Four halves of the inverse property in loop extensions

Uzi Vishne

Abstract. Any two of the left, right, weak and antiautomorphic inverse properties of a loop imply the full inverse property. Considering these properties in the context of nuclear loop extensions $1 \to K \to L \to Q \to 1$, we discover an action of the infinite dihedral group on $\mathrm{C}^2(Q, K)$ whose subspaces fixed under odd subgroups precisely correspond to these classical loop properties.

When in doubt, look for the group!
(André Weil)

1 Introduction

A set equipped with a (nonassociative) binary operation is called a **loop** if it has a unit element, and left and right multiplications are invertible. Thus every element has a unique left inverse and a unique right inverse. A loop has the **inverse property** if the left and right inverses coincide, and the identities $x^{-1}(xy) = (yx)x^{-1} = y$ hold. Any group has the inverse property, but there are plenty of other examples (see [4]). This paper is concerned with a cohomological structure governing various generalizations of the inverse property.

Let L be a loop. The actions on L by left and right multiplication by $x \in L$ are denoted ℓ_x and r_x, respectively. The left and right inverses of x are denoted x^λ and x^ρ, respectively. The maps $\lambda, \rho : L \to L$ satisfy $\lambda\rho = \rho\lambda = \mathrm{id}$. We consider the following properties of loops, all studied by multiple authors before.

(LI) $x^\lambda(xy) = y$ (the **left inverse property**).

(RI) $(yx)x^\rho = y$ (the **right inverse property**).

(WI) $(xy)z = 1$ precisely when $x(yz) = 1$ (the **weak inverse property**).

(AI) $(xy)^\lambda = y^\lambda x^\lambda$, equivalently $(xy)^\rho = y^\rho x^\rho$ (the **antiautomorphic inverse property**).

2020 Mathematics Subject Classification: 20N05
Keywords: Inverse property, weak inverse, antiautomorphic inverse loops, loop extensions.
Partially supported by an Israeli Science Foundation, grant number 1623/16.

(IP) both left and right inverse properties (the **inverse property**).

(Inv) All elements are invertible ($\lambda = \rho$).

(H) The map λ^2 (equivalently ρ^2) is a loop homomorphism.

The logical dependencies are given in Figure 1 (up-side down, anticipating the refinement given in Figure 2, see Section 7). We call (LI), (RI), (WI) and (AI) the "**four halves**" of the inverse property, because, as we show below, any two of these conditions imply the inverse property (IP) and thus all the others.

We study these properties for loops arising as nuclear extensions of a group Q by an abelian group K. Let $\mathrm{C}^2(Q,K) = \{c : Q \times Q \to K\}$ be the function space parameterizing the extensions via the classical factor set construction. We say that a subspace $X \subseteq \mathrm{C}^2(Q,K)$ "is" the loop property P if the extension (K,Q,c) has P precisely when $c \in X$. The purpose of this paper is to exhibit an action of the infinite dihedral group, which was discovered by Artzy [5, Prop. 3.2], in the cohomological context. Let D_∞ denote the infinite dihedral group, and C_∞ its cyclic subgroup of index 2. We say that a subgroup is **even** if it is contained in C_∞, and **odd** otherwise.

Theorem 1.1. *There is an action of D_∞ on the space $\mathrm{C}^2(Q,K)$, such that the subspaces fixed under subgroups of D_∞ are:*

- (LI), (RI), (AI) *and* (IP) *(for odd subgroups) and*
- (W_{2n+1}) *and* (H^n) *(for even subgroups).*

A loop has the property (H^n) if λ^{2n} is a homomorphism; thus (H^1) = (H). The m-inverse properties (W_m), defined in Section 8, are variations on the weak inverse property, which is (WI) = (W_{-1}).

The action of D_∞ in the theorem preserves the coboundaries $\mathrm{B}^2(Q,K)$ elementwise, and is in particular well-defined on the quotient space $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$ which classifies extensions up to equivalence.

As we see below, any two of the four halves define the group action, and in this sense could have defined the other properties. Notice that there are infinitely many odd subgroups, a-priori each with its own fixed subspace. The fact that our action has finitely many fixed subspaces under odd subgroups indicates a strong connection between the four halves and places (W_{2n+1}) and (H^n) as their conceptual derivatives.

Section 2 provides a brief sketch of the properties of loops we encounter in this paper. The proofs follow standard arguments, and are given here for completeness. In Section 3 we define loop extensions arising from an action of a group Q on an abelian group K, and characterize the four properties (LI), (RI), (WI) and (AI) of the extension (K,Q,c) in terms of conditions on the factor set $c \in \mathrm{C}^2(Q,K)$. Further details are given in Section 4, where we find similar characterization for (Inv) and (H).

$$\begin{tikzcd}
 & (\mathrm{H}) & & \\
 & (\mathrm{Inv}) \arrow[u] & & \\
(\mathrm{AI}) \arrow[ur] & (\mathrm{LI}) \arrow[u] & (\mathrm{RI}) \arrow[ul] & (\mathrm{WI}) \arrow[uull] \\
 & (\mathrm{IP}) \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Figure 1: Logical dependencies of loop properties

In Section 5 we introduce the action of the infinite dihedral group D_∞ on $\mathrm{C}^2(Q, K)$; the action preserves equivalence classes of extensions. Proposition 6.1 ties the loop properties with the dihedral action, and Theorem 7.1 proves the odd part of Theorem 1.1. Section 8 studies the m-inverse properties, denoted here (W_m), which include the k-fold weak inverse properties $(\mathrm{W}^k\mathrm{IP})$. Theorem 8.8 covers the even part of Theorem 1.1. Finally, in Section 9 we specialize to the case $Q = \mathbb{Z}_4$ and provide some examples and counterexamples.

We thank the referee for helpful remarks on an earlier version of this paper, which in particular led to the current Section 8.

2 Four halves of the inverse property

In this section we provide equivalent formulations for each of the four halves of (IP), and prove:

Proposition 2.1. *Any two of the properties* (LI), (RI), (WI) *and* (AI) *imply the (full) inverse property.*

Counterexamples, showing that none of the four halves implies (IP) on its own, are given in Corollary 9.3.

2.1 The left and right inverse properties

Let L be a loop. If the inverse of ℓ_x has the form ℓ_y for some y, then necessarily $\ell_x^{-1} = \ell_{x^\lambda}$. Indeed, if $xy = \ell_x \ell_y(1) = 1$ then $y = x^\lambda$. Likewise if the inverse of r_x has the form r_y, then $r_x^{-1} = r_{x^\rho}$.

Proposition 2.2. *a. The left inverse property is equivalent to* $\ell_x^{-1} = \ell_{x^\lambda}$ *for every* x.

b. The right inverse property is equivalent to $r_x^{-1} = r_{x^\rho}$ *for every* x.

c. Each of the properties (LI) *and* (RI) *implies* (Inv).

Proof. The identity $x^\lambda(xy) = y$ is equivalent to $\ell_{x^\lambda}\ell_x = \mathrm{id}$ so $\ell_x^{-1} = \ell_{x^\lambda}$. Now suppose $\ell_{x^\lambda} = \ell_x^{-1}$ for all x. Then $\ell_{x^{\lambda^2}} = \ell_{x^\lambda}^{-1} = \ell_x$, implying $x^{\lambda^2} = x$, and so $\lambda^2 = \mathrm{id}$. But then $\rho = \lambda^{-1} = \lambda$, so all elements are invertible. The proof for right inverse is similar. □

The left (resp. right) inverse property holds for all isotopes of a loop L, if and only if L satisfies the left (resp. right) Bol axiom $\ell_x\ell_y\ell_x = \ell_{x(yx)}$ (resp. $r_xr_yr_x = r_{(xy)x}$), [12, Thm 3.1].

