On generalized associativity in groupoids

Reza Akhtar

Abstract. Following an approach developed by Niemenmäa and Kepka, we prove that if a division groupoid $G$ satisfies the identity $R_{x_1}L_{x_2} \ldots R_{x_{2n-1}}L_{x_{2n}}y = L_{x_{2n}}R_{x_{2n-1}} \ldots L_{x_2}R_{x_1}y$ for some $n \neq 2$, then $G$ is an abelian group. Using equational reasoning, we also give a new proof of a result of Niemenmäa and Kepka that a division groupoid in which the generalized associative law $x_1(x_2(\ldots x_{n-1}x_n)\ldots) = ((\ldots(x_1x_2)\ldots)x_{n-1})x_n$ holds must be a group.

1. Introduction

Let $G$ be a groupoid, with composition written as juxtaposition. For $a \in G$, we define the left multiplication map $L_a : G \to G$ by $x \mapsto ax$ and the right multiplication map $R_a : G \to G$ by $x \mapsto xa$. If these maps are surjective for all $a \in G$, we call $G$ a division groupoid. If these maps are bijective for all $a \in G$, we call $G$ a quasigroup. For more on quasigroups, we refer the reader to [2].

Since the operation on a groupoid is not in general associative, direct study of such objects is usually rather difficult. One way around this problem is to construct an auxiliary group whose properties reflect those of the groupoid operation, and then use this group to study the original structure. This approach was exploited successfully by Niemenmäa and Kepka in [1], in which they showed that any division groupoid satisfying the identity

$$I_n : x_1(x_2(\ldots x_{n-1}x_n)\ldots) = ((\ldots(x_1x_2)\ldots)x_{n-1})x_n$$

is in fact a group. While it is clear that $I_n$ constitutes a generalization of associativity, it is far from obvious that it implies associativity.

At the end of [1], the authors define a groupoid identity $M = N$ to be linear if $M$ and $N$ contain the same set of indeterminates, and each such indeterminate occurs exactly once on each side. They then pose the question of determining which linear groupoid identities imply associativity. Considering that the associative law $(xy)z = x(yz)$ may be written (in terms of the multiplication maps) as $R_zL_yx = L_yR_zx$, it is perhaps natural to consider the following family of linear groupoid identities:

$$J_n : R_{x_1}L_{x_2} \ldots R_{x_{2n-1}}L_{x_{2n}}y = L_{x_{2n}}R_{x_{2n-1}} \ldots L_{x_2}R_{x_1}y$$
as generalizations of the associative law, which is the case \( n = 1 \). Modifying the techniques of [1], we show, in the first part of this article, that if \( n \geq 2 \), then a division groupoid satisfies \( \mathcal{I}_n \) if and only if it is an abelian group. In the second part of the article, we use equational reasoning to give a much shorter proof of the original Niemenmäki-Kepka result that \( \mathcal{I}_n \) implies associativity. The first part of that proof is a relatively straightforward argument that any division groupoid satisfying \( \mathcal{I}_n \) is in fact a quasigroup; this is essentially the same as the reasoning in the original paper [1]. In the second part of the proof, however, we use an inductive argument to show that any quasigroup satisfying \( \mathcal{I}_n \) implies associativity, thereby circumventing the need to introduce an auxiliary group structure. The ideas in this part of the proof were inspired by output from Prover9 for the implication \( I_4 \implies I_5 \); however, our proof follows a different path from that outlined in the Prover9 output.

Following [1], we make the following definitions. Let \( G \) be a groupoid and \( P(G) \) the set of permutations of \( G \).

\[
AL(G) = \{ f \in P(G) : f(xy) = g(x)y \text{ for some } g \in P(G) \text{ and all } x, y \in G \}
\]

\[
AR(G) = \{ g \in P(G) : f(xy) = g(x)y \text{ for some } f \in P(G) \text{ and all } x, y \in G \}
\]

\[
BL(G) = \{ f \in P(G) : f(xy) = xg(y) \text{ for some } g \in P(G) \text{ and all } x, y \in G \}
\]

\[
BR(G) = \{ g \in P(G) : f(xy) = xg(y) \text{ for some } f \in P(G) \text{ and all } x, y \in G \}
\]

We say that \( G \) is \( AL \)-transitive if for all \( x, y \in G \) there exists \( f \in AL(G) \) such that \( f(x) = y \). The notions of \( AR \), \( BL \) and \( BR \)-transitivity are defined similarly.

