

INVOLUTIVE LATIN SOLUTIONS OF THE YANG-BAXTER EQUATION

MARCO BONATTO, MICHAEL KINYON, DAVID STANOVSKÝ, AND PETR VOJTĚCHOVSKÝ

ABSTRACT. Wolfgang Rump showed that there is a one-to-one correspondence between nondegenerate involutive set-theoretic solutions of the Yang-Baxter equation and binary algebras in which all left translations L_x are bijections, the squaring map is a bijection, and the identity $(xy)(xz) = (yx)(yz)$ holds. We call these algebras *rumples* in analogy with quandles, another class of binary algebras giving solutions of the Yang-Baxter equation. We focus on latin rumples, that is, on rumples in which all right translations are bijections as well.

We prove that an affine latin ruple of order n exists if and only if $n = p_1^{p_1 k_1} \dots p_m^{p_m k_m}$ for some distinct primes p_i and positive integers k_i . A large class of affine solutions is obtained from nonsingular near-circulant matrices A, B satisfying $[A, B] = A^2$. We characterize affine latin rumples as those latin rumples for which the displacement group generated by $L_x L_y^{-1}$ is abelian and normal in the group generated by all translations.

We develop the extension theory of rumples sufficiently to obtain examples of latin rumples that are not affine, not even isotopic to a group. Finally, we investigate latin rumples in which the dual identity $(zx)(yx) = (zy)(xy)$ holds as well, and we show, among other results, that the generators $L_x L_y^{-1}$ of their displacement group have order dividing four.

1. INTRODUCTION

The quantum Yang-Baxter equation is one of the fundamental equations of mathematical physics. A *set-theoretic solution* of the Yang-Baxter equation over a set X is a mapping $r : X \times X \rightarrow X \times X$ such that

$$(YB) \quad (r \times 1)(1 \times r)(r \times 1) = (1 \times r)(r \times 1)(1 \times r)$$

holds as an equality of mappings $X \times X \times X \rightarrow X \times X \times X$. The study of set-theoretic solutions of (YB) was initiated by Drinfeld [9] and it has resulted in a rich line of research devoted to the existence and classification of set-theoretic solutions of various kinds.

The space of set-theoretic solutions is vast, containing classical algebraic structures such as monoids, distributive lattices and certain self-distributive structures, as well as classes of algebras that have only recently begun to receive attention.

A set-theoretic solution $r = (r_1, r_2)$ of (YB) is

- *left nondegenerate* if for each $x \in X$, the mapping $y \mapsto r_1(x, y)$ is a permutation of X ;
- *right nondegenerate* if for each $y \in X$, the mapping $x \mapsto r_2(x, y)$ is a permutation of X ;
- *nondegenerate* if r is both left and right nondegenerate;
- *bijective* if r is a permutation of $X \times X$;
- *involutive* if $r^2 = \text{id}_{X \times X}$.

Date: October 8, 2019.

2000 Mathematics Subject Classification. Primary: 16T25. Secondary: 20N05.

Key words and phrases. Quantum Yang-Baxter equation, nondegenerate involutive solution, involutive latin solution, cycle set, affine quasigroup.

M. Kinyon partially supported by Simons Foundation Collaboration Grant 359872. D. Stanovský partially supported by GAČR grant 18-20123S. P. Vojtěchovský partially supported by 2019 PROF grant of the University of Denver.

Bijjective nondegenerate solutions correspond to biracks [12, 10], while involutive nondegenerate solutions correspond to nondegenerate cycle sets [33].

An algebraic definition of a nondegenerate cycle set can be given as follows. A *left quasigroup* is a binary algebra (X, \cdot) in which all left translations $L_x : y \mapsto xy$ are bijections of X . A *cycle set* is then a left quasigroup (X, \cdot) in which the identity

$$(R_\ell) \quad (x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)$$

holds. This can also be conveniently expressed using left translations, namely as

$$(R'_\ell) \quad L_{x \cdot y} L_x = L_{y \cdot x} L_y.$$

A binary algebra (X, \cdot) is *uniquely 2-divisible* if the squaring map

$$\sigma : X \rightarrow X; \quad x \mapsto x \cdot x = x^2$$

is a bijection of X . A cycle set X is *nondegenerate* if it is uniquely 2-divisible.

We propose to rename nondegenerate cycle sets as *rumples*, both to acknowledge Rump's contributions and to highlight the similarity of rumples to quandles. Thus, a *rumple* is a uniquely 2-divisible left quasigroup satisfying (R_ℓ) .

Several structures, algebraic or otherwise, have been developed to construct and classify solutions of (YB). For example, bijective 1-cocycles [11], I-type structures [4, 19], cycle sets [7, 33, 39] and braces [6, 16, 34] all stem from the study of involutive, nondegenerate solutions. Braces have been generalized to skew-braces [20] for bijective, nondegenerate solutions. Skew braces have been generalized to semi-braces [5] for left nondegenerate solutions.

Many rumples of a combinatorial flavor are obtained from so-called multipermutational solutions of (YB); they include the 2-reductive medial quandles studied in [23]. We are more interested in rumples that are algebraically connected or, even more strongly, that are quasigroups. Since the multiplication tables of finite quasigroups are precisely latin squares, it is customary to designate quasigroups within various classes of algebras by the adjective *latin*, cf. latin quandles. The main results of this paper are concerned with *latin rumples*.

We conclude this introduction with a summary of the paper. In §2, we introduce additional notation and terminology, and besides adumbrating Rump's basic results [33] in our preferred notation and terminology, we also discuss how rumples interact with other kinds of set-theoretic solutions of (YB), such as biracks, racks, biquandles and quandles. In the brief §3, we build upon Rump's results and show that there is a one-to-one correspondence between latin rumples and involutive, nondegenerate solutions $r = (r_1, r_2)$ of (YB) in which both r_1 and r_2 are quasigroups.

In §4, we give a thorough study of affine latin rumples. We answer the question for which finite orders n there exist affine latin rumples (see Theorem 4.11), we obtain a class of latin rumples from matrices $A, B \in GL_p(p)$ that are close to circulant matrices and satisfy $[A, B] = A^2$ or equivalently, $[B, A^{-1}] = I$. This last equation is the Heisenberg commutation relation, and so finding solutions of (YB) based on such matrices is essentially the same as classifying finite dimensional modules of the first Weyl algebra over finite fields with invertible generators ([27], p.7). We do not pursue this connection any further here, but consider it to be an interesting possible future direction for the study of affine rumples. We conclude the section by paying close attention to the displacement group and using it to characterize affine latin rumples within the class of all latin rumples (see Theorem 4.18).

In §5, we study latin rumples isotopic to groups (a class that properly contains affine latin rumples) and we again characterize them in terms of their displacement groups (see Theorem 5.3). In §6 we develop the theory of central extensions of latin rumples and we construct latin rumples that are not affine, nor even isotopic to a group. Finally, in §7 we study latin rumples which satisfy

not only the identity (R_ℓ) but also its mirror image

$$(R_r) \quad (z \cdot x) \cdot (y \cdot x) = (z \cdot y) \cdot (x \cdot y),$$

or equivalently,

$$(R'_r) \quad R_{y \cdot x} R_x = R_{x \cdot y} R_y.$$

2. RUMPLES

2.1. Quasigroup properties. In a left quasigroup (X, \cdot) , we denote by $x \setminus y$ the unique solution $u \in X$ to the equation $x \cdot u = y$, and refer to the binary operation \setminus as *left division*. Then

$$(2.1) \quad x \cdot (x \setminus y) = y = x \setminus (x \cdot y)$$

holds for every $x, y \in Q$. Conversely, any algebra (X, \cdot, \setminus) satisfying (2.1) is a left quasigroup with left division \setminus . A homomorphism of left quasigroups $(X_1, \cdot_1, \setminus_1) \rightarrow (X_2, \cdot_2, \setminus_2)$ is a mapping $f : X_1 \rightarrow X_2$ satisfying $f(x \cdot_1 y) = f(x) \cdot_2 f(y)$ for every $x, y \in X$. It then follows that $f(x \setminus_1 y) = f(x) \setminus_2 f(y)$, too.

Dually, a *right quasigroup* is a binary algebra (X, \cdot) in which all right translations $R_x : y \rightarrow yx$ are bijections of X . Then the unique solution $v \in X$ to $v \cdot x = y$ will be denoted by y/x . Right division satisfies the identities $(x \cdot y)/y = x = (x/y) \cdot y$. A *quasigroup* is a left quasigroup that is also a right quasigroup.

We adopt the following notational convention for quasigroups. The multiplication operation will be denoted by both juxtaposition and by \cdot . The \cdot multiplication is less binding than the division operations, which are in turn less binding than juxtaposition. For instance, $x/yz \cdot uv$ abbreviates $(x/(y \cdot z)) \cdot (u \cdot v)$.

The *left multiplication group* of a left quasigroup X is the permutation group generated by all left translations, i.e.,

$$\text{LMlt}(X) = \langle L_x : x \in X \rangle.$$

If X is a quasigroup, we also define the *multiplication group* as the permutation group generated by all left and right translations, i.e.,

$$\text{Mlt}(X) = \langle L_x, R_x : x \in X \rangle.$$

Two binary algebras $(X_1, \cdot_1), (X_2, \cdot_2)$ are *isotopic* if there are bijections $f, g, h : X_1 \rightarrow X_2$ such that $f(x) \cdot_2 g(y) = h(x \cdot_1 y)$ holds for all $x, y \in X_1$.

2.2. Rump left quasigroups and rumples. A left quasigroup satisfying (R_ℓ) will be called a *Rump left quasigroup*. Thus Rump left quasigroups are the *cycle sets* of [33], and also the *RC quasigroups* of [7] (but note that RC quasigroups need not be quasigroups).

If (X, \cdot) is a uniquely 2-divisible binary algebra, then for every $x \in X$ there exists a unique element $x^{1/2} \in X$, the *square root of x* , such that $x^{1/2} x^{1/2} = x$. As already mentioned in §1, we define a *ruple* to be a uniquely 2-divisible, Rump left quasigroup (i.e., a nondegenerate cycle set in Rump's own terminology).

Rump proved that, in our terminology, a finite Rump left quasigroup is a ruple, that is, is uniquely 2-divisible [33, Thm. 2]. Rump's proof, though short on its own, uses deep structure theory. Here we give a short combinatorial proof that uses nothing more than the left Rump identity (R_ℓ) .

Theorem 2.1. *Let (X, \cdot) be a Rump left quasigroup such that $\text{LMlt}(X)$ is a torsion group. Then the squaring map $\sigma : X \rightarrow X$ is surjective.*

Proof. Let (X, \cdot) be a Rump left quasigroup and fix $c \in X$. Define a sequence $(c_n)_{n \geq 0}$ by setting $c_0 = c$ and $c_n = (c_{n-1} \setminus c)c_{n-1}$ for $n \geq 1$. Then

$$c_n^2 = (c_{n-1} \setminus c)c_{n-1} \cdot (c_{n-1} \setminus c)c_{n-1} = c_{n-1}(c_{n-1} \setminus c) \cdot c_{n-1}c_{n-1} = L_c(c_{n-1}^2)$$

for every $n \geq 1$, using (R_ℓ) in the second equality. By induction, we have $c_n^2 = L_c^{n+1}(c)$ for every $n \geq 0$. Since $\text{LMlt}(X)$ is a torsion group, there exists $n \geq 0$ such that $L_c^{n+1} = \text{id}_X$. Then $\sigma(c_n) = c_n^2 = L_c^{n+1}(c) = c$. \square

Corollary 2.2 (Rump [33, Thm. 2]). *Every finite Rump left quasigroup is a rump.*

The number of rumples up to isomorphism has been recorded for small orders in the On-Line Encyclopedia of Integer Sequences [35] as sequence A290887:

order	1	2	3	4	5	6	7	8
number of rumples	1	2	5	23	88	595	3456	34528

2.3. Rumples and the Yang-Baxter equation. The left component function r_1 of a left nondegenerate solution $r = (r_1, r_2)$ of (YB) is a left quasigroup and thus has its own left division operation. It turns out to be useful to view r_1 itself as the left division operation $r_1(x, y) = x \setminus y$ of a left quasigroup (X, \cdot, \setminus) . Put another way, it is more convenient to work with the operation \cdot defined by $x \cdot y = z$ if and only if $r_1(x, z) = y$ instead of $r_1(x, y) = z$. In the special case of involutive left nondegenerate solutions, the right component function r_2 must also have a specific form.

