Quasigroups and Related Systems **24** (2016), 1 – 6

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 $R_{x_1}L_{x_2}\dots R_{x_{2n-1}}L_{x_{2n}}y = L_{x_{2n}}R_{x_{2n-1}}\dots L_{x_2}R_{x_1}y$ 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 $x_1(x_2(\dots x_{n-1}x_n)\dots)) = ((\dots(x_1x_2)\dots)x_{n-1})x_n$ 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 quaisgroups, 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

$$\mathcal{I}_n : x_1(x_2(\dots(x_{n-1}x_n)\dots)) = ((\dots(x_1x_2)\dots)x_{n-1})x_n$$

is in fact a group. While it is clear that $\mathcal{I}_n$ 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 $R_zL_xy = L_xR_zy$, it is perhaps natural to consider the following family of linear groupoid identities:

$$\mathcal{J}_n : R_{x_1}L_{x_2}\dots R_{x_{2n-1}}L_{x_{2n}}y = L_{x_{2n}}R_{x_{2n-1}}\dots L_{x_2}R_{x_1}y$$

2010 Mathematics Subject Classification: 20N05
Keywords: quasigroup, identity, associativity, generalized associativity.

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 $n \geqslant 2$, then a division groupoid satisfies $\mathcal{J}_n$ 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 Niemenmäa-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 $I_4 \Longrightarrow I_3$; 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

$$\begin{aligned} f(z) &= f(h(a)) = f(h(cd)) = f(ck(d)) = g(c)k(d) = h(g(c)d) = h(f(cd)) \\ &= hf(a) = hf'(a) = hf'(cd) = h(g'(c)d) = g'(c)k(d) = f'(ck(d)) \\ &= f'(h(cd)) = f'(h(a)) = f'(z). \end{aligned}$$

The proof of the second statement is similar. □

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 $xy = A(x) * c * B(y)$ 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

$$\mathcal{J}_n : R_{x_1} L_{x_2} \dots R_{x_{2n-1}} L_{x_{2n}} y = L_{x_{2n}} R_{x_{2n-1}} \dots L_{x_2} R_{x_1} y$$

as another generalization of the associative law. We may rewrite $\mathcal{J}_n$ in two different ways:

$$L_{x_2} \dots R_{x_{2n-1}} L_{x_{2n}} y \cdot x_1 = L_{x_{2n}} R_{x_{2n-1}} \dots L_{x_2}(y x_1), \tag{1}$$

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

These formulas witness that if G is a groupoid in which $\mathcal{J}_n$ is satisfied, then $L_{x_{2n}} R_{x_{2n-1}} \dots L_{x_2} \in AL(G) \cap AR(G)$ and $R_{x_1} L_{x_2} \dots R_{x_{2n-1}} \in BL(G) \cap BR(G)$. 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 $n \geqslant 2$. Then G satisfies $\mathcal{J}_n$ if and only if G is an abelian group.*

Proof. Suppose first that G is a division groupoid satisfying $\mathcal{J}_n$. 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 $c_1, \dots, c_{2n-2}$ such that $L_{c_1} R_{c_2} \dots R_{c_{2n-2}} L_a b = b$. Now $L_{c_1} R_{c_2} \dots R_{c_{2n-2}} L_a \in AL(G)$, so by Lemma 1.1, $L_{c_1} R_{c_2} \dots R_{c_{2n-2}} L_a = 1_G$. 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 $d_1, \dots, d_{2n-1} \in G$ such that $L_{d_1} R_{d_2} \dots L_{d_{2n-1}} a = f(a)$. Because we have $L_{d_1} R_{d_2} \dots L_{d_{2n-1}}$ and f are both members of $AL(G)$, Lemma 1.1 implies that $f = L_{d_1} R_{d_2} \dots L_{d_{2n-1}}$, 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

$$\mathcal{J}_n : R_{x_1} L_{x_2} \dots R_{x_{2n-1}} L_{x_{2n}} y = L_{x_{2n}} R_{x_{2n-1}} \dots L_{x_2} R_{x_1} y$$

implies an identity in $(G,+)$; when this is written out, each of the indeterminates $x_1,\dots,x_n$ occurs in exactly one term on each side, with some automorphism of $(G,+)$ applied to it. For example, in the case $n=2$ we have:

$$A^2x_2+Ac+ABA^2x_4+ABAc+ABABy+ABc+AB^2x_3+c+Bx_1 \\ = Ax_4+c+BA^2x_2+BAc+BABAy+BABc+BAB^2x_1+Bc+B^2x_3.$$

