AUTOMORPHISMS OF DIHEDRAL-LIKE AUTOMORPHIC LOOPS

MOUNA ABORAS AND PETR VOJTĚCHOVSKÝ

Abstract. Automorphic loops are loops in which all inner mappings are automorphisms. A large class of automorphic loops is obtained as follows: Let m be a positive even integer, G an abelian group, and α an automorphism of G that satisfies $\alpha^2 = 1$ if $m > 2$. Then the *dihedral-like automorphic loop* $\mathrm{Dih}(m, G, \alpha)$ is defined on $\mathbb{Z}_m \times G$ by

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

We prove that two finite dihedral-like automorphic loops $\mathrm{Dih}(m, G, \alpha)$, $\mathrm{Dih}(\overline{m}, \overline{G}, \overline{\alpha})$ are isomorphic if and only if $m = \overline{m}$, $G = \overline{G}$, and α is conjugate to $\overline{\alpha}$ in the automorphism group of 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.

1. Introduction

A groupoid $(Q, \cdot)$ is a *quasigroup* if for every $x \in Q$ the translations

$$L_x : Q \to Q,\ yL_x = xy, \quad R_x : Q \to Q,\ yR_x = yx$$

are bijections of Q. If Q is a quasigroup with $1 \in Q$ such that $x1 = 1x = x$ holds for every $x \in Q$, then Q is a *loop*.

Given a loop Q, the *multiplication group* of Q is the permutation group

$$\mathrm{Mlt}(Q) = \langle L_x, R_x : x \in Q \rangle,$$

and the *inner mapping group* of Q is the subgroup

$$\mathrm{Inn}(Q) = \{\varphi \in \mathrm{Mlt}(Q) : 1\varphi = 1\}.$$

It is well known, cf. [2], that

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

where

$$L_{x,y} = L_x L_y L_{yx}^{-1}, \quad R_{x,y} = R_x R_y R_{xy}^{-1}, \quad T_x = R_x L_x^{-1}.$$

An *automorphic loop* (or *A-loop*) is a loop Q in which every inner mapping is an automorphism, that is, $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Note that every group is an automorphic loop, but the converse is certainly not true. The study of automorphic loops began with [3], and many structural results were obtained in [11].

2010 *Mathematics Subject Classification.* Primary: 20N05. Secondary: 20D45.

Key words and phrases. Automorphic loop, A-loop, automorphism group, dihedral-like automorphic loop, dihedral group, generalized dihedral group, dicyclic group, generalized dicyclic group, inner mapping group, multiplication group.

Research partially supported by the Simons Foundation Collaboration Grant 210176 to Petr Vojtěchovský.

1.1. **Dihedral-like automorphic loops.** Consider the following construction: Let $m > 1$ be an integer, G an abelian group, and α an automorphism of G. Define $\mathrm{Dih}(m, G, \alpha)$ on $\mathbb{Z}_m \times G$ by

$$(i, u)(j, v) = (i + j, ((-1)^j u + v)\alpha^{ij}), \tag{1.1}$$

where we assume that i, $j \in \{0, \ldots, m-1\}$ and where we do not reduce modulo m in the exponent of α. To save space, we will write

$$s_j = (-1)^j.$$

Among other results, it was proved in [1] that $\mathrm{Dih}(m, G, \alpha)$ is a loop, and that this loop is automorphic if and only if one of the following conditions hold:

- $m = 2$, or
- $m > 2$ is even and $\alpha^2 = 1$, or
- m is odd, $\alpha = 1$ and $\exp(G) \leq 2$, in which case $Q = \mathbb{Z}_m \times G$ is an abelian group.

To avoid uninteresting cases, we say in this paper that $Q = \mathrm{Dih}(m, G, \alpha)$ is a *dihedral-like automorphic loop* if either $m = 2$ or ($m > 2$ is even and $\alpha^2 = 1$).

The dihedral-like automorphic loops with $m = 2$ were first discussed in [11], particularly the case $\mathrm{Dih}(2, \mathbb{Z}_n, \alpha)$.

Dihedral-like automorphic loops are of interest because they account for many small automorphic loops. For instance, by [11, 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 $\mathrm{Dih}(2, \mathbb{Z}_p, \alpha)$.

1.2. **Notational conventions.** Throughout the paper we will use extensively the following properties and conventions:

- the word "nonassociative" means "not associative,"
- automorphic loops are power-associative [3], and hence powers and two-sided inverses are well-defined,
- the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_m$ will be denoted by E,
- since m is even, we have $s_{i \bmod m} = s_i$ for every integer i, and it therefore does not matter whether we reduce modulo m in the subscript of s_i,
- $s_{j+k} = s_j s_k$ for every j, k,
- $(s_j u)\alpha = s_j(u\alpha)$ for every j and u,
- except for the exponents of α and other automorphisms, all statements should be read modulo m. (For instance, $E = 0$ if $m = 2$.)

If $\alpha^2 = 1$ then $\alpha^i = \alpha^{i \bmod m}$ for every integer i, so it does not matter in this case whether we reduce modulo m in the exponent of α. If $\alpha^2 \neq 1$ (and thus $m = 2$) we will assume that all variables are taken from $\{0, 1\}$, and we employ $i \oplus j$ whenever necessary to distinguish the addition in $\mathbb{Z}_m$ from the addition of integers.