Lemma 2.3. *Let (X, \cdot, \setminus) be a left quasigroup. Then the mapping $r : X \times X \rightarrow X \times X$ defined by $r(x, y) = (x \setminus y, r_2(x, y))$ is involutive if and only if $r_2(x, y) = (x \setminus y)x$ for all $x, y \in X$.*

Proof. If $r^2 = \text{id}_{X \times X}$, then $(x \setminus y) \setminus r_2(x, y) = x$ and so $r_2(x, y) = (x \setminus y)x$. Conversely, if $r_2(x, y) = (x \setminus y)x$, then it is straightforward to check that $r^2 = \text{id}_{X \times X}$. \square

The following result explains why one is led naturally to the left Rump identity (R_ℓ) from set-theoretic solutions of (YB).

Theorem 2.4 (Rump [33, Prop. 1]). *There is a one-to-one correspondence between Rump left quasigroups and involutive left nondegenerate solutions of the Yang-Baxter equation.*

- (1) *If (X, \cdot) is a Rump left quasigroup, then $r(x, y) = (x \setminus y, (x \setminus y)x)$ is an involutive left nondegenerate solution of (YB).*
- (2) *If $r(x, y) = (r_1(x, y), r_2(x, y))$ is an involutive left nondegenerate solution of (YB), then the operation \cdot given by $x \cdot y = z \iff r_1(x, z) = y$ defines a Rump left quasigroup (X, \cdot) .*

The correspondence of Theorem 2.4 restricts to rumples and nondegenerate solutions.

Theorem 2.5 (Rump [33, Props. 1 and 2]). *There is a one-to-one correspondence between rumples and involutive nondegenerate solutions of the Yang-Baxter equation.*

- (1) *If (X, \cdot) is a rump, then $r(x, y) = (x \setminus y, (x \setminus y)x)$ is an involutive nondegenerate solution of (YB).*
- (2) *If $r(x, y) = (r_1(x, y), r_2(x, y))$ is an involutive nondegenerate solution of (YB), then the operation \cdot given by $x \cdot y = z \iff r_1(x, z) = y$ defines a rump (X, \cdot) .*

Note that involutive solutions are obviously bijective. Bijective nondegenerate solutions of the Yang-Baxter equation are called *biracks*. Biracks can be used to construct coloring invariants of knots and links [10, Chapter 5]. Invariance with respect to the 3rd Reidemeister move is equivalent to the Yang-Baxter equation, while the invariance with respect to the 2nd Reidemeister move is ensured by bijectivity and nondegeneracy. To achieve invariance with respect to the 1st Reidemeister move, it suffices to impose the condition

- (2.2) there is a permutation t of X such that $r(t(x), x) = (t(x), x)$,

cf. [30]. A *biquandle* is a birack satisfying (2.2). See [10] or [12] for an alternative axiomatization of biracks and biquandles based on exchange laws.

Via the correspondence of Theorem 2.5, rumples form a subclass of biquandles:

Proposition 2.6. *Let X be a ruple and let $r(x, y) = (x \setminus y, (x \setminus y)x)$ be the corresponding nondegenerate involutive solution. Then (X, r) is a biquandle.*

Proof. It remains to verify the condition (2.2). Let $t(x) = \sigma^{-1}(x) = x^{1/2}$. Then $r(t(x), x) = r(x^{1/2}, x) = (x^{1/2} \setminus x, (x^{1/2} \setminus x)x^{1/2}) = (x^{1/2}, x) = (t(x), x)$. \square

A *rack* is a birack $r = (r_1, r_2)$ satisfying $r_2(x, y) = x$. Algebraically, a rack is a left quasigroup satisfying the left self-distributive law

$$(xy)(xz) = x(yz).$$

We point out that if a left quasigroup (X, \cdot) is a rack with left division \setminus , then (X, \setminus) is also a rack and conversely. Hence the correspondence between racks and bijective nondegenerate solutions with $r_2(x, y) = x$ can be stated in terms of left division operations, analogously to the correspondence in Theorem 2.5. Note that for racks, the condition (2.2) is equivalent to idempotence $xx = x$. Idempotent racks are known as *quandles* [25, 31].

The definitions of racks and Rump left quasigroups are syntactically very similar but they behave quite differently as algebraic structures.

The analogy between quandles and rumples can be further strengthened by the following compilation of two results in the literature; see Stein [38] for finite latin quandles and Etingof, Schedler and Soloviev [11, Theorem 2.15] for finite rumples.

Proposition 2.7. *If X is a finite latin quandle or a finite ruple, then the group $\text{LMlt}(X)$ is solvable.*

2.4. Intersection of rumples and quandles. There is a class of natural examples in the intersection of quandles and rumples:

Example 2.8. The conjugation quandle over a group G satisfies (R_ℓ) if and only if G is nilpotent of class 2.

It is easy to characterize the intersection of rumples and racks. A left quasigroup is called *2-reductive* if it satisfies the identity $(xy)z = yz$. Expressing the Rump identity by (R'_ℓ) , i.e., $L_{xy}L_x = L_{yx}L_y$, left distributivity by $L_{xy}L_x = L_xL_y$, and 2-reductivity by $L_{xy} = L_y$, we immediately obtain:

Proposition 2.9. *For a left quasigroup, any two of the following three conditions imply the third:*

- *left distributivity;*
- *left Rump identity;*
- *2-reductivity.*

The intersection of the classes of Rump left quasigroups and racks is the class of 2-reductive racks.

In the context of the Yang-Baxter equation, the intersection of rumples and racks corresponds to multipermutational solutions of level 2 with $r_2(x, y) = x$. Following [11, §3.2], a solution (X, r) is called *multipermutational of level n* if the n -th retract $\text{Ret}^n(X, r)$ is trivial. (Level 2 has been studied extensively in [18, 24]). A rack is multipermutational of level 2 if and only if $L_{yx} = L_{zx}$ for every x, y, z , which is in turn equivalent to 2-reductivity, since $L_{yx} = L_{xx} = L_x$.

The intersection of rumples and quandles is the class of 2-reductive quandles which was studied in [23, §6, 8], where a general construction was given and 2-reductive quandles were counted up to isomorphism for all orders up to 16.

See [28] on the interplay between self-distributivity and other types of solutions to the Yang-Baxter equation.

2.5. Δ -bijectivity. A binary algebra (X, \cdot) is said to be Δ -bijective if the mapping

$$\Delta_{(\cdot)} : X \times X \rightarrow X \times X, \quad (x, y) \mapsto (xy, yx)$$

is bijective. In this subsection we show that a Rump left quasigroup is Δ -bijective if and only if it is a rump. The idea comes from [33] but our proofs are different.

Lemma 2.10. *Let (X, \cdot) be a Δ -bijective binary algebra. Then $\Delta_{(\cdot)}^{-1} = \Delta_{(*)}$ for some binary operation $*$ on X .*

Proof. Write $\Delta_{(\cdot)}^{-1}(x, y) = (x * y, x \diamond y)$. The equation $\Delta_{(\cdot)} \Delta_{(\cdot)}^{-1} = \text{id}_{X \times X}$ then says

$$(2.3) \quad (x * y)(x \diamond y) = x \quad \text{and} \quad (x \diamond y)(x * y) = y,$$

while the first component of $\Delta_{(\cdot)}^{-1} \Delta_{(\cdot)} = \text{id}_{X \times X}$ yields $(xy) * (yx) = x$. Replacing x with $x \diamond y$ and y with $x * y$, we get

$$x \diamond y = [(x \diamond y)(x * y)] * [(x * y)(x \diamond y)] = y * x,$$

using (2.3) in the second equality. □

Lemma 2.11. *Every Δ -bijective binary algebra is uniquely 2-divisible.*

Proof. Let $*$ be the binary operation on X such that $\Delta_{(*)} = \Delta_{(\cdot)}^{-1}$ (by Lemma 2.10). The components of the equations $\Delta_{(\cdot)} \Delta_{(*)}(x, x) = (x, x)$ and $\Delta_{(*)} \Delta_{(\cdot)}(x, x) = (x, x)$ give $(x * x)(x * x) = x$ and $(xx) * (xx) = x$. Thus $x * x$ is the unique square root of x in (X, \cdot) . □

The converse implication of Lemma 2.11 is not true for general binary algebras, as witnessed by a nontrivial cyclic group of odd order.

Lemma 2.12. *Every rump (X, \cdot) is Δ -bijective and*

$$\Delta_{(\cdot)}^{-1}(x, y) = ((x \setminus y^2)^{1/2}, (y \setminus x^2)^{1/2})$$

holds for all $x, y \in X$.

Proof. Set $x * y = (x \setminus y^2)^{1/2}$. We will show that $\Delta_{(\cdot)}^{-1} = \Delta_{(*)}$. Consider the identity $yx \cdot yx = xy \cdot xx$, a consequence of (R_ℓ) . This is equivalent to $(xy) \setminus (yx)^2 = x^2$, and then taking square roots, we have $(xy) * (yx) = x$. Reversing the roles of x and y , we also have $(yx) * (xy) = y$. This establishes $\Delta_{(*)} \Delta_{(\cdot)} = \text{id}_{X \times X}$.

Next set $u = (x \setminus y^2)^{1/2}$. Then

$$(2.4) \quad (u \setminus x)u \cdot (u \setminus x)z = u(u \setminus x) \cdot uz = x \cdot uz,$$

using (R_ℓ) . Taking $z = u$, we have $[(u \setminus x)u]^2 = x \cdot u^2 = y^2$ and so $(u \setminus x)u = y$. Using this in (2.4), we have $y \cdot (u \setminus x)z = x \cdot uz$. Setting $z = u \setminus x$, we get $y \cdot (u \setminus x)^2 = x^2$, and so $(u \setminus x)^2 = y \setminus x^2$. Taking square roots and then multiplying on the left by u , we obtain $(x \setminus y^2)^{1/2} (y \setminus x^2)^{1/2} = x$. Reversing the roles of x and y , we also have $(y \setminus x^2)^{1/2} (x \setminus y^2)^{1/2} = y$. This establishes $\Delta_{(\cdot)} \Delta_{(*)} = \text{id}_{X \times X}$. □

Combining Lemmas 2.11 and 2.12, we obtain:

Proposition 2.13. *A Rump left quasigroup is Δ -bijective if and only if it is a rump.*

Remark 2.14. Let (X, \cdot) be a rump. Motivated by the particular form of $\Delta_{(\cdot)}^{-1}$ in Lemma 2.12, define $X^\partial = (X, *)$ by

$$x * y = (x \setminus y^2)^{1/2}.$$

Then X^∂ is a rump, called the *dual rump* of X . The left division in X^∂ is $x \setminus^* y = (xy^2)^{1/2}$ and the unique square root of x in X^∂ is xx . If X is latin, then so is X^∂ with $x / ^* y = y^2 / x^2$. Finally, $(X^\partial)^\partial = X$ but the two rumpes X and X^∂ are not necessarily isomorphic. See [7] for more details.

2.6. The displacement group. Displacement groups have proven to be very useful in the theory of quandles (see [2, 22]). It will become apparent that they are also important for rumples.

Let X be a left quasigroup. The *positive displacement group* $\text{Dis}^+(X)$ and the *negative displacement group* $\text{Dis}^-(X)$ are the subgroups of $\text{LMlt}(X)$ defined, respectively, by

$$\text{Dis}^+(X) = \langle L_x L_y^{-1} : x, y \in X \rangle \quad \text{and} \quad \text{Dis}^-(X) = \langle L_x^{-1} L_y : x, y \in X \rangle.$$

The *displacement group* $\text{Dis}(X)$ is the group

$$\text{Dis}(X) = \langle L_x L_y^{-1}, L_x^{-1} L_y : x, y \in X \rangle.$$

Note that for a fixed $e \in X$, we have $\text{Dis}^+(X) = \langle L_x L_e^{-1} : x \in X \rangle$ and $\text{Dis}^-(X) = \langle L_e^{-1} L_x : x \in X \rangle$ since $L_x L_y^{-1} = L_x L_e^{-1} (L_y L_e^{-1})^{-1}$ and $L_x^{-1} L_y = (L_e^{-1} L_x)^{-1} L_e^{-1} L_y$.

The Rump identity (R'_ℓ) can be restated as $L_x L_y^{-1} = L_{xy}^{-1} L_{yx}$, hence, for Rump left quasigroups,

$$\text{Dis}^+(X) \leq \text{Dis}^-(X) = \text{Dis}(X).$$

Lemma 2.15. *Let X be a rack or a ruple. Then $\text{Dis}(X) = \text{Dis}^+(X) = \text{Dis}^-(X)$.*

Proof. The argument is easy for racks. We have $L_x L_y = L_{xy} L_x$ and hence $L_y L_x^{-1} = L_x^{-1} L_{xy}$, which implies $\text{Dis}^+(X) \leq \text{Dis}^-(X)$. Also, $L_x^{-1} L_y = L_x^{-1} L_{x(xy)} = L_{xy} L_x^{-1}$, which implies $\text{Dis}^-(X) \leq \text{Dis}^+(X)$.

