

# DIHEDRAL-LIKE CONSTRUCTIONS OF AUTOMORPHIC LOOPS

MOUNA ABORAS

ABSTRACT. Automorphic loops are loops in which all inner mappings are automorphisms. We study a generalization of the dihedral construction for groups. Namely, if  $(G, +)$  is an abelian group,  $m \geq 1$  and  $\alpha \in \text{Aut}(G)$ , let  $\text{Dih}(m, G, \alpha)$  be defined on  $\mathbb{Z}_m \times G$  by

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

The resulting loop is automorphic if and only if  $m = 2$  or  $(\alpha^2 = 1$  and  $m$  is even). The case  $m = 2$  was introduced by Kinyon, Kunen, Phillips, and Vojtěchovský. We present several structural results about the automorphic dihedral loops in both cases.

## 1. INTRODUCTION

A set  $Q$  with a binary operation  $(\cdot)$  is a *loop* if for every  $x \in Q$  the right and left translations  $R_x, L_x : Q \rightarrow Q$ ,  $yR_x = y \cdot x$ ,  $yL_x = x \cdot y$  are bijections of  $Q$ , and if there is a neutral element  $1 \in Q$  such that  $1 \cdot x = x \cdot 1 = x$  for every  $x \in Q$ .

Let  $Q$  be a loop. The group generated by  $R_x$  and  $L_x$  for all  $x \in Q$  is called the *multiplication group* of  $Q$  and it is denoted by  $\text{Mlt}(Q)$ . The subgroup of  $\text{Mlt}(Q)$  stabilizing the neutral element of  $Q$  is called the *inner mapping group* of  $Q$  and it is denoted by  $\text{Inn}(Q)$ . It is well known that the inner mapping group  $\text{Inn}(Q)$  is the permutation group generated by

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

where  $x, y \in Q$ .

A loop is *automorphic* (also known as *A-loop*) if  $\text{Inn}(Q) \leq \text{Mlt}(Q)$ , 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.

Automorphic loops were first studied in 1956 by Bruck and Paige [3]. Structure theory for commutative and general automorphic loops was developed in [1], [5], [6]. In this paper, we generalize a construction of dihedral automorphic loops introduced by Kinyon, Kunen, Phillips and Vojtěchovský [1], where they focused on the special case  $m = 2$ . Here, we consider for an integer  $m \geq 1$ , an abelian group  $(G, +)$  and an automorphism  $\alpha$  of  $G$  the loop  $\text{Dih}(m, G, \alpha)$  defined on  $\mathbb{Z}_m \times G$  by

$$(1) \quad (i, u)(j, v) = (i \oplus j, (s_j u + v)\alpha^{ij}),$$

where  $s_j = (-1)^{j \bmod m}$ , and where we interpret  $\alpha^{ij}$  as ordinary integral exponent. To make the multiplication formula unambiguous we demand that  $i, j \in \{0, 1, \dots, m-1\}$ . Then we

---

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

*Key words and phrases*. Dihedral automorphic loop, automorphic loop, inner mapping group, multiplication group, nucleus, commutant, center, commutator, associator subloop, derived subloop.

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

have  $\alpha^i \alpha^j = \alpha^{i+j}$ . There are several observations that we will use without reference for  $i, j \in \mathbb{Z}_m, u \in G$ :

- $s_i(s_j u) = (s_i s_j)u$ , so we can write this as  $s_i s_j u$ ,
- $s_i s_j u = s_j s_i u$ ,
- $s_i(u\alpha) = (s_i u)\alpha$ ,
- $s_i s_j = s_{i \oplus j}$ , when  $m$  is even.

Note that with  $m = 1$  the multiplication (1) reduces to  $(i, u)(j, v) = (i + j, u + v)$ , so  $\text{Dih}(1, G, \alpha) = \mathbb{Z}_1 \times G = G$ . We will thus assume throughout the paper that  $m > 1$ .

This paper is organized as follows: Section 2 presents definitions and preliminary results about A-loops. We recall without proofs some facts from [1]. In Section 3 we determine all parameters  $m, G, \alpha$  that yield automorphic loops. In Section 4 we show how to obtain the nuclei, the commutant and the center. In Section 5 we calculate the associator subloop  $A(Q)$  and the derived subloop  $Q'$ .

## 2. DEFINITIONS AND PRELIMINARY RESULTS

In this section we introduce relevant definitions of loop theory [2], and we present some results on automorphic loops.

**Definition 2.1.** *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  $x \cdot y = y^{n-1} \cdot x$ .*

The group  $D_{2n}$  is isomorphic to  $\text{Dih}(2, \mathbb{Z}_n, 1)$ . The generalized dihedral group  $D_{2n}(G)$  is isomorphic to  $\text{Dih}(2, G, 1)$ .

Since it suffices to check the automorphic condition on the generators of  $\text{Inn}(Q)$ , we see that a loop  $Q$  is an automorphic loop if and only if, for all  $x, y, u, v \in Q$ ,

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

In fact it is not necessary to verify all of the conditions  $(A_r)$ ,  $(A_\ell)$  and  $(A_m)$ :

**Proposition 2.2** ([4]). *Let  $Q$  be a loop satisfying  $(A_m)$  and  $(A_\ell)$ . Then  $Q$  is automorphic.*

**Definition 2.3.** *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,*

$$C(Q) = \{a \in Q : x \cdot a = a \cdot x, \forall x \in Q\}.$$

**Definition 2.4.** *The left, right, and middle nucleus of a loop  $Q$  are defined, respectively, by*

$$\begin{aligned} N_\lambda(Q) &= \{a \in Q : ax \cdot y = a \cdot xy, \forall x, y \in Q\}, \\ N_\rho(Q) &= \{a \in Q : xy \cdot a = x \cdot ya, \forall x, y \in Q\}, \\ N_\mu(Q) &= \{a \in Q : xa \cdot y = x \cdot ay, \forall x, y \in Q\}. \end{aligned}$$

*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.

