Dihedral-like Constructions of Automorphic Loops

Mouna Ramadan Aboras

University of Denver

Follow this and additional works at: https://digitalcommons.du.edu/etd

Part of the Algebra Commons, and the Algebraic Geometry Commons

Recommended Citation


This Dissertation is brought to you for free and open access by the Graduate Studies at Digital Commons @ DU. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons @ DU. For more information, please contact jennifer.cox@du.edu,dig-commons@du.edu.
Dihedral-like constructions of
automorphic loops

A DISSERTATION
Presented to
the Faculty of Natural Sciences and Mathematics
University of Denver

IN PARTIAL FULFILLMENT
of the Requirements for the Degree
of Doctor of Philosophy

BY
MOUNA ABOEAS
JUNE 2015
ADVISOR: PETR VOJTĚCHOVSKÝ
Abstract

In this dissertation we study dihedral-like constructions of automorphic loops. Automorphic loops are loops in which all inner mappings are automorphisms. We start by describing a generalization of the dihedral construction for groups. Namely, if $(G, +)$ is an abelian group, $m > 1$ and $\alpha \in \text{Aut}(G)$, let $\text{Dih}(m, G, \alpha)$ on $\mathbb{Z}_m \times G$ be defined by

$$(i, u)(j, v) = (i + j, ((-1)^j u + v)\alpha^{ij}).$$

We prove that the resulting loop is automorphic if and only if $m = 2$ or $(\alpha^2 = 1$ and $m$ is even) or $(m$ is odd, $\alpha = 1$ and $\exp(G) \leq 2)$. In the last case, the loop is a group. The case $m = 2$ was introduced by Kinyon, Kunen, Phillips, and Vojtěchovský.

We study basic structural properties of dihedral-like automorphic loops. We describe certain subloops, including: nucleus, commutant, center, associator subloop and derived subloop. We prove theorems for dihedral-like automorphic loops analogous to the Cauchy and Lagrange theorems for groups, and further we discuss the coset decomposition in dihedral-like automorphic loops.

We show that two finite dihedral-like automorphic loops $\text{Dih}(m, G, \alpha)$ and $\text{Dih}(\overline{m}, \overline{G}, \overline{\alpha})$ are isomorphic if and only if $m = \overline{m}$, $G \cong \overline{G}$ and $\alpha$ is conjugate to $\overline{\alpha}$ in $\text{Aut}(G)$. We describe the automorphism group of $Q$ and its subgroup consisting of inner mappings of $Q$. 
Finally, due to the solution to the isomorphism problem, we are interested in studying conjugacy classes of automorphism groups of finite abelian groups. Then we describe all dihedral-like automorphic loops of order $< 128$ up to isomorphism. We conclude with a description of all dihedral-like automorphic loops of order $< 64$ up to isotopism.
Acknowledgements

I would like to thank everyone who have helped and inspired me during my doctoral study. My deepest appreciation goes to my advisor and mentor, Professor Petr Vojtěchovský, for his rich patience in discussions, motivation, support, guidance, and generosity. Without his patience I could have never reached as far as I have. Furthermore, Michael Kinyon has been a constant source of assistance, especially during the early stage of my study. I would like to thank the rest of my thesis committee-Prof. Scott Leutenegger, Prof. Nikolaos Galatos, Prof. Andrew Linshaw and Prof. Izabella Stuhl for their time and effort. I also extend my appreciation to the Department of Mathematics for providing me with financial support to attend conferences.

My special thanks also go to Liane Beights for her help. To all the people whom I met over my years of education who helped me along the way by their kindness, advice, instruction, and encouragement.

Finally, I would like to thank my beloved husband, Abdualhmed who went through graduate school along with me. To my parents, Mr. Ramadan and Mrs. Bhalula, who have taught me what real hard work really is.
# Contents

1 Introduction .......................... 1
   1.1 Structure of the thesis ............. 3
   1.2 Notation .......................... 5
   1.3 Background on loop theory ......... 6
   1.4 Background on automorphic loops 14
   1.5 Advanced results in automorphic loops 15

2 Parameters that yield automorphic loops 18
   2.1 The multiplication formula ....... 18
   2.2 Middle inner mappings ............ 20
   2.3 Left inner mappings ............... 23
   2.4 Main result ........................ 32
   2.5 Inner mappings in the automorphic case 33
   2.6 Groups among dihedral-like automorphic loops 35

3 Basic Properties ....................... 37
   3.1 Nuclei ............................ 37
   3.2 Commutant ......................... 39
   3.3 Center and central nilpotence .... 40
   3.4 Associators and the associator subloops 42
   3.5 Commutators and the derived subloops 45
   3.6 Cauchy’s and Lagrange’s Theorem for dihedral-like automorphic loops 47
      3.6.1 Cauchy’s and Lagrange’s theorems 47

4 Automorphisms of dihedral-like automorphic loops 49
   4.1 Squaring and conjugation .......... 50
   4.2 The isomorphism problem .......... 51
   4.3 All isomorphisms .................. 54
   4.4 Automorphism groups ............... 59
   4.5 The inner mapping groups .......... 61

5 Enumeration ........................... 64
   5.1 Conjugacy classes in automorphism groups of abelian groups .... 65
   5.2 Dihedral-like automorphic loops of order < 128 up to isomorphism 73
5.3 Dihedral-like automorphic loops up to isotopism ............... 82

Bibliography ........................................... 86

Appendix ............................................... 90

vi
Chapter 1

Introduction

Loops are essentially non-associative groups. More precisely, they are binary algebraic structures in which the left and right translation maps $L_x$ and $R_x$ defined by $L_x : y \mapsto xy$ and $R_x : y \mapsto yx$ are bijections, and they have a two-sided identity element 1. In other words, they are quasigroups with identity. Thus, the set of left and right translation maps generates a permutation group, called the multiplication group. The subgroup of the multiplication group stabilizing the neutral element of the loop is called the inner mapping group of the loop. These permutation groups provide a strong connection between loop theory and group theory. In principle, we can transform loop theoretical problems into group theoretical problems. The foundations of loop theory were laid in 1946 by Bruck [5].

The generalized dihedral group $\text{Dih}(G)$ is a certain semidirect product $\mathbb{Z}_2 \rtimes G$, where $G$ is an abelian group and $\mathbb{Z}_2$ is the cyclic group of order 2. If $G$ is cyclic, then $\text{Dih}(G)$ is called a dihedral group—it is a group that captures symmetries of regular $n$-gons. The group $\text{Dih}(\mathbb{Z}_n)$ is often denoted by $D_{2n}$ to indicate the number of its elements.
In 1956, R. H. Bruck and L. J. Paige (who was Bruck’s student) defined a new class of loops, called automorphic loops (or sometimes just A-loops), which are loops in which every inner mapping is an automorphism.

Groups and commutative Moufang loops (but not all Moufang loops) are automorphic loops. They discussed in detail the basic properties for automorphic loops in [4]. In the same paper they also showed that automorphic loops with the inverse property are diassociative and that there exist non-commutative diassociative A-loops. Bruck and Paige conjectured that every diassociative automorphic loop is a Moufang loop. In 1958, J. M. Osborn offered a proof of this conjecture in the commutative case in [31]. In 2000, Kinyon, Kunen, and Phillips solved the general case.

Automorphic loops have been widely discussed in the literature, following the papers of Jedlička, Kinyon and Vojtěchovský [22]. A detailed account can be found in Section 1.3.

The goal of this dissertation is a study of a large class of automorphic loops obtained as follows: Let $m$ be a positive even integer, $G$ an abelian group, and $\alpha$ an automorphism of $G$ that satisfies $\alpha^2 = 1$ if $m > 2$. The dihedral-like automorphic loop $\text{Dih}(m, G, \alpha)$ is defined on $\mathbb{Z}_m \times G$ by

$$(i, u)(j, v) = (i + j, ((-1)^j u + v)\alpha^{ij}).$$

A special case of this definition with $m = 2$ was introduced by Kinyon, Kunen, Phillips, and Vojtěchovský in [25]. Dihedral-like automorphic loops are of interest because they account for many small automorphic loops. For instance, by [25,
Corollary 9.9], an automorphic loop of order $2p$, with $p$ an odd prime, is either the cyclic group $\mathbb{Z}_{2p}$ or a loop $\text{Dih}(2, \mathbb{Z}_p, \alpha)$. The notion of associative dihedral-like automorphic loops encompasses dihedral groups $\text{Dih}(2, \mathbb{Z}_n, 1) = D_{2n}$, the generalized dihedral groups $\text{Dih}(2, G, 1) = \text{Dih}(G)$, and certain generalized dicyclic groups $\text{Dih}(4, G, 1)$.

### 1.1 Structure of the thesis

This dissertation consists of five parts.

In Chapter 1, we briefly recall definitions and preliminary results about loops in Section 1.3, and about automorphic loops in Section 1.4.

In Chapter 2, we characterize the parameters in the construction $\text{Dih}(m, G, \alpha)$ that yield automorphic loops.

In Chapter 3, we describe certain subloops of dihedral-like automorphic loops, e.g., nucleus, commutant, center, commutator subloop, associator subloop, and derived subloop. Also, we point out when the subloops are normal. We conclude the chapter by having a look at central nilpotency of dihedral-like automorphic loop. We prove Cauchy’s and Lagrange’s theorems, and we discuss coset decompositions in dihedral-like automorphic loops.

In Chapter 4, we solve the isomorphism problem for dihedral-like automorphic loops. We prove that $\text{Dih}(m, G, \alpha)$ and $\text{Dih}(\overline{m}, \overline{G}, \overline{\alpha})$ are isomorphic if and only if $m = \overline{m}$, $G \cong \overline{G}$ and $\alpha$ is conjugate to $\overline{\alpha}$ in $\text{Aut}(G)$. Moreover, for a finite dihedral-like automorphic loop $Q$ we describe the structure of the automorphism group of $Q$ and its subgroup consisting of inner mappings of $Q$.
In Chapter 5, we build on the solution of the isomorphism problem from Chapter 4. We describe all dihedral-like automorphic loops of order $< 128$. We also investigate dihedral-like automorphic loops up to isotopy.

Appendix includes the GAP code [30] that was used during this research.
1.2 Notation

The following notation will be used throughout the work,

- $G$: an abelian group
- $xy$: $x \cdot y$
- $x \cdot yz$: $x \cdot (y \cdot z)$
- $R_x$: the right translation by $x$
- $L_x$: the left translation by $x$
- $N(Q)$: nucleus of $Q$
- $Z(Q)$: center of $Q$
- $C(Q)$: commutant of $Q$
- $x \backslash y = yL_x^{-1}$: left division operation
- $y/x = yR_x^{-1}$: right division operation
- $[x, y]$: the commutator of $x$ and $y$
- $[x, y, z]$: the associator of $x, y$ and $z$
- $Q'$: the derived subloop of $Q$
- $D_{2n}$: the dihedral group of order $2n$
- $A(Q)$: the associator subloop of $Q$
- $\mathbb{Z}_n$: the cyclic group of order $n$
- $\mathbb{Z}_n^k$: the group $\mathbb{Z}_n \times \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n$
- $\mathbb{Z}_n^*$: the multiplicative group of the cyclic group $\mathbb{Z}_n$
- $\mathbb{F}_n$: the finite field of order $n$
- $GL_n(\mathbb{F}_k)$: the general linear group of $n \times n$ matrices over $\mathbb{F}_k$
- $G \rtimes_\phi H$: the semi-direct product of $G$ and $H$ with respect to the action
- $G \times H$: the direct product of $G$ and $H$
- $H \leq G$: $H$ is a subloop of $G$
- $H \triangleleft G$: $H$ is a normal subloop of $G$
$H \cong G$ \hspace{1cm} $H$ is isomorphic to $G$

$\ker(\phi)$ \hspace{1cm} the kernel of $\phi$

$\text{Im}(\phi)$ \hspace{1cm} the image of $\phi$

1.3 Background on loop theory

The purpose of this section is to fix basic terminology conventions and briefly review background results, for the convenience of the reader. Many of the following definitions can be found in [3] or [32].

Definition 1.3.1. Let $Q$ be a set with a binary operation $\cdot$ and $x \in Q$. Then

(i) the map $L_x : Q \to Q$ defined by $yL_x = xy$ is called the left translation by $x$, or the left multiplication by $x$.

(ii) the map $R_x : Q \to Q$ defined by $yR_x = yx$ is called the right translation by $x$, or the right multiplication by $x$.

Definition 1.3.2. A loop is a set $Q$ with a binary operation $\cdot$ such that

(i) all left translations and all right translations are bijections, and

(ii) there exists $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$.

Since the left and right translations of a loop are bijective, the inverse mappings $L_x^{-1}$ and $R_x^{-1}$ exist. Let $x/y = yL_x^{-1}$ and $x/y = xR_y^{-1}$ and note that $x/y = z \iff x \cdot z = y$ and $x/y = z \iff z \cdot y = x$.

From now on, let $Q$ be a loop.

Definition 1.3.3. The group generated by both types of translations

$$\text{Mlt}(Q) = \langle L_x, R_x : x \in Q \rangle,$$
is called the multiplication group of $Q$, while the left and right multiplication groups are defined, respectively, by $\text{Mlt}_l(Q) = \langle L_x : x \in Q \rangle$, $\text{Mlt}_r(Q) = \langle R_x : x \in Q \rangle$.

**Definition 1.3.4.** The stabilizer in $\text{Mlt}(Q)$ of the neutral element 1 of $Q$ is called the inner mapping group of $Q$, i.e,

$$\text{Inn}(Q) = \text{Mlt}(Q)_1 = \{ \xi \in \text{Mlt}(Q) : 1\xi = 1 \},$$

while the left and right inner mapping groups are defined, respectively, by $\text{Inn}_l(Q) = \text{Mlt}_l(Q)_1 = \{ \xi \in \text{Mlt}_l(Q) : 1\xi = 1 \}$, $\text{Inn}_r(Q) = \text{Mlt}_r(Q)_1 = \{ \xi \in \text{Mlt}_r(Q) : 1\xi = 1 \}$.

**Definition 1.3.5.** Let $x$ and $y$ be elements of a loop $Q$. Define bijections $T_x$, $R_{x,y}$ and $L_{x,y}$ by

$$T_x = R_x L_x^{-1} \quad \text{(middle inner mappings (generalized conjugations))}$$

$$R_{x,y} = R_x R_y R_{xy}^{-1}, \quad \text{(right inner mappings)}$$

$$L_{x,y} = L_x L_y L_{yx}^{-1}. \quad \text{(left inner mappings)}$$

The mappings $L_{x,y}, R_{x,y}$ measure nonassociativity, while $T_x$ measures noncommutativity. It turns out [32] that

$$\text{Inn}(Q) = \langle L_{x,y}, R_{x,y}, T_x : x, y \in Q \rangle,$$

$$\text{Inn}_l(Q) = \langle L_{x,y} : x, y \in Q \rangle,$$

$$\text{Inn}_r(Q) = \langle R_{x,y} : x, y \in Q \rangle.$$

**Definition 1.3.6.** A loop $Q$ is an inverse property loop if every $x \in Q$ has a unique two-sided inverse, which we denote $x^{-1}$, and if, for all $x, y \in Q$, the following
identities hold

\[ x^{-1}(xy) = y, \quad \text{(the left inverse property)} \]

and

\[ (yx)x^{-1} = y. \quad \text{(the right inverse property)} \]

**Definition 1.3.7.** A loop \( Q \) has the anti-automorphic inverse property (or AAIP) if it has two-sided inverses and satisfies the identity

\[ (xy)^{-1} = y^{-1}x^{-1} \quad \text{(AAIP)} \]

for all \( x, y \in Q \).

Inverse property loops satisfy the anti-automorphic inverse property.

Let \( Q_1, Q_2 \) be loops.

**Definition 1.3.8.** A mapping \( \phi : Q_1 \rightarrow Q_2 \) is a homomorphism if \( \phi(g \cdot h) = \phi(g) \cdot \phi(h) \) for all \( g, h \in Q_1 \).

**Definition 1.3.9.** A homomorphism \( \phi : Q_1 \rightarrow Q_2 \) is called an isomorphism if it is bijection. An isomorphism \( \phi : Q_1 \rightarrow Q_1 \) is called an automorphism. The set of all automorphisms of a loop \( Q \) forms a group under composition, called the automorphism group of \( Q \), denoted by \( \text{Aut}(Q) \).

**Definition 1.3.10.** A direct product of two groups \( (H, \cdot) \) and \( (K, \star) \) is a group \( G = \{(h, k) : h \in H, k \in K\} \) with operation \( \circ \) defined by \( (h_1, k_1) \circ (h_2, k_2) = \)
A semidirect product of two groups \((H, \cdot)\) and \((K, \star)\) is a group \(G = \{(h, k) : h \in H, k \in K\}\) with operation \(\circ\) defined by \((h_1, k_1) \circ (h_2, k_2) = (h_1 \cdot \phi_{k_1}(h_2), k_1 \star k_2)\), where \(\phi : K \rightarrow \text{Aut}(H)\) is a homomorphism. The semidirect product is denoted by \(G = H \rtimes K\), or by \(H \rtimes_{\phi} K\) if \(\phi\) is to be emphasized.

**Definition 1.3.11.** Let \(H\) be a nonempty subset of a loop \(Q\). We say \(H\) is a subloop \((H \triangleleft Q)\) of \(Q\) if it is closed under the three binary operations \(\cdot\) (multiplication), \(\backslash\) (left division), and \(/\) (right division).

**Definition 1.3.12.** Let \(H\) be a subloop of a loop \(Q\). Then \(H\) is a normal subloop \((H \triangleleft Q)\) of \(Q\) if for all \(x, y \in Q\)

\[
xH = Hx, (xH)y = x(Hy), x(yH) = (xy)H.
\]

**Definition 1.3.13.** Let \(Q\) be a loop and \(H \leq Q\). For a given \(x \in Q\), define \(xH = \{x \cdot h : h \in H\}\) and \(Hx = \{h \cdot x : h \in H\}\) to be the left coset and right coset of \(x\) with respect to \(H\) (or modulo \(H\)), respectively.

**Definition 1.3.14.** Let \(H\) be a normal subloop of a loop \(Q\). The cosets \(Hx\) for \(x\) in \(Q\) form a loop with operation \((Hx)(Hy) = H(xy)\). This loop is called the factor loop of \(Q\) over \(H\), denoted by \(Q/H\).

**Definition 1.3.15.** Let \(Q\) be a finite loop and let \(H\) be a subloop of \(Q\). We say that \(H\) is Lagrange-like if \(|H|\) divides \(|Q|\). We also say that \(Q\) has the Lagrange’s property if every \(H \leq Q\) is Lagrange-like.

Unlike for groups, left (right) cosets of a subloop of a loop need not partition the loop. For example, let \(Q = \{1, 2, 3, 4, 5\}\), with a binary operation \(\cdot\) defined by
We can see that \( H = \{1, 2\} \leq Q \) and the left cosets modulo \( H \) are 
\[
\begin{array}{c|ccccc}
\cdot & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 \\
2 & 2 & 1 & 5 & 3 & 4 \\
3 & 3 & 4 & 1 & 5 & 2 \\
4 & 4 & 5 & 2 & 1 & 3 \\
5 & 5 & 3 & 4 & 2 & 1 \\
\end{array}
\]

Since \(|Q| = 5\) and \(|H| = 2\), we can see that \( H \) is not Lagrange-like. In particular, the left cosets of \( H \) do not partition \( Q \).

**Definition 1.3.16.** The left, right, and middle nucleus of a loop \( Q \) are defined, respectively, by

\[
N_\lambda(Q) = \{a \in Q : ax \cdot y = a \cdot xy, \forall x, y \in Q\},
\]

\[
N_\rho(Q) = \{a \in Q : xy \cdot a = x \cdot ya, \forall x, y \in Q\},
\]

\[
N_\mu(Q) = \{a \in Q : xa \cdot y = x \cdot ay, \forall x, y \in Q\}.
\]

The nucleus of \( Q \) is defined as \( N(Q) = N_\lambda(Q) \cap N_\rho(Q) \cap N_\mu(Q) \).

Each of the nuclei is a subloop. All nuclei are in fact groups. If \( Q \) is an inverse property loop, all these nuclei are equal \([14]\):

\[
N_\lambda(Q) = N_\mu(Q) = N_\rho(Q) = N(Q).
\]

**Definition 1.3.17.** A loop \( Q \) has a left (right) coset decomposition modulo a subloop \( H \) if the left (right) cosets form a partition of \( Q \). If \( Q \) has left and right coset
decompositions modulo $H$, then we say that $Q$ has a coset decomposition modulo $H$.

**Proposition 1.3.18.** ([32, Theorem I.2.12]) A loop $Q$ has a left coset decomposition modulo a subloop $H$ if and only if for any $x \in Q$ and $h \in H$, $(xh)H = xH$.

**Theorem 1.3.19.** ([32, Theorem I.2.16]) Let $Q$ be a finite loop and let $H$ be a subloop of $Q$. If $Q$ has a left (or right) coset decomposition with respect to $H$, then $H$ is Lagrange-like.

**Definition 1.3.20.** The commutant of a loop $Q$, denoted by $C(Q)$, is the set of all elements that commute with every element of $Q$. In symbols,

$$C(Q) = \{ x \in Q : xy = yx, \forall y \in Q \}.$$

**Definition 1.3.21.** For a subset $H$ of a loop $Q$, the commutant of $H$ in $Q$ is defined by

$$C_Q(H) = \{ x \in Q : xy = yx, \forall y \in H \}$$

**Definition 1.3.22.** The center $Z(Q)$ of a loop $Q$ is the set of all elements of $Q$ that commute and associate with all other elements of $Q$. It can be characterized as $Z(Q) = C(Q) \cap N(Q)$.

The center is always a normal subloop of $Q$.

**Definition 1.3.23.** Let $Q_1$, $Q_2$ be loops. A loop $Q$ is an extension of $Q_1$ by $Q_2$ if $Q_1$ is a normal subloop of $Q$ such that $Q/Q_1$ is isomorphic to $Q_2$. An extension $Q$ of $Q_1$ by $Q_2$ in central if $Q_1$ is an abelian group and $Q_1 \leq Z(Q)$.  

11
Definition 1.3.24. Let $Q$ be a loop. The upper central series of $Q$ is

$$Z_0(Q) \leq Z_1(Q) \leq Z_2(Q) \leq \cdots \leq Z_n(Q) \leq \cdots \leq Q,$$

where $Z_0(Q) = \{1\}$ and $Z_i(Q)$ is the preimage of $Z(Q/Z_{i-1}(Q))$ under the quotient map. If there exists some $n$ such that $Z_n(Q) = Q$ then $Q$ is said to be (centrally) nilpotent of class $n$.

The concepts of the commutator of two elements and the associator of three elements in loops can be defined in a way that is similar to the commutator definition from groups.

Definition 1.3.25. Let $Q$ be a loop and $x, y, z \in Q$. The commutator $[x, y]$ is the unique element of $Q$ satisfying the equation

$$x \cdot y = (y \cdot x) \cdot [x, y].$$

The associator $[x, y, z]$ is the unique element of $Q$ satisfying the equation

$$(x \cdot y) \cdot z = (x \cdot (y \cdot z)) \cdot [x, y, z].$$

Definition 1.3.26. The associator subloop of a loop $Q$, denoted by $A(Q)$, is the smallest normal subloop of $Q$ containing all associators $[x, y, z]$ of $Q$. Equivalently, $A(Q)$ is the smallest normal subloop of $Q$ such that $Q/A(Q)$ is associative.

Definition 1.3.27. The derived subloop of a loop $Q$, denoted by $Q'$, is the smallest normal subloop of $Q$ containing all associators $[x, y, z]$ and all commutators $[x, y]$, of $Q$ where $x, y, z \in Q$. Equivalently, $Q'$ is the smallest normal subloop of $Q$ such that $Q/Q'$ is a commutative group.
Definition 1.3.28. Let \((H, \cdot)\) and \((L, \circ)\) be groupoids. If \((U, V, W) : (H, \cdot) \rightarrow (L, \circ)\) are bijections, the triple \((U, V, W)\) is called an isotopism if and only if

\[ xU \circ yV = (x \cdot y)W, \quad \forall x, y \in H. \]

The groupoids \((H, \cdot)\) and \((L, \circ)\) are isotopic if and only if there is an isotopism \((H, \cdot) \leftarrow (L, \circ)\).