Suppose now that X is a ruple. From the remark preceding the lemma, $\text{Dis}^+(X) \leq \text{Dis}^-(X)$. Using Δ -bijectivity, for every $a, b \in X$, there exist $x, y \in X$ such that $xy = a$ and $yx = b$. Thus $L_a^{-1} L_b = L_x L_y^{-1}$ by (R'_ℓ) and we get $\text{Dis}^-(X) \leq \text{Dis}^+(X)$. \square

Problem 2.16. If X is a Rump left quasigroup, does $\text{Dis}^+(X) = \text{Dis}^-(X)$?

Proposition 2.17. *Let X be a left quasigroup such that $\text{Dis}(X) = \text{Dis}^+(X) = \text{Dis}^-(X)$. Then:*

- (1) $\text{Dis}(X) \leq \text{LMlt}(X)$.
- (2) $\text{LMlt}(X)/\text{Dis}(X)$ is a cyclic group.
- (3) $\text{Dis}(X) = \{L_{x_1}^{k_1} \dots L_{x_n}^{k_n} : 0 \leq n, x_i \in X, \sum k_i = 0\}$.

Proof. (1) It is sufficient to prove that every conjugate of $L_x L_y^{-1}$ by $L_z^{\pm 1}$ is in $\text{Dis}(X)$. Clearly, $L_z^{-1} L_x L_y^{-1} L_z \in \text{Dis}(X)$. For the other conjugate, write $L_x L_y^{-1} = L_{x_1}^{-1} L_{y_1} \dots L_{x_n}^{-1} L_{y_n}$ for some $x_1, \dots, x_n, y_1, \dots, y_n \in X$, and regroup $L_z L_x L_y^{-1} L_z^{-1} = (L_z L_{x_1}^{-1}) (L_{y_1} L_{x_2}^{-1}) \dots (L_{y_n} L_z^{-1}) \in \text{Dis}(X)$.

(2) Fix $e \in X$. For every $x \in X$, we have $L_x^{-1} L_e \in \text{Dis}(X)$, and thus $L_x \text{Dis}(X) = L_e \text{Dis}(X)$. Consequently, for $\alpha = L_{x_1}^{k_1} \dots L_{x_n}^{k_n} \in \text{LMlt}(X)$ we have $\alpha \text{Dis}(X) = L_e^{k_1 + \dots + k_n} \text{Dis}(X)$, so $\text{LMlt}(X)/\text{Dis}(X) = \langle L_e \text{Dis}(X) \rangle$.

(3) Let $S = \{L_{x_1}^{k_1} \dots L_{x_n}^{k_n} : 0 \leq n, x_i \in X, \sum k_i = 0\}$. Every $\alpha \in S$ can be written as $\alpha = L_{x_1}^{k_1} \dots L_{x_n}^{k_n}$, where $k_i = \pm 1$ for every $1 \leq i \leq n$. We prove by induction on n that $\alpha \in \text{Dis}(X)$. If $n = 2$, we are done by the definition of $\text{Dis}(X)$, so suppose that $n > 2$. If $k_1 = k_n$ then there must be an m such that $1 < m < n$ and $\sum_{i=1}^m k_i = 0 = \sum_{i=m+1}^n k_i$. By the induction hypothesis, α is then a product of two elements of $\text{Dis}(X)$. Finally suppose that $k_1 = -k_n$. Then $\sum_{i=2}^{n-1} k_i = 0$ and hence $\alpha = L_x \beta L_y^{-1}$ or $\alpha = L_x^{-1} \beta L_y$ for some $\beta \in \text{Dis}(X)$ and some $x, y \in X$. In the former case, we can write $\beta = L_{u_1}^{-1} L_{v_1} \dots L_{u_s}^{-1} L_{v_s}$ for some u_i, v_i and observe that $\alpha = L_x \beta L_y^{-1}$ is a product of factors of the form $L_a L_b^{-1}$, while in the latter case we can write $\beta = L_{u_1} L_{v_1}^{-1} \dots L_{u_s} L_{v_s}^{-1}$ and observe that $\alpha = L_x^{-1} \beta L_y$ is a product of factors of the form $L_a^{-1} L_b$. \square

We deduce the following result for racks and rumples. For racks, this was already known, cf. [22, Prop. 2.1].

Proposition 2.18. *The conditions (1)–(3) of Proposition 2.17 hold when X is a rack or a ruple.*

3. LATIN RUMPLES

Recall that a rump is a uniquely 2-divisible left quasigroup satisfying the identity (R_ℓ) . A *latin rump* is a rump that is a quasigroup. It is not necessary to assume unique 2-divisibility in the definition of a latin rump:

Proposition 3.1. *A binary algebra (X, \cdot) is a latin rump if and only if it is a quasigroup satisfying (R_ℓ) . Furthermore, in a latin rump (X, \cdot) , the squaring map is given by $\sigma = R_{ee}L_eR_e^{-1}$, where e is any element of X .*

Proof. Suppose that (X, \cdot) is a quasigroup satisfying (R_ℓ) and let $e \in X$. The bijection $\sigma = R_{ee}L_eR_e^{-1}$ then satisfies

$$\sigma(x) = e(x/e) \cdot ee = (x/e)e \cdot (x/e)e = x^2,$$

where we have used (R_ℓ) in the second step. □

Latin rumples form a very natural class of set-theoretic solutions of the Yang-Baxter equation.

Theorem 3.2. *There is a one-to-one correspondence between latin rumples and involutive solutions $r = (r_1, r_2)$ of the Yang-Baxter equation in which both r_1, r_2 are quasigroup operations.*

Proof. Let $(r_1, r_2) : X \times X \rightarrow X \times X$ be an involutive solution of the Yang-Baxter equation in which both r_1, r_2 are quasigroup operations. By Theorem 2.5, the operation \cdot defined by $xy = z \iff r_1(x, z) = y$ defines a rump (X, \cdot) . Since r_1 is a quasigroup (not just a left quasigroup), (X, \cdot) is latin.

Conversely, if (X, \cdot) is a latin rump then Theorem 2.5 shows that $r = (r_1, r_2)$ with $r_1(x, y) = x \setminus y$ and $r_2(x, y) = (x \setminus y)x$ is an involutive nondegenerate solution, and so $(X, r_1) = (X, \setminus)$ is a left quasigroup and (X, r_2) is a right quasigroup. Since (X, \cdot) is a quasigroup, (X, r_1) is also a quasigroup. To show that r_2 is a left quasigroup, we note that the equation $(x \setminus y)x = z$ has a unique solution y in X , namely $y = x(z/x)$. □

Example 3.3. An exhaustive search using the finite model builder Mace4 [32] reveals that up to isomorphism there are only two nontrivial latin rumples of order less than 12, namely

$$\begin{array}{c|cccc} X_{4,1} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 3 & 2 \\ 1 & 2 & 3 & 1 & 0 \\ 2 & 1 & 0 & 2 & 3 \\ 3 & 3 & 2 & 0 & 1 \end{array} \quad \text{and} \quad \begin{array}{c|cccc} X_{4,2} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 3 & 0 & 2 \\ 1 & 0 & 2 & 1 & 3 \\ 2 & 2 & 0 & 3 & 1 \\ 3 & 3 & 1 & 2 & 0 \end{array} .$$

It turns out that both $X_{4,1}$ and $X_{4,2}$ are self-dual in the sense of Remark 2.14, and both satisfy the right Rump identity (R_r) .

We will need additional structure theory to find more latin rumples.

4. AFFINE LATIN RUMPLES

4.1. Linear and affine representations. Let $(G, +)$ be an abelian group with identity element 0, let φ and ψ be endomorphisms of $(G, +)$, and let $c \in G$. Then the binary algebra $(G, *)$ defined by

$$(4.1) \quad x * y = \varphi(x) + \psi(y) + c$$

is called *affine over* $(G, +)$. If $c = 0$, it is called *linear over* $(G, +)$. We will denote the algebra $(G, *)$ by $\text{Aff}(G, +, \varphi, \psi, c)$ or by $\text{Aff}(G, \varphi, \psi, c)$ if the group operation on G is understood from the context.

Note that $\text{Aff}(G, +, \varphi, \psi, c)$ is a left quasigroup if and only if $\psi \in \text{Aut}(G, +)$, and it is latin if and only if $\varphi, \psi \in \text{Aut}(G, +)$. Also note that (4.1) shows that an affine quasigroup $\text{Aff}(G, +, \varphi, \psi, c)$ is isotopic to the abelian group $(G, +)$.

An algebra $(G, *)$ is called *affine* (resp. *linear*) if it is affine (resp. linear) over some abelian group $(G, +)$. In the literature, affine quasigroups are also called *central* or *T-quasigroups* [36, 37]. (We will resist the urge to use the *T*-terminology for Rump quasigroups.)

Our definitions of linear and affine binary algebras are compatible with the definitions of linear and affine solutions of the Yang-Baxter equation from [11, Section 3.1]. Formally, linear (affine) nondegenerate involutive solutions correspond, in the sense of Theorem 2.5, to linear (affine) rumples.

Proposition 4.1. *An affine binary algebra $\text{Aff}(G, +, \varphi, \psi, c)$ satisfies (R_ℓ) if and only if*

$$(4.2) \quad [\varphi, \psi] = \varphi\psi - \psi\varphi = \varphi^2.$$

If $\text{Aff}(G, +, \varphi, \psi, c)$ is a quasigroup then (4.2) holds if and only if

$$(4.3) \quad [\psi, \varphi^{-1}] = 1,$$

which is further equivalent to

$$(4.4) \quad [\varphi^{-1}, \psi^{-1}] = \psi^{-2}.$$

Proof. Let us write φx instead of $\varphi(x)$, etc. For $x, y, z \in G$ we have

$$(x * y) * (x * z) = (\varphi x + \psi y + c) * (\varphi x + \psi z + c) = \varphi^2 x + \varphi \psi y + \varphi c + \psi \varphi x + \psi^2 z + \psi c + c,$$

while

$$(y * x) * (y * z) = (\varphi y + \psi x + c) * (\varphi y + \psi z + c) = \varphi^2 y + \varphi \psi x + \varphi c + \psi \varphi y + \psi^2 z + \psi c + c.$$

Hence the identity $(x * y) * (x * z) = (y * x) * (y * z)$ holds if and only if $\varphi^2 u + \psi \varphi u = \varphi \psi u$ for every $u \in G$. Multiplying $\varphi \psi - \psi \varphi = \varphi^2$ by φ^{-1} from both sides, we obtain $\psi \varphi^{-1} - \varphi^{-1} \psi = 1$. Multiplying further by ψ^{-1} from both sides, we obtain $\varphi^{-1} \psi^{-1} - \psi^{-1} \varphi^{-1} = \psi^{-2}$. \square

Note that the constant c plays no role in Proposition 4.1.

As the following example shows, an affine ruple can admit multiple affine representations; even the underlying abelian group is not necessarily determined up to isomorphism.

Example 4.2. The ruple with multiplication table

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	1	0	3	2
3	3	2	1	0

is isomorphic to both $\text{Aff}(\mathbb{Z}_4, 2, -1, 1)$ and $\text{Aff}(\mathbb{Z}_2^2, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix})$.

The situation is different for affine latin rumples, however, because for any affine quasigroup, the underlying abelian group is uniquely determined. This follows from the fact that isotopic groups are isomorphic [36, Prop. 1.4].

When classifying affine quasigroups (and affine latin rumples in particular) up to isomorphism, the following theorem is very useful.

Theorem 4.3 (Drápal [8, Thm. 3.2]). *Let $Q = \text{Aff}(G, +, \varphi, \psi, c)$ and $Q' = \text{Aff}(G, +, \varphi', \psi', c')$ be affine quasigroups. Then Q is isomorphic to Q' if and only if there are $\alpha \in \text{Aut}(G, +)$ and $u \in \text{Im}(1 - \varphi - \psi)$ such that $\varphi' = \varphi^\alpha = \alpha \varphi \alpha^{-1}$, $\psi' = \psi^\alpha = \alpha \psi \alpha^{-1}$ and $c' = \alpha(c + u)$.*

When F is a field, the endomorphisms of the additive group $(F^n, +)$ can be identified with $n \times n$ matrices with entries in F , as we already did in Example 4.2. In this context, we will denote the generic endomorphisms φ and ψ by A and B , respectively, and (4.1) becomes $x * y = Ax + By + c$.

