ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 16 (2019) 527–547
https://doi.org/10.26493/1855-3974.1475.3d3
(Also available at http://amc-journal.eu)

Smooth skew morphisms of dihedral groups*

Na-Er Wang , Kan Hu

Department of Mathematics, Zhejiang Ocean University, Zhoushan, Zhejiang 316022, P.R. China and
Key Laboratory of Oceanographic Big Data Mining & Application of Zhejiang Province, Zhoushan, Zhejiang 316022, P.R. China

Kai Yuan

School of Mathematics, Capital Normal University, Beijing 100037, P.R. China

Jun-Yang Zhang

School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, P.R. China

Received 4 September 2017, accepted 17 January 2019, published online 28 March 2019

Abstract

A skew morphism φ of a finite group A is a permutation on A fixing the identity element of A and for which there exists an integer-valued function π on A such that $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in A$. In the case where $\pi(\varphi(a)) = \pi(a)$, for all $a \in A$, the skew morphism is smooth. The concept of smooth skew morphism is a generalization of that of t-balanced skew morphism. The aim of this paper is to develop a general theory of smooth skew morphisms. As an application we classify smooth skew morphisms of dihedral groups.

Keywords: Cayley map, skew morphism, smooth subgroup.

Math. Subj. Class.: 05E18, 20B25, 05C10

*The authors are grateful to the anonymous referees for their helpful comments and suggestions which have improved the content and presentation of the paper. This research was supported by the following grants: Zhejiang Provincial Natural Science Foundation of China (No. LY16A010010, LQ17A010003); National Natural Science Foundation of China (No. 11801507, 11671276); Teacher Professional Development Program of Zhejiang Provincial Education Department (No. FX2017029); Basic Research and Frontier Exploration Project of Chongqing (No. cstc2018jcyjAX0010); Science and Technology Research Program of Chongqing Municipal Education Commission (No. KJQN201800512); Natural Science Foundation of Fujian (No. 2016J01027).

E-mail addresses: wangnaer@zjou.edu.cn (Na-Er Wang), hukan@zjou.edu.cn (Kan Hu), pktide@163.com (Kai Yuan), jyzhang@cqnu.edu.cn (Jun-Yang Zhang)

1 Introduction

Throughout the paper all groups considered are finite, unless stated otherwise. A *skew morphism* φ of a finite group A is a bijection on the underlying set of A fixing the identity element of A and for which there exists an integer-valued function $\pi\colon A \to \mathbb{Z}$ such that $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$, for all $a, b \in A$. Note that π is not uniquely determined by φ, however, as a permutation if φ has order n, then π can be viewed as a function $\pi\colon A \to \mathbb{Z}_n$. In this sense the function π is uniquely determined by φ, and it will be called *the power function* of φ.

Jajcay and Širáň introduced the concept of skew morphism as an algebraic tool to investigate regular Cayley maps [10]. Conder, Jajcay and Tucker have shown in [5] that skew morphisms are also closely related to group factorisations with a cyclic complement. Thus the study of skew morphisms is important for both combinatorics and algebra.

Let X be a generating set of a group A such that $1 \notin X$ and $X = X^{-1}$, let P be a cyclic permutation of X. A *Cayley map* $M = \mathrm{CM}(A, X, P)$ is a 2-cell embedding of the Cayley graph $\mathrm{Cay}(A, X)$ into an orientable closed surface such that the local cyclic orientation of the arcs (g, x) emanating from any vertex g induced by the orientation of the supporting surface agrees with the prescribed cyclic permutation P of X. An automorphism of M is an automorphism of the underlying Cayley graph which extends to an orientation-preserving self-homeomorphism of the supporting surface. It is well known that the automorphism group $\mathrm{Aut}(M)$ of M acts semi-regularly on the arcs of M. In the case where this action is transitive, and hence regular, the map M is called a *regular Cayley map*. The left regular representation of A induces a subgroup of map automorphisms which acts transitively on the vertices of M. It follows that M is regular if and only if M admits an automorphism which fixes a vertex, say the identity vertex 1, and maps the arc $(1, x)$ to $(1, P(x))$. It is a nontrivial result proved by Jajcay and Širáň that a Cayley map $\mathrm{CM}(A, X, P)$ is regular if and only if there is a skew morphism φ of A such that the restriction $\varphi\restriction_X$ of φ to X is equal to P [10, Theorem 1]. A skew morphism of A will be called a *Cayley skew morphism* if it has an inverse-closed generating orbit. Thus the study of regular Cayley maps of a group A is equivalent to the study of Cayley skew morphisms of A.

Among the variety of problems considered with regard to skew morphisms the most important seems to be the classification of regular Cayley maps for given families of groups. This problem is completely settled for cyclic groups [6], and only partial results are known for other abelian groups [4, 5, 23]. For dihedral groups D_n of order $2n$, if n is odd this problem was solved in [14], whereas if n is even only partial classification is at hand [11, 12, 17, 21, 24, 25]. For other non-abelian groups the interested reader is referred to [18, 20, 21].

Although skew morphisms are usually investigated along with regular Cayley maps, they also deserve to be studied independently in a purely algebraic setting. Let $G = AC$ be a group factorisation, where A and C are subgroups of G with $A \cap C = 1$. If $C = \langle c \rangle$ is cyclic, then the commuting rule $ca = \varphi(a)c^{\pi(a)}$, for all $a \in A$, determines a skew morphism φ of A with the associated power function π. Conversely, each skew morphism φ of A determines a group factorisation $L_A\langle\varphi\rangle$ with $L_A \cap \langle\varphi\rangle = 1$, where L_A denotes the left regular representation of A [5, Proposition 3.1]. Thus, there is a correspondence between skew morphisms and group factorisations with cyclic complements.

Let φ be a skew morphism of a group A. A subgroup N of A is *φ-invariant* if $\varphi(N) = N$. Note that the restriction of φ to N is a skew morphism of N, so it is important to study φ-invariant subgroups. The first important φ-invariant subgroup is $\mathrm{Fix}\,\varphi$, the subgroup consisting of fixed points of φ [10]. Later, Zhang discovered in [25]

another important φ-invariant subgroup, called the *core* of φ and denoted by $\operatorname{Core}\varphi$. This is a normal subgroup of A, so φ induces a skew morphism $\bar{\varphi}$ of the quotient group $\bar{A} := A/\operatorname{Core}\varphi$ in a natural way. As a consequence, we obtain a new φ-invariant subgroup $\operatorname{Smooth}\varphi = \{a \in A \mid \bar{a} \in \operatorname{Fix}\bar{\varphi}\}$ by means of coverings of skew morphisms; see Section 3.

Section 4 is devoted to a study of the extremal case where $\operatorname{Smooth}\varphi = A$. In this case the skew morphism φ is termed *smooth*. We prove that a skew morphism φ of A is smooth if and only if $\pi(\varphi(a)) = \pi(a)$ for all $a \in A$. It follows that the power function of a smooth skew morphism takes constant value on orbits of φ, so smooth skew morphisms may be viewed as a generalization of t-balanced Cayley skew morphisms studied in [4]. Note that for abelian groups smooth skew morphisms are identical with the *coset-preserving* skew morphisms studied by Bachratý and Jajcay in [1]. We establish in Theorems 4.5 and 4.9 an unexpected relationship between smooth skew morphisms and kernel-preserving skew morphisms. Note that a skew morphism φ of A is *kernel-preserving* if its kernel $\operatorname{Ker}\varphi$ is a φ-invariant subgroup of A.

Kovács and Kwon [13] have recently announced a complete classification of regular Cayley maps of dihedral groups. Thus, to complete the classification of skew morphisms of dihedral groups, it remains to determine the non-Cayley skew morphisms. As shown in [8], every non-Cayley skew morphism of dihedral groups is smooth. Our last aim of this paper is to employ the newly-developed theory to give a classification of smooth skew morphisms of the dihedral groups, see Section 5.

2 Preliminaries

In this section we summarize some basic results concerning skew morphisms which will be used throughout the paper.

Let φ be a skew morphism of a group A, let π be the power function of φ, and let n be the order of φ. As already mentioned above, the sets

$$\operatorname{Ker}\varphi = \{a \in A \mid \pi(a) = 1\}, \qquad \operatorname{Fix}\varphi = \{a \in A \mid \varphi(a) = a\}$$

and

$$\operatorname{Core}\varphi = \bigcap_{i=1}^{n} \varphi^i(\operatorname{Ker}\varphi)$$

form subgroups of A. Note that, for any two elements $a, b \in A$, $\pi(a) = \pi(b)$ if and only if $ab^{-1} \in \operatorname{Ker}\varphi$. Thus, the index $|A : \operatorname{Ker}\varphi|$ is equal to the number of distinct values of the power function. This number is called the *skew type* of φ, and it is strictly less than n if φ is not trivial. Clearly, φ is an automorphism of A if and only if it has skew type 1. If φ is not an automorphism, then it will be termed *proper*. On the other hand, $\operatorname{Core}\varphi$ is the largest φ-invariant subgroup contained in $\operatorname{Ker}\varphi$, and in particular, it is normal in A [25].

Lemma 2.1 ([10]). *Let φ be a skew morphism of a group A, let π be the power function of φ, and let n be the order of φ. Then, for any $a, b \in A$,*

$$\varphi^k(ab) = \varphi^k(a)\varphi^{\sigma(a,k)}(b) \qquad \textit{and} \qquad \pi(ab) \equiv \sigma(b, \pi(a)) \pmod{n},$$

where k is an arbitrary positive integer and $\sigma(a,k) = \sum_{i=1}^{k} \pi(\varphi^{i-1}(a))$.

Lemma 2.2 ([7]). *Let φ be a skew morphism of a group A, let π be the power function of φ. Then for any automorphism γ of A, $\psi = \gamma^{-1}\varphi\gamma$ is a skew morphism of A with power function $\pi_\psi = \pi\gamma$. Moreover,* $\operatorname{Ker}\psi = \gamma^{-1}(\operatorname{Ker}\varphi)$ *and* $\operatorname{Core}\psi = \gamma^{-1}(\operatorname{Core}\varphi)$.