Consequently, we have

$$\alpha^i \alpha^j = \alpha^{i+j}$$

in all situations, a key property in calculations. Since $ij + (i \oplus j)k = i(j \oplus k) + jk$ holds for every i, j, $k \in \{0, 1\}$ when $m = 2$, we also have

$$\alpha^{ij+(i\oplus j)k} = \alpha^{i(j\oplus k)+jk} \tag{1.2}$$

in all situations.

1.3. **Groups among dihedral-like automorphic loops.** Groups are easy to spot among dihedral-like automorphic loops:

Lemma 1.1. *Let $Q = \mathrm{Dih}(m, G, \alpha)$ 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 $\mathrm{Dih}(m, G, 1)$ is a semidirect product $\mathbb{Z}_m \ltimes_\varphi G$ with multiplication

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

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

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

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

which holds, by (1.2), if and only if

$$s_{j+k}u\alpha^{ij+(i\oplus j)k} + w\alpha^{(i\oplus j)k} = s_{j+k}u\alpha^{i(j\oplus k)} + w\alpha^{jk+i(j\oplus k)}. \tag{1.3}$$

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 (1.3) reduces to the trivial identity $s_{j+k}u + w = s_{j+k}u + w$.

The rest is clear from (1.1). Note that the mapping φ 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* $\mathrm{Dih}(2, \mathbb{Z}_n, 1) = D_{2n}$, the *generalized dihedral groups* $\mathrm{Dih}(2, G, 1) = \mathrm{Dih}(G)$, and certain generalized dicyclic groups $\mathrm{Dih}(4, G, 1)$.

Recall that for an abelian group A and an element $y \in A$ of order two the *generalized dicyclic group* $\mathrm{Dic}(A, y)$ is the group generated by A and another element x such that $x^2 = y$ and $x^{-1}ax = a^{-1}$ for every $a \in A$, cf. [12, p. 170]. If $A = \mathbb{Z}_{2n}$ and y is the unique element of order two in A, then $\mathrm{Dic}(A, y) = \mathrm{Dic}_{4n}$ is the *dicyclic group*.

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

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

On the other hand, not every (generalized) dicyclic group is found among dihedral-like groups, e.g. Dic_{16}. This can be verified directly with the `LOOPS` [14] package for `GAP` [6].

1.4. **Summary of results.** In this paper we prove that two finite dihedral-like automorphic loops $\mathrm{Dih}(m, G, \alpha)$, $\mathrm{Dih}(\overline{m}, \overline{G}, \overline{\alpha})$ are isomorphic if and only if $m = \overline{m}$, $G = \overline{G}$, and α is conjugate to $\overline{\alpha}$ in $\mathrm{Aut}(G)$. We describe the automorphism groups and inner mapping groups of all finite dihedral-like automorphic loops. 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. [12, p. 169]. If $\exp(G) \leq 2$, then $\mathrm{Dih}(2, G, 1)$ is an elementary abelian 2-group whose automorphism group is the general linear group $GL(2, |G|)$. If $\exp(G) > 2$, then $\mathrm{Aut}(\mathrm{Dih}(2, G, 1))$ is the *holomorph*

$$\mathrm{Hol}(G) = \mathrm{Aut}(G) \ltimes G, \quad (\alpha, u)(\beta, v) = (\alpha\beta, u\beta + v).$$

We will recover these results as special cases.

1.5. **Related constructions.** Several recent papers deal with constructions of automorphic loops. Recall that for a loop Q, the *middle nucleus* is defined as

$$N_\mu(Q) = \{y \in Q : (xy)z = x(yz) \text{ for every } x,\, z \in Q\}.$$

Following [9], for an abelian group G and a bijection α of G, let $G(\alpha)$ be defined on $\mathbb{Z}_2 \times G$ by $(0,u)(0,v) = (0,u+v)$, $(0,u)(1,v) = (1,u+v) = (1,u)(0,v)$, $(1,u)(1,v) = (0,(u+v)\alpha)$. By [9, Corollary 2.3], every commutative loop with middle nucleus of index at most two is of the form $G(\alpha)$.

We shall see (cf. Lemma 3.1) that all dihedral-like automorphic loops have middle nucleus of index at most two. In [9, Proposition 2.7], all commutative automorphic loops with middle nucleus of index at most two are described.

Let G be an elementary abelian 2-group and $\alpha \in \mathrm{Aut}(G)$. Then $G(\alpha) = \mathrm{Dih}(2, G, \alpha)$. A special case of [9, Corollary 2.6] then says that for α, $\beta \in \mathrm{Aut}(G)$ with $\alpha \neq 1 \neq \beta$, the loops $\mathrm{Dih}(2, G, \alpha)$, $\mathrm{Dih}(2, G, \beta)$ are isomorphic if and only if α, β are conjugate in $\mathrm{Aut}(G)$.

Examples of centerless commutative automorphic loops can be found in [13]. Commutative automorphic loops of order p^3 are classified in [4]. Nuclear semidirect products that yield commutative automorphic loops are studied in [8]. Nonassociative commutative automorphic loops of order pq are constructed in [5].

Finally, [11] contains additional constructions of (not necessarily commutative) automorphic loops, as well as an extensive list of references on automorphic loops.