2.2 The antiautomorphic inverse property

Proposition 2.3. *The following properties of a loop are equivalent.*

(a) $(xy)^\lambda = y^\lambda x^\lambda$ *(namely antiautomorphic inverse).*

(a′) $(xy)^\rho = y^\rho x^\rho$.

(b) $r_y = \rho\ell_{y^\lambda}\lambda$.

(b′) $r_y = \lambda\ell_{y^\rho}\rho$.

(c) $r_{x^\lambda} = \lambda\ell_x\rho$.

(c′) $r_{x^\rho} = \rho\ell_x\lambda$.

Proof. Condition (a) is equivalent to (b) by the action on x, and to (c) by the action on y. Condition (a′) is equivalent to (b′) by the action on x, and to (c′) by the action on y. Taking $x = y^\lambda$ in (c′) we get (b). □

Proposition 2.4. *(IP)* $\Longrightarrow$ *(AI)* $\Longrightarrow$ *(Inv).*

Proof. Assuming (IP) we have $(xy)^{-1} = ((xy)^{-1}x)x^{-1} = ((xy)^{-1}(xy \cdot y^{-1}))x^{-1} = y^{-1}x^{-1}$. Assuming (AI), we have $xx^\lambda = (x^\rho)^\lambda x^\lambda = (xx^\rho)^\lambda = 1^\lambda = 1$, so $x^\lambda = x^\rho$. □

For example, every automorphic loop (=all inner maps are automorphisms) has the antiautomorphic inverse property [8, Cor. 6.6]. Artzy proved that an (IP) loop all of whose isotopes satisfy (AI) is a Moufang loop [2] (see also [1]).

2.3 The weak inverse property

Weak inverse loops are of interest mostly due to Osborn's theorem that their one-sided nuclei coincide [11].

Proposition 2.5. *The following properties of a loop are equivalent.*

(a) $x(yz) = 1$ *if and only if* $(xy)z = 1$ *(namely weak inverse).*

(b) *if* $x(yz) = 1$ *then* $(xy)z = 1$.

(b′) *if* $(xy)z = 1$ *then* $x(yz) = 1$.

(c) $(yz)^\lambda y = z^\lambda$.

(c′) $y(xy)^\rho = x^\rho$.

(d) $r_y = \lambda \ell_y^{-1} \rho$.

Proof. Condition (b) says that if $x = (yz)^\lambda$ then $xy = z^\lambda$, namely $(yz)^\lambda y = z^\lambda$, which is condition (c). Action on z interprets this condition as $r_y \lambda \ell_y = \lambda$, which is condition (d). Similarly (b′) is equivalent to (c′) and to (d); and (a) = (b) +(b′). □

Proposition 2.6. *The property* (AI)*, together with either* (LI) *or* (RI)*, implies* (WI).

Proof. If $(xy)z = 1$ then $z = (xy)^{-1} = y^{-1}x^{-1}$ by (AI) and then $x(yz) = x(y(y^{-1}x^{-1})) = xx^{-1} = 1$ by (LI). Similarly if $x(yz) = 1$ then $x = (yz)^{-1} = z^{-1}y^{-1}$ by the (AI) and then $(xy)z = (z^{-1}y^{-1} \cdot y)z = z^{-1}z = 1$ by (RI). □

Osborn [11, p. 296] notes that (WI) $\Longrightarrow$ (H) (but (WI)$\not\Longrightarrow$(Inv), see Example 9.5).

2.4 Any two suffice

We move to prove Proposition 2.1.

Proof. The inverse property clearly implies both (LI), (RI), and by Proposition 2.4 it also implies (AI). By Proposition 2.6, (WI) follows as well.

1. Assume (LI) and (RI). The inverse property holds by Proposition 2.2.(c).

2. Assume (WI) and either (LI) or (RI). All elements are invertible. Now Proposition 2.5.(d) gives $r_y = \lambda \ell_y^{-1} \lambda^{-1}$, so taking y^{-1} for y we get $r_{y^{-1}} = \lambda \ell_{y^{-1}}^{-1} \lambda^{-1}$, implying that $r_y r_{y^{-1}} = \lambda (\ell_{y^{-1}} \ell_y)^{-1} \lambda^{-1}$, so the left inverse property $r_y r_{y^{-1}} = \mathrm{id}$ is equivalent to the right inverse property $\ell_{y^{-1}} \ell_y = \mathrm{id}$; but we assume one of them holds, so both do.

3. Assume (AI) and either (LI) or (RI). Then by Proposition 2.3.(b′), $r_y = \lambda \ell_{y^{-1}} \lambda^{-1}$, so taking y^{-1} for y we get $r_{y^{-1}} = \lambda \ell_y \lambda^{-1}$, implying once more $r_y r_{y^{-1}} = \lambda (\ell_{y^{-1}} \ell_y)^{-1} \lambda^{-1}$. The argument continues as in 2.

4. Finally if (WI) and (AI) hold, then $\lambda \ell_{y^\lambda} \rho = r_y = \lambda \ell_y^{-1} \rho$ by Propositions 2.3.(b′) and 2.5.(d), implying $\ell_{y^\lambda} = \ell_y^{-1}$ which is the left inverse property, and we are done by 2. or 3.

□

3 Loop extensions

Let L' and L'' be loops. A loop L is an **extension** of L' by L'' if there is a short exact sequence of loop homomorphisms $1 \longrightarrow L'' \longrightarrow L \longrightarrow L' \longrightarrow 1$. This classical construction is systematically studied in the recent paper [9] (also see the references therein). The extension is **nuclear** if the image of L'' is contained in the nucleus of L. Our focus here is on loops obtained as nuclear extensions of a group by an abelian group.

Let Q be a group acting on an abelian group K. We denote the action by $q\colon k \mapsto k^q$, so that $k^{qq'} = (k^{q'})^q$. For a function $c\colon Q \times Q \to K$ satisfying $c_{1,q} = c_{q,1} = 1$ for all $q \in Q$, let (K,Q,c) denote the set $K \times Q = \{kq\colon\, k \in K, q \in Q\}$ with the binary operation

$$kq \cdot k'q' = kk'^q c_{q,q'}(qq').$$

We always have that K is a normal nuclear subgroup of the loop (K,Q,c). It is well known that (K,Q,c) is a group if and only if c satisfies the 2-cocycle condition

$$c_{q,q'}c_{qq',q''} = c^q_{q',q''}c_{q,q'q''}. \tag{1}$$

The semidirect extension $L = K \rtimes Q$ with respect to the given action corresponds to the trivial co-cycle $c = 1$.

We say that c, c' are **equivalent** (and write $c \approx c'$) if there are $a_q \in K$, $a_1 = 1$, such that $c'_{q,q'} = a_q a^q_{q'} a^{-1}_{qq'} c_{q,q'}$. There is an extension isomorphism $(K,Q,c) \to (K,Q,c')$, namely a loop isomorphism preserving K elements-wise and each of the cosets Kq, if and only if $c \approx c'$.

The "diagonal" entries $c_{q,q^{-1}}$ of the function $c\colon Q \times Q \to K$ play a special role in the computations to follow. We thus denote

$$\gamma_q = c_{q,q^{-1}}, \tag{2}$$

always understood as depending on c. Writing $k^{-q} = (k^{-1})^q = (k^q)^{-1}$, we have in (K,Q,c) that

$$(kq)^\lambda = k^{-q^{-1}}\gamma^{-1}_{q^{-1}}q^{-1}, \tag{3}$$

$$(kq)^\rho = k^{-q^{-1}}\gamma_q^{-q^{-1}}q^{-1}. \tag{4}$$

Proposition 3.1. *The loop (K,Q,c) satisfies the property:*

(LI) *if* $c_{p,q}c^p_{p^{-1},pq} = \gamma^p_{p^{-1}}$.