Proof. Since γ is an automorphism of A, for any $a, b \in A$, we have

$$\begin{aligned}\psi(ab) &= \gamma^{-1}\varphi\gamma(ab) = \gamma^{-1}\varphi(\gamma(a)\gamma(b)) = \gamma^{-1}\big(\varphi(\gamma(a))\varphi^{\pi\gamma(a)}(\gamma(b))\big)\\ &= \gamma^{-1}\varphi\gamma(a)\gamma^{-1}\varphi^{\pi\gamma(a)}\gamma(b) = \psi(a)\psi^{\pi\gamma(a)}(b).\end{aligned}$$

Thus, ψ is a skew morphism of A with power function $\pi_\psi = \pi\gamma$. Since $|\psi| = |\varphi|$, we have

$$\begin{aligned}a \in \operatorname{Ker}\psi \iff \pi_\psi(a) \equiv 1 \pmod{|\psi|} \iff\\ \pi\gamma(a) \equiv 1 \pmod{|\varphi|} \iff a \in \gamma^{-1}(\operatorname{Ker}\varphi).\end{aligned}$$

Therefore, $\operatorname{Ker}\psi = \gamma^{-1}(\operatorname{Ker}\varphi)$. Similarly, $\operatorname{Core}\psi = \gamma^{-1}(\operatorname{Core}\varphi)$. □

Lemma 2.3 ([1, 5]). *Let φ be a skew morphism of a group A, let π be the power function of φ, and let n be the order of φ. Then for any positive integer k, $\mu = \varphi^k$ is a skew morphism of A if and only if the congruences*

$$kx \equiv \sigma(a,k) \pmod{n} \tag{2.1}$$

are solvable for all $a \in A$. Moreover, if μ is a skew morphism of A, then it has order $m = n/\gcd(n,k)$ and for each $a \in A$, $\pi_\mu(a)$ is the solution of the equation (2.1) in $\mathbb{Z}_m$.

Lemma 2.4 ([5]). *Let φ be a skew morphism of a group A. If A is nontrivial, then $|\varphi| \le |A|$ and $|\operatorname{Ker}\varphi| > 1$.*

Lemma 2.5 ([9]). *Let φ be a skew morphism of a group A, and let O_a denote the orbit of φ containing the element $a \in A$. Then for each $a \in A$, $O_{a^{-1}} = O_a^{-1}$, where $O_a^{-1} = \{g^{-1} \mid g \in O_a\}$.*

The following result was partially obtained for Cayley skew morphisms in [4].

Lemma 2.6 ([7]). *Let φ be a skew morphism of a group A, and let π the power function of φ, and let n be the order of φ. Then for any $a \in A$,*

$$\sigma(a,m) \equiv 0 \pmod{m},$$

where $m = |O_a|$ is length of the orbit O_a containing a. Moreover, $\sigma(a,n) \equiv 0 \pmod{n}$.

Proof. By Lemma 2.1, we have

$$1 = \varphi^m(aa^{-1}) = \varphi^m(a)\varphi^{\sigma(a,m)}(a^{-1}) = a\varphi^{\sigma(a,m)}(a^{-1}),$$

so $\varphi^{\sigma(a,m)}(a^{-1}) = a^{-1}$. By Lemma 2.5, $m = |O_{a^{-1}}|$. Thus, $\sigma(a,m) \equiv 0 \pmod{m}$. Since m divides n, we obtain

$$\sigma(a,n) = \sum_{i=1}^{n} \pi(\varphi^{i-1}(a)) = \frac{n}{m}\sigma(a,m) \equiv 0 \pmod{n},$$

as required. □

Lemma 2.7 ([7]). *Let φ be a skew morphism of a group A. Then for any $a, b \in A$, $|O_{ab}|$ divides* $\operatorname{lcm}(|O_a|, |O_b|)$.

Proof. Denote $c = |O_a|$, $d = |O_b|$ and $\ell = \operatorname{lcm}(|O_a|, |O_b|)$. Then $\ell = cp = dq$ for some positive integers p, q. By Lemma 2.1, we have $\varphi^\ell(ab) = \varphi^\ell(a)\varphi^{\sigma(a,\ell)}(b) = a\varphi^{\sigma(a,\ell)}(b)$. By Lemma 2.6,

$$\sigma(a,\ell) = \sum_{i=1}^{\ell} \pi(\varphi^{i-1}(a)) = p\sum_{i=1}^{c} \pi(\varphi^{i-1}(a)) = p\sigma(a,c) \equiv 0 \pmod{\ell}.$$

Thus, $\varphi^\ell(ab) = ab$, and consequently, $|O_{ab}|$ divides ℓ. □

Lemma 2.8. *Let φ be a skew morphism of a group A, and let π the power function of φ, and let n be the order of φ. If $A = \langle a_1, \ldots, a_r\rangle$, then $n = \operatorname{lcm}(|O_{a_1}|, \ldots, |O_{a_r}|)$. Moreover, for any $g \in A$, $\varphi(g)$ and $\pi(g)$ are completely determined by the action of φ and the values of π on the generating orbits $O_{a_1}, \ldots, O_{a_r}$.*

Proof. The first part was first proved in [26, Lemma 3.1]. The reader is invited to give an alternative proof using Lemma 2.7 (and induction on the length of words in the generators).

To prove the second part we use induction on the length k of g in the generators. If $k = 1$ then g is a generator of A, the assertion is trivially true. Assume that the assertion is true for words of length k. Then, for a word g of length $k+1$, we have $g = ha$, where h is a word of length k and $a \in \{a_1, \ldots, a_r\}$. By Lemma 2.1, we have

$$\varphi(g) = \varphi(ha) = \varphi(h)\varphi^{\pi(h)}(a) \quad \text{and} \quad \pi(g) \equiv \pi(ha) \equiv \sum_{i=1}^{\pi(h)} \pi(\varphi^{i-1}(a)) \pmod{n}.$$

Since $\varphi(h)$ and $\pi(h)$ are completely determined by the action of φ and the values of π on the generating orbits, so are $\varphi(g)$ and $\pi(g)$, as required. □

Lemma 2.9. *Let φ be a skew morphism of a group A, let π the power function of φ, and let n be the order of φ. If N is a φ-invariant normal subgroup of A, then*

(a) φ induces a skew morphism $\bar\varphi$ of $\bar A = A/N$ by defining $\bar\varphi$ as $\bar\varphi(\bar a) = \overline{\varphi(a)}$ and the power function $\bar\pi\colon \bar A \to \mathbb{Z}_m$ associated with $\bar\varphi$ is determined by $\bar\pi(\bar a) \equiv \pi(a) \pmod m$ where $m = |\bar\varphi|$,

(b) $\operatorname{Ker}\varphi N/N \le \operatorname{Ker}\bar\varphi$, $\operatorname{Core}\varphi N/N \le \operatorname{Core}\bar\varphi$ *and* $\operatorname{Fix}\varphi N/N \le \operatorname{Fix}\bar\varphi$.

Proof. The proof of (a) can be found in [26, Lemma 3.3] while (b) is obvious. □

3 Invariant subgroups

In this section, we introduce covering techniques to the study of skew morphisms and define several new invariant subgroups.

Proposition 3.1. *Let φ be a skew morphism of a group A. If M and N are φ-invariant subsets of A, so are $M \cap N$ and MN.*

Proof. For any $y \in \varphi(M \cap N)$, there exists $x \in M \cap N$ such that $y = \varphi(x)$. Since M and N are both φ-invariant, $\varphi(x) \in M$ and $\varphi(x) \in N$, so $y \in M \cap N$, whence $\varphi(M \cap N) = M \cap N$. Therefore $M \cap N$ is also φ-invariant. Similarly for any $y \in \varphi(MN)$, there exist $u \in M$ and $v \in N$ such that $y = \varphi(uv)$. We have $y = \varphi(uv) = \varphi(u)\varphi^{\pi(u)}(v) \in \varphi(M)\varphi(N) = MN$, so $\varphi(MN) = MN$, whence MN is also φ-invariant. □

Let Π be a finite set of primes, a positive integer k will be called a Π-*number* if all prime factors of k belong to Π. For instance, if $\Pi = \{2, 3\}$, then $2, 6, 9$ are Π-numbers, whereas $5, 10, 30$ are not. We define 1 to be a Π-number for any set Π of primes.

Now let φ be a skew morphism of a group A. An orbit of φ will be called a Π-*orbit* if its length is a Π-number. Define $\mathrm{Orbit}^{\Pi}\varphi$ to be the union of all Π-orbits of φ, namely,

$$\mathrm{Orbit}^{\Pi}\varphi = \{a \in A \mid |O_a| \text{ is a } \Pi\text{-number}\}.$$

Proposition 3.2. *Let φ be a skew morphism of A, and let Π be a finite set of primes, then $\mathrm{Orbit}^{\Pi}\varphi$ is a φ-invariant subgroup of A containing $\mathrm{Fix}\,\varphi$.*

Proof. By definition, all fixed points of φ belong to $\mathrm{Orbit}^{\Pi}\varphi$, so $\mathrm{Orbit}^{\Pi}\varphi$ is not empty. Moreover, for any $a, b \in \mathrm{Orbit}^{\Pi}\varphi$, $|O_a|$ and $|O_b|$ are Π-numbers, so $\mathrm{lcm}(|O_x|, |O_y|)$ is also a Π-number. By Lemma 2.7, $|O_{ab}|$ divides $\mathrm{lcm}(|O_a|, |O_b|)$. It follows that $|O_{ab}|$ is also a Π-number. Hence, $ab \in \mathrm{Orbit}^{\Pi}\varphi$. Therefore, $\mathrm{Orbit}^{\Pi}\varphi$ is a subgroup of A, which is clearly φ-invariant. □

Example 3.3. Consider the skew morphism of the cyclic group $\mathbb{Z}_{21}$ defined by

$$\varphi = (0)\,(1, 2, 4, 8, 16, 11)\,(3, 6, 12)\,(5, 10, 20, 19, 17, 13)\,(7, 14)\,(9, 18, 15).$$

This is an automorphism of $\mathbb{Z}_{21}$. We have

$$\mathrm{Orbit}^{\{2\}}\varphi = \langle 7\rangle, \quad \mathrm{Orbit}^{\{3\}}\varphi = \langle 3\rangle, \quad \mathrm{Orbit}^{\{5\}}\varphi = \langle 0\rangle, \quad \text{and} \quad \mathrm{Orbit}^{\{2,3\}}\varphi = \mathbb{Z}_{21}.$$

Now we introduce covering techniques to the study of skew morphisms.