2. Squaring and conjugation

The squaring map $x \mapsto x^2$ and the conjugation maps T_x are key to understanding the loops $Q = \mathrm{Dih}(m, G, \alpha)$. 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.

Denote by G_2 the subgroup of G consisting of all elements of G of order at most two.

Lemma 2.1. *Let* $\mathrm{Dih}(m, G, \alpha)$ *be a finite dihedral-like automorphic loop. Then:*

(i) $(i,u)\chi \leq 2|G|$ *for every* i, u,
(ii) $(i,u)\chi = 0$ *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* $m/2$ *is even.*

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

$$2j \equiv i \pmod{m} \tag{2.1}$$

and

$$(s_j v + v)\alpha^{jj} = u. \tag{2.2}$$

Since $\mathbb{Z}_m \to \mathbb{Z}_m$, $k \mapsto 2k$ is a homomorphism with kernel $\{0, m/2\}$, the congruence (2.1) has either zero solutions or two solutions in $\mathbb{Z}_m$, proving (i).

If i is odd then (2.1) never holds, proving (ii). For the rest of the proof we can assume that i is even, and we denote by ℓ, $\ell + m/2$ the two solutions to (2.1).

Suppose that $u \neq 0$. If ℓ 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 ℓ, $\ell + m/2$ are even. Then (2.2) 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 ℓ, $\ell + m/2$ is odd. Without loss of generality, assume that ℓ is odd. With $j = \ell$, (2.2) holds for every $v \in G$. With $j = \ell + m/2$, (2.2) 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 $(2,0)\chi = 2|G|$. □

Lemma 2.2. *Let $Q = \mathrm{Dih}(m, G, 1)$ be a dihedral-like group. Then*

$$(i,u)T_{(j,v)} = (j,v)^{-1} \cdot (i,u)(j,v) = (i, (1-s_i)v + s_j u)$$

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

In particular, with $I_{(i,u)} = \{(i,u), (i,u)^{-1}\}$, 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 $(i,u)T_{(j,v)} \notin I_{(i,u)}$.*

Proof. Note that $(i,u)^{-1} = (-i, -s_i u)$. Since Q is a group and $s_{i+j} = s_i s_j$, we have

$$\begin{aligned}(i,u)T_{(j,v)} = (i,u)R_{(j,v)}L^{-1}_{(j,v)} = (j,v)^{-1} \cdot (i,u)(j,v) = \\ = (-j, -s_j v) \cdot (i+j, s_j u + v) = (i, s_{i+j}(-s_j v) + s_j u + v) = (i, (1-s_i)v + s_j u),\end{aligned}$$

as claimed. 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 $(-i,u) = (-i, -s_i u) = (i,u)^{-1}$. □

3. The isomorphism problem

Suppose that $\varphi : \mathrm{Dih}(m, G, \alpha) \to \mathrm{Dih}(\overline{m}, \overline{G}, \overline{a})$ is an isomorphism of finite dihedral-like loops. Let us first show that $m = \overline{m}$ and $G = \overline{G}$. We will need the following result, which is a combination of [11, Proposition 9.1] and [1, Lemma 4.1]. We give a short proof covering both cases. Denote by E the subgroup of $\mathbb{Z}_m$ generated by 2.

Lemma 3.1. *Let $Q = \mathrm{Dih}(m, G, \alpha)$ be a nonassociative dihedral-like automorphic loop. Then $N_\mu(Q) = E \times G$.*

Proof. Note that $(j,v) \in N_\mu(Q)$ if and only if (1.3) holds for all (i,u), $(k,w) \in Q$. Suppose that $(j,v) \in N_\mu(Q)$. With $u = 0$, $i = 1$ and $k = 0$, (1.3) becomes $w = w\alpha^j$, so $\alpha^j = 1$. Since $\alpha \neq 1$, by Lemma 1.1, we conclude that $j \in E$. Conversely, if $j \in E$, then (1.3) reduces to the trivial identity $s_k u\alpha^{ik} + w\alpha^{ik} = s_k u\alpha^{ik} + w\alpha^{ik}$, and $(j,v) \in N_\mu(Q)$ follows. □

Proposition 3.2. *Let $Q = \mathrm{Dih}(m, G, \alpha)$ 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 2.1, 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 1.1. 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 1.1. Let $I = \{x \in Q : xT_y \in I_x \text{ for every } y \in Q\}$. By Lemma 2.2, 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 $N_\mu(Q) = E \times G$ by Lemma 3.1, and we determine G as above. □

To resolve the isomorphism problem, Propositon 3.2 implies that it remains to study the situation when $\varphi : \mathrm{Dih}(m, G, \alpha) \to \mathrm{Dih}(m, G, \beta)$ is an isomorphism of finite dihedral-like automorphic loops. By Lemma 2.1, we have

$$(2,0)\varphi \in E \times 0. \tag{3.1}$$

If $\alpha \neq 1$ or $\exp(G) > 2$, then Lemmas 2.2 and 3.1 imply that

$$(0 \times G)\varphi \subseteq E \times G. \tag{3.2}$$

Note that (3.2) can be violated when $\alpha = 1$ and $\exp(G) = 2$, for instance by some automorphisms of the generalized dihedral group $\mathrm{Dih}(2, \mathbb{Z}_2 \times \mathbb{Z}_2, 1)$.