(RI) *if* $c_{p,q}c_{pq,q^{-1}} = \gamma^p_q$.

(WI) *if* $c_{p,q}c^{-p}_{q,(pq)^{-1}} = \gamma_p\gamma^{-1}_{pq}$.

(AI) *if* $c_{p,q}c^{pq}_{q^{-1},p^{-1}} = \gamma^p_{p^{-1}}\gamma^{pq}_{q^{-1}}\gamma^{-pq}_{(pq)^{-1}}$, *equivalently if* $c_{p,q}c^{pq}_{q^{-1},p^{-1}} = \gamma_p\gamma^p_q\gamma^{-1}_{pq}$.

Proof. Computation with the defining identities, based on Equations (3) and (4). For the antiautomorphic inverse property we used both (a) and (a′) of Proposition 2.3 (so each of the conditions $c_{p,q}c^{pq}_{q^{-1},p^{-1}} = \gamma^{p}_{p^{-1}}\gamma^{pq}_{q^{-1}}\gamma^{-pq}_{(pq)^{-1}}$ and $c_{p,q}c^{pq}_{q^{-1},p^{-1}} = \gamma_p\gamma^{p}_{q}\gamma^{-1}_{pq}$ suffices). □

4 Detecting (Inv) and (H)

Recall that $\mathrm{C}^1(Q,K) = \{a : Q \to K\}$ and $\mathrm{C}^2(Q,K) = \{c : Q \times Q \to K\}$ are the spaces of unary and binary functions from Q to the abelian group K. The differential map $\delta^1 : \mathrm{C}^1(Q,K) \to \mathrm{C}^2(Q,K)$, defined by

$$(\delta^1 a)_{p,q} = a_p a^p_q a^{-1}_{pq},$$

gives rise to the groups of cocycles

$$\mathrm{Z}^1(Q,K) = \mathrm{Ker}(\delta^1)$$

and coboundaries

$$\mathrm{B}^2(Q,K) = \mathrm{Im}(\delta^1)$$

(see [3]). The loop extensions (K,Q,c), up to equivalence, are in correspondence with the quotient $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$. The properties listed in Proposition 3.1 are well-defined up to equivalence of c because they are preserved by loop isomorphism; alternatively by direct computation.

For any $k \in K$ and $q \in Q$, we have in (K,Q,c) that

$$(kq)(kq)^{\lambda} = (kq^{-1})^{\rho}(kq^{-1}) = \gamma^{-q}_{q^{-1}}\gamma_q,$$

which is independent of k (compare to [6, Lemma 4.2], that every element of a Buchsteiner loop satisfies $x^{\rho}x = xx^{\lambda}$). Motivated by this quantity, we define a function $\psi : \mathrm{C}^2(Q,K) \to \mathrm{C}^1(Q,K)$ by

$$(\psi c)_q = c^{-q}_{q^{-1},q}c_{q,q^{-1}} = \gamma^{-q}_{q^{-1}}\gamma_q.$$

Proposition 4.1. *The function ψ is a well-defined group homomorphism*

$$\psi : \mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K) \to \mathrm{C}^1(Q,K).$$

Proof. Verify that $(\psi\delta^1 a) = a^{-q}_{q^{-1}}a^{-1}_q \cdot a^1_q a^q_{q^{-1}} = 1$ for every $a \in \mathrm{C}^1(Q,K)$, showing that ψ is trivial on $\mathrm{B}^2(Q,K)$. □

In particular, ψc is defined in terms of the equivalence class of the loop (K,Q,c). Complementing Proposition 3.1, we have:

Proposition 4.2. *The loop (K,Q,c) satisfies the property:*

(Inv) *if* $\psi c = 1$.

(H) *if* $\delta^1\psi c = 1$.

Proof. The first statement follows from the computation $(kq)(kq)^\lambda = (\psi c)_q$ (for any $k \in K$ and $q \in Q$). By (3) we find that $(kq)^{\lambda^2} = k\gamma_{q^{-1}}^q\gamma_q^{-1}q$ and $(kq)^{\rho^2} = k\gamma_q\gamma_{q^{-1}}^{-q}q$, namely

$$(kq)^{\lambda^2} = (\psi c)_q^{-1} \cdot kq; \tag{5}$$

$$(kq)^{\rho^2} = (\psi c)_q \cdot kq. \tag{6}$$

This proves the first claim. One can then verify that λ^2 is a homomorphism if and only if $(\delta^1\psi c)_{q,q'} = \gamma_{q^{-1}}^q\gamma_q^{-1}(\gamma_{q'^{-1}}^{q'}\gamma_{q'}^{-1})^q(\gamma_{(qq')^{-1}}^{qq'}\gamma_{qq'}^{-1})^{-1} = 1$. $\square$

Taking $q = p^{-1}$ in the condition for (AI) given in Proposition 3.1, we obtain the condition of (Inv) as stated in Proposition 4.2, consistently with the implication (AI) $\implies$ (Inv) of Proposition 2.4.

4.1 Extensions of $\mathbb{Z}_2$

As an illustration we consider extensions with the largest nucleus, namely the case when $Q = \langle\sigma\rangle$ is the cyclic group of order 2. (The case $Q = \mathbb{Z}_4$ is described in Section 9). Since $|Q| = 2$, the factor set c is determined by the single value $\gamma_\sigma = c_{\sigma,\sigma} \in K$. Let us describe the properties of (K, Q, c) in this case.

Example 4.3. Suppose $L = (K, Q, c)$ is a nuclear loop extension of $Q = \mathbb{Z}_2$ by an abelian group. Then:

a. (WI) always holds.

b. (Inv) implies associativity.

Indeed, the conditions in Proposition 3.1 hold trivially when $p = 1$ or $q = 1$, so it remains to substitute $p = q = \sigma$. We find that (WI) holds trivially. Also, $(\psi c)_\sigma = \gamma_\sigma^{-1}\gamma_\sigma^\sigma$, so $\psi c = 1$ if and only if $\gamma_\sigma \in K^\sigma$, which is equivalent to associativity.

We also note that the loops in this subsection are all conjugacy closed, see [7].

5 A dihedral action

We use the conditions for (LI) and (RI) in Proposition 3.1 to define operators

$$\alpha, \beta : \mathrm{C}^2(Q, K) \to \mathrm{C}^2(Q, K)$$

as follows:

$$
\begin{aligned}
(\alpha c)_{p,q} &= \gamma_{p^{-1}}^{p}\, c_{p^{-1},pq}^{-p}, \\
(\beta c)_{p,q} &= \gamma_{q}^{p}\, c_{pq,q^{-1}}^{-1},
\end{aligned}
$$

where tautologically $\gamma_q = c_{q,q^{-1}}$ by (2).

Remark 5.1. The maps α, β are built on top of the involutorial maps $(p,q) \mapsto (p^{-1}, pq)$ and $(p,q) \mapsto (pq, q^{-1})$, generating an action of the symmetric group S_3 on the space of pairs Q^2. In fact, if $Q = \mathbb{Z}$ we obtain the irreducible representation $S_3 \hookrightarrow \mathrm{GL}_2(\mathbb{Z})$ generated by the involutions $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$.