By Proposition 4.1, there is then an affine latin rumple over $(F^n, +)$ if and only if any of the equivalent equations

$$(4.5) \quad [A, B] = A^2,$$

$$(4.6) \quad [B, A^{-1}] = I,$$

$$(4.7) \quad [A^{-1}, B^{-1}] = B^{-2}$$

have a solution in $\text{Aut}(F^n, +) = \text{GL}_n(F)$. Here, (4.6) is a particular instance of the canonical commutation relation used, for instance, in the matrix interpretation of the Heisenberg uncertainty principle. It is also the defining relation of the (first) Weyl algebra [27, p.7], and so finding matrices satisfying (4.3) is essentially the same as classifying modules over the Weyl algebra with the constraint that the generators should be invertible matrices.

Lemma 4.4. *Let F be a field and $A, B \in \text{GL}_n(F)$. If $\text{Aff}(F^n, +, A, B, c)$ is an affine latin rumple then the matrices A, A^2, B^{-1} and B^{-2} have trace 0.*

Proof. From (4.5), we have $\text{tr}(A^2) = \text{tr}(AB) - \text{tr}(BA) = 0$. Also, $A = A^{-1}A^2 = A^{-1}[A, B] = B - A^{-1}BA$, and so $\text{tr}(A) = \text{tr}(B) - \text{tr}(A^{-1}BA) = 0$. From (4.7), we have $\text{tr}(B^{-2}) = 0$. Finally, $B^{-1} = BB^{-2} = B[A^{-1}, B^{-1}] = BA^{-1}B^{-1} - A^{-1}$, and so $\text{tr}(B^{-1}) = 0$. \square

Example 4.5. A straightforward calculation in GAP [14] combining Proposition 4.1 and Theorem 4.3 allows us to determine all affine latin rumples over $\mathbb{Z}_2^2, \mathbb{Z}_2^4, \mathbb{Z}_3^3$ and $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$ up to isomorphism. For the first three abelian groups, see Table 1. There are 18 affine latin rumples over the group $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$. Larger abelian groups that admit affine latin rumples are beyond the reach of standard GAP routines.

4.2. The spectrum of affine latin rumples. For an abelian group G , let $N_{alr}(G)$ be the number of affine latin rumples over G up to isomorphism. For a positive integer n , let $N_{alr}(n)$ be the number of affine latin rumples of size n up to isomorphism. In this section we determine the spectrum of finite affine latin rumples, that is, the set $\{n \in \mathbb{N} : N_{alr}(n) > 0\}$. We also show that $N_{alr}(G) = \prod_p N_{alr}(G_p)$, where G_p are p -primary components of G ; $N_{alr}(\mathbb{Z}_p^k) > 0$ if and only if p divides k ; $N_{alr}(\mathbb{Z}_{p^{a_1}}^{b_1} \times \cdots \times \mathbb{Z}_{p^{a_r}}^{b_r}) = 0$ if p does not divide some b_i ; and $N_{alr}(\mathbb{Z}_n) = 0$.

Proposition 4.6. *Let $G = \prod_p G_p$ be a decomposition of a finite abelian group G into its p -primary components G_p . Then $N_{alr}(G) = \prod_p N_{alr}(G_p)$.*

Proof. This is immediate from the fact that $\text{Aut}(G)$ is isomorphic to $\prod_p \text{Aut}(G_p)$. \square

Given a permutation π of $\{1, \dots, n\}$, the associated permutation matrix P_π is defined by

$$P_\pi(x_1, \dots, x_n)^T = (x_{\pi(1)}, \dots, x_{\pi(n)})^T.$$

Proposition 4.7. *Let F be a field. There exists a solution $A, B \in \text{GL}_n(F)$ of the equation (4.5) if and only if F has positive characteristic dividing n .*

Proof. Suppose that $A, B \in \text{GL}_n(F)$ satisfy (4.5). From the equivalent identity (4.6) we see that $n = \text{tr}(I) = \text{tr}(BA^{-1}) - \text{tr}(A^{-1}B) = 0$, which can happen only if F has positive characteristic dividing n .

Conversely, suppose that F has positive characteristic dividing n . Let $A = (a_{i,j}) = P_\pi$ for $\pi = (1, \dots, n)^{-1}$, i.e., $a_{i+1,i} = 1 = a_{1,n}$ for all $i = 1, \dots, n-1$ and $a_{i,j} = 0$ otherwise. Let $B = I - D$,

TABLE 1. Affine latin rumples of small orders

$\text{Aff}(\mathbb{Z}_2^2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix})$	$\text{Aff}(\mathbb{Z}_2^2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix})$
$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_2^4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_3^3, \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_3^3, \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_3^3, \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_3^3, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\right)$
$\text{Aff}\left(\mathbb{Z}_3^3, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right)$	$\text{Aff}\left(\mathbb{Z}_3^3, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\right)$

where $D = (d_{i,j})$ is the matrix defined by $d_{i+1,i} = i$ for all $i = 1, \dots, n-1$ and $d_{i,j} = 0$ otherwise. Then

$$[B, A^{-1}] = (I - D)A^{-1} - A^{-1}(I - D) = A^{-1}D - DA^{-1} = I,$$

where the last equality follows from the fact that $A^{-1}D$ is a diagonal matrix with diagonal $(1, 2, \dots, n-1, 0)$, DA^{-1} is a diagonal matrix with diagonal $(0, 1, 2, \dots, n-1)$, and $0 - (n-1) = 1$ since the characteristic of F divides n . \square

The following lemma is standard [26, Thms. 41 and 42]. Recall that a *congruence* of a quasigroup $(X, \cdot, \backslash, /)$ is an equivalence relation \sim on X such that $xy \sim uv$, $x \backslash y \sim u \backslash v$ and $x / y \sim u / v$ whenever $x \sim u$ and $y \sim v$.

Lemma 4.8. *Let $X = \text{Aff}(G, +, \varphi, \psi, c)$ be an affine quasigroup. The congruences of X are in one-to-one correspondence with subgroups of $(G, +, 0)$ that are invariant under φ and ψ . Given a congruence \sim , the corresponding subgroup is the equivalence class of \sim containing 0 . Given a subgroup H , the corresponding congruence is defined by $x \sim y$ if and only if $x - y \in H$.*

If $X = \text{Aff}(G, +, \varphi, \psi, c)$ is an affine latin ruple and H is a subgroup of $(G, +)$ invariant under φ and ψ , we denote by X/H the factor of X modulo the congruence of X corresponding to H .

Proposition 4.9. *Let p be a prime and let X be an affine latin rumple over $\mathbb{Z}_{p^{a_1}}^{b_1} \times \cdots \times \mathbb{Z}_{p^{a_r}}^{b_r}$. Then each b_1, \dots, b_r is divisible by p .*

Proof. Let $G = \mathbb{Z}_{p^{a_1}}^{b_1} \times \cdots \times \mathbb{Z}_{p^{a_r}}^{b_r}$ with $a_1 > a_2 > \cdots > a_r$. We may assume without loss of generality that $(X, *) = \text{Aff}(G, \varphi, \psi, 0)$ for some $\varphi, \psi \in \text{Aut}(G)$. The subset $pG = \{px : x \in G\}$ is a characteristic subgroup of G and hence invariant under φ and ψ . By Lemma 4.8, the rumple X/pG is affine over the group $G/pG \cong \mathbb{Z}_p^{b_1 + \cdots + b_r}$. By Proposition 4.7, p divides $\sum_{i=1}^r b_i$.

The map $x \mapsto px$ is an endomorphism of X as $p(x*y) = p(\varphi x + \psi y) = \varphi(px) + \psi(py) = (px)*(py)$. The image pX is isomorphic to a quotient of X , and hence is affine over pG by Lemma 4.8. Applying p repeatedly, we conclude that the rumple $p^{a_r}X$ is affine over the group $p^{a_r}G$, which is isomorphic to $\mathbb{Z}_{p^{c_1}}^{b_1} \times \cdots \times \mathbb{Z}_{p^{c_{r-1}}}^{b_{r-1}}$ for suitable $c_1, \dots, c_{r-1} > 0$. As above, we deduce that p divides $\sum_{i=1}^{r-1} b_i$.

Hence p divides b_r . Repeating the above argument with $p^{a_r}X$ instead of X finishes the proof. \square

Proposition 4.10. *Let p be a prime. An affine latin rumple of order p^k exists if and only if p divides k .*

Proof. If p divides k then Proposition 4.7 furnishes an example over the elementary abelian group \mathbb{Z}_p^k . For the converse, suppose that there is an affine latin rumple over $G = \mathbb{Z}_{p^{a_1}}^{b_1} \times \cdots \times \mathbb{Z}_{p^{a_r}}^{b_r}$ with $|G| = p^{a_1 b_1 + \cdots + a_r b_r} = p^k$. By Proposition 4.9, p divides each of b_1, \dots, b_r and thus p divides k . \square

Combining Propositions 4.6 and 4.10, we obtain:

Theorem 4.11. *Let p_1, \dots, p_m be distinct primes. An affine latin rumple of order $p_1^{k_1} \cdots p_m^{k_m}$ exists if and only if p_i divides k_i for every $1 \leq i \leq m$.*

We do not fully understand for which finite abelian groups G we get $N_{alr}(G) = 0$. For instance, among the abelian groups of order 64, Proposition 4.9 guarantees $N_{alr}(G) = 0$ for all groups except for $G = \mathbb{Z}_8^2, \mathbb{Z}_4^2 \times \mathbb{Z}_2^2$ and \mathbb{Z}_2^6 , while Proposition 4.7 yields $N_{alr}(\mathbb{Z}_2^6) > 0$. Computer calculations show that $N_{alr}(\mathbb{Z}_8^2) = 0$ and $N_{alr}(\mathbb{Z}_4^2 \times \mathbb{Z}_2^2) = 18$.

Problem 4.12. For which finite abelian groups G is there a latin rumple affine over G ?

We conclude this subsection with a supplemental nonexistence result.

Lemma 4.13. *There are no affine latin rumples over cyclic groups.*

Proof. Since all endomorphisms of a cyclic group G commute, we have $[\varphi, \psi] = 0$ for every $\varphi, \psi \in \text{End}(G)$. If $\varphi^2 = [\varphi, \psi]$ holds, φ cannot be invertible. \square

4.3. A class of affine latin rumples. In this subsection we expand upon the example from the proof of Proposition 4.7. Recall that a square matrix is a *circulant* if it is constant on all broken diagonals, and denote by $\text{Circ}(c_1, \dots, c_n)$ the $n \times n$ circulant matrix with first row equal to (c_1, \dots, c_n) . As in the proof of Proposition 4.7, let $D = (d_{i,j})$ be the $n \times n$ matrix defined by $d_{i+1,i} = 1$ for all $i = 1, \dots, n-1$ and $d_{i,j} = 0$ otherwise.

Lemma 4.14. *Let $A = \text{Circ}(0, \dots, 0, 1)$ be the permutation matrix corresponding to the n -cycle $(1, \dots, n)^{-1}$. Then an $n \times n$ matrix B satisfies $[A, B] = A^2$ if and only if $B = \text{Circ}(c_1, \dots, c_n) - D$ for some c_1, \dots, c_n .*

Proof. Since A is invertible, we can work with the equivalent identity $[B, A^{-1}] = I$ instead. Using $A^{-1} = \text{Circ}(0, 1, 0, \dots, 0)$ and $B = (b_{i,j})$, we have

$$BA^{-1} - A^{-1}B = \begin{pmatrix} b_{1,n} - b_{2,1}, & b_{1,1} - b_{2,2}, & \cdots & b_{1,n-1} - b_{2,n} \\ b_{2,n} - b_{3,1}, & b_{2,1} - b_{3,2}, & \cdots & b_{2,n-1} - b_{3,n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{n-1,n} - b_{n,1}, & b_{n-1,1} - b_{n,2}, & \cdots & b_{n-1,n-1} - b_{n,n} \\ b_{n,n} - b_{1,1}, & b_{n,1} - b_{1,2}, & \cdots & b_{n,n-1} - b_{1,n} \end{pmatrix}.$$

Then $[B, A^{-1}] = I$ holds if and only if we have (reading off the main diagonal)

$$(4.8) \quad b_{1,n} - b_{2,1} = b_{2,1} - b_{3,2} = \cdots = b_{n-1,n-2} - b_{n,n-1} = b_{n,n-1} - b_{1,n} = 1,$$

and (reading off the broken diagonal just above the main diagonal)

$$(4.9) \quad b_{1,1} - b_{2,2} = b_{2,2} - b_{3,3} = \cdots = b_{n-1,n-1} - b_{n,n} = b_{n,n} - b_{1,1} = 0,$$

and similarly on the remaining broken diagonals. All solutions of the linear system (4.8) are of the form $b_{1,n} = c, b_{2,1} = c - 1, \dots, b_{n,n-1} = c - n$ for some c , while all solutions of (4.9) are of the form $b_{1,1} = b_{2,2} = \cdots = b_{n,n} = c$ for some c . The claim follows. \square

In order to construct an affine latin rumple from $A = \text{Circ}(0, \dots, 0, 1)$ and $B = \text{Circ}(c_1, \dots, c_n) - D$, we must ensure that B is invertible. The following result characterizes invertible matrices of the form $\text{Circ}(c_1, \dots, c_n) - D$ with entries in \mathbb{Z}_p in the special case when $n = p$. (By Proposition 4.9, the case $n = p$ is precisely the case we care about.)