If one of two isotopic groupoids is a quasigroup, then both are quasigroups, but if one of two isotopic quasigroups is a loop, the other need not be a loop.

If \(H = L\) and \(W = I\) (identity mapping) then \((U, V, I)\) is called a principal isotopism, and we call \(L\) a principal isotope of \(H\). If in addition \(L\) is a loop such that for some \(f, g \in L, U = R_g\) and \(V = L_f\), then \((R_g, H_f, I) : (L, \cdot) \rightarrow (L, \circ)\) is called an \(f, g\)-principal isotopism.

Note that isotopic groups are necessarily isomorphic, but this is certainly not true for loops in general [32].

Definition 1.3.29. Let \(Q\) be a loop. Then \(Q\) is power-associative if \(\langle x \rangle\) is a subgroup for all \(x \in Q\).

A loop \(Q\) with the property \(x(yz) = (xy)z\) for all \(x, y, z \in Q\) is called a group.

Definition 1.3.30. The dihedral group of order \(2n\), denoted by \(D_{2n}\), is the group generated by two elements \(x\) and \(y\) with presentation \(x^2 = y^n = 1\) and \(xy = y^{-1}x\).

Definition 1.3.31. Let \(G\) be a group. The exponent of \(G\), denoted \(\exp(G)\), is the smallest positive integer if it exists \(m\) such that, for every \(g \in G\), \(g^m = 1\).

Definition 1.3.32. ([28, p. 170]) Let \(A\) be an abelian group and let \(y \in A\) be of
order two. The generalized dicyclic group $\text{Dic}(A, y)$ is the group generated by $A$ and another element $x$ such that $x^2 = y$ and $x^{-1}ax = a^{-1}$ for every $a \in A$. So $D_{2n} \cong \text{Dic}(\mathbb{Z}_n, 0)$. If $A = \mathbb{Z}_{2n}$ and $y$ is the unique element of order two in $A$, then $\text{Dic}(A, y) = \text{Dic}_{4n}$ is the dicyclic group of order $4n$.

1.4 Background on automorphic loops

In this section, we present some definitions and results on automorphic loops which will be used throughout this work.

Definition 1.4.1. A loop $Q$ is left automorphic (i.e. $Q$ is an $A_{\ell}$-loop) if $\text{Inn}_{\ell}(Q) \leq \text{Aut}(Q)$, and $Q$ is right automorphic (i.e. $Q$ is an $A_r$-loop) if $\text{Inn}_r(Q) \leq \text{Aut}(Q)$. Finally, $Q$ is an automorphic loop (i.e. $Q$ is an $A$-loop) if $\text{Inn}(Q) \leq \text{Aut}(Q)$, that is, if every inner mapping of $Q$ is an automorphism of $Q$.

Note that groups are automorphic loops, but the converse is certainly not true.

Proposition 1.4.2. [4] A loop $Q$ is an automorphic loop if and only if, for all $x, y, u, v \in Q$,

\[
\begin{align*}
(uv)R_{x,y} &= uR_{x,y} \cdot vR_{x,y}, & (A_r) \\
(uv)L_{x,y} &= uL_{x,y} \cdot vL_{x,y}, & (A_{\ell}) \\
(uv)T_x &= uT_x \cdot vT_x. & (A_m)
\end{align*}
\]

(1.4.1)

It turns out that to check that a particular loop is automorphic, it is not necessary to verify all of the conditions $(A_r)$, $(A_{\ell})$ and $(A_m)$.
Proposition 1.4.3. ([25, Theorem 6.7]) Let $Q$ be a loop satisfying $(A_ℓ)$ and $(A_m)$. Then $Q$ is automorphic.

Proposition 1.4.4. Let $Q$ be an automorphic loop and let $H ⊆ Q$. Then $C_Q(H) ≤ Q$. Furthermore, if $H ⊆ Q$ then $C_Q(H) ≤ Q$. In particular, the commutant $C(Q) ≤ Q$.

Proposition 1.4.5. ([4, Theorem 2.4]) Every automorphic loop is power-associative.

Proposition 1.4.6. [25] Let $Q$ be an automorphic loop. Then:

(i) $N_λ(Q) = N_μ(Q) ⊆ N_ν(Q)$.

(ii) Each nucleus is normal in $Q$.

1.5 Advanced results in automorphic loops

In this section we list main result on automorphic loops obtained in the last 10 years. We do not need most of these results, but they illustrate that certain aspects of the theory are well developed. The examples of dihedral-like automorphic loops should be useful in further developing the theory.

We start with results on commutative automorphic loops. In [21], [22] and [23] Jedlička, Kinyon and Vojtěchovský proved the following results.

Theorem 1.5.1. ([22, Theorem 5.1(Decomposition for Finite Commutative automorphic loops)]) A finite commutative automorphic loop is a direct product $A × B$ of a loop $A$ of order $2^k$ and of a loop $B$ of odd order.

However, the subloop $B$ of odd order does not necessarily decompose as a direct product of $p$–loops in commutative automorphic loops. See [7] for an example of order $pq$. 

15
Theorem 1.5.2. ([21, Theorem 1.1]) A commutative automorphic loop of order $p^k$, $p$ an odd prime, is centrally nilpotent.

Theorem 1.5.3. ([22, Theorem 3.12(Odd Order Theorem)]) A commutative automorphic loop of odd order is solvable, satisfies Lagrange’s theorem and Cauchy’s theorem.

Theorem 1.5.4. ([23, Proposition 5.1]) Commutative automorphic loops of order $p$, $2p$, $4p$, $p^2$, $2p^2$, and $4p^2$ ($p$ an odd prime) are groups.

They also showed that there is a commutative automorphic loop of order 8 that is not centrally nilpotent.

Later, Greer improved upon some of these results and showed in [15]:

Theorem 1.5.5. ([15, Theorem 6.7]) A commutative automorphic loop of odd order possesses Sylow $p$- and Hall $\pi$-subloops.

De Barros, Griskov and Vojtěchovský classified commutative automorphic loops of order $p^3$ up to isomorphism:

Theorem 1.5.6. [23] For every prime $p$ there are precisely 7 commutative automorphic loops of order $p^3$ up to isomorphism.

Finally, Kinyon, Grishkov and Nagy proved in [12]:

Theorem 1.5.7. [12] There are no finite simple nonassociative commutative automorphic loops.
Let us now give some theorems on general automorphic loops.

**Theorem 1.5.8.** ([6, Theorem 6.1(Csörgő)]) Automorphic loops of order $p^2$ ($p$ prime) are groups.

Jedlička, Kinyon and Vojtěchovský constructed automorphic loops of order $p^3$ ($p$ prime) with trivial center.

Johnson, Kinyon, Nagy and Vojtěchovský proved:

**Proposition 1.5.9.** ([24, Corollary 6.6]) Every automorphic loop has the antiautomorphic inverse property.

**Theorem 1.5.10.** ([24, Theorem 1.2]) There are no finite simple nonassociative automorphic loops of order less than 2500.

It is an open problem whether there are finite simple nonassociative automorphic loops.

Kinyon, Kunen, Phillips and Vojtěchovský proved:

**Theorem 1.5.11.** ([25, Theorem 6.6(Odd Order Theorem)]) Every automorphic loop of odd order is solvable, satisfies Lagrange’s theorem and Cauchy’s theorem.

In the same paper, they also constructed the family of dihedral-like automorphic loops $\text{Dih}(m, G, \alpha)$ for $m = 2$ and established some properties of these loops.
Chapter 2

Parameters that yield
automorphic loops

Much of the work described in this section is from my own paper [1] and includes some remarks from the joint work with a professor of mine, Vojtěchovský [2]. The goal of this chapter is to introduce the dihedral-like automorphic loop $\text{Dih}(m, G, \alpha)$, and to determine all parameters $m, G, \alpha$ which yield automorphic loops.

2.1 The multiplication formula

Let $m \geq 1$ be an integer, $(G, +)$ an abelian group, and $\alpha$ an automorphism of $G$. Let $Z_m = (\mathbb{Z}_m, \oplus)$ be the cyclic group of order $m$. Define multiplication on $Z_m \times G$ by

$$(i, u)(j, v) = (i \oplus j, (s_j u + v)\alpha^{ij}),$$

where $s_j = (-1)^j \mod m$. The resulting loop will be called a *dihedral-like loop*.

If $m = 1$, we obtain the direct product $Z_1 \times G \cong G$. We will therefore assume from now on that $m > 1$. 

18
We interpret the multiplication formula (2.1.1) in two ways. In the modular case, we reduce all exponents of $\alpha$ modulo $m$, and we denote the resulting loop by $\text{Dih}_{\text{mod}}(m, G, \alpha)$. In the integral case, we interpret all exponents of $\alpha$ as integers, we demand that $i, j$ are from $\{0, \ldots, m - 1\}$ to avoid ambiguity, and we denote the resulting loop by $\text{Dih}_{\text{int}}(m, G, \alpha)$.

An inspection of all cases shows that for $m = 2$ the two interpretations coincide. But, as the following example illustrates, the two cases might produce non-isomorphic loops in general.

**Example 2.1.1.** $Q_1 = \text{Dih}_{\text{int}}(5, \mathbb{Z}_4, \alpha)$ is not isomorphic to $Q_2 = \text{Dih}_{\text{mod}}(5, \mathbb{Z}_4, \alpha)$, where $\alpha$ is the unique nontrivial automorphism of $\mathbb{Z}_4$ (GAP calculation).

When we wish to speak about both cases at once, we simply use $\text{Dih}(m, G, \alpha)$ to mean $\text{Dih}_{\text{int}}(m, G, \alpha)$ or $\text{Dih}_{\text{mod}}(m, G, \alpha)$. As we shall see later, cf. Theorem 2.4.1, the loop $\text{Dih}_{\text{int}}(m, G, \alpha)$ is automorphic if and only if the corresponding loop $\text{Dih}_{\text{mod}}(m, G, \alpha)$ is automorphic, and in such a situation the two loops actually coincide. The notation $\text{Dih}(m, G, \alpha)$ is therefore safe for automorphic loops, no matter how the exponents of $\alpha$ are interpreted in the multiplication formula (2.1.1).

We will take advantage of the following observations:

- $s_i s_j = s_j s_i$ for every $i, j \in \mathbb{Z}_m$,
- $s_i s_j = s_{i+j} = s_{i \oplus j}$ if $m$ is even (but not necessarily when $m$ is odd),
- $s_i(s_j u) = (s_i s_j)u$ for every $i, j \in \mathbb{Z}_m, u \in G$, and we write $s_i s_j u$,
- $(s_i u) \alpha = s_i (u \alpha)$ for every $i \in \mathbb{Z}_m, u \in G$, and we write $s_i u \alpha$,
- $\alpha^i \alpha^j = \alpha^{i+j}$ and $(\alpha^i)^{-1} = \alpha^{-i}$ in the integral case (but not necessarily in the modular case).
For an abelian group \((G, +)\) denote by \(2G\) the subgroup \(2G = \{u + u; u \in G\}\). Note that if \(\alpha \in \text{Aut}(G)\) then the restriction \(\alpha|_{2G}\) of \(\alpha\) to \(2G\) is an automorphism of \(2G\).

**Lemma 2.1.2.** \(Q = \text{Dih}(m, G, \alpha)\) is a group iff \(\alpha = 1\) and \((2G = 0\) or \(m\) is even).

**Proof.** We have \((i, u)(j, v) \cdot (k, w) = (i, u) \cdot (j, v)(k, w)\) if and only if \((i \oplus j, (s_j u + v)\alpha^{ij})(k, w) = (i, u)(j \oplus k, (s_k v + w)\alpha^{jk})\) if and only if \((i \oplus j \oplus k, (s_k(s_j u + v)\alpha^{ij} + w)\alpha^{(i \oplus j)k}) = (i \oplus j \oplus k, (s_j \in k u + (s_k v + w)\alpha^{jk})\alpha^{i(j \oplus k)})\) if and only if \((s_k(s_j u + v)\alpha^{ij} + w)\alpha^{(i \oplus j)k} = (s_j \in k u + (s_k v + w)\alpha^{jk})\alpha^{i(j \oplus k)}\). With \(u = 0, k = 0\) and \(i = j = 1\), this reduces to \(v\alpha + w = (v + w)\alpha\), so \(\alpha = 1\) is necessary. Furthermore, if \(\alpha = 1\) then

\[
(s_k(s_j u + v)\alpha^{ij} + w)\alpha^{(i \oplus j)k} = (s_j \in k u + (s_k v + w)\alpha^{jk})\alpha^{i(j \oplus k)} \tag{2.1.2}
\]

reduces to \(s_k(s_j u + v) + w = s_j \in k u + (s_k v + w)\) so \(Q\) is a group iff

\[
s_k s_j u = s_j \in k u \tag{2.1.3}
\]

for every \(j, k \in \mathbb{Z}_m\) and every \(u \in G\).

If \(2G = 0\) then \(u = -u\) and (2.1.3) holds. If \(m\) is even then \(s_k s_j = s_j \in k\) and (2.1.3) holds again. Conversely, suppose that (2.1.3) holds. If \(m\) is even, we are done, so suppose that \(m\) is odd. With \(k = 1, j = m - 1\) the identity (2.1.3) yields \(-u = u\), or \(2G = 0\).

\[\square\]

### 2.2 Middle inner mappings

Recall that \(yT_x = x \setminus (yx)\).

**Lemma 2.2.1.** Let \(Q = \text{Dih}(m, G, \alpha)\) and \((i, u), (j, v) \in Q\). Then

\[
(j, v)T_{(i, u)} = (j, s_i v + (1 - s_j)u). \tag{2.2.1}
\]
In particular, with $\alpha = 1$ and $I_{(i,u)} = \{(i,u), (i,u)^{-1}\}$, we have:

(i) $(0,u)T_{(j,v)} \in I_{(0,u)}$ for every $u \in G$,

(ii) if $\exp(G) > 2$ then for every odd $i$ and every $u \in G$ there is $(j,v) \in Q$ such that $(i,u)T_{(j,v)} \not\in I_{(i,u)}$.

Proof. The following conditions are equivalent:

\[
(j,v)T_{(i,u)} = (k,w),
\]

\[
(j,v)(i,u) = (i,u)(k,w),
\]

\[
(j \oplus i, (s_i u + u)\alpha^{ij}) = (i \oplus k, (s_k u + w)\alpha^{ik}).
\]

We deduce $k = j$, and extend the chain of equivalences with

\[
(s_i u + u)\alpha^{ij} = (s_j u + w)\alpha^{ij},
\]

\[
s_i u + u = s_j u + w,
\]

\[
w = s_i u + (1 - s_j)u,
\]

as claimed. Note that $(i,u)^{-1} = (-i, -s_i u)$. For $i = 0$, we get $(0,u)T_{(j,v)} = (0, s_j u) \in I_{(0,u)}$.

Suppose that $i$ is odd, $\exp(G) > 2$ and let $v \in G$ be of order bigger than 2. We get $(i,u)T_{(0,v)} = (i, 2v + u)$, which is different from both $(i,u)$ and $(-i,u) = (-i, -s_i u) = (i,u)^{-1}$.

Lemma 2.2.2. Let $Q = \text{Dih}(m,G,\alpha)$ and $(i,u) \in Q$. Then $T_{(i,u)} \in \text{Aut}(Q)$ iff

\[
(1 - s_j \oplus k)u = (1 - s_j s_k)u\alpha^{jk}
\]

for every $j, k \in \mathbb{Z}_m$. 

21
Proof. We will use (2.2.1) without reference. We have

\[(j,v)(k,w)T_{(i,u)} = (j \oplus k, (s_kv + w)\alpha^{jk})T_{(i,u)}
= (j \oplus k, s_i(s_kv + w)\alpha^{jk} + (1 - s_j \oplus k)u)
= (j \oplus k, s_is_kv\alpha^{jk} + s_iw\alpha^{jk} + (1 - s_j \oplus k)u),\]

while

\[(j,v)T_{(i,u)} \cdot (k,w)T_{(i,u)} = (j, s_iv + (1 - s_j)u) \cdot (k, s_iw + (1 - s_k)u)
= (j \oplus k, [s_k(s_iv + (1 - s_j)u) + s_iw + (1 - s_k)u]\alpha^{jk})
= (j \oplus k, s ks_iv\alpha^{jk} + s_iw\alpha^{jk} + [(s_k - s_k s_j + 1 - s_k)u]\alpha^{jk})
= (j \oplus k, s ks_iv\alpha^{jk} + s_iw\alpha^{jk} + (1 - s_k s_j)u\alpha^{jk}),\]

so \(T_{(i,u)} \in \text{Aut}(Q)\) iff (2.2.2) holds for every \(j, k \in \mathbb{Z}_m\).

Let us call a loop \(Q\) satisfying \((A_m)\) a middle automorphic loop.

**Proposition 2.2.3.** Let \(Q = \text{Dih}(m, G, \alpha)\).

(i) If \(m = 2\) then \(Q\) is a middle automorphic loop.

(ii) If \(m > 2\) is odd then \(Q\) is a middle automorphic loop iff \(2G = 0\).

(iii) If \(m > 2\) is even then \(Q\) is a middle automorphic loop iff \(\alpha^2 | 2G = 1_{2G}\).

Proof. Consider \(T_{(i,u)}\). Suppose that \(m = 2\). A quick inspection of all cases \(j, k \in \{0,1\}\) shows that (2.2.2) always holds.

Suppose that \(m > 2\) is odd. With \(j = 2\) and \(k = m - 1\), condition (2.2.2) becomes \((1 - s_{2s(m-1)})u = (1 - s_{2s^m-1})u\alpha^{2(m-1)}\), or \(2u = 0\), so we certainly must have \(2G = 0\) for every \(T_{(i,u)}\) to be an automorphism. Conversely, when \(2G = 0\) then (2.2.2) reduces to \(0 = 0\).
Suppose that $m > 2$ is even. Then (2.2.2) becomes $(1 - s_j \oplus k)u = (1 - s_j \oplus k)u \alpha^{jk}$.

If (2.2.2) holds, we take $j = 2$, $k = 1$ to deduce $2u = (2u)\alpha^2$. Conversely, if $2u = (2u)\alpha^2$, we claim that (2.2.2) holds. Indeed, when $j \oplus k$ is even then we obtain $0 = 0$, so suppose that $j \oplus k$ is odd. Then one of $j$, $k$ is odd and the other is even, so both $jk$ and $(jk) \mod m$ are even. Therefore (2.2.2) becomes $2u = (2u)\alpha^{2\ell}$ for some integer $\ell$, which is a consequence of $2u = (2u)\alpha^2$.

\[ \square \]

### 2.3 Left inner mappings

Recall that $z_{L,x,y} = (yx) \setminus (y(xz))$.

**Lemma 2.3.1.** Let $Q = \text{Dih}(m, G, \alpha)$ and $(i, u), (j, v), (k, w) \in Q$. Then

\[ (k, w)L_{(j, v), (i, u)} = (k, s_j \oplus k)u \alpha^{i(j \oplus k)}(\alpha^{(i \oplus j)k})^{-1} + s_k v \alpha^j k \alpha^{i(j \oplus k)}(\alpha^{(i \oplus j)k})^{-1} + w \alpha^j k \alpha^{i(j \oplus k)}(\alpha^{(i \oplus j)k})^{-1} - s_k s_j u \alpha^{ij} - s_k v \alpha^{ij}. \]  

(2.3.1)

**Proof.** The following conditions are equivalent:

\[ (k, w)L_{(j, v), (i, u)} = (\ell, x), \]

\[ (i, u) \cdot (j, v)(k, w) = (i, u)(j, v) \cdot (\ell, x), \]

\[ (i, u)(j \oplus k, (s_k v + w)\alpha^{jk}) = (i \oplus j, (s_j u + v)\alpha^{ij})(\ell, x), \]

\[ (i \oplus j \oplus k, (s_j \oplus k u + (s_k v + w)\alpha^{jk})\alpha^{i(j \oplus k)}) = (i \oplus j \oplus \ell, (s_l (s_j u + v)\alpha^{ij} + x)\alpha^{(i \oplus j)\ell}). \]

We deduce that $\ell = k$ and the result follows upon solving for $x$ in the equation

\[ (s_j \oplus k u + (s_k v + w)\alpha^{jk})\alpha^{i(j \oplus k)} = (s_k (s_j u + v)\alpha^{ij} + x)\alpha^{(i \oplus j)k}. \]  

\[ \square \]
Lemma 2.3.2. Let $Q = \text{Dih}(m, G, \alpha)$ and $(i, u), (j, v) \in Q$. Then $L_{(j,v),(i,u)} \in \text{Aut}(Q)$ iff
\[
\begin{align*}
&\quad s_{\ell} s_{j} u_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk} + s_{\ell} s_{j} v_{\alpha} j^k (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk}
+ s_{\ell} w_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk} - s_{\ell} s_{k} s_{j} u_{\alpha} i^j \alpha^{jk}
+ s_{\ell} w_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk} - s_{\ell} s_{k} v_{\alpha} i^j \alpha^{jk}
+ x_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk} - s_{\ell} s_{j} u_{\alpha} i^j \alpha^{jk} - s_{\ell} w_{\alpha} i^j \alpha^{jk}
= s_{j \oplus k} w_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + s_{k \oplus \ell} v_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1}
+ s_{\ell} w_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + x_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} - s_{k \oplus \ell} s_{j} u_{\alpha} i^j - s_{k \oplus \ell} v_{\alpha} i^j
\end{align*}
\]
for every $k, \ell \in \mathbb{Z}_m$ and every $w, x \in G$.

Proof. We will use (2.3.1) without reference. We have
\[
(k, w)L_{(j,v),(i,u)} \cdot (\ell, x)L_{(j,v),(i,u)} = (k, s_{j \oplus k} u_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1}
+ s_{k} v_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + w_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} - s_{k} s_{j} u_{\alpha} i^j - s_{k} v_{\alpha} i^j)
\cdot (\ell, s_{j} u_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + s_{\ell} v_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + x_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1}
- s_{\ell} s_{j} u_{\alpha} i^j - s_{\ell} v_{\alpha} i^j) = (k \oplus \ell, [s_{\ell} s_{j} u_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1}
+ s_{\ell} s_{k} v_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + s_{\ell} w_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} - s_{\ell} s_{k} s_{j} u_{\alpha} i^j
- s_{\ell} s_{k} v_{\alpha} i^j + s_{\ell} s_{j} u_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} + s_{\ell} v_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1}
+ x_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} - s_{\ell} s_{j} u_{\alpha} i^j - s_{\ell} v_{\alpha} i^j] \alpha^{jk}) = (k \oplus \ell, s_{\ell} s_{j} u_{\alpha} i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk} + s_{\ell} s_{k} v_{\alpha} j^k i^j (j \oplus k) (\alpha^{(i \oplus j)k})^{-1} \alpha^{jk}
\end{align*}
\]
\]
+ s_ℓ w \alpha^{jk} \alpha^{i(j \oplus k)}(\alpha^{(i \oplus j)k})^{-1} \alpha^{k\ell} - s_\ell s_k s_j u \alpha^{ij} \alpha^{k\ell} - s_\ell s_k v \alpha^{ij} \alpha^{k\ell} \\
+ s_j \oplus \ell u \alpha^{i(j \oplus \ell)}(\alpha^{(i \oplus j)\ell})^{-1} \alpha^{k\ell} + s_\ell v \alpha^{\ell \alpha^{i(j \oplus \ell)}(\alpha^{(i \oplus j)\ell})^{-1} \alpha^{k\ell} \\
+ x \alpha^{\ell \alpha^{i(j \oplus \ell)}(\alpha^{(i \oplus j)\ell})^{-1} \alpha^{k\ell} - s_\ell s_j u \alpha^{ij} \alpha^{k\ell} - s_\ell v \alpha^{ij} \alpha^{k\ell}),

while

\begin{align*}
((k, w) \cdot (\ell, x)) L_{(j, v), (i, u)} &= (k \oplus \ell, (s_\ell w + x) \alpha^{k\ell}) L_{(j, v), (i, u)} = (k \oplus \ell,

s_{j \oplus (k \oplus \ell)} u \alpha^{i(j \oplus k \oplus \ell)}(\alpha^{(i \oplus j)(k \oplus \ell)})^{-1} + (s_\ell w + x) \alpha^{k\ell} \alpha^{j(k \oplus \ell)} \alpha^{i(j \oplus k \oplus \ell)}(\alpha^{(i \oplus j)(k \oplus \ell)})^{-1} \\
- s_{k \oplus \ell} u \alpha^{ij} - s_{k \oplus \ell} v \alpha^{ij}) = (k \oplus \ell, s_{j \oplus (k \oplus \ell)} u \alpha^{i(j \oplus k \oplus \ell)}(\alpha^{(i \oplus j)(k \oplus \ell)})^{-1} \\
+ s_\ell w \alpha^{k\ell} \alpha^{j(k \oplus \ell)} \alpha^{i(j \oplus k \oplus \ell)}(\alpha^{(i \oplus j)(k \oplus \ell)})^{-1} + x \alpha^{k\ell} \alpha^{j(k \oplus \ell)} \alpha^{i(j \oplus k \oplus \ell)}(\alpha^{(i \oplus j)(k \oplus \ell)})^{-1} \\
- s_{k \oplus \ell} u \alpha^{ij} - s_{k \oplus \ell} v \alpha^{ij})
\end{align*}

So $L_{(j, v), (i, u)} \in \text{Aut}(Q)$ iff (2.3.2) holds for every $i, j, k \in \mathbb{Z}_m$. 

