Paramedial groupoids

Jung R.Cho, Jaroslav Ježek and Tomáš Kepka

By a paramedial groupoid we mean a groupoid satisfying the equation $ax \cdot yb = bx \cdot ya$. This equation is, in certain sense, symmetric to the equation of mediality $xa \cdot by = xb \cdot ay$ and, in fact, the theories of both varieties of groupoids are parallel. The present paper, initiating the study of paramedial groupoids, is meant as a modest contribution to the enormously difficult task of describing algebraic properties of varieties determined by strong linear identities (and, especially, of the corresponding simple algebras).[1]

1. Introduction

Let G be a groupoid (i.e., a non-empty set equipped with a binary operation). For any $x \in G$, we define transformations L_x ($= L_{G,x}$, the left translation by x) and R_x ($= R_{G,x}$, the right translation by x) of G by $L_x(y) = xy$ and $R_x(y) = yx$ for every $y \in G$.

An element x is said to be

- left (right) injective if the left (right) translation $L_x(R_x)$ is an injective transformation of G;
- injective if x is both left and right injective;
- left (right) projective if $L_x(R_x)$ is a projective transformation of G;
- projective if x is both left and right projective;
- left (right) bijective if $L_x(R_x)$ is a bijective transformation (i.e., a permutation) of G;
- bijective if x is both left and right bijective.

We denote by $A_l(G)$ and $B_l(G)$ ($A_r(G)$ and $B_r(G)$) the set of left (right) injective and left (right) projective elements, resp., and we put $C_l(G) = A_l(G) \cap B_l(G)$, $C_r(G) = A_r(G) \cap B_r(G)$, $A(G) = A_l(G) \cap A_r(G)$, $B(G) = B_l(G) \cap B_r(G)$ and $C(G) = C_l(G) \cap C_r(G)$.

The groupoid G is said to be

- left (right) cancellative if $A_l(G) = G$ ($A_r(G) = G$);
- left (right) divisible if $B_l(G) = G$ ($B_r(G) = G$);
- cancellative (divisible) if G is both left and right cancellative (divisible);
- a left (right) quasigroup if $C_l(G) = G$ ($C_r(G) = G$);
- a quasigroup if G is both left and right quasigroup;
- left (right) regular if, for all $a, b, c, d \in G$, $ca = cb$ ($ac = bc$) implies $da = db$ ($ad = bd$);
- regular if G is both left and right regular.

For every groupoid G, we define a transformation o_G of G by $o_G(x) = xx$ ($= x^2$), $x \in G$.

[1]While working on this paper, the first author was supported by Korea Science Foundation and the last two authors were partially supported by the Grant Agency of the Czech Republic, Grant No 201/96/0312

Let H be a subgroupoid of a groupoid G. We denote by $Mul(G,H)$ the transformation semigroup (acting on G) generated by all $L_{G,x}$ and $R_{G,x}$, $x \in H$. The semigroup $Mul(G) = Mul(G,G)$ is called the multiplication semigroup of G.

Let G, H be groupoids. A mapping $f : G \to H$ is said to be an antihomomorphism if $f(xy) = f(y)f(x)$ for all $x, y, \in G$; this is equivalent to the fact that f is a homomorphism of G into the opposite groupoid H^{op} (and consequently $ker(f)$ is a congruence of G).

A groupoid G possesses at least one antiautomorphism f iff G and G^{op} are isomorphic; then f^2 is an automorphism of G and $f(xf(x)) = f^2(x)f(x)$, $x \in G$. If, moreover, $f^2 = id_G$, then $f(xf(x)) = xf(x)$.

A groupoid G is said to be

- a Z-semigroup if $xy = uv$ for all $x, y, u, v \in G$;
- a LZ-semigroup if $xy = x$ for all $x, y = G$;
- a RZ-semigroup if $xy = y$ for all $x, y = G$;
- a band if G is an idempotent semigroup;
- a rectangular band if G is a band and $xyx = x$ for all $x, y \in G$;
- unipotent if $xx = yy$ for all $x, y = G$
- zeropotent if $xx \cdot y = y \cdot xx = xx$ for all $x, y \in G$;
- left (right) permutable if $x \cdot yz = y \cdot xz$ ($zy \cdot x = zx \cdot y$) for all $x, y, z \in G$;
- left (right) modular if $x \cdot yz = z \cdot yx$ ($zy \cdot x = xy \cdot z$) for all $x, y, z \in G$;
- medial if $xa \cdot by = xb \cdot ay$ for all $a, b, x, y \in G$;
- paramedial if $ax \cdot yb = bx \cdot ya$ for all $a, b, x, y \in G$;
- entropic (extropic) if G is a homomorphic image of a cancellative medial (paramedial) groupoid.