Proposition 4.15. *Let p be a prime, $c_1, \dots, c_p \in \mathbb{Z}_p$ and $B = \text{Circ}(c_1, \dots, c_p) - D$. Then $\det(B) \equiv c_1 + \cdots + c_{p-1} \pmod{p}$.*

Proof. Call a selection P of p cells from the square $\mathbb{Z}_p \times \mathbb{Z}_p$ a permutation pattern if every row and every column contain precisely one cell from P . Given a permutation pattern P and an integer k , let P^k be the pattern with cells $\{(i+k, j+k) : (i, j) \in P\}$, where we add coordinates modulo p . Let $[P] = \{P^k : k \in \mathbb{Z}\}$. We will add contributions to $\det(B)$ in groups corresponding to the classes $[P]$ of permutation patterns. Observe that all permutations corresponding to the patterns in a given class $[P]$ have the same sign since they have the same cycle structure.

Suppose that P is a (broken) diagonal so that $[P] = \{P\}$. If the diagonal in B corresponding to P is constant with all entries equal to c_i , for some $1 \leq i \leq p-1$, then its contribution to $\det(B)$ is $c_i^p \equiv c_i \pmod{p}$. In the nonconstant case the contribution of P is $c_p(c_p - 1) \cdots (c_p - (p-1)) \equiv 0 \pmod{p}$ since one of the factors is equal to 0.

Now suppose that P is not a diagonal. We claim that $P = P^m$ if and only if p divides m and thus $[P] = \{P^k : 0 \leq k < p\}$. Indeed, if $P = P^m$, $\gcd(m, p) = 1$ and $(i, j) \in P$, then P must contain the distinct cells $(i + km, j + km)$, $0 \leq k < p$, and hence P is a diagonal. Suppose that P intersects the nonconstant diagonal of B in d cells. If $d = 0$ then every P^k contributes the same amount to $\det(B)$ and hence the contribution of $[P]$ is congruent to 0 modulo p . We can therefore assume that $d > 0$ and note that $d \leq p-2$ because if P contains $p-1$ cells from the nonconstant diagonal of B then P must also contain the last cell from the nonconstant diagonal, a contradiction. The contribution of P is then of the form $\pm c_{i_1} \cdots c_{i_{p-d}}(c_p - j_1) \cdots (c_p - j_d)$, where $1 \leq i_k < p$ and $0 \leq j_d < p$, while the contribution of P^k is $\pm c_{i_1} \cdots c_{i_{p-d}}(c_p - j_1 - k) \cdots (c_p - j_d - k)$. The combined contribution of $[P]$ is therefore $\pm c_{i_1} \cdots c_{i_{p-d}} \cdot s$, where

$$s = \sum_{0 \leq k < p} (c_p - j_1 - k) \cdots (c_p - j_d - k) \equiv \sum_{0 \leq k < p} (c_p - j_1 + k) \cdots (c_p - j_d + k).$$

We will show that $s \equiv 0 \pmod{p}$, finishing the proof.

For $1 \leq i \leq d$, let $e_i = c_p - j_i$ so that $s = \sum_{0 \leq k < p} (e_1 + k) \cdots (e_d + k)$. Let us view s as a polynomial in variables e_1, \dots, e_d and let us determine the coefficients of all monomials. The monomial $e_1 \cdots e_d$ has coefficient $1 + 1 + \cdots + 1 = p \equiv 0 \pmod{p}$. Every monomial of the form $e_{i_1} \cdots e_{i_\ell}$ with $0 \leq \ell < d$ has coefficient $0 + 1^{d-\ell} + 2^{d-\ell} + \cdots + (p-1)^{d-\ell}$.

It now suffices to show that $1^t + 2^t + \cdots + (p-1)^t \equiv 0 \pmod{p}$ for every $1 \leq t \leq p-2$ since we have already observed that $1 \leq d-\ell \leq d \leq p-2$. Let ω be a primitive $(p-1)$ st root of unity in \mathbb{Z}_p . Then $1^t + 2^t + \cdots + (p-1)^t = 1^t + \omega^t + \omega^{2t} + \cdots + \omega^{(p-2)t} = (1 - \omega^{(p-1)t})(1 - \omega^t)^{-1} \equiv 0 \pmod{p}$ since $\omega^{p-1} = 1$ and $\omega^t \neq 1$. \square

Corollary 4.16. Let $A = \text{Circ}(0, \dots, 0, 1)$ and $B = (c_1, \dots, c_p) - D$ be $p \times p$ matrices, where $c_1, \dots, c_p \in \mathbb{Z}_p$ satisfy $c_1 + \dots + c_{p-1} \not\equiv 0 \pmod{p}$. Then for every $c \in \mathbb{Z}_p$, $\text{Aff}(\mathbb{Z}_p^p, A, B, c)$ is an affine latin rumple of order p^p .

Remark 4.17. The isomorphism problem for affine latin rumples of the form $\text{Aff}(\mathbb{Z}_p^p, A, B, c)$ with $A = \text{Circ}(0, \dots, 0, 1)$ and $B = (c_1, \dots, c_p) - D$ is tractable for small values of p . It is also possible to generalize the construction of Corollary 4.16 further by considering matrices that do not differ much from $\text{Circ}(0, \dots, 0, 1)$, say $A = \text{Circ}(0, \dots, 0, 1) + aE_{i+1,i}$, where $E_{i,j}$ is the matrix whose only nonzero entry 1 is located in row i and column j . One can then obtain statements analogous to Lemma 4.14 and Proposition 4.15. The details will be presented elsewhere.

4.4. A characterization of affine latin rumples. In this subsection we obtain a characterization of affine latin rumples among latin rumples in terms of the displacement group and the multiplication group. According to Proposition 2.17, for every rumple X , the displacement group $\text{Dis}(X)$ is normal in $\text{LMlt}(X)$, and thus $\text{Dis}(X)$ is normal in $\text{Mlt}(X)$ if and only if $\text{Dis}(X)^{R_x^{\pm 1}} \subseteq \text{Dis}(X)$ for every $x \in X$.

Recall that a permutation group G acts *regularly* on X if for every $x, y \in X$ there is a unique $g \in G$ such that $g(x) = y$.

Theorem 4.18. The following conditions are equivalent for a latin rumple X :

- (1) X is affine;
- (2) $\text{Dis}(X)$ is abelian and normal in $\text{Mlt}(X)$.

Proof. Suppose that (1) holds. In an affine rumple $(X, *) = \text{Aff}(G, \varphi, \psi, c)$, we have

$$L_x L_y^{-1}(z) = \varphi(x) + \psi(\psi^{-1}(z - \varphi(y) - c)) + c = \varphi(x) - \varphi(y) + z.$$

Hence, since φ is surjective, we have $\text{Dis}(X) = \{\alpha_x : x \in X\}$, where $\alpha_x(z) = x + z$. It is now clear that $\text{Dis}(X)$ is an abelian group. Moreover,

$$\begin{aligned} \alpha_x^{R_y}(z) &= \alpha_x(z/y) * y = \varphi(x + \varphi^{-1}(z - \psi(y) - c)) + \psi(y) + c = \varphi(x) + z, \\ \alpha_x^{R_y^{-1}}(z) &= \alpha_x(z * y)/y = \varphi^{-1}((\varphi(z) + \psi(y) + c) + x - \psi(y) - c) = \varphi^{-1}(x) + z \end{aligned}$$

shows that $\alpha_x^{R_y} = \alpha_{\varphi(x)}$ and $\alpha_x^{R_y^{-1}} = \alpha_{\varphi^{-1}(x)}$ are elements of $\text{Dis}(X)$.

Now suppose that (2) holds. Pick $e \in X$ arbitrarily and let $G = \text{Dis}(X)$, $\varphi(f) = f^{R_{ee}}$, $\psi(f) = f^\sigma$, where $\sigma = R_{ee} L_e R_e^{-1}$ (cf. Proposition 3.1), and $c = L_{ee} L_e^{-1}$. We will show that X is isomorphic to $\text{Aff}(G, \varphi, \psi, c)$. First observe that both φ, ψ are well-defined because $\text{Dis}(X) \trianglelefteq \text{Mlt}(X)$. Consider the map

$$\xi : X \rightarrow \text{Aff}(G, \varphi, \psi, c), \quad x \mapsto L_x L_e^{-1}$$

and note that ξ is injective since X is a (left) quasigroup. The identity $L_{y/(e \setminus x)} L_e^{-1}(x) = y$ shows that $\text{Dis}(X)$ is transitive and hence regular, being abelian. This implies that $G = \text{Dis}(X) = \{L_x L_e^{-1} : x \in G\}$ and thus that ξ is bijective. It remains to prove that ξ is a homomorphism. We want to show that $\xi(x) * \xi(y) = \varphi(L_x L_e^{-1}) \psi(L_y L_e^{-1}) c = (L_x L_e^{-1})^{R_{ee}} (L_y L_e^{-1})^\sigma (L_{ee} L_e^{-1})$ is equal to $\xi(xy) = L_{xy} L_e^{-1}$. Since $\text{Dis}(X)$ is regular, it is sufficient to check that the two permutations agree at a single point, for instance at $e \cdot ee$. Now,

$$\begin{aligned} (\xi(x) * \xi(y))(e \cdot ee) &= (L_x L_e^{-1})^{R_{ee}} (L_y L_e^{-1})^\sigma (L_{ee} L_e^{-1})(e \cdot ee) = (L_x L_e^{-1})^{R_{ee}} \sigma L_y L_e^{-1} \sigma^{-1}(ee \cdot ee) \\ &= (L_x L_e^{-1})^{R_{ee}} \sigma L_y L_e^{-1}(ee) = (L_x L_e^{-1})^{R_{ee}} \sigma(ye) \\ &= (L_x L_e^{-1})^{R_{ee}} (ye \cdot ye) \stackrel{(R_e)}{=} (L_x L_e^{-1})^{R_{ee}} (ey \cdot ee) \\ &= R_{ee} L_x L_e^{-1}(ey) = xy \cdot ee = L_{xy} L_e^{-1}(e \cdot ee) = \xi(xy)(e \cdot ee). \quad \square \end{aligned}$$

Corollary 4.19. *The following conditions are equivalent for a latin rumples X :*

- (1) X is linear;
- (2) X contains an idempotent element and $\text{Dis}(X)$ is abelian and normal in $\text{Mlt}(X)$.

Proof. If X is linear then 0 is an idempotent element. Conversely, in the construction in the proof of Theorem 4.18, use an idempotent element e and observe that $c = L_{ee}L_e^{-1} = 1$, the identity element in $\text{Dis}(X)$. \square

5. LATIN RUMPLES ISOTOPIC TO GROUPS

For the purposes of the present section, we extend the definition of linear representation. Let (G, \circ) be an arbitrary loop, not necessarily associative or commutative. A binary algebra $(G, *)$ is called *right linear* (resp. *left linear*) over (G, \circ) if there exist $\varphi : G \rightarrow G$ and $\psi \in \text{End}(G, \circ)$ (resp. $\varphi \in \text{End}(G, \circ)$ and $\psi : G \rightarrow G$) such that

$$x * y = \varphi(x) \circ \psi(y)$$

for all $x, y \in G$. As in the case of linear representations, note that $(G, *)$ is a left quasigroup if and only if φ is bijective, and a right quasigroup if and only if ψ is bijective.

Let us recall basic facts about loop isotopes (see [36] for details). For a quasigroup X , fix $e, f \in X$ and define a binary operation $\circ_{e,f} : X \times X \rightarrow X$ by

$$x \circ_{e,f} y = (x/e)(f \setminus y).$$

Then $(X, \circ_{e,f})$ is a loop with identity element fe and X is isotopic to $(X, \circ_{e,f})$. Loop isotopes of this form are said to be *principal*. Thus every quasigroup X is isotopic to a loop and every loop isotope of X is isomorphic to a principal loop isotope of X . Moreover, a group is isomorphic to all of its loop isotopes. Therefore, if a quasigroup X is isotopic to a group G then all loop isotopes of X are isomorphic to G .

The left multiplication group $\text{LMlt}(X, \circ_{e,f})$ is generated by all permutations of the form $L_{x/e}L_f^{-1}$, $x \in X$. From this observation, we see immediately that $\text{Dis}^+(X) = \text{LMlt}(X, \circ_{e,f})$ for every $e, f \in X$.