Proposition 3.3. *Suppose that $\varphi : \mathrm{Dih}(m, G, \alpha) \to \mathrm{Dih}(m, G, \beta)$ is an isomorphism of finite dihedral-like automorphic loops such that either $\alpha \neq 1$ or $\exp(G) > 2$. Then there are $\gamma \in \mathrm{Aut}(G)$ and $z \in G$ such that*

(i) $(E \times u)\varphi = E \times u\gamma$ *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 $\mathrm{Dih}(m, G, \beta)$ by $*$, and fix $u \in G$. By (3.2), $(0,u)\varphi \in E \times v$ 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 (3.1), and where the last inclusion follows from (1.1). Hence $(E \times u)\varphi \subseteq E \times v$, and the equality holds because E is finite and φ is one-to-one.

We can therefore define $\gamma : G \to G$ by $(E \times u)\varphi = E \times u\gamma$. Since φ is one-to-one, γ is one-to-one. Due to finiteness of G, γ 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 γ 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 $(1,0)\varphi * (1,u)\varphi \in ((E+1) \times z) * ((E+1) \times (z+u\gamma)) \subseteq E \times (-z + z + u\gamma)\beta = E \times u\gamma\beta$ for every $u \in G$. Hence $\alpha\gamma = \gamma\beta$, proving (iii). □

Theorem 3.4. *Two finite dihedral-like automorphic loops* $\mathrm{Dih}(m, G, \alpha)$ *and* $\mathrm{Dih}(\overline{m}, \overline{G}, \overline{\alpha})$ *are isomorphic if and only if* $m = \overline{m}$, $G = \overline{G}$ *and* α *is conjugate to* $\overline{\alpha}$ *in* $\mathrm{Aut}(G)$.

Proof. By Proposition 3.2, we can assume that $m = \overline{m}$ and $G = \overline{G}$. Let $(Q, \cdot) = \mathrm{Dih}(m, G, \alpha)$ and $(\overline{Q}, *) = \mathrm{Dih}(m, G, \overline{\alpha})$.

Suppose that $\varphi : Q \to \overline{Q}$ is an isomorphism. If $\alpha = 1$, then Q is a group by Lemma 1.1, hence $\overline{Q}$ is a group, hence $\overline{\alpha} = 1$ by Lemma 1.1, and so α, $\overline{\alpha}$ are trivially conjugate in $\mathrm{Aut}(G)$. We can therefore assume that $\alpha \neq 1 \neq \overline{\alpha}$. Then Q, $\overline{Q}$ are nonassociative by Lemma 1.1, so Proposition 3.3 implies $\alpha^\gamma = \overline{\alpha}$ for some $\gamma \in \mathrm{Aut}(G)$.

Conversely, suppose that $\alpha^\gamma = \overline{\alpha}$ for some $\gamma \in \mathrm{Aut}(G)$. Define a bijection $\varphi : Q \to \overline{Q}$ by $(i, u)\varphi = (i, u\gamma)$. Then $((i, u)(j, v))\varphi = (i + j, (s_j u + v)\alpha^{ij})\varphi = (i + j, (s_j u + v)\alpha^{ij}\gamma)$, while $(i, u)\varphi * (j, v)\varphi = (i, u\gamma) * (j, v\gamma) = (i + j, (s_j u\gamma + v\gamma)\overline{\alpha}^{ij}) = (i + j, (s_j u + v)\gamma\overline{\alpha}^{ij})$. Since $\alpha^{ij}\gamma = \gamma\overline{\alpha}^{ij}$ holds for every i, $j \in \mathbb{Z}_m$ (due to the fact that either $m = 2$ or $\alpha^2 = 1 = \overline{\alpha}^2$), we see that φ is a homomorphism. □

We recover [11, Corollary 9.4] as a special case of Theorem 3.4, using the fact that $\mathrm{Aut}(\mathbb{Z}_n)$ is a commutative group:

Corollary 3.5. *The dihedral-like automorphic loops* $\mathrm{Dih}(2, \mathbb{Z}_n, \alpha)$, $\mathrm{Dih}(2, \mathbb{Z}_n, \beta)$ *are isomorphic if and only if* $\alpha = \beta$.

4. All isomorphisms

In this section we refine Proposition 3.3 and describe all isomorphisms between finite dihedral-like automorphic loops, except for the case when both $\alpha = 1$ and $\exp(G) \leq 2$. In the next section we deal with the special case of automorphisms.

Given two finite dihedral-like automorphic loops $\mathrm{Dih}(m, G, \alpha)$ and $\mathrm{Dih}(m, G, \beta)$, let

$$\mathrm{Iso}(m, G, \alpha, \beta)$$

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

$$\mathrm{Par}(m, G, \alpha, \beta)$$

consisting of all quadruples

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

such that:

- $\gamma \in \mathrm{Aut}(G)$ 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 4.1. Let us observe the following facts about the parameters:

Let ϕ 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 $h : G \to \langle m/2\rangle \cong \mathbb{Z}_2$ 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 α-invariant subgroups of index at most 2 in G.