In general, the automorphisms applied to the indeterminates $x_1,\dots,x_{2n}$ on the left are (respectively, in order):

$$B, A^2, (AB)B, (AB)A^2, (AB)^2B, (AB)^2A^2, \dots, (AB)^{n-1}B, (AB)^{n-1}A^2$$

and on the right the automorphisms are:

$$(BA)^{n-1}B^2, (BA)^{n-1}A, \dots, (BA)^2B^2, (BA)^2A, (BA)B^2, (BA)A, B^2, A.$$

For $2\leqslant i\leqslant 2n$, set $x_i=\begin{cases} B^{-1}(c) & \text{if } i \text{ is odd,}\\ A^{-1}c & \text{if } i \text{ is even.}\end{cases}$

Next, set $y=A^{-1}(c)$ and substitute these values into the identity to obtain: $d+Bx_1=(BA)^{n-1}B^2x_1$ for some $d\in G$. Evaluating at $x_1=0$, the fact that B and $(BA)^{n-1}B^2$ are automorphisms of G forces $d=0$, so $Bx_1=(BA)^{n-1}B^2x_1$ and hence $(BA)^{n-1}B=1_G$.

Now for $i\neq 2$, $1\leqslant i\leqslant n$, set $y=(BA)^{-1}(c)$; then, substitute this and the same values for x_i (as above) into the identity to obtain $A^2x_2+d'=(BA)^{n-1}Ax_2$ for some $d'\in G$. Reasoning as before, we have $d'=0$, so $(BA)^{n-1}A^{-1}=1_G$. Thus, $A^{-1}=B$, so $B=(BA)^{n-1}B=1_G$, which in turn implies $A=1_G$.

Therefore, $xy=x+c+y$, and so we compute:

$$(xy)z=(x+c+y)z=(x+c+y)+c+z=x+c+(y+c+z)=x(y+c+z)=x(yz).$$

This shows that the quasigroup G is, in fact, a group. Now that we know that G has a neutral element e, simply set all x_i, $i\neq 1,3$ equal to e in the identity $\mathcal{J}_n$ to obtain $R_{x_1}R_{x_3}=R_{x_3}R_{x_1}$. Applying this equality of functions to e, we have $x_1x_3=x_3x_1$ for all $x_1,x_3\in G$, so G is abelian.

Conversely, if G is an abelian group, then the identities $R_xL_y=L_yR_x$, $R_xR_y=R_yR_x$ and $L_xL_y=L_yL_x$ hold in G. Now all left and right multiplication maps commute with each other, so $\mathcal{J}_n$ must hold. □

3. The Niemenmäa-Kepka Theorem

We conclude by giving a new proof of the main result of [1]. The first part of the proof (Proposition 3.1 below) follows the reasoning of [1, Theorem 4.1].

Proposition 3.1. *Let $n\geqslant 3$. Then a division groupoid satisfying $\mathcal{I}_n$ is a quasigroup.*

Proof. Note that $\mathcal{I}_n$ can be interpreted in two ways:

$$L_{x_1} \dots L_{x_{n-2}}(x_{n-1}x_n) = R_{x_{n-1}} \dots R_{x_3}R_{x_2}x_1 \cdot x_n, \tag{3}$$

$$R_{x_n} \dots R_{x_3}(x_1x_2) = x_1 \cdot L_{x_2} \dots L_{x_{n-1}}x_n. \tag{4}$$

In particular, for any division groupoid G satisfying $\mathcal{I}_n$, the first formula shows that $L_{x_1} \dots L_{x_{n-2}} \in AL(G)$, and the second formula that $R_{x_n} \dots R_{x_3} \in BL(G)$. 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 $y_1, \dots, y_{n-3} \in G$ such that $L_{y_1} \dots L_{y_{n-3}}L_ab = b$. By the rigidity principle (Lemma 1.1), $L_{y_1} \dots L_{y_{n-3}}L_a = 1_G$; 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

$$\lambda(x_1, \dots, x_n) = ((x_1x_2) \cdots x_{n-1})x_n,$$

$$\rho(x_1, \dots, x_n) = x_1(x_2 \cdots (x_{n-1}x_n)).$$

Then $\mathcal{I}_n$ is simply the statement $\lambda(x_1, \dots, x_n) = \rho(x_1, \dots, x_n)$. All of the identities in the list below can be proved by direct calculation.

