UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

Skew-morphisms of Abelian Groups

Diplomová práca

2015

Bc. Martin Bachratý

UNIVERZITA KOMENSKÉHO V BRATISLAVE

Fakulta matematiky, fyziky a informatiky

Skew-morphisms of abelian groups

Diplomová práca

Bc. Martin Bachratý

Študijný odbor: Matematika 1113

Študijný program: Matematika

Vedúci DP:

Doc. RNDr. Róbert Jajcay, PhD.

Bratislava 2015

46167309

Comenius University in Bratislava
Faculty of Mathematics, Physics and Informatics

THESIS ASSIGNMENT

Name and Surname:	Bc. Martin Bachratý
Study programme:	Mathematics (Single degree study, master II. deg., full time form)
Field of Study:	9.1.1. Mathematics
Type of Thesis:	Diploma Thesis
Language of Thesis:	English
Secondary language:	Slovak

Title: Skew-morphisms of abelian groups

Aim: The aim of the work is to gain insights into the structure of the skew-mprphisms of abelian groups that will allow us to construct or eventually classify skew-morphisms for infinite classes of abelian groups.

Supervisor:	doc. RNDr. Róbert Jajcay, PhD.
Department:	FMFI.KAGDM - Department of Algebra, Geometry and Didactics of Mathematics
Head of department:	prof. RNDr. Pavol Zlatoš, PhD.
Assigned:	28.11.2013
Approved:	02.12.2013

prof. RNDr. Ján Filo, CSc.
Guarantor of Study Programme

Student

Supervisor

46167309

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Martin Bachratý
Študijný program: matematika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: 9.1.1. matematika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: anglický
Sekundárny jazyk: slovenský

Názov: Skew-morphisms of abelian groups
Koso-morfizmy abelovskych grup

Cieľ: Cieľom práce je porozumenie štruktúry koso-morfizmov abelovských grúp, ktoré povedie ku konštrukcii a prípadnej klasifikácii koso-morfizmov pre nekonečné triedy abelovských grúp.

Vedúci: doc. RNDr. Róbert Jajcay, PhD.
Katedra: FMFI.KAGDM - Katedra algebry, geometrie a didaktiky matematiky
Vedúci katedry: prof. RNDr. Pavol Zlatoš, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 28.11.2013

Dátum schválenia: 02.12.2013

prof. RNDr. Ján Filo, CSc.
garant študijného programu

....

študent vedúci práce

I declare this thesis was written on my own, with the only help provided by my supervisor and the referred-to literature.

....

Acknowledgment

I would like to express my deep gratitude to Róbert Jajcay, my supervisor, for his patient guidance and useful critiques of this diploma thesis.

Abstract

A skew-morphism of a finite group G is a permutation φ of its elements fixing the identity such that for each $g \in G$ there exists a non-negative integer i_g satisfying $\varphi(gh) = \varphi(g)\varphi^{i_g}(h)$ for all $h \in G$. Skew-morphisms plays an important role in the study of regular Cayley maps and the theory of permutation groups.

In this thesis we study properties of skew-morphisms of abelian groups by investigating their powers. Using this approach we obtain new results, which help us better understand the structure of skew-morphisms of abelian, and in particular, cyclic groups. For the case of cyclic groups we present a complete classification of the class of coset-preserving skew-morphisms which is an important subclass of skew-morphisms.

Keywords: Skew-morphism; Cayley graph; Cayley map; embedding; power; abelian group; cyclic group.

Abstrakt

Koso-morfizmus konečnej grupy G je taká permutácia φ jej prvkov, ktorá zachováva identitu a spĺňa nasledujúcu vlastnosť: pre každý prvok $g \in G$ existuje nezáporné celé číslo i_g spĺňajúce $\varphi(gh) = \varphi(g)\varphi^{i_g}(h)$ pre všetky $h \in G$. Koso-morfizmy zohrávajú dôležitú úlohu pri štúdiu regulárnych Cayleyho máp aj v teórii permutačných grúp.

V tejto práci študujeme vlastnosti koso-morfizmov abelovských grúp pomocou skúmania ich mocnín. Použitím tohto prístupu sme získali nové výsledky, ktoré nám umožňujú lepšie pochopiť štruktúru koso-morfizmov pre abelovské, a konkrétne cyklické grupy. Pre cyklické grupy sme objavili kompletnú klasifikáciu triedy koso-morfizmov zachovávajúcich triedy jadra mocninovej funkcie, ktorá je dôležitou podtriedou všetkých koso-morfizmov.

Kľúčové slová Koso-morfizmus; Cayleyho graf; Cayleyho mapa; vnorenie; mocnina; abelovská grupa; cyklická grupa.

Contents

Chapter 1

Introduction

1.1 The main aim

The concept of a skew-morphism was first introduced by Jajcay and Širáň in [15] in the context of regular Cayley maps. Skew-morphisms constitute a special class of identity-preserving permutations of finite groups, and their structure helps us investigate Cayley maps. However, their structure is not fully understood even for the simplest classes of finite groups. For example, the complete classification of skew-morphisms for the class of cyclic groups is still not completed (see [16]), and the largest list of all skew-morphisms of cyclic groups [7] goes only up to the order 60.

In this thesis we use (and extend) an approach developed in [1] for the study of the skew-morphisms of abelian groups. This approach investigates skew-morphisms by studying their powers. We show that each non-trivial skew-morphism of an abelian group with a generating orbit possesses a power which is a non-trivial coset-preserving skew-morphism. Consequently, each non-trivial skew-morphism of a cyclic group possesses a power which is a non-trivial coset-preserving skew-morphism. This result underlines the importance of the class of coset-preserving skew-morphisms (introduced in Section 2.6) for understanding the structure of all skew-morphisms of cyclic groups. One of the main results of this thesis is a complete classification of coset-preserving skew-morphisms of cyclic groups.

1.2 Content of chapters

The thesis is organized as follows. In Chapter 1 we outline the aim of this thesis, introduce essential preliminaries and recap the short history of the problem. Definitions and properties concerning skew-morphisms along with examples are given in Chapter 2. In this chapter we also introduce coset-preserving skew-morphisms, an important subclass of skew-morphisms. This class plays an important role in Chapter 3, which is devoted to skew-morphisms of abelian groups and contains some of the main results of this thesis. In Chapter 4 we conclude this thesis and outline possible directions of our future research.

1.3 Brief history of skew-morphisms

One of the first results concerning Cayley maps is due to Biggs [3], who was the first to notice the connection between the existence of a special group automorphism and the regularity of, what we call today, a balanced Cayley map. These results were later extended by Širáň and Škoviera in the series of articles [20, 21, 22], who introduced antibalanced Cayley maps and antiautomorphisms. The paper [13] builds further on these results and introduces the concept of a rotary mapping and a rotary extension. These and several other results are generalized and unified by the concept of a skew-morphism introduced in [15].

Since their introduction, skew-morphisms were considered in many papers. One of the main branches of this research studies the class of the t-balanced skew-morphisms (see Section 2.6.1). Many interesting results on this topic are summarized in [8] and [11]. A complete classification of the t-balanced skew-morphisms for cyclic groups was introduced by Kwon in [17]. In [16], Kovács and Nedela ivestigate skew-morphisms of cyclic groups in the context of their associated Schur rings. Results in [14] and [1] indicate that skew-morphisms also play a role in the study of non-regular Cayley maps.

1.4 Cayley graphs and Cayley maps

In this thesis we study skew-morphisms regardless of whether they support a Cayley map or not. However, we include brief summary of the theory of Cayley maps, as it is the original and main motivation for the study of skew-morphisms. The fundamental theorems connecting skew-morphisms and Cayley maps are summarized in Section 2.2. For a survey of the theory of Cayley maps see [18]. For group-theoretic terms not defined here we refer the reader to [5] and for terms from topological graph theory to [12].

1.4.1 Cayley graphs

A concept similar to a concept of Cayley graphs were first considered by Cayley in [6]. Cayley graphs constitute a central tool in combinatorial and geometric group theory, for their high level of symmetry. We will use slightly different definition than that of Cayley, by which we obtain undirected graphs (Cayley's original definition produces colored directed graphs).

Definition 1 *Let G be a group and let X be a generating and symmetric set that does not contain the identity element of G, i.e., X generates the whole of G, for every $x \in X$ we have $x^{-1} \in X$ and $1_G \notin X$. The Cayley graph $\Gamma = \Gamma(G, X)$ is the simple loopless graph with the set of elements of G serving as the vertex set $V(\Gamma)$ and two vertices g and h adjacent if and only if $h^{-1}g \in X$.*

Note that, by the symmetry condition on X, we have $h^{-1}g \in X$ if and only if $(h^{-1}g)^{-1} = g^{-1}h \in X$, so the resulting Cayley graph Γ is undirected and well defined. It is also connected and loopless, as X generates G and does not contain 1_G. We demonstrate this definition on the following examples.

EXAMPLES (1) Let $G = (\mathrm{Z}_6, +)$ and let $X = \{1, 3, 5\}$. Note that X is symmetric, as $1 + 5 \equiv 0 \pmod 6$ and $3 + 3 \equiv 0 \pmod 6$. The vertex set of Cayley graph $\Gamma(G, X)$ is

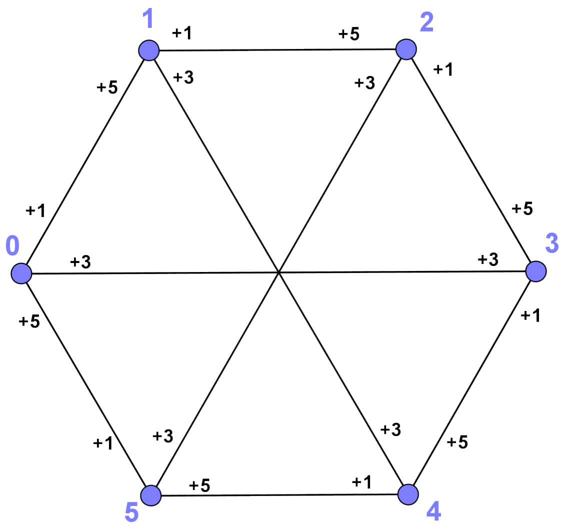

Fig. 1.1: Cayley graph $\Gamma(\mathrm{Z}_6, \{1,\ 3,\ 5\})$

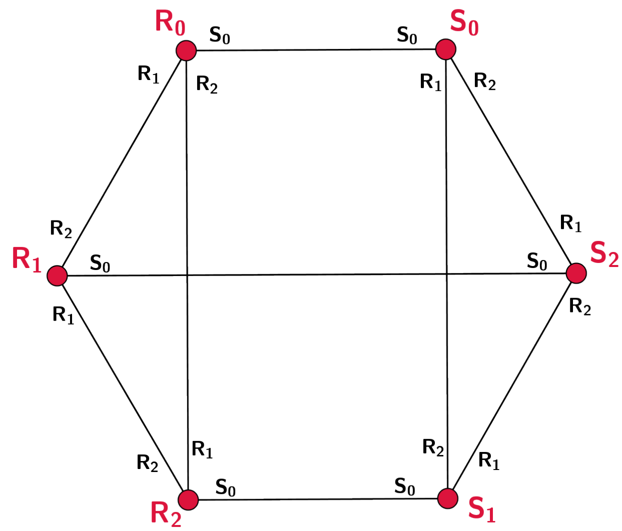

Fig. 1.2: Cayley graph $\Gamma(\mathfrak{D}_3, \{R_1,\ R_2,\ S_0\})$

$V(\Gamma) = \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ and the edge set consist of the following tuples:

$$E(\Gamma) = \{\{0,1\},\ \{0,3\},\ \{0,5\},\ \{1,2\},\ \{1,4\},\ \{2,3\},\ \{2,5\},\ \{3,4\},\ \{4,5\}\}.$$

The resulting Cayley graph is a vertex-transitive cubic graph of the order 6 (see Figure 1.1). Recall that graph Γ is vertex-transitive if for any two vertices $a,\ b \in V(\Gamma)$ there is a graph automorphism mapping a to b.

(2) Let $G = \mathfrak{D}_3$ be the dihedral group of the symmetries of the equilateral triangle. Let X be a set containing all non-trivial rotations and one of the reflections of equilateral triangle, i.e., $X = \{R_1,\ R_2,\ S_0\}$. The resulting Cayley graph $\Gamma(\mathfrak{D}_3, \{R_1,\ R_2,\ S_0\})$ is again vertex-transitive, cubic and of the order 6, but it is clearly non-isomorphic to the previous graph $\Gamma(\mathrm{Z}_6, \{1,\ 3,\ 5\})$, as only the latter one contains a triangle (see Figure 1.2).

The property of being a vertex-transitive graph in both of the previous examples is no coincidence. For each element $a \in G$, we can define an action L_a of a on a Cayley graph $\Gamma(G, X)$ via left multiplication, that is, $L_a(g) = ag$. A straightforward verification shows that the set of these translations forms a subgroup of $Aut(\Gamma(G, X))$ isomorphic to the underlying group G. As this action of G on $V(\Gamma)$ is transitive, every Cayley graph $\Gamma(G, X)$ is vertex-transitive. Moreover, we see that every Cayley graph $\Gamma(G, X)$ has a subgroup of

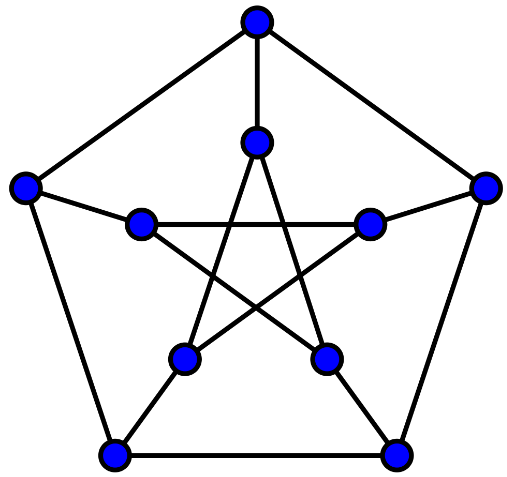

Fig. 1.3: The Petersen graph

$Aut(\Gamma(G, X))$ isomorphic to G acting regularly on its vertex set. It was shown in [19] that the converse also holds, thus we obtain the following characterization of Cayley graphs.

Theorem 1 (Sabidussi's Theorem) *A graph Γ is a Cayley graph of a group G if and only if it admits a regular action of G on $V(\Gamma)$ by graph automorphisms.*

All Cayley graphs are vertex-transitive, but the converse does not hold true. The smallest example of a non-Cayley vertex-transitive graph is the Petersen graph from Figure 1.3.

Because of their high level of symmetry, Cayley graphs play an important role in the study of highly symmetric objects. We will focus on their application in the study of regular maps that concerns the concept of a Cayley map.

1.4.2 Maps

To define a Cayley map, we must define a more general concept of an orientable map. *A surface S* is a connected (not necessarily compact) 2-manifold without boundary. From now on and throughout the paper, we will assume in addition that S is orientable and that it is oriented clockwise.

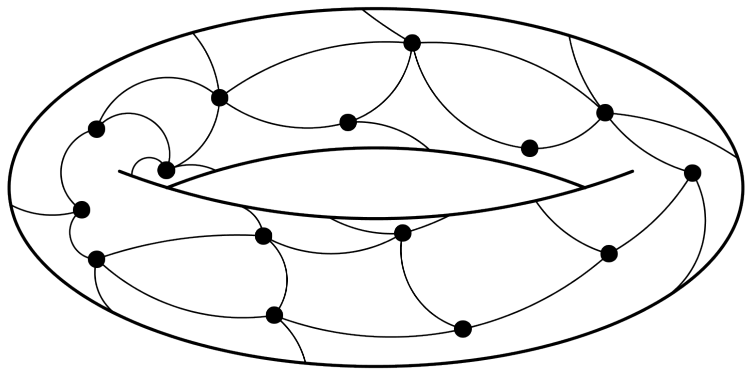

Fig. 1.4: A map on the torus

Definition 2 *An orientable map $\mathcal{M}$ is a 2-cell embedding of a graph Γ as a closed subset of a surface S. The graph Γ is the underlying graph of $\mathcal{M}$.*

The term '2-cell' means that each face of $\mathcal{M}$ (i.e., each component of the complement of the graph in the surface) is homeomorphic to the interior of the unit disc and 'closed' implies that the graph has no accumulation points as a topological subspace of the surface. The length of a face boundary, that is, the number of edges in a walk once around the perimeter of the face, is the covalence of the face. An example of an orientable map on the torus can be seen in Figure 1.4. From now on, by *a map* we will understand *an orientable map*. We note that the underlying graph of a map is always connected, as disconnected graphs does not admit a 2-cell embedding.

