São Paulo Journal of Mathematical Sciences (2020) 14:152–164
https://doi.org/10.1007/s40863-019-00130-x

ORIGINAL ARTICLE

Isomorphism invariants for linear quasigroups

Jonathan D. H. Smith[1] · **Stefanie G. Wang**[2]

Published online: 9 April 2019

Abstract
For a unital ring S, an S-linear quasigroup is a unital S-module, with automorphisms ρ and λ giving a (nonassociative) multiplication $x \cdot y = x^\rho + y^\lambda$. If S is the field of complex numbers, then ordinary characters provide a complete linear isomorphism invariant for finite-dimensional S-linear quasigroups. Over other rings, it is an open problem to determine tractably computable isomorphism invariants. The paper investigates this isomorphism problem for $\mathbb{Z}$-linear quasigroups. We consider the extent to which ordinary characters classify $\mathbb{Z}$-linear quasigroups and their representations of the free group on two generators. We exhibit non-isomorphic $\mathbb{Z}$-linear quasigroups with the same ordinary character. For a subclass of $\mathbb{Z}$-linear quasigroups, equivalences of the corresponding ordinary representations are realized by permutational intertwinings. This leads to a new equivalence relation on $\mathbb{Z}$-linear quasigroups, namely permutational similarity. Like the earlier concept of central isotopy, permutational similarity is intermediate between isomorphism and isotopy.

Keywords Quasigroup · Isotopy · Group isotope · T-quasigroup · Ordinary character · Permutation similarity

Mathematics Subject Classification 20N05

1 Introduction

Quasigroups $(Q, \cdot)$ are nonassociative analogues of groups, retaining the cancelativity of the multiplication. A pique[1] $(P, \cdot, e)$ is a quasigroup with a nullary operation that

[1] An acronym for "Pointed Idempotent QUasigroup(E)".

✉ Jonathan D. H. Smith
jdhsmith@iastate.edu

Stefanie G. Wang
sgwang.math@gmail.com

[1] Department of Mathematics, Iowa State University, Ames, IA 50011, USA

[2] Department of Mathematics, Trinity College, Hartford, CT 06106, USA

selects an idempotent element e. The inner multiplication group of a pique P is the stabilizer of e in the group of permutations of P generated by all the right and left multiplications.

For a commutative, unital ring S, an S-linear pique or S-linear quasigroup is an S-module A equipped with automorphisms ρ and λ that furnish a pique multiplication $x \cdot y = x^{\rho} + y^{\lambda}$, with 0 as the pointed idempotent. Two S-linear piques are S-isomorphic if they are isomorphic via an invertible S-linear transformation (module isomorphism).

Finite-dimensional $\mathbb{C}$-linear piques are classified up to $\mathbb{C}$-linear isomorphism by their so-called ordinary characters, obtained from the representation of the free group on two generators that they afford. Given a finite $\mathbb{Z}$-linear pique A, one may linearize the underlying combinatorial structure to obtain a $\mathbb{C}$-linear pique $\mathbb{C}A$, the so-called complexification of the $\mathbb{Z}$-linear pique A. Our primary concern is the extent to which ordinary characters of complexifications classify $\mathbb{Z}$-linear piques. The main result (Theorem 3.11) shows that for a large class of $\mathbb{Z}$-linear pique structures, namely on cyclic groups of order not divisible by 8, two piques that have the same complexified ordinary character are permutationally similar, i.e., the permutation actions of their respective inner multiplication groups are similar.

1.1 Outline of the paper

We begin with definitions and examples of quasigroups and linear quasigroups in Sect. 2. We define linear quasigroups and their S-linear representations for a commutative unital ring S. Theorem 2.12 identifies S-linear piques with the S-linear representations of the free group on two generators that they afford. This allows us to study the representations in lieu of the piques. Permutational similarity is defined in Sect. 2.4, while Sect. 2.5 defines ordinary characters and the complexifications of $\mathbb{Z}$-linear piques. Theorem 2.16 observes that isomorphic $\mathbb{Z}$-linear piques have the same ordinary character.

Section 3 considers isomorphism invariants for $\mathbb{Z}$-linear piques on cyclic groups of finite order not divisible by 8. Linear piques defined on $\mathbb{Z}/_n$ for $n < 5$ are classified up to isomorphism by the ordinary characters of their complexifications, the permutation characters introduced in Definition 3.1 (Sect. 3.2). However, ordinary character theory does not suffice to cover all linear piques. Indeed, Proposition 3.12 exhibits non-isomorphic pique structures on $\mathbb{Z}/_5$ having the same permutation character. The main result (Theorem 3.11) proves that linear piques defined on cyclic groups of order not divisible by 8, having the same permutation character, are permutationally similar. The final Sect. 3.6 observes that the same statement actually still applies for pique structures on $\mathbb{Z}/_8$.