If G is a rectangular band, then $xyz = xzx \cdot yz = x \cdot zxyz = xz$ for all $x, y, z \in G$.

G is unipotent iff $ker(o_G) = G \times G$; in that case, G contains a unique idempotent element 0 and $0 = xx$ for every $x \in G$.

G is zeropotent iff G is unipotent and $0x = 0 = x0$ for every $x \in G$ (i.e., 0 is an absorbing element).

1.1 Lemma.

(i) Every left (right) modular groupoid is medial.

(ii) Every left (right) permutable right (left) modular groupoid is paramedial.

Proof. (i) $xa \cdot by = y(b \cdot xa) = y(a \cdot xb) = xb \cdot ay$.

(ii) $ax \cdot yb = y(ax \cdot b) = y(bx \cdot a) = bx \cdot ya$.

1.2 Lemma. Let G be a paramedial groupoid possessing a left (right) neutral element e. Then G is left (right) permutable and right (left) modular. Moreover, if e is a neutral element, then G is a commutative semigroup.

Proof. If e is left neutral, then $ax \cdot b = ax \cdot eb = bx \cdot ea = bx \cdot a$ and $x \cdot yb = ex \cdot yb = ey \cdot xb = y \cdot xb$ (we have used the fact that G is medial by 1.1(i)). If e is neutral, then $ab = ae \cdot eb = be \cdot ea = ba$.

1.3 Lemma. Let G be unipotent and left (right) cancellative. Then G is paramedial if and only if G is medial.

Proof. If G is paramedial, then $(xa \cdot by)(xb \cdot ay) = (ay \cdot by)(xb \cdot xa) = (yy \cdot ba)(ab \cdot xx) = (0 \cdot ba)(ab \cdot 0) = (0 \cdot ba)(ab \cdot bb) = (0 \cdot ba)(bb \cdot ba) = (0 \cdot ba)(0 \cdot ba) = 0 = (xa \cdot by)(xa \cdot by)$. If G is medial, then $(ax \cdot yb)(bx \cdot ya) = (ax \cdot bx)(yb \cdot ya) = (ab \cdot xx)(yy \cdot ba) = (ab \cdot 0)(0 \cdot ba) = (ab \cdot 0)(aa \cdot ba) = (ab \cdot 0)(ab \cdot aa) = (ab \cdot 0)(ab \cdot 0) = 0 = (ax \cdot yb)(ax \cdot yb)$.

1.4 Lemma. Every idempotent paramedial groupoid is commutative.

Proof. $xy = xy \cdot xy = yy \cdot xx = yx$.

1.5 Corollary. A paramedial groupoid G is medial, provided that at least one of the following conditions is satisfied:

(1) G possesses a left (right) neutral element.
(2) G is unipotent and left (right) cancellative.
(3) G is idempotent.
(4) G is commutative.

2. Basic properties of paramedial groupoids

2.1 Lemma. Let G be a paramedial groupoid. Then:

(i) o_G is an antiendomorphism of G.
(ii) $o_G(G)$ is a subgroupoid of G.
(iii) $ker(o_G)$ is a congruence of G.

2.2 Proposition. Let G be a paramedial groupoid with o_G injective. Then G is a subgroupoid of a paramedial groupoid Q satisfying the following properties:

(1) Q is the union of a chain $Q_0 \subseteq Q_1 \subseteq Q_2 \subseteq \dots$ of subgroupoids such that $Q_0 = G$, $Q_i \cong G$ and $o^2(Q_i) = Q_{i-1}$ for every $i \geq 1$.
(2) o_Q is an antiautomorphism of Q.
(3) G and Q satisfy the same groupoid equations.
(4) Q is (left, right) cancellative (or regular) iff G is so.
(5) If G is simple, then Q is so.