A map can be described in the following, purely algebraic way, which proves very useful in the study of its properties. Let $D(\mathcal{M})$ denote the set of darts of a map $\mathcal{M}$, (i.e., the set of edges with direction). Note that $|D(\mathcal{M})| = 2|E(\Gamma)|$, where Γ is the underlying graph of $\mathcal{M}$. The map $\mathcal{M}$ can be described in terms of two specific permutations of $D(\mathcal{M})$. The first permutation is λ, the dart-reversing involution associated with the underlying graph Γ (note that λ is independent of the embedding). The other permutation is ρ, defined as follows. For each dart $e \in D(\mathcal{M})$, $\rho(e)$ is the clockwise next dart of the embedded graph emanating from the same vertex as e. The full information about the embedding is carried by the pair λ, ρ of permutations of $D(\mathcal{M})$ in the following sense: Vertices, edges and faces

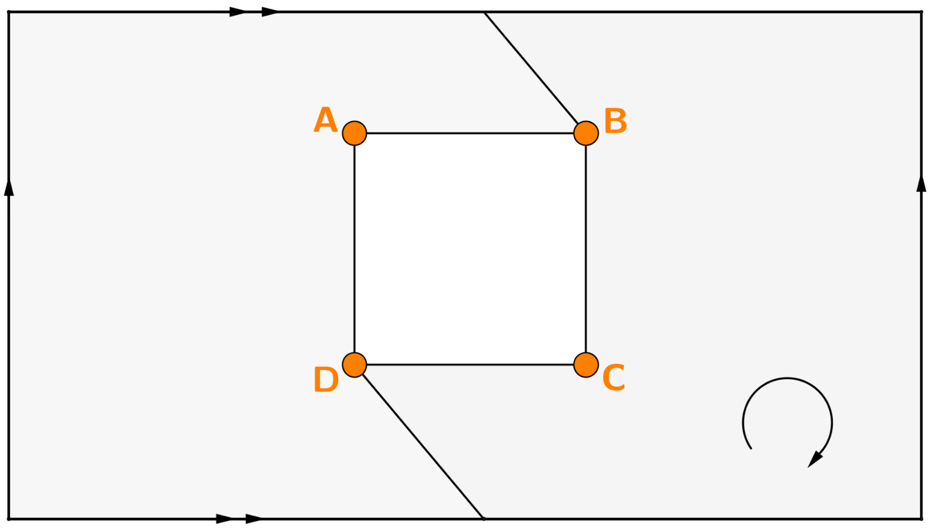

Fig. 1.5: An incorrect embedding of a graph

of $\mathcal{M}$ are represented by orbits of the permutations ρ, λ and $\rho\lambda$, respectively. Incidence between these elements is given by non-empty intersections of the corresponding orbits. We illustrate these observations in the following example.

EXAMPLES In both examples we consider embeddings of the complete graph on 4 vertices without one edge in the torus. We will denote this graph by Γ and its vertices by A, B, C and D, with the missing edge between A and C.

(1) In Figure 1.5 we see an embedding, which is not 2-cell, as the emphasized face is not homeomorphic to the interior of the unit disc. Thus, not every embedding of a connected graph gives rise to a map. One can also easily verify that this embedding is not a map, by simple counting argument using the Euler characteristic of the surface. Let $|V|$, $|E|$ and $|F|$ denote the number of vertices, edges and faces of a map. In this case, we have 4 vertices, 5 edges and 2 faces. If our embedding was indeed a map, then the Euler characteristic of the torus would be $\chi = |V| - |E| + |F| = 1$, which is not the case, as the Euler characteristic of the torus is $\chi = 0$.

(2) It is straightforward to check that the embedding of Γ in Figure 1.6 is a map. We will denote this map by $\mathcal{M}$. The number of faces of $\mathcal{M}$ is $\chi - |V| + |E| = 0 - 4 + 5 = 1$

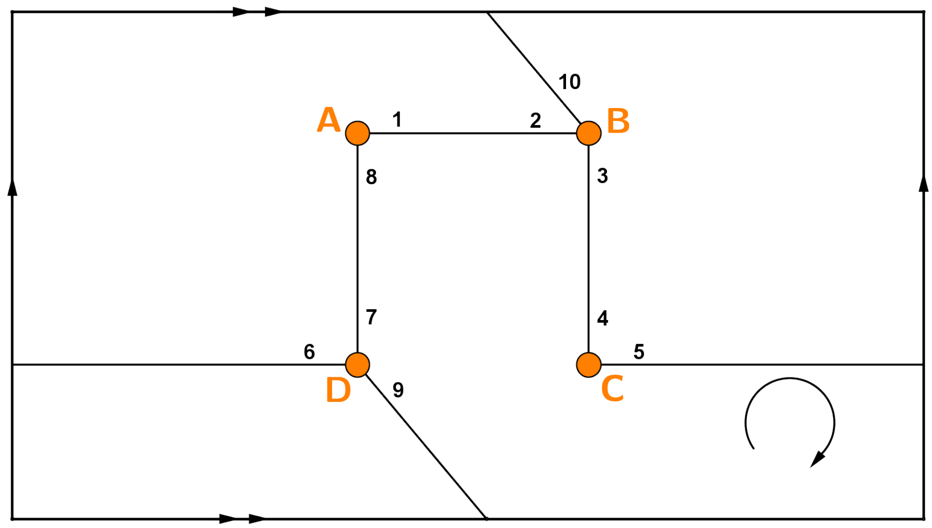

Fig. 1.6: A correct embedding of a graph

(note that each of the numbers χ, $|V|$, $|E|$, and $|F|$ is uniquely determined by the other three). The set of darts $D(\mathcal{M})$ has 10 elements. Adapting the notation from Figure 1.6 we have

$$\lambda = (1,8)(2,10,3)(4,5)(6,7,9), \quad \rho = (1,2)(3,4)(5,6)(7,8)(9,10),$$
$$\lambda\rho = (1,7,10,4,6,8,2,9,5,3)$$

We have the following one-to-one correspondence between the orbits of ρ and the vertices of Γ:

$$\mathcal{O}_{(1,8)} \leftrightarrow A \qquad \mathcal{O}_{(2,10,3)} \leftrightarrow B \qquad \mathcal{O}_{(4,5)} \leftrightarrow C \qquad \mathcal{O}_{(6,7,9)} \leftrightarrow D,$$

and the following one-to-one correspondence between the orbits of λ and the edges of Γ:

$$\mathcal{O}_{(1,2)} \leftrightarrow \{A,\ B\} \qquad \mathcal{O}_{(3,4)} \leftrightarrow \{B,\ C\} \qquad \mathcal{O}_{(5,6)} \leftrightarrow \{C,\ D\}$$
$$\mathcal{O}_{(7,8)} \leftrightarrow \{D,\ A\} \qquad \mathcal{O}_{(9,10)} \leftrightarrow \{D,\ B\}.$$

To find all edges incident with a vertex, e.g. vertex corresponding to the orbit $\mathcal{O}_{(2,10,3)}$ of ρ, we have to find all orbits of λ which contain one of the darts 2, 10 or 3. Thus the vertex which corresponds to the orbit $\mathcal{O}_{(2,10,3)}$ of ρ is incident with three edges corresponding to the three orbits $\mathcal{O}_{(1,2)}$, $\mathcal{O}_{(3,4)}$ and $\mathcal{O}_{(9,10)}$ of λ.

In what follows, we use the extended notation $\mathcal{M} = \mathcal{M}(\rho, \lambda)$ to denote the map whenever necessary. We proceed to define the automorphism group of a map.

Definition 3 *Let $\mathcal{M}(\rho, \lambda)$ be a map. The automorphism group $Aut(\mathcal{M})$ of the map $\mathcal{M}$ is the group of all permutations of the set $D(\mathcal{M})$ preserving the map structure (i.e., the incidence of vertices, edges and faces) of $\mathcal{M}$ and the orientation of the surface. In terms of permutations ρ and λ, the automorphism group $Aut(\mathcal{M})$ is formed by all permutations of the dart set $D(\mathcal{M})$ that commute with both ρ and λ.*

It is well-known [4] that the automorphism group of any map $\mathcal{M}$ acts semiregularly on its set of darts (i.e., the stabilizer of each of the darts in $Aut(\mathcal{M})$ is a trivial group). This implies the upper bound $|Aut(\mathcal{M})| \leq |D(\mathcal{M})|$. This leads to the definition of maps with the richest possible automorphism group.

A map $\mathcal{M}$ is a *regular map* if $|Aut(\mathcal{M})| = |D(\mathcal{M})|$. The study of regular maps is one of the main topics of the graph theory as it is related to many different branches of mathematics (the theory of Riemann surfaces, hyperbolic geometry, Galois theory, etc.).

1.4.3 Cayley maps

A regular action of the set of all left translations L_a on a vertices of a Cayley graph suggests a high level of symmetry of its embedding as a map. Since an automorphism of a map must preserve not only the structure of the underlying graph but also incidence of its faces and the orientation of the surface, the regular action will carry over only for embeddings that 'look the same' at each vertex. A precise formulation of this leads to the concept of the Cayley map.

Definition 4 *Let $\Gamma(G, X)$ be a Cayley graph, and let p be any permutation of the generating set X. A* Cayley map *$\mathcal{M} = CM(G, X, p)$ is a 2-cell embedding of the graph $\Gamma(G, X)$ with the property that for each vertex $g \in V(\Gamma)$, the cyclic permutation of darts (g, x), $x \in X$, induced by a clockwise orientation coincides with p.*

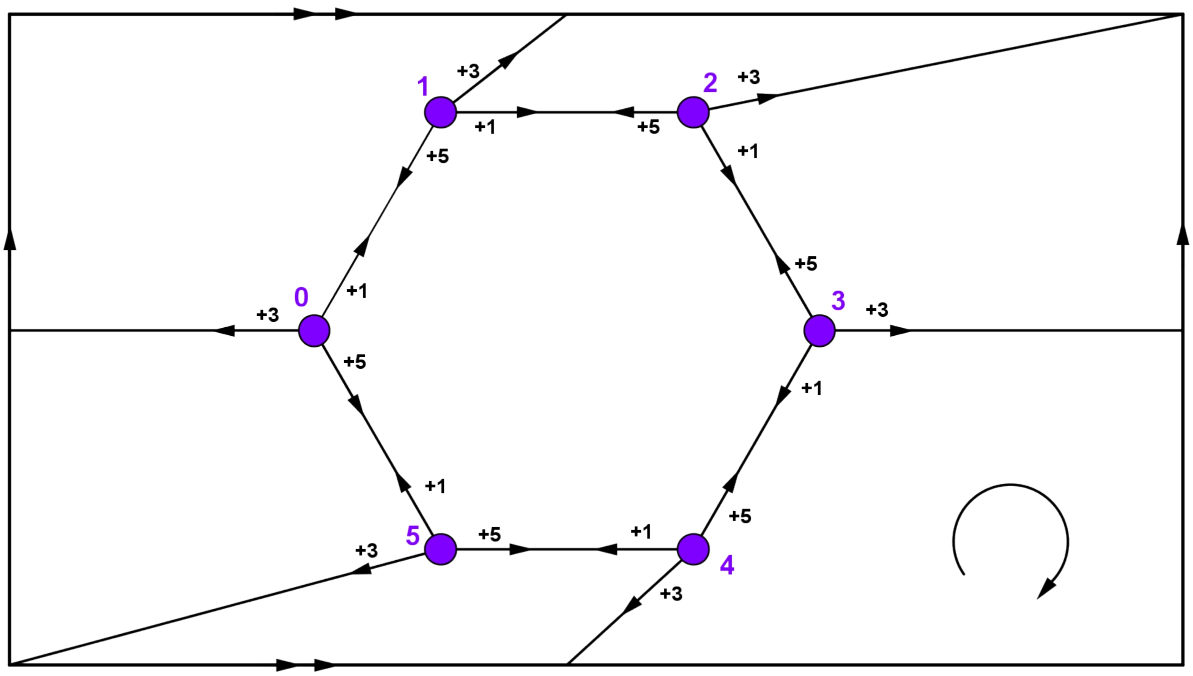

Fig. 1.7: A Cayley map

The action of G on itself via left multiplication in a Cayley map $\mathcal{M} = CM(G, X, p)$ induces, for each element $a \in G$, a map automorphism L_a of $\mathcal{M}$, $L_a(g, x) = (ag, x)$, for all $g \in G$ and $x \in X$. Thus, the automorphism group $Aut(\mathcal{M})$ of a Cayley map M acts transitively on the set of vertices via a copy of G. Note that for a Cayley map $\mathcal{M} = CM(G, X, p)$ we have $|D(\mathcal{M})| = |G| \cdot |X|$.

Combining our observations, we obtain the following bounds on the size of the automorphism group of a Cayley map $|G| \leq |Aut(\mathcal{M})| \leq |G| \cdot |X|$. A *regular Cayley map* is a Cayley map $\mathcal{M} = CM(G, X, p)$, which is regular, i.e., $|Aut(\mathcal{M})| = |G| \cdot |X|$.

The above definitions are demonstrated in the following example.

Example Consider the Cayley map $\mathcal{M}(\rho, \lambda) = CM(\mathrm{Z}_6, \{1, 3, 5\}, (1, 5, 3))$, shown in Figure 1.7. Let a_b denote a dart directed from the vertex a to the vertex b. The dart set of $\mathcal{M}$ consists of these 18 elements:

$$D(\mathcal{M}) = \{0_1, 0_3, 0_5, 1_2, 1_4, 1_0, 2_3, 2_5, 2_1, 3_4, 3_0, 3_2, 4_5, 4_1, 4_3, 5_0, 5_2, 5_4\}.$$

Using this notation we have

$$\lambda = (0_1, 1_0)\,(0_3, 3_0)\,(0_5, 5_0)\,(1_2, 2_1)\,(1_4, 4_1)\,(2_3, 3_2)\,(2_5, 5_2)\,(3_4, 4_3)\,(4_5, 5_4)$$
$$\rho = (0_1, 0_5, 0_3)\,(1_2, 1_0, 1_4)\,(2_3, 2_1, 2_5)\,(3_4, 3_2, 3_0)\,(4_5, 4_3, 4_1)\,(5_0, 5_4, 5_2).$$

We proceed to determine the number of automorphisms of $\mathcal{M}$. Let us first recall that we already know six automorphisms of $\mathcal{M}$, in particular all left translations L_a, for $a \in \mathrm{Z}_6$. Next suppose the following permutation of $D(\mathcal{M})$:

$$\upsilon = (0_1, 0_5, 0_3)\,(5_0, 3_0, 3_1)\,(1_2, 5_4, 3_2, 1_4, 5_2, 3_4)\,(2_1, 4_5, 2_3, 4_1, 2_5, 4_3).$$

Since $\upsilon\rho = \rho\upsilon$ and $\upsilon\lambda = \lambda\upsilon$, we have $\upsilon \in Aut(\mathcal{M})$.

We proceed by considering the following 18 automorphisms of $\mathcal{M}$ generated by L_0, L_1, L_2, L_3, L_4, L_5 and υ:

$$L_0,\ \upsilon,\ \upsilon^2,\ L_1,\ L_1\upsilon,\ L_1\upsilon^2,\ L_2,\ L_2\upsilon,\ L_2\upsilon^2,\ L_3,\ L_3\upsilon,\ L_3\upsilon^2,\ L_4,\ L_4\upsilon,\ L_4\upsilon^2,\ L_5,\ L_5\upsilon,\ L_5\upsilon^2.$$

These automorphisms are all distinct, as

$$\begin{array}{lll}
L_0(0_1) = 0_1, & \upsilon(0_1) = 0_5, & \upsilon^2(0_1) = 0_3, \\
L_1(0_1) = 1_2, & L_1\upsilon(0_1) = 1_0, & L_1\upsilon^2(0_1) = 1_4, \\
L_2(0_1) = 2_3, & L_2\upsilon(0_1) = 2_1, & L_2\upsilon^2(0_1) = 2_5, \\
L_3(0_1) = 3_4, & L_3\upsilon(0_1) = 3_2, & L_3\upsilon^2(0_1) = 3_0, \\
L_4(0_1) = 4_5, & L_4\upsilon(0_1) = 4_3, & L_4\upsilon^2(0_1) = 4_1, \\
L_5(0_1) = 5_0, & L_5\upsilon(0_1) = 5_4, & L_5\upsilon^2(0_1) = 5_2.
\end{array}$$

Thus, we have $18 \le |Aut(\mathcal{M})| \le |G| \cdot |X| = 6 \cdot 3 = 18$, hence $|Aut(\mathcal{M})| = 18$. So the Cayley map $CM(\mathrm{Z}_6, \{1,\ 3,\ 5\}, (1, 5, 3))$ is a regular Cayley map.

Chapter 2

Properties of skew-morphisms

In this chapter we introduce the concept of a skew-morphism. Definition and basic examples of skew-morphisms are presented in Section 2.1. Before we proceed to investigate properties of skew-morphisms, we introduce in Sections 2.2 and 2.3 fundamental theorems connecting skew-morphisms and the theories of Cayley maps and permutation groups. Basic properties of skew-morphisms for arbitrary groups are summarized in Section 2.4, while Section 2.5 is devoted to properties of skew-morphisms of abelian groups. In Section 2.6 we introduce two important subclasses of skew-morphisms — t-balanced skew-morphisms and coset-preserving skew-morphisms, which play a key role in Chapter 3. Powers of skew-morphisms (as powers of permutations) are studied in Section 2.7

2.1 Definition and examples of skew-morphisms

The following definition of a skew-morphism is due to Jajcay and Širáň [15].

Definition 5 *Let G be a finite group (from now on and throughout the thesis we restrict ourself to finite groups). A permutation $\varphi : G \to G$ is a skew-morphism of G if it stabilizes the unit element of G, that is $\varphi(1_G) = 1_G$, and for each $g \in G$ there exist a non-negative integer i such that*

$$\varphi(gh) = \varphi(g)\varphi^i(h), \text{ for each } h \in G.$$

The order of φ is the smallest positive integer $|\varphi| = n$ for which φ^n is the identity permutation $\mathrm{id_G}$*. The orbit of an arbitrary element $g \in G$ of a skew-morphism φ will be denoted by $\mathcal{O}_g$.*

Note that the order of a skew-morphism is always finite, as we restrict ourself to finite groups. Any group automorphism is also a skew-morphism with $i = 1$ for all $g \in G$, thus the concept of a skew-morphism is a generalization of the concept of a group automorphism.