Definition 3.4. Let φ_i be skew morphisms of finite groups A_i, $i = 1, 2$. If there is an epimorphism $\theta\colon A_1 \to A_2$ such that the identity

$$\theta\varphi_1(a) = \varphi_2\theta(a)$$

holds for all $a \in A_1$, then φ_1 will be called a *covering* (or a lift) of φ_2, and φ_2 will be called a *projection* (or a quotient) of φ_1. The covering will be denoted by $\varphi_1 \to \varphi_2$, and the epimorphism $\theta\colon A_1 \to A_2$ will be said to be associated with the covering.

Lemma 3.5. *Let $\varphi_1 \to \varphi_2$ be a covering between skew morphisms φ_i of groups A_i, $i = 1, 2$, and let $\theta\colon A_1 \to A_2$ be the associated epimorphism. Then*

(a) every φ_1-invariant subgroup M of A_1 projects to a φ_2-invariant subgroup $\theta(M)$ of A_2,

(b) every φ_2-invariant subgroup N of A_2 lifts to a φ_1-invariant subgroup $\theta^{-1}(N)$ of A_1.

Proof. (a): For any $y \in \theta(M)$, $y = \theta(x)$ for some $x \in M$. Since M is φ_1-invariant, $\varphi_1(x) \in M$, so $\varphi_2(y) = \varphi_2\theta(x) = \theta\varphi_1(x) \in \theta(M)$, whence $\theta(M)$ is φ_1-invariant.

(b): For any $x \in \theta^{-1}(N)$, $y = \theta(x) \in N$. Since N is φ_2-invariant, $\varphi_2(y) \in N$, so $\theta\varphi_1(x) = \varphi_2\theta(x) = \varphi_2(y) \in N$. Hence $\varphi_1(x) \in \theta^{-1}(N)$. □

Since $\{1\}$, $\mathrm{Fix}\,\varphi_2$ and $\mathrm{Core}\,\varphi_2$ are all φ_2-invariant subgroups of A_2, by Lemma 3.5, $\mathrm{Ker}\,\theta = \theta^{-1}(1)$, $\theta^{-1}(\mathrm{Fix}\,\varphi_2)$ and $\theta^{-1}(\mathrm{Core}\,\varphi_2)$ are all φ_1-invariant subgroups of A_1. In particular, both $\mathrm{Ker}\,\theta$ and $\theta^{-1}(\mathrm{Core}\,\varphi_2)$ are normal in A_1.

Now we are ready to introduce another new φ-invariant subgroup for skew morphisms. Let φ be a skew morphism of a group A, and let π be the power function of φ. Recall that $\mathrm{Core}\,\varphi$ is a normal φ-invariant subgroup of A. Let $\mathrm{Smooth}\,\varphi$ be a subset of A defined by

$$\mathrm{Smooth}\,\varphi = \{a \in A \mid \varphi(a) \equiv a \pmod{\mathrm{Core}\,\varphi}\}.$$

Proposition 3.6. *Let φ be a skew morphism of a group A, let π be the power function of φ, and let $\bar{\varphi}$ be the φ-induced skew morphism of $\bar{A} = A/\mathrm{Core}\,\varphi$. Then, for any $a \in A$, the following are equivalent:*

(a) $a \in \mathrm{Smooth}\,\varphi$,

(b) $\pi(\varphi^i(a)) = \pi(a)$ *for all positive integers* i,

(c) $\bar{a} \in \mathrm{Fix}\,\bar{\varphi}$.

Proof. (a) $\Longrightarrow$ (b): Since $a \in \mathrm{Smooth}\,\varphi$, by definition, $\varphi(a) = ua$ for some $u \in \mathrm{Core}\,\varphi$, and so $\varphi^i(a) = \varphi^{i-1}(u)\cdots\varphi(u)ua$ for all positive integers i. Since $\mathrm{Core}\,\varphi$ is a φ-invariant subgroup, we have $\varphi^{i-1}(u)\cdots\varphi(u)u \in \mathrm{Core}\,\varphi$. Therefore, $\pi(\varphi^i(a)) = \pi(a)$.

(b) $\Longrightarrow$ (c): Since $\pi(\varphi(a)) = \pi(a)$, we have $\varphi(a) = ua$ for some $u \in \mathrm{Ker}\,\varphi$ and then $\varphi^2(a) = \varphi(ua) = \varphi(u)\varphi(a) = \varphi(u)ua$. Since $\pi(\varphi^2(a)) = \pi(a)$, we get $\varphi(u)u \in \mathrm{Ker}\,\varphi$ and hence $\varphi(u) \in \mathrm{Ker}\,\varphi$. Repeating the above process, we get $\varphi^i(u) \in \mathrm{Ker}\,\varphi$ for all positive integers i. Consequently, $u \in \mathrm{Core}\,\varphi$ and hence $\bar{\varphi}(\bar{a}) = \bar{a}$, that is, $\bar{a} \in \mathrm{Fix}\,\bar{\varphi}$.

(c) $\Longrightarrow$ (a): Since $\bar{a} \in \mathrm{Fix}\,\bar{\varphi}$, we have $\bar{\varphi}(\bar{a}) = \bar{a}$ and so $\varphi(a) = ua$ for some $u \in \mathrm{Core}\,\varphi$. Since $\mathrm{Core}\,\varphi \trianglelefteq A$, we obtain $a \in \mathrm{Smooth}\,\varphi$. □

The following result is a direct corollary of Proposition 3.6.

Corollary 3.7. *Suppose that φ, A, $\bar{\varphi}$ and $\bar{A}$ are defined as Proposition 3.6. Then*

$$\mathrm{Fix}\,\overline{\varphi} = \overline{\mathrm{Smooth}\,\varphi}$$

and $\mathrm{Smooth}\,\varphi$ *is a φ-invariant subgroup of A. In particular,*

(a) $\mathrm{Smooth}\,\varphi = \mathrm{Core}\,\varphi$ *if and only if* $\mathrm{Fix}\,\bar{\varphi} = \bar{1}$,

(b) $\mathrm{Smooth}\,\varphi = A$ *if and only if* $\mathrm{Fix}\,\bar{\varphi} = \bar{A}$, *and*

(c) $\mathrm{Smooth}\,\varphi = \mathrm{Fix}\,\varphi$ *if* $\mathrm{Core}\,\varphi = 1$.

Example 3.8 ([22])**.** Consider a skew morphism of the cyclic group $\mathbb{Z}_{18}$ defined by

$$\varphi = (0)\,(1,15,17,7,3,5,13,9,11)\,(2,14,8)\,(4,10,16)\,(6)\,(12),$$
$$\pi = [1]\,[2,5,8,2,5,8,2,5,8]\,[7,7,7]\,[4,4,4]\,[1]\,[1].$$

Then $\mathrm{Core}\,\varphi = \mathrm{Ker}\,\varphi = \langle 6\rangle$, so $\bar{\varphi} = (\bar{0})\,(\bar{1},\bar{3},\bar{5})\,(\bar{2})\,(\bar{4})$ and $\mathrm{Smooth}\,\varphi = \langle 2\rangle$.

The following example is due to Conder, as mentioned in [1],

Example 3.9. Consider a skew morphism

$$\varphi = (1)\,(a, a^2)\,(b, bc, c)\,(ab, a^2bc, ac, a^2b, abc, a^2c),$$
$$\pi = [\,1\,]\,[\,1, 1\,]\,[\,1, 4, 4\,]\,[\,1, 4, 4, 1, 4, 4\,]$$

of the non-abelian group $A = D_3 \times C_2$, where

$$D_3 = \langle a, b \mid a^3 = b^2 = (ab)^2 = 1\rangle \qquad \text{and} \qquad C_2 = \langle c \mid c^2 = 1\rangle.$$

We have $\operatorname{Ker}\varphi = \langle a, b\rangle$ and $\operatorname{Core}\varphi = \langle a\rangle$. Thus, $\bar{\varphi} = (\bar{1})\,(\bar{b}, \bar{b}\bar{c}, \bar{c})$, and hence

$$\operatorname{Smooth}\varphi = \operatorname{Core}\varphi.$$

4 Smooth skew morphisms

In this section we establish a relationship between kernel-preserving skew morphisms and smooth skew morphisms.

In general, the kernel $\operatorname{Ker}\varphi$ of a skew morphism φ does not have to be a φ-invariant subgroup. However, as we already mentioned above, a skew morphism φ will be called *kernel-preserving* if $\operatorname{Ker}\varphi$ is φ-invariant. Clearly, φ is kernel-preserving if and only if $\operatorname{Core}\varphi = \operatorname{Ker}\varphi$. It is well known that every skew morphism φ of an abelian group is kernel-preserving [4, Lemma 5.1]. For non-abelian groups, there do exist skew morphisms which are not kernel-preserving, see Example 3.9.

Kernel-preserving skew morphisms have many interesting properties.

