|\mathcal{O}| \geq 2(2 + n - s) \geq 2(n-1)$, and this forces $m = 2|\mathcal{O}| = 2n - 2$ and $|\mathcal{O}| = n - 1$. Indeed $s = 3$ (because if $s \leq 2$ then $m = 2|\mathcal{O}| \geq 2(2 + n - s) \geq 2n = |D_n|$), and it follows that $\mathcal{O}$ consists of z, plus the $n/2$ non-central involutions conjugate to z', and the φ-images of $n/2 - 2$ of the latter elements. The three possibilities for x must be z, w and zw for some non-central involution w.

If y is any involution in $\mathcal{O} \setminus \{z, w, zw\}$, then as above, zy is also an involution, but $\varphi(y)$ is not, so $\varphi(zy) = \varphi(z)\varphi(y) = z'\varphi(y)$ is an involution, and therefore zy cannot lie in $\mathcal{O}$. Hence zy is not conjugate to y, so $n/2$ is odd, and also $z'\varphi(y) = \varphi(zy) \notin \mathcal{O}$, and so $\varphi(y) = v^t$ where t is odd. Again there are $n/2 - 1$ possibilities for v^t $(= \varphi(y) \neq z)$, but only $n/2 - 2$ of them lie in $\mathcal{O}$, so exactly one of them lies outside $\mathcal{O}$, say v^i $(\neq z)$. The inverse v^{-i} of this element must lie in $\mathcal{O}$, and be the φ-image of some involution $y \in \mathcal{O}$, but then $1 = \varphi(yy) = \varphi(y)\varphi^{\pi(y)}(y) = v^{-i}\varphi^{\pi(y)}(y)$, and so $v^i = \varphi^{\pi(y)}(y) \in \mathcal{O}$, contradiction.

Thus φ preserves the kernel K, as claimed. □

Theorem 8.2. *If φ is a skew morphism of D_n, where $n \geq 3$, then* $\ker\varphi \neq C_n$.

Proof. Assume the contrary, and let $K = \ker\varphi = C_n$. Then by Theorem 8.1, we know that $\varphi(K) = K$, and therefore φ induces an automorphism of K. In particular, there exists some unit r mod n such that $\varphi(y) = y^r$ for every $y \in K$. But now let $x = \varphi(u)$. Then $x \in D_n \setminus C_n$, so x is an involution in D_n lying outside $K = C_n$; and then since $y \in \ker\varphi = K$, it follows that for all $y \in K$ we have $\varphi(yu) = \varphi(y)\varphi(u) = y^r x$. Hence $\varphi(v^i) = v^{ir}$ and $\varphi(v^i u) = v^{ir}x$ for $0 \leq i < n$. This, however, makes φ coincide with the automorphism of D_n that takes $v \mapsto v^r$ and $u \mapsto x$. In particular, φ is an automorphism (with kernel D_n), contradiction. Thus $\ker\varphi \neq C_n$. □

The above theorem has an immediate consequence for the theory of *t-balanced* skew morphisms, as considered in [3]. For $t \neq 1$, the kernel of any t-balanced skew morphism of a group A is a subgroup of index 2 in A, and Theorem 8.2 implies that if A is dihedral (of order 6 or more), then the kernel is not the maximal cyclic subgroup, so must be a dihedral subgroup of half the order of A. This observation, together with the classification in [14] of all t-balanced skew morphisms of the dihedral groups giving rise to regular Cayley maps,

could lead to a classification of *all* t-balanced skew morphisms of the dihedral groups (not just those giving rise to regular Cayley maps).

Before writing this paper, our computations for skew morphisms of the dihedral groups of small order led us to think that the kernel of a skew morphism of D_n (for $n \geq 3$) might never be a subgroup of C_n. This, however, is not the case. It was shown by Zhang and Du [18] that for every odd integer $m > 1$, the dihedral group D_{8m} (of order $16m$) has a skew morphism of order $4m$ with kernel a subgroup of index 2 in C_{8m}.

We noted earlier that the dihedral group D_3 of order 6 has skew morphisms of order 4 with kernel of order 2. In fact, there is a skew morphism of $D_3 = \langle\, u, v \mid u^2 = v^3 = (uv)^2 = 1 \,\rangle$ acting as the 4-cycle (u, v, v^2, uv), with kernel $\langle uv \rangle$. Somewhat surprisingly, this kind of skew morphism does not occur for dihedral groups of larger prime degree:

Theorem 8.3. *For every prime $p > 3$, every skew morphism of the dihedral group D_p is an automorphism.*

We have two proofs of this theorem. The first uses a theorem of Huppert on factorisations of groups as a product of an abelian subgroup and a dihedral subgroup, and the second is based on recent work on regular Cayley maps for dihedral groups by Kovács, Marušič and Muzychuk [12] (which uses a related theorem of Huppert and Itô).