Proposition 5.2. *The operators α, β define an action of the infinite dihedral group D_∞ on $\mathrm{C}^2(Q,K)$; namely $\alpha^2 = \beta^2 = \mathrm{id}$.*

Proof. We have that

$$
(\alpha^2 c)_{p,q} = (\alpha c)_{p^{-1},p}^{p} (\alpha c)_{p^{-1},pq}^{-p} = (c_{p,p^{-1}}^{p^{-1}} c_{p,1}^{-p^{-1}})^{p} (c_{p,p^{-1}}^{p^{-1}} c_{p,q}^{-p^{-1}})^{-p} = c_{p,q};
$$

and

$$
(\beta^2 c)_{p,q} = (\beta c)_{q,q^{-1}}^{p} (\beta c)_{pq,q^{-1}}^{-1} = (c_{q^{-1},q}^{q} c_{1,q}^{-1})^{p} (c_{q^{-1},q}^{pq} c_{p,q}^{-1})^{-1} = c_{p,q};
$$

thus $\langle \alpha, \beta \rangle$ is a dihedral group (which by Proposition 5.6 below is infinite for a generic K). □

Remark 5.3. Both α and β act trivially on $\mathrm{B}^2(Q,K)$, so $\langle \alpha, \beta \rangle$ acts on the quotient space $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$. (However, see Example 9.7 below.)

Indeed, we also have that

$$
\begin{aligned}
(\alpha \delta^1 a)_{p,q} &= (\delta^1 a)_{p^{-1},p}^{p} (\delta^1 a)_{p^{-1},pq}^{-p} = (a_{p^{-1}} a_p^{p^{-1}} a_1^{-1})^{p} (a_{p^{-1}} a_{pq}^{p^{-1}} a_q^{-1})^{-p} \\
&= a_p a_{pq}^{-1} a_q^{p} = (\delta^1 a)_{p,q},
\end{aligned}
$$

and likewise $\beta \delta^1 a = \delta^1 a$.

Remark 5.4. We point out some useful computations.

1. The diagonal entries of α and β are

$$
(\alpha c)_{p,p^{-1}} = (\beta c)_{p,p^{-1}} = c_{p^{-1},p}^{p};
$$

and therefore

$$
(\alpha \beta c)_{p,p^{-1}} = (\beta \alpha c)_{p,p^{-1}} = c_{p,p^{-1}}.
$$

2. Define $\Gamma : \mathrm{C}^2(Q,K) \to \mathrm{C}^1(Q,K)$ by $\Gamma c = \gamma$, namely $(\Gamma c)_p = c_{p,p^{-1}}$; then $\Gamma \alpha \beta = \Gamma$.

3. We have that $\psi\alpha c = \psi\beta c = \psi c^{-1}$. Therefore $\psi\alpha\beta = \psi$.

Proof. Taking $q = p^{-1}$ in the definition of α, β gives (1). (2) follows from the definition of $\Gamma c = \gamma$. Since ψc can be computed from $\Gamma c = \gamma$, we conclude (3) from (2). □

Let us compute some elements in the orbit of $c \in \mathrm{C}^2(Q, K)$ under the action.

Proposition 5.5. *The following formulas hold:*

$$
\begin{aligned}
(\alpha\beta c)_{p,q} &= \gamma_p \gamma_{pq}^{-1}\, c^{p}_{q,(pq)^{-1}}; &(7)\\
(\beta\alpha c)_{p,q} &= \gamma^{pq}_{q^{-1}} \gamma^{-pq}_{(pq)^{-1}}\, c^{pq}_{(pq)^{-1},p}; &(8)\\
(\alpha\beta\alpha c)_{p,q} &= \gamma^{p}_{p^{-1}} \gamma^{pq}_{q^{-1}} \gamma^{-pq}_{(pq)^{-1}}\, c^{-pq}_{q^{-1},p^{-1}}; &(9)\\
(\beta\alpha\beta c)_{p,q} &= \gamma_p \gamma^{p}_{q} \gamma^{-1}_{pq}\, c^{-pq}_{q^{-1},p^{-1}}. &(10)
\end{aligned}
$$

Proof. Direct computation, aided by Proposition 5.4.(1). □

Careful substitution then proves:

Proposition 5.6. *We have the equality* $(\alpha\beta)^3 c = c \cdot \delta^1 \psi c$.

We write $X^G = \{x \in X : (\forall g \in G)\, gx = x\}$ for the subspace of X fixed under the action of a group G.

Corollary 5.7. We have that

$$\mathrm{C}^2(Q, K)^{\left\langle(\alpha\beta)^3\right\rangle} = \psi^{-1} \mathrm{Z}^1(Q, K).$$

Proof. By Proposition 5.6, the elements fixed under $(\alpha\beta)^3$ are those c for which $\delta^1\psi c = 1$, namely $\psi c \in \mathrm{Z}^1(Q, K) = \mathrm{Ker}(\delta^1)$. □

Notice that while the dihedral group D_∞ acts on the full space $\mathrm{C}^2(Q, K)$ (in a free manner, if K has elements of infinite order), there is an action of its quotient $\langle\alpha, \beta\rangle / \left\langle(\alpha\beta)^3\right\rangle \cong S_3$ on the fixed subspace $\mathrm{C}^2(Q, K)^{\left\langle(\alpha\beta)^3\right\rangle}$.

6 Loops and the dihedral action

We now interpret the loop properties from the introduction in terms of the dihedral action introduced in Section 5.

Proposition 6.1. *Let* $c \in \mathrm{C}^2(Q, K)$. *The loop* (K, Q, c) *has the property:*

(LI) *if and only if* $\alpha c = c$.

(RI) *if and only if* $\beta c = c$.

(WI) *if and only if* $\alpha\beta c = c$.

(AI) *if and only if* $\alpha\beta\alpha c = c$, *if and only if* $\beta\alpha\beta c = c$.

(IP) *if and only if* $\alpha c = \beta c = c$.

Proof. This is an interpretation of the conditions of Proposition 3.1, in the language of the operators as spelled out in Proposition 5.5. For example, (K, Q, c) has (LI) when $c_{p,q} = \gamma^{p}_{p^{-1}} c^{-p}_{p^{-1},pq} = (\alpha c)_{p,q}$. □

The dual description of (AI) in Proposition 6.1 allows us to extract a curious fact (especially in light of $\alpha\beta\alpha$ and $\beta\alpha\beta$ not being conjugate in the group, see Remark 7.3):

Corollary 6.2. $\mathrm{C}^2(Q, K)^{\langle\alpha\beta\alpha\rangle} = \mathrm{C}^2(Q, K)^{\langle\beta\alpha\beta\rangle}$.

Even more surprising, the loop theoretic description of the fixed subspaces gives the following inclusions:

Corollary 6.3. We have that

$$\mathrm{C}^2(Q, K)^{\langle\alpha\rangle}, \quad \mathrm{C}^2(Q, K)^{\langle\beta\rangle}, \quad \mathrm{C}^2(Q, K)^{\langle\alpha\beta\alpha\rangle} \subseteq \mathrm{Ker}(\psi) \subseteq \mathrm{C}^2(Q, K)^{\left\langle(\alpha\beta)^3\right\rangle}.$$

Proof. If $c \in \mathrm{C}^2(Q, K)$ is fixed under α, β or $\alpha\beta\alpha$, then (K, Q, c) has the properties (LI), (RI) or (AI) respectively, implying (Inv) in each case; but (Inv) means $\psi c = 1$ by Proposition 4.2. This proves the first statement. Likewise if $\psi c = 1$ then clearly $\delta^1\psi c = 1$, and by Corollary 5.7 we then get that $(\alpha\beta)^3 c = c$. □

We also note the trivial inclusion $\mathrm{C}^2(Q, K)^{\langle\alpha\beta\rangle} \subseteq \mathrm{C}^2(Q, K)^{\left\langle(\alpha\beta)^3\right\rangle}$, which in the same manner encodes the implication (WI) $\Longrightarrow$ (H).