A key property undergirding both parts of this paper is a rigidity principle which appears in [1] as Lemma 2.5. We give a slightly modified version of this below.

**Lemma 1.1.** [1, Lemma 2.5] Suppose a division groupoid \( G \) is \( BL \)-transitive. If \( f, f' \in AL(G) \) and \( f(a) = f'(a) \) for some \( a \in G \), then \( f = f' \). The same is true if \( G \) is assumed to be \( AL \)-transitive and \( f, f' \in BL(G) \).

**Proof.** Suppose first that \( G \) is \( BL \)-transitive and \( f, f' \in AL(G) \), \( a \in G \) are such that \( f(a) = f'(a) \). Select \( c \in G \) arbitrarily, and use surjectivity of \( L_c \) to find \( d \in G \) such that \( a = cd \). Next, given \( z \in G \), use \( BL \)-transitivity to find \( h \in BL(G) \) such that \( h(a) = z \). Let \( g, g', k \in P(G) \) witness that the formulas \( f(xy) = g(x)y \), \( f'(xy) = g'(x)y \), and \( h(xy) = xk(y) \) hold for \( x, y \in G \). Now

\[
f(z) = f(h(a)) = f(h(cd)) = f(ck(d)) = g(c)k(d) = h(g(c)d) = h(f(cd))
\]

\[
= hf(a) = hf'(a) = hf'(cd) = h(g'(c)d) = g'(c)k(d) = f'(ck(d))
\]

\[
= f'(h(cd)) = f'(h(a)) = f'(z).
\]

The proof of the second statement is similar. \( \square \)
We will also need the following key result:

**Proposition 1.2.** [1, Proposition 3.4] Let $G$ be a quasigroup which is both $AL$- and $BL$-transitive and satisfies $AL(G) \subseteq AR(G)$, $BL(G) \subseteq BR(G)$. Then there exists a binary operation $*$ such that $(G, *)$ is a group and $xy = A(x) \ast c \ast B(y)$ for some $c \in G$ and some automorphisms $A, B$ of $(G, *)$.

## 2. A generalized form of associativity

In this section, we consider the identity

$$J_n : R_{x_1}L_{x_2} \cdots R_{x_{2n-1}}L_{x_{2n}}y = L_{x_{2n}}R_{x_{2n-1}} \cdots L_{x_2}R_{x_1}y$$

as another generalization of the associative law. We may rewrite $J_n$ in two different ways:

$$L_{x_2} \cdots R_{x_{2n-1}}L_{x_{2n}}y \cdot x_1 = L_{x_{2n}}R_{x_{2n-1}} \cdots L_{x_2}(yx_1), \quad (1)$$

$$R_{x_1}L_{x_2} \cdots R_{x_{2n-1}}(x_{2n}y) = x_{2n} \cdot R_{x_{2n-1}} \cdots L_{x_2}R_{x_1}y. \quad (2)$$

These formulas witness that if $G$ is a groupoid in which $J_n$ is satisfied, then $L_{x_2}R_{x_{2n-1}} \cdots L_{x_{2n}} \in AL(G) \cap AR(G)$ and $R_{x_1}L_{x_2} \cdots R_{x_{2n-1}} \in BL(G) \cap BR(G)$. In particular, if $G$ is a division groupoid, then $G$ is both $AL$-transitive and $BL$-transitive.

We are now ready to prove our main result.

**Theorem 2.1.** Let $G$ be a division groupoid and $n \geq 2$. Then $G$ satisfies $J_n$ if and only if $G$ is an abelian group.