1.2 Related invariants

Given a commutative, unital ring S and an S-module A, the S-linear piques constructed on A are all isotopic to the abelian group $(A, +, 0)$. Their classification up to isomorphism may be regarded as a special case of the main problem considered

by Drápal in [4], namely the isomorphism problem for isotopes of a given (not necessarily abelian) group. However, the general solution to the isomorphism problem provided by [4] appears to be computationally intractable, leaving open the search for less powerful but rather more accessible invariants. This situation is analogous to that prevailing in knot theory, where the existence of complete invariants does not preclude the continuing search for various weaker invariants with a lower computational complexity.

1.3 Conventions

The paper follows the general algebraic convention of placing a function to the right of its argument, either on the line or as a superfix. This convention allows composites of functions to be read in natural order from left to right, and serves to minimize the occurrence of brackets, which otherwise proliferate when one studies non-associative structures.

2 Linear piques

2.1 Quasigroups and piques

Definition 2.1 A *quasigroup* $(Q, \cdot, \backslash, /)$ is an algebra with three binary operations, multiplication $\cdot$, left division $\backslash$, and right division $/$, such that for all $x, y \in Q$,

$$y\backslash(y \cdot x) = x = (x \cdot y)/y \tag{2.1}$$
$$y \cdot (y\backslash x) = x = (x/y) \cdot y \tag{2.2}$$

are satisfied.

Definition 2.2 A *pique* $(Q, \cdot, /, \backslash, e)$ is a quasigroup with a pointed idempotent element e such that $e \cdot e = e$.

Definition 2.3 [10, Sect. 2.4] Let $(Q, \cdot, /, \backslash, e)$ be a pique. The stabilizer of e in the group of permutations of Q generated by all the right multiplications $R(q)\colon x \mapsto x \cdot q$ and left multiplications $L(q)\colon x \mapsto q \cdot x$ (for $q \in Q$) is called the *inner multiplication group* of the pique.

A pique is a pointed set, where the idempotent element serves as the basepoint. Maps between pointed sets send basepoint to basepoint. For pique homomorphisms, the pointed idempotent element of the domain maps to the pointed idempotent element of the codomain.

Example 2.4 Each group is an associative pique, with the identity element as the pointed idempotent element. The inner multiplication group is the inner automorphism group.

Example 2.5 Integers under subtraction form a nonassociative pique, with 0 as the pointed idempotent. The unique nontrivial element of the inner multiplication group is the negation $\mathbb{Z} \to \mathbb{Z}\colon n \mapsto -n$.

2.2 Linear piques

Definition 2.6 Suppose that S is a commutative, unital ring. A pique $(A, \cdot, /, \backslash, 0)$ is said to be *S-linear* if there is a unital S-module structure $(A, +, 0)$, with S-module automorphisms λ and ρ such that

$$x \cdot y = x^{\rho} + y^{\lambda},\ x/y = (x - y^{\lambda})^{\rho^{-1}}, \text{ and } x\backslash y = (y - x^{\rho})^{\lambda^{-1}} \tag{2.3}$$

for $x, y \in A$.

We identify λ, ρ as the left and right multiplications by the pointed idempotent 0.

Example 2.7 On the one hand, the quasigroup $(\mathbb{Z}/_4, x \circ_1 y)$ with the nonassociative multiplication $x \circ_1 y = x(1\ 2\ 3) + y(1\ 2)$ is a pique with 0 as the pointed idempotent element. However, neither (1 2 3) nor (1 2) is an automorphism of $\mathbb{Z}/_4$. On the other hand, the quasigroup $(\mathbb{Z}/_4, x \circ_2 y)$ with the nonassociative multiplication $x \circ_2 y = x(1\ 3) + y(1\ 3)$ is also a pique with 0 as the pointed idempotent element. More importantly, the permutation (1 3) corresponds to the automorphism of $\mathbb{Z}/_4$ defined by $x \mapsto 3x$, so $(\mathbb{Z}/_4, x \circ_2 y)$ is a $\mathbb{Z}$-linear pique.