Proof. Suppose φ is a skew morphism of $A = D_p = \langle\, u, v \mid u^2 = v^p = (uv)^2 = 1 \,\rangle$ that is not an automorphism. We know that the kernel $K = \ker \varphi$ is non-trivial, and that $K \neq A$ since φ is not an automorphism, and also by Theorem 8.2 (indeed by the first paragraph of its proof) that $|K| \neq p$. Thus $|K| = 2$. Without loss of generality we can now assume that K is generated by u, and again $\varphi(K)$ is a subgroup isomorphic to K, so $x = \varphi(u)$ is an involution. Moreover, the power function must take $|A : K| = p$ distinct values, so the order of φ is at least $p + 1$.

Next, let G be the skew product AY, where Y is a cyclic subgroup generated by y, representing the skew morphism φ (as described in Section 3). By a theorem of Huppert [6, Satz 1], any product of a dihedral group with an abelian group is soluble, and therefore $G = AY$ is soluble. Also by above, we know that $|Y| > p$, and on the other hand, by our Theorem 4.2, we know that $|Y| < |A| = 2p$, and so $p < |Y| < 2p$. In particular, $|Y|$ is not divisible by p, and it follows that the cyclic subgroup P generated by v is a Sylow p-subgroup of $G = AY$. The normaliser $N_G(P)$ contains $A = D_p$, so $|G : N_G(P)|$ divides $|Y|$, which is at most $2p$. On the other hand, $|G : N_G(P)|$ is the number n_p of Sylow p-subgroups of G, and by Sylow's third theorem, this is congruent to 1 mod p, and hence must be 1 or $p + 1$. But n_p cannot be 1, for otherwise P would be normal in G, and then P would be normalised by y, so P would lie in the kernel of φ, which is not the case. Thus $|G : N_G(P)| = n_p = p + 1$. Moreover, since $|G : N_G(P)|$ divides $|Y|$, which is at most $2p$, we find $|Y| = p + 1$ as well.

Thus φ has order $p + 1$, and the values of its power function on $A = D_p$ are $1, 2, \ldots, p$, in some order. Also $|G| = |A||Y| = 2p(p + 1)$.

Now let N be a minimal normal subgroup of G. Then N is characteristically simple, and as G is soluble, N is elementary abelian. If N intersects A non-trivially, then $A \cap N$ is a non-trivial normal subgroup of A and hence has order p, and since $\gcd(p, 2(p+1)) = 1$ it follows that $N = P$, which is impossible since P is not normal in G. Thus $A \cap N$ is trivial. In particular, $|AN/N| = |A/(A \cap N)| = |A|$. Also the fact that $|AN/N| = |A| = 2p$ implies that the normaliser of PN/N in G/N has order divisible by $2p$, and hence its index in G/N is at most the index of AN/N in G/N, which is $|G/N|/(2p) = (p+1)/|N|$. In particular, this implies that $|N|$ divides $p+1$.

This also implies that in the quotient G/N, the index of the normaliser of the cyclic Sylow p-subgroup PN/N is at most $(p+1)/2$. It follows that G/N has a unique normal Sylow p-subgroup, which must be PN/N. In particular, PN is normal in G. On the other hand, P cannot be normal in PN, for otherwise P would be the unique Sylow p-subgroup of PN, and would then be characteristic in PN and therefore normal in G, which is a contradiction. Thus $|N| > p$, and it follows that $|N| = p+1$ (since we already know that $|N|$ divides $p+1$). In particular, $p+1$ is a prime-power, and since p is odd, $p+1$ must be a power of 2, so N is an elementary abelian 2-group. Since Y is cyclic, this implies $|Y \cap N| \leq 2$, and hence the subgroup YN has order $|YN| = |Y||N|/|Y \cap N| = (p+1)^2$ or $(p+1)^2/2$. Since this is coprime to p, but has to divide $|G| = 2p(p+1)$, we find that $(p+1)^2/2$ divides $2(p+1)$, and hence $p+1$ divides 4. Thus $p = 3$.

In other words, if $p > 3$ then no such skew morphism exists. □

Alternative proof. Let φ be any non-trivial skew morphism of D_p, with power function π. Now if φ fixes every involution in D_p, then $\varphi(v^i) = \varphi(uuv^i) = \varphi(u)\varphi^{\pi(u)}(uv^i) = u(uv^i) = v^i$ for $1 \leq i < p$, and so φ fixes all elements of D_p, contradiction. Hence there is at least one orbit X of φ on D_p of length greater than 1 containing an involution. If this orbit X contains an element of order p, then these two elements generate D_p, so X generates D_p. Similarly, if X contains another involution, then the product of these two involutions is an element of order p, and hence X generates D_p. Also by a standard argument, X is closed under taking inverses, since it contains an involution x: if $y = \varphi^i(x)$, then by Lemma 2.1(a), we have $1 = \varphi^i(1) = \varphi^i(xx) = \varphi^i(x)\varphi^{\sigma(i,x)}(x)$ and so $y^{-1} = (\varphi^i(x))^{-1} = \varphi^{\sigma(i,x)}(x) \in X$.

