PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 2, October 1993

A NOTE ON MEDIAL DIVISION GROUPOIDS

J. JEŽEK AND T. KEPKA

(Communicated by Maurice Auslander)

ABSTRACT. In 1949 Sholander showed that every medial cancellation groupoid can be embedded into a medial quasigroup. In this note we prove the dual assertion that every medial division groupoid is a homomorphic image of a medial quasigroup.

1. INTRODUCTION

By a groupoid we mean a nonempty set with one binary operation, for which we use the multiplicative notation as a default. A groupoid is called *medial* (in some papers *entropic*, in [4] *alternation*) if it satisfies the identity

$$(xy)(uv) = (xu)(yv).$$

While [2] can serve as a reference on the theory of medial groupoids, the book [3] gives numerous examples and connections with other parts of mathematics.

Given a groupoid G and an element $a \in G$, the *left translation* L_a of G is the mapping of G into itself defined by $L_a(x) = ax$ for any $x \in G$. Similarly, the right translation R_a is defined by $R_a(x) = xa$. We say that G is a *cancellation* groupoid if all its translations are injective mappings. If all the translations are surjective, G is a *division* groupoid. A *quasigroup* is a cancellation and division groupoid.

As it is easy to see, a homomorphic image of a division groupoid is a division groupoid. In particular, a homomorphic image of a medial quasigroup is a medial division groupoid. The aim of this paper is to prove that each medial division groupoid can be obtained as a homomorphic image of a medial quasigroup.

Our proof will be based on an auxiliary construction given in §2 which is, in fact, a two-dimensional version of the ergodic-theoretic construction of an automorphism on a measure space naturally extending an endomorphism (see [1, Chapter 10, §4] for the entropic theory of dynamical systems).

Let us remark that, according to [2, Proposition 6.4.1], finitely generated medial division groupoids are already quasigroups.

For a groupoid G we define a binary relation t_G on G by $(a, b) \in t_G$ iff $L_a = L_b$ and $R_a = R_b$. Clearly, t_G is a congruence of G.

Received by the editors July 17, 1991 and, in revised form, March 5, 1992.
1991 *Mathematics Subject Classification*. Primary 20N05, 08A05.
Key words and phrases. Medial groupoid, quasigroup, division.

A groupoid G is said to be *regular* if for any $a, b, c \in G$, $ac = bc$ implies $L_a = L_b$ and $ca = cb$ implies $R_a = R_b$. Clearly, every cancellation groupoid is regular. Both the class of cancellation groupoids and the class of regular groupoids are quasivarieties.

From [2] we shall need the following two results.

Lemma 1. *Let G be a medial division groupoid. Then the factor G/t_G is regular.*

Proof. See [2, Lemma 6.2.3]. □

Lemma 2. *Let G be a regular medial division groupoid. Then there exist an abelian group $G(+)$, two commuting surjective endomorphisms f, g of $G(+)$, and an element $q \in G$ such that*

$$xy = f(x) + g(y) + q$$

for all $x, y \in G$.

Proof. See [2, Corollary 6.1.2]. □

2. Bi-unary algebras: an auxiliary construction

Lemma 3. *Let S be a nonempty set and f, g be two commuting surjective transformations of S. Then there are a set A, two commuting permutations F, G of A, and a mapping φ of A onto S such that $\varphi F = f\varphi$ and $\varphi G = g\varphi$.*

Proof. Let N denote the set of positive integers. Denote by A the set of the mappings $a : N \times N \to S$ such that

$$f(a(i+1, j)) = g(a(i, j+1)) = a(i, j)$$

for all $i, j \in N$. (It is possible to imagine the elements of A as being infinite matrices over the set S.) For $a \in A$ define elements $F(a)$ and $G(a)$ of A by

$$F(a)(i, j) = f(a(i, j)), \qquad G(a)(i, j) = g(a(i, j)).$$

With respect to $fg = gf$, it is easy to check that both $F(a)$ and $G(a)$ belong to A for any $a \in A$. The mappings F, G commute, as

$$FG(a)(i, j) = fg(a(i, j)) = gf(a(i, j)) = GF(a)(i, j).$$

We are going to show that F is a permutation of A. If $a, b \in A$ are elements such that $F(a) = F(b)$, then for all $i, j \in N$ we have

$$\begin{aligned} a(i, j) &= f(a(i+1, j)) = F(a)(i+1, j) \\ &= F(b)(i+1, j) = f(b(i+1, j)) = b(i, j) \end{aligned}$$

and consequently $a = b$. Given an element $c \in A$, we can define d by $d(i, j) = c(i+1, j)$ for all i, j and check that $d \in A$ and $F(d) = c$.

In the same way one can prove that also G is a permutation of A. Define a mapping $\varphi : A \to S$ by $\varphi(a) = a(1, 1)$. For all $a \in A$ we have

$$\varphi F(a) = F(a)(1, 1) = f(a(1, 1)) = f\varphi(a)$$

and thus $\varphi F = f\varphi$. Similarly, $\varphi G = g\varphi$. It remains to show that φ is a mapping onto S.