Lemma 4.1. *Let φ be a skew morphism of a group A, π be the power function of φ, and let n be the order of φ. If φ is kernel-preserving, then*

(a) $\operatorname{Ker}\varphi$ is a normal subgroup of A, and φ restricted to $\operatorname{Ker}\varphi$ is an automorphism of $\operatorname{Ker}\varphi$,

(b) for some positive integer k, if $\mu = \varphi^k$ is a skew morphism of A, then $\operatorname{Ker}\varphi \le \operatorname{Ker}\mu$,

(c) for any automorphism γ of A, $\gamma^{-1}\varphi\gamma$ is a kernel-preserving skew morphism of A,

(d) for any pair of elements $a \in A$ and $u \in \operatorname{Ker}\varphi$ there is a unique element $v \in \operatorname{Ker}\varphi$ such that $au = va$ and $\varphi(a)\varphi^{\pi(a)}(u) = \varphi(v)\varphi(a)$. In particular, if A is abelian then $\pi(a) \equiv 1 \pmod m$ where m is the order of the restriction of φ to $\operatorname{Ker}\varphi$.

Proof. (a): Since φ is kernel-preserving, $\operatorname{Ker}\varphi = \operatorname{Core}\varphi$, which is a normal subgroup of A. Moreover, for all $a, b \in \operatorname{Ker}\varphi$, we have $\varphi(ab) = \varphi(a)\varphi(b)$, so φ restricted to $\operatorname{Ker}\varphi$ is an automorphism of $\operatorname{Ker}\varphi$.

(b): For any $a \in \operatorname{Ker}\varphi = \operatorname{Core}\varphi$, $\pi(\varphi^{i-1}(a)) = 1$, $i = 1, 2, \ldots, n$. By Lemma 2.3, the power function π_μ of μ is determined by the the congruence $k\pi_\mu(a) \equiv \sigma(a, k) = k \pmod n$, so $\pi_\mu(a) \equiv 1 \pmod{n/\gcd(n, k)}$, which implies that $a \in \operatorname{Ker}\mu$.

(c): This is an immediate consequence of Lemma 2.2.

(d): Since $\operatorname{Ker}\varphi \trianglelefteq A$, for any pair (a, u) of elements $a \in A$ and $u \in \operatorname{Ker}\varphi$, there is a unique element $v \in \operatorname{Ker}\varphi$ such that $au = va$. Then $\varphi(a)\varphi^{\pi(a)}(u) = \varphi(au) = \varphi(va) = \varphi(v)\varphi(a)$. In particular, if A is abelian, then $u = v$ and $\varphi^{\pi(a)}(u) = \varphi(u)$ for all $u \in \operatorname{Ker}\varphi$, so $\pi(a) \equiv 1 \pmod m$, where m is the order of the restriction of φ to $\operatorname{Ker}\varphi$. □

Proposition 4.2. *Every kernel-preserving skew morphism of a non-abelian simple group A is an automorphism of A.*

Proof. If φ is not an automorphism of A, then $1 < \operatorname{Ker}\varphi < A$ by Lemma 2.4. Since φ is kernel-preserving, by Lemma 4.1(a) $\operatorname{Ker}\varphi \trianglelefteq A$, a contradiction. □

Let φ be a skew morphism of a group A. Recall that $\operatorname{Smooth}\varphi$ consists of elements $a \in A$ such that $\varphi(a) \equiv a \pmod{\operatorname{Core}\varphi}$. If $\operatorname{Smooth}\varphi = A$, then φ will be called a *smooth* skew morphism. The concept of smooth skew morphism was first introduced by Hu in the unpublished manuscript [7]. Bachratý and Jajcay rediscovered it under the name of *coset-preserving* skew morphisms [1].

Lemma 4.3. *Let φ be a skew morphism of a group A. If φ is smooth, then every subgroup of A containing $\operatorname{Core}\varphi$ is φ-invariant; in particular, φ is kernel-preserving.*

Proof. Suppose that φ is a smooth skew morphism of A. By Proposition 3.6, the induced skew morphism $\bar{\varphi}$ of $\bar{A} = A/\operatorname{Core}\varphi$ is the identity permutation on $\bar{A}$, so every subgroup of $\bar{A}$ is $\bar{\varphi}$-invariant. Therefore, by Lemma 3.5, every subgroup of A containing $\operatorname{Core}\varphi$ is φ-invariant. In particular, since $\operatorname{Core}\varphi \leq \operatorname{Ker}\varphi$, $\varphi(\operatorname{Ker}\varphi) = \operatorname{Ker}\varphi$. □

The following lemma characterizes smooth skew morphisms in terms of their power functions.

Lemma 4.4. *Let φ be a skew morphism of a group A, and let π be the power function of φ. Then φ is smooth if and only if $\pi(\varphi(a)) = \pi(a)$, for all $a \in A$.*

Proof. If φ is smooth, then, by Proposition 3.6, $\pi(\varphi(a)) = \pi(a)$, for all $a \in A$. Conversely, suppose that, for any $a \in A$, $\pi(\varphi(a)) = \pi(a)$. Then $\varphi(a) = ua$ for some $u \in \operatorname{Ker}\varphi$. By the assumption, we have $\pi(\varphi^{n-1}(u)) = \cdots = \pi(\varphi(u)) = \pi(u) = 1$, where $n = |\varphi|$, so $u \in \operatorname{Core}\varphi$. Therefore, $\varphi(a) \equiv a \pmod{\operatorname{Core}\varphi}$, that is, φ is smooth. □

The smallest positive integer d such that $\pi(\varphi^d(a)) \equiv \pi(a) \pmod{|\varphi|}$, for all $a \in A$, is called the *period* of φ. It is easily seen that d is a divisor of n uniquely determined by φ. Bachratý and Jajcay proved that if A is abelian, then $\mu = \varphi^d$ is a smooth skew morphism of A; in particular, if φ is nontrivial and contains a generating orbit, then d is a proper divisor of n [1]. In what follows we present a generalization.

Theorem 4.5. *Let φ be a skew morphism of a group A, let d be the period of φ, and let $\bar{\varphi}$ be the φ-induced skew morphism of $\bar{A} = A/\operatorname{Core}\varphi$. Then the following hold true:*

(a) d is equal to the order of $\bar{\varphi}$,

(b) $\sigma(a, d) \equiv 0 \pmod{d}$ for all $a \in A$,

(c) $\mu = \varphi^d$ is a smooth skew morphism of A,

(d) $\mu = \varphi^d$ is an automorphism of A if and only if $\sigma(a, d) \equiv d \pmod{n}$ for all $a \in A$.

Proof. Denote $n = |\varphi|$ and $m = |\bar{\varphi}|$.

(a): By the assumption, for any $a \in A$, we have $\pi(\varphi^d(a)) = \pi(a)$, and so $\varphi^d(a) = ua$ for some $u \in \operatorname{Ker}\varphi$. Thus,

$$\pi(\varphi^{d+1}(a)) = \pi(\varphi(ua)) = \pi(\varphi(u)\varphi(a)).$$

Since $\pi(\varphi^{d+1}(a)) = \pi(\varphi(a))$, we obtain $\varphi(u) \in \operatorname{Ker}\varphi$. Repeating this process we get $\varphi^{i-1}(u) \in \operatorname{Ker}\varphi$, $i = 1, 2, \ldots, n$. Thus, $u \in \operatorname{Core}\varphi$, and consequently, $\bar{\varphi}^d(\bar{a}) = \bar{a}$.

Therefore, $m \leq d$. On the other hand, since $|\bar{\varphi}| = m$, $\bar{\varphi}^m(\bar{a}) = \bar{a}$ for any $a \in A$, so $\varphi^m(a) = ua$ for some $u \in \operatorname{Core}\varphi$. Thus, $\pi(\varphi^m(a)) = \pi(ua) = \pi(a)$. The minimality of d then implies that $d \leq m$.

(b): For each $a \in A$, by (a) we have

$$\sigma(a,n) = \sum_{i=1}^{n} \pi(\varphi^{i-1}(a)) = \frac{n}{d} \sum_{i=1}^{d} \pi(\varphi^{i-1}(a)) = \frac{n}{d}\sigma(a,d) \pmod{n}.$$

By Lemma 2.6, $\sigma(a,n) = 0 \pmod{n}$ and hence, $\sigma(a,d) \equiv 0 \pmod{d}$.

(c): By (b) and Lemma 2.3, $\mu = \varphi^d$ is a skew morphism of A with its power function determined by $\pi_\mu(a) \equiv \sigma(a,d)/d \pmod{n/d}$. Since $\pi(\mu(a)) = \pi(\varphi^d(a)) \equiv \pi(a) \pmod{n}$, we obtain $\pi_\mu(\mu(a)) \equiv \pi_\mu(a) \pmod{n/d}$. Therefore, μ is smooth by Proposition 4.4.

(d): Since $\pi_\mu(a) \equiv \sigma(a,d)/d \pmod{n/d}$, μ is an automorphism if and only if $\sigma(a,d) \equiv d \pmod{n}$. □

Corollary 4.6. *Let φ be a kernel-preserving skew morphism of a group A, and let n be the order of φ. If φ is nontrivial, then the period d of φ is a proper divisor of n, and so $\mu = \varphi^d$ is a nontrivial smooth skew morphism of A.*

Proof. If φ is nontrivial, then $|A : \operatorname{Ker}\varphi| < |\varphi| = n$. By Lemma 2.4, $d = |\bar{\varphi}| \leq |\bar{A}| = |A : \operatorname{Ker}\varphi|$. Thus, d is a proper divisor of n and therefore, φ^d is a nontrivial smooth skew morphism by Theorem 4.5. □

Example 4.7 ([22])**.** Consider the skew morphism of the cyclic group $\mathbb{Z}_{18}$ given by

$$\varphi = (0)\,(1,5,13,11,7,17)\,(2,16,8,10,14,4)\,(3,5)\,(6,12)\,(9),$$
$$\pi = [1]\,[3,5,3,5,3,5]\,[5,3,5,3,5,3]\,[1,1]\,[1,1]\,[1].$$

Then $\operatorname{Ker}\varphi = \operatorname{Core}\varphi = \langle 3 \rangle$ and $\bar{\varphi} = (\bar{0})\,(\bar{1},\bar{2})$. Note that φ has period 2, which is precisely the order of $\bar{\varphi}$. Since $\sigma(x,2) \equiv 0 \pmod{2}$, for all $x \in \mathbb{Z}_{18}$, by Theorem 4.5(c), $\mu = \varphi^2$ is an automorphism of A.