To facilitate the purported correspondence, define

$$\Psi : \mathrm{Iso}(m, G, \alpha, \beta) \to \mathrm{Par}(m, G, \alpha, \beta)$$

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

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

and, conversely,

$$\Phi : \mathrm{Par}(m, G, \alpha, \beta) \to \mathrm{Iso}(m, G, \alpha, \beta)$$

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

$$(i, u)\varphi = (ic + uh, (i \bmod 2)z + u\gamma). \tag{4.1}$$

Proposition 4.2. *Let* $\mathrm{Dih}(m, G, \alpha)$, $\mathrm{Dih}(m, G, \beta)$ *be finite dihedral-like automorphic loops such that either* $\alpha \neq 1$ *or* $\exp(G) > 2$. *Then* $\Psi : \mathrm{Iso}(m, G, \alpha, \beta) \to \mathrm{Par}(m, G, \alpha, \beta)$ *and* $\Phi : \mathrm{Par}(m, G, \alpha, \beta) \to \mathrm{Iso}(m, G, \alpha, \beta)$ *are mutually inverse bijections.*

Proof. Throughout the proof we write $\bar{i}$ instead of i mod 2. Let $(Q_\alpha, \cdot) = \mathrm{Dih}(m, G, \alpha)$, $(Q_\beta, *) = \mathrm{Dih}(m, G, \beta)$, and suppose that $\varphi : Q_\alpha \to Q_\beta$ is an isomorphism. By Proposition 3.3, there are $\gamma \in \mathrm{Aut}(G)$, $z \in G$, $c \in E + 1$ 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

$$(i + 1, 0)\varphi = (i, 0)\varphi * (1, 0)\varphi = (ic, \bar{i}z) * (c, z) = ((i + 1)c, (-\bar{i}z + z)\beta^{icc})$$

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

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

since uh is even. We have recovered the formula (4.1).

Since φ 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 $(0, u)\varphi * (0, v)\varphi = (uh, u\gamma) * (vh, v\gamma) = (uh + vh, u\gamma + v\gamma)$, h is a homomorphism $G \to E$. Moreover, $((0, u)(1, 0))\varphi = (1, -u)\varphi = (c - uh, z - u\gamma)$ and $(0, u)\varphi * (1, 0)\varphi = (uh, u\gamma) * (c, z) = (c + uh, -u\gamma + z)$ 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 $(1, 0)\varphi * (1, u)\varphi = (c, z) * (c + uh, z + u\gamma) \in (2c + uh) \times G$, so $\alpha h = h$. This means that $(\gamma, z, h, c) \in \mathrm{Par}(m, G, \alpha, \beta)$, and we have proved along the way that $\Psi\Phi = 1$.

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

$$\begin{aligned}((i,u)(j,v))\varphi &= (i+j, (s_j u + v)\alpha^{ij})\varphi \\ &= ((i+j)c + (s_j u + v)\alpha^{ij} h, \overline{i+j}z + (s_j u + v)\alpha^{ij}\gamma),\end{aligned}$$

and

$$\begin{aligned}(i,u)\varphi * (j,v)\varphi &= (ic + uh, \bar{i}z + u\gamma) * (jc + vh, \bar{j}z + v\gamma) \\ &= ((i+j)c + (u+v)h, (s_{jc+vh}(\bar{i}z + u\gamma) + \bar{j}z + v\gamma)\beta^{(ic+uh)(jc+vh)}).\end{aligned}$$

Since $\alpha h = h$ and $h : G \to \langle m/2 \rangle$, we see that $(s_j u + v)\alpha^{ij} h = (s_j u + v)h = (u+v)h$. 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

$$\overline{i+j}z + (s_j u + v)\alpha^{ij}\gamma = (s_j(\bar{i}z + u\gamma) + \bar{j}z + v\gamma)\beta^{ij}.$$

But $\alpha^\gamma = \beta$, so $\alpha^{ij}\gamma = \gamma\beta^{ij}$ for all i, j, and we need to show

$$\overline{i+j}z = (s_j \bar{i}z + \bar{j}z)\beta^{ij}.$$

When j is even, this reduces to the trivial identity $\bar{i}z = \bar{i}z$. When j is odd, we need to show

$$\overline{i+1}z = (-\bar{i}z + z)\beta^i.$$

When i is even, we get $z = z$. When i is odd, we get $0 = (-z + z)\beta^i$.

Hence φ is an isomorphism. From (4.1) we get $(0,u)\varphi = (uh, u\gamma)$ and $(1,0)\varphi = (c, z)$, proving $\Phi\Psi = 1$. □

Example 4.3. Let $m = 12$, $G = \mathbb{Z}_4$, let $\alpha = \beta$ be the unique nontrivial automorphism of G, and let $Q = \mathrm{Dih}(m, G, \alpha)$. Then $\mathrm{Iso}(m, G, \alpha, \beta) = \mathrm{Aut}(Q)$. There are 2 choices for γ (since $\mathrm{Aut}(G)$ 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, $|\mathrm{Aut}(Q)| = |\mathrm{Par}(m, G, \alpha, \beta)| = 64$.

Example 4.4. 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 $\alpha \in \mathrm{Aut}(G)$ be determined by $u\alpha = uv^2$, $v\alpha = v$, and $\beta \in \mathrm{Aut}(G)$ by $u\beta = uv^2$, $v\beta = v^3$. Note that $\mathrm{Aut}(G) \cong \mathrm{Dih}(2, \mathbb{Z}_4, 1)$. Let us calculate $|\mathrm{Par}(m, G, \alpha, \beta)|$. There are 4 choices for $\gamma \in \mathrm{Aut}(G)$ 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, $|\mathrm{Iso}(m, G, \alpha, \beta)| = |\mathrm{Par}(m, G, \alpha, \beta)| = 64$.