7 The fixed subspaces

The element $\alpha\beta$ of D_∞ is well defined up to inversion, as the generator of the unique subgroup C_∞ of index 2. Moreover, C_∞ contains all the non-torsion elements of D_∞, and these are the elements of even length in terms of the generators α, β (or any other pair of generating involutions). Recall that a subgroup is even if it is contained in C_∞, and odd otherwise. We analyze odd subgroups in this section, and even subgroups in Section 8.

Theorem 7.1. *Any fixed subspace* $\mathrm{C}^2(Q, K)^H$, *under an odd subgroup* $H \leq D_\infty$, *is one of the subspaces*

$$\textit{(LI)} = \mathrm{C}^2(Q, K)^{\langle\alpha\rangle}, \qquad \textit{(RI)} = \mathrm{C}^2(Q, K)^{\langle\beta\rangle}, \qquad \textit{(AI)} = \mathrm{C}^2(Q, K)^{\langle\alpha\beta\alpha\rangle}$$

and

$$\textit{(IP)} = \mathrm{C}^2(Q, K)^{\langle\alpha,\beta\rangle}.$$

Proof. For $g, g' \in D_\infty$, let us write that $g \approx g'$ if $\mathrm{C}^2(Q,K)^{\langle g\rangle} = \mathrm{C}^2(Q,K)^{\langle g'\rangle}$. Since $\mathrm{C}^2(Q,K)^{\langle ghg^{-1}\rangle} = g(\mathrm{C}^2(Q,K)^{\langle h\rangle})$, this equivalence relation is stable under joint conjugation. Corollary 6.2 tells us that $\alpha\beta\alpha \approx \beta\alpha\beta$. Conjugation by α gives $\beta \approx \alpha\beta\alpha\beta\alpha$. These facts can be restated as $(\alpha\beta)^i\alpha \approx (\alpha\beta)^{i-3}\alpha$ for $i = 1, 2$. We have that $(\alpha\beta)^j(\alpha\beta)^k\alpha(\alpha\beta)^{-j} = (\alpha\beta)^{k+2j}\alpha$, which now implies $(\alpha\beta)^i\alpha \approx (\alpha\beta)^{i-3}\alpha$ for any $i \in \mathbb{Z}$. It follows that every odd element has the same fixed subspace as one of the three elements $\alpha, \beta, \alpha\beta\alpha$ (corresponding to $i = 0, -1, 1$).

Now let $H \leq D_\infty$ be an odd subgroup. Since the intersection with $\langle\alpha\beta\rangle$ is cyclic, we may write $H = \langle g, (\alpha\beta)^k\rangle$ where g is an odd element and $k \in \mathbb{Z}$. Then $\mathrm{C}^2(Q,K)^H = \mathrm{C}^2(Q,K)^{\langle g\rangle} \cap \mathrm{C}^2(Q,K)^{\langle(\alpha\beta)^k\rangle}$, so by the previous paragraph g can be replaced by one of the elements $\alpha, \beta, \alpha\beta\alpha$. By Corollary 6.3 we conclude that $\mathrm{C}^2(Q,K)^H \subseteq \mathrm{C}^2(Q,K)^{\langle(\alpha\beta)^3, (\alpha\beta)^k\rangle}$. If k is divisible by 3 it follows that $\mathrm{C}^2(Q,K)^H = \mathrm{C}^2(Q,K)^{\langle g\rangle}$; and otherwise $\mathrm{C}^2(Q,K)^H = \mathrm{C}^2(Q,K)^{\langle g,\alpha\beta\rangle} = \mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle}$. □

Recall that $\mathrm{Z}^2(Q,K)$ is the space of elements $c \in \mathrm{C}^2(Q,K)$ satisfying the 2-cocycle condition (1); namely those c for which (K,Q,c) is a group. Since every group has the inverse property (IP), we proved:

Corollary 7.2. $\mathrm{Z}^2(Q,K) \subseteq \mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle}$.

In other words, our group D_∞ acts trivially on the cohomology group $\mathrm{H}^2(Q,K) = \mathrm{Z}^2(Q,K)/\mathrm{B}^2(Q,K)$, which explains why it went unobserved in the classical theory of group extensions. The facts proved in Sections 6–7 are summarized in Figure 2.

7.1 The opposite loop

The opposite serves as a left-right mirror, explaining expected symmetries. Recall that the opposite loop L^{op} has the same underlying set as L, with the reverse multiplication.

Remark 7.3. We have that $(K,Q,c)^{\mathrm{op}} \cong (K,Q,\tau c)$ via the map $(kq)^{\mathrm{op}} \mapsto k^{q^{-1}}q^{-1}$, where $\tau : \mathrm{C}^2(Q,K) \to \mathrm{C}^2(Q,K)$ is defined by $(\tau c)_{p,q} = c_{q^{-1},p^{-1}}^{pq}$. (This is an isomorphism of loops, even if not an equivalence of extensions since K is not fixed elementwise). We have that $\tau^2 = 1$ and $\tau\alpha = \beta\tau$ by computation. Consequently, the group $\langle\alpha,\beta,\tau\rangle = \langle\tau,\alpha\rangle$, which is by itself infinite dihedral, acts by conjugation on its subgroup $\langle\alpha,\beta\rangle$ as the full group of automorphisms. The action of $\langle\tau,\alpha\rangle$ on loops is discussed in [5].

It follows that a-priori

$$\begin{aligned} \mathrm{C}^2(Q,K)^{\langle\beta\rangle} &= \tau(\mathrm{C}^2(Q,K)^{\langle\alpha\rangle}), \\ \mathrm{C}^2(Q,K)^{\langle\beta\alpha\beta\rangle} &= \tau(\mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle}), \\ \mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle} &= \tau(\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle}); \end{aligned}$$

$$
\begin{tikzcd}[column sep=small]
 & \mathrm{C}^2(Q,K) \arrow[d, dash] & & \\
 & \text{(H)}=\mathrm{C}^2(Q,K)^{\langle(\alpha\beta)^3\rangle} \arrow[d, dash] \arrow[ddrr, dash] & & \\
 & \text{(Inv)}=\mathrm{Ker}(\psi) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
\text{(AI)}=\mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle} \arrow[dr, dash] & \text{(LI)}=\mathrm{C}^2(Q,K)^{\langle\alpha\rangle} \arrow[d, dash] & \text{(RI)}=\mathrm{C}^2(Q,K)^{\langle\beta\rangle} \arrow[dl, dash] & \text{(WI)}=\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle} \arrow[dll, dash] \\
 & \text{(IP)}=\mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle} \arrow[d, dash] & & \\
 & \text{(Associative)}=\mathrm{Z}^2(Q,K) \arrow[d, dash] & & \\
 & \text{(Trivial)}=\mathrm{B}^2(Q,K) & &
\end{tikzcd}
$$

Figure 2: Subgroups of $\mathrm{C}^2(Q,K)$, ordered by inclusion, and the respective properties of the loops (K,Q,c)

indeed (LI) and (RI) are dual with respect to the opposite, while the other properties are left-right symmetric.

We also have that $\psi\tau = \psi$, in line with the fact that (Inv) is invariant to taking the opposite.

8 Generalizations of the weak inverse property

Following an insightful suggestion by the referee, we show in this section how the "doubly weak inverse property" and some of its generalizations fall under the framework of fixed subgroups of $\mathrm{C}^2(Q, K)$.