Let us revisit the skew morphism φ of the non-abelian group $D_3 \times C_2$ considered in Example 3.9. It has period 3, which is a proper divisor of the order of φ. As we already mentioned, the skew morphism is not kernel-preserving. This leads us to pose the following problem.

Problem 4.8. Let d be the period of a nontrivial skew morphism φ of a group A. If φ is not kernel-preserving, under what condition is $\mu = \varphi^d$ nontrivial?

We close this section with some important properties of smooth skew morphisms, see also [1, 7].

Theorem 4.9. *Let φ be a skew morphism of A, let π be the power function of φ, and let n be the order of φ. If φ is smooth, then*

(a) $\pi\colon A \to \mathbb{Z}_n^*$ is a group homomorphism from A to the multiplicative group $\mathbb{Z}_n^*$ with $\operatorname{Ker}\pi = \operatorname{Ker}\varphi$,

(b) for any φ-invariant normal subgroup N of A, the induced skew morphism $\bar{\varphi}$ on A/N is also smooth; in particular, if $N = \operatorname{Ker}\varphi$ then $\bar{\varphi}$ is the identity permutation,

(c) for any positive integer k, $\mu = \varphi^k$ is a smooth skew morphism,

(d) for any automorphism γ of A, $\psi = \gamma^{-1}\varphi\gamma$ is a smooth skew morphism of A.

Proof. (a): Since φ is smooth, $\pi(a) = \pi(\varphi(a)) = \cdots = \pi(\varphi^{n-1}(a))$. By Lemma 2.1, we have

$$\pi(ab) \equiv \sum_{i=1}^{\pi(a)} \pi(\varphi^{i-1}(b)) \equiv \pi(a)\pi(b) \pmod{n}.$$

Since $1 \equiv \pi(ab^{-1}) = \pi(a)\pi(a^{-1}) \pmod{n}$, $\pi(a) \in \mathbb{Z}_n^*$. Therefore, π is a group homomorphism from A to the multiplicative group $\mathbb{Z}_n^*$.

(b): Since φ is smooth, for any $a \in A$, we have $\pi(\varphi(a)) = \pi(a)$, and so $\bar{\pi}(\bar{\varphi}(\bar{a})) = \bar{\pi}(\bar{a}) \pmod{m}$, where $m = |\bar{\varphi}|$. By Lemma 4.4, $\bar{\varphi}$ is smooth.

(c): For any positive integer k, since $\pi(\varphi^{i-1}(a)) = \pi(a)$, $i = 1, 2, \ldots, k$, we have

$$\sigma(a, k) = \sum_{i=1}^{k} \pi(\varphi^{i-1}(a)) \equiv k\pi(a) \pmod{n}.$$

It follows that the equations $kx \equiv \sigma(a, k) \pmod{n}$ are solvable for all $a \in A$. Thus, by Lemma 2.3, $\mu = \varphi^k$ is a skew morphism of A and the associated power function $\pi_\mu \colon A \to \mathbb{Z}_m$ is determined by $\pi_\mu(a) \equiv \pi(a) \pmod{m}$, where $m = n/\gcd(n, k)$ is the order of μ. Since $\pi_\mu(\mu(a)) \equiv \pi(\varphi^k(a)) \equiv \pi(a) \equiv \pi_\mu(a) \pmod{m}$, by Lemma 4.4, μ is also smooth.

(d): By Lemma 2.2, $\psi = \gamma^{-1}\varphi\gamma$ is a skew morphism with $\operatorname{Core}\psi = \gamma^{-1}(\operatorname{Core}\varphi)$. For any $a \in A$, since φ is smooth, $\varphi(\gamma(a)) \equiv \gamma(a) \pmod{\operatorname{Core}\varphi}$, or equivalently, $\gamma^{-1}\varphi\gamma(a) \equiv a \pmod{\gamma^{-1}(\operatorname{Core}\varphi)}$. Thus, $\psi(a) \equiv a \pmod{\operatorname{Core}\psi}$ and hence, ψ is smooth. □

5 Smooth skew morphisms of dihedral groups

Throughout this section, D_n will denote the dihedral group of order $2n$ with presentation

$$D_n = \langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle, \quad n \geq 3. \tag{5.1}$$

Moreover, for positive integers u and k, $\tau(u, k)$ and $\rho(u, k)$ are functions defined by

$$\tau(u, k) = \sum_{i=1}^{k} u^{k-1} \qquad \text{and} \qquad \rho(u, k) = \sum_{i=1}^{k} (-u)^{k-1}. \tag{5.2}$$

If k is even, we use $\lambda(u, k)$ to denote the function defined by

$$\lambda(u, k) = \sum_{i=1}^{k/2} u^{2(i-1)}. \tag{5.3}$$

The following result on normal subgroups of D_n is well known.

Lemma 5.1 ([16, Section 1.6, Exercise 8]). *Let K be a proper normal subgroup of D_n, $n \geq 3$.*

(a) if n is odd then $K = \langle a^u \rangle$, where u divides n,

(b) if n is even, then either $K = \langle a^2, b\rangle$, $K = \langle a^2, ab\rangle$ or $K = \langle a^u\rangle$, where u divides n.

Lemma 5.2 ([5]). *Let φ be a skew morphism of D_n, $n \geq 3$, then $\operatorname{Ker}\varphi \neq \langle a\rangle$.*

Lemma 5.3. *Let φ be a smooth skew morphism of D_n, $n \geq 3$. If n is odd, then φ is an automorphism of A, whereas if n is even and φ is not an automorphism of D_n, then $\operatorname{Ker}\varphi = \langle a^2\rangle$, $\operatorname{Ker}\varphi = \langle a^2, ab\rangle$ or $\operatorname{Ker}\varphi = \langle a^2, b\rangle$. Moreover, the involutory automorphism of D_n taking $a \mapsto a^{-1}, b \mapsto ab$ transposes the smooth skew morphisms of D_n with kernels $\langle a^2, b\rangle$ and $\langle a^2, ab\rangle$.*

Proof. Assume that φ is not an automorphism of D_n, then $1 < \operatorname{Ker}\varphi < D_n$. Since φ is smooth, by Theorem 4.9(a), the power function $\pi\colon D_n \to \mathbb{Z}^*_{|\varphi|}$ is a group homomorphism with $\operatorname{Ker}\pi = \operatorname{Ker}\varphi$. It follows that $\operatorname{Ker}\varphi$ is a proper normal subgroup of A. Since $\mathbb{Z}^*_{|\varphi|}$ is abelian, $D'_n \leq \operatorname{Ker}\varphi$, where D'_n is the derived subgroup of D_n.

If n is odd then $D'_n = \langle a\rangle$, which is a maximal subgroup of D_n. By Lemma 5.2 $\operatorname{Ker}\varphi \neq \langle a\rangle$, so $\operatorname{Ker}\varphi = D_n$, and hence φ is automorphism of D_n, a contradiction.

On the other hand, if n is even, then $D'_n = \langle a^2\rangle$, so $\langle a^2\rangle \leq \operatorname{Ker}\varphi$. By Lemma 5.1, one of the following three cases may happen: $\operatorname{Ker}\varphi \leq \langle a\rangle$, $\operatorname{Ker}\varphi = \langle a^2, b\rangle$, or $\operatorname{Ker}\varphi = \langle a^2, ab\rangle$. For the first case, by Lemma 5.2, we have $\operatorname{Ker}\varphi \neq \langle a\rangle$, so $\operatorname{Ker}\varphi = \langle a^2\rangle$.

Finally, by Theorem 4.9(d), the automorphism of D_n taking $a \mapsto a^{-1}, b \mapsto ab$ transposes the smooth skew morphisms of D_n with kernels $\langle a^2, b\rangle$ and $\langle a^2, ab\rangle$. □

The following result classifies smooth skew morphisms of the dihedral groups D_n with $\operatorname{Ker}\varphi = \langle a^2\rangle$ for even integers $n \geq 4$.

Theorem 5.4. *Let $D_n = \langle a, b\rangle$ be the dihedral group of order $2n$, where $n \geq 4$ is an even number. Then every smooth skew morphism φ of D_n with $\operatorname{Ker}\varphi = \langle a^2\rangle$ is defined by*

$$\begin{cases} \varphi(a^{2i}) = a^{2iu}, \\ \varphi(a^{2i+1}) = a^{2iu+2r+1}, \\ \varphi(a^{2i}b) = a^{2iu+2s}b, \\ \varphi(a^{2i+1}b) = a^{2iu+2r+2s\tau(u,e)+1}b \end{cases} \quad \text{and} \quad \begin{cases} \pi(a^{2i}) = 1, \\ \pi(a^{2i+1}) = e, \\ \pi(a^{2i}b) = f, \\ \pi(a^{2i+1}b) = ef, \end{cases} \tag{5.4}$$

where r, s, u, e, f are nonnegative integers satisfying the following conditions

(a) $r, s \in \mathbb{Z}_{n/2}$ and $u \in \mathbb{Z}^*_{n/2}$,

(b) the order of φ is the smallest positive integer k such that $r\tau(u,k) \equiv 0 \pmod{n/2}$ and $s\tau(u,k) \equiv 0 \pmod{n/2}$,

(c) $e, f \in \mathbb{Z}^*_k$ generate the Klein four group,

(d) $u^{e-1} \equiv 1 \pmod{n/2}$ and $u^{f-1} \equiv 1 \pmod{n/2}$,

(e) $r\tau(u, e-1) \equiv u - 2r - 1 \pmod{n/2}$ and $s\tau(u, f-1) \equiv 0 \pmod{n/2}$,

(f) $r\tau(u, f-1) + s\tau(u, e-1) \equiv u - 2r - 1 \pmod{n/2}$.