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

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

Theorem 3.3. *A quasigroup satisfying $\mathcal{I}_n$ is a group.*

Proof. We will argue that when $n \geqslant 4$, $\mathcal{I}_n$ implies $\mathcal{I}_{n-1}$, 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.

$$
\begin{aligned}
&y(\lambda(x_1,\dots,x_{n-1})\rho(z_1,\dots,z_{n-2}))\\
&\qquad = y(\lambda(x_1,\dots,x_{n-1},\rho(z_1,\dots,z_{n-2}))) && (HL)\\
&\qquad = y(\rho(x_1,\dots,x_{n-1},\rho(z_1,\dots,z_{n-2}))) && (\mathcal{I}_n)\\
&\qquad = \rho(y,x_1,\dots,x_{n-1},\rho(z_1,\dots,z_{n-2}))) && (HR)\\
&\qquad = \rho(y,x_1,\dots,x_{n-2},x_{n-1},z_1,\dots,z_{n-2}) && (CR)\\
&\qquad = \rho(y,x_1,\dots,x_{n-2},\rho(x_{n-1},z_1,\dots,z_{n-2})) && (CR)\\
&\qquad = \lambda(y,x_1,\dots,x_{n-2},\rho(x_{n-1},z_1,\dots,z_{n-2})) && (\mathcal{I}_n)\\
&\qquad = \lambda(y,x_1,\dots,x_{n-2})\rho(x_{n-1},z_1,\dots,z_{n-2}) && (HL)\\
&\qquad = \rho(\lambda(y,x_1,\dots,x_{n-2}),x_{n-1},z_1,\dots,z_{n-2}) && (HR)\\
&\qquad = \lambda(\lambda(y,x_1,\dots,x_{n-2}),x_{n-1},z_1,\dots,z_{n-2}) && (\mathcal{I}_n)\\
&\qquad = \lambda(y,x_1,\dots,x_{n-1},z_1,\dots,z_{n-2}) && (CL)\\
&\qquad = \lambda(\lambda(y,x_1,\dots,x_{n-1}),z_1,\dots,z_{n-2}) && (CL)\\
&\qquad = \lambda(\rho(y,x_1,\dots,x_{n-1}),z_1,\dots,z_{n-2}) && (\mathcal{I}_n)\\
&\qquad = \lambda(y\rho(x_1,\dots,x_{n-1}),z_1,\dots,z_{n-2}) && (HR)\\
&\qquad = \lambda(y,\rho(x_1,\dots,x_{n-1}),z_1,\dots,z_{n-2}) && (DR)\\
&\qquad = \rho(y,\rho(x_1,\dots,x_{n-1}),z_1,\dots,z_{n-2}) && (\mathcal{I}_n)\\
&\qquad = y\rho(\rho(x_1,\dots,x_{n-1}),z_1,\dots,z_{n-2}) && (HR)\\
&\qquad = y(\rho(x_1,\dots,x_{n-1})\rho(z_1,\dots,z_{n-2})) && (HR).
\end{aligned}
$$

Now cancel y from the left, and then cancel $\rho(z_1,\dots,z_{n-2})$ from the right to obtain $\lambda(x_1,\dots,x_{n-1}) = \rho(x_1,\dots,x_{n-1})$, which is $\mathcal{I}_{n-1}$. □

References

[1] **M. Niemenmäa and T. Kepka**, *On a general associativity law in groupoids*, Monatshefte für Math. **113** (1992), 51 – 57.

[2] **H. Plugfelder**, *Quasigroups and loops: Introduction*, Sigma Series in Pure Mathematics **7**, 1990.

Received December 11, 2014
Revised February 15, 2016

Department of Mathematics, Miami University, Oxford, OH 45056, USA
E-mail: akhtarr@miamioh.edu