Let us call a loop satisfying $(A_\ell)$ a \textit{left automorphic loop}. We deduce that $Q = \text{Dih}(m, G, \alpha)$ is a left automorphic loop iff (2.3.2) holds for every $i, j, k, \ell \in \mathbb{Z}_m$ and every $u, v, w, x \in G$. We show that this very complicated condition is equivalent to two comparatively simple conditions, which we then analyze separately.

First, setting $u = v = w = 0$ and letting $x$ range over $G$ in (2.3.2) yields the condition

$$\alpha^{\ell \alpha^{i(j \oplus \ell)}(\alpha^{(i \oplus j)\ell})^{-1} \alpha^{k\ell} = \alpha^{k\ell} \alpha^{j(k \oplus \ell)} \alpha^{i(j \oplus k \oplus \ell)}(\alpha^{(i \oplus j)(k \oplus \ell)})^{-1}. \tag{2.3.2}$$

With $\ell = 0$ this further simplifies to

$$\alpha^{ij} = \alpha^{jk} \alpha^{i(j \oplus k)}(\alpha^{(i \oplus j)k})^{-1},$$
which is equivalent to
\[ \alpha^{ij} \alpha^{(i\oplus j)k} = \alpha^{i(j \oplus k)} \alpha^{jk}. \] (2.3.3)

Suppose that (2.3.3) holds for every \( i, j, k \). Then the automorphisms at \( w \) in (2.3.2) agree since
\[
\begin{align*}
\alpha^{jk} \alpha^{i(j \oplus k)} & = \alpha^{ij} \alpha^{(i \oplus j)k} \alpha^{(i \oplus j)k}^{-1} = \alpha^{ij} \\
& = \alpha^{ij} \alpha^{i(j \oplus k)(k \oplus \ell)} \alpha^{(i \oplus j)(k \oplus \ell)}^{-1} \\
& = \alpha^{ij} \alpha^{i(k \oplus \ell) \alpha^{i(j \oplus k)(k \oplus \ell)}}. \\
\end{align*}
\]

Focusing on \( x \) in (2.3.2), the following conditions are equivalent:
\[
\begin{align*}
\alpha^{j\ell} \alpha^{i(j \oplus \ell)(k \oplus \ell)}^{-1} & = \alpha^{j(k \oplus \ell)} \alpha^{i(j \oplus k)(k \oplus \ell)}^{-1}, \\
\alpha^{j\ell} \alpha^{i(j \oplus \ell)(k \oplus \ell)} & = \alpha^{j(k \oplus \ell)} \alpha^{i(j \oplus k)(k \oplus \ell)}, \\
\alpha^{ij} \alpha^{(i \oplus j)(k \oplus \ell)} & = \alpha^{ij} \alpha^{(i \oplus j)(k \oplus \ell)}, \\
\end{align*}
\]

where we have used (2.3.3) twice in the last step. Since the last identity is trivially true, we see that (2.3.3) implies that the automorphisms at \( x \) in (2.3.2) agree, too. Let us now focus on \( v \) in (2.3.2). Using (2.3.3), the following conditions are

\[26\]
equivalent:
\[
\begin{align*}
& s_{t} s_{k} v \alpha^{j} k \alpha^{i} (i \oplus j)^{k} (\alpha^{i} (i \oplus j)^{k})^{-1} \alpha^{k \ell} - s_{t} s_{k} v \alpha^{i} j \alpha^{k k} + s_{t} v \alpha^{j} \ell \alpha^{i} (i \oplus j)^{\ell} (\alpha^{i} (i \oplus j)^{\ell})^{-1} \alpha^{k \ell} \\
& - s_{t} v \alpha^{i} j \alpha^{k k} = s_{k \oplus \ell} v \alpha^{j} (k \oplus j)^{k} \alpha^{i} (i \oplus j)^{k} (\alpha^{i} (i \oplus j)^{k})^{-1} - s_{k \oplus \ell} v \alpha^{i} j,
\end{align*}
\]

Upon canceling several \(\alpha^{t} \alpha^{-t}\) and the automorphism \(\alpha^{ij}\) present in all summands, we see that the above is equivalent to
\[
\begin{align*}
& s_{t} s_{k} v \alpha^{k \ell} - s_{t} s_{k} v \alpha^{k \ell} + s_{t} v \alpha^{k \ell} - s_{t} v \alpha^{k \ell} = s_{k \oplus \ell} v - s_{k \oplus \ell} v,
\end{align*}
\]
which is trivially true. Hence (2.3.3) implies that the automorphisms at \(v\) in (2.3.2) agree, too. Finally, we focus on \(u\) in (2.3.2). Note that the equality
\[
\alpha^{i (j \oplus \ell)} (\alpha^{i (i \oplus j) \ell})^{-1} = \alpha^{i j} (\alpha^{j \ell})^{-1}
\]
immediately follows from (2.3.3). Using this identity, the following conditions are equivalent:
\[
\begin{align*}
& s_{t} s_{j} s_{k} u \alpha^{i (j \oplus k)} (\alpha^{i (i \oplus j) k})^{-1} \alpha^{k \ell} - s_{t} s_{k} s_{j} u \alpha^{i j} \alpha^{k \ell} + s_{j \oplus \ell} u \alpha^{i j} \alpha^{i (i \oplus j) \ell} (\alpha^{i (i \oplus j) \ell})^{-1} \alpha^{k \ell} \\
& - s_{t} s_{j} u \alpha^{i j} \alpha^{k \ell} = s_{j \oplus \ell} s_{j} s_{k} u \alpha^{i j} \alpha^{k \ell} + s_{j \oplus \ell} u \alpha^{i j} (\alpha^{i \ell})^{-1} \alpha^{k \ell} \\
& - s_{t} s_{j} u \alpha^{i j} \alpha^{k \ell} = s_{j \oplus \ell} s_{j} u \alpha^{i j} (\alpha^{i \ell})^{-1} - s_{k \oplus \ell} s_{j} u \alpha^{i j}.
\end{align*}
\]
Upon canceling $\alpha^{ij}$ and rearranging, we obtain the identity

$$s_\ell s_j u (\alpha^{jk})^{-1} \alpha^{k\ell} + s_j \ell u (\alpha^{j\ell})^{-1} \alpha^{k\ell} + s_k \ell s_j u$$  \hspace{1cm} (2.3.4)

$$= s_\ell s_k s_j u \alpha^{k\ell} + s_\ell s_j u \alpha^{k\ell} + s_j \ell s_k u (\alpha^{j(k\ell)})^{-1}.$$

We have proved:

**Lemma 2.3.3.** Let $Q = \text{Dih}(m, G, \alpha)$. Then $Q$ is left automorphic iff (2.3.3) and (2.3.4) hold for every $i, j, k, \ell \in \mathbb{Z}_m$ and every $u \in G$.

Let us now analyze the condition (2.3.3), treating the integral and modular cases separately.

**Lemma 2.3.4.** Let $Q = \text{Dih}_{\text{int}}(m, G, \alpha)$. If $m = 2$ then (2.3.3) holds. If $m > 2$ then (2.3.3) holds iff $|\alpha|$ divides $m$.

**Proof.** Recall that we can use $\alpha^i \alpha^j = \alpha^{i+j}$ in this case. Hence we need to consider the condition

$$ij + (i \oplus j) k = i(j \oplus k) + jk.$$  \hspace{1cm} (2.3.5)

When $m = 2$ then (2.3.5) holds by a quick inspection of the cases, and thus (2.3.3) holds as well. Suppose that $m > 2$. With $i = j = 1$, $k = m - 1$ the condition (2.3.5) reduces to $1 + 2(m - 1) = 1 \cdot 0 + m - 1$, or $m = 0$. Thus if (2.3.3) holds then $\alpha^m = 1$. Conversely, if $\alpha^m = 1$, then (2.3.3) holds because (2.3.5) is valid modulo $m$. \qed

**Lemma 2.3.5.** Let $Q = \text{Dih}_{\text{mod}}(m, G, \alpha)$. If $m \leq 3$ then (2.3.3) holds. If $m > 3$ then (2.3.3) holds iff $|\alpha|$ divides $m$.

**Proof.** The case $m = 2$ is covered by Lemma 2.3.4. An inspection of all cases shows that (2.3.3) holds when $m = 3$, so suppose that $m > 3$. Note that (2.3.3) can be rewritten as

$$\alpha^{ij} \mod m \alpha^{(ik+jk)} \mod m = \alpha^{(ij+ik)} \mod m \alpha^{jk} \mod m.$$  \hspace{1cm} (2.3.6)
If $m$ is even, let $i = j = 1$, $k = m/2$ and note that $1 + m/2 < m$ (thanks to $m > 2$). Then (2.3.6) reduces to $\alpha^1\alpha^0 = \alpha^{1+m/2}\alpha^{m/2}$, which implies that $|\alpha|$ divides $m$. If $m$ is odd, let $i = j = 1$, $k = (m + 1)/2$ and note that $1 + (m + 1)/2 < m$ (thanks to $m > 3$). Then (2.3.6) reduces to $\alpha^1\alpha^1 = \alpha^{1+(m+1)/2}\alpha^{(m+1)/2}$, which again implies that $|\alpha|$ divides $m$.

Conversely, suppose that $|\alpha|$ divides $m$. Since $\alpha^\ell \mod m$ differs from $\alpha^\ell$ by $\alpha^{km}$ for some $k$, we are done by Lemma 2.3.4.

We will now add condition (2.3.4).

**Lemma 2.3.6.** Let $Q = \text{Dih}(m, G, \alpha)$. If (2.3.3) and (2.3.4) hold then $\alpha^{m-2} = 1$.

**Proof.** When $m = 2$, the conclusion is trivially true. Let us therefore assume that $m > 2$. With $k = 1$, $j = \ell = m - 1$, (2.3.4) becomes

$$s_{m-1}u(\alpha^{m-1})^{-1}\alpha^{m-1} + s_{m-2}u(\alpha^{(m-1)^2})^{-1}\alpha^{m-1} + s_{m-1}u = -u\alpha^{m-1} + u\alpha^{m-1} + s_{m-1}u,$$

or, equivalently,

$$u = u(\alpha^{(m-1)^2})^{-1}\alpha^{m-1},$$

using $s_{m-1} = -s_{m-2}$. Thus $\alpha^{m-1} = \alpha^{(m-1)^2} = \alpha^{m^2 - 2m + 1}$. In the modular case, we deduce $\alpha^{m-1} = \alpha^1$, i.e., $\alpha^{m-2} = 1$. In the integral case, we have $\alpha^m = 1$ by Lemma 2.3.4, and we again deduce $\alpha^{m-2} = 1$. \qed

**Lemma 2.3.7.** Let $Q = \text{Dih}(m, G, \alpha)$ be a left automorphic loop.

(i) If $m > 2$ is even then $\alpha^2 = 1$.

(ii) If $m > 2$ is odd then $\alpha = 1$. 29
Proof. By Lemma 2.3.3, $Q$ satisfies (2.3.3) and (2.3.4). If $m = 3$ then Lemma 2.3.6 implies $\alpha = 1$. If $m > 3$ then $|\alpha|$ divides both $m$ and $m - 2$, by Lemmas 2.3.4, 2.3.5 and 2.3.6, so $\alpha^2 = 1$. If $m > 3$ is odd, the condition $\alpha^2 = 1$ and the fact that $|\alpha|$ divides $m$ yield $\alpha = 1$.

\[\square\]

**Lemma 2.3.8.** Let $Q = \text{Dih}(m, G, \alpha)$.

(i) If $m = 2$ then (2.3.4) holds.

(ii) If $m$ is even and $\alpha^2 = 1$ then (2.3.4) holds.

(iii) If $m > 2$ is odd and $\alpha = 1$ then (2.3.4) implies $2G = 0$.

Proof. Suppose that $m = 2$. We can then reduce all subscripts modulo 2 in (2.3.4) and use $s_is_j = s_{i+j}$. Hence (2.3.4) becomes

\[
s_{\ell+j+k}u(\alpha^j\alpha^{-k})^{-1}\alpha^{k\ell} + s_{j+\ell}u(\alpha^{j\ell})^{-1}\alpha^{k\ell} + s_{k+\ell+j}u
\]

\[= s_{\ell+k+j}u\alpha^{k\ell} + s_{\ell+j}u\alpha^{k\ell} + s_{j+k+\ell}u(\alpha^{(j+k}\ell))^{-1}.\]

where all subscripts are reduced modulo 2. When $j$ is even, (2.3.7) becomes

\[s_{k+\ell}u\alpha^{k\ell} + s_{\ell}u\alpha^{k\ell} + s_{k+\ell}u = s_{k+\ell}u\alpha^{k\ell} + s_{\ell}u\alpha^{k\ell} + s_{k+\ell}u,\]

a valid identity. If $j$ is odd and $k$ is even, (2.3.7) becomes

\[-s_{\ell}u - s_{\ell}u\alpha^{-\ell} - s_{\ell}u = -s_{\ell}u - s_{\ell}u - s_{\ell}u\alpha^{-\ell},\]

clearly true. If $j$, $k$ are odd and $\ell$ is even, (2.3.7) becomes

\[u\alpha^{-1} - u = u - u + u\alpha^{-1},\]
again true. Finally, if \( j, k, \ell \) are odd, (2.3.7) becomes

\[-u + u - u = -u\alpha + u\alpha - u,\]

which holds trivially.

Suppose that \( m \) is even and \( \alpha^2 = 1 \). Then we can reduce all subscripts and superscripts in (2.3.4) modulo 2, and we proceed as in case (i).

For the rest of the proof let \( m > 2 \) be odd and suppose that \( \alpha = 1 \). Then (2.3.4) becomes

\[s_{\ell}s_{j\oplus k}u + s_{j\oplus \ell}u + s_{k\oplus \ell}s_{j}u = s_{\ell}s_{k}s_{j}u + s_{\ell}s_{j}u + s_{j\oplus k\oplus \ell}u.\]

With \( j = m - 1 \) and \( k = \ell = 1 \) we obtain \(-u + u + u = u - u - u\), or \( 2u = 0 \).

**Proposition 2.3.9.** Let \( Q = \text{Dih}(m, G, \alpha) \).

(i) If \( m = 2 \) then \( Q \) is left automorphic.

(ii) If \( m > 2 \) is even then \( Q \) is left automorphic iff \( \alpha^2 = 1 \).

(iii) If \( m > 2 \) is odd then \( Q \) is left automorphic iff \( \alpha = 1 \) and \( 2G = 0 \), in which case \( Q \) is a group.

**Proof.** We will use Lemma 2.3.3 without reference.

Suppose that \( m = 2 \). Then (2.3.3) holds by Lemmas 2.3.4 and 2.3.5, and (2.3.4) holds by Lemma 2.3.8.

Suppose that \( m > 2 \) is even. If \( Q \) is left automorphic then \( \alpha^2 = 1 \) by Lemma 2.3.7. Conversely, suppose that \( \alpha^2 = 1 \). Then (2.3.4) holds by Lemma 2.3.8. Since also \( \alpha^m = 1 \), (2.3.3) holds by Lemmas 2.3.4 and 2.3.5.

Finally, suppose that \( m > 2 \) is odd. If \( Q \) is left automorphic then \( \alpha = 1 \) by Lemma 2.3.7. By Lemma 2.3.8, \( 2G = 0 \). Conversely, suppose that \( \alpha = 1 \) and \( 2G = 0 \). Then \( Q \) is a group by Lemma 2.1.2, so also a left automorphic loop. \( \Box \)
2.4 Main result

The main result of this section is as follows:

**Theorem 2.4.1.** Let $m > 1$ be an integer, $G$ an abelian group, and $\alpha$ an automorphism of $G$. Let $Q = \text{Dih}(m, G, \alpha)$ be defined by (2.1.1).

(i) If $m = 2$ then $Q$ is automorphic.

(ii) If $m > 2$ is even then $Q$ is automorphic iff $\alpha^2 = 1$.

(iii) If $m > 2$ is odd then $Q$ is automorphic iff $\alpha = 1$ and $2G = 0$, in which case $Q$ is a group.

*Proof.* The claim follows from Propositions 2.2.3 and 2.3.9.

Since we are primarily interested in nonassociative loops, we make the following definition:

**Definition 2.4.2.** The loop $\text{Dih}(m, G, \alpha)$ with multiplication (2.1.1) is said to be a dihedral-like automorphic loop if $m = 2$ or ($m > 2$ is even and $\alpha^2 = 1$).

As indicated at the beginning of this section, we now observe that the two interpretations (integral and modular) of (2.1.1) coincide in the automorphic case. Indeed, if $m = 2$, we have already observed that the two interpretations coincide. If $m > 2$ is even and $\alpha^2 = 1$, we can reduce the exponent of $\alpha$ modulo 2, and the two interpretations again coincide.

Moreover, in the automorphic case it is safe to write $s_{i+j}$ instead of $s_{i\oplus j}$ and $s_is_j$, $\alpha^{i+j}$ instead of $\alpha^i\alpha^j$, and so on. However $\alpha^{i+j}$ can still differ from $\alpha^{i\oplus j}$ when $m = 2$ and $|\alpha| > 2$. 
2.5 Inner mappings in the automorphic case

We conclude with an explicit calculation of inner mappings in dihedral-like automorphic loops. Recall that \( zR_{x,y} = ((zx)y)/(xy) \).

**Lemma 2.5.1.** Let \( Q = \text{Dih}(m,G,\alpha) \) and \((i,u), (j,v), (k,w) \in Q\). Then

\[
(k,w)R_{(j,v),(i,u)} = (k, s_i s_j w \alpha^{jk} \alpha^{i(j\oplus k)} (\alpha^{i\oplus j}k)^{-1} + s_i s_j v \alpha^{jk} \alpha^{i(j\oplus k)} (\alpha^{i\oplus j}k)^{-1} + s_i s_j u \alpha^{ij} (\alpha^{i\oplus j}k)^{-1} - s_i s_j u \alpha^{ij}).
\] (2.5.1)

**Proof.** The following conditions are equivalent:

\[
(k,w)R_{(j,v),(i,u)} = (\ell, x),
\]

\[
(k,w)(j,v) \cdot (i,u) = (\ell, x) \cdot (j,v)(i,u),
\]

\[
(k \oplus j, (s_jw + v)\alpha^{kj})(i,u) = (\ell, x) \cdot (j \oplus i, (s_iv + u)\alpha^{ij}),
\]

\[
(k \oplus j \oplus i, [s_1s_j w \alpha^{kj} + s_i v \alpha^{kj} + u]\alpha^{(k\oplus j)i}) = (\ell \oplus j \oplus i, [s_j w x + s_i v \alpha^{ij} + u \alpha^{ij}]\alpha^{(j\oplus i)}).
\]

We deduce that \( \ell = k \), and the result follows upon solving for \( x \) in the equation

\[
(s_1s_j w \alpha^{kj} + s_i v \alpha^{kj} + u)\alpha^{(k\oplus j)i} = (s_i s_j x + s_i v \alpha^{ij} + u \alpha^{ij})\alpha^{k(j\oplus i)}.\]

\[\square\]

**Proposition 2.5.2.** Let \( Q = \text{Dih}(m,G,\alpha) \) be a dihedral-like automorphic loop. Then

\[
(k,w)T_{(i,u)} = (k, (1 - s_k)u + s_i w),
\]

\[
(k,w)R_{(j,v),(i,u)} = (k, w \alpha^{ij} + s_i + j u \alpha^{ij} (\alpha^{-jk} - 1)),
\]

\[
(k,w)L_{(j,v),(i,u)} = (k, w \alpha^{ij} + s_j + k u \alpha^{ij} (\alpha^{-jk} - 1)).
\]
for every \((i, u), (j, v), (k, w) \in Q\).

**Proof.** First note that the three types of generators must preserve the first coordinate. To calculate \(T_{(i,u)}\), note that the following conditions are equivalent:

\[
(k, w)T_{(i,u)} = (k, t),
\]
\[
(k, w)(i, u) = (i, u)(k, t),
\]
\[
(s_i w + u)\alpha^{ik} = (s_k u + t)\alpha^{ik},
\]
\[
s_i w + u = s_k u + t,
\]
\[
t = (1 - s_k)u + s_i w.
\]

For \(R_{(j,v),(i,u)}\), the following conditions are equivalent, using (2.3.3):

\[
(k, w)R_{(j,v),(i,u)} = (k, t),
\]
\[
(k, w)(j, v) \cdot (i, u) = (k, t) \cdot (j, v)(i, u),
\]
\[
(s_i (s_j w + v)\alpha^{jk} + u)\alpha^{i(j\oplus k)i} = (s_i + j t + (s_i v + u)\alpha^{ij})\alpha^{i(j\oplus k)k},
\]
\[
s_{i+j} w \alpha^{jk+(j\oplus k)i} + u \alpha^{i(j\oplus k)i} = s_{i+j} t \alpha^{i(j\oplus k)k} + u \alpha^{ij+(i\oplus j)k},
\]
\[
t = w \alpha^{ij} + s_{i+j} u \alpha^{ij-jk} - s_{i+j} u \alpha^{ij}.
\]
For $L_{(j,v),(i,u)}$, the following conditions are equivalent, using (2.3.3):

$$(k, w)L_{(j,v),(i,u)} = (k, t),$$

$$(i, u) \cdot (j, v)(k, w) = (i, u)(j, v) \cdot (k, t),$$

$$(s_{j+k}u + (s_kv + w)\alpha^{jk})\alpha^{i(j \oplus k)} = (s_k(s_ju + v)\alpha^{ij} + t)\alpha^{(i \oplus j)k},$$

$$s_{j+k}u\alpha^{i(j \oplus k)} + w\alpha^{jk+i(j \oplus k)} = s_{j+k}u\alpha^{ij+(i \oplus j)k} + t\alpha^{(i \oplus j)k},$$

$$t = w\alpha^{ij} + s_{j+k}u\alpha^{ij-jk} - s_{j+k}u\alpha^{ij}.$$ 

$\Box$

2.6 Groups among dihedral-like automorphic loops

Groups are easy to spot among dihedral-like automorphic loops. The next lemma is a special case of Lemma 2.1.2.

Lemma 2.6.1. Let $Q = \text{Dih}(m, G, \alpha)$ be a dihedral-like automorphic loop. Then $Q$ is a group if and only if $\alpha = 1$, and it is a commutative group if and only if $\alpha = 1$ and $\exp(G) \leq 2$.

Moreover, the group $\text{Dih}(m, G, 1)$ is a semidirect product $\mathbb{Z}_m \rtimes_{\varphi} G$ with multiplication

$$(i, u)(j, v) = (i + j, u\varphi_j + v),$$

where $\varphi : \mathbb{Z}_m \to \text{Aut}(G)$, $j \mapsto \varphi_j$ is given by $u\varphi_j = s_ju$.