**Definition 2.5.** 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

$$Z(Q) = C(Q) \cap N(Q).$$

**Definition 2.6.** Let  $S$  be a subloop of a loop  $Q$ . Then  $S$  is normal if for all  $a, b \in Q$

$$aS = Sa, (aS)b = a(Sb), a(bS) = (ab)S.$$

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

**Proposition 2.7** ([3]). Let  $Q$  be an automorphic loop. Then:

- (i)  $N_\lambda(Q) = N_\rho(Q) \subseteq N_\mu(Q)$ .
- (ii) Each nucleus is normal in  $Q$ .

**Definition 2.8.** 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 2.9.** 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 2.10.** The derived subloop of a loop  $Q$ , denoted by  $Q'$ , is the smallest normal subloop of  $Q$  containing all commutators  $[x, y]$  and all associators  $[x, y, z]$  of  $Q$ . Equivalently,  $Q'$  is the smallest normal subloop of  $Q$  such that  $Q/Q'$  is a commutative group.

### 3. PARAMETERS THAT YIELD AUTOMORPHIC LOOPS

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 3.1.** Let  $Q = \text{Dih}(m, G, 1)$ . Then  $Q$  is a group iff  $m$  is even or  $2G = 0$ .

*Proof.* With  $\alpha = 1$  the multiplication formula (1) becomes  $(i, u)(j, v) = (i \oplus j, s_j u + v)$ . We have

$$\begin{aligned} (i, u)(j, v) \cdot (k, w) &= (i \oplus j, s_j u + v)(k, w) = (i \oplus j \oplus k, s_k(s_j u + v) + w), \\ (i, u) \cdot (j, v)(k, w) &= (i, u)(j \oplus k, s_k v + w) = (i \oplus j \oplus k, s_{j \oplus k} u + s_k v + w), \end{aligned}$$

so  $Q$  is a group iff

$$(2) \quad s_k s_j u = s_{j \oplus k} u$$

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

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

**3.1. Middle inner mappings.** Recall that  $yT_x = x \setminus (yx)$ .

**Lemma 3.2.** *Let  $Q = \text{Dih}(m, G, \alpha)$  and  $(i, u), (j, v) \in Q$ . Then*

$$(3) \quad (j, v)T_{(i, u)} = (j, s_i v + (1 - s_j)u).$$

*Proof.* Note that  $(j, v)T_{(i, u)} = (k, w)$  iff  $(j, v)(i, u) = (i, u)(k, w)$  iff  $(j \oplus i, (s_i v + u)\alpha^{ij}) = (i \oplus k, (s_k u + w)\alpha^{ik})$ . We deduce  $k = j$ , and extend the chain of equivalences with  $(s_i v + u)\alpha^{ij} = (s_j u + w)\alpha^{ij}$  iff  $s_i v + u = s_j u + w$  iff  $w = s_i v + (1 - s_j)u$ .  $\square$

**Lemma 3.3.** *Let  $Q = \text{Dih}(m, G, \alpha)$  and  $(i, u) \in Q$ . Then  $T_{(i, u)} \in \text{Aut}(Q)$  iff*

$$(4) \quad (1 - s_{j \oplus k})u = (1 - s_j s_k)u\alpha^{jk}$$

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

*Proof.* We will use (3) without reference. We have

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

while

$$\begin{aligned} (j, v)T_{(i, u)} \cdot (k, w)T_{(i, u)} &= (j, s_i v + (1 - s_j)u) \cdot (k, s_i w + (1 - s_k)u) \\ &= (j \oplus k, [s_k(s_i v + (1 - s_j)u) + s_i w + (1 - s_k)u]\alpha^{jk}) \\ &= (j \oplus k, s_k s_i v \alpha^{jk} + s_i w \alpha^{jk} + [(s_k - s_k s_j + 1 - s_k)u]\alpha^{jk}) \\ &= (j \oplus k, s_k s_i v \alpha^{jk} + s_i w \alpha^{jk} + (1 - s_k s_j)u\alpha^{jk}), \end{aligned}$$

so  $T_{(i, u)} \in \text{Aut}(Q)$  iff (4) holds for every  $j, k \in \mathbb{Z}_m$ .  $\square$

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

**Proposition 3.4.** *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  $\alpha^2 \upharpoonright_{2G} = 1_{2G}$ .*

*Proof.* Consider  $T_{(i, u)}$ . Suppose that  $m = 2$ . A quick inspection of all cases  $j, k \in \{0, 1\}$  shows that (4) always holds.

Suppose that  $m > 2$  is odd. With  $j = 2$  and  $k = m - 1$ , condition (4) becomes  $(1 - s_{2 \oplus (m-1)})u = (1 - s_2 s_{m-1})u\alpha^{2(m-1)}$ , or  $2u = 0$ , so we certainly must have  $2G = 0$  for every  $T_{(i, u)}$  to be an automorphism. Conversely, when  $2G = 0$  then (4) reduces to  $0 = 0$ .