Example 2.8 [9, Sect. 3.2] [11, Sect. 3] Suppose that S is a commutative unital ring. Then S-linear representations of the free group F on two generators are equivalent to S-linear piques. Indeed, suppose that F is free on elements R and S. If $\alpha\colon G \to \mathrm{End}_S(A)$ is an S-linear representation, then an S-linear pique $(A, \cdot, /, \backslash, 0)$ is defined by $x \cdot y = x^{\rho} + y^{\lambda}$ with $\rho = R\alpha$ and $\lambda = L\alpha$. Conversely, if $(A, \cdot, /, \backslash, 0)$ is an S-linear pique, then $R \mapsto R(0)$ and $L \mapsto L(0)$ extends to an S-linear representation α of F on A.

Remark 2.9 Linear piques, along with their shifted versions $x \cdot y = x^{\rho} + y^{\lambda} + c$ (also described as "T-quasigroups" [2,5]), have been studied for potential applications in cryptography and related fields [1].

2.3 Equivalent representations

Throughout this section, S will denote a commutative, unital ring.

Definition 2.10 Let $\langle R, L\rangle$ be the free group on the doubleton $\{R, L\}$.

(a) Let $(A, \cdot, /, \backslash, 0)$ be an S-linear pique with $x \cdot y = x^{\rho} + y^{\lambda}$. Then the group homomorphism

$$\alpha\colon \langle R, L\rangle \to \mathrm{Aut}_S(A, +, 0);\ R \mapsto \rho\,,\ L \mapsto \lambda$$

is described as the *S-linear representation* that is *afforded* by $(A, \cdot, /, \backslash, 0)$.

(b) Consider two S-modules $(A, +, 0)$ and $(B, +, 0)$. Then corresponding S-linear representations $\alpha\colon \langle R, L\rangle \to \mathrm{Aut}_S(A, +, 0)$ and $\beta\colon \langle R, L\rangle \to \mathrm{Aut}_S(B, +, 0)$ are *equivalent* whenever there exists an S-module isomorphism $f : A \to B$ such that for all g in $\langle R, L\rangle$, the diagram

$$\begin{array}{ccc} A & \xrightarrow{g^\alpha} & A \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[g^\beta]{} & B \end{array} \tag{2.4}$$

commutes. We call f the *intertwining*.

Note that the pair of equations

$$R^\alpha f = f R^\beta \qquad \text{and} \qquad L^\alpha f = f L^\beta \tag{2.5}$$

is equivalent to the commuting of (2.4). Alternatively, one may require that the diagram

$$\begin{array}{ccccc} A & \xleftarrow{L^\alpha} & A & \xrightarrow{R^\alpha} & A \\ {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xleftarrow[L^\beta]{} & B & \xrightarrow[R^\beta]{} & B \end{array} \tag{2.6}$$

commutes.

Lemma 2.11 *Suppose that $f\colon (A, \circ_1) \to (B, \circ_2)$ is a pique isomorphism between S-linear piques $(A, \circ_1)$ and $(B, \circ_2)$. Let α and β be the respective S-linear representations that they afford. Then the equations (2.5) hold.*

Proof One has

$$\begin{aligned} aR^\alpha f &= (a \circ_1 0)^f = a^f \circ_2 0 = a^f R^\beta \quad \text{and} \\ aL^\alpha f &= (0 \circ_1 a)^f = 0 \circ_2 a^f = a^f L^\beta. \end{aligned}$$

for each element a of A. □

Theorem 2.12 *Let $(A, \circ_1)$ and $(B, \circ_2)$ be two S-linear piques. Then they are isomorphic by an S-linear transformation $f\colon A \to B$ if and only if the S-linear representations they afford are equivalent.*

Proof Let $f\colon (A, \circ_1) \to (B, \circ_2)$ be an S-linear pique isomorphism. Suppose that $\alpha\colon \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$ and $\beta\colon \langle R, L\rangle \to \mathrm{Aut}(B, +, 0)$ are the respective S-linear representations afforded by the S-linear piques. By Lemma 2.11, the equations (2.5) hold. It follows that f is an intertwining witnessing the equivalence of α and β.

Now let $\alpha\colon \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$ and $\beta\colon \langle R, L\rangle \to \mathrm{Aut}(B, +, 0)$ be equivalent S-linear representations, with an intertwining $f\colon A \to B$. Then for x, y in A, one has

$$\begin{aligned}(x \circ_1 y)f &= (xR^{\alpha} + yL^{\alpha})f \\ &= (xR^{\alpha})f + (yL^{\alpha})f \\ &= xfR^{\beta} + yfL^{\beta} \\ &= xf \circ_2 yf\,,\end{aligned}$$

so that $f\colon (A, \circ_1) \to (B, \circ_2)$ is an S-linear pique isomorphism. □

2.4 Permutational similarity

In what follows, we will consider a modified version of the commuting diagram (2.6).