Proof. We have $(i, u)(j, v) \cdot (k, w) = (i, u) \cdot (j, v)(k, w)$ if and only if

$$(s_k(s_ju + v)\alpha^{ij} + w)\alpha^{(i \oplus j)k} = (s_{j+k}u + (s_kv + w)\alpha^{jk})\alpha^{i(j \oplus k)},$$

35
which holds, by (2.3.3), if and only if

\[ s_{j+k} u \alpha^{i+j+(i\oplus j)k} = s_{j+k} u \alpha^{i(j\oplus k)} + w \alpha^{j+k+i(j\oplus k)}. \] (2.6.1)

With \( u = 0, k = 0 \) and \( i = j = 1 \), this reduces to \( w = w \alpha \), so \( \alpha = 1 \) is necessary. Conversely, if \( \alpha = 1 \), then (2.6.1) reduces to the trivial identity \( s_{j+k} u + w = s_{j+k} u + w \).

The rest is clear from (2.1.1). Note that the mapping \( \varphi \) is a homomorphism thanks to \( s_{j+k} = s_j s_k \).

We will call associative dihedral-like automorphic loops dihedral-like groups. The dihedral-like groups encompass the dihedral groups \( \text{Dih}(2, \mathbb{Z}_n, 1) = D_{2n} \), the generalized dihedral groups \( \text{Dih}(2, G, 1) = \text{Dih}(G) \), and certain generalized dicyclic groups \( \text{Dih}(4, G, 1) \).

It is easy to see that \( \text{Dih}(4, G, 1) \) is isomorphic to \( \text{Dic}(\mathbb{Z}_2 \times G, (1, 0)) \), by letting \( A = E \times G, y = (2, 0) \) and \( x = (1, 0) \). In particular, if \( n \) is odd, then \( \text{Dih}(4, \mathbb{Z}_n, 1) \) is isomorphic to \( \text{Dic}_{4n} \).

Dihedral-like groups contain additional classes of groups. For instance, \( \text{Dih}(6, \mathbb{Z}_5, 1) \) of order 30 is obviously not generalized dicyclic, and it is not isomorphic to the unique generalized dihedral group \( \text{Dih}(2, \mathbb{Z}_{15}, 1) \) of order 30.

On the other hand, not every (generalized) dicyclic group is found among dihedral-like groups, e.g. \( \text{Dic}_{16} \).
Chapter 3

Basic Properties

This chapter is based on my 2013 paper [1], but includes new work on the case $m = 2, \alpha^2 \neq 1$. It also adds versions of the Cauchy and Lagrange theorems for dihedral-like automorphic loops.

The object of this chapter is to study certain subloops of dihedral-like automorphic loops, such as the nuclei, the commutant, the center, the associator subloops and the derived subloops.

3.1 Nuclei

In this section, we describe nuclei of all dihedral-like automorphic loops. In general, all nuclei are subloops but are not necessarily normal. For loops in general there is no connection between the nuclei but in case of automorphic loops, the inclusions $N(Q) = N_\rho(Q) = N_\lambda(Q) \subseteq N_\mu(Q)$ were proved in [4]. The following proposition shows the structure of nuclei of all dihedral-like automorphic loops.
For an abelian group \( G \) and \( \alpha \in \text{Aut}(G) \), let \( G_2 = \{ u \in G : |u| \leq 2 \} \), let \( \text{Fix}(\alpha) = \{ u \in G : u = u\alpha \} \), and \( \text{Fix}(\alpha)_2 = G_2 \cap \text{Fix}(\alpha) \). \( E \) denotes the subgroup \( \langle 2 \rangle \) of \( \mathbb{Z}_m \). If \( m = 2 \), we interpret \( E \) as \( \langle 0 \rangle = 0 \).

**Lemma 3.1.1.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a dihedral-like automorphic loop. Then \( E \times G \) is an abelian subgroup of \( Q \).

**Proof.** On \( E \times G \), the multiplication formula becomes \((i, u)(j, v) = (i + j, (u + v)\alpha^{ij})\).

If \( \alpha^2 = 1 \) then \( \alpha^{ij} = 1 \) since \( i, j \in E \). If \( \alpha^2 \neq 1 \) then \( m = 2 \) and thus \( i, j = 0 \). So in either case we get \((i, u)(j, v) = (i + j, u + v)\). \( \square \)

**Proposition 3.1.2.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a dihedral-like automorphic loop. Then:

(i) If \( \alpha = 1 \) then \( N(Q) = N_\mu(Q) = N_\lambda(Q) = N_\rho(Q) = Q \).

(ii) If \( \alpha \neq 1 \) then \( N_\mu(Q) = E \times G \).

(iii) If \( \alpha \neq 1 \) then \( N(Q) = N_\lambda(Q) = N_\rho(Q) = E \times \text{Fix}(\alpha) \).

**Proof.** If \( \alpha = 1 \) then \( Q \) is a group by Lemma 2.6.1 and thus \( N(Q) = N_\mu(Q) = N_\lambda(Q) = N_\rho(Q) = Q \), proving (i).

Suppose that \( \alpha \neq 1 \). Note that in automorphic loops (that satisfy (2.3.3) by Lemma 2.3.3) the formula of Lemma 2.3.1 simplifies to

\[
(k, w)L_{(j,v),(i,u)} = (k, s_{j+k}u\alpha^{ij-jk} + s_k v\alpha^{ij} + w\alpha^{ij} - s_k s_j u\alpha^{ij} - s_k v\alpha^{ij})
\]

\[
= (k, s_{j+k}u\alpha^{ij-jk} - s_k s_j u\alpha^{ij} + w\alpha^{ij}). \tag{3.1.1}
\]

Since \((j, v) \in N_\mu(Q)\) iff \((k, w) = (k, w)L_{(j,v),(i,u)}\) for all \((i, u), (k, w)\), we conclude that \((j, v) \in N_\mu(Q)\) iff

\[
s_{j+k}u\alpha^{ij-jk} - s_k s_j u\alpha^{ij} + w\alpha^{ij} = w \tag{3.1.2}
\]
for all \((i, u), (k, w) \in Q\). With \(u = 0, i = 1\) this reduces to \(w \alpha^j = w\), so \(\alpha^j = 1\) is necessary. If \(m = 2\) then \(\alpha^j = 1\) and \(\alpha \neq 1\) this implies \(j = 0\) and if \(\alpha^2 = 1\) then \(\alpha^j = 1\) and \(\alpha \neq 1\) this implies \(j \in E\). Altogether, we obtain \(j \in E\). Conversely, if \(j \in E\) then (3.1.2) holds thanks to \(s_{j+k} = s_k s_j\) (since \(m\) is even). This proves (ii).

For (iii), suppose again that \(\alpha \neq 1\). Note that \((i, u) \in N_\lambda(Q)\) iff \((k, w) \in L(j, v), (i, u) = (k, w)\) for all \((j, v), (k, w) \in Q\). We deduce from (3.1.1) that \((i, u) \in N_\lambda(Q)\) iff (3.1.2) holds for all \((j, v), (k, w)\).

If \((i, u) \in N_\lambda(Q)\) then \(i \in E\) by the fact that \(N_\lambda(Q) \leq N_\mu(Q)\) in all automorphic loops, so (3.1.2) reduces to \(s_{j+k} u \alpha^{-j} - s_{j+k} u = 0\), i.e., \(u \alpha^{-j} = u\) for all \(j, k\). With \(j = k = 1\) we see that \(u \in \text{Fix}(\alpha)\). Conversely, if \(u \in \text{Fix}(\alpha)\) and \(i \in E\) then (3.1.2) clearly holds.

We recover [12, Proposition 9.1] as a special case of Proposition 3.1.2

### 3.2 Commutant

The next lemma characterizes the commutant \(C(Q)\) in a dihedral-like automorphic loop

**Lemma 3.2.1.** Let \(Q = \text{Dih}(m, G, \alpha)\) be a dihedral-like automorphic loop. Then:

(i) If \(\exp(G) \leq 2\) then \(C(Q) = Q\).

(ii) If \(\exp(G) > 2\) then \(C(Q) = E \times G_2\).

In either case, \(C(Q) \leq Q\).

**Proof.** By Lemma 2.2.1, \((i, u) \in C(Q)\) iff

\[
s_i v + (1 - s_j) u = v
\]  

(3.2.1)
holds for all \((j, v) \in Q\). If \(\exp(G) = 2\) then (3.2.1) holds. If \(\exp(G) > 2\) then (3.2.1) holds for all \((j, v)\) iff \(i \in E\) and \(u \in G_2\). For the rest of the proof we can assume that \(\exp(G) > 2\) and thus that \(C(Q) = E \times G_2\).

Thus, to show \(C(Q) \leq Q\), we only need to check that \(C(Q)\) is closed under multiplication and inverses, and this is clear from the multiplication formula.

If \((j, v) \in C(Q)\) then, by Lemma 2.2.1, \((j, v)T_{(i,u)} \in \{(j, \pm v)\} \in C(Q)\). If \((k, w) \in C(Q)\) then, by (3.1.1), \((k, w)L_{(j,v),(i,u)} = (k, sjua^{ij} - sju^{ij} + wa^{ij}) \in \{(k, w), (k, w\alpha)\} \in C(Q)\). The proof is similar for right inner mappings. Hence \(C(Q) \trianglelefteq Q\). \(\square\)

### 3.3 Center and central nilpotence

**Lemma 3.3.1.** Let \(Q = \text{Dih}(m, G, \alpha)\) be a dihedral-like automorphic loop. Then:

(i) If \(\exp(G) \leq 2\) and \(\alpha = 1\) then \(Z(Q) = Q\).

(ii) If \((\exp(G) \leq 2\) and \(\alpha \neq 1\)) or \(\exp(G) > 2\) then \(Z(Q) = E \times \text{Fix}(\alpha)_2\).

**Proof.** Suppose that \(\alpha = 1\). Then \(Q\) is a group by Lemma 2.6.1 and \(Z(Q) = C(Q)\). If \(\exp(G) \leq 2\) then \(Z(Q) = Q\) by Lemma 3.2.1. If \(\exp(G) > 2\) then \(C(Q) = E \times G_2 = E \times \text{Fix}(\alpha)_2\), by Lemma 3.2.1.

Now suppose that \(\alpha \neq 1\). If \(\exp(G) \leq 2\) then \(C(Q) = Q\) and \(Z(Q) = N(Q) = E \times \text{Fix}(\alpha)_2 = E \times \text{Fix}(\alpha)\) by Lemma 3.1.2 (iii). If \(\exp(G) > 2\) then \(Z(Q) = N(Q) \cap C(Q) = E \times \text{Fix}(\alpha)_2\) by Lemmas 3.1.2 (iii) and 3.2.1. \(\square\)

**Proposition 3.3.2.** Let \(Q\) be a dihedral-like automorphic loop. Then \(Q/Z(Q) \cong \text{Dih}(2, G/H, \beta)\), where \(H = \text{Fix}(\alpha)_2\) and \(\beta \in \text{Aut}(G/H)\) is defined by \((u + H)\beta = u\alpha + H\).
Proof. By Lemma 3.3.1, \( Z(Q) = E \times \text{Fix}(\alpha)_2 \). The mapping \( \beta \) is well-defined (if \( u + H = v + H \) then \( u - v \in H \subseteq \text{Fix}(\alpha) \), \( u\alpha - v\alpha = (u - v)\alpha = u - v \in H \), \( u\alpha + H = v\alpha + H \)) and obviously a surjective homomorphism. Since \( \alpha \) fixes elements of \( H \) pointwise, we have \( u + H \in \ker(\beta) \) iff \( u \in H \), so \( \beta \in \text{Aut}(G/H) \).

Consider \( f : Q \to \text{Dih}(2, G/H, \beta) \) defined by \( (i, u)f = (i \mod 2, u + H) \). Since

\[
(i, u)f(j, v)f = (i \mod 2, u + H)(j \mod 2, v + H)
\]

\[
= ((i + j) \mod 2, (s_j(u + H) + (v + H))\beta^{ij})
\]

\[
= ((i + j) \mod 2, (s_ju + v)\alpha^{ij} + H)
\]

\[
= (i + j, (s_ju + v)\alpha^{ij})f = ((i, u)(j, v))f,
\]

\( f \) is a homomorphism, obviously onto \( \text{Dih}(2, G/H, \beta) \). Finally, \( \ker(f) = E \times H = Z(Q) \).

\[\square\]

Corollary 3.3.3. Every dihedral-like automorphic loop \( \text{Dih}(m, G, \alpha) \) is a central extension of an elementary abelian 2-group by a dihedral-like automorphic loop of the form \( \text{Dih}(2, K, \beta) \) with \( K \) isomorphic to a factor of \( G \).

As an application of the results in this section, let us have a look at central nilpotency of dihedral-like automorphic loops. Let \( Q = \text{Dih}(m, G, \alpha) \) be a dihedral-like automorphic loop.

If \( \alpha = 1 \) and \( \exp(G) \leq 2 \) then \( Z(Q) = Q \) by Lemma 3.3.1. If \( \alpha = 1 \) and \( \exp(G) > 2 \) then \( Q \) is a group and \( Z(Q) = E \times \text{Fix}(\alpha)_2 = E \times G_2 \), and since

\[
(i, u)Z(Q) \cdot (j, v)Z(Q) = (i \oplus j, s_ju + v)(E \times G_2) = ((i + j) \mod 2, s_ju + v)Z(Q),
\]

we see that \( Q/Z(Q) \) is isomorphic to the generalized dihedral group \( \text{Dih}(2, G/G_2, 1) \).

Now suppose that \( \alpha \neq 1 \). Then \( Q/Z(Q) \cong \text{Dih}(2, G/H, \beta) \), where \( H = \text{Fix}(\alpha)_2 \). If \( H \neq 1 \), we proceed by induction, else \( G/H = G \), \( \beta = \alpha \) and \( Z(Q/Z(Q)) = 1 \).

Example 3.3.4. If \( G \) is an abelian group of odd order and \( \alpha \in \text{Aut}(G) \) then
Suppose that $|G| = 2^n$ and $\alpha \in \text{Aut}(G)$ is such that $\alpha \neq 1$. Since the involution $\alpha$ fixes the neutral element of $G$ and permutes the subgroup $G_2$ of even order (a divisor of $|G|$), we have $H = \text{Fix}(\alpha)_2 \neq 1$. Thus $Q/Z(Q) = \text{Dih}(2, G/H, \beta)$ and $2^\ell = |G/H| < |G|$. By induction, $Q$ is centrally nilpotent of class $\leq n$.

Finally suppose that $G = \mathbb{Z}_{2^n}$, $\alpha \in \text{Aut}(G)$. Whether $\alpha = 1$ or not, we have $Q/Z(Q) = \text{Dih}(2, G/H, \beta)$ for $H = \text{Fix}(\alpha)_2 = \{0, 2^{n-1}\}$ and some $\beta \in \text{Aut}(G/H)$, because $2^{n-1}$ is the unique element of order 2 in $G$. By induction, $Q$ has nilpotence class $n$.

### 3.4 Associators and the associator subloops

Recall that in a loop $Q$, the associator $[x, y, z]$ is defined as $(x \cdot yz) \setminus (xy \cdot z)$.

**Lemma 3.4.1.** Let $Q = \text{Dih}(m, G, \alpha)$ be a dihedral-like automorphic loop. Then

$$[(i, u), (j, v), (k, w)] = (0, (s_j v + u(id - \alpha^{-jk})\alpha^{ij} + w(1 - \alpha^{ij}))\alpha^{(i \oplus j)k}) \quad (3.4.1)$$

for $(i, u), (j, v), (k, w) \in Q$.

**Proof.** When $m$ is odd and $\alpha = 1$ then $Q$ is a group and (3.4.1) yields $[(i, u), (j, v), (k, w)] = 1$. The case when $m$ is even and $\alpha \neq 1$ follows by straightforward calculation, but since the identity (2.3.3) is involved, we give all the details: Let $(\ell, x) = [(i, u), (j, v), (k, w)]$ so

$$(i, u)(j, v) \cdot (k, w) = ((i, u) \cdot (j, v)(k, w))(\ell, x),$$

$$(i \oplus j, (s_j u + v)\alpha^{ij}) \cdot (k, w) = ((i, u) \cdot (j \oplus k, (s_k v + w)\alpha^{jk}))(\ell, x),$$

$$(i \oplus j \oplus k, [(s_k + j u + s_k v)\alpha^{ij} + w]\alpha^{(i \oplus j)k})$$
\[\begin{align*}
&= (i \oplus j \oplus k, [s_j \circ k u + s_k v \alpha^{jk} + w \alpha^{jk}] \alpha^{j(k \oplus k)})(\ell, x), \\
&(i \oplus j \oplus k, s_j \circ k u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{j(i \oplus j)k} + w \alpha^{(i \oplus j)k}) \\
&= (i \oplus j \oplus k, s_j \circ k u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{jk+i(j \oplus k)} + w \alpha^{jk+i(j \oplus k)})(\ell, x), \\
&(i \oplus j \oplus k, s_j \circ k u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{i(j \oplus j)k} + w \alpha^{(i \oplus j)k}) \\
&= (i \oplus j \oplus k, s_j \circ k u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{jk+i(j \oplus k)} + w \alpha^{jk+i(j \oplus k)})(\ell, x).
\end{align*}\]

Here we have used identity (2.3.3) in the last step. We obtain

\[\begin{align*}
(i \oplus j \oplus k, s_j \circ k u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{ij+(i \oplus j)k} + w \alpha^{(i \oplus j)k})
&= (i \oplus j \oplus k, [s_j \circ k u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{i(j \oplus j)k} + w \alpha^{j(k \oplus k)} + w \alpha^{j(i \oplus k)} + w \alpha^{j(k \oplus i)}])\alpha^{j(k \oplus k)}(\ell, x).
\end{align*}\]

We deduce \( \ell = 0 \), and can rewrite the above expression as

\[\begin{align*}
s_k + j u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{ij+(i \oplus j)k} + w \alpha^{(i \oplus j)k}
&= s_{j+k} u \alpha^{ij+(i \oplus j)k} + s_k v \alpha^{ij+(i \oplus j)k} + w \alpha^{ij+(i \oplus j)k} + x, \text{ i.e.} \\
x &= (s_{j+k} u (1 - \alpha^{-jk}) \alpha^{ij} + w (1 - \alpha^{ij})) \alpha^{(i \oplus j)k}.
\end{align*}\]

\[\Box\]

**Proposition 3.4.2.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a dihedral-like automorphic loop.

Then

\[A(Q) = \langle [x, y, z] x, y, z \in Q \rangle = \{ [x, y, z] | x, y, z \in Q \} = 0 \times (1 - \alpha) G.\]

In particular, \( A(Q) \) is an abelian group.
Proof. Here we check all choices of $i, j, k \pmod{2}$, using Lemma 3.4.1.

\[(0, u), (0, v), (0, w)] = (0, u(1 - 1) + w(1 - 1)) = (0, 0).
\[(0, u), (1, v), (0, w)] = (0, -u(1 - 1) + w(1 - 1)) = (0, 0).
\[(0, u), (0, v), (1, w)] = (0, -u(1 - 1) + w(1 - 1)) = (0, 0).
\[(0, u), (1, v), (1, w)] = (0, u(\alpha^{-1}) + w(1 - 1)) = (0, u(\alpha^{-1})\alpha) = (0, -u(1 - \alpha)).
\[(1, u), (0, v), (0, w)] = (0, u(1 - 1) + w(1 - 1)) = (0, 0).
\[(1, u), (1, v), (0, w)] = (0, -(u(1 - 1)\alpha + w(1 - 1))) = (0, w(1 - \alpha)).
\[(1, u), (0, v), (1, w)] = (0, -(u(1 - 1) + w(1 - 1))\alpha) = (0, 0).
\[(1, u), (1, v), (1, w)] = (0, u(\alpha)\alpha + w(1 - \alpha))
\quad = (0, u(\alpha^{-1})\alpha + w(1 - \alpha))
\quad = (0, (u - w)(1 - \alpha)).
\]

We can see that $[(i, u), (j, v), (k, w)] \in 0 \times (1 - \alpha)G$.

Second, $[(1, u), (1, v), (0, w)] = (0, (1 - \alpha)w)$. This shows that $\{[x, y, z]|x, y, z \in Q\} = 0 \times (1 - \alpha)G$. Next, we need to show $0 \times (1 - \alpha)G$ is subloop of $Q$. Let $(0, u(1 - \alpha))$ and $(0, v(1 - \alpha))$ be two elements of $0 \times (1 - \alpha)G$. Then

\[(0, u(1 - \alpha)) \cdot (0, v(1 - \alpha)) = (0, (u + v)(1 - \alpha)),
(0, u(1 - \alpha)) \setminus (0, v(1 - \alpha)) = (0, (v - u)(1 - \alpha)),
(0, u(1 - \alpha)) \cap (0, v(1 - \alpha)) = (0, (u - v)(1 - \alpha)),
\]

Finally, to show it is normal we use Lemmas 2.2.1 and 2.3.1 to obtain:
\[ (0, w(1 - \alpha))L_{(j,v),(i,u)} = (0, s_j u \alpha^{ij} + v \alpha^{ij} + w(1 - \alpha)\alpha^{ij} - s_j u \alpha^{ij} - v \alpha^{ij}) \]
\[ = (0, w(1 - \alpha)\alpha^{ij}), \]
\[ (0, w(1 - \alpha))T_{(i,u)} = (0, s_i w(1 - \alpha) + (1 - 1)u) \]
\[ = (0, s_i w(1 - \alpha)), \]
\[ (0, w(1 - \alpha))R_{(j,v),(i,u)} = (0, (w(1 - \alpha) + s_{-(i+j)} u(1 - 1))\alpha^{ij}) \]
\[ = (0, w(1 - \alpha)\alpha^{ij}). \]

\[ \square \]

### 3.5 Commutators and the derived subloops

Recall that in a loop \( Q \), the commutator \([x, y]\) is defined as \((yx)\setminus(xy)\).

**Lemma 3.5.1.** *In a dihedral-like automorphic loop \( Q = \text{Dih}(m, G, \alpha) \) we have*

\[
[(i, u), (j, v)] = (0, \left((s_j - 1)u + (1 - s_i)v\right)\alpha^{ij}) \tag{3.5.1}
\]

*for \((i, u), (j, v) \in Q.\)*

**Proof.** Let \((k, w) = [(i, u), (j, v)]\), so \((i, u)(j, v) = (j, v)(i, u). (k, w)\), hence,

\[
(i \oplus j, (s_j u + v)\alpha^{ij}) = (j \oplus i, (s_i v + u)\alpha^{ij}). (k, w) \iff
\]
\[
(i \oplus j, s_j u \alpha^{ij} + v \alpha^{ij}) = (i \oplus j \oplus k, (s_{k+i} v \alpha^{ij} + s_k u \alpha^{ij} + w)\alpha^{(i\oplus j)k}).
\]

We deduce \( k = 0 \), and can rewrite the above expression as \( w = (s_j - 1)u \alpha^{ij} + (1 - s_i)v \alpha^{ij}. \)

\[ \square \]
Proposition 3.5.2. Let \( Q = \text{Dih}(m, G, \alpha) \) be a dihedral-like automorphic loop. Then
\[
\langle [x, y] | x, y \in Q \rangle = \{ [x, y] | x, y \in Q \} = 0 \times 2G
\]
is a normal subloop of \( Q \).

Proof. Here we check all choices of \( i, j \pmod{2} \), using Lemma 3.5.1.

\[
[(0, u), (0, v)] = (0, 0).
\]
\[
[(0, u), (1, v)] = (0, -2u).
\]
\[
[(1, u), (0, v)] = (0, 2v).
\]
\[
[(1, u), (1, v)] = (0, -2(u - v)\alpha).
\]

We can see that \([ (i, u), (j, v) ] \in 0 \times 2G \).

Second, \([ (1, 0), (0, v) ] = (0, 2v) \). This shows that \( \{ [x, y] | x, y \in Q \} = 0 \times 2G \). It’s easy to see from (2.1.1) that \( 0 \times 2G \) is a subloop of \( Q \). Finally, to show that \( 0 \times 2G \) is normal in \( Q \), we calculate, using Lemmas 2.2.1 and 2.3.1 and an analog of Lemma 2.3.1:

\[
(0, 2w)L_{(j,v),(i,u)} = (0, 2w\alpha^{1+ij}),
\]
\[
(0, 2w)T_{(i,u)} = (0, 2sw),
\]
\[
(0, 2w)R_{(j,v),(i,u)} = (0, 2w\alpha^{ij}).
\]

\[\square\]

Proposition 3.5.3. Let \( Q = \text{Dih}(m, G, \alpha) \) be a dihedral-like automorphic loop. Then
\[
Q' = 0 \times ((1 - \alpha)G + 2G).
\]
In particular, $Q'$ is an abelian group.