8.1 The m-inverse properties

For $m \in \mathbb{Z}$, a loop is said to have the m**-inverse property**, which we denote here by (W_m), if it satisfies the equivalent conditions

$$(xy)^{\rho^m} x^{\rho^{m+1}} = y^{\rho^m}; \tag{11}$$

$$x^{\lambda^{m+1}} (yx)^{\lambda^m} = y^{\lambda^m}; \tag{12}$$

$$\rho^m \ell_x \rho^{-m} = r^{-1}_{x^{\rho^{m+1}}}; \tag{13}$$

$$\lambda^m r_x \lambda^{-m} = \ell^{-1}_{x^{\lambda^{m+1}}}. \tag{14}$$

Indeed, (11)=(13) and (12)=(14) by the action on y, and (14) is obtained from (13) by taking $x^{\lambda^{m+1}}$ for x.

These properties were introduced by Karkliňš and Karkliň [10], see [6, Section 3]. By Proposition 2.5(c) the weak inverse property is (WI)=(W_{-1}). One of the key facts on this sequence, proven in [6, Lemma 3.1], is that

$$(\mathrm{W}_m) \implies (\mathrm{W}_{-2m-1}), \tag{15}$$

resulting in the chain

$$(\mathrm{WI}) = (\mathrm{W}^1\mathrm{IP}) \Rightarrow (\mathrm{W}^2\mathrm{IP}) \Rightarrow (\mathrm{W}^3\mathrm{IP}) \Rightarrow (\mathrm{W}^4\mathrm{IP}) \Rightarrow \cdots$$

where $(\mathrm{W}^k\mathrm{IP})$ is defined for $k \geq 1$ as (W_m) for $m = \frac{(-2)^k-1}{3}$. The "doubly weak inverse property" $(\mathrm{W}^2\mathrm{IP})$=$(\mathrm{W}_1)$ holds in any Buchsteiner loop, where (WI) does not necessarily hold.

Before characterizing the possible m-inverse properties of any given loop, we propose a change of indices, and write (W'_{1+3m}) instead of (W_m). Although hard to justify in terms of the defining identities (11)–(14), the formulation of various facts becomes cleaner in this manner. For example (15) reads $(\mathrm{W}'_\ell) \implies (\mathrm{W}'_{-2\ell})$, and $(\mathrm{W}^k\mathrm{IP}) = (\mathrm{W}'_{(-2)^k})$.

We call a subset of $1 + 3\mathbb{Z}$ a **principal ideal** if it is has the form $(1 + 3\mathbb{Z})\ell$ for some $\ell \in 1 + 3\mathbb{Z}$. Notice that every two numbers $\ell, \ell' \in 1 + 3\mathbb{Z}$ have a unique greatest common divisor in $1+3\mathbb{Z}$, which we denote by $\gcd(\ell,\ell')$. For example, $\gcd(40,100)=-20$.

Proposition 8.1. *1.* $(\mathrm{W}_{m'})+(\mathrm{W}_{m''})+(\mathrm{W}_{m'''}) \implies (\mathrm{W}_{m'-m''+m'''})$.

2. If $1+3m \mid 1+3m'$ then $(W_m) \implies (W_{m'})$.

3. $(\mathrm{W}'_\ell)+(\mathrm{W}'_{\ell'}) \implies (\mathrm{W}'_{\gcd(\ell,\ell')})$.

Proof. For completeness we copy the proof of the case $p=-1$ from [6, Lemma 3.1]: assuming (W_m), we have that $x^{\lambda^{-2m}}(yx)^{\lambda^{-(2m+1)}} = x^{\rho^{2m}}(yx)^{\rho^{2m+1}} \overset{(11)}{=} ((yx)^{\rho^m}\cdot y^{\rho^{m+1}})^{\rho^m}\cdot((yx)^{\rho^m})^{\rho^{m+1}} \overset{(11)}{=} (y^{\rho^{m+1}})^{\rho^m} = y^{\lambda^{-2m-1}}$, proving (W_{-2m-1}).

1. Assume $(\mathrm{W}_{m'})$, $(\mathrm{W}_{m''})$ and $(\mathrm{W}_{m'''})$ hold. Applying (13) and (14) alternatively, we have that

$$\begin{aligned}
\rho^{m'-m''+m'''}\ell_x\rho^{-(m'-m''+m''')} &= \rho^{m'''}\lambda^{m''}\rho^{m'}\ell_x\rho^{-m'}\lambda^{-m''}\rho^{-m'''}\\
&= \rho^{m'''}\lambda^{m''}r^{-1}_{x^{\rho^{m'+1}}}\lambda^{-m''}\rho^{-m'''}\\
&= \rho^{m'''}\ell_{x^{\rho^{m'-m''}}}\rho^{-m'''}\\
&= r^{-1}_{x^{\rho^{m'-m''+m'''+1}}},
\end{aligned}$$

   which is $(\mathrm{W}_{m'-m''+m'''})$.

2. Taking m', m'' in the previous claim to be m and $-2m-1$, it now follows that $(\mathrm{W}'_{1+3m})+(\mathrm{W}'_{(1+3p)(1+3m)}) = (\mathrm{W}'_{1+3m})+(\mathrm{W}'_{(4+3p)(1+3m)})$, and we are done by induction on p.

3. Let $I\subseteq 1+3\mathbb{Z}$ be the set of integers p for which (W'_p) is a consequence of the pair (W'_ℓ) and $(\mathrm{W}'_{\ell'})$. Let $a\in I$ be minimal in terms of absolute value. Assuming a does not divide $\gcd(\ell,\ell')$, let b be a minimal element of I, in terms of absolute value, not divisible by a. By (15) we have that $-2a\in I$. If a,b have different signs, then $-a-b=a-b+(-2a)\in I$ by the first part, but $|-a-b|<|b|$. If a,b have the same sign, then again $2a-b=a-b+a\in I$, but $|2a-b| = \left|2\frac{a}{b}-1\right||b| < |b|$ because $|a|<|b|$. In either case we have a contradiction.

□

Corollary 8.2. Let L be any loop. The set of integers $p\in 1+3\mathbb{Z}$ for which L satisfies (W'_p), if nonempty, is a principal ideal.

Thus, if L satisfies any of the m-inverse properties, there is a minimal one, of which all of the others are formal consequences of. This may be called the "inverse level" of L. Corollary 8.2 is shown in [5] by using isotrophisms.

8.2 m-inverse for loop extensions

As always, let Q be a group acting on an abelian group K.

Proposition 8.3. *Let m be an odd integer. For $c \in \mathrm{C}^2(Q,K)$, $L = (K,Q,c)$ satisfies* (W_m) *if and only if*

$$(\alpha\beta)^{(3m+1)/2}c = c.$$

Proof. Write $m = 2n+1$. By (5)–(6) we have that

$$(kq)^{\rho^{2n}} = (\psi c)_q^n \cdot kq, \tag{16}$$

regardless of the sign of n. Taking $x = kp$ and $y = k'q$ in (11), acting by pq on the resulting equality and rearranging, we find that (K,Q,c) is has the property (W_m) if and only

$$c_{p,q} = (\delta^1\gamma)_{p,q}(\delta^1\psi c)^n_{p,q}\gamma^{-p}_{p^{-1}}c^{pq}_{(pq)^{-1},p}.$$

Next, we compute by Equation (7) that $((\alpha\beta)^2c)_{p,q} = (\delta^1\gamma)_{p,q}\gamma^{-p}_{p^{-1}}c^{pq}_{(pq)^{-1},p}$. Applying Proposition 5.6 to $(\alpha\beta)^2c$ in place of c, we then find that

$$((\alpha\beta)^{3n+2}c)_{p,q} = (\delta^1\gamma)_{p,q}(\delta^1\psi c)^n_{p,q}\gamma^{-p}_{p^{-1}}c^{pq}_{(pq)^{-1},p},$$

and the result follows. □

Remark 8.4. In terms of n, Proposition 8.3 reads that $L = (K,Q,c)$ satisfies (W_{2n+1}) if and only if $(\alpha\beta)^{3n+2}c = c$. To cover the other non-zero residue of 3 substitute $-n-1$ for n, to find that $(\mathrm{W}_{-(2n+1)})$ holds if and only if $(\alpha\beta)^{-(3n+1)}c = c$, which is equivalent to $(\alpha\beta)^{3n+1}c = c$.