Thus X generated D_p and is closed under inverses, and by the theory described briefly in Section 2, it follows that there exists a regular Cayley map $M = \mathrm{CM}(D_p, X, \rho)$ for D_p in which ρ is the restriction of φ to X.

Finally, the regular Cayley maps for dihedral groups of odd degree have been classified, by Kovács, Marušič and Muzychuk. In particular, it follows from [12, Theorem 3.2 and Corollary 3.3] that for each odd integer $n > 1$ not divisible by 3, every regular Cayley map for D_n is *balanced*, which means that the corresponding skew morphism of D_n is an automorphism. Thus φ is an automorphism of D_p, as required. □

We believe Theorem 8.3 can be generalised. It might even be true that every skew morphism of D_n is an automorphism, whenever n is an odd integer not divisible by 3. We leave this as an open question.

9. The skew morphism group of a group

Let us define $\mathrm{Skew}(A)$ as the set of all skew morphisms of A, and $\mathrm{SkewGroup}(A)$ as the group generated by these, considered as a subgroup of $\mathrm{Sym}(A)$. We may call $\mathrm{SkewGroup}(A)$ the *skew morphism group* of A.

We have already seen that in some cases, $\mathrm{SkewGroup}(A) = \mathrm{Skew}(A) = \mathrm{Aut}(A)$. For example, this happens for the abelian groups given in Theorem 7.5, and for dihedral groups of prime degree $p > 3$. In other cases, however, $|\mathrm{SkewGroup}(A)| > |\mathrm{Skew}(A)| > |\mathrm{Aut}(A)|$.

The group C_6 has four skew morphisms, only two of which are automorphisms, and they generate a subgroup of $\mathrm{Sym}(C_6)$ of order 6, isomorphic to D_3. On the other hand, D_3 has 12 skew morphisms, only 6 of which are automorphisms, and the skew morphisms generate a subgroup of $\mathrm{Sym}(D_3)$ of order 120, isomorphic to S_5. Similarly, C_8 has 4 automorphisms but 6 skew morphisms, generating a group of order 8, isomorphic to D_4, while $C_4 \times C_2$ has 8 automorphisms but 16 skew morphisms, generating a group of order 5040, isomorphic to S_7. Also C_9 has 10 skew morphisms, of which 6 are automorphisms, and the skew morphisms generate a group of order 18, and $C_3 \times C_3$ has 48 automorphisms but 64 skew morphisms, which generate a group of order 40320, isomorphic to S_8.

Remarkably, we have not found an example of a finite group A for which the set $\mathrm{Skew}(A)$ itself is a group, when $\mathrm{Skew}(A)$ is larger than $\mathrm{Aut}(A)$. In other words, the only A for which we know $\mathrm{Skew}(A)$ is a group are those for which $\mathrm{Skew}(A) = \mathrm{Aut}(A)$. This creates another open question worth further investigation.

Finally, we prove the following analogue of the fact that the automorphism group of every cyclic group is abelian.

Theorem 9.1. *If A is a finite cyclic group, then* $\mathrm{SkewGroup}(A)$ *is soluble.*

Proof. We let $S = \mathrm{SkewGroup}(A)$, and use induction on $|A|$. If $|A|$ is prime, then by Corollary 4.4 we know that $S = \mathrm{Skew}(A) = \mathrm{Aut}(A)$, which is cyclic, and so we may suppose that A has composite order.

Let q be the largest prime divisor of $|A|$, and let J be the unique subgroup of A of order q. If φ is any skew morphism of A, then by Corollary 5.7, the order of $K = \ker \varphi$ is divisible by q, and so K contains J. Moreover, since φ preserves K, it follows that φ preserves J.

Now let N be the subgroup of S generated by all skew morphisms of A that fix J elementwise. This is the kernel of the action of S on J (which takes every skew morphism φ of A to the automorphism it induces on J), and so N is normal in S. Also S/N is isomorphic to a subgroup of $\mathrm{Aut}(J)$, and therefore S/N is abelian.

Next, we show N is soluble.

To do this, we first note that every skew morphism φ of A preserves the partition of A into cosets of J (for if $\varphi(x) = y$ then $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)y \in Jy$ for all $a \in J$), and induces a skew morphism of A/J. It follows that S can be regarded as a subgroup of the wreath product of $\mathrm{Sym}(J)$ by $T = \mathrm{SkewGroup}(A/J)$. Since the latter can be regarded as

a permutation group on the set of $|A:J|$ cosets of J in A, we find that S is an imprimitive subgroup of $\mathrm{Sym}(A)$, with $|A:J|$ blocks of imprimitivity, each of size $|J|$.