Proof. The proof is immediate from Propositions 3.5.2 and 3.4.2, since $Q' = 0 \times (G(1 - \alpha) + 2G)$ is a normal subloop of $Q$. \hfill \square

Lemma 3.5.4. Let $Q = \text{Dih}(m, G, \alpha)$ be a dihedral-like automorphic loop. Then

(i) $A(Q)$ and $Q'$ are normal subloops of $N_{\mu}(Q)$.

(ii) $N_{\mu}(Q)/A(Q)$ is an abelian group.

Proof. We will give a proof based on the fact that associator subloop $A(Q)$ of $Q$ is the smallest normal subloop of $Q$ such that $Q/A(Q)$ is a group, $N_{\mu}(Q) \leq Q$ and $Q/N_{\mu}(Q) \cong \mathbb{Z}_2$, so this illustrates that $A(Q) \leq N_{\mu}(Q)$. Similarly, $Q' \leq N_{\mu}(Q)$, since $\mathbb{Z}_2$ is an abelian group.

(ii) $N_{\mu}(Q)/A(Q)$ is an abelian group because $A(Q) \leq N_{\mu}(Q)$, and $N_{\mu}(Q)$ is an abelian group. \hfill \square

### 3.6 Cauchy’s and Lagrange’s Theorem for dihedral-like automorphic loops

#### 3.6.1 Cauchy’s and Lagrange’s theorems

In this section, we will prove the Cauchy’s and Lagrange’s Theorems for dihedral-like automorphic loops. We start with Cauchy’s theorem, which is easy. For an abelian group $G$ and $E$ as (2), let $Q_E$ denote by $E \times G$.

**Theorem 3.6.1.** (Cauchy’s Theorem)

Let $Q = \text{Dih}(m, G, \alpha)$ be a finite dihedral-like automorphic loop. If a prime $p$ divides the order of $Q$, then $Q$ contains an element of order $p$.

Proof. Let $|Q|$ be a finite dihedral-like automorphic loop and suppose that $p$ is a prime number which divides $|Q|$ where $|Q| = |G| \cdot m$. It follows that $p$ divides $|G|$ or
$p$ divides $m$. Recall $\mathbb{Z}_m \cong \mathbb{Z}_m \times 0 \leq Q$, $G \cong 0 \times G \leq Q$. By Cauchy’s theorem for $\mathbb{Z}_m$ and $G$, either $\mathbb{Z}_m$ or $G$ contains an element of order $p$.

**Lemma 3.6.2.** Let $Q = \text{Dih}(m, G, \alpha)$ be a finite dihedral-like automorphic loop. If $S \leq Q$ then either $S \leq Q_E$ or $|S \cap Q_E| = |S \setminus Q_E|$.

**Proof.** Suppose $S \not\leq Q_E$. Then there exist $(i, u) \in S \setminus Q_E$. Consider $\phi = L_{(i, u)}$. Then $\phi(S \cap Q_E) \subseteq S \setminus Q_E$ and $\phi(S \setminus Q_E) \subseteq S \cap Q_E$ so $|S \cap Q_E| = |S \setminus Q_E|$.

**Theorem 3.6.3.** (Lagrange’s Theorem)

Let $Q = \text{Dih}(m, G, \alpha)$ be a finite dihedral-like automorphic loop. If $S \leq Q$ then the order of $S$ divides the order of $Q$.

**Proof.** Consider $S \leq Q$. If $S \leq Q_E$ then $S$ is a subgroup of the group $Q_E$, so $|S| \mid |Q_E|$ by Lagrange’s theorem for groups, therefore $|S| \mid |Q| = 2|Q_E|$. If $S \leq Q_E$, then by lemma 3.6.2 $|S \cap Q_E| = \frac{|S|}{2}$, $|S \cap Q_E| \mid |Q_E|$, so $|S| = 2|S \cap Q_E|$ divides $2|Q_E| = |Q|$.

**Corollary 3.6.4.** (Elementwise Lagrange)

Let $Q = \text{Dih}(m, G, \alpha)$ be a dihedral-like automorphic loop and let $a \in Q$. Then the order of $a$ divides the order of $Q$.

From [26] we know a loop $Q$ has a left coset decomposition modulo $H$ if any two left cosets of $H$ in $Q$ are either disjoint or coincide.

There exists a finite dihedral-like automorphic loop $Q$ with a subloop $H$ of order dividing that of $Q$ such that $Q$ does not have a left nor a right coset decomposition modulo $H$. For example: Let $Q = \text{Dih}(2, \mathbb{Z}_4, \alpha)$ where $\alpha$ be the unique nontrivial automorphism of $\mathbb{Z}_4$ and $H$ be a certain subloop of order 2.
Chapter 4

Automorphisms of dihedral-like automorphic loops

This chapter is based on a joint paper [2] with Petr Vojtěchovský. This paper focuses on proving that two finite dihedral-like automorphic loops $\text{Dih}(m, G, \alpha)$, $\text{Dih}(\overline{m}, \overline{G}, \overline{\alpha})$ are isomorphic if and only if $m = \overline{m}$, $G \cong \overline{G}$, and $\alpha$ is conjugate to $\overline{\alpha}$ in $\text{Aut}(G)$. Moreover, for a finite dihedral-like automorphic loop $Q$ we describe the structure of the automorphism group of $Q$ and its subgroup consisting of inner mappings of $Q$.

We do not know how to generalize these results to infinite dihedral-like automorphic loops.

Note that automorphism groups of generalized dihedral groups are well understood, cf. [28, p. 169]. If $\exp(G) \leq 2$, then $\text{Dih}(2, \mathbb{Z}_2^n, 1)$ is an elementary abelian 2-group whose automorphism group is the general linear group $GL_{n+1}(F_2)$. 

49
If \( \exp(G) > 2 \), then \( \text{Aut(Dih}(2, G, 1)) \) is the holomorph

\[ \text{Hol}(G) = \text{Aut}(G) \ltimes G, \quad (\alpha, u)(\beta, v) = (\alpha\beta, u\beta + v). \]

We will recover these results as special cases.

### 4.1 Squaring and conjugation

The squaring map \( x \mapsto x^2 \) and the conjugation map \( T_x \) are key to understanding the loops \( Q = \text{Dih}(m, G, \alpha) \). For \((i, u) \in Q\), let

\[(i, u)\chi = |\{(j, v) \in Q : (j, v)^2 = (i, u)\}|,

that is, \((i, u)\chi\) counts the number of times \((i, u)\) is a square in \(Q\).

**Lemma 4.1.1.** Let \( \text{Dih}(m, G, \alpha) \) be a finite dihedral-like automorphic loop. Then:

(i) \((i, u)\chi \leq 2|G|\) for every \(i, u\),

(ii) \((i, 0)\chi = 0\) for every odd \(i\) and every \(u\),

(iii) \((i, u)\chi \leq |G|\) whenever \(u \neq 0\),

(iv) \((i, 0)\chi = |G| + |G_2|\) when \(i\) is even and \(m/2\) is odd,

(v) \((2, 0)\chi = 2|G|\) when \(i\) is even and \(m/2\) is even.

**Proof.** Fix \((i, u) \in Q\). Note that \((j, v)(j, v) = (i, u)\) if and only if

\[2j \equiv i \pmod{m} \tag{4.1.1}\]

and

\[(s_jv + v)\alpha^{jj} = u. \tag{4.1.2}\]
Since \( \mathbb{Z}_m \to \mathbb{Z}_m, k \mapsto 2k \) is a homomorphism with kernel \( \{0, m/2\} \), the congruence (4.1.1) has either zero solutions or two solutions in \( \mathbb{Z}_m \), proving (i).

If \( i \) is odd then (4.1.1) never holds, proving (ii). For the rest of the proof we can assume that \( i \) is even, and we denote by \( \ell, \ell + m/2 \) the two solutions to (4.1.1).

Suppose that \( u \neq 0 \). If \( \ell \) is odd, then \((s_\ell v + v)\alpha^{\ell_\ell} = 0 \neq u \) for every \( v \in G \), so \((i, u)\chi \leq |G| \). Similarly if \( \ell + m/2 \) is odd, so we can assume that both \( \ell, \ell + m/2 \) are even. Then (4.1.2) becomes \( 2v = u \). The mapping \( G \to G, w \mapsto 2w \) is a homomorphism with kernel \( G_2 \). If \( G = G_2 \) then \( 2v = 0 \) for all \( v \in G \), so \((i, u)\chi = 0 \). Otherwise \( |G_2| \leq |G|/2 \) and \((i, u)\chi \leq 2|G_2| \leq |G| \). We have proved (iii) and can assume for the rest of the proof that \( u = 0 \).

Suppose that \( m/2 \) is odd. Then precisely one of \( \ell, \ell + m/2 \) is odd. Without loss of generality, assume that \( \ell \) is odd. With \( j = \ell \), (4.1.2) holds for every \( v \in G \). With \( j = \ell + m/2 \), (4.1.2) becomes \( 2v = 0 \), which holds if and only if \( v \in G_2 \), proving (iv).

Finally, suppose that \( m/2 \) is even. Then \( \ell = 1 \) and \( \ell + m/2 \) are both odd, so \((2, 0)\chi = 2|G| \).

\[ \square \]

### 4.2 The isomorphism problem

Suppose that \( \varphi : \text{Dih}(m, G, \alpha) \to \text{Dih}(\overline{m}, \overline{G}, \overline{\alpha}) \) is an isomorphism of finite dihedral-like groups. Let us first show that \( m = \overline{m} \) and \( G \cong \overline{G} \).

**Proposition 4.2.1.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a finite dihedral-like automorphic loop. Then the parameters \( m, G \) can be recovered from \( Q \).

**Proof.** Let \( s = \max\{(x)\chi : x \in Q\} \) and \( S = \{x \in Q; (x)\chi = s\} \). By Lemma 4.1.1, if \( m/2 \) is odd then \( s = |G| + |G_2| \) and \( S = E \times 0 \), while if \( m/2 \) is even then \( s = 2|G| \) and \( (2, 0) \in S \subseteq E \times 0 \). We therefore recover \( E \times 0 = \langle S \rangle \) from the known set \( S \). Since \( |E \times 0| = m/2 \), the parameter \( m \) is also uniquely determined.
Suppose that \( Q \) is a commutative group. Then \( \exp(G) \leq 2 \) by Lemma 2.6.1. Since \( |G| = |Q|/m \) is known, \( G \) is uniquely determined.

Now suppose that \( Q \) is a group that is not commutative. Then \( \exp(G) > 2 \) by Lemma 2.6.1. Let \( I = \{ x \in Q : xT_y \in I_x \text{ for every } y \in Q \} \). By Lemma 2.2.1, \( I \) contains \( 0 \times G \) and has empty intersection with \( (E + 1) \times G \). Hence \( \langle S \cup I \rangle = E \times G \leq Q \), so \( E \times G \) is determined. Since \( E \) is known, the Fundamental Theorem of Finite Abelian Groups implies that \( G \) is also known.

Finally, suppose that \( Q \) is nonassociative. Then \( N_\alpha(Q) = E \times G \) by Proposition 3.1.2(ii), and we determine \( G \) as above.

To resolve the isomorphism problem, Proposition 4.2.1 implies that it remains to study the situation when \( \varphi : \text{Dih}(m, G, \alpha) \to \text{Dih}(m, G, \beta) \) is an isomorphism of finite dihedral-like automorphic loops. By Lemma 4.1.1, we have

\[
(2,0) \varphi \in E \times 0. \tag{4.2.1}
\]

If \( \alpha \neq 1 \) or \( \exp(G) > 2 \), then Lemma 2.2.1 and Proposition 3.1.2(ii) imply that

\[
(0 \times G) \varphi \subseteq E \times G. \tag{4.2.2}
\]

Note that (4.2.2) can be violated when \( \alpha = 1 \) and \( \exp(G) = 2 \), for instance by some automorphisms of the generalized dihedral group \( \text{Dih}(2, \mathbb{Z}_2 \times \mathbb{Z}_2, 1) \).

**Proposition 4.2.2.** Suppose that \( \varphi : \text{Dih}(m, G, \alpha) \to \text{Dih}(m, G, \beta) \) is an isomorphism of finite dihedral-like automorphic loops such that either \( \alpha \neq 1 \) or \( \exp(G) > 2 \).

Then there are \( \gamma \in \text{Aut}(G) \) and \( z \in G \) such that

1. \( (E \times u) \varphi = E \times u\gamma \) for every \( u \in G \),
(ii) \(((E + 1) \times u)\varphi = (E + 1) \times (z + u\gamma)\) for every \(u \in G\),

(iii) \(\alpha \gamma = \beta\).

Proof. Denote the multiplication in \(\text{Dih}(m, G, \beta)\) by \(*\), and fix \(u \in G\). By (4.2.2), \((0, u)\varphi \in E \times v\) for some \(v \in G\). We claim that \((E \times u)\varphi = E \times v\). If \((2i, u)\varphi \in E \times v\) for some \(i\), then \((2i + 2, u)\varphi = ((2, 0)(2i, u))\varphi = (2, 0)\varphi * (2i, u)\varphi \in (E \times 0) * (E \times v) \subseteq E \times v\), where we have used (4.2.1), and where the last inclusion follows from (2.1.1).

Hence \((E \times u)\varphi \subseteq E \times v\), and the equality holds because \(E\) is finite and \(\varphi\) is one-to-one.

We can therefore define \(\gamma : G \to G\) by \((E \times u)\varphi = E \times u\gamma\). Since \(\varphi\) is one-to-one, \(\gamma\) is one-to-one. Due to finiteness of \(G\), \(\gamma\) is also onto \(G\). Moreover, \(((0, u)(0, v))\varphi = (0, u + v)\varphi \in E \times (u + v)\gamma\) and \((0, u)\varphi * (0, v)\varphi \in (E \times u\gamma) * (E \times v\gamma) \subseteq E \times (u\gamma + v\gamma)\) show that \(\gamma\) is a homomorphism, proving (i).

We have seen that \((E \times G)\varphi = E \times G\), and therefore also \(((E + 1) \times G)\varphi = (E + 1) \times G\). Let \(z \in G\) be such that \((1, 0)\varphi \in (E + 1) \times z\). Since \((E + 1) \times u = (1, 0)(E \times u)\), we have \(((E + 1) \times u)\varphi = (1, 0)\varphi * (E \times u)\varphi \in ((E + 1) \times z) * (E \times u\gamma) \subseteq (E + 1) \times (z + u\gamma)\), proving (ii).

Finally, we have \(((1, 0)(1, u))\varphi = (2, u\alpha)\varphi \in E \times u\alpha\gamma\) and \((1, 0)\varphi * (1, u)\varphi \in ((E + 1) \times z) * ((E + 1) \times (z + u\gamma)) \subseteq E \times (z + u\gamma)\beta = E \times u\gamma\beta\) for every \(u \in G\). Hence \(\alpha \gamma = \gamma \beta\), proving (iii).

\[\square\]

**Theorem 4.2.3.** Two finite dihedral-like automorphic loops \(\text{Dih}(m, G, \alpha)\) and \(\text{Dih}(\overline{m}, \overline{G}, \overline{\alpha})\) are isomorphic if and only if \(m = \overline{m}\), \(G \cong \overline{G}\) and \(\alpha\) is conjugate to \(\overline{\alpha}\) in \(\text{Aut}(G)\).

Proof. By Proposition 4.2.1, we can assume that \(m = \overline{m}\) and \(G \cong \overline{G}\). Let \((Q, \cdot) = \text{Dih}(m, G, \alpha)\) and \((\overline{Q}, \ast) = \text{Dih}(\overline{m}, \overline{G}, \overline{\alpha})\).

Suppose that \(\varphi : Q \to \overline{Q}\) is an isomorphism. If \(\alpha = 1\), then \(Q\) is a group by Lemma 2.6.1, hence \(\overline{Q}\) is a group, hence \(\overline{\alpha} = 1\) by Lemma 2.6.1, and so \(\alpha, \overline{\alpha}\) are trivially conjugate in \(\text{Aut}(G)\). We can therefore assume that \(\alpha \neq 1 \neq \overline{\alpha}\). Then \(Q\),
\(Q\) are nonassociative by Lemma 2.6.1, so Proposition 4.2.2 implies \(α^γ = \bar{α}\) for some \(γ \in \text{Aut}(G)\).

Conversely, suppose that \(α^γ = \bar{α}\) for some \(γ \in \text{Aut}(G)\). Define a bijection \(ϕ : Q \to \bar{Q}\) by \((i, u)ϕ = (i, uγ)\). Then \(((i, u)(j, v))ϕ = (i + j, (s_ju + v)α^{ij})ϕ = (i + j, (s_ju + v)α^{ij}γ)\), while \((i, u)ϕ * (j, v)ϕ = (i, uγ)(j, vγ) = (i + j, (s_juγ + vγ)\bar{α}^{ij}) = (i + j, (s_ju + v)γ\bar{α}^{ij})\). Since \(α^{ij}γ = γ\bar{α}^{ij}\) holds for every \(i, j \in \mathbb{Z}_m\) (due to the fact that either \(m = 2\) or \(α^2 = 1 = \bar{α}^2\)), we see that \(ϕ\) is a homomorphism.

\[\square\]

We recover [25, Corollary 9.4] as a special case of Theorem 4.2.3, using the fact that \(\text{Aut}(\mathbb{Z}_n)\) is a commutative group:

**Corollary 4.2.4.** The dihedral-like automorphic loops \(\text{Dih}(2, \mathbb{Z}_n, α)\), \(\text{Dih}(2, \mathbb{Z}_n, β)\) are isomorphic if and only if \(α = β\).

### 4.3 All isomorphisms

In this section we refine Proposition 4.2.2 and describe all isomorphisms between finite dihedral-like automorphic loops, except for the case when both \(α = 1\) and \(\exp(G) \leq 2\). In the next section we deal with the special case of automorphisms.

Given two finite dihedral-like automorphic loops \(\text{Dih}(m, G, α)\) and \(\text{Dih}(m, G, β)\), let

\[\text{Iso}(m, G, α, β)\]

be the (possibly empty) set of all isomorphisms \(\text{Dih}(m, G, α) \to \text{Dih}(m, G, β)\). We will show that there is a one-to-one correspondence between \(\text{Iso}(m, G, α, β)\) and the parameter set

\[\text{Par}(m, G, α, β)\]
consisting of all quadruples

\((\gamma, z, c, h)\)

such that:

- \(\gamma \in \text{Aut}(G)\) satisfies \(\alpha^{\gamma} = \beta\),
- \(z \in G\),
- \(c \in \mathbb{Z}_m\) is odd and \(\gcd(c, m/2) = 1\),
- \(h\) is a homomorphism \(G \to \langle m/2 \rangle\) that is trivial if \(m/2\) is odd, and that satisfies \(\alpha h = h\) if \(m/2\) is even.

**Remark 4.3.1.** Let us observe the following facts about the parameters:

Let \(\phi\) be the Euler function, that is, \(n\phi = |\{k : 1 \leq k \leq n, \gcd(k, n) = 1\}|\). We claim that there are \((m/2)\phi\) choices for \(c\) when \(m/2\) is odd, and \(2 \cdot (m/2)\phi\) choices for \(c\) when \(m/2\) is even. Indeed, there are \((m/2)\phi\) integers \(1 \leq k \leq m/2\) such that \(\gcd(k, m/2) = 1\), and we have \(\gcd(k, m/2) = \gcd(k + m/2, m/2)\). If \(m/2\) is even, then all such \(k\) are necessarily odd, \(k + m/2\) is also odd, and so there are \(2 \cdot (m/2)\phi\) choices for \(c\). If \(m/2\) is odd, then precisely one of \(k\) and \(k + m/2\) is odd, and we therefore find precisely \((m/2)\phi\) choices for \(c\).

If \(h : G \to \langle m/2 \rangle\) is a homomorphism, then \(K = \ker(h)\) is a subgroup of \(G\) of index at most 2. The condition \(\alpha h = h\) then guarantees that \(K\alpha = K\). Conversely, if \(K \leq G\) is of index at most two and such that \(K\alpha = K\), then \(h : G \to \langle m/2 \rangle\) defined by

\[
uh = \begin{cases} 
0, & \text{if } u \in K, \\
m/2, & \text{if } u \in G \setminus K 
\end{cases}
\]

is a homomorphism satisfying \(\alpha h = h\). We can therefore count the homomorphisms \(h\) by counting \(\alpha\)-invariant subgroups of index at most 2 in \(G\).
To facilitate the purported correspondence, define

\[ \Psi : \text{Iso}(m, G, \alpha, \beta) \to \text{Par}(m, G, \alpha, \beta) \]

by \( \varphi \Psi = (\gamma, z, c, h) \), where

\[ (0, u) \varphi = (uh, u\gamma), \quad (1, 0) \varphi = (c, z), \]

and, conversely,

\[ \Phi : \text{Par}(m, G, \alpha, \beta) \to \text{Iso}(m, G, \alpha, \beta) \]

by \( (\gamma, z, c, h) \Phi = \varphi \), where

\[ (i, u) \varphi = (ic + uh, (i \mod 2)z + u\gamma). \quad (4.3.1) \]

**Proposition 4.3.2.** Let \( \text{Dih}(m, G, \alpha) \), \( \text{Dih}(m, G, \beta) \) be finite dihedral-like automorphic loops such that either \( \alpha \neq 1 \) or \( \exp(G) > 2 \). Then \( \Psi : \text{Iso}(m, G, \alpha, \beta) \to \text{Par}(m, G, \alpha, \beta) \) and \( \Phi : \text{Par}(m, G, \alpha, \beta) \to \text{Iso}(m, G, \alpha, \beta) \) are mutually inverse bijections.

**Proof.** Throughout the proof we write \( \bar{i} \) instead of \( i \mod 2 \). Let \( (Q_\alpha, \cdot) = \text{Dih}(m, G, \alpha) \), \( (Q_\beta, \ast) = \text{Dih}(m, G, \beta) \), and suppose that \( \varphi : Q_\alpha \to Q_\beta \) is an isomorphism. By Proposition 4.2.2, there are \( \gamma \in \text{Aut}(G) \), \( z \in G \), \( c \in E + 1 \) and \( h : G \to E \) such that \( (0, u) \varphi = (uh, u\gamma) \) and \( (1, 0) \varphi = (c, z) \). Now, if for some \( i \in \mathbb{Z}_m \) we have \( (i, 0) \varphi = (ic, \bar{i}z) \), then

\[ (i + 1, 0) \varphi = (i, 0) \varphi \ast (1, 0) \varphi = (ic, \bar{i}z) \ast (c, z) = ((i + 1)c, (\bar{i}z + z)\beta^{icc}) \]

because \( c \) is odd. When \( i \) is odd, the second coordinate becomes \( (\bar{i}z + z)\beta^{icc} = 0 = i + \bar{1}z \), while if \( i \) is even, it becomes \( z = \bar{i} + \bar{1}z \). By induction, \( (i, 0) \varphi = (ic, \bar{i}z) \) for
every $i \in \mathbb{Z}_m$, and we have

$$(i, u)\varphi = (i, 0)\varphi \ast (0, u)\varphi = (ic, \bar{iz}) \ast (uh, u\gamma) = (ic + uh, \bar{iz} + u\gamma),$$

since $uh$ is even. We have recovered the formula (4.3.1).