Suppose that  $m > 2$  is even. Then (4) becomes  $(1 - s_{j \oplus k})u = (1 - s_j s_k)u\alpha^{jk}$ . When  $j \oplus k$  is even then this becomes  $0 = 0$ . Suppose that  $j \oplus k$  is odd. Then one of  $j, k$  is odd and the other is even, so that  $jk$  is even, and (4) becomes  $2u = (2u)\alpha^{2\ell}$  for some  $\ell$ . With  $j = 2, k = 1$  we obtain  $2u = (2u)\alpha^2$ , which is equivalent to  $\alpha^2 \upharpoonright_{2G} = 1_{2G}$ . Conversely, when  $\alpha^2 \upharpoonright_{2G} = 1_{2G}$  then (4) holds.  $\square$

**3.2. Left inner mappings.** Recall that  $zL_{x,y} = (yx)\backslash(y(xz))$ .

**Lemma 3.5.** *Let  $Q = \text{Dih}(m, G, \alpha)$  and  $(i, u), (j, v), (k, w) \in Q$ . Then*

$$(5) \quad (k, w)L_{(j,v),(i,u)} = (k, s_{j\oplus k}u\alpha^{i(j\oplus k)-(i\oplus j)k} + s_kv\alpha^{jk+i(j\oplus k)-(i\oplus j)k} \\ + w\alpha^{jk+i(j\oplus k)-(i\oplus j)k} - s_ks_ju\alpha^{ij} - s_kv\alpha^{ij}).$$

*Proof.* The following conditions are equivalent:

$$\begin{aligned} (k, w)L_{(j,v),(i,u)} &= (\ell, x), \\ (i, u) \cdot (j, v)(k, w) &= (i, u)(j, v) \cdot (\ell, x), \\ (i, u)(j \oplus k, (s_kv + w)\alpha^{jk}) &= (i \oplus j, (s_ju + v)\alpha^{ij})(\ell, x), \\ (i \oplus j \oplus k, (s_{j\oplus k}u + (s_kv + w)\alpha^{jk})\alpha^{i(j\oplus k)}) &= (i \oplus j \oplus \ell, (s_\ell(s_ju + v)\alpha^{ij} + x)\alpha^{(i\oplus j)\ell}). \end{aligned}$$

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

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

□

**Lemma 3.6.** *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*

$$(6) \quad \begin{aligned} &s_\ell s_{j\oplus k}u\alpha^{i(j\oplus k)-(i\oplus j)k+k\ell} + s_\ell s_kv\alpha^{jk+i(j\oplus k)-(i\oplus j)k+k\ell} + s_\ell w\alpha^{jk+i(j\oplus k)-(i\oplus j)k+k\ell} \\ &\quad - s_\ell s_ks_ju\alpha^{ij+k\ell} - s_\ell s_kv\alpha^{ij+k\ell} + s_{j\oplus \ell}u\alpha^{i(j\oplus \ell)-(i\oplus j)\ell+k\ell} \\ &\quad + s_\ell v\alpha^{j\ell+i(j\oplus \ell)-(i\oplus j)\ell+k\ell} + x\alpha^{j\ell+i(j\oplus \ell)-(i\oplus j)\ell+k\ell} - s_\ell s_ju\alpha^{ij+k\ell} - s_\ell v\alpha^{ij+k\ell} \\ &= s_{j\oplus k\oplus \ell}u\alpha^{i(j\oplus k\oplus \ell)-(i\oplus j)(k\oplus \ell)} + s_{k\oplus \ell}v\alpha^{j(k\oplus \ell)+i(j\oplus k\oplus \ell)-(i\oplus j)(k\oplus \ell)} \\ &\quad + s_\ell w\alpha^{k\ell+j(k\oplus \ell)+i(j\oplus k\oplus \ell)-(i\oplus j)(k\oplus \ell)} + x\alpha^{k\ell+j(k\oplus \ell)+i(j\oplus k\oplus \ell)-(i\oplus j)(k\oplus \ell)} \\ &\quad - s_{k\oplus \ell} s_ju\alpha^{ij} - s_{k\oplus \ell} v\alpha^{ij} \end{aligned}$$

for every  $k, \ell \in \mathbb{Z}_m$  and every  $w, x \in G$ .

*Proof.* This follows from Lemma 3.5, upon comparing  $(k, w)L_{(j,v),(i,u)} \cdot (\ell, x)L_{(j,v),(i,u)}$  with  $((k, u)(\ell, x))L_{(j,v),(i,u)}$ . □

Let us call a loop satisfying  $(A_\ell)$  a *left automorphic loop*. We deduce that  $Q = \text{Dih}(m, G, \alpha)$  is a left automorphic loop iff (6) 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 (6) yields the condition

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

With  $\ell = 0$  this further simplifies to

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

which is equivalent to

$$(7) \quad \alpha^{ij+(i\oplus j)k} = \alpha^{i(j\oplus k)+jk}.$$

Suppose that (7) holds for every  $i, j, k$ . Then the automorphisms at  $w$  in (6) agree since

$$\alpha^{jk+i(j\oplus k)-(i\oplus j)k} = \alpha^{ij+(i\oplus j)k-(i\oplus j)k} = \alpha^{ij} = \alpha^{ij+(i\oplus j)(k\oplus \ell)-(i\oplus j)(k\oplus \ell)} = \alpha^{i(j\oplus k\oplus \ell)+j(k\oplus \ell)-(i\oplus j)(k\oplus \ell)}.$$