Proof. First suppose that φ is a smooth skew morphism of D_n with $\operatorname{Ker}\varphi = \langle a^2\rangle$. Then by Theorem 4.9(b), the induced skew morphism $\bar{\varphi}$ on $D_n/\operatorname{Ker}\varphi$ is the identity permutation, so there exist integers $r, s \in \mathbb{Z}_{n/2}$ such that

$$\varphi(a) = a^{1+2r} \qquad \text{and} \qquad \varphi(b) = a^{2s}b.$$

Since φ is kernel-preserving, the restriction of φ to $\operatorname{Ker}\varphi = \langle a^2\rangle$ is an automorphism, so $\varphi(a^2) = a^{2u}$ where $u \in \mathbb{Z}_{n/2}^*$. Assume that $\pi(a) \equiv e \pmod k$ and $\pi(b) \equiv f \pmod k$, where $k = |\varphi|$.

From the above identities we derive the following formulae by induction:

$$\varphi^j(a) = a^{1+2r\tau(u,j)} \qquad \text{and} \qquad \varphi^j(b) = a^{2s\tau(u,j)}b,$$

where j is a positive integer and $\tau(u,j) = \sum_{i=1}^{j} u^{i-1}$. Since $D_n = \langle a, b\rangle$, by Lemma 2.8, the order $k = |\varphi|$ is equal to $\operatorname{lcm}(|O_a|, |O_b|)$, the least common multiple of the lengths of the orbits containing a and b. That is, k is the smallest positive integer such that $\varphi^k(a) = a$ and $\varphi^k(b) = b$. Using the above formulae we then deduce that k is the smallest positive integer such that $r\tau(u,k) \equiv 0 \pmod{n/2}$ and $s\tau(u,k) \equiv 0 \pmod{n/2}$.

Now we determine the skew morphism and the associated power function. By the assumption we have

$$\begin{aligned}\varphi(a^{2i}) &= (a^{2u})^i = a^{2iu},\\ \varphi(a^{2i}b) &= \varphi(a^{2i})\varphi(b) = a^{2iu+2s}b.\end{aligned}$$

Similarly, we have

$$\begin{aligned}\varphi(a^{2i+1}) &= \varphi(a^{2i}a) = \varphi(a^{2i})\varphi(a) = a^{1+2r+2iu},\\ \varphi(a^{2i+1}b) &= \varphi(a^{2i})\varphi(a)\varphi^e(b) = a^{2iu+1+2r+2s\tau(u,e)}.\end{aligned}$$

Since $\pi\colon D_n \to \mathbb{Z}_k^*$ is a group homomorphism, we have $e^2 \equiv \pi(a)^2 = \pi(a^2) \equiv 1 \pmod k$ and $f^2 \equiv \pi(b)^2 \equiv \pi(b^2) \equiv 1 \pmod k$, so $e^2 \equiv 1 \pmod k$ and $f^2 \equiv 1 \pmod k$. Hence, $\pi(a^{2i}) \equiv 1$, $\pi(a^{2i+1}) \equiv e$, $\pi(a^{2i}b) \equiv f$, $\pi(a^{2i+1}b) \equiv ef$. In particular, since $|D_n : \operatorname{Ker}\varphi| = 4$, $\langle e, f\rangle \le \mathbb{Z}_k^*$ is the Klein four group. Therefore φ and π have the claimed form (5.4).

Moreover, we have

$$\begin{aligned}a^{1+2r+2u^e} &= \varphi(a)\varphi^e(a^2) = \varphi(a)\varphi^{\pi(a)}(a^2) = \varphi(aa^2) = \varphi(a^2a)\\ &= \varphi(a^2)\varphi(a) = a^{1+2r+2u},\end{aligned}$$

and so $u^{e-1} \equiv 1 \pmod{n/2}$. Similarly, since

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

we have

$$a^{2s-2u^f}b = a^{2s}ba^{2u^f} = \varphi(b)\varphi^f(a^2) = \varphi(a^{-2})\varphi(b) = a^{2s-2u}b.$$

Thus, $u^{f-1} \equiv 1 \pmod{n/2}$.

Furthermore, since

$$a^{2u} = \varphi(a^2) = \varphi(a)\varphi^{\pi(a)}(a) = \varphi(a)\varphi^e(a) = a^{2+2r+2r\tau(u,e)},$$

we get

$$r(1+\tau(u,e)) \equiv u-1 \pmod{n/2}. \tag{5.5}$$

Similarly,

$$1 = \varphi(b^2) = \varphi(b)\varphi^{\pi(b)}(b) = \varphi(b)\varphi^f(b) = a^{2s}ba^{2s\tau(u,f)}b = a^{2s-2s\tau(u,f)},$$

we obtain

$$s\tau(u,f) \equiv s \pmod{n/2}. \tag{5.6}$$

Employing induction it is easy to deduce that $\varphi^j(a^{-1}) = a^{1-2u^j+2r\tau(u,j)}$, where j is an arbitrary positive integer. Then

$$\varphi(a)\varphi^e(b) = \varphi(ab) = \varphi(ba^{-1}) = \varphi(b)\varphi^f(a^{-1}).$$

Upon substitution we get

$$\begin{aligned} a^{1+2r+2s\tau(u,e)}b = \varphi(a)\varphi^e(b) = \varphi(b)\varphi^f(a^{-1}) &= a^{2s}ba^{1-2u^f+2r\tau(u,f)} \\ &= a^{2s-1+2u^f-2r\tau(u,f)}b. \end{aligned}$$

Hence,

$$r\tau(u,f) + s\tau(u,e) \equiv s + u^f - r - 1 \pmod{n/2}.$$

Since $u^f \equiv u \pmod{n/2}$, the congruence is reduced to

$$r\tau(u,f) + s\tau(u,e) \equiv s + u - r - 1 \pmod{n/2}. \tag{5.7}$$

Recall that $u^{e-1} \equiv 1 \pmod{n/2}$ and $u^{f-1} \equiv 1 \pmod{n/2}$, so

$$\begin{aligned} \tau(u,e) &\equiv \tau(u,e-1) + 1 \pmod{n/2}, \\ \tau(u,f) &\equiv \tau(u,f-1) + 1 \pmod{n/2}. \end{aligned}$$

Upon substitution the congruences (5.5), (5.6) and (5.7) are reduced to the numerical conditions in (e) and (f).

Conversely, for a quintuple (r,s,u,e,f) of nonnegative integers satisfying the stated numerical conditions, we verify that φ given by (5.4) is a smooth skew morphism of D_n with $\operatorname{Ker}\varphi = \langle a^2\rangle$ and the function π is the associated power function. It is evident that φ is a bijection on D_n and $\varphi(1) = 1$.

It remains to verify the identity $\varphi(xy) = \varphi(x)\varphi^{\pi(x)}(y)$ for all $x, y \in D_n$. By Lemma 2.8, it suffices to verify this for $x, y \in O_a \cup O_b$, where O_a and O_b are the generating orbits of φ of the form

$$\begin{aligned} O_a &= (a, a^{1+2r\tau(u,1)}, a^{1+2r\tau(u,2)}, \ldots, a^{1+2r\tau(u,i)}, \ldots), \\ O_b &= (b, a^{2s\tau(u,1)}b, a^{2s\tau(u,2)}b, \ldots, a^{2s\tau(u,j)}b, \ldots). \end{aligned}$$

It follows that one of the following four cases may happen:

(i) $x, y \in O_a$;

(ii) $x, y \in O_b$;

(iii) $x \in O_a$, $y \in O_b$ or

(iv) $x \in O_b$, $y \in O_a$.

We shall demonstrate the verification for the first case, and leave other cases to the reader.

If $x, y \in O_a$, then $x = a^{1+2r\tau(u,i)}$ and $y = a^{1+2r\tau(u,j)}$ for some i, j. We have

$$\varphi(x)\varphi(y) = \varphi(a^{2r(\tau(u,i)+\tau(u,j))+2}) = a^{2ru(\tau(u,i)+\tau(u,j))+2u}$$

and

$$\varphi(x)\varphi^{\pi(x)}(y) = \varphi(a^{1+2r\tau(u,i)})\varphi^e(a^{1+2r\tau(u,j)}) = a^{2r(\tau(u,i+1)+\tau(u,j+e))+2}.$$

By the numerical conditions (d) and (e), we have

$$\begin{aligned} &r(\tau(u,i+1)+\tau(u,j+e))+1-(ru(\tau(u,i)+\tau(u,j))+u) \\ &\quad = r\Big((\tau(u,i+1)-u\tau(u,i))+(\tau(u,j+e)-u\tau(u,j))\Big)+1-u \\ &\quad \overset{(d)}{\equiv} r\Big(1+(\tau(u,j+e)-u^e\tau(u,j))\Big)+1-u \\ &\quad \equiv r(2+\tau(u,e-1))+1-u \\ &\quad \overset{(e)}{\equiv} 0 \pmod{n/2}. \end{aligned}$$

Therefore, $\varphi(xy) = \varphi(x)\varphi^{\pi(x)}(y)$.

Finally, from the choices of the parameters it is easily seen that distinct quintuples (r, s, u, e, f) give rise to different skew morphisms of D_n, as required. □

Remark 5.5. In Theorem 5.4, consider the particular case where $u = 1$. By Condition (b) we have

$$k = \operatorname{lcm}\left(\frac{n/2}{\gcd(r, n/2)}, \frac{n/2}{\gcd(s, n/2)}\right).$$

The numerical conditions are reduced to

$$\begin{cases} r(e+1) \equiv 0 \pmod{n/2}, \\ s(f-1) \equiv 0 \pmod{n/2}, \\ r(f+1)+s(e-1) \equiv 0 \pmod{n/2}, \end{cases}$$

where $r, s \in \mathbb{Z}_{n/2}$ and $\langle e, f\rangle \leq \mathbb{Z}_k^*$ is the Klein four group. If $n = 8m$, where $m \geq 3$ is an odd number, then it can be easily verified that the quintuple $(r, s, u, e, f) = (m+4, m, 1, 4m-1, 2m-1)$ fulfills the numerical conditions. Therefore, we obtain an infinite family of skew morphisms of D_{8m} of order $4m$ with $\operatorname{Ker}\varphi = \langle a^2\rangle$. This example was first discovered by Zhang and Du in [26, Example 1.4].