Since $\varphi$ is an isomorphism, we see from $(2i, 0)\varphi = (2ic, 0)$ that $\{2ic : i \in \mathbb{Z}_m\} = E$, so $\gcd(2c, m) = 2$, and $\gcd(c, m/2) = 1$. Since $((0, u)(0, v))\varphi = (0, u + v)\varphi = ((u + v)h, (u + v)\gamma)$ and $(0, u)\varphi \ast (0, v)\varphi = (uh, u\gamma) \ast (vh, v\gamma) = (uh + vh, u\gamma + v\gamma)$, $h$ is a homomorphism $G \to E$. Moreover, $((0, u)(1, 0))\varphi = (1, -u)\varphi = (c - uh, z - u\gamma)$ and $(0, u)\varphi \ast (1, 0)\varphi = (uh, u\gamma) \ast (c, z) = (c + uh, -u\gamma + z)$ show that $2uh = 0$ for every $u$, and therefore $h$ is also a homomorphism $G \to \langle m/2 \rangle$. If $m/2$ is odd then $E \cap \langle m/2 \rangle = 0$, so $h$ is trivial. If $m/2$ is even, we further calculate $((1, 0)(1, u))\varphi = (2, u\alpha)\varphi \in (2c + u\alpha h) \times G$ and $(1, 0)\varphi \ast (1, u)\varphi = (c, z) \ast (c + uh, z + v\gamma) \in (2c + uh) \times G$, so $\alpha h = h$. This means that $(\gamma, z, h, c) \in \text{Par}(m, G, \alpha, \beta)$, and we have proved along the way that $\Psi\Phi = 1$.

Conversely, let $(\gamma, z, c, h) \in \text{Par}(m, G, \alpha, \beta)$ be given, and let $\varphi = (\gamma, z, c, h)\Phi$. It is easy to see that $\varphi$ is a bijection, and we proceed to prove that $\varphi$ is a homomorphism. We have

$$((i, u)(j, v))\varphi = (i + j, (s_j u + v)\alpha^{ij})\varphi$$

$$= ((i + j)c + (s_j + v)\alpha^{ij}h, i + jz + (s_j u + v)\alpha^{ij}\gamma),$$

and

$$(i, u)\varphi \ast (j, v)\varphi = (ic + uh, \bar{iz} + u\gamma) \ast (jc + vh, \bar{iz} + v\gamma)$$

$$= ((i + j)c + (u + v)h, (s_jc + v)(\bar{iz} + u\gamma) + jz + v\gamma)\beta^{(ic + uh)(jc + vh)}.$$ 

Since $\alpha h = h$ and $h : G \to \langle m/2 \rangle$, we see that $(s_j u + v)\alpha^{ij} h = (s_j u + v)h = (u + v)h$. 57
Since \( uh, vh \in E, c \in E + 1 \) and either \( m = 2 \) or \( \beta^2 = 1 \), we have \( \beta^{(ic+uh)(jc+vh)} = \beta^{ij} \). Using \( vh \in E \) and \( c \in E + 1 \), we get \( s_{jc+vh} = s_j \). It therefore remains to show that
\[
\overline{i + jz} + (s_ju + v)\alpha^{ij}\gamma = (s_j(\overline{iz} + u\gamma) + \overline{jz} + v\gamma)\beta^{ij}.
\]

But \( \alpha^\gamma = \beta \), so \( \alpha^{ij}\gamma = \gamma\beta^{ij} \) for all \( i, j \), and we need to show
\[
\overline{i + jz} = (s_j\overline{iz} + \overline{jz})\beta^{ij}.
\]

When \( j \) is even, this reduces to the trivial identity \( \overline{iz} = \overline{iz} \). When \( j \) is odd, we need to show
\[
\overline{i + jz} = (-\overline{iz} + z)\beta^i.
\]
When \( i \) is even, we get \( z = z \). When \( i \) is odd, we get \( 0 = (-z + z)\beta^i \).

Hence \( \varphi \) is an isomorphism. From (4.3.1) we get \( (0, u)\varphi = (uh, u\gamma) \) and \( (1, 0)\varphi = (c, z) \), proving \( \Phi \Psi = 1 \). \( \square \)

**Example 4.3.3.** Let \( m = 12 \), \( G = \mathbb{Z}_4 \), let \( \alpha = \beta \) be the unique nontrivial automorphism of \( G \), and let \( Q = \text{Dih}(m, G, \alpha) \). Then \( \text{Iso}(m, G, \alpha, \beta) = \text{Aut}(Q) \). There are 2 choices for \( \gamma \) (since \( \text{Aut}(G) \) is commutative), 4 choices for \( z \in G \), \( 2 \cdot (m/2)\phi = 4 \) choices for \( c \), and 2 choices for \( h \), corresponding to the subgroups \( K = G \) and \( K = \{0, 2\} \). Altogether, \( |\text{Aut}(Q)| = |\text{Par}(m, G, \alpha, \beta)| = 64 \).

**Example 4.3.4.** Let \( m = 6 \), \( u = (1, 2), v = (3, 4, 5, 6) \), \( G = \langle u, v \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \), let \( \alpha \in \text{Aut}(G) \) be determined by \( u\alpha = uv^2 \), \( v\alpha = v \), and \( \beta \in \text{Aut}(G) \) by \( u\beta = uv^2 \), \( v\beta = v^3 \). Note that \( \text{Aut}(G) \cong \text{Dih}(2, \mathbb{Z}_4, 1) \). Let us calculate \( |\text{Par}(m, G, \alpha, \beta)| \). There are 4 choices for \( \gamma \in \text{Aut}(G) \) such that \( \alpha^\gamma = \beta \), 8 choices for \( z \in G \), \( (m/2)\phi = 2 \) choices for \( c \), and 1 choice for \( h \) since \( m/2 \) is odd. Altogether, \( |\text{Iso}(m, G, \alpha, \beta)| = |\text{Par}(m, G, \alpha, \beta)| = 64 \).
4.4 Automorphism groups

In this section we describe automorphism groups of all finite dihedral-like automorphic loops.

**Remark 4.4.1.** The only finite dihedral-like automorphic loops not covered by Proposition 4.3.2 are those loops $Q = \text{Dih}(m, G, \alpha)$ with $\alpha = 1$ and $G$ a finite abelian group of exponent at most two. A direct inspection of (2.1.1) shows that then $Q = \mathbb{Z}_m \times G = \mathbb{Z}_m \times \mathbb{Z}_2^t$ for some $t$. Writing $m = r2^s$ with $r$ odd yields $Q = \mathbb{Z}_r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$. The special case $m = 2$ yields $Q = \mathbb{Z}_2^{t+1}$, whose automorphism group is the general linear group over $GF(2)$ and dimension $t+1$, as we have already mentioned. In general, the automorphism group is isomorphic to $\text{Aut}(\mathbb{Z}_r) \times \text{Aut}(\mathbb{Z}_2^s \times \mathbb{Z}_2^t) \cong \mathbb{Z}_r^* \times \text{Aut}(\mathbb{Z}_2^s \times \mathbb{Z}_2^t)$, and we refer the reader to [17] for more details.

For an abelian group $G$ and an automorphism $\alpha$ of $G$ let

$$\text{Inv}_2(G, \alpha) = \{K \leq G : [G : K] \leq 2, K\alpha = K\}$$

and let

$$C_{\text{Aut}(G)}(\alpha) = \{\gamma \in \text{Aut}(G) : \alpha\gamma = \gamma\alpha\}$$

be the centralizer of $\alpha$ in $\text{Aut}(G)$.

**Proposition 4.4.2.** Let $\text{Dih}(m, G, \alpha)$ be a finite dihedral-like automorphic loop such that either $\alpha \neq 1$ or $\exp(G) > 2$. Then

$$|\text{Aut}(\text{Dih}(m, G, \alpha))| = \begin{cases} |C_{\text{Aut}(G)}(\alpha)| \cdot |G| \cdot (m/2)\phi, & \text{if } m/2 \text{ is odd,} \\ |C_{\text{Aut}(G)}(\alpha)| \cdot |G| \cdot 2 \cdot (m/2)\phi \cdot |\text{Inv}_2(G, \alpha)|, & \text{if } m/2 \text{ is even.} \end{cases}$$

**Proof.** This follows from Proposition 4.3.2, Remark 4.3.1, and the fact that $\alpha^\gamma = \alpha$ if and only if $\gamma \in C_{\text{Aut}(G)}(\alpha)$. \qed
Let us write
\[ \text{Par}(m, G, \alpha) = \text{Par}(m, G, \alpha, \alpha). \]

Proposition 4.3.2 allows us to describe the structure of \( \text{Aut}(\text{Dih}(m, G, \alpha)) \) by working out the multiplication formula on \( \text{Par}(m, G, \alpha) \).

**Theorem 4.4.3.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a finite dihedral-like automorphic loop such that either \( \alpha \neq 1 \) or \( \exp(G) > 2 \). Then \( \text{Aut}(Q) \) is isomorphic to \( (\text{Par}(m, G, \alpha), \circ) \), where

\[
(\gamma_0, z_0, c_0, h_0) \circ (\gamma_1, z_1, c_1, h_1) = (\gamma_0 \gamma_1, z_0 \gamma_1 + z_1, c_0 c_1 + z_0 h_1, h_0 + \gamma_0 h_1). \tag{4.4.1}
\]

**Proof.** For \( 0 \leq i \leq 1 \) let \( \varphi_i = (\gamma_i, z_i, c_i, h_i) \Phi \). Let \( \varphi_2 = \varphi_0 \varphi_1 \), and set \( (\gamma_2, z_2, c_2, h_2) = \varphi_2 \Psi \). Because \( c_0 \) is odd and \( uh_0 \) is even, (4.3.1) yields

\[
(c_2, z_2) = (1, 0) \varphi_2 = (1, 0) \varphi_0 \varphi_1 = (c_0, z_0) \varphi_1 = (c_0 c_1 + z_0 h_1, z_1 + z_0 \gamma_1),
\]

\[
(uh_2, u\gamma_2) = (0, u) \varphi_2 = (0, u) \varphi_0 \varphi_1 = (uh_0, u\gamma_0) \varphi_1 = (uh_0 c_1 + u\gamma_0 h_1, u\gamma_0 \gamma_1).
\]

The image of \( h_0 \) is contained in \( \langle m/2 \rangle \) and \( c_1 \) is odd, so \( h_0 c_1 = h_0 \). We are done by Proposition 4.3.2.

\[ \square \]

Here are some special cases of interest of Theorem 4.4.3:

**Corollary 4.4.4.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a finite dihedral-like automorphic loop such that either \( \alpha \neq 1 \) or \( \exp(G) > 2 \).

(i) If \( m/2 \) is odd then \( \text{Aut}(Q) \cong (C_{\text{Aut}(G)}(\alpha) \ltimes G) \times \mathbb{Z}_{m/2}^* \).

(ii) If \( m = 2 \) then \( \text{Aut}(Q) \cong C_{\text{Aut}(G)}(\alpha) \ltimes G \leq \text{Hol}(G) \).

(iii) If \( \alpha = 1 \) then the projection of \( \text{Aut}(Q) = (\text{Par}(m, G, \alpha), \circ) \) onto the first two coordinates is isomorphic to \( \text{Hol}(G) \).
(iv) If \( \alpha = 1 \) and \( m = 2 \) (so that \( Q \) is a generalized dihedral group) then \( \text{Aut}(Q) \cong \text{Hol}(G) \).

Proof. If \( m/2 \) is odd, the mappings \( h_i \) are trivial. We therefore do not have to keep track of the fourth coordinate in (4.4.1), and in the third coordinate we obtain \( c_0c_1 \).

The elements \( c_i \) can be identified with automorphisms \( g_i \) of \( E \) by letting \( 2g_i = 2c_i \).

Parts (i) and (ii) follow.

If \( \alpha = 1 \) then \( C_{\text{Aut}(G)}(\alpha) = \text{Aut}(G) \), proving (iii). Part (iv) then follows from (ii) and (iii).

\[ \Box \]

4.5 The inner mapping groups

We conclude the chapter with identifying inner mapping groups as subgroups of the automorphism group for dihedral-like automorphic loops.

**Theorem 4.5.1.** Let \( Q = \text{Dih}(m, G, \alpha) \) be a finite dihedral-like automorphic loop such that either \( \alpha \neq 1 \) or \( \exp(G) > 2 \). Then:

(i) \( \text{Inn}_r(Q) = \text{Inn}_G(Q) \) is isomorphic to the subgroup \( \langle \alpha \rangle \times G(1 - \alpha) \) of \( \text{Hol}(G) \),

(ii) \( \text{Inn}(Q) = \langle T_x, R_{x,y} : x, y \in Q \rangle = \langle T_x, L_{x,y} : x, y \in Q \rangle \) is isomorphic to the subgroup \( (\pm \langle \alpha \rangle) \times (2G + G(1 - \alpha)) \) of \( \text{Hol}(G) \).

Proof. Let us first verify that \( \langle \alpha \rangle \times G(1 - \alpha) \) and \( (\pm \langle \alpha \rangle) \times (2G + G(1 - \alpha)) \) are subgroups of \( \text{Hol}(G) \). Indeed, for \( \delta, \varepsilon \in \{1, -1\} \), we have

\[
(\delta \alpha^j, 2u + v(1 - \alpha))(\varepsilon \alpha^j, 2w + z(1 - \alpha)) = (\delta \varepsilon \alpha^{i+j}, (2u + v(1 - \alpha))\varepsilon \alpha^j + 2w + z(1 - \alpha))
\]

\[
= (\delta \varepsilon \alpha^{i+j}, 2(u\varepsilon \alpha^j + w) + (v\varepsilon \alpha^j + z)(1 - \alpha)),
\]

since \( 1 - \alpha \) commutes with \( \pm \alpha^j \).
By Proposition 2.5.2, we have

\[(0, w)T_{(i, u)} = (0, s_i w), \quad (1, 0)T_{(i, u)} = (1, 2u),\]
\[(0, w)R_{(j, v), (i, u)} = (0, w\alpha^{ij}), \quad (1, 0)R_{(j, v), (i, u)} = (1, s_i + j u\alpha^{ij}(\alpha^{-j} - 1)),\]
\[(0, w)L_{(j, v), (i, u)} = (0, w\alpha^{ij}), \quad (1, 0)L_{(j, v), (i, u)} = (1, -s_j u\alpha^{ij}(\alpha^{-j} - 1)).\]

Therefore

\[T_{(i, u)}\Psi = (s_i, 2u, 1, 0),\]
\[R_{(j, v), (i, u)}\Psi = (\alpha^{ij}, s_i + j u\alpha^{ij}(\alpha^{-j} - 1), 1, 0),\]
\[L_{(j, v), (i, u)}\Psi = (\alpha^{ij}, -s_j u\alpha^{ij}(\alpha^{-j} - 1), 1, 0),\]

where we identify the sign \(s_i\) with the automorphism \(u \mapsto s_i u\). Hence \(\text{Inn}(Q)\) is nontrivial only on the first two coordinates of \(\text{Par}(m, G, \alpha)\), and it can therefore be identified with a subgroup of \(\text{Hol}(G)\), by Proposition 4.3.2 and Theorem 4.4.3.

With \(u = 0\) and \(i = j = 1\) we get \((\alpha, 0)\) from both \(R_{(j, v), (i, u)}\) and \(L_{(j, v), (i, u)}\). Taking powers of this element, we see that \(\langle \alpha \rangle \times 0 \subseteq \text{Inn}_r(Q) \cap \text{Inn}_l(Q)\). With \(i = 0\) and \(j = 1\) we get \((1, -u(\alpha^{-1} - 1)) = (1, -u\alpha(1 - \alpha))\) from \(R_{(j, v), (i, u)}\), and \((1, u(\alpha^{-1} - 1)) = (1, u\alpha(1 - \alpha))\) from \(L_{(j, v), (i, u)}\), showing that \(1 \times G(1 - \alpha) \subseteq \text{Inn}_r(Q) \cap \text{Inn}_l(Q)\). Therefore \((\langle \alpha \rangle \times 0)(1 \times G(1 - \alpha)) = \langle \alpha \rangle \times G(1 - \alpha) \subseteq \text{Inn}_r(Q) \cap \text{Inn}_l(Q)\). On the other hand, using the fact that either \(m = 2\) or \(\alpha^2 = 1\), it is easy to see that the generators \(R_{(j, v), (i, u)}\) and \(L_{(j, v), (i, u)}\) belong to \(\langle \alpha \rangle \times G(1 - \alpha)\). This proves (i).

With \(u = 0\) we get \((s_i, 0)\) from \(T_{(i, u)}\), and with \(i = 0\) we get \((0, 2u)\) from \(T_{(i, u)}\). Hence \((\pm 1) \times 0\) and \(0 \times 2G\) are also subsets of \(\text{Inn}(Q)\), and thus \((\pm \langle \alpha \rangle) \times (2G + G(1 - \alpha)) \subseteq \text{Inn}(Q)\). The other inclusion is again clear from an inspection of \(T_{(i, u)}\).

**Corollary 4.5.2.** Let \(Q = \text{Dih}(2, G, 1)\) be a generalized dihedral group such that \(\exp(G) > 2\). Then the inner automorphism group of \(Q\) is isomorphic to \(\mathbb{Z}_2 \times 2G\).
Example 4.5.3. Let \( p \) be an odd prime, \( G = \mathbb{Z}_p \), and \( \alpha \neq 1 \) the unique involutory automorphism of \( G \), that is, \( \alpha = -1 \). Let \( Q = \text{Dih}(2, G, \alpha) \). Then \( \pm\langle \alpha \rangle \cong \mathbb{Z}_2 \cong \langle \alpha \rangle \), and \( G(1 - \alpha) = 2G = G \). Therefore \( \text{Inn}_r(Q) = \text{Inn}_r(Q) = \text{Inn}(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_p \) is isomorphic to the dihedral group of order \( 2p \).

Let us discuss the parameters \((\gamma, w, c, g, K)\) of Proposition 4.4.2. Let \( C = \text{Aut}(G) \langle \alpha \rangle = \{ \delta \in \text{Aut}(G); \alpha \delta = \delta \alpha \} \) be the centralizer of \( \alpha \) in \( \text{Aut}(G) \). Suppose that \( \alpha, \beta \) are conjugate in \( \text{Aut}(G) \). Note that \( \alpha^\gamma = \beta = \alpha^\delta \) iff \( \alpha^{\delta^{-1}} = \alpha \) iff \( \gamma \delta^{-1} \in C = \text{Aut}(G) \langle \alpha \rangle \) iff \( \gamma \in C = \text{Aut}(G) \langle \alpha \rangle \delta \). Hence the first parameter \( \gamma \) ranges over a coset of \( C = \text{Aut}(G) \langle \alpha \rangle \). Since \( A = < 2 > \cong \mathbb{Z}_{m/2} \), the parameter \( g \in \text{Aut}(A) \) can be identified with \( \bar{g} \in \text{Aut}(\mathbb{Z}_{m/2}) \) via \( i\bar{g} = ((2i)g)/2 \), for \( 0 \leq i < m/2 \). The two solutions \( c \in \mathbb{Z}_m \) to \( 2g \cong 2c \pmod{m} \) differ by \( m/2 \). If \( m/2 \) is even then the two solutions have the same parity, necessarily odd, and thus are both suitable parameters for the correspondence. If \( m/2 \) is odd then only one of the two solutions is odd.

Let \( \text{Inv}_G(\alpha) = \{ K \leq G : [G : K] \leq 2, K\alpha = K \} \), and let \( \phi \) be the Euler function. Suppose that \( \alpha \neq 1 \) and \( \beta \) are conjugate in \( \text{Aut}(G) \). It follows from Proposition 4.4.2 and the above comments that the set \( \text{Iso}(m, G, \alpha, \beta) \) of all isomorphisms from \( \text{Dih}(m, G, \alpha) \) to \( \text{Dih}(m, G, \beta) \) has cardinality \( |C = \text{Aut}(G) \langle \alpha \rangle| \cdot |G| \cdot |\phi_{m/2}| \cdot 2 \cdot |\text{Inv}_G(\alpha)| \) if \( m/2 \) is even, and \( |C = \text{Aut}(G) \langle \alpha \rangle| \cdot |G| \cdot |\phi_{m/2}| \) if \( m/2 \) is odd.
Chapter 5

Enumeration

Enumeration is an important part of any algebraic theory. In Section 1.5 we presented several results concerning enumeration of automorphic $p$-loops. Here are some additional known results: look up the tables in [23]

<table>
<thead>
<tr>
<th>$n$</th>
<th>8</th>
<th>15</th>
<th>16</th>
<th>21</th>
<th>24</th>
<th>27</th>
<th>30</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commutative groups</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>commutative nonassociative A-loops</td>
<td>4(3)</td>
<td>1</td>
<td>46(38)</td>
<td>1</td>
<td>4(3)</td>
<td>4</td>
<td>1</td>
<td>?</td>
</tr>
<tr>
<td>commutative nonassociative A-loops with nontrivial center</td>
<td>3(2)</td>
<td>0</td>
<td>44(37)</td>
<td>0</td>
<td>4(3)</td>
<td>4</td>
<td>1</td>
<td>?</td>
</tr>
<tr>
<td>commutative nonassociative A-loops of exponent $p$</td>
<td>2</td>
<td>–</td>
<td>12(11)</td>
<td>–</td>
<td>–</td>
<td>0</td>
<td>–</td>
<td>?</td>
</tr>
<tr>
<td>commutative nonassociative A-loops of exponent $p$ with nontrivial center</td>
<td>1</td>
<td>–</td>
<td>10</td>
<td>–</td>
<td>–</td>
<td>0</td>
<td>–</td>
<td>211 (210)</td>
</tr>
</tbody>
</table>

Table 5.1: Commutative automorphic loops up to isomorphism (up to isotopism)
In this chapter we are concerned with enumeration of dihedral-like automorphic
loops up to isomorphism and up to isotopism.

5.1 Conjugacy classes in automorphism groups of abelian
groups

In Theorem 4.2.3 we showed that two automorphic loops \( \text{Dih}(m, G, \alpha), \text{Dih}(\overline{m}, \overline{G}, \overline{\alpha}) \)
are isomorphic if and only if \( m = \overline{m}, G = \overline{G} \) and \( \alpha \) is conjugate to \( \overline{\alpha} \) in \( \text{Aut}(G) \).
We are therefore interested in conjugacy classes of automorphism groups of finite
abelian groups. First we state some basic results.

Definition 5.1.1. Let \( x, y \in G \). We say that \( x \) is conjugate to \( y \) in \( G \) if \( y = g^{-1}xg \)
for some \( g \in G \). The set of all elements conjugate to \( x \) in \( G \) is \( x^G = \{ g^{-1}xg : g \in G \} \),
and is called the conjugacy class of \( x \) in \( G \).

For a group \( G \), let \( \text{Conj}(G) \) be the set of all conjugacy classes of \( G \), and
\( \text{Conj}_2(G) \) be the set of all conjugacy classes of \( G \) consisting of elements of order
\( \leq 2 \). We call the classes of \( \text{Conj}_2(G) \) involutory.

Theorem 5.1.2. \([10, (Classification of Finite Abelian Groups)] \) Let \( G \) be a finite
group. Then \( G \) is abelian if and only if \( G \cong G_{p_1} \times \cdots \times G_{p_t}, |G_{p_i}| = p_i^{k_i}, \) each \( G_{p_i} \)
is a direct product of cyclic \( p_i \)-groups, and \( p_1, \cdots, p_t \) are distinct primes, \( k_1, \cdots, k_t \)
are positive integers.

Proposition 5.1.3. \([10]\) Let \( H \) and \( K \) be groups. If \( \gcd(|H|, |K|) = 1 \) then \( \text{Aut}(H \times K) \cong \text{Aut}(H) \times \text{Aut}(K) \).
Proposition 5.1.4. Let $H$ and $K$ be groups. Then

(i) $\text{Conj}(H \times K) = \text{Conj}(H) \times \text{Conj}(K)$,

(ii) $\text{Conj}_2(H \times K) = \text{Conj}_2(H) \times \text{Conj}_2(K)$.

Proof. First we prove (i). Let $H$ and $K$ be groups, and let $(x, y) \in H \times K$. We have $\text{Conj}(H \times K) = \{(h, k)^{H \times K} : (h, k) \in H \times K\}$ and $\text{Conj}(H) \times \text{Conj}(K) = \{h^H : h \in H\} \times \{k^K : k \in K\}$. Now, $(h, k)^{H \times K} = \{(x, y)(h, k)(x, y)^{-1} : (x, y) \in H \times K\} = h^H \times k^K$. For part (ii), let $h^H \in \text{Conj}_2(H)$, $k^K \in \text{Conj}_2(K)$. Then $h^H \times k^K = (h, k)^{H \times K} \in \text{Conj}(H \times K)$. But since $|(h, k)| = \text{lcm}(|h|, |k|)$, then $|(h, k)| \leq 2$. Conversely, if $|(h, k)| \leq 2$ then $|h|, |k| \leq 2$.