Proof. Put $H = o^2(G)$ and $f = o^2$. Then H is a subgroupoid of G and f can be viewed as an isomorphism of G onto H. Now, it is clear that there exist a groupoid Q_1 and an isomorphism $g : Q_1 \to G$ such that G is a subgroupoid of Q_1, $g|G = f$ and $G = o^2(Q_1)$. The rest of the proof is clear.

2.3 Example. Let $G(*)$ be a medial groupoid with two antiendomorphisms f and g such that $f^2 = g^2$ and let $w \in G$. Define a multiplication on G by $xy = (f(x) * g(y)) * w$. Then G becomes a paramedial groupoid. (The same remains true if we have defined $xy = w * (f(x) * g(y))$ or $xy = f(x) * g(y)$.)

2.4 Proposition. The following conditions are equivalent for a groupoid G:

(i) G is paramedial and o_G is a permutation.
(ii) There exist an idempotent medial groupoid $G(*)$ and an antiautomorphism f of $G(*)$ such that $xy = f(x) * f(y)$ $(= f(y * x))$ for all $x, y \in G$.

Proof. (i) implies (ii). It is sufficient to put $f = o_G$ and $x * y = f^{-1}(yx)$ for all $x, y \in G$. (ii) implies (i). See 2.3.

2.5 Remark. Consider the situation from 2.4. Let r be a congruence of G. If $(a, b) \in r$, then $(f(a), f(b)) = (aa, bb) \in r$ and $(x * f(a), x * f(b)) = (f^{-1}(x)a, f^{-1}(x)b) \in r$, $(f(a) * x, f(b) * x) \in r$ for every $x \in G$. Now, if r is invariant under f^{-1} (e.g., if G is finite or, more generally, if the order of $f = o_G$ is finite), then r is a congruence of $G(*)$.

Conversely, let r be a congruence of $G(*)$ such that r is invariant under f^{-1}. Then r is also a congruence of G.

2.6 Lemma. Let G be paramedial and $e \in Id(G)$. Then:

(i) $L_e^2 = R_e^2$ is an endomorphism of G.
(ii) L_e is injective (projective, bijective) iff R_e is so.
(iii) $L_e(xy) = R_e(y)R_e(x)$ and $R_e(xy) = L_e(y)L_e(x)$ for all $x, y \in G$.

2.7 Proposition. Let G be a paramedial groupoid and $e \in Id(G) \cap A_l(G)$ ($e \in Id(G) \cap A_r(G)$). Then G is a subgroupoid of a paramedial groupoid Q satisfying the following properties:

(1) Q is the union of a chain $Q_0 \subseteq Q_1 \subseteq Q_2 \subseteq \dots$ of subgroupoids such that $Q_0 = G$, $Q_i \cong G$ and $L_e^2(Q_i) = Q_{i-1}$ ($R_e^2(Q_i) = Q_{i-1}$) for every $i \geq 1$.
(2) Both $L_{Q,e}$ and $R_{Q,e}$ are permutations of Q and $L_{Q,e}^2 = R_{Q,e}^2$ is an automorphism of Q.
(3) G and Q satisfy the same groupoid equations.
(4) Q is (left, right) cancellative (or regular) iff G is so.
(5) If G is simple, then Q is so.

Proof. Using 2.6, we can proceed similarly as in the proof of 2.2.

2.8 Proposition. The following conditions are equivalent for a groupoid G.

(i) G is paramedial and $Id(G) \cap C_l(G) \neq \varnothing$.
(ii) G is paramedial and $Id(G) \cap C_r(G) \neq \varnothing$.
(iii) G is paramedial and $Id(G) \cap C(G) \neq \varnothing$.
(iv) There exist a commutative semigroup $G(+)$ with a neutral element and automorpisms f, g of $G(+)$ such that $f^2 = g^2$ and $xy = f(x) + g(y)$ for all $x, y \in G$.

Moreover, if these (equivalent) conditions are satisfied and G is unipotent, then $G(+)$ is an abelian group and G is a quasigroup.