Definition 2.13 Let A be a finite abelian group, with $\mathbb{Z}$-linear pique structures $(A, \circ_1)$ and $(A, \circ_2)$ affording respective representations

$$\alpha_i\colon \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$$

for $i = 1, 2$. Then the piques $(A, \circ_1)$ and $(A, \circ_2)$, or the representations they afford, are said to be *permutationally similar*, via a permutation π of the underlying set A, if the diagram

$$\begin{array}{ccccc} A & \xleftarrow{L^{\alpha_1}} & A & \xrightarrow{R^{\alpha_1}} & A \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ A & \xleftarrow[L^{\alpha_2}]{} & A & \xrightarrow[R^{\alpha_2}]{} & A \end{array} \tag{2.7}$$

commutes. In other words, the permutation π conjugates both R^{α_1} to R^{α_2} and L^{α_1} to L^{α_2} within the permutation group $A!$ of the set A.

Consider two permutationally similar piques $(A, \circ_1)$ and $(A, \circ_2)$ as in Definition 2.13. If π is not an automorphism of the abelian group $(A, +, 0)$, then the permutational similarity of representations furnished by π is not an equivalence in the sense of Definition 2.10. On the other hand, since both the piques are isotopic to the abelian group A, they are mutually isotopic (compare [10, Sect. I.2] for a discussion of isotopy). Furthermore, Theorem 2.12 shows that if two $\mathbb{Z}$-linear piques on the abelian group A are isomorphic, then they are permutationally similar. Thus permutational similarity is a relationship intermediate between isotopy and isomorphism. As such, it is analogous to the relationship of central isotopy [10, Sect.3.4].

2.5 Ordinary characters of $\mathbb{C}$-linear piques

Definition 2.14 Let G be a group. For a complex vector space V, let $\mathsf{GL}(V)$ be its group of automorphisms.

(a) An *ordinary linear representation* of G is defined as a homomorphism $\rho : G \to \mathsf{GL}(V)$, for some finite-dimensional complex vector space V.
(b) The (*ordinary*) *character* of an ordinary linear representation $\rho\colon G \to \mathsf{GL}(V)$ is the function χ or $\chi_\rho\colon G \to \mathbb{C}; g \mapsto \mathrm{Tr}(g\rho)$.

Definition 2.15 Let $(A, \cdot, /, \backslash, 0)$ be a finite $\mathbb{Z}$-linear pique, affording the $\mathbb{Z}$-linear representation $\alpha : \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$. Let $\mathbb{C}A$ be the complex vector space with basis A. Then the *complexification* of $(A, \cdot, /, \backslash, 0)$ is the $\mathbb{C}$-linear pique structure $(\mathbb{C}A, \cdot, /, \backslash, 0)$ obtained by extension of the pique structure $(A, \cdot, /, \backslash, 0)$. Thus

$$\alpha_{\mathbb{C}}\colon R \mapsto (\mathbb{C}A \to \mathbb{C}A; a \mapsto aR^{\alpha}),\ L \mapsto (\mathbb{C}A \to \mathbb{C}A; a \mapsto aL^{\alpha})$$

serves to specify the $\mathbb{C}$-linear representation $\alpha_{\mathbb{C}}$ that is afforded by the complexification of $(A, \cdot, /, \backslash, 0)$.

Theorem 2.16 *Let $f\colon (A, \cdot, /, \backslash, 0) \to (B, \cdot, /, \backslash, 0)$ be an isomorphism of finite $\mathbb{Z}$-linear piques affording respective $\mathbb{Z}$-linear representations α and β. Then the respective $\mathbb{C}$-linear representations $\alpha_{\mathbb{C}}$ and $\beta_{\mathbb{C}}$ of their complexifications have the same ordinary character.*