Let $\phi$ be the Euler function, so that $\phi(n) = |\{1 \leq k \leq n : \gcd(k, n) = 1\}|$.

Proposition 5.1.5. ([19, Satz 13.19, page 84]).

(i) $\text{Aut}(\mathbb{Z}_n)$ is isomorphic to the multiplicative group of $\mathbb{Z}_n$ of order $\phi(n)$.

(ii) For a prime $p > 2$, $\text{Aut}(\mathbb{Z}_{p^r})$ is a cyclic group of order $\phi(p^r) = p^r - 1(p - 1)$.

(iii) For a prime $p = 2$ and $r \geq 3$,

$$\text{Aut}(\mathbb{Z}_{2^r}) \simeq \mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2$$

(iv) $\text{Aut}(\mathbb{Z}_4) \simeq \mathbb{Z}_2$, and $\text{Aut}(\mathbb{Z}_2)$ is the trivial group.

Corollary 5.1.6. (Conjugacy classes of $\text{Aut}(\mathbb{Z}_p)$)

(i) $p > 2 : |\text{Conj}(\text{Aut}(\mathbb{Z}_{p^r}))| = p^{r-1}(p - 1)$, and $|\text{Conj}_2(\text{Aut}(\mathbb{Z}_{p^r}))| = 2$.

(ii) $p = 2$ and $r \geq 3 : |\text{Conj}(\text{Aut}(\mathbb{Z}_{2^r}))| = 2^{r-1}$ and $|\text{Conj}_2(\text{Aut}(\mathbb{Z}_{2^r}))| = 4$.

(iii) $|\text{Conj}(\text{Aut}(\mathbb{Z}_4))| = 2$ and $|\text{Conj}_2(\text{Aut}(\mathbb{Z}_4))| = 2$. 

66
(iv) $|\text{Conj}(\text{Aut}(\mathbb{Z}_2))| = 1$ and $|\text{Conj}_2(\text{Aut}(\mathbb{Z}_2))| = 1$.

**Proposition 5.1.7.** [10] Let $p$ be a prime and let $G = \mathbb{Z}_p^n$. Then $\text{Aut}(G) \cong \text{GL}_n(\mathbb{F}_p)$.

Recall that $\text{GL}_n(\mathbb{F}_p)$ is a group of order $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$.

We are interested in knowing the number of conjugacy classes in $\text{GL}_n(\mathbb{F}_p)$.

**Theorem 5.1.8.** [27] A generating function for the number of $q_n(p)$ conjugacy classes of finite general linear groups $\text{GL}_n(\mathbb{F}_p)$ is

$$1 + \sum_{n=1}^{\infty} q_n(p)t^n = \prod_{i=1}^{\infty} \frac{1 - t^i}{1 - pt^i}.$$  \hspace{1cm} (5.1.1)

The polynomials $q_n$ have been explicitly calculated from (5.1.1) in [27] for $n \leq 12$.

For our purposes we consider only $q_n$ for $n \leq 5$.

- $q_0(p) = 1$
- $q_1(p) = p - 1$
- $q_2(p) = p^2 - 1$
- $q_3(p) = p^3 - p$
- $q_4(p) = p^4 - p$
- $q_5(p) = p^5 - p^2 - p + 1$

The next proposition determines the size of the conjugacy classes of all dihedral groups, which show up as automorphism groups of certain abelian groups.
Proposition 5.1.9. [20] Let $D_{2n}$ be the dihedral group of order $2n$. Then

$$|\text{Conj}(D_{2n})| = \begin{cases} 
\frac{n}{2} + 3 & \text{if } n = \text{even}, \\
\frac{1}{2}(n + 3) & \text{if } n = \text{odd}.
\end{cases} \quad (5.1.2)$$

The preceding results allow us to count the number of conjugacy classes and involutory conjugacy classes in automorphism groups of many but not all abelian groups of order $< 64$.

In table 5.2 we give information about automorphism groups and their (involuntary) conjugacy classes of abelian groups of order $< 64$. The table is formatted as follows: the column called $n$ lists the order of the abelian group $G$, the column called $G$ gives the isomorphism type of $G$ as a direct product of $p$-primary components, the column called $A$ gives the isomorphism type of $\text{Aut}(G)$, the column called $C$ gives the number of conjugacy classes in $\text{Aut}(G)$, while the column called $C_2$ gives the number of involutory conjugacy classes in $\text{Aut}(G)$. Finally, the column called reference points to results that explain the entries in a given row. We enter $GAP$ here if the result was obtained by an explicit calculation in $GAP$. Note that Proposition 5.1.4 have list all orders $n = p^k$ by induction.

For instance, when $n = 8$ and $G = \mathbb{Z}_2^2$ we know the automorphism group, its order and its conjugacy classes from Lemmas 5.1.7, 5.1.8. However, for involutory conjugacy classes of the automorphism group we use GAP.
| n | $G$   | $A$   | $|A|$ | $C$ | $C_2$ | reference          |
|---|-------|-------|------|-----|-------|--------------------|
| 1 | $\mathbb{Z}_1$ | $\mathbb{Z}_1$ | 1    | 1   | 1     | 5.1.5 and 5.1.6   |
| 2 | $\mathbb{Z}_2$ | $\mathbb{Z}_1$ | 1    | 1   | 1     | 5.1.5 and 5.1.6   |
| 3 | $\mathbb{Z}_3$ | $\mathbb{Z}_2$ | 2    | 2   | 2     | 5.1.5 and 5.1.6   |
| 4 | $\mathbb{Z}_4$ | $\mathbb{Z}_2$ | 2    | 2   | 2     | 5.1.5 and 5.1.6   |
| 5 | $\mathbb{Z}_2^2$ | $\text{GL}(2,2)$ | 6    | 3   | 2     | 5.1.7 and 5.1.8   |
| 6 | $\mathbb{Z}_5$ | $\mathbb{Z}_4$ | 4    | 4   | 2     | 5.1.5 and 5.1.6   |
| 7 | $\mathbb{Z}_2 \times \mathbb{Z}_3$ | $\mathbb{Z}_2$ | 2    | 2   | 2     | 5.1.3 and 5.1.4   |
| 8 | $\mathbb{Z}_7$ | $\mathbb{Z}_6$ | 6    | 6   | 2     | 5.1.5 and 5.1.6   |
| 9 | $\mathbb{Z}_2^3$ | $\mathbb{Z}_2^2$ | 4    | 4   | 4     | 5.1.5 and 5.1.6   |
| 10 | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | $D_8$ | 8    | 5   | 4     | GAP and 5.1.9     |
| 11 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4$ | $\text{GL}(3,2)$ | 168  | 6   | 2     | 5.1.7 and 5.1.8   |
| 12 | $\mathbb{Z}_9$ | $\mathbb{Z}_6$ | 6    | 6   | 2     | 5.1.5 and 5.1.6   |
| 13 | $\mathbb{Z}_2 \times \mathbb{Z}_5$ | $\mathbb{Z}_4$ | 4    | 4   | 2     | 5.1.3 and 5.1.4   |
| 14 | $\mathbb{Z}_{11}$ | $\mathbb{Z}_{10}$ | 10   | 10  | 2     | 5.1.5 and 5.1.6   |
| 15 | $\mathbb{Z}_2 \times \mathbb{Z}_6$ | $D_{12}$ | 12   | 6   | 4     | GAP and 5.1.9     |
| 16 | $\mathbb{Z}_3 \times \mathbb{Z}_4$ | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | 4    | 4   | 4     | 5.1.3 and 5.1.4   |
| 17 | $\mathbb{Z}_{13}$ | $\mathbb{Z}_{12}$ | 12   | 12  | 2     | 5.1.5 and 5.1.6   |
| 18 | $\mathbb{Z}_2 \times \mathbb{Z}_7$ | $\mathbb{Z}_6$ | 6    | 6   | 2     | 5.1.3 and 5.1.4   |
| 19 | $\mathbb{Z}_3 \times \mathbb{Z}_5$ | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | 8    | 8   | 4     | 5.1.3 and 5.1.4   |
| 20 | $\mathbb{Z}_{16}$ | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | 8    | 8   | 4     | 5.1.5 and 5.1.6   |
| 21 | $\mathbb{Z}_2 \times \mathbb{Z}_8$ | $\mathbb{Z}_2 \times D_8$ | 16   | 10  | 8     | GAP and 5.1.9     |
| 22 | $\mathbb{Z}_4^2$ | $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times A_4) : \mathbb{Z}_2$ | 96   | 14  | 7     | GAP               |
| 23 | $\mathbb{Z}_4^4$ | $\text{GL}(4,2)$ | 20160 | 14  | 4     | 5.1.8 and 5.1.7   |

Table 5.2: Automorphism groups and their conjugacy classes of groups for abelian: groups of order $< 64$.
<table>
<thead>
<tr>
<th></th>
<th>$\mathbb{Z}_{17}$</th>
<th>$\mathbb{Z}_{16}$</th>
<th>16</th>
<th>16</th>
<th>2</th>
<th>5.1.5 and 5.1.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_9$</td>
<td>$\mathbb{Z}_6$</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_3^2$</td>
<td>$\text{GL}(2, 3)$</td>
<td>48</td>
<td>8</td>
<td>3</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>19</td>
<td>$\mathbb{Z}_{19}$</td>
<td>$\mathbb{Z}_{18}$</td>
<td>18</td>
<td>18</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>20</td>
<td>$\mathbb{Z}_2^2 \times \mathbb{Z}_5$</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_6$</td>
<td>24</td>
<td>12</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_5$</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_4$</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>21</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_7$</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_6$</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>22</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{11}$</td>
<td>$\mathbb{Z}_{10}$</td>
<td>10</td>
<td>10</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>23</td>
<td>$\mathbb{Z}_{23}$</td>
<td>$\mathbb{Z}_{22}$</td>
<td>22</td>
<td>22</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>24</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$</td>
<td>$\mathbb{Z}_{12} \times \mathbb{D}_8$</td>
<td>16</td>
<td>10</td>
<td>8</td>
<td>GAP</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_8$</td>
<td>$\mathbb{Z}_3^3$</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>25</td>
<td>$\mathbb{Z}_{25}$</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_5$</td>
<td>20</td>
<td>20</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_5^2$</td>
<td>$\text{GL}(2, 5)$</td>
<td>480</td>
<td>24</td>
<td>2</td>
<td>5.1.7 and 5.1.8</td>
</tr>
<tr>
<td>26</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{13}$</td>
<td>$\mathbb{Z}_{12}$</td>
<td>12</td>
<td>12</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>27</td>
<td>$\mathbb{Z}_{27}$</td>
<td>$\mathbb{Z}_{18}$</td>
<td>18</td>
<td>18</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_9$</td>
<td>$\mathbb{Z}_{108}$</td>
<td>108</td>
<td>20</td>
<td>4</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_3^3$</td>
<td>$\text{GL}(3, 3)$</td>
<td>11232</td>
<td>24</td>
<td>4</td>
<td>5.1.7 and 5.1.8</td>
</tr>
<tr>
<td>28</td>
<td>$\mathbb{Z}_2^2 \times \mathbb{Z}_7$</td>
<td>$\mathbb{Z}_2^2 \times \mathbb{Z}_6$</td>
<td>36</td>
<td>18</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_7$</td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_2$</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>29</td>
<td>$\mathbb{Z}_{29}$</td>
<td>$\mathbb{Z}_{28}$</td>
<td>28</td>
<td>28</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>30</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{15}$</td>
<td>$\mathbb{Z}_8$</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}<em>3 \times \mathbb{Z}</em>{10}$</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_2$</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>31</td>
<td>$\mathbb{Z}_{31}$</td>
<td>$\mathbb{Z}_{30}$</td>
<td>30</td>
<td>30</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>32</td>
<td>$\mathbb{Z}_{32}$</td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_2$</td>
<td>16</td>
<td>16</td>
<td>4</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{16}$</td>
<td>$\mathbb{Z}_{32}$</td>
<td>32</td>
<td>20</td>
<td>9</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_8$</td>
<td>$\mathbb{Z}_{128}$</td>
<td>128</td>
<td>26</td>
<td>17</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_2^5)</td>
<td>GL(5, 2)</td>
<td>9999360</td>
<td>27</td>
<td>3</td>
<td>5.1.7 and 5.1.8</td>
</tr>
<tr>
<td>---</td>
<td>----------------</td>
<td>----------</td>
<td>----------</td>
<td>----</td>
<td>---</td>
<td>------------------</td>
</tr>
<tr>
<td>33</td>
<td>(\mathbb{Z}<em>3 \times \mathbb{Z}</em>{11})</td>
<td>(\mathbb{Z}_{10} \times \mathbb{Z}_2)</td>
<td>20</td>
<td>20</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>34</td>
<td>(\mathbb{Z}<em>2 \times \mathbb{Z}</em>{17})</td>
<td>(\mathbb{Z}_{16})</td>
<td>16</td>
<td>16</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>35</td>
<td>(\mathbb{Z}_5 \times \mathbb{Z}_7)</td>
<td>(\mathbb{Z}_6 \times \mathbb{Z}_4)</td>
<td>24</td>
<td>24</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>36</td>
<td>(\mathbb{Z}_2^2 \times \mathbb{Z}_9)</td>
<td>(\mathbb{Z}_6 \times \mathbb{Z}_6)</td>
<td>36</td>
<td>18</td>
<td>4</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_2^2 \times \mathbb{Z}_3^2)</td>
<td>(\mathbb{Z}_{96})</td>
<td>96</td>
<td>16</td>
<td>6</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_4 \times \mathbb{Z}_9)</td>
<td>(\mathbb{Z}_6 \times \mathbb{Z}_2)</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>37</td>
<td>(\mathbb{Z}_{37})</td>
<td>(\mathbb{Z}_{36})</td>
<td>36</td>
<td>36</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>38</td>
<td>(\mathbb{Z}_{19} \times \mathbb{Z}_2)</td>
<td>(\mathbb{Z}_{18})</td>
<td>18</td>
<td>14</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>39</td>
<td>(\mathbb{Z}<em>3 \times \mathbb{Z}</em>{13})</td>
<td>(\mathbb{Z}_{12} \times \mathbb{Z}_2)</td>
<td>24</td>
<td>24</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>40</td>
<td>(\mathbb{Z}<em>2 \times \mathbb{Z}</em>{20})</td>
<td>(\mathbb{Z}_{32})</td>
<td>32</td>
<td>20</td>
<td>8</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}<em>4 \times \mathbb{Z}</em>{10})</td>
<td>(\mathbb{Z}_{16})</td>
<td>16</td>
<td>16</td>
<td>8</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>41</td>
<td>(\mathbb{Z}_{41})</td>
<td>(\mathbb{Z}_{40})</td>
<td>40</td>
<td>40</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>42</td>
<td>(\mathbb{Z}<em>2 \times \mathbb{Z}</em>{21})</td>
<td>(\mathbb{Z}_6 \times \mathbb{Z}_2)</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>43</td>
<td>(\mathbb{Z}_{43})</td>
<td>(\mathbb{Z}_{42})</td>
<td>42</td>
<td>42</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>44</td>
<td>(\mathbb{Z}<em>2^2 \times \mathbb{Z}</em>{11})</td>
<td>(\mathbb{Z}_{60})</td>
<td>60</td>
<td>30</td>
<td>4</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_{11} \times \mathbb{Z}_4)</td>
<td>(\mathbb{Z}_{10} \times \mathbb{Z}_2)</td>
<td>20</td>
<td>20</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>45</td>
<td>(\mathbb{Z}_3^2 \times \mathbb{Z}_5)</td>
<td>(\mathbb{Z}_{48} \times \mathbb{Z}_4)</td>
<td>192</td>
<td>32</td>
<td>6</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_5 \times \mathbb{Z}_9)</td>
<td>(\mathbb{Z}_6 \times \mathbb{Z}_4)</td>
<td>24</td>
<td>24</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>46</td>
<td>(\mathbb{Z}<em>2 \times \mathbb{Z}</em>{23})</td>
<td>(\mathbb{Z}_{22} \times \mathbb{Z}_1)</td>
<td>22</td>
<td>22</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>47</td>
<td>(\mathbb{Z}_{47})</td>
<td>(\mathbb{Z}_{46})</td>
<td>46</td>
<td>46</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>48</td>
<td>(\mathbb{Z}<em>3 \times \mathbb{Z}</em>{16})</td>
<td>(\mathbb{Z}_{8} \times \mathbb{Z}_2)</td>
<td>16</td>
<td>16</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_2^4 \times \mathbb{Z}_3)</td>
<td>(\mathbb{Z}_{40320})</td>
<td>40320</td>
<td>28</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_4^2 \times \mathbb{Z}_3)</td>
<td>(\mathbb{Z}_{96} \times \mathbb{Z}_2)</td>
<td>192</td>
<td>28</td>
<td>16</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Z}_6 \times \mathbb{Z}_8)</td>
<td>(\mathbb{Z}_{32})</td>
<td>32</td>
<td>20</td>
<td>16</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>49</td>
<td>(\mathbb{Z}_{49})</td>
<td>(\mathbb{Z}_{42})</td>
<td>42</td>
<td>42</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_7^2$</td>
<td>$\text{GL}(2, 7)$</td>
<td>2016</td>
<td>48</td>
<td>3</td>
<td>5.1.7 and 5.1.8</td>
</tr>
<tr>
<td>----</td>
<td>------------------</td>
<td>------------------</td>
<td>------</td>
<td>----</td>
<td>---</td>
<td>----------------</td>
</tr>
<tr>
<td>50</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{25}$</td>
<td>$\mathbb{Z}<em>1 \times \mathbb{Z}</em>{20}$</td>
<td>20</td>
<td>20</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}<em>5 \times \mathbb{Z}</em>{10}$</td>
<td>$\mathbb{Z}_{32}$</td>
<td>32</td>
<td>20</td>
<td>16</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>51</td>
<td>$\mathbb{Z}<em>3 \times \mathbb{Z}</em>{17}$</td>
<td>$\mathbb{Z}_{32}$</td>
<td>32</td>
<td>32</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>52</td>
<td>$\mathbb{Z}<em>2^2 \times \mathbb{Z}</em>{13}$</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{12}$</td>
<td>24</td>
<td>24</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}<em>2^2 \times \mathbb{Z}</em>{13}$</td>
<td>$\mathbb{Z}_{72}$</td>
<td>72</td>
<td>36</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>53</td>
<td>$\mathbb{Z}_{53}$</td>
<td>$\mathbb{Z}_{52}$</td>
<td>52</td>
<td>52</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>54</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{27}$</td>
<td>$\mathbb{Z}<em>1 \times \mathbb{Z}</em>{18}$</td>
<td>18</td>
<td>18</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_9$</td>
<td>$\mathbb{Z}_{108}$</td>
<td>108</td>
<td>20</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>55</td>
<td>$\mathbb{Z}<em>5 \times \mathbb{Z}</em>{11}$</td>
<td>$\mathbb{Z}_{10} \times \mathbb{Z}_4$</td>
<td>40</td>
<td>40</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>56</td>
<td>$\mathbb{Z}_2^4 \times \mathbb{Z}_7$</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_6$</td>
<td>24</td>
<td>24</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{28}$</td>
<td>$\mathbb{Z}_{16} \times \mathbb{Z}_3$</td>
<td>48</td>
<td>30</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>57</td>
<td>$\mathbb{Z}<em>3 \times \mathbb{Z}</em>{19}$</td>
<td>$\mathbb{Z}_{18} \times \mathbb{Z}_2$</td>
<td>36</td>
<td>36</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>58</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{29}$</td>
<td>$\mathbb{Z}_{28} \times \mathbb{Z}_1$</td>
<td>28</td>
<td>28</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>59</td>
<td>$\mathbb{Z}_{59}$</td>
<td>$\mathbb{Z}_{58}$</td>
<td>58</td>
<td>58</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>60</td>
<td>$\mathbb{Z}<em>5 \times \mathbb{Z}</em>{12}$</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_4$</td>
<td>16</td>
<td>16</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>61</td>
<td>$\mathbb{Z}_2^2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$</td>
<td>$\mathbb{Z}_{48}$</td>
<td>48</td>
<td>24</td>
<td>8</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_{61}$</td>
<td>$\mathbb{Z}_{60}$</td>
<td>60</td>
<td>60</td>
<td>2</td>
<td>5.1.5 and 5.1.6</td>
</tr>
<tr>
<td>62</td>
<td>$\mathbb{Z}<em>2 \times \mathbb{Z}</em>{41}$</td>
<td>$\mathbb{Z}_{30} \times \mathbb{Z}_4$</td>
<td>30</td>
<td>30</td>
<td>2</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td>63</td>
<td>$\mathbb{Z}_3^2 \times \mathbb{Z}_7$</td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_6$</td>
<td>36</td>
<td>36</td>
<td>4</td>
<td>5.1.3 and 5.1.4</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_3^2 \times \mathbb{Z}_7$</td>
<td>$\mathbb{Z}_{288}$</td>
<td>288</td>
<td>48</td>
<td>6</td>
<td>5.1.3 and 5.1.4</td>
</tr>
</tbody>
</table>
5.2 Dihedral-like automorphic loops of order $< 128$ up to isomorphism