5. Automorphism groups

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

Remark 5.1. The only finite dihedral-like automorphic loops not covered by Proposition 4.2 are those loops $Q = \mathrm{Dih}(m, G, \alpha)$ with $\alpha = 1$ and G a finite abelian group of exponent at most two. A direct inspection of (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 $\mathrm{Aut}(\mathbb{Z}_r) \times \mathrm{Aut}(\mathbb{Z}_{2^s} \times \mathbb{Z}_2^t) \cong \mathbb{Z}_r^* \times \mathrm{Aut}(\mathbb{Z}_{2^s} \times \mathbb{Z}_2^t)$, and we refer the reader to [7] for more details.

For an abelian group G and an automorphism α of G let

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

and let

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

be the *centralizer* of α in $\mathrm{Aut}(G)$.

Proposition 5.2. *Let* $\mathrm{Dih}(m,G,\alpha)$ *be a finite dihedral-like automorphic loop such that either* $\alpha \neq 1$ *or* $\exp(G) > 2$. *Then*

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

Proof. This follows from Proposition 4.2, Remark 4.1, and the fact that $\alpha^\gamma = \alpha$ if and only if $\gamma \in C_{\mathrm{Aut}(G)}(\alpha)$. □

Let us write

$$\mathrm{Par}(m,G,\alpha) = \mathrm{Par}(m,G,\alpha,\alpha).$$

Proposition 4.2 allows us to describe the structure of $\mathrm{Aut}(\mathrm{Dih}(m,G,\alpha))$ by working out the multiplication formula on $\mathrm{Par}(m,G,\alpha)$.

Theorem 5.3. *Let* $Q = \mathrm{Dih}(m,G,\alpha)$ *be a finite dihedral-like automorphic loop such that either* $\alpha \neq 1$ *or* $\exp(G) > 2$. *Then* $\mathrm{Aut}(Q)$ *is isomorphic to* $(\mathrm{Par}(m,G,\alpha),\circ)$, *where*

$$(\gamma_0,z_0,c_0,h_0) \circ (\gamma_1,z_1,c_1,h_1) = (\gamma_0\gamma_1, z_0\gamma_1 + z_1, c_0c_1 + z_0h_1, h_0 + \gamma_0h_1). \tag{5.1}$$

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, (4.1) yields

$$(c_2,z_2) = (1,0)\varphi_2 = (1,0)\varphi_0\varphi_1 = (c_0,z_0)\varphi_1 = (c_0c_1 + z_0h_1, z_1 + z_0\gamma_1),$$
$$(uh_2,u\gamma_2) = (0,u)\varphi_2 = (0,u)\varphi_0\varphi_1 = (uh_0,u\gamma_0)\varphi_1 = (uh_0c_1 + u\gamma_0h_1, u\gamma_0\gamma_1).$$

The image of h_0 is contained in $\langle m/2\rangle$ and c_1 is odd, so $h_0c_1 = h_0$. We are done by Proposition 4.2. □

Here are some special cases of interest of Theorem 5.3:

Corollary 5.4. *Let* $Q = \mathrm{Dih}(m,G,\alpha)$ *be a finite dihedral-like automorphic loop such that either* $\alpha \neq 1$ *or* $\exp(G) > 2$.

(i) *If* $m/2$ *is odd then* $\mathrm{Aut}(Q) \cong (C_{\mathrm{Aut}(G)}(\alpha) \ltimes G) \times \mathbb{Z}^*_{m/2}$.
(ii) *If* $m = 2$ *then* $\mathrm{Aut}(Q) \cong C_{\mathrm{Aut}(G)}(\alpha) \ltimes G \leq \mathrm{Hol}(G)$.
(iii) *If* $\alpha = 1$ *then the projection of* $\mathrm{Aut}(Q) = (\mathrm{Par}(m,G,\alpha),\circ)$ *onto the first two coordinates is isomorphic to* $\mathrm{Hol}(G)$.
(iv) *If* $\alpha = 1$ *and* $m = 2$ *(so that* Q *is a generalized dihedral group) then* $\mathrm{Aut}(Q) \cong \mathrm{Hol}(G)$.

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 (5.1), 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 $C_{\mathrm{Aut}(G)}(\alpha) = \mathrm{Aut}(G)$, proving (iii). Part (iv) then follows from (ii) and (iii). □

6. The inner mapping groups

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

Proposition 6.1. *Let $Q = \mathrm{Dih}(m, G, \alpha)$ be a dihedral-like automorphic loop. Then*

$$\begin{aligned}(k,w)T_{(i,u)} &= (k,(1-s_k)u + s_i w),\\ (k,w)R_{(j,v),(i,u)} &= (k, w\alpha^{ij} - s_i u\alpha^{ij}(\alpha^{-jk}-1)),\\ (k,w)L_{(j,v),(i,u)} &= (k, w\alpha^{ij} + u\alpha^{ij}(\alpha^{-jk}-1)).\end{aligned}$$

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:

$$\begin{aligned}(k,w)T_{(i,u)} &= (k,t),\\ (k,w)(i,u) &= (i,u)(k,t),\\ (s_i w + u)\alpha^{ik} &= (s_k u + t)\alpha^{ik},\\ s_i w + u &= s_k u + t,\\ t &= (1-s_k)u + s_i w.\end{aligned}$$