Proof The bijection $f\colon A \to B$ may be extended to a unique $\mathbb{C}$-linear isomorphism $\mathbb{C}f\colon \mathbb{C}A \to \mathbb{C}B$. By Lemma 2.11, one has $g^{\alpha} f = fg^{\beta}$ for all g in $\langle R, L\rangle$. By linearity, one then has $g^{\alpha_{\mathbb{C}}}(\mathbb{C}f) = (\mathbb{C}f)g^{\beta_{\mathbb{C}}}$ for all g in $\langle R, L\rangle$. Let χ_A and χ_B be the respective characters of $\alpha_{\mathbb{C}}$ and $\beta_{\mathbb{C}}$. Then

$$\chi_B(g\beta_{\mathbb{C}}) = \mathrm{Tr}(g\beta_{\mathbb{C}}) = \mathrm{Tr}\big((\mathbb{C}f)^{-1} g^{\alpha_{\mathbb{C}}} (\mathbb{C}f)\big) = \mathrm{Tr}(g\alpha_{\mathbb{C}}) = \chi_A(g\alpha_{\mathbb{C}})$$

for each g in $\langle R, L\rangle$. □

Remark 2.17 Although the result will not be needed for subsequent work in the current paper, it should be noted that Theorem 2.12, along with [9, Prop. 634], [10, Th. 12.4], implies that finite-dimensional $\mathbb{C}$-linear quasigroups are classified up to $\mathbb{C}$-linear isomorphism by their ordinary characters.

3 Linear piques on finite cyclic groups

3.1 Permutation characters

The following definition provides a purely combinatorial specification for the character of the ordinary representation that is afforded by the complexification of a finite $\mathbb{Z}$-linear pique (compare [7, Exercise 2.2]).

Definition 3.1 Let $(A, \cdot, /, \backslash, 0)$ be a finite $\mathbb{Z}$-linear pique, affording the $\mathbb{Z}$-linear representation $\alpha : \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$. For an element g of $\langle R, L\rangle$, the *permutation character* $\chi(g)$ is the number of fixed points of the permutation g^{α} of the set A.

Although the group $\langle R, L\rangle$ is infinite, the permutation character is determined by the fixed-point numbers for each member of the finite set $\langle R, L\rangle^{\alpha}$ of permutations of A, the inner multiplication group of the pique $(A, \cdot, /, \backslash, 0)$. We generally use cycle notation for permutations of A, recognizing the number of fixed points of a permutation as the number of one-cycles in its cycle decomposition.

For $1 < n \in \mathbb{Z}$, we will consider $\mathbb{Z}$-linear piques defined on finite cyclic groups $(\mathbb{Z}/_n, +.0)$. We write $(\mathbb{Z}/_n)^*$ for the group of units of the monoid $(\mathbb{Z}/_n, \cdot, 1)$, the set of residues coprime to n. We use the isomorphism

$$(\mathbb{Z}/_n)^* \to \mathrm{Aut}(\mathbb{Z}/_n, +, 0); r \mapsto (x \mapsto rx)$$

[8, 5.7.11] to identify automorphisms of finite cyclic groups. Thus the order of the automorphism group $\mathrm{Aut}(\mathbb{Z}/_n, +, 0)$ is given by the Euler function $\varphi(n)$. We note the following for future reference.

Lemma 3.2 *Let p be a prime number, and let k be a positive integer. Then an automorphism of $\mathbb{Z}/_{p^k}$ has p^j many fixed points, for some $0 < j \leq k$.*

Proof The set of fixed points of a group automorphism forms a subgroup of the group in question. The result then follows by Lagrange's Theorem. □

3.2 Linear piques on small cyclic groups

We build piques on $\mathbb{Z}/_3$ by assigning automorphisms of $(\mathbb{Z}/_3, +, 0)$ to R, L. Since R, L can be 1 or 2, we have four possibilities for the binary multiplication. Here, we exhibit the permutation character table for $\mathbb{Z}$-linear representations of each linear pique defined on $\mathbb{Z}/_3$ (Table 1).

The ordinary characters of R, L are distinct for linear piques of order 3. By Theorem 2.16, the four piques are all mutually non-isomorphic. Thus the permutation character completely resolves the isomorphism classes of linear piques of order 3:

Proposition 3.3 *Linear piques defined on $\mathbb{Z}/_3$ are classified completely up to isomorphism by their permutation characters.*

In similar vein, one obtains the following:

Proposition 3.4 *Linear piques defined on each of $\mathbb{Z}/_2$ and $\mathbb{Z}/_4$ are classified completely up to isomorphism by their permutation characters.*

Table 1 Permutation characters for linear piques on $\mathbb{Z}/_3$

$x \cdot y$	R	L	$\chi(R)$	$\chi(L)$
$x + y$	(1)	(1)	3	3
$x + 2y$	(1)	(1 2)	3	1
$2x + y$	(1 2)	(1)	1	3
$2x + 2y$	(1 2)	(1 2)	1	1

3.3 Cyclic groups of prime power order

Consider a cyclic group $\mathbb{Z}/_{p^k}$, where p is a prime and k is a positive integer.