Table 5.3 provides a list of dihedral-like automorphic loops $Q = \text{Dih}(m, G, \alpha)$ of order $< 128$ up to isomorphism. It is based on Theorem 4.2.3 and Table 5.2. For example, when $n = 14$, we have the possibility of $m = 14, 2$ and $G = \mathbb{Z}_1, \mathbb{Z}_7$, respectively, so we can look up the conjugacy classes and involutory conjugacy classes of $\text{Aut} (\mathbb{Z}_1)$, $\text{Aut} (\mathbb{Z}_7)$ in the respective rows of Table 5.1. Note that $C_2$ comes into play iff $m > 2$. 
Table 5.3: A list of dihedral-like automorphic loops of order \( \leq 126 \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( m )</th>
<th>( G )</th>
<th>( C )</th>
<th>( C_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>( Z_4 )</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2 ( Z_2 )</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>( Z_2 )</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>( Z_5 )</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2 ( Z_2 )</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>( Z_3 )</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>( Z_3 \times Z_2 )</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>( Z_7 )</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2 ( Z_2 )</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4 ( Z_4 )</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3 ( Z_2 )</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>( Z_8 )</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2 ( Z_4 \times Z_2 )</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3 ( Z_2 )</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>18</td>
<td>( Z_1 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$n$</td>
<td>$m$</td>
<td>$G$</td>
<td>$C$</td>
<td>$C_2$</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>2</td>
<td>32</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>16</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>$\mathbb{Z}_2^2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_8$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_2$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_2^3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{16}$</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_2^4$</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_2$</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_2^4$</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>34</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{17}$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>36</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>18</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_9$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_2^3$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{18}$</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_3$</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>38</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$G$</th>
<th>$C$</th>
<th>$C_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>40</td>
<td>$\mathbb{Z}_{19}$</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>20</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>10</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>8</td>
<td>$\mathbb{Z}_2^2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_4$</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{10} \times \mathbb{Z}_2$</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>42</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>$\mathbb{Z}_7$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_7 \times \mathbb{Z}_3$</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>44</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>22</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_{11}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{11} \times \mathbb{Z}_2$</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>46</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{23}$</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>48</td>
<td>$\mathbb{Z}_1$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>24</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>$\mathbb{Z}_8$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>$n$</td>
<td>$m$</td>
<td>$G$</td>
<td>$C$</td>
<td>$C_2$</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>$Z_4 \times Z_2$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>$Z_2^3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$Z_4 \times Z_3$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$Z_6 \times Z_2$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>$Z_8 \times Z_3$</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>$Z_6 \times Z_4$</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>$Z_2 \times Z_{12}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>$Z_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>$Z_{25}$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>24</td>
<td>$Z_5 \times Z_5$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>52</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>1</td>
<td>$Z_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$Z_{13}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>$Z_{13} \times Z_2$</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>54</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>2</td>
<td>$Z_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>$Z_9$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>$Z_3^2$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>18</td>
<td>$Z_{27}$</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>$Z_9 \times Z_3$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>24</td>
<td>$Z_3^3$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>56</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>1</td>
<td>$Z_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>$Z_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$Z_2^2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$Z_7$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$Z_7 \times Z_2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$Z_{14} \times Z_2$</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$Z_7 \times Z_4$</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>58</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$Z_{29}$</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>60</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>$Z_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>2</td>
<td>$Z_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>$Z_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$Z_3 \times Z_2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>$Z_5 \times Z_2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$Z_5 \times Z_3$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$Z_6 \times Z_5$</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>62</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$Z_{31}$</td>
<td>30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>64</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td>$Z_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>$Z_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>$Z_2^2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$Z_8$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$Z_4 \times Z_2$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$Z_2^3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$Z_{16}$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$Z_8 \times Z_2$</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$n$</td>
<td>$m$</td>
<td>$G$</td>
<td>$C$</td>
<td>$C_2$</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_4$</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{32}$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{32}$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_4$</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{16} \times \mathbb{Z}_2$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_2^5$</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>66</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>$\mathbb{Z}_{11}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}<em>3 \times \mathbb{Z}</em>{11}$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>68</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$\mathbb{Z}_{17}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{17} \times \mathbb{Z}_2$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>70</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>$\mathbb{Z}_7$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_7 \times \mathbb{Z}_5$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>72</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td></td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$G$</th>
<th>$C$</th>
<th>$C_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td>$\mathbb{Z}_9 \times \mathbb{Z}_3$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$\mathbb{Z}_9 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_3$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_9 \times \mathbb{Z}_4$</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_6$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{18} \times \mathbb{Z}_2$</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{12} \times \mathbb{Z}_3$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>74</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{37}$</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>76</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td></td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$\mathbb{Z}_{19}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{19} \times \mathbb{Z}_2$</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>78</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>$\mathbb{Z}_{13}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$\mathbb{Z}_{13} \times \mathbb{Z}_3$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>80</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>$\mathbb{Z}_8$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_2$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>$\mathbb{Z}_2^3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>m</td>
<td>$G$</td>
<td>$C$</td>
<td>$C_2$</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-------------</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$Z_{11} \times Z_4$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>$Z_5 \times Z_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$Z_{10} \times Z_2$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$Z_5 \times Z_4$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$Z_{20} \times Z_2$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$Z_{10} \times Z_4$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$Z_8 \times Z_5$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>82</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>41</td>
<td>$Z_{41}$</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>84</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>2</td>
<td>$Z_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>$Z_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>$Z_3 \times Z_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>$Z_7$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>$Z_7 \times Z_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$Z_7 \times Z_3$</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$Z_7 \times Z_6$</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>86</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>43</td>
<td>$Z_{43}$</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>88</td>
<td>$Z_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>2</td>
<td>$Z_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>2</td>
<td>$Z_4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>2</td>
<td>$Z_2 \times Z_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>$Z_{11}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$Z_{11} \times Z_2$</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

| 2   | 2   | $Z_{22} \times Z_2$ | 30  |       |
| 90  | 90  | $Z_1$      | 1   |       |
| 30  | 2   | $Z_3$    | 2   |       |
| 18  | 2   | $Z_5$    | 2   |       |
| 10  | 2   | $Z_9$    | 2   |       |
| 10  | 3   | $Z_3 \times Z_3$ | 3   |       |
| 6   | 4   | $Z_5 \times Z_3$ | 4   |       |
| 2   | 24  | $Z_9 \times Z_5$ | 24  |       |
| 2   | 32  | $Z_{15} \times Z_3$ | 32  |       |
| 92  | 92  | $Z_1$      | 1   |       |
| 46  | 1   | $Z_2$    | 1   |       |
| 4   | 2   | $Z_{23}$ | 2   |       |
| 2   | 22  | $Z_{23} \times Z_2$ | 22  |       |
| 94  | 94  | $Z_1$      | 1   |       |
| 2   | 46  | $Z_{47}$ | 46  |       |
| 96  | 96  | $Z_1$      | 1   |       |
| 48  | 1   | $Z_2$    | 1   |       |
| 32  | 2   | $Z_3$    | 2   |       |
| 24  | 2   | $Z_4$    | 2   |       |
| 24  | 2   | $Z_2^2$ | 2   |       |
| 16  | 2   | $Z_3 \times Z_2$ | 2   |       |
| 12  | 4   | $Z_8$    | 4   |       |
| 12  | 4   | $Z_4 \times Z_2$ | 4   |       |
| 12  | 2   | $Z_2^3$ | 2   |       |
| 8   | 4   | $Z_4 \times Z_3$ | 4   |       |
| 8   | 4   | $Z_6 \times Z_2$ | 4   |       |

78
<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$G$</th>
<th>$C$</th>
<th>$C_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_2$</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>$\mathbb{Z}_2^2$</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>$\mathbb{Z}_2^4$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_3$</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>$\mathbb{Z}_{24} \times \mathbb{Z}_2$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>32</td>
<td>$\mathbb{Z}_{16} \times \mathbb{Z}_3$</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>64</td>
<td>$\mathbb{Z}_{12} \times \mathbb{Z}_4$</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>98</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>$\mathbb{Z}_7$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>98</td>
<td>$\mathbb{Z}_{49}$</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>100</td>
<td>$\mathbb{Z}_7 \times \mathbb{Z}_7$</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>$\mathbb{Z}_{25}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_5^2$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{25} \times \mathbb{Z}_2$</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>102</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>34</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>$\mathbb{Z}_{17}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{17} \times \mathbb{Z}_3$</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>52</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>26</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$G$</th>
<th>$C$</th>
<th>$C_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>26</td>
<td>$\mathbb{Z}_2^2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>$\mathbb{Z}_{13}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\mathbb{Z}_{13} \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{13} \times \mathbb{Z}_4$</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{26} \times \mathbb{Z}_2$</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>106</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>108</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>54</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>36</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>18</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>$\mathbb{Z}_9$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_3$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>56</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>22</td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>$\mathbb{Z}_{11}$</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\mathbb{Z}_{11} \times \mathbb{Z}_5$</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>112</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>56</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>----------------</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>$\mathbb{Z}_2^2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>$\mathbb{Z}_7$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$\mathbb{Z}_8$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_2$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$\mathbb{Z}_2^3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$\mathbb{Z}_7 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_7 \times \mathbb{Z}_4$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_{14} \times \mathbb{Z}_2$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{14} \times \mathbb{Z}_4$</td>
<td>30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_8 \times \mathbb{Z}_7$</td>
<td>24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>114</td>
<td>114</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>$\mathbb{Z}_{19}$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{19} \times \mathbb{Z}_3$</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>116</td>
<td>116</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_{29}$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{29} \times \mathbb{Z}_2$</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>118</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{59}$</td>
<td>58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>120</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>$\mathbb{Z}_2^2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_2$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_2$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$\mathbb{Z}_4 \times \mathbb{Z}_3$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>$\mathbb{Z}_5 \times \mathbb{Z}_4$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_6 \times \mathbb{Z}_5$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{30} \times \mathbb{Z}_2$</td>
<td>24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{12} \times \mathbb{Z}_5$</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>122</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{61}$</td>
<td>60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>124</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_{31}$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{31} \times \mathbb{Z}_2$</td>
<td>30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>126</td>
<td>$\mathbb{Z}_1$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>$\mathbb{Z}_7$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$\mathbb{Z}_9$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_3$</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>$\mathbb{Z}_7 \times \mathbb{Z}_3$</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_{21} \times \mathbb{Z}_3$</td>
<td>24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_9 \times \mathbb{Z}_7$</td>
<td>36</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The information from Table 5.3 allows us to count small dihedral-like automorphic loops up to isomorphism by simply summing up the entries for a given order. The result is provided in Table 5.10. The table is formatted as follows: the row called \( n \) lists the order of the loop, the row called \( X \) gives the number of dihedral-like automorphic loops of order \( n \) up to isomorphism, and the row called \( Y \) denotes the number of nonassociative dihedral-like automorphic loops up to isomorphism. For instance, with \( n = 18 \) we sum up the four entries 1, 2, 6, 8 from Table 5.2 to get \( X = 17 \), and we subtract 4 (corresponding to \( \alpha = 1 \)) to get \( Y = 14 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
<th>16</th>
<th>18</th>
<th>20</th>
<th>22</th>
<th>24</th>
<th>26</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X )</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>21</td>
<td>17</td>
<td>8</td>
<td>11</td>
<td>20</td>
<td>13</td>
</tr>
<tr>
<td>( Y )</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>14</td>
<td>13</td>
<td>4</td>
<td>9</td>
<td>12</td>
<td>11</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| \( n \) | 28 | 30 | 32 | 34 | 36 | 38 | 40 | 42 | 44 | 46 | 48 | 50 | 52 |
| \( X \) | 10 | 13 | 75 | 17 | 33 | 19 | 30 | 17 | 14 | 23 | 46 | 47 | 16 |
| \( Y \) | 6 | 9 | 63 | 15 | 25 | 17 | 22 | 13 | 10 | 21 | 33 | 43 | 12 |

| \( n \) | 54 | 56 | 58 | 60 | 62 | 64 | 66 | 68 | 70 | 72 | 74 | 76 | 78 |
| \( X \) | 70 | 40 | 29 | 22 | 31 | 180 | 25 | 20 | 29 | 75 | 37 | 22 | 29 |
| \( Y \) | 63 | 32 | 27 | 14 | 29 | 164 | 21 | 16 | 25 | 62 | 35 | 18 | 25 |

| \( n \) | 80 | 82 | 84 | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 |
| \( X \) | 84 | 41 | 26 | 43 | 60 | 70 | 26 | 47 | 157 | 93 | 55 | 37 | 70 |
| \( Y \) | 70 | 39 | 18 | 41 | 52 | 62 | 22 | 45 | 139 | 89 | 47 | 33 | 62 |

| \( n \) | 106 | 108 | 110 | 112 | 114 | 116 | 118 | 120 | 122 | 124 | 126 |
| \( X \) | 53 | 68 | 45 | 82 | 41 | 32 | 59 | 72 | 61 | 34 | 73 |
| \( Y \) | 51 | 55 | 41 | 79 | 37 | 28 | 57 | 57 | 59 | 30 | 65 |

Table 5.10: A list of dihedral-like automorphic loops up to isomorphism
5.3 Dihedral-like automorphic loops up to isotopism

Automorphic loops do not behave well with respect to isotopy.

**Theorem 5.3.1.** ([4]) Let \((Q, \cdot)\) be an automorphic loop. A necessary and sufficient condition that every loop isotopic to \(Q\) be an automorphic loop is that \(Q' \leq N(Q)\).

**Theorem 5.3.2.** Let \(Q\) be a dihedral-like automorphic loop. A necessary and sufficient condition that every loop isotopic to \(Q\) be an automorphic loop is that \(\alpha = 1\) or \((\alpha |_{2G} = 1_{2G} \text{ and } \alpha^2 = 1)\)

**Proof.** We have \(Q' = 0 \times (G(1 - \alpha) + 2G)\) and

\[
N(Q) = \begin{cases} 
Q & \text{if } \alpha = 1, \\
E \times \text{Fix}(\alpha) & \text{if } \alpha \neq 1.
\end{cases}
\]

If \(\alpha = 1\) then \(Q' \leq N(Q)\). Suppose that \(\alpha \neq 1\), then \(Q' = 0 \times (G(1 - \alpha) + 2G) \leq E \times \text{Fix}(\alpha) \iff \text{Fix}(\alpha) \iff x(1 - \alpha)\alpha = x(1 - \alpha), \forall \alpha, \alpha \mid_{2G} = 1_{2G} \iff (x - x\alpha)\alpha = x\alpha - x\alpha^2 = x - x\alpha \iff 2x\alpha = x + x\alpha^2 \iff 2x = x + x\alpha^2 \iff x = x\alpha^2 \iff \alpha^2 = 1\)

The next example shows that there exists a principal loop isotope of a dihedral-like automorphic loop \(Q\) that is not even an automorphic loop.

**Example 5.3.3.** Let \(m = 2, G = \mathbb{Z}_3, \alpha \in \text{Aut}(G), \alpha \neq 1\). It follows that \(\alpha^2 = 1\), but \(\alpha \mid_{2G} = \alpha \mid_{G} \neq 1\) so there must be a principal loop isotope of \(Q = \text{Dih}(2, \mathbb{Z}_3, \alpha)\) that is not even an automorphic loop. We verified this by GAP.
The next example shows that there is a dihedral-like automorphic loop $Q$ whose every loop isotope is automorphic, but not necessarily isomorphic to $Q$.

**Example 5.3.4.** Let $Q = \text{Dih}(4, \mathbb{Z}_2 \times \mathbb{Z}_2, \alpha)$ where $\alpha = (3, 4)$. By Theorem 5.3.2 every loop isotope of $Q$ is an automorphic loop. We find a principal isotope $Q_1$ by GAP such that $Q_1 \not\cong Q$.

Recall that in a loop $Q$, the principal isotopism $(R(g), L(f), \ell)$ is defined as $x \circ y = xR(g)^{-1} \cdot yL(f)^{-1}$ for all $x, y \in G$.

**Lemma 5.3.5.** In a loop $Q = \text{Dih}(m, G, \alpha)$ we have

$$(i, u) \circ (j, v) = ((i + j) - (k + \ell), s_{j-\ell-k}u\alpha^{-k(i-k)+(i-k)(j-\ell)}$$

$$- s_{j-\ell-k}w\alpha^{(i-k)(j-\ell)} + v\alpha^{-\ell(i-\ell)+(i-k)(i-\ell)}$$

$$- s_{\ell-r}r\alpha^{(i-k)(j-\ell)}$$

for $(i, u), (j, v) \in Q$.

**Proof.** Let $x = (i, u), y = (j, v), g = (k, w), f = (\ell, r), z = (a, b)$, so $(a, b) \cdot (k, w) = (i, u)$, then $(a + k, (s_k b + w)\alpha^k) = (i, u)$, hence $a + k = i \implies a = i - k$. Now $(s_k b + w)\alpha^k = u \iff (s_k b + w)\alpha^{(i-k)k} = u \iff s_k b + w = u\alpha^{-(i-k)k} \iff s_k b = u\alpha^{-(i-k)k} \iff b = s_{-k}u\alpha^{-(i-k)k} - s_{-k}w$. Therefore $(a, b) = (i - k, s_{-k}u\alpha^{-(i-k)k} - s_{-k}w)$. Also $(\ell, r) \cdot (a, b) = (j, v) \iff (\ell + a, (s_\ell r + b)\alpha^\ell a) = (j, v) \iff j = \ell + a \iff a = j - \ell, (s_\ell r + b)\alpha^\ell a = v, \iff (s_{(j-\ell)r} + b)\alpha^{\ell(j-\ell)} = v \iff s_{(j-\ell)r} + b = v\alpha^{-\ell(i-\ell)} \iff b = v\alpha^{-\ell(i-\ell)} - s_{(j-\ell)r}$. Hence $(a, b) = (j - \ell, v\alpha^{-\ell(i-\ell)} - s_{(j-\ell)r})$.

So $x \circ y = ((i - k, s_{-k}u\alpha^{-(i-k)k} - s_{-k}w) \ast (j - \ell, v\alpha^{-\ell(j-\ell)} - s_{(j-\ell)r}) = (i - k + j - \ell, [s_{j-\ell}(s_{-k}u\alpha^{-(i-k)k} - s_{-k}w) + v\alpha^{-\ell(j-\ell)} - s_{(j-\ell)r}]\alpha^{(i-k)(j-\ell)} = ((i +
\[ j - (k + \ell), [s_{i-\ell-k}u\alpha^{-k(i-k)} - s_{j-\ell-k}w + v\alpha^{-\ell(j-\ell)} - s_{(j-\ell)r}]\alpha^{(i-k)(j-\ell)} = ((i + j) - (k + \ell), s_{j-\ell-k}u\alpha^{-(i-k)(j-\ell)} - s_{j-\ell-k}w\alpha^{(i-k)(j-\ell)} + v\alpha^{-\ell(i-\ell)+(i-k)(i-\ell)} - s_{(j-\ell)r}\alpha^{(i-k)(j-\ell)}). \]

We used the LOOPS package for GAP to compute the dihedral-like automorphic loops up to isotopism. The table is formatted as follows: the row called \( n \) lists the order of the loop, the row called \( \zeta_n(a) \) gives the number of dihedral-like automorphic loops of order \( n \) up to isotopism, and the row called \( \zeta_n(b) \) denotes the number of nonassociative dihedral-like automorphic loops up to isomorphism.

<table>
<thead>
<tr>
<th>( n )</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
<th>16</th>
<th>18</th>
<th>20</th>
<th>22</th>
<th>24</th>
<th>26</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \zeta_n(a) )</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>20</td>
<td>14</td>
<td>7</td>
<td>7</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>( \zeta_n(b) )</td>
<td>-</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>13</td>
<td>10</td>
<td>3</td>
<td>5</td>
<td>12</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( n )</th>
<th>28</th>
<th>30</th>
<th>32</th>
<th>34</th>
<th>36</th>
<th>38</th>
<th>40</th>
<th>42</th>
<th>44</th>
<th>46</th>
<th>48</th>
<th>50</th>
<th>52</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \zeta_n(a) )</td>
<td>8</td>
<td>11</td>
<td>?</td>
<td>10</td>
<td>?</td>
<td>11</td>
<td>25</td>
<td>13</td>
<td>10</td>
<td>13</td>
<td>?</td>
<td>?</td>
<td>11</td>
</tr>
<tr>
<td>( \zeta_n(b) )</td>
<td>4</td>
<td>7</td>
<td>?</td>
<td>8</td>
<td>?</td>
<td>8</td>
<td>17</td>
<td>9</td>
<td>6</td>
<td>11</td>
<td>?</td>
<td>?</td>
<td>7</td>
</tr>
</tbody>
</table>

Table 5.11: A list of dihedral-like automorphic loops up to isotopism

From Table 5.11 we conjectured and eventually proved the result:

**Theorem 5.3.6.** Let \( Q_1 = \text{Dih}(2, G, \alpha) \) and \( Q_2 = \text{Dih}(2, G, \alpha^{-1}) \) be dihedral-like automorphic loops. Then \( Q_1 \) is isotopic to \( Q_2 \). In particular, if \( \alpha \) is not conjugate to \( \alpha^{-1} \) in \( \text{Aut}(G) \), then \( Q_1, Q_2 \) are isotopic but not isomorphic.

**Proof.** Let \((Q_1, \cdot) = \text{Dih}(2, G, \alpha), (Q_2, \circ) = \text{Dih}(2, G, \beta)\). For \((i, u) \in Q_1\), define a bijection \( f, g, h : Q_1 \to Q_2 \) by
\[ f(i, u) = (i \oplus 1, (-u)\alpha), \quad g(i, u) = (i \oplus 1, u\alpha), \quad \text{and} \quad h(i, u) = (i, u\alpha^i). \] Then

\[
f(i, u) \circ g(j, v) = (i \oplus 1, (-u)\alpha) \circ (j \oplus 1, v\alpha),
\]

\[
= (i \oplus j, (-s_{j+1}u\alpha + v\alpha)\beta^{(i\oplus 1)(j\oplus 1)}),
\]

\[
= (i \oplus j, (s_j u + v)\alpha\beta^{(i+1)(j+1)}),
\]

on the other hand,

\[
= h((i, u) \cdot (j, v)),
\]

\[
= h(i \oplus j, (s_j u + v)\alpha^{ij}),
\]

\[
= (i \oplus j, (s_j u + v)\alpha^{ij} \alpha^{i\oplus j}).
\]

The condition \( \alpha \beta^{(i\oplus 1)(j\oplus 1)} = \alpha^{ij} \alpha^{i\oplus j} \) holds when \( \beta = \alpha^{-1} \) by inspection of all case \( i, j \in \{0, 1\} \). \( \square \)
Bibliography


GAP Codes

This is a library of GAP functions that are used in this thesis. The Loops package (Version 4.5.4) is required.

DihLoop

This function takes $m$, $G$, alpha as an input, where $m$ is a positive integer, $G$ is an abelian group, and alpha is an automorphism of $G$. The function returns the loop constructed on $\mathbb{Z}_m \times G$ by $(i, u)(j, v) = (i + j, \alpha^{ij}((-1)^j u + v))$. alpha is assumed to be given as a permutation of $\{1, \ldots, n\}$.

DihLoop := function( m, G, alpha )
    # G is an abelian group
    # loop constructed on $\mathbb{Z}_m \times G$ using an automorphism alpha of G
    # the multiplication rule is
    # $(i, u)*(j, v) = (i+j, \alpha^{i*j}((-1)^j*u + v))$
    # it is assumed that alpha is given as a permutation of $\{1,\ldots,n\}$
    local n, elms, ct, i, j, u, v, k, beta, w;
    G := IntoLoop(G);
    n := Size(G);
    elms := Elements( G );
    ct := List([1..m*n], i -> 0*[1..m*n]);
    for i in [0..m-1] do for j in [0..m-1] do for u in G do for v in G do
        k := (i+j) mod m;
        beta := alpha^(i*j);
        if IsOddInt( j ) then
            w := Position( elms, u^(-1)*v)^beta;
        else
            w := Position( elms, u*v )^beta;
        end;
    end;
end;

DihLoopReduced

This function is the same as DihLoop except that the exponents of $\alpha$ are reduced modulo $m$.

DihLoopReduced := function( m, G, alpha )
# G is an abelian group
# loop constructed on $\mathbb{Z}_m \times G$ using an automorphism alpha of G
# the multiplication rule is
# $(i,u) \ast (j,v) = (i+j, \alpha^{(i\cdot j \mod m)}((-1)^j u + v) )$
# it is assumed that alpha is given as a permutation of $\{1,..,n\}$
local n, elms, ct, i, j, u, v, k, beta, w;
G := IntoLoop(G);
n := Size(G);
elms := Elements( G );
ct := List([1..m*n], i -> 0*[1..m*n]);
for i in [0..m-1] do for j in [0..m-1] do for u in G do for v in G do
k := (i+j) mod m;
beta := alpha^((i\cdot j) mod m);
if IsOddInt( j ) then
  w := Position( elms, u^(-1)*v )^beta;
else
  w := Position( elms, u*v )^beta;
fi;
ct[i*n+Position(elms,u)][j*n+Position(elms,v)] := k*n+w;
od; od; od; od;
return LoopByCayleyTable(ct);
end;
By default, the Loops package let demand of a loop of order $n$ as $\ell_1, \ell_2, \ldots, \ell_n$. The following conversion function allow us to identify an element $\ell_i$ with ordered pair $(i, u) \in \mathbb{Z}_m \times G$. Similarly for mappings among dihedral-like automorphic loops.

\textbf{ConvertIntToPair}

\begin{verbatim}
ConvertIntToPair := function( j, m, G )
local u, i, n;
    n := Size( G );
    u := ((j-1) mod n)+1;
    i := ((j-1)-(u-1))/n;
    return [i, Elements(G)[u]];
end;
\end{verbatim}
The function is used to enumerate all dihedral-like automorphic loops up to isomorphism. It relies on Theorem 4.2.3

AllDihLoop

AllDihLoop1 := function( n, m )
    # n is the order of the resulting loop
    # m is the even parameter m
    # therefore |G| = n/m
    local lps, redlps, gps, G, A, c, C, Qs, nC, i, j, f, alpha;
    lps := [];
    gps := AllGroups( n/m );
    gps := Filtered( gps, IsAbelian );
    gps := List( gps, IntoLoop );
    for G in gps do
        A := AutomorphismGroup( G );
        C := List( ConjugacyClasses(A), x -> Random(x) );
        if m > 2 then
            C := Filtered( C, c -> Order( c ) <= 2 );
        fi;
        for c in C do
            Add( lps, DihLoop( m, G, c ) );
            #Add( redlps, DihLoopReduced( m, G, c ) );
        od;
    od;
    #return [lps, redlps];
\begin{verbatim}
return lps;
end;

AllDihLoop := function( n )
    local lps, m;
    lps := [ ];
    for m in [1..n] do
        if IsEvenInt(m) and IsInt(n/m) then
            lps := Concatenation( lps, AllDihLoop1( n, m ) );
        fi;
    od;
    return lps;
end;

The library of small dihedral-like automorphic loops is available from the author upon request.
\end{verbatim}