Example 5.6. By computations using the MAGMA system we found that the smallest n for which there is a smooth skew morphism φ of D_n with $\operatorname{Ker}\varphi = \langle a^2\rangle$ is the number 24. In this case, all such skew morphisms have order 12, and the corresponding quintuples (r, s, u, e, f) are listed below:

$$\begin{aligned} (r,s,u,e,f) = {} & (1,3,1,11,5),(1,4,1,11,7),(1,9,1,11,5),(1,10,1,11,7), \\ & (5,2,1,11,7),(5,3,1,11,5),(5,8,1,11,7),(5,9,1,11,5), \\ & (7,3,1,11,5),(7,4,1,11,7),(7,9,1,11,5),(7,10,1,11,7), \\ & (11,,2,1,11,7),(11,3,1,11,5),(11,8,1,11,7),(11,9,1,11,5). \end{aligned}$$

Note that in each case we have $u = 1$, so the restriction of φ to $\operatorname{Ker}\varphi$ is the identity automorphism of $\operatorname{Ker}\varphi$. However, further computations show that, for other n, there do exist examples with $u \neq 1$.

For even numbers n, by Lemma 5.3, the involutory automorphism γ of D_n taking $a \mapsto a^{-1}$, $b \mapsto ab$ transposes the smooth skew morphisms of D_n with kernels $\langle a^2, b\rangle$ or $\langle a^2, ab\rangle$. Thus, to complete the classification of smooth skew morphisms of D_n, it suffices to determine the smooth skew morphisms of D_n with kernel $\operatorname{Ker}\varphi = \langle a^2, b\rangle$.

Theorem 5.7. *Let D_n be the dihedral group of order $2n$, where $n \geq 8$ is an even number. If φ is a smooth skew morphism of D_n with $\operatorname{Ker}\varphi = \langle a^2, b\rangle$, then φ belongs to one of the following two families of skew morphisms:*

(I) skew morphisms of order k defined by

$$\begin{cases} \varphi(a^{2i}) = a^{2iu}, \\ \varphi(a^{2i+1}) = a^{2iu+2r+1}, \\ \varphi(ba^{2i}) = ba^{2iu+2s}, \\ \varphi(ba^{2i+1}) = ba^{2r+2s+2iu+1} \end{cases} \quad \text{and} \quad \begin{cases} \pi(a^{2i}) = 1, \\ \pi(a^{2i+1}) = e, \\ \pi(ba^{2i}) = 1, \\ \pi(ba^{2i+1}) = e, \end{cases} \tag{5.8}$$

where r, s, u, k, e are nonnegative integers satisfying the following conditions

(a) $r, s \in \mathbb{Z}_{n/2}$ *and* $u \in \mathbb{Z}^*_{n/2}$,
(b) k *is the smallest positive integer such that* $r\tau(u,k) \equiv 0 \pmod{n/2}$ *and* $s\tau(u,k) \equiv 0 \pmod{n/2}$,
(c) $e \in \mathbb{Z}^*_k$ *such that* $e \not\equiv 1 \pmod{k}$ *and* $e^2 \equiv 1 \pmod{k}$,
(d) $u^{e-1} \equiv 1 \pmod{n/2}$,
(e) $r\tau(u, e-1) \equiv u - 2r - 1 \pmod{n/2}$ *and* $s\tau(u, e-1) \equiv -u + 2r + 1 \pmod{n/2}$.

(II) skew morphisms of order $2(e-1)$ defined by

$$\begin{cases} \varphi(a^{2i}) = a^{2iu}, \\ \varphi(a^{2i+1}) = ba^{2r-2iu+1}, \\ \varphi(ba^{2i}) = ba^{2s+2iu}, \\ \varphi(ba^{2i+1}) = a^{2r-2s-2iu+1} \end{cases} \quad \text{and} \quad \begin{cases} \pi(a^{2i}) = 1, \\ \pi(a^{2i+1}) = e, \\ \pi(ba^{2i}) = 1, \\ \pi(ba^{2i+1}) = e, \end{cases} \tag{5.9}$$

where r, s, u, e are nonnegative integers satisfying the following conditions

(a) $r, s \in \mathbb{Z}_{n/2}$, $u \in \mathbb{Z}^*_{n/2}$ *and* $e > 1$ *is an odd number,*
(b) $u^{e-1} \equiv -1 \pmod{n/2}$,
(c) $s\tau(u, e-1) \equiv u + 2r + 1 \pmod{n/2}$,
(d) $r\rho(u, e-1) \equiv s\lambda(u, e-1) - 1 \pmod{n/2}$.

Proof. First suppose that φ is a smooth skew morphism of D_n with $\operatorname{Ker}\varphi = \langle a^2, b\rangle$. By Theorem 4.9, the induced skew morphism $\bar{\varphi}$ of $D_n/\operatorname{Ker}\varphi$ is the identity permutation and

the restriction of φ to $\operatorname{Ker}\varphi = \langle a^2, b\rangle$ is an automorphism of $\operatorname{Ker}\varphi$. It follows that there exist integers $r, s, u \in \mathbb{Z}_{n/2}$ and $\ell \in \mathbb{Z}_2$ such that

$$\varphi(a) = b^\ell a^{1+2r}, \qquad \varphi(b) = ba^{2s} \qquad \text{and} \qquad \varphi(a^2) = a^{2u}.$$

Assume that $\pi(a) \equiv e \pmod{k}$, where $k = |\varphi|$ denotes the order of φ. Since $b \in \operatorname{Ker}\varphi$, $\pi(b) \equiv 1 \pmod{k}$. By Theorem 4.9, the power function $\pi\colon D_n \to \mathbb{Z}_k$ is a group homomorphism from D_n to the multiplicative group $\mathbb{Z}_k^*$, so

$$e^{-1} \equiv \pi(a^{-1}) \equiv \pi(b^{-1}ab) \equiv \pi(a) \equiv e \pmod{k},$$

and hence $e^2 \equiv 1 \pmod{k}$. It follows that $\pi(a^{2i}) \equiv \pi(a^{2i}b) \equiv 1$ and $\pi(a^{2i+1}) \equiv \pi(a^{2i+1}b) \equiv e$. Since φ has skew type 2, $e \not\equiv 1 \pmod{k}$. To proceed we distinguish two cases:

Case (I): $\ell = 0$.

In this case, we have

$$\varphi(a) = a^{1+2r}, \qquad \varphi(b) = ba^{2s} \qquad \text{and} \qquad \varphi(a^2) = a^{2u}.$$

Then

$$\varphi(a^{2i}) = \varphi(a^2)^i = a^{2iu},$$
$$\varphi(ba^{2i}) = \varphi(b)\varphi(a^2)^i = ba^{2iu+2s}.$$

Similarly,

$$\varphi(a^{2i+1}) = \varphi(a^{2i}a) = \varphi(a^2)^i\varphi(a) = a^{2iu+2r+1},$$
$$\varphi(ba^{2i+1}) = \varphi(ba^{2i}a) = \varphi(b)\varphi(a^{2i})\varphi(a) = ba^{2r+2s+2iu+1}.$$

Hence, the skew morphism has the form given by (5.8).

Using induction it is easy to prove that

$$\varphi^j(a) = a^{1+2r\tau(u,j)} \qquad \text{and} \qquad \varphi^j(b) = ba^{2s\tau(u,j)},$$

where j is a positive integer and $\tau(u,j) = \sum_{i=1}^{j} u^{i-1}$. Since $D_n = \langle a, b\rangle$, $k = |\varphi|$ is the smallest positive integer such that $\varphi^k(a) = a$ and $\varphi^k(b) = b$, which implies that

$$r\tau(u,k) \equiv 0 \pmod{n/2} \qquad \text{and} \qquad s\tau(u,k) \equiv 0 \pmod{n/2}.$$

Moreover, we have

$$a^{1+2r+2u^e} = \varphi(a)\varphi^e(a^2) = \varphi(aa^2) = \varphi(a^2a) = \varphi(a^2)\varphi(a) = a^{1+2r+2u},$$

so $u^{e-1} \equiv 1 \pmod{n/2}$.

Furthermore, since

$$a^{2u} = \varphi(a^2) = \varphi(a)\varphi^e(a) = a^{1+2r}a^{1+2r\tau(u,e)} = a^{2+2r+2r\tau(u,e)},$$

we obtain

$$r\big(\tau(u,e)+1\big) \equiv u - 1 \pmod{n/2}. \tag{5.10}$$

Similarly,

$$\varphi(a)\varphi^e(b) = \varphi(ab) = \varphi(ba^{-1}) = \varphi(b)\varphi(a^{-1}) = \varphi(b)\varphi(a^{-2}a) = \varphi(b)\varphi(a^{-2})\varphi(a).$$

By the above formula we have

$$\varphi(a)\varphi^e(b) = a^{1+2r}ba^{2s\tau(u,e)} = ba^{-1-2r+2s\tau(u,e)}$$

and

$$\varphi(b)\varphi(a^{-2})\varphi(a) = ba^{1+2r+2s-2u}.$$

Consequently, upon substitution we obtain

$$s(\tau(u,e)-1) \equiv -u+2r+1 \pmod{n/2}. \tag{5.11}$$

Recall that $u^{e-1} \equiv 1 \pmod{n/2}$, so

$$\tau(u,e) = \tau(u,e-1) + u^{e-1} \equiv \tau(u,e-1)+1 \pmod{n/2}.$$

Upon substitution the equations (5.10) and (5.11) are reduced to

$$\begin{aligned} r\tau(u,e-1) &\equiv u-2r-1 \pmod{n/2},\\ s\tau(u,e-1) &\equiv -u+2r+1 \pmod{n/2}. \end{aligned}$$

Case (II): $\ell = 1$.