Lemma 3.5 [8, 5.7.12] *If p is an odd prime and k is a positive integer, or $p = 2$ and $k \in \{1, 2\}$, then $\mathrm{Aut}(\mathbb{Z}/_{p^k}, +, 0)$ is a cyclic group of order $\varphi(p^k) = p^{k-1}(p-1)$.*

Lemma 3.6 *Let $\mathbb{Z}$-linear representations $\alpha_i : \langle R, L\rangle \to \mathrm{Aut}(\mathbb{Z}/_{p^k})$ have equal respective permutation characters χ_i, for $i = 1, 2$. Then for each element g of $\langle R, L\rangle$, the automorphisms g^{α_1} and g^{α_2} have the same order.*

Proof Suppose, without loss of generality, that $s = |\langle g^{\alpha_1}\rangle| \geq |\langle g^{\alpha_2}\rangle| = t$. Then $\chi_1(g^t) = \chi_2(g^t) = p^k$, so that $g^{\alpha_1 t} = g^{t\alpha_1} = 1$ and $s \leq t$. □

In the following, a *linear permutation representation* of a finite group is the linearization of a permutation representation. Thus let $G \to X!$ be a homomorphism from a group G to the group $X!$ of bijections of a finite set X. Then, for a commutative, unital ring S, let SX denote the free S-module on X. The corresponding linear permutation representation of G on the module SX sends each group element g to the permutation matrix determined by the action of g on X.

Lemma 3.7 [3, Ex. 2.1] *Two linear permutation representations of a finite cyclic group, with the same character, are isomorphic.*

Proposition 3.8 *Let p be a prime number, and let k be a positive integer. Suppose that two linear pique structures defined on $\mathbb{Z}/p^k$ have the same permutation character. Suppose that one of the three following hypotheses applies:*

(a) *Let p be an odd prime;*
(b) *Let $p = 2$ and $k \in \{1, 2\}$;*
(c) *Let $p = 2$ and $k > 2$, but assume that the inner multiplication groups of the two piques are cyclic.*

Then the corresponding representations are permutationally similar.

Proof Suppose that, for $i = 1, 2$, the piques correspond to respective representations $\alpha_i : \langle R, L\rangle \to \mathrm{Aut}(\mathbb{Z}/_{p^k})$. Recall that the image of $\langle R, L\rangle$ under α_i is the inner multiplication group of the corresponding pique.

Suppose, without loss of generality, that $|\langle R, L\rangle^{\alpha_1}| \geq |\langle R, L\rangle^{\alpha_2}|$. Let g be an element of $\langle R, L\rangle$ whose image under α_1 generates $\langle R, L\rangle^{\alpha_1}$, so the order of g^{α_1} is $|\langle R, L\rangle^{\alpha_1}|$. Then by Lemma 3.6, the order of g^{α_2} is $|\langle R, L\rangle^{\alpha_1}|$. Thus $|\langle R, L\rangle^{\alpha_1}| = |\langle R, L\rangle^{\alpha_2}|$, and g^{α_2} generates $\langle R, L\rangle^{\alpha_2}$. Consider the finite cyclic group $G \cong \langle g^{\alpha_1}\rangle \cong \langle g^{\alpha_2}\rangle$, with permutation representations $\gamma_i : G \to \mathrm{Aut}(\mathbb{Z}/_{p^k})$; $g^{\alpha_i t} \mapsto g^{t\alpha_i}$ for $i = 1, 2$. The respective permutation characters are equal, so by Lemma 3.7, the two permutation representations γ_i of G are isomorphic. It follows that the representations α_1, α_2 are permutationally similar. □

Remark 3.9 The first two rows of Table 2 provide an illustration of Proposition 3.8(c).

3.4 Cyclic groups of order not divisible by 8

For any positive integer m, consider a factorization

$$m = \prod_{i=1}^{s} p_i^{k_i}$$

with distinct primes $p_1 < \cdots < p_s$ for $1 \leq i \leq s$. Write $q_i = p_i^{k_i}$ for $1 \leq i \leq s$. We refer to q_i as the p_i-*part* of m. Now for $1 < n \in \mathbb{Z}$, fix the notation $n = \prod_{i=1}^{s} p_i^{k_i}$, with distinct primes $p_1 < \cdots < p_s$ and positive exponents $k_1, \ldots, k_s$, for $1 \leq i \leq s$.