**Proof.** Suppose first that $G$ is a division groupoid satisfying $J_n$. We argue first that $G$ must be a quasigroup. Given $a \in G$, fix $b \in G$, and use surjectivity of the multiplication maps to select $c_1, \ldots, c_{2n-2}$ such that $L_{c_1}R_{c_2} \cdots R_{c_{2n-2}}L_a b = b$. Now $L_{c_1}R_{c_2} \cdots R_{c_{2n-2}}L_a \in AL(G)$, so by Lemma 1.1, $L_{c_1}R_{c_2} \cdots R_{c_{2n-2}}L_a = 1_G$. Therefore, $L_a$ is injective.

Next, we show that $G$ satisfies the remaining hypotheses of Proposition 1.2. Given $f \in AL(G)$, fix $a \in G$ and use surjectivity of the multiplication maps to select $d_1, \ldots, d_{2n-1} \in G$ such that $L_{d_1}R_{d_2} \cdots R_{d_{2n-1}}a = f(a)$. Because we have $L_{d_1}R_{d_2} \cdots R_{d_{2n-1}}$ and $f$ are both members of $AL(G)$, Lemma 1.1 implies that $f = L_{d_1}R_{d_2} \cdots L_{d_{2n-1}}$, so $f \in AR(G)$ also. Thus, $AL(G) \subseteq AR(G)$. The proof of the inclusion $BL(G) \subseteq BR(G)$ is similar.

Now we use Proposition 1.2 to deduce the existence of a binary operation $+$ on $G$ such that $(G, +)$ is a group and $xy = A(x) + c + B(y)$ for some automorphisms $A$ and $B$ of $(G, +)$. (Even though $(G, +)$ is not assumed to be an abelian group, we will still use additive notation to avoid confusion with the groupoid operation on $G$.) The identity

$$J_n : R_{x_1}L_{x_2} \cdots R_{x_{2n-1}}L_{x_{2n}}y = L_{x_{2n}}R_{x_{2n-1}} \cdots L_{x_2}R_{x_1}y$$
Proposition 3.1. Let $n \geq 3$. Then a division groupoid satisfying $I_n$ is a quasigroup.
Proof. Note that $I_n$ can be interpreted in two ways:

\[ L_{x_1} \ldots L_{x_{n-2}}(x_{n-1}x_n) = R_{x_{n-1}} \ldots R_{x_3} x_1 \cdot x_n, \quad (3) \]

\[ R_{x_n} \ldots R_{x_3}(x_1x_2) = x_1 \cdot L_{x_2} \ldots L_{x_{n-1}} x_n. \quad (4) \]

In particular, for any division groupoid $G$ satisfying $I_n$, the first formula shows that $L_{x_1} \ldots L_{x_{n-2}} \in AL(G)$, and the second formula that $R_{x_n} \ldots R_{x_3} \in BL(G)$. Since all left and right multiplication maps are surjective, it follows that $G$ is both $AL$-transitive and $BL$-transitive.

We now show that for $a \in G$, the map $L_a$ is injective. To this end, fix $b \in G$ and use surjectivity of the left multiplication maps to select $y_1, \ldots, y_{n-3} \in G$ such that $L_{y_1} \ldots L_{y_{n-3}} L_a b = b$. By the rigidity principle (Lemma 1.1), $L_{y_1} \ldots L_{y_{n-3}} L_a = 1_G$; so $L_a$ has a left inverse and is hence injective. The proof of the injectivity of $R_a$ is similar.

We are now ready to give a new proof of [1, Theorem 4.1]. To prepare, define

\[ \lambda(x_1, \ldots, x_n) = ((x_1x_2) \cdots x_{n-1})x_n, \]

\[ \rho(x_1, \ldots, x_n) = x_1(x_2 \cdots (x_{n-1}x_n)). \]

Then $I_n$ is simply the statement $\lambda(x_1, \ldots, x_n) = \rho(x_1, \ldots, x_n)$. All of the identities in the list below can be proved by direct calculation.