Proof. The first three conditions are equivalent by 2.6(ii). Now, let $e \in Id(G) \cap C(G)$, $f = R_e$, $g = L_e$, and let $x + y = f^{-1}(x)g^{-1}(y)$. Then e is a neutral element of $G(+)$ and $xy = f(x) + g(y)$. Further, it is easy to check directly that $G(+)$ is medial, and hence $G(+)$ is a commutative semigroup. Of course, $f(x + y) = f(f^{-1}(x)g^{-1}(y)) = ygf^{-1}(x) = f^{-1}f(y)g^{-1}g^2f^{-1}(x) = f^{-1}f(y)g^{-1}f(x) = f(y) + f(x) = f(x) + f(y)$. Quite similarly, g is an automorphism of $G(+)$.

Finally, if G is unipotent, then $e = f^{-1}(x)f^{-1}(x) = x + gf^{-1}(x)$ and we conclude that $G(+)$ is a group.

2.9 Proposition. Let G be a unipotent paramedial groupoid ($\{0\} = Id(G) = o_G(G)$). Then:

(i) $L_0R_0 = R_0L_0$ is an endomorphism of G.
(ii) If L_0 (R_0) is injective, then G is a medial cancellative groupoid.

Proof. (i) $0 \cdot x0 = xx \cdot x0 = 0x \cdot xx = 0x \cdot 0$, $0(xy \cdot 0) = 0(xy \cdot 00) = 0(0y \cdot 0x) = (00)(0y \cdot 0x) = (0x \cdot 0)(0y \cdot 0) = (0 \cdot x0)(0 \cdot y0)$.

(ii) By 2.6(ii), both L_0 and R_0 are injective. If $ab = ac$, then $b0 \cdot 0 = b0 \cdot aa = a0 \cdot ab = a0 \cdot ac = c0 \cdot aa = c0 \cdot 0$, and hence $b = c$. Similarly, G is right cancellative and, finally, G is medial by 1.3.

3. Injective and projective elements in paramedial groupoids

3.1 Lemma. Let G be a paramedial groupoid and $a, b, x, y \in G$. Then:

(i) $L_{ax}L_y = R_{ya}R_x$.
(ii) $L_{ax}R_b = L_{bx}R_a$.
(iii) $R_{yb}L_a = R_{ya}L_b$.

3.2 Proposition. The following conditions are equivalent for a paramedial groupoid G.

(i) G is left cancellative (left divisible).

(ii) G is right cancellative (right divisible).
(iii) G is cancellative (divisible).

Proof. Use 3.1(i) (notice that $G = GG$ in the divisible case).

3.3 Corollary. The following conditions are equivalent for a paramedial groupoid G:

(i) G is a left quasigroup.
(ii) G is a right quasigroup.
(iii) G is a quasigroup.

3.4 Lemma. Let G be a paramedial groupoid and $a, b \in G$.

(i) If $ab \in A_l(G)$, then $a, b \in A_r(G)$.
(ii) If $ab \in A_r(G)$, then $a, b \in A_l(G)$.
(iii) If $ab \in A(G)$, then $a, b \in A(G)$.

Proof. The transformation $L_{ab}L_{ab} = R_{ab\cdot a}R_b$ (3.1(i)) is injective, and hence R_b is injective. Further, $L_{ab}R_b = L_{bb}R_a$ (3.1(ii)) is injective, and hence R_a is so.

3.5 Proposition. Let G be a divisible paramedial groupoid such that $A_l(G) \neq \varnothing$ ($A_r(G) \neq \varnothing$). Then G is a quasigroup.

Proof. If $a \in G$ and $c \in A_l(G)$, then $c = ab$ and we have $a \in A_r(G)$ by 3.4(i). It follows that G is right cancellative, and hence a quasigroup by 3.2.

3.6 Remark. Let G be a paramedial groupoid.

(i) If G is not cancellative, then $I = G - A(G)$ is non-empty and it follows from 3.4 that I is an ideal of G. In particular, if G is ideal-simple, then either $I = G$ (and $A(G) = \varnothing$) or $I = \{0\}$, where 0 is an absorbing element (and then $A(G)$ is a subgroupoid of G).

(ii) If $A_l(G) \neq \varnothing = A_r(G)$, then $A_l(G) \subseteq G - GG$. In particular, $G \neq GG$ and G is infinite.