Lemma 3.10 *[8, 5.7.3] Let A be an abelian group of order n. For $1 \leq i \leq s$, let A_i be the Sylow p_i-subgroup of A. Then* $\mathrm{Aut}(A) \cong \prod_{i=1}^{s} \mathrm{Aut}(A_i)$.

The Chinese Remainder Theorem gives a direct sum decomposition

$$c\colon \mathbb{Z}/_n \to \bigoplus_{i=1}^{s} \mathbb{Z}/_{q_i}; x \mapsto (x_1, \ldots, x_s)\,. \tag{3.1}$$

In turn, application of Lemma 3.10 to the cyclic group $\mathbb{Z}/_n$ yields the isomorphism

$$a\colon \mathrm{Aut}(\mathbb{Z}/_n) \to \prod_{i=1}^{s} \mathrm{Aut}(\mathbb{Z}/_{q_i}); \theta \mapsto (\theta_1, \ldots, \theta_s)\,. \tag{3.2}$$

For an automorphism θ of $\mathbb{Z}/_n$, let $\pi(\theta)$ be the number of fixed points of θ. For $1 \leq i \leq s$, let $\pi_i(\theta_i)$ be the number of fixed points of θ_i on $\mathbb{Z}/_{q_i}$. By virtue of the set isomorphism $c\colon \mathbb{Z}/_n \to \prod_{i=1}^{s} \mathbb{Z}/_{q_i}$, one has

$$\pi(\theta) = \prod_{i=1}^{s} \pi_i(\theta_i)\,.$$

Then by Lemma 3.2, $\pi_i(\theta_i)$ is the p_i-part of $\pi(\theta)$.

Now restrict the fixed integer n by requiring that it not be divisible by 8. In our notation, this means that $k_1 < 3$ if $p_1 = 2$. As a consequence, the automorphism groups $\mathrm{Aut}(\mathbb{Z}/_{q_i})$ are all cyclic by Lemma 3.5.

Theorem 3.11 *Let A be a finite cyclic group whose order is not divisible by 8. Then if two $\mathbb{Z}$-linear piques on A have the same permutation character, they are permutationally similar.*

Proof By transport of structure, it suffices to examine the case where $A = \mathbb{Z}/_n$, with notation as above. Consider the representations α, α' of $\langle R, L\rangle$ corresponding to the two pique structures. Suppose that their respective permutation characters are χ and χ'. By the hypothesis, these characters coincide. In particular, for each element g of $\langle R, L\rangle$, and for each $1 \leq i \leq s$, the respective p_i-parts of $\chi_i(g)$ and $\chi_i'(g)$ of $\chi(g)$ and $\chi'(g)$ coincide.

For each $1 \leq i \leq s$, and for each element g of $\langle R, L\rangle$, define $g^{\alpha_i} = (g^{\alpha})_i$ and $g^{\alpha_i'} = (g^{\alpha'})_i$ using the notation embodied in (3.2). One obtains respective representations α_i and α_i' of $\langle R, L\rangle$ on $\mathbb{Z}/_{q_i}$, with equal permutation characters $\chi_i(g)$ and $\chi_i'(g)$. By Proposition 3.8, it follows that these representations are permutationally similar, say by permutations $b_i : \mathbb{Z}/_{q_i} \to \mathbb{Z}/_{q_i}$. Then the permutation b of $\mathbb{Z}/_n$, defined by setting $xb = (x_1b_1, \ldots, x_sb_s)c^{-1}$ in the notation of (3.1), yields the desired permutation similarity between α and α'. □

In general, it does not seem to be known to what extent Theorem 3.11 fails for non-cyclic finite abelian groups A.

3.5 Linear piques on $\mathbb{Z}/_5$

Now we consider an explicit example of the preceding work using linear piques defined on $\mathbb{Z}/_5$. Automorphisms of $\mathbb{Z}/_5$ are given by multiplication by non-zero elements. The following table lists the permutations for each element in $(\mathbb{Z}/_5)^*$.

Automorphism	1	2	3	4
Permutation	(1)	(1 2 4 3)	(1 3 4 2)	(1 4)(2 3)

Let $x \circ_1 y = x + 2y$ and $x \circ_2 y = x + 3y$. Since the identity $(xx)x = (yy)y$ holds in $(\mathbb{Z}/_5, \circ_1)$, but not in $(\mathbb{Z}/_5, \circ_2)$, the respective piques are certainly not isomorphic, even as magmas under the quasigroup multiplication.