The powers i from the above definition are uniquely determined in the following sense (as proved in [15]). If φ is a skew-morphism of a group G, then for each $g \in G$ there is an unique non-negative integer $\pi(g) < |\varphi|$ such that

$$\varphi(gh) = \varphi(g)\varphi^{\pi(g)}(h), \text{ for each } h \in G. \tag{2.1}$$

Moreover, if $\varphi \neq \mathrm{id}_G$ then $\pi(g) > 0$ for each $g \in G$. We call a mapping $\pi : G \to \{0, 1, 2, \ldots, |\varphi| - 1\}$ a *power function* of φ. If φ is non-identity, then the power function of φ is a mapping $\pi : G \to \{1, 2, \ldots, |\varphi| - 1\}$.

Let φ be a skew-morphism of G with the power function π, let k be a positive integer and let $g \in G$. We will denote by $\pi(k, g)$ the sum of power functions of k consecutive elements of φ, starting with the element g, i.e., $\pi(k, g) = \pi(g) + \pi(\varphi(g)) + \cdots + \pi(\varphi^{k-1}(g))$. Note that $\pi(1, g) = \pi(g)$.

We demonstrate the above definitions on the following examples.

Examples (1) Let $\varphi = (1, 5, 3)$ be a permutation of a cyclic group $\mathrm{Z}_6 = (\mathrm{Z}_6, +)$. This permutation is identity-preserving, as $\varphi(0) = 0$. The permutation φ is a skew-morphism if and only if there exist a power function $\pi : \mathrm{Z}_6 \to \{1, 2\}$ such that $\varphi(g+h) = \varphi(g)+\varphi^{\pi(g)}(h)$, for each $g, h \in \mathrm{Z}_6$. We proceed to find this function or to prove that it does not exist. Recall that if the power function exists, then it is unique.

As $\varphi(2) = 2$, we have

$$\varphi(1 + 1) = \varphi(2) = 2 = 5 + 3 = \varphi(1) + \varphi(1)^2,$$

thus, if π exists, then $\pi(1) = 2$. In a completely analogous way we obtain $\pi(3) = 2$ and $\pi(5) = 2$. Take $h = 2, 4, 6$ and consider the following calculations

$$\varphi(0 + h) = h = 0 + h = \varphi(0) + \varphi(h).$$

Thus, if π exists, then necessarily $\pi(0) = \pi(2) = \pi(4) = 1$.

One can easily verify that $\varphi = (1, 5, 3)$ and $\pi : \mathrm{Z}_6 \to \{1, 2\}$, defined by $\pi(2i) = 1$ and $\pi(2i + 1) = 2$ for $i = 0, 1, 2$, satisfy the equation $\varphi(g + h) = \varphi(g) + \varphi^{\pi(g)}(h)$, for each $g, h \in \mathrm{Z}_6$. Hence, φ is a skew-morphism of Z_6 with the power function π.

(2) Let $\varphi = (1, 5, 3, 7)\,(2, 6, 4)$ be an identity-preserving permutation of a cyclic group Z_8. Suppose that φ is a skew-morphism of Z_8 with the power function π.

As $\varphi(0) = 0$, we have

$$\varphi(5 + 3) = \varphi(0) = 0 = 3 + 5 = \varphi(5) + \varphi^3(3),$$

hence $\pi(5) \equiv 3 \pmod 4$ as $|\mathcal{O}_3| = 4$. On the other hand

$$\varphi(5 + 2) = \varphi(7) = 1 = 3 + 6 = \varphi(5) + \varphi(2),$$

thus $\pi(5) \equiv 1 \pmod 3$ as $|\mathcal{O}_2| = 3$. The only solution of the two congruences modulo $|\varphi| = 12$ equals 7, and thus, $\pi(5) = 7$. But then

$$6 = \varphi(2) = \varphi(5 + 5) = \varphi(5) + \varphi^7(5) = 3 + 1 = 4,$$

which is a contradiction. Thus φ is not a skew-morphism of Z_8.

Basic properties of a power function, some of which we already mentioned, are summarized in the following lemma.

Lemma 1 ([15]) *Let φ be a skew-morphism of a group G with the power function π. Then the following hold:*

(i) *For any $g \in G$ the equation $\varphi(gh) = \varphi(g)\varphi^i(h)$ holds for each $h \in G$ if and only if $i \equiv \pi(g) \pmod{|\varphi|}$;*

(ii) *If* $\pi(g) = 0$ *for some* $g \in G$*, then* φ *is an identity permutation;*

(iii) $\pi(1_G) = 1$*;*

(iv) *For any* $g, h \in G$ *we have*

$$\pi(gh) \equiv \sum_{i=0}^{\pi(g)-1} \pi(\varphi^i(h)) \equiv \pi(\pi(g), h) \pmod{|\varphi|}.$$

For convenience, we use the following notation of the power function. Let

$$\varphi = (a_1, \varphi(a_1), \ldots, \varphi^{i_1-1}(a_1))\,(a_2, \ldots, \varphi^{i_2-1}(a_2)) \cdots (a_j, \ldots, \varphi^{i_j-1}(a_j))$$

be a skew-morphism of a group G with the power function π. We will write π in the form

$$[\pi(a_1),\, \pi(\varphi(a_1)),\, \ldots, \pi(\varphi^{i_1-1}(a_1))]\,[\pi(a_2),\, \ldots, \pi(\varphi^{i_2-1}(a_2))]\, \ldots\, [\pi(a_j),\, \ldots, \pi(\varphi^{i_j-1}(a_j))].$$

For example we will write the power function of the skew-morphism $\varphi = (1, 5, 3)$ of Z_6 from the above example as $[2, 2, 2]$. Note that this notation does not hold the complete information of π as it does not include values of π of stabilized elements of φ.

2.2 Skew-morphisms and Cayley maps

In this section we present several theorems introduced in [15] and [1] that connect the concept of skew-morphisms and the theory of Cayley maps. The first of these theorems sums up the relevance of skew-morphisms for regular Cayley maps.

Theorem 2 ([15]) *A Cayley map* $\mathcal{M} = CM(G, X, p)$ *is regular if and only if there exists a skew-morphism* φ *of* G *such that* $\varphi(x) = p(x)$ *for all* $x \in X$*.*

Such a skew-morphism for a regular Cayley map $\mathcal{M}$ is uniquely determined and will be referred to as the *skew-morphism associated to* $\mathcal{M}$. The above theorem extends to a characterization of groups admitting regular Cayley maps.

Theorem 3 ([15]) *A group G admits a regular Cayley map $\mathcal{M} = CM(G, X, p)$ if and only if there exists a skew-morphism φ of G that has a symmetric orbit X that generates the group G.*

Throughout the thesis we will often refer to skew-morphisms that are relevant for regular Cayley maps, i.e., skew-morphisms that has a symmetric orbit which generates the whole group. We will call them *skew-morphisms that give rise to regular Cayley maps.*

We proceed to introduce the concept of a $(1/k)$-regular Cayley maps. Let $\mathcal{M}$ be a Cayley map. An action of a subgroup $H \leq Aut(\mathcal{M})$ is said to be $(1/k)$-dart-transitive if H acts on the set $D(\mathcal{M})$ of darts of $\mathcal{M}$ via k orbits. We say that Cayley map $\mathcal{M}$ is $(1/k)$-regular if it is not $(1/j)$-regular for any $0 < j < k$ and its full automorphism group $Aut(M)$ acts $(1/k)$-transitively on $D(\mathcal{M})$(by 1/1-regularity of $\mathcal{M}$ we mean regularity of $\mathcal{M}$).

The last theorem of this section, which generalize Theorem 2.4 from [14], is an analogue of Theorem 2 for the case of $(1/k)$-regular Cayley maps.

Theorem 4 ([1]) *Let k be a positive integer and $\mathcal{M} = CM(G, X, p)$ be a Cayley map that is not $(1/j)$-regular for any $0 < j < k$. Then $\mathcal{M}$ is $(1/k)$-regular if and only if there exists a skew-morphism φ of G whose restriction to X is equal to p^k.*

The above theorem states that skew-morphisms are relevant also in the study of Cayley maps which are not regular.

2.3 Skew-morphisms and permutation groups

Before presenting the result that connect skew-morphisms with the theory of permutation groups, we need to introduce a few concept of this theory. For a survey of the theory of permutation groups see [5].

Let G be a (finite) group and let g be an arbitrary element of G. Then we can define the permutation g_L of G by $g_L(h) = gh$ for each $h \in G$. Let G_L denote the permutation group induced by these permutations. Note that G is isomorphic to G_L under the mapping $g \mapsto g_L$. We will denote by $\mathrm{Sym}(G)$ the group of all permutations of the set of elements of G. Thus, G_L is a subgroup of $\mathrm{Sym}(G)$.

For an arbitrary groups $H_1, H_2 \leq \mathrm{Sym}(G)$ we denote by H_1H_2 the subgroup generated by all elements of the form $h_1h_2 = h_2 \circ h_1$ where $h_1 \in H_1$ and $h_2 \in H_2$. Note that $H_1H_2 \leq \mathrm{Sym}(G)$. The subgroup generated by the permutation $\tau \in \mathrm{Sym}(G)$ will be denoted by $\langle \tau \rangle$.

The following theorem characterizes skew-morphisms in terms of permutation groups.

Theorem 5 ([1]) *Let G be a group, and let φ be a permutation of G that fixes 1_G. Then φ is skew-morphism of G if and only if $|G_L\langle\varphi\rangle| = |G_L| \cdot |\varphi|$.*

Note that the characterization in terms of permutation groups does not use the concept of the power function.

2.4 Basic properties of skew-morphisms

In this section we present several basic properties of skew-morphisms introduced in [1] and [15] that will be useful throughout this thesis.

The definition of a skew-morphism of G tells us that $\varphi(gh) = \varphi(g)\varphi^{\pi(g)}(h)$ for any $g,\ h \in G$. We obtain the formula for computing $\varphi^2(gh)$ by the following calculation:

$$\begin{aligned}\varphi^2(gh) &= \varphi(\varphi(gh)) = \varphi(\varphi(g) \cdot \varphi^{\pi(g)}(h)) = \\ &= \varphi(\varphi(g))\, \varphi^{\pi(\varphi(g))}(\varphi^{\pi(g)}(h)) = \\ &= \varphi^2(g)\, \varphi^{\pi(g)+\pi(\varphi(g))}(h).\end{aligned}$$

As the exponent $\pi(g)+\pi(\varphi(g))$ equals $\pi(2,g)$, we obtain the formula $\varphi^2(gh) = \varphi^2(g)\,\varphi^{\pi(2,g)}(h)$ for each $g,\, h \in G$.

We proceed to calculate $\varphi^3(gh)$. Using the formula for $\varphi^2(gh)$ we obtain

$$\varphi^3(gh) = \varphi(\varphi^2(gh)) = \varphi(\varphi^2(g)\,\varphi^{\pi(g)+\pi(\varphi(g))}(h)) =$$

$$= \varphi(\varphi^2(g))\, \varphi^{\pi(\varphi^2(g))}(\varphi^{\pi(g)+\pi(\varphi(g))}(h)) =$$
$$= \varphi^3(g)\, \varphi^{\pi(g)+\pi(\varphi(g))+\pi(\varphi^2)(g)}(h).$$

As $\pi(g) + \pi(\varphi(g)) + \pi(\varphi^2)(g) = \pi(3, g)$, we obtain the formula $\varphi^3(gh) = \varphi^3(g)\, \varphi^{\pi(3,g)}(h)$ for each g, $h \in G$.

By an induction argument on the exponent i of φ^i one can easily verify that for any positive integer k we have

$$\varphi^k(gh) = \varphi^k(g)\, \varphi^{\pi(k,g)}(h) \text{ for each } g,\, h \in G. \tag{2.2}$$

The above equation plays key role in Section 2.7, which is devoted to the study of powers of skew-morphisms.

We proceed to present important algebraic properties of the power function π of a skew-morphism φ of G (we will suppose that φ is non-trivial). We begin with the investigation of the set $\ker \pi = \{g \in G \mid \pi(g) = 1\}$. Note that, by Lemma 1 (iii), we have $1_G \in \ker \pi$ and $\ker \pi$ is closed under group multiplication as for g, $h \in \ker \pi$ we have

$$\pi(gh) = \pi(\pi(h), g) = \pi(1, g) = \pi(g) = 1.$$

The set $\ker \pi$ is also closed under taking inverses, since, for $g \in \ker \pi$

$$1 = \pi(1_G) = \pi(g^{-1}g) = \pi(\pi(g), g^{-1}) = \pi(1, g^{-1}) = \pi(g^{-1}),$$

thus $g^{-1} \in \ker \pi$ as well. Summing up, we proved that $\ker \pi$ is subgroup of G.

Using similar arguments based on Equation 2.1, we can prove that also the set $\operatorname{Fix} \varphi$ of elements fixed by φ form a subgroup of G. These results and several others are summarized in the following lemma (see [15] for the complete proof).

Lemma 2 ([15]) *Let φ be a skew-morphism of a group G with the power function π. Then the following hold:*

(i) *The set* $\ker \pi = \{g \in G \mid \pi(g) = 1\}$ *is a subgroup of G;*

(ii) $\pi(g) = \pi(h)$ *if and only if* g *and* h *belong to the same right coset of the subgroup* $\ker\pi$ *in* G*;*

(iii) *The set* $\mathrm{Fix}\,\varphi = \{g \in G \mid \varphi(g) = g\}$ *is a subgroup of* G*;*

(iv) $\pi(ghg^{-1}) = 1$ *for all* $h \in \ker\pi \cap \mathrm{Fix}\,\varphi$ *and all* $g \in G$*;*

(v) *The group* $\ker\pi \cap \mathrm{Fix}\,\varphi$ *is a normal subgroup of* $\mathrm{Fix}\,\varphi$.

2.5 Properties of skew-morphisms of abelian groups

The aim of this thesis is the study of skew-morphisms of abelian and, in particular, cyclic groups. In the abelian case, skew-morphisms satisfy many additional useful properties, which do not hold in general for non-abelian groups. Some of these properties are presented in this section.

Let φ be a skew-morphism of an abelian group A with the power function π. Recall that the set $\ker\pi = \{a \in A \mid \pi(a) = 1\}$ is a subgroup of A. Let us first consider the following calculation for arbitrary elements $a \in \ker\pi$ and $b \in A$:

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

hence $\varphi^{\pi(b)}(a) = \varphi(a)$ for all $a \in \ker\pi$ and $b \in A$. It follows that any $a \in \ker\pi$ is either a fixed element of φ, or $\pi(b) \equiv 1$ modulo the length $|\mathcal{O}_a|$ of the orbit of a for each $b \in A$.

Using this observation, it was shown in [8] that in the case of abelian groups, a skew-morphism φ preserves $\ker\pi$ setwise (the proof is based on computing the image under φ of the products of the form $\varphi(a)b$ in two different ways). Consequently, the restriction of φ to the group $\ker\pi \leq A$ is a group automorphism of $\ker\pi$, as $\varphi(ab) = \varphi(a)\varphi(b)$ for each $a,\, b \in \ker\pi$.

We proceed to investigate the value of the power function of a fixed element of a skew-morphism. Suppose that $a \in A$ is fixed by φ, i.e., $\varphi(a) = a$. Then for any $b \in A$ we have

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

and

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

As A is abelian we have $ab = ba$, and thus, $\varphi(ab) = \varphi(ba)$. It follows that $\varphi^{\pi(a)}(b) = \varphi(b)$ for each $b \in A$, hence $\pi(a) = 1$.

These results are summarized in the following lemma.

Lemma 3 ([8]) *Let φ be a skew-morphism of an abelian group A with the power function π. Then the following hold:*

(i) *The skew-morphism φ preserves* $\ker\pi$ *setwise, i.e.,* $\varphi(\ker\pi) = \ker\pi$*;*

(ii) *The restriction of φ to* $\ker\pi$ *is a group automorphism of* $\ker\pi$*;*

(iii) *For each $a \in A$, the number $\pi(a)$ is congruent to* 1 *modulo the length of every non-trivial orbit of φ on* $\ker\pi$*;*

(iv) *If $a \in A$ is stabilized by φ, i.e, $\varphi(a) = a$, then $\pi(a) = 1$; in particular, $\pi(1_A) = 1$.*

We proceed to illustrate an important property of skew-morphisms of abelian groups on the following example.

Example A permutation $\varphi = (1, 5, 15, 13, 17, 9, 7, 11, 3)\,(2, 8, 14)\,(4, 16, 10)$ of a group Z_{18} which appears on the list [7] is a skew-morphism of Z_{18}. The distribution of the values of the power function on the orbits of φ is

[8, 5, 2, 8, 5, 2, 8, 5, 2] [7, 7, 7] [4, 4, 4].

Thus the group $\ker\pi \le Z_{18}$ consist of elements 0, 6 and 12 and is isomorphic to Z_3. As all elements of $\ker\pi$ are fixed by φ, an automorphism of $\ker\pi$ induced by φ is the identity. Note that the above notation holds complete information about the power function, since the values of π for stabilized elements are 1 by Lemma 3 (iv).