3.7 Lemma. Let G be a paramedial groupoid and $a, b, c \in G$.

(i) If $ab, c \in B_l(G)$, then $ca \in B_r(G)$.
(ii) If $ab, c \in B_r(G)$, then $bc \in B_l(G)$.
(iii) If $ab \in B_l(G)$ and $c \in B_r(G)$, then $cb \in B_l(G)$.
(iv) If $ab \in B_r(G)$ and $c \in B_l(G)$, then $ac \in B_r(G)$.

Proof. Use 3.1.

3.8 Lemma. Let G be a paramedial groupoid. Then:

(i) $B_l(G)B_l(G) \subseteq B_r(G)$ and $B_r(G)B_r(G) \subseteq B_l(G)$.
(ii) $B_l(G)B_r(G) \subseteq B(G)$ and $B_r(G)B_l(G) \subseteq B(G)$.

Proof. (i) If $a, b \in B_l(G)$, then $b = be$ for some $e \in G$ and we have $ab \in B_r(G)$ by 3.7(i).

(ii) Let $a \in B_l(G)$ and $b \in B_r(G)$. By (i), $aa \in B_r(G)$, $bb \in B_l(G)$, and hence, given $x \in G$, there are $y, z, u, v \in G$ such that $y \cdot aa = x = bb \cdot z$ and $y = ub$, $z = av$. Now, $x = y \cdot aa = ub \cdot aa = ab \cdot au$ and $x = bb \cdot z = bb \cdot av = vb \cdot ab$. We have proved that $ab \in B(G)$.

3.9 Proposition. Let G be a paramedial groupoid.

(i) If $B_l(G) \neq \varnothing$ (or $B_r(G) \neq \varnothing$), then $B(G) \neq \varnothing$.
(ii) $B_l(G) \cup B_r(G)$ is either empty or a subgroupoid of G.
(iii) $B(G)$ is either empty or a subgroupoid of G.

Proof. Use 3.8.

3.10 Lemma. Let G be a paramedial groupoid and $a, b, c, d, e \in G$.

(i) If $a \in B_l(G)$ and $be = b \in A_l(G)$, then $ab \in A_r(G)$.
(ii) If $bc = ae = a \in A_l(G)$ and $e = ad$, then $ab \in A_r(G)$.
(iii) $B_l(G)C_l(G) \subseteq C_r(G)$ and $C_l(G)B_l(G) \subseteq C_r(G)$.
(iv) If $b \in B_r(G)$ and $ea = a \in A_r(G)$, then $ab \in A_l(G)$.
(v) If $ca = eb = b \in A_r(G)$ and $e = db$, then $ab \in A_l(G)$.
(vi) $C_r(G)B_r(G) \subseteq C_l(G)$ and $B_r(G)C_r(G) \subseteq C_l(G)$.

Proof. (i) Let $ac = e$ and $x \cdot ab = y \cdot ab$. Then $b \cdot bx = be \cdot bx = (be \cdot ac)(bx) = (ce \cdot ab)(bx) = (x \cdot ab)(b \cdot ce) = (y \cdot ab)(b \cdot ce) = (ce \cdot ab)(by) = (be \cdot ac)(by) = b \cdot by$, and hence $x = y$.

(ii) If $x \cdot ab = y \cdot ab$, then $a \cdot ax = ae \cdot ax = (bc \cdot ad)(ax) = (dc \cdot ab)(ax) = (x \cdot ab)(a \cdot dc) = (y \cdot ab)(a \cdot dc) = a \cdot ay$, so that $x = y$.

(iii) Combine (i), (ii) and 3.8(i).

3.11 Lemma. Let G be a paramedial groupoid and $a, b \in G$.

(i) If $ab \in B_r(G)$ and $b \in C_r(G)$, then $a \in B_l(G)$.
(ii) If $ab \in B_l(G)$ and $a \in C_l(G)$, then $b \in B_r(G)$.
(iii) If $ab \in B_l(G)$ and $b \in C_r(G)$, then $a \in B_r(G)$.
(iv) If $ab \in B_r(G)$ and $a \in C_l(G)$, then $b \in B_l(G)$.