For $R_{(j,v),(i,u)}$, the following conditions are equivalent, using (1.2):

$$\begin{aligned}(k,w)R_{(j,v),(i,u)} &= (k,t),\\ (k,w)(j,v)\cdot(i,u) &= (k,t)\cdot(j,v)(i,u),\\ (s_i(s_j w + v)\alpha^{jk} + u)\alpha^{(j\oplus k)i} &= (s_{i+j}t + (s_i v + u)\alpha^{ij})\alpha^{(i\oplus j)k},\\ s_{i+j}w\alpha^{jk+(j\oplus k)i} + u\alpha^{(j\oplus k)i} &= s_{i+j}t\alpha^{(i\oplus j)k} + u\alpha^{ij+(i\oplus j)k},\\ t &= w\alpha^{ij} + s_{i+j}u\alpha^{ij-jk} - s_{i+j}u\alpha^{ij}.\end{aligned}$$

We claim that $s_{i+j}u\alpha^{ij}(\alpha^{-jk}-1) = -s_i u\alpha^{ij}(\alpha^{-jk}-1)$. Indeed, $s_{i+j} = s_i s_j$, so we are done if j is odd, and when j is even then $\alpha^{-jk} - 1 = 0$ in both sides of the equation.

For $L_{(j,v),(i,u)}$, the following conditions are equivalent, using (1.2):

$$\begin{aligned}(k,w)L_{(j,v),(i,u)} &= (k,t),\\ (i,u)\cdot(j,v)(k,w) &= (i,u)(j,v)\cdot(k,t),\\ (s_{j+k}u + (s_k v + w)\alpha^{jk})\alpha^{i(j\oplus k)} &= (s_k(s_j u + v)\alpha^{ij} + t)\alpha^{(i\oplus j)k},\\ s_{j+k}u\alpha^{i(j\oplus k)} + w\alpha^{jk+i(j\oplus k)} &= s_{j+k}u\alpha^{ij+(i\oplus j)k} + t\alpha^{(i\oplus j)k},\\ t &= w\alpha^{ij} + s_{j+k}u\alpha^{ij-jk} - s_{j+k}u\alpha^{ij}.\end{aligned}$$

Again, we claim that $s_{j+k}u\alpha^{ij}(\alpha^{-jk}-1) = u\alpha^{ij}(\alpha^{-jk}-1)$. Indeed, if j is even or k is even then $\alpha^{-jk}-1 = 0$ in both sides, and if both j, k are odd then $s_{j+k} = 1$. □

By [10, Theorem 7.5], every automorphic loop satisfies the *antiautomorphic inverse property*, that is, $(xy)^{-1} = y^{-1}x^{-1}$. With $J : x \mapsto x^{-1}$ the inversion map, the antiautomorphic inverse property can be rewritten as $L_x J = J R_{xJ}$, so it follows that $L_{x,y}J = JR_{xJ,yJ}$. Since

$L_{x,y}$ is an automorphism in automorphic loops, we also have $L_{x,y}J = JL_{x,y}$. Altogether, we have obtained:

Lemma 6.2 ([11])**.** *In an automorphic loop,* $L_{x,y} = R_{x^{-1},y^{-1}}$.

Recall that $\mathrm{Inn}(Q) = \langle T_x, R_{x,y}, L_{x,y} : x, y \in Q\rangle$, and also consider the *right* and *left inner mapping groups*

$$\mathrm{Inn}_r(Q) = \langle R_{x,y} : x, y \in Q\rangle, \quad \mathrm{Inn}_\ell(Q) = \langle L_{x,y} : x, y \in Q\rangle.$$

Theorem 6.3. *Let* $Q = \mathrm{Dih}(m, G, \alpha)$ *be a finite dihedral-like automorphic loop such that either* $\alpha \neq 1$ *or* $\exp(G) > 2$*. Then:*

(i) $\mathrm{Inn}_r(Q) = \mathrm{Inn}_\ell(Q)$ *is isomorphic to the subgroup* $\langle\alpha\rangle \ltimes G(1-\alpha)$ *of* $\mathrm{Hol}(G)$*,*
(ii) $\mathrm{Inn}(Q) = \langle T_x, R_{x,y} : x, y \in Q\rangle = \langle T_x, L_{x,y} : x, y \in Q\rangle$ *is isomorphic to the subgroup* $(\pm\langle\alpha\rangle) \ltimes (2G + G(1-\alpha))$ *of* $\mathrm{Hol}(G)$*.*

Proof. We obtain $\mathrm{Inn}_r(Q) = \mathrm{Inn}_\ell(Q)$ and $\mathrm{Inn}(Q) = \langle T_x, R_{x,y} : x, y \in Q\rangle = \langle T_x, L_{x,y} : x, y \in Q\rangle$ as an immediate consequence of Lemma 6.2.

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

$$\begin{aligned}(\delta\alpha^i, 2u + v(1-\alpha))(\varepsilon\alpha^j, 2w + z(1-\alpha)) &= (\delta\varepsilon\alpha^{i+j}, (2u + v(1-\alpha))\varepsilon\alpha^j + 2w + z(1-\alpha)) \\ &= (\delta\varepsilon\alpha^{i+j}, 2(u\varepsilon\alpha^j + w) + (v\varepsilon\alpha^j + z)(1-\alpha)),\end{aligned}$$

since $1-\alpha$ commutes with $\pm\alpha^j$.