Focusing on  $x$  in (6), the following conditions are equivalent:

$$\begin{aligned}\alpha^{j\ell+i(j\oplus\ell)-(i\oplus j)\ell+k\ell} &= \alpha^{k\ell+j(k\oplus\ell)+i(j\oplus k\oplus\ell)-(i\oplus j)(k\oplus\ell)}, \\ \alpha^{j\ell+i(j\oplus\ell)-(i\oplus j)\ell} &= \alpha^{j(k\oplus\ell)+i(j\oplus k\oplus\ell)-(i\oplus j)(k\oplus\ell)}, \\ \alpha^{j\ell+i(j\oplus\ell)+(i\oplus j)(k\oplus\ell)} &= \alpha^{j(k\oplus\ell)+i(j\oplus k\oplus\ell)+(i\oplus j)\ell}, \\ \alpha^{ij+(i\oplus j)\ell+(i\oplus j)(k\oplus\ell)} &= \alpha^{ij+(i\oplus j)(k\oplus\ell)+(i\oplus j)\ell},\end{aligned}$$

where we have used (7) twice in the last step. Since the last identity is trivially true, we see that (7) implies that the automorphisms at  $x$  in (6) agree, too. Let us now focus on  $v$  in (6). Using (7), the following conditions are equivalent:

$$\begin{aligned}s_\ell s_k v \alpha^{jk+i(j\oplus k)-(i\oplus j)k+k\ell} - s_\ell s_k v \alpha^{ij+k\ell} + s_\ell v \alpha^{j\ell+i(j\oplus\ell)-(i\oplus j)\ell+k\ell} - s_\ell v \alpha^{ij+k\ell} \\ = s_{k\oplus\ell} v \alpha^{j(k\oplus\ell)+i(j\oplus k\oplus\ell)-(i\oplus j)(k\oplus\ell)} - s_{k\oplus\ell} v \alpha^{ij}, \\ s_\ell s_k v \alpha^{ij+(i\oplus j)k-(i\oplus j)k+k\ell} - s_\ell s_k v \alpha^{ij+k\ell} + s_\ell v \alpha^{ij+(i\oplus j)\ell-(i\oplus j)\ell+k\ell} - s_\ell v \alpha^{ij+k\ell} \\ = s_{k\oplus\ell} v \alpha^{ij+(i\oplus j)(k\oplus\ell)-(i\oplus j)(k\oplus\ell)} - s_{k\oplus\ell} v \alpha^{ij}.\end{aligned}$$

Upon canceling several  $\alpha^{n-n}$  and the automorphism  $\alpha^{ij}$  present in all summands, we see that the above is equivalent to

$$s_\ell s_k v \alpha^{k\ell} - s_\ell s_k v \alpha^{k\ell} + s_\ell v \alpha^{k\ell} - s_\ell v \alpha^{k\ell} = s_{k\oplus\ell} v - s_{k\oplus\ell} v,$$

which is trivially true. Hence (7) implies that the automorphisms at  $v$  in (6) agree, too. Finally, we focus on  $u$  in (6). Note that

$$\alpha^{i(j\oplus\ell)-(i\oplus j)\ell} = \alpha^{ij-j\ell}$$

immediately follows from (7). Using this identity, the following conditions are equivalent:

$$\begin{aligned}s_\ell s_{j\oplus k} u \alpha^{i(j\oplus k)-(i\oplus j)k+k\ell} - s_\ell s_k s_j u \alpha^{ij+k\ell} + s_{j\oplus\ell} u \alpha^{i(j\oplus\ell)-(i\oplus j)\ell+k\ell} - s_\ell s_j u \alpha^{ij+k\ell} \\ = s_{j\oplus k\oplus\ell} u \alpha^{i(j\oplus(k\oplus\ell))-(i\oplus j)(k\oplus\ell)} - s_{k\oplus\ell} s_j u \alpha^{ij}, \\ s_\ell s_{j\oplus k} u \alpha^{ij-jk+k\ell} - s_\ell s_k s_j u \alpha^{ij+k\ell} + s_{j\oplus\ell} u \alpha^{ij-j\ell+k\ell} - s_\ell s_j u \alpha^{ij+k\ell} \\ = s_{j\oplus k\oplus\ell} u \alpha^{ij-j(k\oplus\ell)} - s_{k\oplus\ell} s_j u \alpha^{ij}, \\ s_\ell s_{j\oplus k} u \alpha^{-jk+k\ell} - s_\ell s_k s_j u \alpha^{k\ell} + s_{j\oplus\ell} u \alpha^{-j\ell+k\ell} - s_\ell s_j u \alpha^{k\ell} \\ = s_{j\oplus k\oplus\ell} u \alpha^{-j(k\oplus\ell)} - s_{k\oplus\ell} s_j u.\end{aligned}$$

Upon rearranging, we obtain the identity

$$(8) \quad s_\ell s_{j\oplus k} u \alpha^{-jk+k\ell} + s_{j\oplus\ell} u \alpha^{-j\ell+k\ell} + s_{k\oplus\ell} s_j u = s_\ell s_k s_j u \alpha^{k\ell} + s_\ell s_j u \alpha^{k\ell} + s_{j\oplus k\oplus\ell} u \alpha^{-j(k\oplus\ell)}.$$

We have proved:

**Lemma 3.7.** *Let  $Q = \text{Dih}(m, G, \alpha)$ . Then  $Q$  is left automorphic iff (7) and (8) hold for every  $i, j, k, \ell \in \mathbb{Z}_m$  and every  $u \in G$ .*

Let us now analyze the two conditions (7) and (8).