For us, the most important property is the periodic distribution of the power function on the orbits of φ (with period 3 for the orbit $\mathcal{O}_1$, and period 1 for orbits $\mathcal{O}_2$ and $\mathcal{O}_4$). We proceed to specify the concept of a periodicity of power functions, which is relevant for all skew-morphisms of abelian groups.

We will consider the concept of the *periodicity* (of the power function) in the following sense. Let φ be a skew-morphism of an abelian group A with the power function π. We define the *periodicity of an element* $a \in A$ as the smallest positive integer p_a such that $\pi(a) = \pi(\varphi^{p_a}(a))$. We claim that the periodicities of two arbitrary elements a and b belonging to the same orbit of φ are always the same, i.e., $p_a = p_b$ for each a, $b \in \mathcal{O}_a$.

First, observe that for any positive integer l and any $h \in \ker\pi$ and $g \in A$ we have

$$\varphi^l(hg) = \varphi^l(h)\,\varphi^{\pi(l,h)}(g) = \varphi^l(h)\varphi^l(g)$$

as

$$\pi(l,h) = \sum_{i=0}^{l-1} \pi(\varphi^i(h)) = \sum_{i=0}^{l-1} 1 = l.$$

Since $\pi(a) = \pi(\varphi^{p_a}(a))$, elements a and $\varphi^{p_a}(a)$ belong to the same right coset of $\ker\pi$ by Lemma 2 (ii). Therefore there exists $h_a \in \ker\pi$ such that $\varphi^{p_a}(a) = h_a a$. As a and b belong to the same orbit we have $b = \varphi^k(a)$ for some positive integer k. Now consider the following calculation:

$$\begin{aligned}\varphi^{p_a}(b) = \varphi^{p_a}(\varphi^k(a)) = \varphi^{p_a+k}(a) = \varphi^k(\varphi^{p_a}(a)) = \\ = \varphi^k(h_a a) = \varphi^k(h_a)\varphi^k(a) = \\ = \varphi^k(h_a)\,b.\end{aligned}$$

Note that $\varphi^k(h_a) \in \ker\pi$ by Lemma 3 (i), and thus, $\varphi^{p_a}(b)$ and b belong to the same right coset of $\ker\pi$. It follows that $\pi(b) = \pi(\varphi^{p_a}(b))$, hence $p_b \leq p_a$. On the other hand we have $\pi(a) = \pi(\varphi^{p_b}(a))$ and consequently $p_a \leq p_b$. Combining both inequalities we obtain $p_a = p_b$.

The above observation allows us to define the *periodicity of an orbit* $\mathcal{O}$ of φ, denoted by $p_{\mathcal{O}}$, as the periodicity of any $a \in \mathcal{O}$. The *periodicity of a skew-morphism* φ denoted by

p_φ, is defined to be the smallest positive integer such that $\pi(a) = \pi(\varphi^{p_\varphi}(a))$ for all $a \in A$, or equivalently, as the least common multiple of periodicities of all orbits of φ.

Another important property of the periodicity states that periodicities of elements a, $b \in A$ that belong to the same right coset are the same, i.e., if $\pi(a) = \pi(b)$, then $p_a = p_b$. To verify this, first note that there exists $h_a \in \ker \pi$ such that $b = h_a a$, as $\pi(a) = \pi(b)$. Thus for any positive integer k we have

$$\varphi^k(b) = \varphi^k(h_a a) = \varphi^k(h_a)\varphi^k(a).$$

As $\varphi^k(h_a) \in \ker \pi$ we have $\pi(\varphi^k(a)) = \pi(\varphi^k(b))$ for any positive integer which proves our claim. Moreover, if we take $k = 1$, we obtain $\pi(\varphi(a)) = \pi(\varphi(b))$, which means that for any element $a \in A$, the value of the power function at $\varphi(a)$ is uniquely determined by its value at a.

The most important properties of the periodicity of skew-morphisms of abelian groups are summarized in the following lemma.

Lemma 4 *Let φ be a skew-morphism of an abelian group A with the power function π. Then the following hold:*

(i) *If a, b belong to the same orbit of φ, then $p_a = p_b$;*

(ii) *If $\pi(a) = \pi(b)$ for a, $b \in A$, then $\pi(\varphi(a)) = \pi(\varphi(b))$ and $p_a = p_b$;*

(iii) *The periodicity p_a equals 1 for each $a \in \ker \pi$;*

(iv) *The number p_a divides both $|\mathcal{O}_a|$ and $|\varphi|$;*

(v) *The values $\pi(a)$ and $\pi(\varphi^k(a))$ are the same for some positive integer k if and only if $p_a \mid k$;*

(vi) *The periodicity p_a of $a \in A$ divides the number $\pi(p_a, b)$ for each $b \in \mathcal{O}_a$;*

(vii) *If a and b belong to the same orbit of φ, then $\pi(p_a, a) = \pi(p_a, b)$ and $\pi(jp_a, b) = j \cdot \pi(p_a, b)$ for any positive integer j;*

(viii) *The periodicity p_{ab} of the product of elements a, $b \in A$ divides the least common multiple of periodicities of a and b, i.e., $p_{ab} \,|\, \mathrm{lcm}(p_a, p_b)$;*
in particular, $p_{a_1 a_2 \ldots a_k} \,|\, \mathrm{lcm}(p_{a_1}, p_{a_2}, \ldots, p_{a_k})$ for $a_1, \ldots, a_k \in A$.

Proof. The properties (i), (ii), (iv) follow directly from our previous calculations. The property (iii) is a straightforward consequence of the fact that φ preserves $\ker \pi$. For the proof of properties (v) and (vi) we refer the reader to [1]. The property (vii) follows from (i) and definition of the periodicity. We proceed to prove the property (viii).

First observe that for any $c \in A$ we have $\pi(c) = \pi(\varphi^{ip_c}(c))$ for any positive integer i, and thus, $\varphi^{ip_c}(c) = hc$ for some $h \in \ker \pi$. Let $p = \mathrm{lcm}(p_a, p_b)$ and let k_a and k_b denote positive integers satisfying $p = p_a k_a = p_b k_b$. Consider the following calculation:

$$\begin{aligned} \varphi^p(ab) &= \varphi^p(a)\, \varphi^{\pi(p,a)}(b) = \\ &= \varphi^{k_a p_a}(a)\, \varphi^{ip_b}(b) = \\ &= h_1 a h_2 b = h_1 h_2 ab, \end{aligned}$$

for some positive integer i and h_1, $h_2 \in \ker \pi$. The first equation holds by Equation 2.2 and the third equation is a consequence of the above observation.

To prove the key second equation, note that $\pi(p, a) = \pi(p_a k_a, a) = \pi(p_a, a) k_a$ by (vii) and $\pi(p_a, a) = jp_a$ for some positive integer j by (vi). Thus

$$\pi(p, a) = \pi(p_a, a) k_a = jp_a k_a = jp = jk_b p_b = ip_b$$

for a positive integer $i = jk_a$.

Hence $\varphi^p(ab)$ and ab belong to the same right coset of $\ker \pi$, and thus, $p_{ab} \,|\, p$ by the property (v). The second part of (viii) can be easily obtained by induction. □

2.6 Subclasses of skew-morphisms

In this section we present t-balanced and coset-preserving skew-morphisms, two important subclasses of skew-morphisms. Both of them plays an important role as fundamental tools for studying and constructing skew-morphisms of abelian groups (see Section 3.2). The concept of t-balanced skew-morphisms arisen in the context of t-balanced Cayley maps, which is a natural generalization of the previously studied notions of balanced and anti-balanced Cayley maps introduced in [20]. The concept of coset-preserving skew-morphisms is a generalization of t-balanced skew-morphisms and was introduced in [1].

2.6.1 t-balanced skew-morphisms

The following definition of a t-balanced regular Cayley map can be found in, e.g., [8]. Let $\mathcal{M} = CM(G, X, p)$ be a regular Cayley map with an associated skew-morphism φ and the power function π. We will say that the map $\mathcal{M}$ is t-balanced, for $t \not\equiv 1 \pmod{|X|}$, if $\pi(x) = t$ for each $x \in X$.

Consequently, a t-balanced skew-morphism was defined as a skew-morphism associated to some t-balanced regular Cayley map. The power function π of a t-balanced skew-morphism φ admits only two values, namely 1 and t, and the set $\ker \pi$ is preserved by φ (see [8]). A complete classification of t-balanced regular Cayley maps for the class of cyclic groups through sets of admissible parameters was presented in [17].

We will use a slightly different definition of a t-balanced skew-morphism that no longer requires the existence of a generating orbit that is closed under taking inverses.

Definition 6 *Let φ be a skew-morphism of a group G with the power function π. We will say that φ is t-balanced for a positive integer $t \neq 1$ if the power function π admits exactly two values 1 and t and if φ preserves $\ker \pi$ setwise.*

Note that the above definition extends the original definition introduced for regular Cayley maps, as the power function π of a skew-morphism φ associated to a t-balanced regular Cayley map always admits exactly two distinct values 1 and t and the skew-morphism φ preserves $\ker \pi$. Also note that a group automorphism is not a t-balanced skew-morphism, as the power function of an automorphism admits only value 1. We proceed to introduce some properties of t-balanced skew-morphisms.

Let φ be a t-balanced skew-morphism of a group G with the power function π. First observe that the index of the subgroup $\ker\pi$ in G is $[G : \ker\pi] = 2$ as π admits exactly two values. Since the set $\pi^{-1}(t) = \{g \in G \mid \pi(g) = t\}$ is the complement of the set $\ker\pi$, which is preserved by φ, it is preserved by φ as well. Thus for each g, $h \in G$ that belong to the same orbit of φ we have $\pi(g) = \pi(h)$.

Applying this observation we obtain

$$\pi(k, g) = \pi(g) + \pi(\varphi(g)) + \cdots + \pi(\varphi^{k-1}(g)) = k\pi(g)$$

for each positive integer k and $g \in G$. Let g be an element of G such that $\pi(g) = t$, i.e., $g \notin \ker\pi$. Suppose that g and g^2 are in the same coset of $\ker\pi$. Then $g^2 = gh$ for some $h \in \ker\pi$, hence $g = h$, a contradiction. It follows that $g^2 \in \ker\pi$, and thus, $\pi(g^2) = 1$. Now by Lemma 1 (iv) we obtain

$$1 \equiv \pi(gg) \equiv \pi(\pi(g), g) \equiv \pi(g)\pi(g) \equiv t^2 \pmod{|\varphi|}.$$

Summing up we have proved that known basic properties of t-balanced skew-morphisms associated with regular Cayley maps holds also in the case of our more general definition of a t-balanced skew-morphism.

Lemma 5 *Let φ be a t-balanced skew-morphism of a group G, i.e., π admits exactly two distinct values* 1 *and t and* $\ker\pi$ *is preserved by φ. Then the following hold:*

(i) $[G : \ker\pi] = 2$*; in particular, G is of an even order;*

(ii) $\pi(g) = \pi(h)$ *for each g, $h \in G$ that belong to the same orbit of φ;*

(iii) $t^2 \equiv 1 \pmod{|\varphi|}$.

We conclude this subsection with the following lemma which states an interesting sufficient condition for a skew-morphism to be t-balanced.

Lemma 6 *Let φ be a skew-morphism of a group G with the power function π such that φ preserves* $\ker\pi$*. Let $X \subseteq G$ be a set closed under taking inverses that generates G with the property $\pi(x) = t$ for each $x \in X$. Then the following hold:*

(i) *If* $t = 1$, *then* φ *is an automorphism of* G*;*

(ii) *If* $t \neq 1$, *then* φ *is a* t*-balanced skew-morphism of* G*.*

Proof. Let k be a positive integer and let S_k denote the set of all elements of G that can be written as a product of exactly k elements of X, i.e., $g \in S_k$ if and only if $g = x_1 x_2 \dots x_k$ for some $x_1, \dots, x_k \in G$. Since X generates G, there exists a positive integer N such that

$$G = \bigcup_{i=1}^{N} S_i.$$

Suppose that $t \neq 1$. We claim that the value of the power function π is t for all elements in S_{2k-1} and 1 for all elements in S_{2k} for any positive integer k. It clearly holds for the set S_1 as it equals X. For any $g \in S_2$ we have $g = x_1 x_2 = x_1(x_2^{-1})^{-1}$ for some $x_1, x_2 \in X$. Note that $x_2^{-1} \in X$ as X is symmetric, thus $\pi(x_1) = \pi(x_2^{-1})$, or equivalently, x_1 and x_2^{-1} belong to the same right coset of $\ker \pi$. It follows that $g = x_1(x_2^{-1})^{-1} \in \ker \pi$, hence $\pi(g) = 1$ for each $g \in S_2$. We proceed by induction on the index i of S_i. Let our claim hold for each $0 < i < n$. We consider two cases:

If $n = 2k - 1$ for some positive integer k, then $h \in \ker \pi$ for each $h \in S_{n-1} = S_{2(k-1)}$. For each $g \in S_n$ we have $g = x_1 \dots x_n$ for some $x_1, \dots, x_n \in S_1$, thus each element $g \in S_n$ can be written in the form $g = hx$ for some $x \in S_1$ and $h \in S_{n-1} \subseteq \ker \pi$ (e.g., we can take $h = x_1 \dots x_{n-1}$ and $x = x_n$). Elements g and x belong to the same right coset of $\ker \pi$, as $gx^{-1} = hxx^{-1} = h \in \ker \pi$. Thus $\pi(g) = t$ for each $g \in S_{2k-1}$.

If $n = 2k$ for some positive integer k, then for each $g \in S_n$ there exists $h \in S_{n-1}$ and $x \in S_1$ such that $g = hx = h(x^{-1})^{-1}$. As $x^{-1} \in S_1$ and $h \in S_{2k-1}$, we have $\pi(h) = \pi(x^{-1}) = t$, and hence $g = h(x^{-1})^{-1} \in \ker \pi$. Thus $\pi(g) = 1$ for each $g \in S_{2k}$.

We proved that the elements of the sets S_k admit only two values of the power function, namely 1 and t. Thus all elements of G admit only two values of the power function. Moreover, φ is not an automorphism, as elements of $X \neq \emptyset$ (generating set is always non-empty) are not in $\ker \pi$. Thus, we have proved (ii).

The same proof works for (i), as we did not use the fact $t \neq 1$ in the proof that the power function admits only values t and 1. Hence, in the case $t = 1$, the value of the power function of φ equals 1 for all elements in G and φ is a group automorphism. $\square$

Note that in the case of skew-morphisms of abelian groups, we can leave out the assumption that φ preserves $\ker \pi$, as it is always true by Lemma 3 (i). However, in general case we can not leave out this assumption, since there exists skew-morphisms of non-abelian groups which admits exactly two power function values but does not preserve the kernel of their power function, and thus, they are not t-balanced (see [2] for example).

2.6.2 Coset-preserving skew-morphisms

We proceed to introduce a class of skew-morphisms that, like the t-balanced skew-morphisms, preserve all cosets of $\ker \pi$, but do not restrict the number of distinct values of the power function π. The following definition coincides with the definition of skew-morphisms with the constant orbit power function in [1], the only difference being in the name.

Definition 7 *Let φ be a skew-morphism of a group G with the power function π. We will say that φ is coset-preserving if it preserve all cosets of* $\ker \pi$*, that is, $\pi(g) = \pi(h)$ for any two elements $g, h \in G$ that belong to the same orbit of φ.*

Note that the concept of coset-preserving skew-morphisms includes both the group automorphisms and the t-balanced skew-morphisms. On the other hand, not every skew-morphism is coset-preserving, as we have seen in the example in Section 2.5. In Table 2.1 we present the number of all skew-morphisms, the number of coset-preserving skew-morphisms, the number of t-balanced skew-morhpisms and the number of automorphisms for cyclic groups Z_n up to the order 30 (taking advantage of the list [7]). The omitted groups have the property that all of their skew-morphisms are group automorphisms.

In view of the periodicity of a skew-morphism (introduced in Section 2.5), coset-preserving skew-morphisms constitute the most trivial class of skew-morphisms with the periodicity 1.

The order n	$\lvert$Skew $\mathrm{Z}_n\rvert$	$\lvert$CP Skew $\mathrm{Z}_n\rvert$	$\lvert$t-bal $\mathrm{Z}_n\rvert$	$\lvert$Auto $\mathrm{Z}_n\rvert$
6	4	4	2	2
8	6	6	2	4
9	10	6	0	6
10	8	8	4	4
12	8	8	4	4
14	12	12	6	6
16	20	20	12	8
18	30	14	8	6
20	24	24	8	8
21	24	24	0	12
22	20	20	10	10
24	24	24	16	8
25	68	20	0	20
26	24	24	12	12
27	85	30	0	18
28	24	24	12	12
30	32	32	24	8

Tab. 2.1: The distribution of skew-morphisms for small cyclic groups

In the last lemma of this section we present another useful property of the power function for the class of coset-preserving skew-morphisms.

Lemma 7 *Let φ be a non-trivial coset-preserving skew-morphism of an abelian group A with the power function π. Then π is a homomorphism from A into the multiplicative group $\mathrm{Z}^*_{|\varphi|}$.*

Proof. This result follows straightforward from Lemma 1 (iv) as

$$\pi(ab) \equiv \pi(\pi(a), b) \equiv \pi(a)\pi(b) \pmod{|\varphi|}$$

for each a, $b \in A$. □

2.7 Powers of skew-morphisms

Every automorphism ϕ of a group G satisfies the property that for any positive integer k, the permutation ϕ^k is an automorphism of G as well. The following example shows that, in general, this property does not hold for skew-morphisms.