Taking $m = -1$ in Proposition 8.3 recaptures the fact that $\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle}$ corresponds to the weak inverse property, (WI). For $m = 1$ we obtain that $\mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^2\right\rangle}$ is the doubly weak inverse property (W^2IP). More generally, taking $m = \frac{(-2)^k-1}{3}$, we obtain:

Corollary 8.5. The extension $L = (K,Q,c)$ satisfies the property (W^kIP) if and only if $c \in \mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^{2^{k-1}}\right\rangle}$.

8.3 Generalizations of (H)

Let (H^m) denote the property of a loop that ρ^{2m}, equivalently λ^{2m}, are homomorphisms. Here m is allowed to be negative. By [6, Lemma 3.1],

$$(\mathrm{W}'_{2\ell}) \implies (\mathrm{H}^\ell)$$

for any $\ell \equiv 2 \pmod 3$; for example, $(\mathrm{W}^k\mathrm{IP}) \implies (\mathrm{H}^{2^{k-1}})$; and in particular $(\mathrm{WI}) = (\mathrm{W}^1\mathrm{IP}) \implies (\mathrm{H}^1) = (\mathrm{H})$.

The following proposition complements Proposition 8.3, as we see in the theorem below.

Proposition 8.6. *The following are equivalent for the loop* (K, Q, c)*:*

1. (H^n) *(namely* λ^{2n} *and* ρ^{2n} *are homomorphisms)*
2. $(\delta^1 \psi c)^n = 1$.
3. $(\alpha\beta)^{3n} c = c$.

Proof. Since $(kq)^{\rho^{2n}} = (\psi c)_q^n \cdot kq$ by Example 16, it immediately follows that ρ^{2n} is a homomorphism if and only if $(\delta^1\psi(c^m) = 1$. But by Proposition 5.6 we also have that $(\alpha\beta)^{3n}c = (\delta^1\psi c)^n \cdot c$. □

The same computation yields the following observation, concerning weak versions of (Inv):

Proposition 8.7. *The following are equivalent for* $c \in \mathrm{C}^2(Q, K)$*:*

1. $\lambda^{2n} = 1$ *holds in* (K, Q, c).
2. $(\psi c)^n = 1$.

8.4 Invariants of even subgroups

Theorem 8.8. *The subspaces of* $\mathrm{C}^2(Q, K)$ *fixed under subgroups of* $C_\infty = \langle \alpha\beta \rangle$ *are*

$$(W_{2n+1}) = \mathrm{C}^2(Q, K)^{\left\langle (\alpha\beta)^{3n+2} \right\rangle}$$

and

$$(H^n) = \mathrm{C}^2(Q, K)^{\left\langle (\alpha\beta)^{3n} \right\rangle}.$$

Proof. Combine Remark 8.4 and Proposition 8.6, noting that any nontrivial subgroup of $\langle \alpha\beta \rangle$ can be uniquely represented in one of the forms $\left\langle (\alpha\beta)^{3n+2} \right\rangle$ (for $n \in \mathbb{Z}$) and $\left\langle (\alpha\beta)^{3n} \right\rangle$ (for $n > 0$). □

Proof of Theorem 1.1. The action of D_∞ on $\mathrm{C}^2(Q, K)$ is defined in Proposition 5.2. The subspaces fixed under odd subgroups are given in Theorem 7.1. The subspaces fixed under even subgroups are given in Theorem 8.8. □

9 Extensions of $\mathbb{Z}_4$

In this final section we describe the extensions (K, Q, c) for $Q = \langle \sigma \rangle$ the cyclic group of order 4, acting on an arbitrary abelian group K. This is a case of interest in light of the fact that any Buchsteiner loop is a nuclear extension of an abelian group of exponent 4 (see [6, Theorem 7.14]).

For brevity we denote $c_{\sigma^i, \sigma^j} = c_{ij}$ (and $a_{\sigma^i} = a_i$), and write c in a 3×3 matrix form, omitting the trivial row and column corresponding to the identity element of Q.

We are interested in c up to equivalence, so we may multiply c by $\delta^1 a$ for some $a \in \mathrm{C}^1(Q,K)$. Note that $(\delta^1 a)_2 = a_1 a_1^\sigma a_2^{-1}$ and $(\delta^1 a)_3 = a_1 a_2^\sigma a_3^{-1}$, so choosing a_2 and then a_3 properly, we may henceforth assume $c_{11} = c_{12} = 1$. Equivalence under this reduction amounts to entry-wise multiplication by $\delta^1 a = \begin{pmatrix} 1 & 1 & N(a_1) \\ 1 & N(a_1) & N(a_1) \\ N(a_1) & N(a_1) & N(a_1) \end{pmatrix}$ where $N(k) = kk^\sigma k^{\sigma^2} k^{\sigma^3}$ and $a_1 \in K$ is arbitrary. Solving the equations in Proposition 3.1 for $c_{ij} \in K$, we find:

Proposition 9.1. *The conditions for the loop $(K, \mathbb{Z}_4, c)$ to satisfy the respective properties are as follows:*

(LI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ k' & \pi & \pi k'^{-\sigma^2} \\ k^{\sigma^3} & k^{\sigma^3} & k^{\sigma^3} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^{\sigma^2} = \pi$.

(RI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ k' & \pi & k^\sigma \\ k^{\sigma^3} & \pi^\sigma & k^{\sigma^2} k'^{-1} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^{\sigma^2} = \pi$.

(WI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ \pi & k & k' \\ \pi^{-1} k & \pi^{-1} k'^{\sigma^3} & k'^{\sigma^2} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^\sigma = \pi^{-1}$.

(AI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ k' & \pi & \pi k^\sigma k^{-1} \\ k^{\sigma^3} & \pi^\sigma k^{\sigma^3} k^{-1} k'^{-\sigma} & \pi^{-1} k^{\sigma^2} k^{\sigma^3} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^{\sigma^2} = \pi$.

(Inv) *if* $c_{13} = c_{31}^\sigma$ *and* $c_{22}^{\sigma^2} = c_{22}$.

(H) *if there is* $\mu \in K$ *such that* $c_{13} = \mu^{-1} c_{31}^\sigma$ *and* $c_{22}^{\sigma^2} = \mu\mu^\sigma c_{22}$.

Intersecting any two of the conditions for (LI), (RI), (AI) and (WI), we obtain:

Proposition 9.2. *(K, Q, c) has* (IP) *when* $c \approx \begin{pmatrix} 1 & 1 & \pi \\ \pi\pi^{-\sigma} & \pi & \pi^\sigma \\ \pi^\sigma & \pi^\sigma & \pi^\sigma \end{pmatrix}$ *for* $\pi \in K$ *satisfying* $\pi^{\sigma^2} = \pi$. *This loop is a group when* $\pi \in K^\sigma$.