On the other hand, the representations of $(\mathbb{Z}/_5, \circ_1)$ and $(\mathbb{Z}/_5, \circ_2)$ have the same permutation character. In each case, R maps to the identity, and L maps to a 4-cycle. Let $\{e_i \mid 0 \leq i < 5\}$ be the standard basis for $\mathbb{C}^5$. Consider the permutation matrix

$$P_{(2\ 3)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

of the permutation (2 3). Define the linear transformation

$$\tau : \mathbb{C}^5 \to \mathbb{C}^5; e_i \mapsto e_i P_{(2\ 3)}\,.$$

Since the 4-cycles (1 2 4 3) and (1 3 4 2) are conjugated by (2 3), the ordinary representations for the non-isomorphic $\mathbb{Z}$-linear piques $(\mathbb{Z}/_5, \circ_1)$ and $(\mathbb{Z}/_5, \circ_2)$ are permutationally similar. We may summarize as follows.

Proposition 3.12 *There is a pair of $\mathbb{Z}$-linear piques on $\mathbb{Z}/_5$ which have the same permutation character, and are permutationally similar, but which are not isomorphic.*

3.6 Linear piques defined on $\mathbb{Z}/8$

In this section, to provide some context for Theorem 3.11, we examine the classification of $\mathbb{Z}$-linear pique structures defined on $\mathbb{Z}/8$. To construct a $\mathbb{Z}$-linear pique on $\mathbb{Z}/8$, we must assign ρ, λ the values 1, 3, 5, or 7. The following table lists the permutations for each element in $(\mathbb{Z}/8)^*$.

Automorphism	1	3	5	7
Permutation	(1)	(1 3)(2 6)(5 7)	(1 5)(3 7)	(1 7)(2 6)(3 5)

If two linear piques have the same permutation characters, then the permutations associated with R, L must have the same cycle type. The only possibilities for isomorphic ordinary representations are listed in the following table. We omit opposite quasigroups.

The permutations for 3 and 7 are conjugated by (3 7), while those for 1 and 5 are fixed under conjugation by (3 7). Thus for equivalent complexified ordinary representations, the permutation matrix $P_{(3\ 7)}$ serves as a permutation intertwining. We may summarize as follows, referring to Table 2.

Proposition 3.13 *If a pair of $\mathbb{Z}$-linear piques on $\mathbb{Z}/8$ have the same permutation character, then they are permutationally similar.*

Table 2 Partial character table for linear piques on $\mathbb{Z}/8$

$x \cdot y$	R	L	$\chi(R)$	$\chi(L)$	$\chi(L^2)$	$\chi(RL)$
$x+3y$	(1)	(1 3)(2 6)(5 7)	8	2	8	2
$x+7y$	(1)	(1 7)(2 6)(3 5)	8	2	8	2
$5x+3y$	(1 5)(3 7)	(1 3)(2 6)(5 7)	4	2	8	2
$5x+7y$	(1 5)(3 7)	(1 7)(2 6)(3 5)	4	2	8	2

Acknowledgements We are grateful to a referee for helpful comments on an earlier version of this paper.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Abraham, A., Dvorský, J., Ochodková, E., Snášel, V.: Large quasigroups in cryptography and their properties testing, NaBIC 2009, IEEE, 2010, 965–971 (2009). https://doi.org/10.1109/NABIC.2009.5393884
2. Belyavskaya, G.B.: Abelian quasigroups are T-quasigroups. Quasigroups Relat Syst **1**, 8–21 (1994)
3. Cameron, P.: Permutation Groups. Cambridge University Press, Cambridge (1999)
4. Drápal, A.: Group isotopes and a holomorphic action. Results Math. **54**, 253–272 (2009)
5. Němec, P., Kepka, T.: "T-quasigroups", I. Acta Univ. Carolinae-Math. et Phys. **12**(1), 39–49 (1971)
6. Němec, P., Kepka, T.: "T-quasigroups", II. Acta Univ. Carolinae-Math. et Phys. **12**(2), 31–49 (1971)
7. Serre, J.-P.: Linear Representations of Finite Groups. Springer-Verlag, New York, NY (1977)
8. Scott, W.R.: Group Theory. Prentice-Hall, Englewood Cliffs, NJ (1964)
9. Smith, J.D.H.: Representation Theory of Infinite Groups and Finite Quasigroups. Les Presses de l'Université de Montréal, Montreal (1986)
10. Smith, J.D.H.: An Introduction to Quasigroups and Their Representations. Chapman and Hall/CRC, Boca Raton, FL (2007)
11. Smith, J.D.H.: Groups, triality, and hyperquasigroups. J. Pure Appl. Algebra **216**, 811–825 (2012)