EXAMPLE A permutation $\varphi = (1, 2, 7, 5, 4, 8)\,(3, 6)$ of a group Z_9 is a skew-morphism of Z_9 (see [7]) with the distribution of the values of the power function on the orbits of φ

$$[3,\ 5,\ 3,\ 5,\ 3,\ 5]\ [1,\ 1].$$

We will investigate whether the permutation $\varphi^3 = (1, 5)\,(2, 4)\,(7, 8)\,(3, 6)$ is a skew-morphism of Z_9 as well. Let us suppose that $\varphi^3 = \tau$ is a skew-morphism of Z_9 with the power function $\overline{\pi}$. It follows that

$$\tau(gh) = \tau(g)\tau^{\overline{\pi}(g)}(h) = \varphi^3(g)\varphi^{3\overline{\pi}(g)}(h)$$

for each g, $h \in \mathrm{Z}_9$. On the other hand we have

$$\tau(gh) = \varphi^3(gh) = \varphi^3(g)\varphi^{\pi(3,g)}(h)$$

for each g, $h \in \mathrm{Z}_9$ by Equation 2.2. Hence for any $g \in \mathrm{Z}_9$ we have $\varphi^{3\overline{\pi}(g)}(h) = \varphi^{\pi(3,g)}(h)$ for each $h \in \mathrm{Z}_9$, thus

$$3\overline{\pi}(g) \equiv \pi(3, g) \pmod{|\varphi|}.$$

For $g = 1$ we obtain the congruence

$$3\overline{\pi}(1) \equiv 11 \pmod{6},$$

which does not have a solution, and thus, $\overline{\pi}$ does not exist. Concluding, we have shown that φ^3 is not a skew-morphism of Z_9.

We proceed to define the power of a skew-morphism. Let φ be a skew-morphism and let k be a positive integer. We call the permutation φ^k the k-th power of the skew-morphism φ. In this section and Sections 3.1 and 3.2 we study powers of skew-morphisms which are skew-morphisms as well.

Generalizing observations from the above example we obtain the following lemma that characterize positive integers k such that φ^k is also a skew-morphism.

Lemma 8 ([1]) *Let φ be a skew-morphism of a group G with the power function π and let k be a positive integer. Then φ^k is a skew-morphism of G if and only if the congruence*

$$k \cdot x_g \equiv \pi(k, g) \pmod{|\varphi|}$$

has a solution x_g for each $g \in G$.
Moreover, if φ^k is a skew-morphism of G with the power function $\overline{\pi}$, then for each $g \in G$ the solution x_g is unique modulo $|\varphi^k|$ and the value of $\overline{\pi}$ at g can be computed by

$$\overline{\pi}(g) = x_g \pmod{|\varphi^k|}.$$

Note that solutions x_g are not necessarily unique modulo $|\varphi|$, but they are unique modulo $|\varphi^k|$.

A straightforward consequence of the above lemma is the fact that any power of a t-balanced skew-morphism φ of G is a skew-morphism of G, as $\pi(k, g) = k \cdot \pi(g)$ for each positive integer k and any $g \in G$, and thus, the congruence

$$k \cdot x_g \equiv \pi(k, g) \equiv k \cdot \pi(g) \pmod{|\varphi|}$$

has a solution for each $g \in G$. The values of the power function $\overline{\pi}$ of the resulting skew-morphism φ^k will be $\overline{\pi}(g) = 1$, if $\pi(g) = 1$ or $\overline{\pi}(g) = \left(t \pmod{|\varphi^k|}\right)$, if $\pi(g) = t$. Thus, the resulting power φ^k is either a group automorphism or a t-balanced skew-morphism, depending on whether $t \equiv 1 \pmod{|\varphi^k|}$ or not.

Using similar methods it is easy to verify that any power of a coset-preserving skew-morphism of a group G is a coset-preserving skew-morphism of G as well. Summing up we obtain the following lemma.

Lemma 9 ([1]) *Let* $\mathrm{Sym}\, G$ *be a group of all permutations of a group* G *and let* A, B *and* C *denote the subsets of* $\mathrm{Sym}\, G$ *consisting of all automorphisms,* t*-balanced skew-morphisms and coset-preserving skew-morphisms, respectively. Then the following hold:*

(i) *The set* $A \subseteq \mathrm{Sym}\, G$ *is closed under taking powers, i.e., if* $\tau \in A$*, then* $\tau^k \in A$ *for any positive integer* k*;*

(ii) *The set* $A \cup B \subseteq \mathrm{Sym}\, G$ *is closed under taking powers;*

(iii) *The set* $C \subseteq \mathrm{Sym}\, G$ *is closed under taking powers.*

The following lemma, which is an easy consequence of Lemma 8, states that in the study of powers of skew-morphisms that are skew-morphisms as well, it is sufficient, in a sense, to study only those exponents of powers that divide the order of a skew-morphism.

Lemma 10 ([1]) *Let* φ *be a skew-morphism of a group* G*, and let* k *be a positive integer. Then* φ^k *is a skew-morphism if and only if* $\varphi^{(|\varphi|,k)}$ *is a skew-morphism, where* $(|\varphi|, k)$ *denotes the greatest common divisor of numbers* $|\varphi|$ *and* k*.*
In particular, if $|\varphi|$ *and* k *are relatively prime, then* φ^k *is a skew-morphism and* $|\varphi^k| = |\varphi|$*.*

Chapter 3

Skew-morphisms of abelian groups

In this chapter, we investigate the nature of skew-morphisms for abelian and, in particular, cyclic groups using results presented in Sections 2.5 and 2.7. A main theorem regarding powers of skew-morphisms of abelian groups is presented and proved in Section 3.1 (the weaker form of the theorem was introduced in [1]). Section 3.2 is devoted to the most important consequences of the theorem from the first section. A complete classification of coset-preserving skew-morphisms for cyclic groups is introduced in Section 3.3.

3.1 Main theorem regarding powers for abelian groups

The following theorem states an important property of the periodicity of skew-morphisms of abelian groups.

Theorem 6 *Let φ be a skew-morphism of an abelian group A with the power function π and the peridocity $p = p_\varphi$. Then a permutation φ^p is a coset-preserving skew-morphism of A.*
Furthermore, if a and b belong to the same orbit of φ and $\overline{\pi}$ is the power function of φ^p, then $\overline{\pi}(a) = \overline{\pi}(b)$.

Proof. Let us first prove that φ^p is a skew-morphism of A. For an arbitrary element $a \in A$ we have $p_a k_a = p$ for some positive integer k_a, as p is the least common multiple of periodicities of all orbits of φ and the periodicity of a equals the periodicity of its orbit. By Lemma 4 (vi), (vii) we have $p_a \mid \pi(p_a, a)$ and $\pi(p, a) = \pi(p_a k_a, a) = k_a \pi(p_a, a)$. It follows that $p \mid \pi(p, a)$ for each $a \in A$. Hence the congruence

$$p \cdot x_a \equiv \pi(p, a) \pmod{|\varphi|}$$

has a solution x_a for each $a \in A$, thus φ^p is a skew-morphism of A by Lemma 8.

We proceed to show that a skew-morphism φ^p with the power function $\overline{\pi}$ is coset-preserving. Let a, $b \in A$ be two arbitrary elements that belong to the same orbit of φ^p. Clearly, a and b also belong to the same orbit of φ, and thus, $p_a = p_b$ and $\pi(p_a, a) = \pi(p_a, b)$ by Lemma 4 (vii). Hence $p = p_a k = p_b k$ for some positive integer k and $\pi(p_a, a) = \pi(p_a, b) = \pi(p_b, b)$. Considering the following calculation

$$\pi(p, a) = \pi(p_a k, a) = k\pi(p_a, a) = k\pi(p_b, b) = \pi(p_b k, a) = \pi(p, b),$$

we obtain $\pi(p, a) = \pi(p, b)$ for each a, $b \in A$ that belong to the same orbit of φ^p.

It follows easily that numbers x_a and x_b are solutions of the same equation

$$p \cdot x \equiv \pi(p, a) \pmod{|\varphi|},$$

thus

$$\overline{\pi}(a) = (x_a \pmod{|\varphi^p|}) = (x_b \pmod{|\varphi^p|}) = \overline{\pi}(b)$$

for each pair a, $b \in A$ that belong to the same orbit of φ^p, that is, φ^p is a coset-preserving skew-morphism of A.

Note that we have actually proved that $\pi(a) = \pi(b)$ for any a and b belonging to the same orbit of φ, which proves the second part of the theorem. $\square$

Recall that a skew-morphism is coset-preserving if and only if $p_\varphi = 1$. Thus, for an arbitrary non-trivial coset-preserving skew-morphism φ, its p_φ-th power is a non-trivial coset-preserving skew-morphism as $\varphi^{p_\varphi} = \varphi$. However, general skew-morphisms of abelian groups do not have to have the property that φ^{p_φ} is non-trivial. A skew-morphism φ may contain orbits of relatively prime periodicities, which in turn may cause p_φ become too big, and therefore φ^{p_φ} may turn out to be trivial.

Our next goal is to find additional assumptions under which we can prove that φ^{p_φ} is a non-trivial coset-preserving skew-morphism. The answer presented in the following section states that it is sufficient for a skew-morphism to have a generating orbit.

3.2 Corollaries of the main theorem

In this section we present some important consequences of Theorem 6. As mentioned before, our first goal is to prove that the p_φ-th power of a skew-morphism φ with a generating orbit is always non-trivial.

Assume that a non-trivial skew-morphism φ of an abelian group A has a generating orbit $|\mathcal{O}|$. It has been shown in [14] that the order of a skew-morphism φ with a generating orbit $\mathcal{O}$ is necessarily equal to the size of $\mathcal{O}$, i.e., $|\varphi| = |\mathcal{O}|$. As the periodicities of all elements in $\mathcal{O}$ are the same, namely $p_\mathcal{O}$, and every element $a \in A$ can be written as a product of the finite number of elements in $\mathcal{O}$, we obtain $p_a \,|\, p_\mathcal{O}$ for each $a \in A$ by Lemma 4 (viii). It follows that $p_\varphi = p_\mathcal{O}$.

In the previous section we already mentioned that in the case of coset-preserving skew-morphisms is the power φ^{p_φ} non-trivial. Hence, suppose that $p_\varphi = p_\mathcal{O} > 1$. Note that elements in $\mathcal{O}$ admit at most $|\varphi| - 1 = |\mathcal{O}| - 1$ distinct values, namely $1, 2, \ldots, |\varphi| - 1$ by Lemma 1 (ii). It follows that at least two elements in $\mathcal{O}$ are assigned the same power function value, and hence the periodicity of $\mathcal{O}$ does not equal the size of $\mathcal{O}$. Concluding, the coset-preserving skew-morphism φ^{p_φ} is non-trivial as $p_\varphi = p_\mathcal{O} < |\mathcal{O}| = |\varphi|$.

Combining this observation with Theorem 6 we obtain the following theorem.

Theorem 7 *Let φ be a non-trivial skew-morphism of an abelian group A with a generating orbit $\mathcal{O}$. Then $p_\varphi = p_\mathcal{O}$ and φ^{p_φ} is a non-trivial coset-preserving skew-morphism of A.*

The following result is a straightforward consequence of the above theorem and the observation that any skew-morphism of a cyclic group $\mathrm{Z}_n = (\mathrm{Z}_n, +)$ has at least one generating orbit, e.g., the orbit containing a generator of Z_n.

Theorem 8 *Let φ be a non-trivial skew-morphism of a cyclic group Z_n. Then $p_\varphi = p_g$ for any generator g of Z_n and φ^{p_φ} is a non-trivial coset-preserving skew-morphism of Z_n.*

We conclude this section with the most important consequence of Theorem 6, which states that all non-trivial skew-morphisms of abelian groups that give rise to regular Cayley maps have a non-trivial power that is either a t-balanced skew-morphism or an automorphism.

Theorem 9 *Let φ be a non-trivial skew-morphism of an abelian group A that give rises to a Cayley map, i.e., a skew-morphism with a generating orbit closed under inverses. Then φ^{p_φ} is either a non-trivial automorphism of A or a non-trivial t-balanced skew-morphism of A.*
In the case when A is of odd order, φ^{p_φ} is necessarily a group automorphism of A.

Proof. Let $\mathcal{O}$ be a generating orbit closed under inverses and let X denote the set of elements of $\mathcal{O}$. Then φ^{p_φ} is a non-trivial coset-preserving skew-morphism of A by Theorem 7. Let us denote the power function of φ^{p_φ} by $\overline{\pi}$. Then by the second part of Theorem 6 we have $\overline{\pi}(a) = \overline{\pi}(b)$ for each a, $b \in \mathcal{O}$. Thus the value of $\overline{\pi}$ is the same at all elements of X. Moreover, the set X is generating and closed under inverses. Since each skew-morphism of an abelian group preserves the kernel of its power function, it follows that φ^{p_φ} is either an automorphism of A or a t-balanced skew-morphism of A by Lemma 6, which proves the first part of the theorem.

The second part follows from the fact that groups of odd order do not admit t-balanced skew-morphisms by Lemma 5 (i). $\square$

3.3 Coset-preserving skew-morphisms for cyclic groups

As we have shown in the previous section, all skew-morphisms of cyclic groups have powers that are non-trivial coset-preserving skew-morphisms. Thus a classification of all coset-preserving skew-morphism of cyclic groups presented in this section is a significant step toward the classification of all skew-morphisms of cyclic groups (a very indirect classification of skew-morphisms of cyclic groups that give rise to regular Cayley maps can be found in [10]). This classification also generalizes a classification of the t-balanced regular Cayley maps of cyclic groups introduced in [17], as coset-preserving skew-morphisms constitute a much wider class than the t-balanced skew-morphisms that give rise to regular Cayley maps.

The key to the classification of coset-preserving skew-morphisms of cyclic groups lies in finding necessary and sufficient sets of parameters that uniquely determine such skew-morphisms. In Subsection 3.3.1 we introduce determining parameters for coset-preserving skew-morphisms of cyclic groups. In Subsection 3.3.2 we build a permutation for the given set of parameters and in Subsection 3.3.3 we prove that this permutation is a coset-preserving skew-morphism with the corresponding set of parameters.

3.3.1 Parameters of coset-preserving skew-morphisms

Let φ be a non-trivial coset-preserving skew-morphism of a cyclic group G. Throughout this section, we will use the following notation. The equation $a = b$ means that a and b are equal as integers. We will understand the congruence $a \equiv b$ without a specified modulus as congruence modulo $|G|$. In all other cases we specify the modulus. We will denote the size of $\ker \pi$ by d. We proceed to define five parameters of φ.

The first parameter n of φ is the order of G, i.e., φ is a skew-morphism of $G \cong \mathrm{Z}_n$. Note that n is a positive integer.

The second parameter k of φ is the smallest non-zero element of $\ker \pi$. It was shown in [9] that the kernel of skew-morphisms of finite groups is always non-trivial, hence, k

is well defined. As all subgroups of Z_n are generated by their smallest elements, we have $\ker\pi = \langle k\rangle$, and thus, $k \mid n$.

The third parameter h of φ is the difference of elements $\varphi(1)$ and 1 modulo $|G| = n$, i.e., we have $h \equiv \varphi(1) - 1$, or equivalently, $\varphi(1) \equiv 1 + h$. As φ is non-trivial and the orbit of 1 is generating, we have $|\mathcal{O}_1| = |\varphi| > 1$, thus $h \neq 0$. Moreover, $h \in \ker\pi$ as φ is coset-preserving, and thus, $h \in \{k, 2k, \ldots, (d-1)k\}$ (recall that $d = |\ker\pi|$).

The fourth parameter s of φ is the smallest positive integer satisfying $\varphi(k) \equiv s \cdot k$. Note that this congruence always has a solution, since $\varphi(k) \in \ker\pi = \{0, k, 2k, \ldots, (d-1)k\}$. Recall that the restriction of φ to $\ker\pi$ is a group automorphism. As $|\ker\pi| = d$, we have $(d, s) = 1$ and $\varphi(b) \equiv s \cdot b$ for each $b \in \ker\pi$.

The fifth parameter e of φ is the value of the power function at 1. Note that

$$\pi(a) \equiv \pi(1)^a \equiv e^a \pmod{|\varphi|}$$

for each $a \in \mathrm{Z}_n$ by Lemma 7. As k is the smallest element of $\ker\pi$, the values $e^1, e^2, \ldots, e^k$ are distinct modulo $|\varphi|$ and $e^k \equiv 1 \pmod{|\varphi|}$. Thus the order of e in the multiplicative group $\mathrm{Z}^*_{|\varphi|}$ equals k.