**Lemma 3.8.** *Let  $Q = \text{Dih}(m, G, \alpha)$ . If  $m = 2$  then (7) holds. If  $m > 2$  then (7) holds iff  $\alpha^m = 1$ .*

*Proof.* Consider the condition

$$(9) \quad ij + (i \oplus j)k = i(j \oplus k) + jk.$$

When  $m = 2$  then (9) holds by a quick inspection of the cases, and thus (7) holds as well. Suppose that  $m > 2$ . With  $i = j = 1, k = m - 1$  the condition (9) reduces to  $1 + 2(m - 1) = 1 \cdot 0 + m - 1$ , or  $m = 0$ , thus if (7) holds then  $\alpha^m = 1$ . Conversely, if  $\alpha^m = 1$ , then (7) holds because (9) is valid modulo  $m$ .  $\square$

**Lemma 3.9.** *Let  $Q = \text{Dih}(m, G, \alpha)$ . If (7) and (8) hold then  $\alpha^{m-2} = 1$ .*

*Proof.* When  $m = 2$  the conclusion is trivially true. Let us therefore assume that  $m > 2$  and, using Lemma 3.8, that  $\alpha^m = 1$ . Let  $k = 1, j = \ell = m - 1$ . Then (8) becomes

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

or, equivalently,

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

Since  $s_{m-1} = -s_{m-2}$  and  $(m - 1)^2 \equiv 1 \pmod{m}$ , the last identity is equivalent to  $u = u\alpha^{-1+m-1} = u\alpha^{m-2}$ , or to  $\alpha^{m-2} = 1$ .  $\square$

**Lemma 3.10.** *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  $\alpha = 1$ .*

*Proof.* By Lemma 3.7,  $Q$  satisfies (7) and (8). Suppose that  $m > 2$ . Then Lemma 3.8 implies  $\alpha^m = 1$  and Lemma 3.9 implies  $\alpha^{m-2} = 1$ . Thus  $\alpha^2 = 1$ . If  $m$  is also odd then  $\alpha^2 = 1$  and  $\alpha^m = 1$  imply  $\alpha = 1$ .  $\square$

**Lemma 3.11.** *Let  $Q = \text{Dih}(m, G, \alpha)$ .*

- (i) *If  $m = 2$  then (8) holds.*
- (ii) *If  $m$  is even and  $\alpha^2 = 1$  then (8) holds.*
- (iii) *If  $m > 2$  is odd and  $\alpha = 1$  then (8) implies  $2G = 0$ .*

*Proof.* Suppose that  $m = 2$ . We can then reduce all subscripts modulo 2 in (8) and use  $s_i s_j = s_{i+j}$ . Hence (8) becomes

$$(10) \quad s_{\ell+j+k}u\alpha^{-jk+k\ell} + s_{j+\ell}u\alpha^{-j\ell+k\ell} + s_{k+\ell+j}u = s_{\ell+k+j}u\alpha^{k\ell} + s_{\ell+j}u\alpha^{k\ell} + s_{j+k+\ell}u\alpha^{-j(k\oplus\ell)}.$$

where all subscripts are reduced modulo 2. When  $j$  is even (that is,  $j=0$ ), (10) 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, (10) 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, (10) becomes

$$u\alpha^{-1} - u + u = u - u + u\alpha^{-1},$$

again true. Finally, if  $j, k, \ell$  are odd, (10) 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 (8) 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 (8) 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  $2u = 0$ .  $\square$

**Proposition 3.12.** *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 3.7 without reference.

Suppose that  $m = 2$ . Then (7) holds by Lemma 3.8 and (8) holds by Lemma 3.11.

Suppose that  $m > 2$  is even. If  $Q$  is left automorphic then  $\alpha^2 = 1$  by Lemma 3.10. Conversely, suppose that  $\alpha^2 = 1$ . Then (8) holds by Lemma 3.11. Since also  $\alpha^m = 1$ , (7) holds by Lemma 3.8.

Finally, suppose that  $m > 2$  is odd. If  $Q$  is left automorphic then  $\alpha = 1$  by Lemma 3.10. By Lemma 3.11,  $2G = 0$ . Conversely, suppose that  $\alpha = 1$  and  $2G = 0$ . Then  $Q$  is a group by Lemma 3.1, so certainly also a left automorphic loop.  $\square$

### 3.3. Main result.

**Theorem 3.13.** *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 (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, 3.4 and 3.12.  $\square$

From now on we will refer to loops  $Q = \text{Dih}(m, G, \alpha)$  that are automorphic (equivalently, that satisfy the conditions of Theorem 3.13) as *dihedral automorphic loops*. Since nonassociative examples of dihedral automorphic loops are obtained only when  $m = 2$  or when  $m > 2$  is even and  $\alpha^2 = 1$ , we will from now on safely write  $s_i s_j = s_{i+j} = s_{i \oplus j}$ , and we do not have to reduce exponents of  $\alpha$  modulo  $m$ .

*Remark 3.14.* If in the multiplication formula (1) we also reduce in the exponent of  $\alpha$  (that is, we have  $(i, u) \cdot (j, v) = (i \oplus j, (s_j u + v) \alpha^{ij \pmod{m}})$ ), then the resulting loop  $\text{Dih}_{\text{red}}(m, G, \alpha)$  is not necessarily isomorphic to  $\text{Dih}(m, G, \alpha)$ . However, it can be shown that  $\text{Dih}_{\text{red}}(m, G, \alpha) = \text{Dih}(m, G, \alpha)$  whenever one of the loops is automorphic. See [7] for details.

## 4. NUCLEI, COMMUTANT AND CENTER

In this section we calculate the nuclei, the commutant and the center of dihedral automorphic loops satisfying  $\alpha^2 = 1$ . (So we do not always cover the case  $m = 2$ ,  $\alpha^2 \neq 1$ .)