By Proposition 6.1, we have

$$\begin{aligned}(0,w)T_{(i,u)} &= (0, s_i w), \quad (1,0)T_{(i,u)} = (1, 2u), \\ (0,w)L_{(j,v),(i,u)} &= (0, w\alpha^{ij}), \quad (1,0)L_{(j,v),(i,u)} = (1, u\alpha^{ij}(\alpha^{-j} - 1)).\end{aligned}$$

Therefore

$$\begin{aligned}T_{(i,u)}\Psi &= (s_i, 2u, 1, 0), \\ L_{(j,v),(i,u)}\Psi &= (\alpha^{ij}, u\alpha^{ij}(\alpha^{-j} - 1), 1, 0),\end{aligned}$$

where we identity the sign s_i with the automorphism $u \mapsto s_i u$. Hence $\mathrm{Inn}(Q)$ is nontrivial only on the first two coordinates of $\mathrm{Par}(m, G, \alpha)$, and it can be identified with a subgroup of $\mathrm{Hol}(G)$, by Proposition 4.2 and Theorem 5.3.

With $u = 0$ and $i = j = 1$ we get $(\alpha, 0)$ from $L_{(j,v),(i,u)}$. Taking powers of this element, we see that $\langle\alpha\rangle \times 0 \subseteq \mathrm{Inn}_\ell(Q)$. With $i = 0$ and $j = 1$ we get $(1, u(\alpha^{-1} - 1)) = (1, u\alpha^{-1}(1-\alpha))$ from $L_{(j,v),(i,u)}$, showing that $1 \times G(1-\alpha) \subseteq \mathrm{Inn}_\ell(Q)$. Therefore $(\langle\alpha\rangle \times 0)(1 \times G(1-\alpha)) = \langle\alpha\rangle \times G(1-\alpha) \subseteq \mathrm{Inn}_\ell(Q)$. On the other hand, using the fact that either $m = 2$ or $\alpha^2 = 1$, it is easy to see that the generators $L_{(j,v),(i,u)}$ 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 $\mathrm{Inn}(Q)$, and thus $(\pm\langle\alpha\rangle) \ltimes (2G + G(1-\alpha)) \subseteq \mathrm{Inn}(Q)$. The other inclusion is again clear from an inspection of $T_{(i,u)}$. □

Corollary 6.4. *Let* $Q = \mathrm{Dih}(2, G, 1)$ *be a generalized dihedral group such that* $\exp(G) > 2$*. Then the inner automorphism group of* Q *is isomorphic to* $\mathbb{Z}_2 \ltimes 2G$*.*

Example 6.5. 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 $Q = \mathrm{Dih}(2, G, \alpha)$. Then $\pm\langle\alpha\rangle \cong \mathbb{Z}_2 \cong \langle\alpha\rangle$, and $G(1-\alpha) = 2G = G$. Therefore $\mathrm{Inn}_\ell(Q) = \mathrm{Inn}_r(Q) = \mathrm{Inn}(Q) \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_p$ is isomorphic to the dihedral group of order $2p$.

References

[1] M. Aboras, *Dihedral-like constructions of automorphic loops*, Comment. Math. Univ. Carolin. **55**, **3** (2014), 269–284.

[2] R.H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[3] R.H. Bruck and L.J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (**2**) **63** (1956), 308–323.

[4] D.A.S. De Barros, A. Grishkov and P. Vojtěchovský, *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), no. **5**, 1250100.

[5] A. Drápal, *A class of commutative loops with metacyclic inner mapping groups*, Comment. Math. Univ. Carolin. **49** (2008), no. **3**, 357–382.

[6] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.5.7; 2012. *http://www.gap-system.org.*

[7] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), no. **10**, 917–923.

[8] J. Hora and P. Jedlička, *Nuclear semidirect product of commutative automorphic loops*, J. Algebra Appl. **13** (2014), 1350077.

[9] P. Jedlička, M. Kinyon and P. Vojtěchovský, *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. **9**, 3243–3267.

[10] K.W. Johnson, M.K. Kinyon, G.P. Nagy and P. Vojtěchovský, *Searching for small simple automorphic loops*, London Mathematical Society Journal of Computation and Mathematics **14** (2011), 200–213.

[11] M.K. Kinyon, K. Kunen, J.D. Phillips, and P. Vojtěchovský, *The structure of automorphic loops*, to appear in Transactions of the American Mathematical Society.

[12] G.A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and Applications of Finite Groups*, John Wiley & Sons, Inc., 1916.

[13] G.P. Nagy, *On centerless commutative automorphic loops*, Comment. Math. Univ. Carolin. **55**, **4** (2014), 485–491.

[14] G.P. Nagy and P. Vojtěchovský, LOOPS: Computing with quasigroups and loops, version 2.2.0, a package for GAP, available at `http://www.math.du.edu/loops`.

Department of Mathematics, University of Denver, 2280 S Vine St, Denver, Colorado 80208, U.S.A.

E-mail address, Aboras: `mmrm9804@yahoo.com`

E-mail address, Vojtěchovský: `petr@math.du.edu`