We proceed to show that φ is completely determined by its five parameters $(n;\, k,\, h,\, s,\, e)$. By Equation 2.2 we have

$$\begin{aligned}\varphi(a) &\equiv \varphi(1 + (a-1)) \equiv \varphi(1) + \varphi^e(a-1) \equiv \\ &\equiv \varphi(1) + \varphi^e(1 + (a-2)) \equiv \varphi(1) + \varphi^e(1) + \varphi^{\pi(e,1)}(a-2) \equiv \varphi(1) + \varphi^e(1) + \varphi^{e^2}(a-2).\end{aligned}$$

for each $a \in \mathrm{Z}_n$. By an induction argument on a, we obtain

$$\varphi(a) \equiv \varphi(1) + \varphi^e(1) + \varphi^{e^2}(1) + \cdots + \varphi^{e^{a-1}}(1), \text{ for each } a \in \mathrm{Z}_n \tag{3.1}$$

as

$$\pi(e^i, 1) \equiv \pi(1) + \pi(\varphi(1)) + \cdots + \pi(\varphi^{e^i - 1}(1)) \equiv e^i \cdot e \equiv e^{i+1} \pmod{|\varphi|}\,.$$

Thus $\varphi(a)$ is uniquely determined for any $a \in \mathrm{Z}_n$ by the orbit $\mathcal{O}_1$ of 1 and the parameter e. We proceed to show that $\mathcal{O}_1$ is uniquely determined by the parameters h and s.

We claim that the following equation holds

$$\varphi^i(1) \equiv 1 + s^0h + s^1h + \cdots + s^{i-1}h, \text{ for each positive integer } i. \tag{3.2}$$

It clearly holds for $i = 1$ by the definition of h. We proceed by induction: Let Equation 3.2 hold for all $i < N$. Then

$$\begin{aligned}\varphi^N(1) &\equiv \varphi(\varphi^{N-1}(1)) \equiv \varphi(1 + s^0h + s^1h + \cdots + s^{N-2}h) \equiv \\ &\equiv \varphi((s^0h + s^1h + \cdots + s^{N-2}h) + 1) \equiv \varphi(s^0h + s^1h + \cdots + s^{N-2}h) + \varphi(1) \equiv \\ &\equiv s^1h + s^2h + \cdots + s^{N-1}h + 1 + h\end{aligned}$$

proves our claim, where the key equations $\pi(s^0h + s^1h + \cdots + s^{N-2}h) = 1$ and $\varphi(s^0h + s^1h + \cdots + s^{N-2}h) \equiv s \cdot (s^0h + s^1h + \cdots + s^{N-2}h)$ holds as $(s^0h + s^1h + \cdots + s^{N-2}h)$ belongs to $\ker \pi$. As $|\varphi| = |\mathcal{O}_1|$, the order of φ is the smallest positive integer r such that $1 \equiv 1 + s^0h + s^1h + \cdots + s^{r-1}h$.

We will call a five-tuple of parameters $(n;\, k,\, h,\, s,\, e)$ of a coset-preserving skew-morphism φ the *parameter set of* φ denoted by $\operatorname{Par}\varphi$. It follows directly from the definition of the parameter set that two non-trivial coset-preserving skew-morphisms of cyclic groups with different parameter sets are not equal, as two coset-preserving skew-morphisms φ and $\overline{\varphi}$ of cyclic groups with different parameter sets are either associated with different groups, or have different kernels $\ker \pi$ and $\ker \overline{\pi}$, or have different values $\varphi(1)$ and $\overline{\varphi}(1)$, or have different values at elements of $\ker \pi$ and $\ker \overline{\pi}$, or have different values of their power functions at 1, respectively (depending on which of the five parameters $(n;\, k,\, h,\, s,\, e)$ they differ). On the other hand, two non-trivial coset-preserving skew-morphisms ψ and $\overline{\psi}$ of cyclic groups with the same parameter sets are equal, as they are uniquely determined by their parameters (see Equations 3.1 and 3.2).

Summing up these observations, we obtain the following theorem.

Theorem 10 *Let φ and ψ be non-trivial coset-preserving skew-morphisms of cyclic groups with the parameter sets $\operatorname{Par}\varphi$ and $\operatorname{Par}\psi$. Then $\varphi = \psi$ if and only if $\operatorname{Par}\varphi = \operatorname{Par}\psi$.*

In the following lemma we present all the properties of parameter sets of coset-preserving skew-morphisms of cyclic groups that we will need in the future subsections.

Theorem 11 *Let φ be a non-trivial coset-preserving skew-morphism of a cyclic group with the parameter set* $\operatorname{Par}\varphi = (n;\, k,\, h,\, s,\, e)$. *Then the following hold:*

(1) *All five parameters are positive integers;*

(2) *The parameter k divides n and $k < n$;*

(3) *Let $d = \frac{n}{k}$. Then $s < d$ and $(s, d) = 1$;*

(4) *The parameter h belongs to the set $\{k,\, 2k,\, \ldots,\, (d-1)k\}$;*

(5) *Let r denote the smallest positive integer such that $1 \equiv 1 + s^0h + s^1h + \cdots + s^{r-1}h$. Then $e < r$ and the order of e in $\mathbb{Z}_r^*$ equals k, in particular, $e^k \equiv 1 \pmod{r}$;*

(6) $s \cdot k \equiv \sum_{i=0}^{k-1}(1 + s^0h + \cdots + s^{e^i-1})$;

(7) $s^{e-1} \equiv 1 \pmod{d}$.

Proof. The properties (1), (2), (3), (4) and (5) follows directly from the definitions of the parameters and the above discussion. The congruence in (6) holds, since $\varphi(k) \equiv sk$ by the definitions of s and k, while on the other hand,

$$\varphi(k) \equiv \sum_{i=0}^{k-1}(1 + s^0h + \cdots + s^{e^i-1})$$

by Equations 3.1 and 3.2.

To prove (7) consider the following calculation:

$$\varphi(k) + \varphi(1) \equiv \varphi(k+1) \equiv \varphi(1+k) \equiv \varphi(1) + \varphi^e(k).$$

Thus $\varphi(k) \equiv \varphi^e(k)$, and hence $sk \equiv s^ek$. Since $n = kd$, it follows $s \equiv s^e \pmod{d}$, or equivalently, $1 \equiv s^{e-1} \pmod{d}$ as $(s, d) = 1$ by (3). $\square$

3.3.2 Building a map τ for a given parameter set

Our next goal is to show that given a five-tuple of parameters satisfying conditions of Theorem 11, we can construct a coset-preserving skew-morphism of a cyclic group with these parameters. In this subsection we employ Equations 3.1 and 3.2 to define a permutation of a cyclic group.

We will say that parameters $(n;\, k,\, h,\, s,\, e)$ are *admissible*, if they satisfy all conditions of Theorem 11. We will refer to them as Conditions (1) to (7).

Let $d = \frac{n}{k}$ and let r be the smallest positive integer such that

$$1 \equiv 1 + s^0 h + s^1 h + \cdots + s^{r-1} h.$$

Note that so far we have no assurance that such an r exists.

We proceed to define a permutation τ of a group Z_n. Instead of $a \equiv b \pmod{n}$ we will write simply $a \equiv b$ as $|\mathrm{Z}_n| = n$. We will define $\tau : \mathrm{Z}_n \to \mathrm{Z}_n$ in two steps: First let $\tau(0) \equiv 0$ and let

$$\tau^i(1) \equiv 1 + s^0 h + s^1 h + \cdots + s^{i-1} h, \text{ for each positive integer } i. \tag{3.3}$$

The above formula (and also the number r) is well-defined by the following lemma.

Lemma 11 *Let $(n;\, k,\, h,\, s,\, e)$ be a set of admissible parameters. Then the following hold:*

(i) *The sum $1 + s^0 h + s^1 h + \cdots + s^{i-1} h$ is non-zero modulo n for each positive integer i;*

(ii) *The number r is well defined, i.e., there exists a positive integer i such that $1 \equiv 1 + s^0 h + s^1 h + \cdots + s^{i-1} h$;*

(iii) *Values $1 + s^0 h + s^1 h + \cdots + s^{i-1} h$ and $1 + s^0 h + s^1 h + \cdots + s^{j-1} h$ are equal modulo n if and only if $i \equiv j \pmod{r}$.*

Proof. Note that $1 + s^0 h + s^1 h + \cdots + s^{i-1} h \equiv 1 \pmod{k}$ as $k \,|\, h$ by Condition (4). The property (i) follows as $k \,|\, n$.

Recall that $n = dk$ and that $(d, s) = 1$. Now suppose that $1 \not\equiv 1 + s^0h + s^1h + \cdots + s^{i-1}h$ for each positive integer i. Since the number of integers modulo n is finite, there must exists two positive integers $i < j$ such that

$$1 + s^0h + s^1h + \cdots + s^{i-1}h \equiv 1 + s^0h + s^1h + \cdots + s^{j-1}h.$$

By subtracting the left side of the congruence from both sides we obtain

$$0 \equiv s^ih + \cdots s^{j-1}h \equiv s^i(s^0h + s^1h + \cdots + s^{j-i-1}h).$$

As $k \mid h$, we have $k \mid s^0h + s^1h + \cdots + s^{j-i-1}h$. It follows that $s^0h + s^1h + \cdots + s^{j-i-1}h = l_1k$ for some positive integer l_1. Thus $l_2n = s^il_1k$ for some positive integers l_1 and l_2 by the above congruence. Dividing both sides by k we obtain $l_2d = s^il_1$. Since $(d, s) = (d, s^i) = 1$, we have $d \mid l_1$, and thus, $n = dk$ divides $l_1k = s^0h + s^1h + \cdots + s^{j-i-1}h$ and congruence from the property (ii) has a positive solution $j - i$. Hence there exists the smallest solution r.

Now observe that all values $1 + s^0h$, $1 + s^0h + s^1h$, $\ldots$, $1 + s^0h + s^1h + \cdots + s^{r-1}h \equiv 1$ are distinct modulo n, as the congruence $1 + s^0h + s^1h + \cdots + s^{i-1}h \equiv 1 + s^0h + s^1h + \cdots + s^{j-1}h$ for some $0 < i < j < r$ would be contrary to the minimality of r, as $1 + s^0h + s^1h + \cdots + s^{j-i-1}h \equiv 1$ by the proof of the property (ii) and $j - i < r$. Now, to prove (iii), it is sufficient to show that $1 + s^0h + s^1h + \cdots + s^{i-1}h \equiv 1 + s^0h + s^1h + \cdots + s^{j-1}h$ for each i and j such that $j = r + i$. This clearly holds, as

$$1 + s^0h + s^1h + \cdots + s^{j-1}h - \big(1 + s^0h + s^1h + \cdots + s^{i-1}h\big) \equiv s^i(1 + s^0h + s^1h + \cdots + s^{r-1}h) \equiv 0.$$

$\square$

Let $Y = \{0, 1, \tau(1), \ldots, \tau^{r-1}(1)\}$. We proceed to define τ for all elements of $\mathrm{Z}_n \setminus Y$:

$$\tau(a) \equiv \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1), \text{ for each } a \in \mathrm{Z}_n \setminus Y. \tag{3.4}$$

Thus we have a well-defined map $\tau : \mathrm{Z}_n \to \mathrm{Z}_n$. In the following lemma we present several important properties of τ.

Lemma 12 *Let $(n;\, k,\, h,\, s,\, e)$ be a set of admissible parameters, and let τ, r and d be defined as above. Then the following hold:*

(i) $\tau^r(1) \equiv 1$;

(ii) $\tau^i(1) \equiv \tau^j(1)$ *if and only if* $i \equiv j \pmod r$;

(iii) $\tau(a) \equiv a \pmod k$ *for each* $a \in \mathrm{Z}_n$;

(iv) $\tau^{e^{lk}}(1) \equiv \tau(1)$ *for each positive integer* l;

(v) $\tau(lk) \equiv s \cdot lk$ *for any positive integer* l;

(vi) $\tau(lk) \equiv \tau^{e^i}(lk)$ *for any positive integers* l *and* i;

(vii) $\tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1) \equiv \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{b-1}}(1)$ *for each pair of positive integers congruent modulo* n;

(viii) $\tau(\tau^i(1)) \equiv \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{\tau^i(1)-1}}(1)$ *for each positive integer* i;

(ix) $\tau(a + lk) \equiv \tau(a) + s \cdot lk$ *for any non-negative integer* a *and any positive integer* l.

Proof. The properties (i) and (ii) follow immediately from Lemma 11. To prove the property (iii), first note that it holds for all elements of Y as $\tau^i(1) \equiv 1 \pmod k$ for each positive integer i by Formula 3.3. Thus for $a \notin Y$ we have

$$\tau(a) \equiv \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1) \equiv 1 + \cdots + 1 \equiv a \pmod k$$

by Formula 3.4. The property (iv) is a straightforward consequence of Condition (5) and the property (ii), as $e^{lk} \equiv (e^k)^l \equiv 1 \pmod r$, and hence $\tau^{e^{lk}}(1) \equiv \tau(1)$.

We proceed to prove the property (v). First observe that for any positive integer l we have $lk \notin Y \setminus \{0\}$ and the claim clearly holds for $lk \equiv 0$, thus

$$\tau(lk) = \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{lk-1}}(1).$$

By the property (iv) we obtain

$$\tau(lk) = l \cdot (\tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{k-1}}(1)).$$

Since $s \cdot k = \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{k-1}}(1)$ by Condition (6), we have $\tau(lk) = s \cdot lk$.

For any positive integer i is $\tau^{i}(lk) \equiv 0 \pmod{k}$ by the property (iii). Thus, by the property (v), we have $\tau^{i}(lk) \equiv s^{i}lk$ for any positive integer i. Also recall that $s^{e-1} \equiv 1 \pmod{d}$ by Condition (7). It follows that $s^{e^i-1} \equiv 1 \pmod{d}$ for any positive integer i as $e-1 \mid e^i - 1$. Thus $s^{e^i} \equiv s^{e^i-1}s \equiv s \pmod{d}$, or equivalently, for any positive integer we have $s^{e^i} = s + jd$ for some integer j. Summing up we obtain

$$\tau^{e^i}(lk) \equiv s^{e^i}lk \equiv (s+jd)\cdot lk \equiv s \cdot lk + jdlk \equiv s \cdot lk$$

which proves (vi).

To prove (vii) suppose without loss of generality that $a \leq b$ (i.e., $b = a + ln$ for some non-negative integer l) and consider the following calculation:

$$\begin{aligned}
&\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a+ln-1}}(1) \equiv \\
&\equiv \Big(\tau(1) + \tau^{e}(1) + \cdots + \tau^{e^{ln-1}}(1)\Big) + \Big(\tau^{e^{ln}}(1) + \tau^{e^{ln+1}}(1) + \cdots + \tau^{e^{a+ln-1}}(1)\Big) \equiv \\
&\equiv \tau(ln) + \Big(\tau^{e^0}(1) + \tau^{e^1}(1) \cdots + \tau^{e^{a-1}}(1)\Big) \equiv \tau(0) + \tau(a) \equiv \tau(a)
\end{aligned}$$

where the key equality $\tau^{e^{ln}}(1) + \tau^{e^{ln+1}}(1) + \cdots + \tau^{e^{a+ln-1}}(1) \equiv \tau^{e^0}(1) + \tau^{e^1}(1) \cdots + \tau^{e^{a-1}}(1)$ holds by (iv). Note that this property yields that in Formula 3.4 we can represent an element $a \in \mathrm{Z}_n$ by all non-negative integers in the residue class $(a) \pmod{n}$. Thus, in what follows, we do not need to verify if $a < n$ when computing τ of the corresponding element of a in Z_n.

We proceed to prove the property (viii) by induction on i. It clearly holds for $i = 0$ as $\tau(\tau^0(1)) \equiv \tau(1)$. Now suppose that

$$\tau(\tau^{i}(1)) \equiv \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{\tau^{i}(1)-1}}(1)$$

for all $i < j$. Then applying properties (iv) and (v) we obtain

$$\begin{aligned}
&\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{s^{j-1}h+\cdots+s^0h+sh+h}}(1) \equiv \\
&\equiv \tau(\tau^{j-2}(1)) + \Big(\tau^{e^{s^{j-2}h+\cdots+s^0h+sh+h+1}}(1) + \cdots \tau^{e^{s^{j-1}h+\cdots+s^0h+sh+h}}(1)\Big) \equiv
\end{aligned}$$

$$\equiv \tau^{j-1}(1)) + \left(\tau^{e^1}(1) + \cdots \tau^{e^{s^{j-1}h}}(1)\right) \equiv$$
$$\equiv \tau^{j-1}(1) + \tau(s^{j-1}h) = 1 + h + sh + \cdots + s^{j-1}h + s^j h \equiv \tau^j(1),$$

which proves our claim. Thus (viii) holds.

Finally, the property (ix) follows directly by properties (iv) and (v) as

$$\tau(a + lk) \equiv \tau(lk) + \tau^{e^{lk}}(1) + \tau^{e^{lk+1}}(1) + \cdots + \tau^{e^{lk+a-1}}(1) \equiv s \cdot lk + \tau(a).$$

□

Note that Formula 3.4 is relevant for all non-zero elements of Z_n by the property (vi) of the above lemma. The remaining task of this subsection is to show that τ is a bijection. As Z_n is finite, it is sufficient to show that τ is an injection. Note that each element a of Z_n can be written uniquely as $a = \overline{a} + l_a \cdot k$ where $\overline{a} \in \{0, 1, \ldots, k-1\}$ and $l_a \in \{0, 1, \ldots, d-1\}$. Now suppose that $\tau(a) \equiv \tau(b)$ for some $a, b \in Z_n$. Then by Lemma 12 (ix) we have

$$\tau(a) \equiv \tau(b)$$
$$\tau(\overline{a} + l_a k) \equiv \tau(\overline{b} + l_b k)$$
$$\tau(\overline{a}) + s l_a k \equiv \tau(\overline{b}) + s l_b k.$$

It follows $\tau(\overline{a}) \equiv \tau(\overline{b}) \pmod{k}$, and thus, $\overline{a} \equiv \overline{b} \pmod{k}$ by Lemma 12 (iii). Since $\overline{a}, \overline{b} \in \{0, 1, \ldots, k-1\}$, we obtain $\overline{a} = \overline{b}$.