Proposition 5.1. *A quasigroup X is isotopic to a group if and only if $\text{Dis}^+(X)$ acts regularly on X . In such a case, $\text{Dis}^+(X)$ is isomorphic to all group isotopes of X .*

Proof. Note that if X is a loop with identity element 1 then $\text{Dis}^+(X) = \text{LMlt}(X)$ since $L_xL_1^{-1} = L_x$. Let us first show that a loop X is a group if and only if $\text{LMlt}(X)$ acts regularly on X . The direct implication is obvious. Conversely, suppose that $\text{LMlt}(X)$ acts regularly on X . For $g \in \text{LMlt}(X)$ there is $x \in X$ such that $g(1) = x$ and thus $g = L_x$ by regularity. Hence the composition of any two left translations L_xL_y is a left translation, necessarily L_{xy} on account of $L_{xy}(1) = L_xL_y(1)$. This means that X is a group.

Now let X be a quasigroup. If X is isotopic to a group G then there is a principal loop isotope $(X, \circ_{e,f})$ isomorphic to G . Then $\text{Dis}^+(X) = \text{LMlt}(X, \circ_{e,f})$ acts regularly on X by the first paragraph. Conversely, suppose that $\text{Dis}^+(X)$ acts regularly on X and let $(X, \circ_{e,f})$ be any loop isotope of X . Then $\text{LMlt}(X, \circ_{e,f}) = \text{Dis}^+(X)$ acts regularly and hence $(X, \circ_{e,f})$ is a group by the first paragraph. \square

Since transitive abelian permutation groups act regularly, we have the following corollary which can be traced to Belousov [1].

Corollary 5.2. *A quasigroup X is isotopic to an abelian group if and only if $\text{Dis}^+(X)$ is abelian.*

Theorem 5.3. *For a latin rumples X , the following conditions are equivalent:*

- (1) X is right linear over a group;
- (2) X is isotopic to a group;
- (3) $\text{Dis}(X)$ acts regularly on X .

Proof. The equivalence of (2) and (3) follows from Proposition 5.1. Obviously, (1) implies (2). We prove that (2) implies (1). Let X be (principally) isotopic to a group (X, \circ) , i.e., there are permutations φ, ψ of X such that $xy = \varphi(x) \circ \psi(y)$ for all $x, y \in X$. We may assume without loss of generality that $\psi(1) = 1$, otherwise, set $\bar{\varphi}(x) = \varphi(x) \circ \psi(1)$ and $\bar{\psi}(y) = \psi(1)^{-1} \circ \psi(y)$ so that $xy = \bar{\varphi}(x) \circ \bar{\psi}(y)$. Writing (R_ℓ) in terms of \circ, φ and ψ (and replacing z with $\psi^{-1}(z)$), we have

$$\varphi(\varphi(x) \circ \psi(y)) \circ \psi(\varphi(x) \circ z) = \varphi(\varphi(y) \circ \psi(x)) \circ \psi(\varphi(y) \circ z)$$

for all $x, y, z \in X$. Rearranging this, we have

$$\varphi(\varphi(y) \circ \psi(x))^{-1} \circ \varphi(\varphi(x) \circ \psi(y)) = \psi(\varphi(y) \circ z) \circ \psi(\varphi(x) \circ z)^{-1},$$

and we note that the left hand side is independent of z . Substituting first $z = 1$ and then $z = \varphi(x)^{-1}$ therefore yields

$$\psi(\varphi(y)) \circ \psi(\varphi(x))^{-1} = \psi(\varphi(y) \circ \varphi(x)^{-1})$$

for all $x, y \in X$. Since φ is a bijection, it follows that ψ is an automorphism and X is right linear over (X, \circ) . \square

Corollary 5.4. *For a latin rumple X , the following conditions are equivalent:*

- (1) X is right linear over an abelian group;
- (2) X is isotopic to an abelian group;
- (3) $\text{Dis}(X)$ is abelian.

We conclude this section with another characterization of affine latin rumple.

Lemma 5.5. *Let (G, \circ) be a group. If a quasigroup $(G, *)$ is both left linear and right linear over (G, \circ) , then there are $\varphi, \psi \in \text{Aut}(G, \circ)$ and $c \in G$ such that $x * y = \varphi(x) \circ c \circ \psi(y)$ for all $x, y \in G$.*

Proof. The direct implication is obvious. For the converse, suppose that for every $x, y \in G$ we have

$$(5.1) \quad x * y = \varphi_1(x) \circ g_1(y) = f_2(x) \circ \psi_2(y)$$

for some bijections g_1, f_2 of G and some automorphisms φ_1, ψ_2 of (G, \circ) . With $x = y = 1$, (5.1) yields $g_1(1) = f_2(1)$ and we will call this element c . Define bijections ψ_1, φ_2 by $g_1(x) = c \circ \psi_1(x)$ and $f_2(x) = \varphi_2(x) \circ c$. Note that $\psi_1(1) = 1 = \varphi_2(1)$. Then (5.1) implies

$$x * y = \varphi_1(x) \circ c \circ \psi_1(y) = \varphi_2(x) \circ c \circ \psi_2(y).$$

With $x = 1$ we obtain $c \circ \psi_1(y) = c \circ \psi_2(y)$ and hence $\psi_1 = \psi_2$. The equality $\varphi_1 = \varphi_2$ follows by setting $y = 1$. We finish the proof by taking $\varphi = \varphi_1$ and $\psi = \psi_2$. \square

Theorem 5.6. *A latin rumple is affine if and only if it is left linear over a group.*

Proof. Let $(X, *)$ be a latin rumple. The necessity is obvious, so assume $(X, *)$ is left linear over a group (X, \circ) . Since $(X, *)$ is isotopic to (X, \circ) , it follows from Theorem 5.3 that $(X, *)$ is also right linear over (X, \circ) . By Lemma 5.5, there are $\varphi, \psi \in \text{Aut}(X, \circ)$ and $c \in X$ such that

$$(5.2) \quad x * y = \varphi(x) \circ c \circ \psi(y)$$

for all $x, y \in X$. It remains to show that (X, \circ) is abelian.

Writing (R_ℓ) in terms of (5.2) and canceling $\psi(c) \circ \psi^2(z)$ on the right, we get

$$(5.3) \quad \varphi^2(x) \circ \varphi(c) \circ \varphi\psi(y) \circ c \circ \psi\varphi(x) = \varphi^2(y) \circ \varphi(c) \circ \varphi\psi(x) \circ c \circ \psi\varphi(y)$$

for all $x, y \in X$. Setting $x = 1$ and rearranging yields

$$(5.4) \quad \varphi\psi(y) = [\varphi(c^{-1} \circ \varphi(y) \circ c)] \circ [c \circ \psi\varphi(y) \circ c^{-1}]$$

for all $y \in X$. Observe that $\alpha(y) = \varphi(c^{-1} \circ \varphi(y) \circ c)$ and $\beta(y) = c \circ \psi\varphi(y) \circ c^{-1}$ define two automorphisms of (X, \circ) . Now, for all $x, y \in X$,

$$\begin{aligned}\alpha(x) \circ \alpha(y) \circ \beta(x) \circ \beta(y) &= \alpha(x \circ y) \circ \beta(x \circ y) = \varphi\psi(x \circ y) = \varphi\psi(x) \circ \varphi\psi(y) \\ &= \alpha(x) \circ \beta(x) \circ \alpha(y) \circ \beta(y),\end{aligned}$$

using (5.4) in the second and fourth equalities. Canceling, we have $\alpha(y) \circ \beta(x) = \beta(x) \circ \alpha(y)$ for all $x, y \in X$. Since α and β are permutations, (X, \circ) is abelian. \square

6. NILPOTENT LATIN RUMPLES

6.1. Central extensions. All the latin rumples X we have seen so far are affine, hence isotopic to an abelian group G and such that $\text{Dis}(X) = G$ is abelian and normal in $\text{Mlt}(X)$. In this section we will present a construction based on central extensions that produces examples of nonaffine latin rumples, even latin rumples not isotopic to groups.

We adapt the general construction of central extensions from the commutator theory of universal algebra [13, §7] to the class of rumples. (See [39] for other types of rumple extensions.)

Let $(G, +)$ be an abelian group, (F, \cdot) a left quasigroup, $\varphi \in \text{End}(G, +)$, $\psi \in \text{Aut}(G, +)$ and $\theta : F \times F \rightarrow G$. A *central extension* $\text{Ext}(G, F, \varphi, \psi, \theta)$ of $(G, +)$ by (F, \cdot) is the binary algebra $(G \times F, *)$ with multiplication

$$(a, x) * (b, y) = (\varphi(a) + \psi(b) + \theta(x, y), x \cdot y).$$

Note that we recover affine rumples as a special case of central extensions by setting $F = 1$.

It is easy to see that $\text{Ext}(G, F, \varphi, \psi, \theta)$ is a left quasigroup with

$$(a, x) \setminus (b, y) = (\psi^{-1}(c - \varphi(a) - \theta(x, x \setminus y)), x \setminus y)$$

and that it is latin if and only if F is latin and $\varphi \in \text{Aut}(G, +)$. Straightforward calculation yields:

Proposition 6.1. *Let $(G, +)$ be an abelian group, F a Rump left quasigroup, $\varphi \in \text{End}(G, +)$, $\psi \in \text{Aut}(G, +)$ and $\theta : F \times F \rightarrow G$. Then $\text{Ext}(G, F, \varphi, \psi, \theta)$ is a Rump left quasigroup if and only if $[\varphi, \psi] = \varphi^2$ and*

$$(6.1) \quad \varphi(\theta(x, y) - \theta(y, x)) + \psi(\theta(x, z) - \theta(y, z)) + \theta(xy, xz) - \theta(yx, yz) = 0$$

for every $x, y, z \in F$.

A Rump left quasigroup is said to be *nilpotent* if it is obtained from the trivial quasigroup by finitely many iterations of central extensions. If a nilpotent Rump left quasigroup can be obtained in n but no fewer steps, we say that it has *nilpotence class* n . (This is in accordance with the abstract definition of nilpotence thanks to [13, Proposition 7.1].)

Proposition 6.2. *Every finite nilpotent latin rumple has order $p_1^{p_1 k_1} \cdots p_r^{p_r k_r}$ for some distinct primes p_1, \dots, p_r and integers k_1, \dots, k_r .*

Proof. Let $X = \text{Ext}(G, F, \varphi, \psi, \theta)$ be a finite nilpotent latin rumple, where we can assume that G is a nontrivial group and F is a rumple of nilpotence class less than n , the nilpotence class of X . Since X is latin, F is also latin and $\varphi, \psi \in \text{Aut}(G)$ satisfy $[\varphi, \psi] = \varphi^2$. Then for any $c \in G$ the affine rumple $Y = \text{Aff}(G, \varphi, \psi, c)$ is latin and hence of order $|G| = |Y| = p_1^{p_1 k_1} \cdots p_r^{p_r k_r}$ by Theorem 4.11. If $n = 1$ then $X = Y$ and we are done. Otherwise $|F|$ and thus also $|X| = |G| \cdot |F|$ have the desired form by induction. \square

6.2. A class of central extensions over the Klein group. Throughout this subsection, let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $A, B \in \text{Aut}(G)$ be given by

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We have already observed that $[A, B] = A^2$ holds.

Let F be a rumple. Then a mapping $\theta : F \times F \rightarrow G$ can be written as

$$\theta(x, y) = \begin{pmatrix} \alpha(x, y) \\ \beta(x, y) \end{pmatrix}$$

for some $\alpha, \beta : F \times F \rightarrow \mathbb{Z}_2$. The cocycle condition (6.1) becomes

$$(6.2) \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha(x, y) - \alpha(y, x) \\ \beta(x, y) - \beta(y, x) \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha(x, z) - \alpha(y, z) \\ \beta(x, z) - \beta(y, z) \end{pmatrix} + \begin{pmatrix} \alpha(xy, xz) - \alpha(yx, yz) \\ \beta(xy, xz) - \beta(yx, yz) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

which is equivalent to the system of linear equations

$$\begin{aligned} \beta(x, y) - \beta(y, x) + \alpha(x, z) - \alpha(y, z) + \alpha(xy, xz) - \alpha(yx, yz) &= 0, \\ \alpha(x, y) - \alpha(y, x) + \alpha(x, z) - \alpha(y, z) + \beta(x, z) - \beta(y, z) + \beta(xy, xz) - \beta(yx, yz) &= 0. \end{aligned}$$

A solution is obtained by setting

$$(6.3) \quad \alpha = 0 \quad \text{and} \quad \beta(x, y) = \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{otherwise.} \end{cases}$$

Indeed, $x = z$ if and only if $yx = yz$, so $\beta(x, z) = \beta(yx, yz)$, $\beta(y, z) = \beta(xy, xz)$, and, of course, $\beta(x, y) = \beta(y, x)$.