In this case we have

$$\varphi(a) = ba^{1+2r}, \qquad \varphi(b) = ba^{2s} \qquad \text{and} \qquad \varphi(a^2) = a^{2u}.$$

Then

$$\begin{aligned} \varphi(a^{2i}) &= a^{2iu},\\ \varphi(ba^{2i}) &= \varphi(b)\varphi(a^{2i}) = ba^{2s+2iu}. \end{aligned}$$

Similarly,

$$\begin{aligned} \varphi(a^{2i+1}) &= \varphi(a^{2i}a) = a^{2iu}ba^{1+2r} = ba^{2r-2iu+1},\\ \varphi(ba^{2i+1}) &= \varphi(b)\varphi(a^{2i})\varphi(a) = a^{2r-2s-2iu+1}. \end{aligned}$$

Hence φ has the form (5.9).

Using induction it is easy to derive the following formula

$$\varphi^j(b) = ba^{2s\tau(u,j)} \qquad \text{and} \qquad \varphi^j(a) = \begin{cases} a^{2r\rho(u,j)-2s\lambda(u,j)+1}, & \text{if } j \text{ is even},\\ ba^{2r\rho(u,j)+2su\lambda(u,j-1)+1}, & \text{if } j \text{ is odd}, \end{cases}$$

where τ, ρ and λ are the functions defined by (5.2) and (5.3). Since $\varphi(a) = ba^{1+2r}$ and $D_n = \langle a, ba^{1+2r}\rangle$, $k = |\varphi| = |O_a|$. Thus, k is the smallest positive integer such that

$$r\rho(u,k) \equiv s\lambda(u,k) \pmod{n/2}.$$

In particular, since elements from the cosets $\langle a\rangle$ and $b\langle a\rangle$ alternate in the orbit O_a, k is even, and hence e is odd. Thus,

$$a^{2u} = \varphi(a^2) = \varphi(a)\varphi^e(a) = \varphi(a)\varphi^e(a) = a^{2r\rho(u,e)-2r+2su\lambda(u,e-1)}.$$

Consequently, we obtain

$$r\rho(u,e) + su\lambda(u,e-1) \equiv r+u \pmod{n/2}. \tag{5.12}$$

Furthermore, we have

$$\begin{aligned} ba^{1+2r+2u^e} &= \varphi(a)\varphi^e(a^2) = \varphi(aa^2) = \varphi(a^2a) \\ &= \varphi(a^2)\varphi(a) = a^{2u}ba^{1+2r} = ba^{2r-2u+1}, \end{aligned}$$

so $u^{e-1} \equiv -1 \pmod{n/2}$. Similarly

$$\begin{aligned} a^{-1-2r+2s\tau(u,e)} &= \varphi(a)\varphi^e(b) = \varphi(ab) = \varphi(ba^{-2}a) \\ &= \varphi(b)\varphi(a^{-2})\varphi(a) = a^{1+2r-2s+2u}. \end{aligned}$$

Hence

$$s\tau(u,e) \equiv 1+2r+u-s \pmod{n/2}. \tag{5.13}$$

Recall that $u^{e-1} \equiv -1 \pmod{n/2}$, so

$$\begin{aligned} \tau(u,e) &\equiv \tau(u,e-1) - 1 \pmod{n/2}, \\ \rho(u,e) &\equiv \rho(u,e-1) - 1 \pmod{n/2}. \end{aligned}$$

Upon substitution the equations (5.12) and (5.13) are reduced to

$$r\rho(u,e-1) + su\lambda(u,e-1) \equiv 2r+u \pmod{n/2}, \tag{5.14}$$

$$s\tau(u,e-1) \equiv 2r+u+1 \pmod{n/2}. \tag{5.15}$$

Subtracting we then get

$$r\rho(u,e-1) \equiv s\lambda(u,e-1) - 1 \pmod{n/2}.$$

Finally, note that

$$\begin{aligned} \rho(u,2(e-1)) &= \sum_{i=1}^{2(e-1)} (-u)^{2(e-1)} \\ &= \sum_{i=1}^{e-1}(-u)^{i-1} + u^{e-1}\sum_{i=1}^{e-1}(-u)^{i-1} \equiv 0 \pmod{n/2}, \end{aligned}$$

and

$$\begin{aligned} \lambda(u,2(e-1)) &= \sum_{i=1}^{e-1} u^{2i} \\ &= \sum_{i=1}^{(e-1)/2} u^{2(i-1)} + u^{e-1}\sum_{i=1}^{(e-1)/2} u^{2(i-1)} \equiv 0 \pmod{n/2}, \end{aligned}$$

Hence,

$$r\rho(u, 2(e-1)) \equiv s\lambda(u, 2(e-1)) \pmod{n/2}.$$

The minimality of k yields $k \mid 2(e-1)$. But $e-1 < k$, which forces $k = 2(e-1)$.

Conversely, in each case for any quadruple (r, s, u, e) satisfying the numerical conditions, it is straightforward to verify that φ of the given form is a smooth skew morphism of D_n with $\operatorname{Ker}\varphi = \langle a^2, b\rangle$ and π is the associated power function. In particular, from the choices of the parameters it is easily seen that distinct quadruples (r, s, u, e) give rise to different skew morphisms of D_n, as required. □

Remark 5.8. Let φ be any skew morphism from (II) of Theorem 5.7. Note that the orbit of φ containing a also contains ba^{2r+1}, so the orbit O_a generates D_n. Clearly, it is closed under taking inverses. Therefore, such skew morphisms give rise to the e-balanced regular Cayley maps of D_n, which were first classified by Kwak, Kwon and Feng [17].

References

[1] M. Bachratý and R. Jajcay, Powers of skew-morphisms, in: J. Širáň and R. Jajcay (eds.), *Symmetries in Graphs, Maps, and Polytopes*, Springer, Cham, volume 159 of *Springer Proceedings in Mathematics & Statistics*, 2016 pp. 1–25, doi:10.1007/978-3-319-30451-9_1, papers from the 5th SIGMAP Workshop held in West Malvern, July 7 – 11, 2014.

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

[3] M. Conder, R. Jajcay and T. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebraic Combin.* **25** (2007), 259–283, doi:10.1007/s10801-006-0037-0.

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

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

[6] M. D. E. Conder and T. W. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.* **366** (2014), 3585–3609, doi:10.1090/s0002-9947-2014-05933-3.

[7] K. Hu, Theory of skew morphisms, 2012, preprint.

[8] K. Hu and Y. S. Kwon, Regular Cayley maps and skew morphisms of dihedral groups: a survey, in preparation.

[9] R. Jajcay and R. Nedela, Half-regular Cayley maps, *Graphs Combin.* **31** (2015), 1003–1018, doi:10.1007/s00373-014-1428-y.

[10] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179, doi:10.1016/s0012-365x(01)00081-4.

[11] I. Kovács and Y. S. Kwon, Regular Cayley maps on dihedral groups with the smallest kernel, *J. Algebraic Combin.* **44** (2016), 831–847, doi:10.1007/s10801-016-0689-3.

[12] I. Kovács and Y. S. Kwon, Classification of reflexible Cayley maps for dihedral groups, *J. Comb. Theory Ser. B* **127** (2017), 187–204, doi:10.1016/j.jctb.2017.06.002.

[13] I. Kovács and Y. S. Kwon, private communication, 2018.

[14] I. Kovács, D. Marušič and M. Muzychuk, On G-arc-regular dihedrants and regular dihedral maps, *J. Algebraic Combin.* **38** (2013), 437–455, doi:10.1007/s10801-012-0410-0.

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

[16] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups: An Introduction*, Universitext, Springer-Verlag, New York, 2004, doi:10.1007/b97433.

[17] J. H. Kwak, Y. S. Kwon and R. Feng, A classification of regular t-balanced Cayley maps on dihedral groups, *European J. Combin.* **27** (2006), 382–393, doi:10.1016/j.ejc.2004.12.002.

[18] J. H. Kwak and J.-M. Oh, A classification of regular t-balanced Cayley maps on dicyclic groups, *European J. Combin.* **29** (2008), 1151–1159, doi:10.1016/j.ejc.2007.06.023.

[19] Y. S. Kwon, A classification of regular t-balanced Cayley maps for cyclic groups, *Discrete Math.* **313** (2013), 656–664, doi:10.1016/j.disc.2012.12.012.

[20] J.-M. Oh, Regular t-balanced Cayley maps on semi-dihedral groups, *J. Comb. Theory Ser. B* **99** (2009), 480–493, doi:10.1016/j.jctb.2008.09.006.

[21] Y. Wang and R. Q. Feng, Regular balanced Cayley maps for cyclic, dihedral and generalized quaternion groups, *Acta Math. Sin.* **21** (2005), 773–778, doi:10.1007/s10114-004-0455-7.

[22] K. Yuan, Y. Wang and J. H. Kwak, Enumeration of skew-morphisms of cyclic groups of small orders and their corresponding Cayley maps, *Adv. Math. (China)* **45** (2016), 21–36.

[23] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for abelian groups, *European J. Combin.* **39** (2014), 198–206, doi:10.1016/j.ejc.2014.01.006.

[24] J.-Y. Zhang, A classification of regular Cayley maps with trivial Cayley-core for dihedral groups, *Discrete Math.* **338** (2015), 1216–1225, doi:10.1016/j.disc.2015.01.036.

[25] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for dihedral groups, *Discrete Math.* **338** (2015), 1163–1172, doi:10.1016/j.disc.2015.01.038.

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