**Lemma 4.1.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop such that  $\alpha^2 = 1$ . If  $\alpha = 1$  then  $N_\mu(Q) = Q$ , else  $N_\mu(Q) = \langle 2 \rangle \times G$ .*



*Proof.* If  $\alpha = 1$  then  $Q$  is a group and thus  $N_\mu(Q) = Q$ . Suppose that  $\alpha \neq 1$ . Note that in automorphic loops (that satisfy (7) by Lemma 3.7) the formula of Lemma 3.5 simplifies to

$$(11) \quad (k, w)L_{(j,v),(i,u)} = (k, s_{j+k}u\alpha^{ij-jk} + s_k v\alpha^{ij} + w\alpha^{ij} - s_k s_j u\alpha^{ij} - s_k v\alpha^{ij}) \\ = (k, s_{j+k}u\alpha^{ij-jk} - s_k s_j u\alpha^{ij} + w\alpha^{ij}).$$

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

$$(12) \quad s_{j+k}u\alpha^{ij-jk} - s_k s_j u\alpha^{ij} + w\alpha^{ij} = w$$

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. Because  $\alpha \neq 1 = \alpha^2$ , we obtain  $j \in \langle 2 \rangle$ . Conversely, if  $j \in \langle 2 \rangle$  then (12) holds thanks to  $s_{j+k} = s_k s_j$  (since  $m$  is even).  $\square$

For an abelian group  $G$  and  $\alpha \in \text{Aut}(G)$ , let  $G_2 = \{u \in G : |u| \leq 2\}$ ,  $\text{Fix}(\alpha) = \{u \in G : u = u\alpha\}$  and  $\text{Fix}(\alpha)_2 = G_2 \cap \text{Fix}(\alpha)$ .

**Lemma 4.2.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop with  $\alpha^2 = 1$ . If  $\alpha = 1$  then  $N(Q) = N_\lambda(Q) = N_\rho(Q) = Q$ , else  $N(Q) = N_\lambda(Q) = N_\rho(Q) = \langle 2 \rangle \times \text{Fix}(\alpha)$ .*

*Proof.* Recall that  $N(Q) = N_\lambda(Q) = N_\rho(Q) \leq N_\mu(Q)$  in all automorphic loops. We are again done if  $\alpha = 1$ , so suppose that  $\alpha \neq 1$ . Note that  $(i, u) \in N_\lambda(Q)$  iff  $(k, w)L_{(j,v),(i,u)} = (k, w)$  for all  $(j, v), (k, w) \in Q$ . We deduce from (11) that  $(i, u) \in N_\lambda(Q)$  iff (12) holds for all  $(j, v), (k, w)$ .

If  $(i, u) \in N_\lambda(Q)$  then  $i \in \langle 2 \rangle$  by Lemma 4.1, so (12) reduces to  $s_{j+k}u\alpha^{-jk} - s_{j+k}u = 0$ , i.e.,  $u\alpha^{-jk} = u$  for all  $j, k$ . With  $j = k = 1$  we see that  $u \in \text{Fix}(\alpha)$ . Conversely, if  $u \in \text{Fix}(\alpha)$  and  $i \in \langle 2 \rangle$  then (12) clearly holds.  $\square$

Recall that the commutant  $C(Q)$  is not necessarily a (normal) subloop of a loop  $Q$ .

**Lemma 4.3.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop such that  $\alpha^2 = 1$ . Then:*

- (i) *If  $\exp(G) \leq 2$  then  $C(Q) = Q$ .*
- (ii) *If  $\exp(G) > 2$  then  $C(Q) = \langle 2 \rangle \times G_2$ .*

*In either case,  $C(Q) \trianglelefteq Q$ .*

*Proof.* By Lemma 3.2,  $(i, u) \in C(Q)$  iff

$$(13) \quad s_i v + (1 - s_j)u = v$$

holds for all  $(j, v) \in Q$ . If  $\exp(G) = 2$  then (13) holds. If  $\exp(G) > 2$  then (13) holds for all  $(j, v)$  iff  $i \in \langle 2 \rangle$  and  $u \in G_2$ . Hence if  $\exp(G) > 2$  then  $C(Q) = \langle 2 \rangle \times G_2$ .

Note that  $\langle 2 \rangle \times G$  is a group. 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 3.2,  $(j, v)T_{(i,u)} \in \{(j, \pm v)\} \in C(Q)$ . If  $(k, w) \in C(Q)$  then, by (11),  $(k, w)L_{(j,v),(i,u)} = (k, s_j u\alpha^{ij} - s_j u\alpha^{ij} + w\alpha^{ij}) \in \{(k, w), (k, w\alpha)\} \in C(Q)$ . The proof is similar for right inner mappings. Hence  $C(Q) \trianglelefteq Q$ .  $\square$

**Lemma 4.4.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop such that  $m$  is even and  $\alpha^2 = 1$ . 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  $Z(Q) = \langle 2 \rangle \times \text{Fix}(\alpha)_2$ .*

*Proof.* Suppose that  $\alpha = 1$ . Then  $Q$  is a group and  $Z(Q) = C(Q)$ . If  $\exp(G) \leq 2$  then  $Z(Q) = Q$  by Lemma 4.3. If  $\exp(G) > 2$  then  $C(Q) = \langle 2 \rangle \times G_2 = \langle 2 \rangle \times \text{Fix}(\alpha)_2$ , by Lemma 4.3.