Lemma 6.3. Suppose that $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, F is a nontrivial affine latin rumple, $A, B \in \text{Aut}(G, +)$ and $\theta : F \times F \rightarrow G$ are given by

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \theta(x, y) = \begin{pmatrix} 0 \\ \beta(x, y) \end{pmatrix}, \quad \beta(x, y) = \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{otherwise.} \end{cases}$$

Then $\text{Ext}(G, F, A, B, \theta)$ is a latin rumple with nonabelian $\text{Dis}(X)$. In particular, X is not affine.

Proof. We have already verified that $[A, B] = A^2$ and (6.1) holds, so X is a latin rumple. Denote a typical element of $G \times F$ by

$$\mathbf{x} = \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, x \right).$$

Straightforward calculation then yields

$$\begin{aligned} L_{\mathbf{x}}(\mathbf{y}) &= \left(\begin{pmatrix} x_2 + y_1 \\ x_1 + y_1 + y_2 + \beta(x, y) \end{pmatrix}, xy \right), \\ L_{\mathbf{x}}^{-1}(\mathbf{y}) &= \left(\begin{pmatrix} -x_2 + y_1 \\ -x_1 + x_2 - y_1 + y_2 - \beta(x, x \setminus y) \end{pmatrix}, x \setminus y \right), \\ L_{\mathbf{x}}^{-1}L_{\mathbf{y}}(\mathbf{z}) &= \left(\begin{pmatrix} -x_2 + y_2 + z_1 \\ -x_1 + x_2 + y_1 - y_2 + z_2 + \beta(y, z) - \beta(x, x \setminus (yz)) \end{pmatrix}, x \setminus (yz) \right), \\ L_{\mathbf{x}}^{-1}L_{\mathbf{y}}L_{\mathbf{u}}^{-1}L_{\mathbf{v}}(\mathbf{z}) &= \left(\begin{pmatrix} w_1 \\ w_2 \end{pmatrix}, x \setminus (y(u \setminus (vz))) \right), \end{aligned}$$

where

$$\begin{aligned} w_1 &= -x_2 + y_2 - u_2 + v_2 + z_1, \\ w_2 &= -x_1 + x_2 + y_1 - y_2 - u_1 + u_2 + v_1 - v_2 + z_2 \\ &\quad + \beta(v, z) - \beta(u, u \setminus (vz)) + \beta(y, u \setminus (vz)) - \beta(x, x \setminus (y(u \setminus (vz)))). \end{aligned}$$

Since F is affine, the group $\text{Dis}(F)$ is abelian and

$$x \setminus (y(u \setminus (vz))) = L_x^{-1} L_y L_u^{-1} L_v(z) = L_u^{-1} L_v L_x^{-1} L_y(z) = u \setminus (v(x \setminus (yz)))$$

holds. We then see that $L_x^{-1} L_y L_u^{-1} L_v(z)$ is equal to $L_u^{-1} L_v L_x^{-1} L_y(z)$ if and only if

$$(6.4) \quad \begin{aligned} &\beta(v, z) - \beta(u, u \setminus (vz)) + \beta(y, u \setminus (vz)) - \beta(x, x \setminus (y(u \setminus (vz)))) \\ &= \beta(y, z) - \beta(x, x \setminus (yz)) + \beta(v, x \setminus (yz)) - \beta(u, u \setminus (v(x \setminus (yz)))) \end{aligned}$$

for every $x, y, u, v, z \in F$. Thus $\text{Dis}(X)$ is nonabelian if (6.4) fails for a choice of elements of F .

Setting $u = y$ in (6.4) yields

$$\beta(v, z) - \beta(x, x \setminus (vz)) = \beta(y, z) - \beta(x, x \setminus (yz)) + \beta(v, x \setminus (yz)) - \beta(y, y \setminus (v(x \setminus (yz)))).$$

Substituting $z = y \setminus x^2$ (which is equivalent to $x \setminus (yz) = x$) and using $\beta(x, x) = 1$ then yields

$$(6.5) \quad \beta(v, y \setminus x^2) - \beta(x, x \setminus (v(y \setminus x^2))) = \beta(y, y \setminus x^2) - 1 + \beta(v, x) - \beta(y, y \setminus (vx)).$$

Select $x \neq y$ in F arbitrarily. Then $x^2 \neq y^2$ by unique 2-divisibility and hence $\beta(y, y \setminus x^2) = \beta(y, y \setminus (yx^2)) = \beta(y^2, x^2) = 0$. Select $v \in F$ such that $v \neq x$ (which yields $\beta(v, x) = 0$), $v \neq y$ (which implies $v \setminus x^2 \neq y \setminus x^2$, $x^2 \neq v(y \setminus x^2)$ and $\beta(x, x \setminus (v(y \setminus x^2))) = 0$), $v \neq y^2/x$ (which implies $\beta(y, y \setminus (vx)) = 0$) and $v \neq y \setminus x^2$ (which yields $\beta(v, y \setminus x^2) = 0$). Altogether, (6.5) becomes $0 = -1$. When $|F| \geq 5$, it is certainly possible to select x, y and $v \in F$ as above. When $|F| < 5$ then $F = X_{4,1}$ or $F = X_{4,2}$ as in Example 3.3. In $X_{4,1}$, choose $x = 0, y = 1$ and $v = 2$. In $X_{4,2}$, choose $x = 0, y = 1$ and $v = 3$.

We have proved that $\text{Dis}(X)$ is nonabelian. By Theorem 4.18, X is not affine. \square

Example 6.4. Note that Lemma 6.3 is only one of many possible solutions to the matrix equation (6.2). The corresponding system of linear equations over \mathbb{Z}_2 can be solved by standard methods of linear algebra. All latin rumples X below were obtained as central extensions of $\mathbb{Z}_2 \times \mathbb{Z}_2$:

- X of order 16 with $\text{Dis}(X) = \mathbb{Z}_2 \times Q_8$, where Q_8 is the quaternion group,
- X of order 16 with $\text{Dis}(X)$ abelian but not normal in $\text{Mlt}(X)$,
- X of order 64 not isotopic to a group and satisfying the right Rump identity (R_r) ,
- X of order 108 with $\text{Dis}(X)$ a nonnilpotent group.

7. BOTH-SIDED RUMPLES

Recall that the two four-element latin rumples of Example 3.3 satisfy the right Rump identity (R_r) . In this section we investigate in a systematic way left quasigroups satisfying both (R_ℓ) and (R_r) . Our first result will show that such left quasigroups are automatically latin rumples.

7.1. The two Rump identities and the squaring map.

Lemma 7.1. *Let X be a left quasigroup and assume that the identity*

$$(7.1) \quad ((x \setminus y) \setminus y)x = y$$

holds for all $x, y \in X$. Then X is a quasigroup.

Proof. Define an operation $/$ on X by setting

$$(7.2) \quad y/x = (x \setminus y) \setminus y$$

and note that (7.1) immediately implies $(y/x)x = y$. Dividing by $(x \setminus y) \setminus y$ on the left in (7.1) yields $((x \setminus y) \setminus y) \setminus y = x$, and thus $yx/x = (x \setminus yx) \setminus yx = ((y \setminus yx) \setminus yx) \setminus yx = y$. \square

Proposition 7.2. *The following conditions are equivalent for a left quasigroup X :*

- (1) X satisfies (R_ℓ) and (R_r) ;
- (2) X is a rumples satisfying (R_r) ;
- (3) X is a latin rumples satisfying (R_r) .

In these equivalent situations, the right division operation is given by (7.2).

Proof. Obviously, (3) \Rightarrow (2) \Rightarrow (1). Suppose that (1) holds and let us establish (3) by showing that (7.1) holds. Indeed, we have

$$\begin{aligned} (x \setminus y)x \cdot ((x \setminus y) \setminus y)x &\stackrel{(R_r)}{=} (x \setminus y)((x \setminus y) \setminus y) \cdot x((x \setminus y) \setminus y) = y \cdot x((x \setminus y) \setminus y) \\ &= x(x \setminus y) \cdot x((x \setminus y) \setminus y) \stackrel{(R_\ell)}{=} (x \setminus y)x \cdot (x \setminus y)((x \setminus y) \setminus y) = (x \setminus y)x \cdot y, \end{aligned}$$

from which (7.1) follows upon canceling $(x \setminus y)x$ on the left. By Lemma 7.1, X is a quasigroup. By Proposition 3.1, X is a rumples. \square

A *both-sided rumples* is a left quasigroup satisfying any of the three equivalent conditions of Proposition 7.2.

It follows from Proposition 7.2 that the notion of both-sided rumples is self-dual. That is, if (X, \cdot) is a both-sided rumples, then so is (X, \cdot_{op}) with $x \cdot_{\text{op}} y = y \cdot x$. Thus if an identity holds in a both-sided rumples then its mirror image also holds. We will occasionally appeal to this observation.

Proposition 7.3. *Let X be a both-sided rumples and let σ be the squaring map on X . Then:*

- (1) σ is an antiautomorphism of X .
- (2) σ^2 is an automorphism of X .
- (3) $\sigma^2(x) = xx \cdot xx = yy \cdot yy = xy \cdot yy = yx \cdot xy$ for every $x, y \in X$.
- (4) $\sigma^2 = L_{yy}L_y = R_{yy}R_y$ for every $y \in X$.

Proof. Note that (2) follows from (1), and (4) follows from (3). Let us prove (1). For every $x, y \in X$ we have

$$\begin{aligned} (xy \cdot yy)(yx \cdot yx) &\stackrel{(R_\ell)}{=} (xy \cdot yy)(xy \cdot xx) \stackrel{(R_\ell)}{=} (yy \cdot xy)(yy \cdot xx) \\ &\stackrel{(R_r)}{=} (yx \cdot yx)(yy \cdot xx) \stackrel{(R_\ell)}{=} (xy \cdot xx)(yy \cdot xx) \stackrel{(R_r)}{=} (xy \cdot yy)(xx \cdot yy) \end{aligned}$$

and we deduce $\sigma(yx) = \sigma(x)\sigma(y)$ upon canceling $xx \cdot yy$ on the left. For (3), we compute

$$(y \setminus xx)y \cdot (y \setminus xx)y \stackrel{(R_\ell)}{=} y(y \setminus xx) \cdot yy = xx \cdot yy \stackrel{(1)}{=} yx \cdot xy.$$

Taking square roots of both sides, we obtain $(y \setminus xx)y = yx$ and therefore

$$yy \cdot yx = yy \cdot (y \setminus xx)y \stackrel{(R_r)}{=} y(y \setminus xx) \cdot y(y \setminus xx) = xx \cdot xx.$$

A dual argument yields $xx \cdot xx = xy \cdot yy$. Finally, substituting xy for x and yx for y into the established identity $yx = (y \setminus xx)y$ yields

$$yx \cdot xy = (yx \setminus (xy \cdot xy)) \cdot yx \stackrel{(R_\ell)}{=} (yx \setminus (yx \cdot yy)) \cdot yx = yy \cdot yx. \quad \square$$

7.2. Both-sided rumples isotopic to groups.

Lemma 7.4. *Let X be a both-sided ruple. Then $x \setminus y \cdot y/x = y$ and $x/y \cdot y \setminus x = yy$ for every $x, y \in X$.*

Proof. The first identity follows from the right division formula in Proposition 7.2. By Proposition 7.3.2, σ^2 is an automorphism with respect to multiplication and hence also with respect to left division in X . By Proposition 7.3.3, $\sigma^2(x) = x(yy) \cdot (yy \cdot yy) = x(yy) \cdot \sigma^2(y)$, so $x(yy) = \sigma^2(x)/\sigma^2(y) = \sigma^2(x/y)$. By Proposition 7.3.3 again, $\sigma^2(u) = vu \cdot uv$, from which we obtain $\sigma^2(x/y) = (y \setminus x \cdot x/y)(x/y \cdot y \setminus x)$ upon substituting x/y for u and $y \setminus x$ for v . Combining, we have

$$x(yy) = \sigma^2(x/y) = (y \setminus x \cdot x/y)(x/y \cdot y \setminus x) = x(x/y \cdot y \setminus x)$$

and we obtain the second identity from the statement by canceling x on the left. \square

Corollary 7.5. *Let X be a both-sided ruple. Then for each $e \in X$, the principal loop isotope $(X, \circ_{e,e})$ defined by $x \circ_{e,e} y = (x/e)(e \setminus y)$ has exponent 2.*

Proof. The principal loop isotope $(X, \circ_{e,e})$ has identity element ee . By Lemma 7.4, $x \circ_{e,e} x = ee$. \square

Corollary 7.6. *If a both-sided ruple X is isotopic to a group, then it is isotopic to an elementary abelian 2-group.*

Proof. If a quasigroup X is isotopic to a group G then all loop isotopes of X are isomorphic to G . We are done by Corollary 7.5. \square

7.3. Generators of the displacement group. In this section we prove that all generators of the displacement group $\text{Dis}(X)$ of a both-sided ruple X have order dividing 4.