**Lemma 3.2.** The following formulas hold for any $m \geq 1$:

- (HL) $\lambda(x_1, \ldots, x_m, y) = \lambda(x_1, \ldots, x_m)y$,
- (HR) $\rho(y, x_1, \ldots, x_m) = y\rho(x_1, \ldots, x_m)$,
- (CL) $\lambda(\lambda(x_1, \ldots, x_\ell), x_{\ell+1}, \ldots, x_m) = \lambda(x_1, \ldots, x_m)$,
- (CR) $\rho(x_1, \ldots, x_\ell, \rho(x_{\ell+1}, \ldots, x_m)) = \rho(x_1, \ldots, x_m)$,
- (DL) $\lambda(yx_1, x_2, \ldots, x_m) = \lambda(y, x_1, x_2, \ldots, x_m)$,
- (DR) $\rho(x_1, \ldots, x_{m-1}, x_my) = \rho(x_1, \ldots, x_{m-1}, x_m, y)$.

**Theorem 3.3.** A quasigroup satisfying $I_n$ is a group.

**Proof.** We will argue that when $n \geq 4$, $I_n$ implies $I_{n-1}$, and then apply induction. The designation at the end of each line shows which statement from Lemma 3.2 was used to deduce it from the previous line.
\[ \begin{align*}
& y(\lambda(x_1, \ldots, x_n-1)\rho(z_1, \ldots, z_{n-2})) \\
& = y(\lambda(x_1, \ldots, x_n-1, \rho(z_1, \ldots, z_{n-2})) \quad (HL) \\
& = y(\rho(x_1, \ldots, x_n-1, \rho(z_1, \ldots, z_{n-2})) \quad (L_n) \\
& = \rho(y, x_1, \ldots, x_{n-1}, \rho(z_1, \ldots, z_{n-2})) \quad (HR) \\
& = \rho(y, x_1, \ldots, x_{n-2}, x_{n-1}, z_1, \ldots, z_{n-2}) \quad (CR) \\
& = \rho(y, x_1, \ldots, x_{n-2}, \rho(x_{n-1}, z_1, \ldots, z_{n-2})) \quad (CR) \\
& = \lambda(y, x_1, \ldots, x_{n-2}, \rho(x_{n-1}, z_1, \ldots, z_{n-2})) \quad (L_n) \\
& = \rho(\lambda(y, x_1, \ldots, x_{n-2}), x_{n-1}, z_1, \ldots, z_{n-2}) \quad (HR) \\
& = \lambda(\lambda(y, x_1, \ldots, x_{n-2}), x_{n-1}, z_1, \ldots, z_{n-2}) \quad (R_n) \\
& = \lambda(y, x_1, \ldots, x_{n-1}, z_1, \ldots, z_{n-2}) \quad (CL) \\
& = \lambda(y, x_1, \ldots, x_{n-1}, z_1, \ldots, z_{n-2}) \quad (CL) \\
& = \lambda(y, \rho(x_1, \ldots, x_{n-1}), z_1, \ldots, z_{n-2}) \quad (HR) \\
& = \lambda(y, \rho(x_1, \ldots, x_{n-1}), z_1, \ldots, z_{n-2}) \quad (DR) \\
& = \rho(y, \rho(x_1, \ldots, x_{n-1}), z_1, \ldots, z_{n-2}) \quad (L_n) \\
& = \rho(y, \rho(x_1, \ldots, x_{n-1}), z_1, \ldots, z_{n-2}) \quad (HR) \\
& = \rho(y, \rho(x_1, \ldots, x_{n-1}), z_1, \ldots, z_{n-2}) \quad (HR). 
\end{align*} \]

Now cancel \( y \) from the left, and then cancel \( \rho(z_1, \ldots, z_{n-2}) \) from the right to obtain \( \lambda(x_1, \ldots, x_{n-1}) = \rho(x_1, \ldots, x_{n-1}) \), which is \( L_{n-1} \).

\[ \square \]

References