Now suppose that  $\alpha \neq 1 = \alpha^2$ . If  $\exp(G) \leq 2$  then  $C(Q) = Q$  and  $Z(Q) = N(Q) = \langle 2 \rangle \times \text{Fix}(\alpha)_2 = \langle 2 \rangle \times \text{Fix}(\alpha)$  by Lemma 4.2. If  $\exp(G) > 2$  then  $Z(Q) = N(Q) \cap C(Q) = \langle 2 \rangle \times \text{Fix}(\alpha)_2$ , by Lemmas 4.2 and 4.3.  $\square$

**Proposition 4.5.** *Let  $Q$  be a dihedral automorphic loop with  $\alpha \neq 1 = \alpha^2$ . 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  $(u + H)\beta = u\alpha + H$ . Moreover,  $\beta^2 = 1$ .*

*Proof.* By Lemma 4.4,  $Z(Q) = \langle 2 \rangle \times \text{Fix}(\alpha)_2$ . 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  $f : Q \rightarrow \text{Dih}(2, G/H, \beta)$  defined by  $(i, u)f = (i \bmod 2, u + H)$ . Since

$$\begin{aligned} (i, u)f(j, v)f &= (i \bmod 2, u + H)(j \bmod 2, v + H) \\ &= ((i + j) \bmod 2, (s_j(u + H) + (v + H))\beta^{ij}) \\ &= ((i + j) \bmod 2, (s_j u + v)\alpha^{ij} + H) \\ &= (i + j, (s_j u + v)\alpha^{ij})f = ((i, u)(j, v))f, \end{aligned}$$

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

**Corollary 4.6.** *Every dihedral automorphic loop  $\text{Dih}(m, G, \alpha)$  with  $\alpha \neq 1 = \alpha^2$  is a central extension of an elementary abelian 2-group by a dihedral automorphic loop of the form  $\text{Dih}(2, K, \beta)$  with  $\beta^2 = 1$  and  $K$  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 automorphic loops. Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop with  $\alpha^2 = 1$  and  $m$  even.

If  $\alpha = 1$  and  $\exp(G) \leq 2$  then  $Z(Q) = Q$  by Lemma 4.4. If  $\alpha = 1$  and  $\exp(G) > 2$  then  $Q$  is a group and  $Z(Q) = \langle 2 \rangle \times \text{Fix}(\alpha)_2 = \langle 2 \rangle \times G_2$ , and since  $(i, u)Z(Q) \cdot (j, v)Z(Q) = (i \oplus j, s_j u + v)(\langle 2 \rangle \times G_2) = ((i + j) \bmod 2, s_j u + v)Z(Q)$ , we see that  $Q/Z(Q)$  is isomorphic to the generalized dihedral group  $\text{Dih}(2, G/G_2, 1)$ .

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

*Example 4.7.* If  $G$  is an abelian group of odd order and  $\alpha \in \text{Aut}(G)$  such that  $\alpha \neq 1 = \alpha^2$  then  $Z(\text{Dih}(2, G, \alpha)) = 1$ .

Suppose that  $|G| = 2^n$  and  $\alpha \in \text{Aut}(G)$  is such that  $\alpha \neq 1 = \alpha^2$ . 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  $G = \mathbb{Z}_{2^n}$ ,  $\alpha \in \text{Aut}(G)$  and  $1 = \alpha^2$ . 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  $\beta \in \text{Aut}(G/H)$  satisfying  $\beta^2 = 1$ , because  $2^{n-1}$  is the unique element of order 2 in  $G$ . By induction,  $Q$  has nilpotence class  $n$ .

## 5. COMMUTATORS AND ASSOCIATORS

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

**Lemma 5.1.** *In a loop  $Q = \text{Dih}(m, G, \alpha)$  we have*

$$(14) \quad [(i, u), (j, v)] = (0, ((s_j - 1)u + (1 - s_i)v)\alpha^{ij})$$

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

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

$$\begin{aligned} (i \oplus j, (s_j u + v)\alpha^{ij}) &= (j \oplus i, (s_i v + u)\alpha^{ij}) \cdot (k, w) \iff \\ (i \oplus j, s_j u \alpha^{ij} + v \alpha^{ij}) &= (i \oplus j \oplus k, (s_k s_i v \alpha^{ij} + s_k u \alpha^{ij} + w)\alpha^{(i \oplus j)k}). \end{aligned}$$

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 5.2.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop with  $\alpha^2 = 1$ . 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.* First, using Lemma 5.1 and looking at all cases  $i, j \pmod{2}$ , it is easy to 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 is easy to see from (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 3.2, 3.5 and an analog of Lemma 3.5:

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

$\square$

**Lemma 5.3.** *In a dihedral automorphic loop  $Q = \text{Dih}(m, G, \alpha)$  with  $\alpha^2 = 1$  we have*

$$(15) \quad [(i, u), (j, v), (k, w)] = (0, (s_{j+k}u(1 - \alpha^{-jk})\alpha^{ij} + w(1 - \alpha^{ij}))\alpha^{(i \oplus j)k})$$

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

*Proof.* When  $m$  is odd and  $\alpha = 1$  then  $Q$  is a group and (15) yields  $[(i, u), (j, v), (k, w)] = 1$ . The case  $m$  even and  $\alpha^2 = 1$  follows by straightforward calculation, but since the identity (7) is involved, we give all the details: let  $(\ell, x) = [(i, u), (j, v), (k, w)]$  so

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

where we have used identity (7) in the last step. We obtain

$$(i \oplus j \oplus k, s_{k+j}u\alpha^{ij+(i\oplus j)k} + s_kv\alpha^{ij+(i\oplus j)k} + w\alpha^{(i\oplus j)k}) = (i \oplus j \oplus k \oplus \ell, [s_{j+k+\ell}u\alpha^{ij+(i\oplus j)k-jk} \\ + s_{k+\ell}v\alpha^{jk+i(j\oplus k)} + s_\ell w\alpha^{jk+i(j\oplus k)} + x]\alpha^{(i\oplus j\oplus k)\ell}).$$