Hence $s \cdot l_a k \equiv s \cdot l_b k$, or equivalently, $sk(l_a - l_b) \equiv 0$. As $n = kd$, $(d, s) = 1$ and $l_a, l_b \in \{0, 1, \ldots, d-1\}$, it follows that $l_a - l_b \equiv 0 \pmod{d}$, and thus, $l_a = l_b$.

Concluding, we have shown $\tau(a) \equiv \tau(b)$ only if $a = \overline{a} + l_a \equiv \overline{b} + l_b = b$, thus τ is permutation of Z_n.

3.3.3 Proof that τ is a coset-preserving skew-morphism

In the previous section we have shown that the map τ defined for an admissible set of parameters (i.e., parameters satisfying the conditions of Theorem 11) by Formulas 3.3

and 3.4 is a well defined identity-preserving permutation of Z_n, which satisfies all the properties of Lemma 12. In this section, we proceed to show that τ defined by parameters $(n;\, k,\, h,\, s,\, e)$ is a coset-preserving skew-morphism of Z_n with the parameter set $\mathrm{Par}\,\tau = (n;\, k,\, h,\, s,\, e)$.

To prove that τ is a skew-morphism, for each $a \in \mathrm{Z}_n$ we must find a positive integer i_a such that

$$\tau(a+b) \equiv \tau(a) + \tau^{i_a}(b),$$

for all $b \in \mathrm{Z}_n$. We will show that the above equation holds for $i_a = e^{(a \pmod{k})}$ and each $b \in \mathrm{Z}_n$. We use the following lemma that states that it is sufficient to verify our claim only for $a \in \{0,\, 1,\, \ldots,\, k-1\}$ and $b \in \{0,\, 1,\, \ldots,\, k-1\}$.

Lemma 13 *Let $a,\, b \in \{0,\, 1,\, \ldots,\, k-1\}$ and let*

$$\tau(a+b) \equiv \tau(a) + \tau^{e^a}(b).$$

Then the following hold for each $\overline{a},\, \overline{b} \in \mathrm{Z}_n$ such that $a \equiv \overline{a} \pmod{k}$ and $b \equiv \overline{b} \pmod{k}$:

$$\tau(\overline{a} + \overline{b}) \equiv \tau(\overline{a}) + \tau^{e^a}(\overline{b}).$$

Proof. As $a \equiv \overline{a} \pmod{k}$ and $b \equiv \overline{b} \pmod{k}$, there exist $l_1, l_2 \in \{0,\, 1,\, \ldots,\, d-1\}$ such that $\overline{a} = a + l_1 k$ and $\overline{b} = a + l_1 k$. Thus to prove our claim we must verify that

$$\tau(a + l_1 k \; + \; b + l_2 k) \equiv \tau(a + l_1 k) + \tau^{e^a}(b + l_2 k). \tag{3.5}$$

Applying Lemma 12 (ix), (v) and (vi) on the left side of Equation 3.5 we obtain

$$\begin{aligned} \tau(a + l_1 k + b + l_2 k) &\equiv \tau(a + b \; + \; l_1 k + l_2 k) \equiv \\ &\equiv \tau(a+b) + s \cdot l_1 k + s \cdot l_2 k \equiv \\ &\equiv \tau(a) + \tau^{e^a}(b) + \tau(l_1 k) + \tau(l_2 k) \equiv \\ &\equiv \tau(a) + \tau(l_1 k) + \tau^{e^a}(b) + \tau^{e^a}(l_2 k). \end{aligned}$$

On the other hand, by repeated application of Lemma 12 (ix) on the right side of Equation 3.5, we obtain

$$\tau(a + l_1 k) + \tau^{e^a}(b + l_2 k) \equiv \tau(a) + \tau(l_1 k) + \tau^{e^a}(b) + s^{e^a} \cdot l_2 k \equiv \tau(a) + \tau(l_1 k) + \tau^{e^a}(b) + \tau^{e^a}(l_2 k)$$

which proves our claim. □

We proceed to verify by induction on b that $\tau(1+b) \equiv \tau(1) + \tau^e(b)$ for each $b \in \{1, \ldots, k-1\}$ and that

$$\tau^i(b) \equiv \tau^i(1) + \tau^{ie}(1) + \cdots + \tau^{ie^{b-1}}(1)$$

for any positive integer i. Observe that both claims clearly hold for $b = 1$ as $\tau(1+1) = \tau(1) + \tau^e(1)$ by Formula 3.4 and $\tau^i(1) = \tau^i(1)$. Now suppose that both claims hold for all $a < b$. Then by Lemma 13 $\tau(c+\bar{b}) \equiv \tau(c)+\tau^e(\bar{b})$ for each $c, \bar{b} \in \mathrm{Z}_n$ such that $c \equiv 1 \pmod{k}$ and $\bar{b} \equiv b \pmod{k}$ for some $b \in \{1, \ldots, a-1\}$. In particular,

$$\tau(\tau^{j_1}(1) + \tau^{j_2}(b)) \equiv \tau(\tau^{j_1}(1)) + \tau^e(\tau^{j_2}(b)) \equiv \tau^{1+j_1}(1) + \tau^{e+j_2}(b)$$

for any positive integers j_1 and j_2 by Lemma 12 (iii). Applying this observation we proceed to compute $\tau^i(a)$ for an arbitrary integer i:

$$\begin{aligned}
\tau^i(a) &\equiv \tau^{i-1}\left(\tau(1+(a-1))\right) \equiv \tau^{i-1}\left(\tau(1) + \tau^e(a-1)\right) \equiv \\
&\equiv \tau^{i-2}\left(\tau(\tau(1) + \tau^e(a-1))\right) \equiv \tau^{i-2}\left(\tau^2(1) + \tau^{2e}(a-1)\right) \equiv \\
&\qquad\vdots \\
&\equiv \tau\left(\tau^{i-1}(1) + \tau^{(i-1)e}(a-1)\right) \equiv \tau^i(1) + \tau^{ie}(a-1) \equiv \\
&\equiv \tau^i(1) + \tau^{ie}(1) + \cdots + \tau^{ie^{a-1}}(1).
\end{aligned}$$

The last congruence holds as $a - 1 < a$, and thus,

$$\tau^{ie}(a-1) \equiv \tau^{ie}(1) + \cdots + \tau^{ie^{a-1}}(1)$$

by the induction assumption.

To prove the remaining claim we apply the above formula to compute $\tau^i(a)$ for $i = e$:

$$\tau(1) + \tau^e(a) \equiv \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^a}(1) \equiv \tau(1+a).$$

We have shown $\tau(1+b) \equiv \tau(1) + \tau^e(b)$ for each $b \in \{1, \ldots, k-1\}$ and

$$\tau^i(b) \equiv \tau^i(1) + \tau^{ie}(1) + \cdots + \tau^{ie^{b-1}}(1) \tag{3.6}$$

for each $b \in \{1, \ldots, k-1\}$ and any positive integer i.

We proceed to show that the equation

$$\tau(a+b) \equiv \tau(a) + \tau^{e^a}(b)$$

holds for each $a, b \in \{0, 1, \ldots, k-1\}$. It clearly holds if $a = 0$ or $b = 0$. Thus, suppose that both a and b are non-zero. Then by Formula 3.6 for $i = e^a$ we have

$$\tau(a) + \tau^{e^a}(b) \equiv \Big(\tau(1) + \cdots + \tau^{e^{a-1}}(1)\Big) + \Big(\tau^{e^a}(1) + \cdots + \tau^{e^{a+b-1}}(1)\Big) \equiv \tau(a+b)$$

which proves our claim. Combining this result with Lemma 13 we have proved that τ is a skew-morphism of Z_n with $i_a = e^{a \pmod k}$ for each $a \in \mathrm{Z}_n$. As τ is a skew-morphism of an abelian group and the orbit of element 1 is generating, we have $|\tau| = |\mathcal{O}_1| = r$. Let π denote the power function of the skew-morphism τ. Then $\pi(a)$ equals $\big(e^{a \pmod k} \pmod r\big)$ for each $a \in \mathrm{Z}_n$ (note that $e^{a \pmod k} \equiv e^a \pmod r$ by Condition (5)). Summing up we obtain the first claim of the following lemma.

Lemma 14 *Let $(n;\, k,\, h,\, s,\, e)$ be the set of admissible parameters, let r be the integer defined in the previous subsection, and let τ be the permutation of Z_n defined by $\tau(0) = 0$ and Formulas 3.3 and 3.4. Then the following hold:*

(i) *The permutation τ is a skew-morphism of Z_n with the power function values $\pi(a) = e^a \pmod r$ for each $a \in \mathrm{Z}_n$;*

(ii) *The skew-morphism τ is coset-preserving;*

(iii) $\mathrm{Par}\,\tau = (n;\, k,\, h,\, s,\, e)$.

Proof. The skew-morphism τ satisfies $\tau(a) \equiv a \pmod k$ for each $a \in \mathrm{Z}_n$ by Lemma 12 (iii). Thus the values e^a and $e^{\tau(a)}$ are equal modulo r as $e^k \equiv 1 \pmod r$ by Condition (5). It follows that τ is a coset-preserving skew-morphism of Z_n. We proceed to prove that the five parameters of τ are equal to n, k, h, s and e respectively.

The first parameter clearly equals n as $|\mathrm{Z}_n| = n$.

The third parameter equals h as $\tau(1) - 1 = 1 + h - 1 = h$.

To verify that the fourth parameter equals s we must prove that s is the smallest positive integer such that $\tau(k) \equiv sk$. The equation holds by Lemma 12 (v). Now suppose that $\tau(k) \equiv \overline{s}k$ for some positive integer $\overline{s} \leq s$. We obtain

$$\begin{aligned} sk &\equiv \overline{s}k \\ s &\equiv \overline{s} \pmod{d}, \end{aligned}$$

and hence $s = \overline{s}$ as $s < d$ by Condition (3). It follows that s is the smallest positive integer satisfying $\tau(k) \equiv sk$, and thus, s is the fourth parameter of τ.

The fifth parameter $\pi(1)$ equals $e \pmod{r}$. As $e < r$ by Condition (5), we obtain $\pi(1) = e$.

Recall that the order of $\pi(1) = e$ modulo $|\tau| = r$ equals k by Condition (5). Hence $\pi(a) = (e^a \pmod{r}) \neq 1$ for all non-zero elements $a \in \mathrm{Z}_n$ smaller than k and $\pi(k) = (e^k \pmod{r}) = 1$. Thus k is the smallest non-zero element of $\ker \pi$, i.e., the second parameter of τ.

Summing up, we have shown $\operatorname{Par} \tau = (n;\, k,\, h,\, s,\, e)$. $\square$

3.3.4 Complete classification and remarks

Summarizing previous subsections, we have obtained the following theorem.

Theorem 12 (1) *Let $(n;\, k,\, h,\, s,\, e)$ be a set of admissible parameters. Then there exists an unique non-trivial coset-preserving skew-morphism τ of the cyclic group Z_n such that* $\operatorname{Par} \tau = (n;\, k,\, h,\, s,\, e)$.

(2) *Let φ be a non-trivial coset-preserving skew-morphism of a cyclic group Z_n. Then* $\operatorname{Par} \varphi$ *is a set of admissible parameters.*

The above theorem yields a complete classification of non-trivial coset-preserving skew-morphisms of cyclic groups by sets of admissible parameters. Note that by restricting to $k = 2$, we obtain a complete classification of the t-balanced skew-morphism of cyclic groups.

Theorem 12 established a one-to-one correspondence between coset-preserving skew-morphisms of cyclic groups and sets of admissible parameters (defined as five-tuples of parameters satisfying Theorem 11). Note that Theorem 11 provides an algorithm for finding all sets of admissible parameters for given n in the polynomial time in n. Moreover, Formulas 3.3 and 3.4 provide an algorithm for constructing skew-morphism for given sets of admissible parameters in polynomial time in n as well. Combining these algorithms, we created a c++ program that allowed us to search for sets of admissible parameters up to the order $n = 2000$, which in turn allowed us to create a complete list of coset-preserving skew-morphisms of cyclic groups of order ≤ 500 (with the list becoming unreasonably big with the increase of the order of the cyclic group, but extendable, if needed). The complete list up to the order 500 contains 177753 coset-preserving skew-morphisms out of which 76115 are automorphisms. The cyclic group with the largest number of coset-preserving skew-morphisms up to the order 500 is the group Z_{480} which admits 2144 coset-preserving skew-morphisms.

3.3.5 Examples

In this subsection we provide two examples that illustrate the introduced complete classification of coset-preserving skew-morphisms of cyclic groups. In the first example we demonstrate the construction of a coset-preserving skew-morphism for the given admissible parameters set. In the second example we present our classification for the cyclic group Z_{18}.

Examples (1) For an arbitrary admissible parameters set $(n;\, k,\, h,\, s,\, e)$, we define the corresponding coset-preserving skew-morphism τ of Z_n by the following:

1. Let $\tau(0) = 0$.

2. According to Formula 3.3, we define $\tau^i(1) = (1 + s^0h + s^1h + \cdots + s^{i-1}h \pmod n)$ for each positive integer i.

   Recall that $\tau^i(1) = \tau^{(i \pmod r)}(1)$ where r is the smallest positive integer satisfying $1 + s^0h + s^1h + \cdots + s^{r-1}h \equiv 0 \pmod n$ by Lemma 11. Moreover, the parameter r equals the length of the orbit $\mathcal{O}_1$ of the corresponding skew-morphism τ of Z_n, thus $r \leq n$. Hence we require at most n computations of the terms $1+s^0h+s^1h+\cdots+s^{j-1}h$ for $1 \leq j \leq r$ to be able to determine $\tau^i(1)$ for each positive integer i.

3. Let $\tau(a) = \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1)$ for all remaining elements of Z_n.

We proceed to present our construction for a set of parameters $(n;\ k,\ h,\ s,\ e) = (20;\ 4,\ 8,\ 1,\ 3)$. It is easy to verify that this parameter set satisfies all the conditions of Theorem 11, and thus, (20; 4, 8, 1, 3) is an admissible parameters set. As the first parameter equals 20, we will build the corresponding coset-preserving skew-morphisms φ of Z_{20}.

1. Let $\varphi(0) = 0$.

2. Let $\varphi^i(1) = (1 + 1^0 \cdot 8 + 1^1 \cdot 8 + \cdots + 1^{i-1} \cdot 8 \pmod{20}) = (1 + 8i \pmod{20})$ for each positive integer i. Since the smallest positive integer r such that $1 + 8r \equiv 0 \pmod{20}$ equals 5, we obtain the following:

$$\varphi^0(1) = 1, \quad \varphi(1) = 9, \quad \varphi^2(1) = 17, \quad \varphi^3(1) = 5, \quad \varphi^4(1) = 13,$$
$$\varphi^i(1) = \varphi^{(i \pmod 5)}(1), \text{ for each } i \geq 5$$

3. It is possible compute $\varphi(a)$ for all remaining elements of Z_{20} by the formula

$$\varphi(a) = \varphi(1) + \varphi^3(1) + \varphi^{3^2}(1) + \cdots + \varphi^{3^{a-1}}(1).$$

   However, it is possible to simplify the computation of φ by the following method: By Lemma 12 (ix) we have $\varphi(a + lk) = \varphi(a) + s \cdot lk$ for any non-negative integer a and positive integer l. Since $k = 4$ and $s = 1$, we obtain $\varphi(a + 4l) = \varphi(a) + 4l$. Thus, to determine φ, it is sufficient to find values $\varphi(0)$, $\varphi(1)$, $\varphi(2)$ and $\varphi(3)$. We already know that $\varphi(0) = 0$ and $\varphi(1) = 1$. We obtain the two remaining values $\varphi(2)$ and $\varphi(3)$ by the following calculation:

$$\varphi(2) = \varphi(1) + \varphi^3(1) = 9 + 5 = 14,$$
$$\varphi(3) = \varphi(1) + \varphi^3(1) + \varphi^9(1) = \varphi(1) + \varphi^3(1) + \varphi^4(1) = 9 + 5 + 13 = 7.$$

By employing the formula $\varphi(a + 4l) = \varphi(a) + 4l$ for $a = 1, 2, 3$ and $l = 1, 2, 3, 4$ we obtain

$$\varphi = (1, 9, 17, 5, 13)(2, 14, 6, 18, 10)(3, 7, 11, 15, 19).$$

The resulting coset-preserving skew-morphism φ of Z_{20} satisfies the equation $\mathrm{Par}\,\varphi = (20;\ 4,\ 8,\ 1,\ 3)$. Note that φ is neither an automorphism nor a t-balanced skew-morphism of Z_{20} as the second parameter $k = 4$ (and thus, the power function π admits 4 distinct values). The group Z_{20} is the smallest cyclic group which admits such coset-preserving skew-morphism (see Table 2.1).

(2) In this example we present the list of all coset-preserving skew-morphisms of Z_{18} provided by our results. For each orbit of a coset-preserving skew-morphism we will write the value of the power function only for one of its elements. For $n = 18$ there exist 13 admissible parameters sets, which in turn give rise to 13 non-trivial coset-preserving skew-morphisms of Z_{18}. Thus, by extending the list by the identity permutation of Z_{18}, we obtain the following list of all coset-preserving skew-morphisms of Z_{18}.