Lemma 7.7. *Let X be a both-sided ruple. Then:*

- (1) $L_{xy}^{-1}L_{yy} = L_{yx}^{-1}L_{xx}$ for every $x, y \in X$.
- (2) $L_{xx}L_{yx}^{-1}L_{yy} = L_{xy}$ for every $x, y \in X$.

Proof. (1) We have

$$L_{yy} = L_{yy}L_yL_y^{-1} \stackrel{7.3.4}{=} \sigma^2L_y^{-1} \stackrel{7.3.2}{=} L_{\sigma^2(y)}^{-1} \sigma^2 \stackrel{7.3.3}{=} L_{xy \cdot yx}^{-1} \sigma^2.$$

Reversing the roles of x and y , we obtain $L_{xx} = L_{yx \cdot xy}^{-1} \sigma^2$. It therefore remains to prove $L_{xy}^{-1}L_{xy \cdot yx}^{-1} = L_{yx}^{-1}L_{yx \cdot xy}^{-1}$, that is, $L_{xy \cdot yx}L_{xy} = L_{yx \cdot xy}L_{yx}$, which is a consequence of (R'_ℓ) .

(2) Let us first establish

$$(7.3) \quad (x \setminus yx)x = yy \quad \text{and} \quad (x \setminus yx)^2 = xy.$$

For the first identity, calculate

$$xx \cdot (x \setminus yx)x \stackrel{(R_r)}{=} x(x \setminus yx) \cdot x(x \setminus yx) = yx \cdot yx \stackrel{7.3.2}{=} xx \cdot yy$$

and cancel xx on the left. For the second identity, observe

$$yx \cdot xy \stackrel{7.3.3}{=} \sigma^2(x) \stackrel{7.3.4}{=} x(x \setminus yx) \cdot (x \setminus yx)^2 = yx \cdot (x \setminus yx)^2$$

and cancel yx on the left. Then

$$\begin{aligned} L_{xx}L_{yx}^{-1}L_{yy} &= L_{xx}L_xL_x^{-1}L_{yx}^{-1}L_{yy} \stackrel{7.3.4}{=} \sigma^2L_x^{-1}L_{yx}^{-1}L_{yy} = \sigma^2(L_{x(x \setminus yx)}L_x)^{-1}L_{yy} \\ &\stackrel{(R'_r)}{=} \sigma^2(L_{(x \setminus yx)x}L_{x \setminus yx})^{-1}L_{yy} \stackrel{(7.3)}{=} \sigma^2L_{x \setminus yx}^{-1}L_{yx}^{-1}L_{yy} = \sigma^2L_{x \setminus yx}^{-1} \stackrel{7.3.4}{=} L_{(x \setminus yx)^2} \stackrel{(7.3)}{=} L_{xy}. \quad \square \end{aligned}$$

Proposition 7.8. *Let X be a both-sided rumple. Then*

$$(L_x L_y^{-1})^4 = 1 = (R_x R_y^{-1})^4$$

for every $x, y \in X$.

Proof. We will prove the first equality. The second equality follows by a dual argument. We have

$$\begin{aligned} (L_x L_y^{-1})^2 &= L_x L_y^{-1} \cdot L_x L_y^{-1} \stackrel{(R'_l)}{=} L_{xy}^{-1} L_{yx} \cdot L_{xx}^{-1} L_{xx} L_x L_y^{-1} L_{yy}^{-1} L_{yy} \\ &\stackrel{7.3.4}{=} L_{xy}^{-1} L_{yx} \cdot L_{xx}^{-1} \sigma^2 \sigma^{-2} L_{yy} \stackrel{7.7.2}{=} L_{xy}^{-1} L_{yy} L_{xy}^{-1} L_{xx} L_{xx}^{-1} L_{yy} = L_{xy}^{-1} L_{yy} L_{xy}^{-1} L_{yy}. \end{aligned}$$

Thus we have

$$\begin{aligned} (L_x L_y^{-1})^4 &= L_{xy}^{-1} L_{yy} L_{xy}^{-1} L_{yy} L_x L_y^{-1} L_x L_y^{-1} \stackrel{7.7.1}{=} L_{xy}^{-1} L_{yy} L_{yx}^{-1} L_{xx} L_x L_y^{-1} L_x L_y^{-1} \\ &\stackrel{7.3.4}{=} L_{xy}^{-1} L_{yy} L_{yx}^{-1} L_{yy} L_y L_y^{-1} L_x L_y^{-1} \stackrel{7.7.1}{=} L_{xy}^{-1} L_{yy} L_y (L_{yx} L_y)^{-1} L_{yy} L_x L_y^{-1} \\ &\stackrel{(R'_l)}{=} L_{xy}^{-1} L_{yy} L_y (L_{xy} L_x)^{-1} L_{yy} L_x L_y^{-1} \stackrel{7.3.4}{=} L_{xy}^{-1} L_{xx} L_{xy}^{-1} L_{yy} L_x L_y^{-1} \\ &\stackrel{7.7.1}{=} L_{xy}^{-1} L_{xx} L_{yx}^{-1} L_{xx} L_x L_y^{-1} = L_{xy}^{-1} L_{xx} L_{yx}^{-1} L_{yy} L_y L_y^{-1} \stackrel{7.7.2}{=} L_{xy}^{-1} L_{xy} = 1. \quad \square \end{aligned}$$

Although Proposition 7.8 is interesting in its own right, it also has an implication for loop isotopes of a both-sided rumple X : it turns out that the conclusion of the proposition is equivalent to the assertion that every loop isotopic to X is power-associative of exponent dividing 4. (The proof is not difficult but it would take us a bit far afield of the main topic of this paper.) Combining this with Corollary 7.5, we can conclude that if X is a both-sided rumple which is not isotopic to a group, then some loop isotope achieves exponent 4. This is because if all loops isotopic to a given quasigroup have exponent 2, then those loops are isomorphic abelian groups [3].

REFERENCES

- [1] V. D. Belousov, *Balanced identities in quasigroups*, (Russian) Mat. Sb. (N.S.) **70**(112) (1966), 55–97. (In Russian.)
- [2] M. Bonatto, D. Stanovský, *Commutator theory for racks and quandles*, <https://arxiv.org/abs/1902.08980>
- [3] R.H. Bruck, *Survey of binary systems*, Springer, 1971.
- [4] F. Chouraqui, E. Godelle, *Finite quotients of groups of I-type*, Adv. Math. **258** (2014), 46–68.
- [5] F. Catino, I. Colazzo, P. Stefanelli, *Semi-braces and the Yang–Baxter equation*, J. Algebra **483** (2017), 163–187.
- [6] F. Cedó, E. Jespers, and J. Okniński, *Braces and the Yang–Baxter equation*, Comm. Math. Physics **327** (2014) 101–116.
- [7] P. Dehornoy, *Set-theoretic solutions of the Yang–Baxter equation, RC-calculus, and Garside germs*, Adv. Math. **282** (2015) 93–127.
- [8] A. Drápal, *Group isotopes and a holomorphic action*, Result. Math. **54** (2009), no. 3–4, 253–272.
- [9] V. G. Drinfeld, *On unsolved problems in quantum group theory*, Quantum Groups, Lecture Notes in Math. **1510**, Springer-Verlag, Berlin, 1992, 1–8.
- [10] M. Elhamdadi, S. Nelson, *Quandles: an introduction to the algebra of knots*, Student Mathematical Library, **74**, American Mathematical Society, Providence, RI, 2015.
- [11] P. Etingof, T. Schedler, A. Soloviev, *Set-theoretical solutions to the quantum Yang–Baxter equation*, Duke Math. J. **100** (1999) 169–209.
- [12] R. Fenn, M. Jordan-Santana, L. Kauffman, *Biquandles and virtual links*, Topology and its Appl. **145** (2004), 157–175.
- [13] R. Freese, R. McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Notes **125**, Cambridge University Press, 1987.
- [14] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.2; 2019*, (<https://www.gap-system.org>).
- [15] T. Gateva-Ivanova, *A combinatorial approach to the set-theoretic solutions of the Yang–Baxter equation*, J. Math. Phys. **45** (2004), 3828–3858.
- [16] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang–Baxter equation, braces and symmetric groups*, Adv. Math. **338** (2018), 649–701.
- [17] T. Gateva-Ivanova, P. Cameron, *Multipermutation solutions of the Yang–Baxter equation*, Comm. Math. Phys. **309** (2012), 583–621.

- [18] T. Gateva-Ivanova, S. Majid, *Quantum spaces associated to multipermutation solutions of level two*, *Algebr. Represent. Theory* **14** (2011), 341–376.
- [19] T. Gateva-Ivanova, M. Van den Bergh, *Semigroups of I-type*, *J. Algebra* **206** (1998), 97–112.
- [20] L. Guarnieri, L. Vendramin, *Skew braces and the Yang-Baxter equation*, *Math. Comp.* **86** (2017), 2519–2534.
- [21] X. Hou, *Finite modules over $\mathbb{Z}[t, t^{-1}]$* , *J. Knot Theory Ramifications* **21** (2012), no. 8, 1250079, 28 pp.
- [22] A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups*, *J. Pure Appl. Algebra* **220** (2016), no. 2, 735–758.
- [23] P. Jedlička, A. Pilitowska, D. Stanovský, A. Zamojska-Dzienio, *The structure of medial quandles*, *J. Algebra* **443** (2015), 300–334.
- [24] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *The construction of multipermutation solutions of the Yang-Baxter equation of level 2*, <https://arxiv.org/abs/1901.01471>
- [25] D. Joyce, *A classifying invariant of knots, the knot quandle*, *J. Pure Appl. Algebra* **23** (1982), no. 1, 37–65.
- [26] T. Kepka, P. Němec, *T-quasigroups II*, *Acta Univ. Carolin. Math. Phys.* **12** (1971), no. 2, 31–49.
- [27] T.Y. Lam, *A first course in noncommutative rings*, *Graduate Texts in Mathematics* **131**, 2ed. Springer, 2001.
- [28] V. Lebed, *Applications of self-distributivity to Yang-Baxter operators and their cohomology*, *J. Knot Theory Ramifications* **27** (2018), no. 11, 1843012, 20 pp.
- [29] V. Lebed, L. Vendramin, *Homology of left non-degenerate set-theoretic solutions to the Yang-Baxter equation*, *Adv. Math.* **304** (2017), 1219–1261.
- [30] V. Lebed, L. Vendramin, *On structure groups of set-theoretic solutions to the Yang-Baxter equation*, *Proc. Edinb. Math. Soc.* (2) **62** (2019), no. 3, 683–717.
- [31] S.V. Matveev, *Distributive groupoids in knot theory* (Russian), *Mat. Sb. (N.S.)* **119(161)** (1982), no. 1, 78–88.
- [32] W. McCune, *Mace4*, <https://www.cs.unm.edu/~mccune/mace4>
- [33] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, *Adv. Math.* **193** (2005), 40–55.
- [34] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, *J. Algebra* **307** (2007), 153–170.
- [35] N. J. A. Sloane, editor, *The On-Line Encyclopedia of Integer Sequences*, published electronically at <https://oeis.org>.
- [36] J. D. H. Smith, *An introduction to quasigroups and their representations*, Chapman & Hall/CRC, 2007.
- [37] D. Stanovský, *A guide to self-distributive quasigroups, or latin quandles*, *Quasigroups and Related Systems* **23** (2015), no. 1, 91–128.
- [38] A. Stein, *A conjugacy class as a transversal in a finite group*, *J. Algebra* **239** (2001), 365–390.
- [39] L. Vendramin, *Extensions of set-theoretic solutions of the Yang-Baxter equation and a conjecture of Gateva-Ivanova*, *J. Pure Appl. Algebra* **220** (2016), no. 5, 2064–2076.

(Bonatto) MATHEMATICS RESEARCH INSTITUTE LUIS A. SANTALÓ (IMAS), UNIVERSIDAD DE BUENOS AIRES, BUENOS AIRES, ARGENTINA

E-mail address: marco.bonatto.87@gmail.com

(Kinyon, Vojtěchovský) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DENVER, DENVER, COLORADO 80208, USA

E-mail address: mkinyon@du.edu

E-mail address: petr@math.du.edu

(Stanovský) DEPARTMENT OF ALGEBRA, FACULTY OF MATHEMATICS AND PHYSICS, CHARLES UNIVERSITY, PRAGUE, CZECH REPUBLIC

E-mail address: stanovsk@karlin.mff.cuni.cz