Let s be an arbitrary element of S. Put $a_{1,1} = s$ and for any $i \geq 2$ choose an element $a_{i,i} \in S$ such that $fg(a_{i,i}) = a_{i-1,i-1}$; this is possible, as fg is surjective. Setting

$$a(i, j) = \begin{cases} g^{i-j}(a_{i,i}) & \text{for } i \geq j, \\ f^{j-i}(a_{j,j}) & \text{for } i < j, \end{cases}$$

we obtain a mapping a of $N \times N$ into S. We only need to prove that $a \in A$, since $\varphi(a) = s$ will then follow from our choice $a_{1,1} = s$. If $i \geq j$, then

$$f(a(i+1, j)) = fg^{i+1-j}(a_{i+1,i+1}) = g^{i-j}(a_{i,i}) = a(i, j).$$

If $j = i + 1$, then

$$f(a(i+1, j)) = f(a_{i+1,i+1}) = f(a_{j,j}) = a(j-1, j) = a(i, j).$$

If $j > i + 1$, then

$$f(a(i+1, j)) = f^{j-i}(a_{j,j}) = a(i, j).$$

We have proved $f(a(i+1, j)) = a(i, j)$ in all cases, and $g(a(i, j+1)) = a(i, j)$ can be checked similarly. □

Remark. Although we shall not use the fact in the following, let us remark that the construction of A, F, G, φ given in the proof of Lemma 3 is universal in the sense that if A_1, F_1, G_1, φ_1 is any other quadruple with the same properties, then there exists a uniquely determined mapping $\psi : A_1 \to A$ such that $\psi F_1 = F\psi$ and $\psi G_1 = G\psi$.

3. Medial division groupoids: the main result

Lemma 4. *Let G be a medial division groupoid. Then G is a homomorphic image of the regular medial division groupoid $G/t_G \times G/t_G$.*

Proof. Let $\varphi : G \to G/t_G$ be the canonical projection. It follows from the definition of t_G that $\psi : G/t_G \times G/t_G \to G$ is a correctly defined mapping if we put $\psi(\varphi(x), \varphi(y)) = xy$ for all $x, y \in G$. By the medial law,

$$\begin{aligned}\psi((\varphi(x), \varphi(y)) \cdot (\varphi(u), \varphi(v))) &= (xu)(yv) = (xy)(uv) \\ &= \psi(\varphi(x), \varphi(y)) \cdot \psi(\varphi(u), \varphi(v))\end{aligned}$$

for any $x, y, u, v \in G$ and we see that ψ is a homomorphism. Since G is a division groupoid, ψ is surjective. The factor G/t_G is a regular medial division groupoid by Lemma 1, and it is clear that the product of regular medial division groupoids is a regular medial division groupoid. □

Theorem 5. *Every medial division groupoid is a homomorphic image of a medial quasigroup.*

Proof. With respect to Lemma 4, it is sufficient to prove that any regular medial division groupoid G is a homomorphic image of a medial quasigroup. By Lemma 2 there are an abelian group $G(+)$, two commuting surjective endomorphisms f, g of $G(+)$, and an element $q \in G$ such that $xy = f(x) + g(y) + q$ for all $x, y \in G$. By Lemma 3 there exist a set A, two commuting permutations F, G of A, and a mapping φ of A onto G such that $\varphi F = f\varphi$ and

$\varphi G = g\varphi$. Denote by $H(+)$ the free abelian group over the set A. The permutations F, G can be uniquely extended to automorphisms α, β of $H(+)$, and we have $\alpha\beta = \beta\alpha$. Moreover, the mapping φ can be extended to a homomorphism h of $H(+)$ onto $G(+)$. Since the homomorphisms $h\alpha$ and fh of $H(+)$ into $G(+)$ coincide on the set of generators A, they coincide everywhere and we have $h\alpha = fh$. Similarly, $h\beta = gh$. Take an element $e \in H$ such that $h(e) = q$ and define a multiplication on H by $xy = \alpha(x) + \beta(y) + e$. Then H becomes a medial quasigroup, and one can easily verify that h is a homomorphism of the quasigroup H onto the groupoid G. $\square$

Remark. For a given medial division groupoid G let Q be a medial quasigroup and r be a congruence of Q such that $G \simeq Q/r$. Among the congruences s of Q such that $s \subseteq r$ and Q/s is a quasigroup, there is a unique largest one; denote it by s_0. Then G is a homomorphic image of the medial quasigroup $Q_0 = Q/s_0$ with the property that no nontrivial congruence of Q_0 contained in the kernel of the homomorphism factors Q_0 to a quasigroup. In this sense, every medial division groupoid has a "quasigroup cover". We do not know, however, if this medial quasigroup cover is unique.

REFERENCES

1. I. P. Cornfeld, S. V. Fomin, and Ya. G. Sinai, *Ergodic theory*, Grundlehren Math. Wiss., vol. 245, Springer-Verlag, New York, 1982.
2. J. Ježek and T. Kepka, *Medial groupoids*, Rozpravy ČSAV, Řada Mat. a Přír. Věd 93/2, Academia, Praha, 1983.
3. A. Romanowska and J. D. H. Smith, *Modal theory—an algebraic approach to order, geometry and convexity*, Helderman Verlag, Berlin, 1985.
4. M. Sholander, *On the existence of the inverse operation in alternation groupoids*, Bull. Amer. Math. Soc. **55** (1949), 746–757.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HAWAII 96822
E-mail address: jarda@kahuna.math.hawaii.edu

DEPARTMENT OF MATHEMATICS, CHARLES UNIVERSITY, SOKOLOVSKÁ 83, PRAHA 8, 18600 CZECH REPUBLIC