COSET-PRESERVING SKEW-MORPHISMS OF Z_{18}:

$\varphi_1 = \mathrm{Id}(\mathrm{Z}_{18})$, automorphism of Z_{18}

$\varphi_2 = (1, 5, 7, 17, 13, 11)\,(2, 10, 14, 16, 8, 4)\,(3, 15)\,(6, 12)$, automorphism of Z_{18}
$\pi(1) = \pi(2) = \pi(3) = \pi(6) = 1$, $\mathrm{Par}\,\varphi = (18;\ 1,\ 4,\ 5,\ 1)$

$\varphi_3 = (1, 7, 13)\,(2, 14, 8)\,(4, 10, 16)\,(5, 17, 11)$, automorphism of Z_{18}
$\pi(1) = \pi(2) = \pi(4) = \pi(5) = 1$, $\mathrm{Par}\,\varphi = (18;\ 1,\ 6,\ 7,\ 1)$

$\varphi_4 = (1, 11, 13, 17, 7, 5)\,(2, 4, 8, 16, 14, 10)\,(3, 15)\,(6, 12)$, automorphism of Z_{18}

$\pi(1) = \pi(2) = \pi(3) = \pi(6) = 1$, $\operatorname{Par}\varphi = (18;\ 1,\ 10,\ 11,\ 1)$

$\varphi_5 = (1, 13, 7)\,(2, 8, 14)\,(4, 16, 10)\,(5, 11, 17)$, automorphism of Z_{18}

$\pi(1) = \pi(2) = \pi(4) = \pi(5) = 1$, $\operatorname{Par}\varphi = (18;\ 1,\ 12,\ 13,\ 1)$

$\varphi_6 = (1, 17)\,(2, 16)\,(3, 15)\,(4, 14)\,(5, 13)\,(6, 12)\,(7, 11)\,(8, 10)$, automorphism of Z_{18}

$\pi(1) = \pi(2) = \pi(3) = \pi(4) = \pi(5) = \pi(6) = \pi(7) = \pi(8) = 1$, $\operatorname{Par}\varphi = (18;\ 1,\ 16,\ 17,\ 1)$

$\varphi_7 = (1, 3, 5, 7, 9, 11, 13, 15, 17)$, 8-balanced skew-morphism of Z_{18}

$\pi(1) = 8$, $\operatorname{Par}\varphi = (18;\ 2,\ 2,\ 1,\ 8)$

$\varphi_8 = (1, 5, 9, 13, 17, 3, 7, 11, 15)$, 8-balanced skew-morphism of Z_{18}

$\pi(1) = 8$, $\operatorname{Par}\varphi = (18;\ 2,\ 4,\ 1,\ 8)$

$\varphi_9 = (1, 7, 13)\,(3, 9, 15)\,(5, 11, 17)$, 2-balanced skew-morphism of Z_{18}

$\pi(1) = \pi(3) = \pi(5) = 2$, $\operatorname{Par}\varphi = (18;\ 2,\ 6,\ 1,\ 2)$

$\varphi_{10} = (1, 9, 17, 7, 15, 5, 13, 3, 11)$, 8-balanced skew-morphism of Z_{18}

$\pi(1) = 8$, $\operatorname{Par}\varphi = (18;\ 2,\ 8,\ 1,\ 8)$

$\varphi_{11} = (1, 11, 3, 13, 5, 15, 7, 17, 9)$, 8-balanced skew-morphism of Z_{18}

$\pi(1) = 8$, $\operatorname{Par}\varphi = (18;\ 2,\ 10,\ 1,\ 8)$

$\varphi_{12} = (1, 13, 7)\,(3, 15, 9)\,(5, 17, 11)$, 2-balanced skew-morphism of Z_{18}

$\pi(1) = \pi(3) = \pi(5) = 2$, $\operatorname{Par}\varphi = (18;\ 2,\ 12,\ 1,\ 2)$

$\varphi_{13} = (1, 15, 11, 7, 3, 17, 13, 9, 5)$, 8-balanced skew-morphism of Z_{18}

$\pi(1) = 8$, $\operatorname{Par}\varphi = (18;\ 2,\ 14,\ 1,\ 8)$

$\varphi_{14} = (1, 17, 15, 13, 11, 9, 7, 5, 3)$, 8-balanced skew-morphism of Z_{18}

$\pi(1) = 8$, $\operatorname{Par}\varphi = (18;\ 2,\ 16,\ 1,\ 8)$

The above list is contained in the list of all skew-morphisms of Z_{18} included in [7]. The remaining skew-morphisms of Z_{18} obtained by [7] not on our list (i.e., skew-morphisms which are not coset-preserving, or equivalently, skew-morphisms with the periodicities at least 2) alongside with their periodicities and corresponding powers are listed below:

$$\varphi_{15} = (1, 11, 7, 5, 13, 17)\,(2, 16, 14, 4, 8, 10)\,(3, 15)\,(6, 12), \quad p_{\varphi_{15}} = 2, \quad \varphi_{15}^2 = \varphi_3$$

$$\varphi_{16} = (1, 17, 7, 11, 13, 5)\,(2, 4, 14, 10, 8, 16)\,(3, 15)\,(6, 12), \quad p_{\varphi_{16}} = 2, \quad \varphi_{16}^2 = \varphi_3$$

$$\varphi_{17} = (1, 5, 13, 11, 7, 17)\,(2, 16, 8, 10, 14, 4)\,(3, 15)\,(6, 12), \quad p_{\varphi_{17}} = 2, \quad \varphi_{17}^2 = \varphi_5$$

$$\varphi_{18} = (1, 17, 13, 5, 7, 11)\,(2, 10, 8, 4, 14, 16)\,(3, 15)\,(6, 12), \quad p_{\varphi_{18}} = 2, \quad \varphi_{18}^2 = \varphi_5$$

$$\varphi_{19} = (1, 9, 5, 7, 15, 11, 13, 3, 17)\,(2, 14, 8)\,(4, 10, 16), \quad p_{\varphi_{19}} = 3, \quad \varphi_{19}^3 = \varphi_9$$

$$\varphi_{20} = (1, 15, 5, 7, 3, 11, 13, 9, 17)\,(2, 8, 14)\,(4, 16, 10), \quad p_{\varphi_{20}} = 3, \quad \varphi_{20}^3 = \varphi_9$$

$$\varphi_{21} = (1, 15, 17, 7, 3, 5, 13, 9, 11)\,(2, 14, 8)\,(4, 10, 16), \quad p_{\varphi_{21}} = 3, \quad \varphi_{21}^3 = \varphi_9$$

$$\varphi_{22} = (1, 3, 17, 7, 9, 5, 13, 15, 11)\,(2, 8, 14)\,(4, 16, 10), \quad p_{\varphi_{22}} = 3, \quad \varphi_{22}^3 = \varphi_9$$

$$\varphi_{23} = (1, 3, 11, 7, 9, 17, 13, 15, 5)\,(2, 14, 8)\,(4, 10, 16), \quad p_{\varphi_{23}} = 3, \quad \varphi_{23}^3 = \varphi_9$$

$$\varphi_{24} = (1, 9, 11, 7, 15, 17, 13, 3, 5)\,(2, 8, 14)\,(4, 16, 10), \quad p_{\varphi_{24}} = 3, \quad \varphi_{24}^3 = \varphi_9$$

$$\varphi_{25} = (1, 11, 15, 13, 5, 9, 7, 17, 3)\,(2, 14, 8)\,(4, 10, 16), \quad p_{\varphi_{25}} = 3, \quad \varphi_{25}^3 = \varphi_{12}$$

$$\varphi_{26} = (1, 17, 3, 13, 11, 15, 7, 5, 9)\,(2, 8, 14)\,(4, 16, 10), \quad p_{\varphi_{26}} = 3, \quad \varphi_{26}^3 = \varphi_{12}$$

$$\varphi_{27} = (1, 17, 9, 13, 11, 3, 7, 5, 15)\,(2, 14, 8)\,(4, 10, 16), \quad p_{\varphi_{27}} = 3, \quad \varphi_{27}^3 = \varphi_{12}$$

$$\varphi_{28} = (1, 5, 15, 13, 17, 9, 7, 11, 3)\,(2, 8, 14)\,(4, 16, 10), \quad p_{\varphi_{28}} = 3, \quad \varphi_{28}^3 = \varphi_{12}$$

$$\varphi_{29} = (1, 5, 3, 13, 17, 15, 7, 11, 9)\,(2, 14, 8)\,(4, 10, 16), \quad p_{\varphi_{29}} = 3, \quad \varphi_{29}^3 = \varphi_{12}$$

$$\varphi_{30} = (1, 11, 9, 13, 5, 3, 7, 17, 15)\,(2, 8, 14)\,(4, 16, 10), \quad p_{\varphi_{30}} = 3, \quad \varphi_{30}^3 = \varphi_{12}$$

We see that each skew-morphism φ not obtained by our classification, i.e., a skew-morphism with the periodicity $p_\varphi \geq 2$, admits the power, namely the p_φ-th power, which is a coset-preserving skew-morphism included in our classification. This is no coincidence, as it holds true for all non-trivial skew-morphisms of cyclic groups by Theorem 8.

In particular, for the group Z_{18} all powers φ^{p_φ} of skew-morphisms satisfying $p_\varphi \geq 2$ equal one of the four following coset-preserving skew-morphisms:

$$\varphi_3 = (1,7,13)\,(2,14,8)\,(4,10,16)\,(5,17,11), \quad \text{automorphism of } \mathrm{Z}_{18},$$

$$\varphi_5 = (1,13,7)\,(2,8,14)\,(4,16,10)\,(5,11,17), \quad \text{automorphism of } \mathrm{Z}_{18},$$

$$\varphi_9 = (1,7,13)\,(3,9,15)\,(5,11,17), \quad \text{2-balanced skew-morphism of } \mathrm{Z}_{18},$$

$$\varphi_{12} = (1,13,7)\,(3,15,9)\,(5,17,11), \quad \text{2-balanced skew-morphism of } \mathrm{Z}_{18}.$$

According to the above list of all skew-morphisms of Z_{18}, coset-preserving skew-morphisms φ_3 and φ_5 both admit 2 second roots which are skew-morphisms with the periodicities 2. Coset-preserving skew-morphisms φ_9 and φ_{12} both admits 6 third roots which are skew-morphisms with the periodicities 3. Thus, all 14 skew-morphisms of Z_{18} which are not coset-preserving are obtained as the root of one of the four coset-preserving skew-morphisms φ_3, φ_5, φ_9 and φ_{12}.

None of the remaining coset-preserving skew-morphisms φ_1, φ_2, φ_4, φ_6, φ_7, φ_8, φ_4, φ_{10}, φ_{11}, φ_{13} and φ_{14} of Z_{18} admits k-th root which is a skew-morphism with the periodicity k.

Chapter 4

Conclusion

In this chapter we summarize the results of this thesis and outline possible directions of further study of skew-morphisms.

4.1 Summary of results

In this section we summarize all the new results of this thesis.

In Section 2.5, we introduced the concept of the periodicity for skew-morphisms of abelian groups and proved some of its important properties (see Lemma 4). The periodicity plays a key role in the study of powers of skew-morphisms of abelian groups as we have shown in Sections 3.1 and 3.2.

In Section 2.6, we introduced additional properties of two important subclasses of skew-morphisms (Lemmas 5, 6 and 7). The first subclass was the class of the t-balanced skew-morphisms, a generalization of the previously introduced concept of skew-morphisms associated to t-balanced regular Cayley maps. The second subclass was consisted of coset-preserving skew-morphisms, the concept introduced in [1].

The two most important results of this thesis are contained in Chapter 3.

The first result states that a skew-morphism φ of an abelian group A with the periodicity p_φ possesses a power, namely the p_φ-th power, which is a coset-preserving skew-morphism of A. Moreover, if φ has a generating orbit, then φ^{p_φ} is a non-trivial coset-preserving skew-morphism of A, and if φ has a generating orbit closed under taking inverses, then φ^{p_φ} is a non-trivial t-balanced skew-morphism of A or a non-trivial automorphism of A (see Theorems 6, 7, 8 and 9).

The second result is the complete classification of coset-preserving skew-morphisms for the class of cyclic groups through sets of admissible parameters presented in Section 3.3. This classification is a significant step toward the classification of all skew-morphisms of cyclic groups, as each skew-morphism of a cyclic group possesses a power which is a non-trivial coset-preserving skew-morphism by Theorem 8.

4.2 Concluding remarks

According to the results of Section 3.2, each skew-morphism of a cyclic group can be constructed as the 'root' of some non-trivial coset-preserving skew-morphism. However, a general permutation might have more than one root and it appears very hard to determine which roots of the coset-preserving skew-morphisms of cyclic groups are skew-morphisms as well. Next step of our research is to study this problem for the most simple non-trivial case. In particular, our aim is to classify all skew-morphisms of cyclic groups with the smallest possible non-trivial periodicity $p_\varphi = 2$, for which φ^2 is a group automorphism.

Another possible direction of research is a further investigation of coset-preserving skew-morphisms of cyclic groups employing their complete classification presented in Section 3.3. As the number of all coset-preserving skew-morphisms for a given cyclic group Z_n equals the number of all admissible parameters sets (see Theorem 11) with the first parameter n, it might be possible to enumerate, or at least bound, this number by a function of n. A straightforward upper bound on the number of all coset-preserving skew-morphisms of Z_n is n^4, as each parameter is non-negative integer less than or equal to n. However, our program for finding all admissible parameters sets for given n indicates that it might be possible to decrease this bound as the number of admissible parameters sets does not exceed n^2 for positive integers n up to 500. Consequently, we might employ the obtained upper bound and Theorem 8 to find an upper bound on the number of all skew-morphisms of a cyclic group Z_n.

Results introduced in Sections 3.1 and 3.2 are based on the concept of the periodicity and its properties (see Section 2.5). Thus these results are relevant only for the case of abelian groups, as a general skew-morphism φ of a non-abelian group might not possesses the periodic distribution of the power function on the orbits of φ (see [2] or [15] for examples). It might prove useful in the study of skew-morphisms of non-abelian groups to determine skew-morphisms for which the concept of the periodicity is still relevant, or to develop a concept similar to the periodicity for the case of skew-morphisms of non-abelian groups

References

[1] M. Bachratý, Powers of skew-morphisms, Bachelor thesis, 2013.

[2] M. Bachratý, R. Jajcay, Powers of skew-morphisms, submitted for publication.

[3] N. Biggs, Cayley maps and symmetrical maps, Proc. Camb. Phil. Soc. 72 (1972) 381–386.

[4] N. Biggs, A.T. White, Permutation groups and combinatorial structures, Mathematical Society Lecture Notes 33, Cambridge University Press, Cambridge, 1979.

[5] P. Cameron, Permutation groups, Cambridge University Press, Cambridge, 1999.

[6] A. Cayley, Desiderata and suggestions: No. 2. The Theory of groups: graphical representation, Amer. J. Math. 1 (2) (1878) 174–176.

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

[8] M. Conder, R. Jajcay, T. Tucker, Regular t-balanced Cayley maps, J. Comb. Theory Ser. B 97 (3) (2007) 453-473.

[9] M. Conder, R. Jajcay T. Tucker, Cyclic complements and skew-morphisms of groups, submitted for publication.

[10] M. Conder, T. Tucker, Regular Cayley maps for cyclic groups, Trans. Amer. Math. Soc. 366 (7) (2014) 3585–3609.

[11] R. Feng, R. Jajcay, Y. Wang, Regular t-balanced Cayley maps for abelian groups, Discrete Math. 311 (21) (2011) 2309-2316.

[12] J.L. Gross and T. Tucker, Topological graph theory, Wiley, New York, 1987 (Dover paperbck, 2001).

[13] R. Jajcay, Automorphism groups of Cayley maps, J. Combin. Theory Ser. B 59 (1993) 297–310.

[14] R. Jajcay, R. Nedela, Half-regular Cayley maps, to appear in Graphs and Combin.

[15] R. Jajcay, J. Širáň, Skew-morphisms of regular Cayley maps, Discrete Math. 244 (1-3) (2002) 167-179.

[16] I. Kovács, R. Nedela, Decomposition of skew-morphisms of cyclic groups, Ars. Math. Contemp. (4) (2011) 329-349.

[17] Y.S. Kwon, A classification of regular t-balanced Cayley maps for cyclic groups, Discrete Math. 313 (2013) 656-664.

[18] R.B. Richter, J. Širáň, R. Jajcay, T.W. Tucker, M.E. Watkins, Cayley maps, J.Combin. Theory Ser. B 95 (2) (2005) 189-245.

[19] G. Sabidussi, On a Class of Fixed-Point-Free Graphs, Proc. Amer. Math. Soc. 9 (5) (1958) 800–804.

[20] J. Širáň, M. Škoviera, Groups with sign structure and their antiautomorphisms, Discrete Math. 108 (1992) 189–202.

[21] M. Škoviera, J. Širáň, Regular maps from Cayley graphs I: balanced Cayley maps, Discrete Math. 109 (1992) 265–276.

[22] J. Širáň, M. Škoviera, Regular maps from Cayley graphs II: antibalanced Cayley maps, Discrete Math. 124 (1994) 179–191.