Also let R be the regular group of permutations of J induced by J on itself by multiplication, and let G be the wreath product $R \operatorname{wr} T$. This is isomorphic to the semi-direct product of $R^{|A:J|}$ $(= R \times R \times \cdots \times R)$ by T. We claim that N is isomorphic to a subgroup of G. For suppose that φ and ν are two elements of N that induce the same permutation on the cosets of J. For any such coset Jx, let Jy be its image under φ. Then without loss of generality φ takes x to y, and so takes ax to $\varphi(a)\varphi(x) = ay$ (since $\varphi \in N$ fixes J), for all a in J. Similarly, ν takes x to cy for some $c \in J$, and so ν takes ax to $acy = c(ay)$ for all $a \in J$. It follows that $(\nu\varphi^{-1})(ay) = \nu(ax) = c(ay)$, and thus $\nu\varphi^{-1}$ induces multiplication by c on the coset Jy. This proves the claim.

But now since $|R| = |J| = q$, the base group $R^{|A:J|} = R \times R \times \cdots \times R$ is an elementary abelian q-group. Also by induction, $T = \mathrm{SkewGroup}(A/J)$ is soluble. It follows that $G = R \operatorname{wr} T$ is soluble, and hence N is soluble.

Thus N is soluble, and S/N is abelian, and therefore S is soluble. □

Acknowledgments

Some very helpful evidence in support of many of the theorems presented in this paper was provided by computations using the Magma system [1].

The first author was supported by a James Cook Fellowship from the Royal Society of New Zealand, and by the Marsden Fund (grant UOA1323). The second author acknowledges support from the projects VEGA 1/0577/14, VEGA 1/0474/15 and NSFC 11371307 and also from the project 'Mobility - Enhancing Research, Science and Education' at Matej Bel University (ITMS code: 26110230082), under the Operational Program Education co-financed by the European Social Fund. The third author is supported by a 5-year grant from the Simons Foundation (grant 317689).

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language, *J. Symbolic Comput.* 24 (1997), 235–265.
[2] M. Conder, R. Jajcay, and T. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebraic Combin.* 25 (2007), 259–283.
[3] M. Conder, R. Jajcay, and T. Tucker, Regular t-balanced Cayley maps, *J. Combin. Theory Ser. B* 97 (2007), 453–473.
[4] M. Conder and T. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.*, to appear.
[5] M. Herzog and G. Kaplan, Large cyclic subgroups contain non-trivial normal subgroups, *J. Group Theory* 4 (2001), 247–253.
[6] B. Huppert, Über die Auflösbarkeit faktorisierbarer Gruppen, *Math. Zeitschrift* 59 (1953), 1–7.
[7] M.V. Horoševskiĭ, Automorphisms of finite groups, *Math. USSR Sbornik* 22 (1974), 584–594.
[8] N. Ito, Über das Produkt von zwei abelschen Gruppen, *Math. Z.* 62 (1955), 400–401.

[9] R. Jajcay, On a new product of groups, *European J. Combin.* 15 (1994), 251–252.
[10] R. Jajcay and R. Nedela, Half-regular Cayley maps, to appear in *Graphs and Combinatorics.*
[11] R. Jajcay and J.Širáň, Skew morphisms of regular Cayley maps, *Discrete Math.* 244 (2002), 167–179.
[12] I. Kovács, D. Marušič and M. Muzychuk On G-arc-regular dihedrants and regular dihedral maps, *J Algebr. Comb.* 38 (2013), 437–455.
[13] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars Math. Contemp.* 4 (2011), 329–349.
[14] J.H. Kwak, Y.S. Kwon and R. Feng, A classification of regular t-balanced Cayley maps on dihedral groups, *European J. Combin.* 27 (3) (2006), 382–392.
[15] 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.
[16] O. Ore, On the application of structure theory to groups, *Bull. Am. Math. Soc.* 44 (1938), 801–806.
[17] R.B. Richter, R. Jajcay, J. Širáň, T.W. Tucker, and M.E. Watkins, Cayley maps, *J. Combin. Theory Ser. B* 95 (2005), 189–245.
[18] J.-Y. Zhang and S.-F. Du, On the skew-morphisms of dihedral groups, submitted manuscript.

Marston D.E. Conder, Department of Mathematics, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

E-mail address: m.conder@auckland.ac.nz

Robert Jajcay, Faculty of Mathematics, Physics and Computer Science, Comenius University, Bratislava, Slovakia

E-mail address: robert.jajcay@fmph.uniba.sk

Thomas W. Tucker, Emeritus Professor, Mathematics Department, Colgate University, Hamilton, NY 13346, U.S.A.

E-mail address: ttucker@colgate.edu