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

$$s_{k+j}u\alpha^{ij+(i\oplus j)k} + s_kv\alpha^{ij+(i\oplus j)k} + w\alpha^{(i\oplus j)k} = s_{j+k}u\alpha^{ij+(i\oplus j)k-jk} + s_kv\alpha^{ij+(i\oplus j)k} + w\alpha^{ij+(i\oplus j)k} + x, \\ x = (s_{j+k}u(1 - \alpha^{-jk})\alpha^{ij} + w(1 - \alpha^{ij}))\alpha^{(i\oplus j)k}.$$

□

**Proposition 5.4.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop with  $\alpha^2 = 1$ . Then*

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

*Proof.* Here we check all choices of  $i, j, k \pmod{2}$ , using Lemma 5.3.

$$\begin{aligned} [(0, u), (0, v), (0, w)] &= (0, u(1 - 1) + w(1 - 1)) = (0, 0), \\ [(0, u), (1, v), (0, w)] &= (0, -u(1 - 1) + w(1 - 1)) = (0, 0), \\ [(0, u), (0, v), (1, w)] &= (0, -u(1 - 1) + w(1 - 1)) = (0, 0), \\ [(0, u), (1, v), (1, w)] &= (0, (u(1 - \alpha^{-1}) + w(1 - 1))\alpha) = (0, u(1 - \alpha^{-1})\alpha) = (0, -u(1 - \alpha)), \\ [(1, u), (0, v), (0, w)] &= (0, u(1 - 1) + w(1 - 1)) = (0, 0), \\ [(1, u), (1, v), (0, w)] &= (0, (-u(1 - 1)\alpha + w(1 - \alpha))) = (0, w(1 - \alpha)), \\ [(1, u), (0, v), (1, w)] &= (0, (-u(1 - 1) + w(1 - 1))\alpha) = (0, 0), \\ [(1, u), (1, v), (1, w)] &= (0, u(1 - \alpha)\alpha + w(1 - \alpha)), \\ &= (0, u(1 - \alpha^{-1})\alpha + w(1 - \alpha)), \\ &= (0, (-u + w)(1 - \alpha)). \end{aligned}$$

We can see that  $[(i, u), (j, v), (k, w)] \in 0 \times (1 - \alpha)G$ . Second,  $[(1, u), (1, v), (0, w)] = (0, w(1 - \alpha))$ . This shows that  $\{[x, y, z] : x, y, z \in Q\} = 0 \times G(1 - \alpha)$ .

Next, we need to show  $0 \times G(1 - \alpha)$  is subloop of  $Q$ . Let  $(0, u(1 - \alpha))$  and  $(0, v(1 - \alpha))$  be two elements of  $0 \times G(1 - \alpha)$ . Then

$$\begin{aligned} (0, u(1 - \alpha)) \cdot (0, v(1 - \alpha)) &= (0, (u + v)(1 - \alpha)), \\ (0, u(1 - \alpha)) \setminus (0, v(1 - \alpha)) &= (0, (v - u)(1 - \alpha)), \\ (0, u(1 - \alpha)) / (0, v(1 - \alpha)) &= (0, (u - v)(1 - \alpha)). \end{aligned}$$

Finally, to show  $0 \times G(1 - \alpha)$  is normal in  $Q$  we use Lemmas 3.2 and 3.5 to obtain:

$$\begin{aligned} (0, w(1 - \alpha))L_{(j,v),(i,u)} &= (0, s_ju\alpha^{ij} + v\alpha^{ij} + w(1 - \alpha)\alpha^{ij} - s_ju\alpha^{ij} - v\alpha^{ij}) \\ &= (0, w(1 - \alpha)\alpha^{ij}), \\ (0, w(1 - \alpha))T_{(i,u)} &= (0, s_iw(1 - \alpha) + (1 - 1)u) \\ &= (0, s_iw(1 - \alpha)), \\ (0, w(1 - \alpha))R_{(j,v),(i,u)} &= (0, (w(1 - \alpha) + s_{-(i+j)}u(1 - 1))\alpha^{ij}) \\ &= (0, w(1 - \alpha)\alpha^{ij}). \end{aligned}$$

□

**Proposition 5.5.** *Let  $Q = \text{Dih}(m, G, \alpha)$  be a dihedral automorphic loop with  $\alpha^2 = 1$ . Then*

$$Q' = 0 \times (G(1 - \alpha) + 2G).$$

*Proof.* The proof is immediate from Propositions 5.2 and 5.4, since  $Q' = 0 \times (G(1 - \alpha) + 2G)$  is a normal subloop of  $Q$ .  $\square$

## 6. ACKNOWLEDGEMENTS.

I would like to express my great appreciation to Dr. Vojtěchovský for many helpful discussions about constructions of automorphic loops and I thank him for his valuable and constructive suggestions during the planning and development of this paper.

## REFERENCES

- [1] 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.
- [2] R. H. Bruck, *A Survey of Binary Systems*, Springer, 1971.
- [3] R. H. Bruck and L. J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. **2** 63 (1956) 308–323.
- [4] K. W. Johnson, M. K. Kinyon, G. P. Nagy and P. Vojtěchovský, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200–213.
- [5] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), no. 1, 365–384.
- [6] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. 9, 3243–3267.
- [7] M. Aboras, *Dihedral-like constructions of automorphic loops*, Thesis. In preparation.