Letting $N : K \to K$ denote the function $N(k) = kk^\sigma k^{\sigma^2} k^{\sigma^3}$, Proposition 9.2 gives a 1-to-1 correspondence between $K^{\sigma^2}/N(K)$ and extensions of $\mathbb{Z}_4$ satisfying (IP), extending the well known correspondence between $\mathrm{H}^2(\mathbb{Z}_4, K) = K^\sigma/N(K)$ and group extensions.

As a complement to Proposition 2.1, we now give counterexamples for each of the implications (LI), (RI), (AI), (WI) + (Inv) $\implies$ (IP).

Corollary 9.3. For each of the four halves, there is a loop of order 8, in fact an extensions of $Q = \mathbb{Z}_4$ by $K = \mathbb{Z}_2$, satisfying this property as well as (Inv), but not any of the other three.

Proof. In any of the formulas of Proposition 9.1 take $\pi = k' = 1$ and $k \neq 1$ to avoid the form of Proposition 9.2. □

Let $K_{(2)}$ denote the 2-torsion subgroup of K.

Proposition 9.4. *Let K be an abelian group on which $Q = \mathbb{Z}_4$ acts. The following are equivalent:*

1. *(WI) $\Longrightarrow$ (Inv) for loops of the form $L = (K, \mathbb{Z}_4, c)$;*
2. *(H) $\Longrightarrow$ (Inv) for loops of the form $L = (K, \mathbb{Z}_4, c)$;*
3. *$K_{(2)} = 1$ and the action is trivial.*

Proof. 2. $\Longrightarrow$ 1. because (WI) $\Longrightarrow$ (H).

1. $\Longrightarrow$ 3. By Proposition 9.1, the condition for (Inv) is that $c_{31} = c_{13}^{\sigma^3}$ and $c_{22}^{\sigma^2} = c_{22}$. For the function c given in the same proposition for (WI), this holds when $k^{\sigma^2} = k$ and $\pi = kk^{-\sigma}$ (which imply $\pi^\sigma = \pi^{-1}$). If the action is nontrivial these conditions are countered by taking $\pi = 1$ and $k \notin K^\sigma$. If the action is trivial and there are elements of order 2, take π to be such an element and $k = 1$. It follows that the action is trivial and $K_{(2)} = 1$.

3. $\Longrightarrow$ 2. Again by Proposition 9.1, (H) $\Longrightarrow$ (Inv) if $\mu\mu^\sigma = \pi^{\sigma^2}\pi^{-1}$ implies $\mu = 1$. This condition can be written as $(\mu\pi^\sigma\pi^{-1})(\mu\pi^\sigma\pi^{-1})^\sigma = 1$, or equivalently $\mu \in \mathrm{Ker}(1+\sigma)\mathrm{Im}(1-\sigma)$, viewing K as a $\mathbb{Z}[Q]$-module, written multiplicatively. If the action is trivial and there are no elements of order 2, we have that $\mathrm{Im}(1-\sigma) = 1$ and $\mathrm{Ker}(1+\sigma) = \mathrm{Ker}(2) = 1$. □

Recall that (LI), (RI) and (AI) each imply (Inv). Following the recipe in the first part of Proposition 9.4, we construct an example showing that (WI)$\not\Longrightarrow$(Inv) for loop extensions.

Example 9.5. Let $L = \{\epsilon^i\sigma^j\}_{i\in\mathbb{Z}_3,\, j\in\mathbb{Z}_4}$ be the (monogenic) loop of order 12 with multiplication rule $\epsilon^i\sigma^j \cdot \epsilon^{i'}\sigma^{j'} = \epsilon^{i+(-1)^j i' + \delta_{j,-j'}(1-\delta_{j,0})}\sigma^{j+j'}$. Then L satisfies (WI) but not (Inv). (This is the loop $(\mathbb{Z}_3, \mathbb{Z}_4, c)$ where $\mathbb{Z}_4$ acts by inversion and c is taken from the formula for (WI) in Proposition 9.1 with $k = \epsilon$ and $k' = \pi = 1$.)

Remark 9.6. An extension $L = (K, Q, c)$ is commutative if Q is commutative, its action on K is trivial, and $c_{p,q} = c_{q,p}$ for all p, q. When $Q = \mathbb{Z}_4$, assuming commutativity means that either (LI) or (RI) implies associativity. On the other hand the examples for (AI)$\not\Longrightarrow$(IP) and (WI)$\not\Longrightarrow$(IP) in Corollary 9.3 are commutative. Example 9.5 for (WI)$\not\Longrightarrow$(Inv) is flexible, but not commutative.

As noted in Remark 5.3, $\langle\alpha,\beta\rangle$ acts on the quotient space $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$, namely on extensions up to equivalence. Clearly,

$$\mathrm{C}^2(Q,K)^{\langle\alpha\rangle}/\mathrm{B}^2(Q,K) \leq (\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K))^{\langle\alpha\rangle},$$

and likewise for β (or any group action). If $K_2 = 1$ this is an equality, because $\alpha c = c \cdot \delta^1 a$ implies $(\delta^1 a)^2 = 1$. However, when K has 2-torsion the situation is more delicate:

Example 9.7. Let $Q = \mathbb{Z}_4$ act on $K = \langle t_0, t_1, t_2, t_3\rangle \cong (\mathbb{Z}_2)^4$ by permuting the indices. Consider the cocycle $c = \begin{pmatrix} 1 & 1 & 1 \\ 1 & t_0t_1 & t_0t_1 \\ t_0t_1t_2t_3 & t_0t_1t_2t_3 & t_0t_1t_2t_3 \end{pmatrix}$. Then $(K,Q,c) \cong (K,Q,\alpha c)$ because $\alpha c{\cdot}c^{-1} \in \mathrm{B}^2(Q,K)$, but $\alpha c \neq c$, and indeed (K,Q,c) does not satisfy (LI): $t_0t_1t_2t_3\sigma^2 = (\sigma^2)^\lambda \cdot (\sigma^2 \cdot \sigma^2) \neq \sigma^2$.

Similar examples can be constructed for the other properties.

References

[1] R. Artzy, "Contributions to the theory of loops", Trans. AMS **60**, 245–354, (1946).

[2] R. Artzy, "On automorphic-inverse proerties in loops", Proc. AMS **10**, 588–591, (1959).

[3] K.S. Brown, "Cohomology of Groups", Graduate Texts in Mathematics **87**, Springer, 1982.

[4] R.H. Bruck, "A survey of binary systems", Berlin-Heidelberg, 1958.

[5] A. Drápal and V.A. Shcherbakov, "Identities and the group of isostrophisms", Commentationes Mathematicae Universitatis Carolinae, **53**(3), 347–374, (2012).

[6] P. Csörgő, A. Drápal, M.K. Kinyon. "Buchsteiner loops", International Journal of Algebra and Computation, **19**(08), (2007).

[7] E.G. Goodaire and D.A. Robinson, "A class of loops which are isomorphic to all loop isotopes", Canad. J. Math. **34**, 662–672, (1982).

[8] K.W. Johnson, M.K. Kinyon, G.P. Nagy and P. Vojtěchovský, "Searching for small simple automorphic loops", LMS J. Comput. Math. **14**, 200–213, (2011).

[9] P. Nagy, "Nuclear Properties of Loop Extensions", Results in Mathematics, **74**:100, (2019).

[10] B.B. Karkliňš and V.B. Karkliň, “Inversnyje lupy”, Mat. Issled. **39**, 87–101, (1976).

[11] J. Marshall Osborn, “Loops with the weak inverse property”, Pacific J Math, **10**(1), (1960).

[12] D.A. Robinson, “Bol Loops”, Tran AMS, **123**(2), 341–354, (1966).

Department of Mathematics,
Bar Ilan University,
Ramat Gan,
Israel
e-mail: vishne@math.biu.ac.il