Proof. (i) By 3.10(vi), $bb \in C_l(G)$. Now, given $x \in G$, there are $y, z \in G$ such that $z \cdot ab = bb \cdot x$ and $yb = z$. We have $bb \cdot ay = yb \cdot ab = z \cdot ab = bb \cdot x$ and $ay = x$.

(iii) By 3.10(vi), $bb \in C_l(G)$. Now, given $x \in G$, there are $y, z \in G$ such that $bb \cdot x = ab \cdot y$ and $y = zb$. We have $bb \cdot x = ab \cdot y = ab \cdot zb = bb \cdot za$ and $za = x$.

3.12 Theorem. Let G be a paramedial groupoid. Then:

(i) $C_l(G) = C_r(G) = C(G)$.
(ii) $C(G)$ is either empty or a subgroupoid of G.

Proof. (i) If $b \in C_r(G)$, then $b = ab$, $a \in G$, and we have $a \in C_l(G)$ by 3.4(ii) and 3.11(i). Further, $b \in A_l(G)$ by 3.4(ii) and $b \in B_l(G)$ by 3.11(iv). Consequently, $b \in C_l(G)$ and we have proved that $C_l(G) \subseteq C_r(G)$.

(ii) By (i) and 3.10(iii), $C(G)$ (if non-empty) is a subgroupoid of G.

4. Multiplication semigroups of paramedial groupoids

4.1 Lemma. Let H be a subgroupoid of a paramedial groupoid G. For every $f \in Mul(G, H)$ there exists $g \in Mul(G, H)$ such that at least one of the following two conditions is satisfied:

(1) $gL_{G,x} = L_{G,f(x)}f$ and $gR_{G,x} = R_{G,f(x)}f$ for every $x \in G$.
(2) $gL_{G,x} = R_{G,f(x)}f$ and $gR_{G,x} = L_{G,f(x)}f$ for every $x \in G$.

Proof. We have $f = S_{1,a_1} \dots S_{n,a_n}$, $n \geq 1$, $a_i \in H$ and $S_i \in \{L, R\}$. Put $g = \overline{S}_{1,b_1} \dots \overline{S}_{n,b_n}$, where $b_i = a_i^2$ and $\overline{L} = R$, $\overline{R} = L$. Then $g \in Mul(G, H)$ and (1) is true for n even and (2) for n odd.

4.2 Proposition. Let H be a subgroupoid of a paramedial groupoid G. Then the semigroup $Mul(G, H)$ is left uniform.

Proof. We have to show that the intersection of any two left ideals of $M = Mul(G, H)$ is non-empty. For, let $f_1, f_2 \in M$, $f_1 = S_{1,a_1} \dots S_{n,a_n}$, $n \geq 1$, $a_i \in H$, $S_i \in \{L, R\}$. Now, using 4.1 and induction, we can find $g_n, \dots, g_1 \in M$ and $h_n, \dots, h_1 \in M$ such that

$$g_n S_{n,a_n} = h_n f_2,$$

$$g_{n-1}S_{n-1,a_{n-1}} = h_{n-1}g_n,$$

$$\vdots$$

$$g_2S_{2,a_2} = h_2g_3$$

$$g_1S_{1,a_1} = h_1g_2.$$

Then $g_1f_1 = g_1S_{1,a_1}\dots S_{n,a_n} = h_1g_2S_{2,a_2}\dots S_{n,a_n} = h_1h_2g_3S_{3,a_3}\dots S_{n,a_n} = \dots = h_1h_2\dots h_{n-1}g_nS_{n,a_n} = h_1h_2\dots h_nf_2$.

4.3 Corollary. The multiplication semigroup $Mul(G)$ is left uniform for every paramedial groupoid G.

In the remaining part of this section, let G be a cancellative paramedial groupoid. By 4.3, $Mul(G)$ is left uniform. Further, every transformation from $Mul(G)$ is injective and consequently $Mul(G)$ is left cancellative.

Let M (N) be the set of $f \in Mul(G)$ which can be written in the form $f = S_{1,a_1}\dots S_{n,a_n}$, where n is even (odd). Clearly, we have $Mul(G) = M \cup N$, M is a subsemigroup of $Mul(G), NN \subseteq M, MN \subseteq N$ and $NM \subseteq N$.

4.4 Lemma. Suppose that $G = GG$. If $f, g \in N(f, g \in M)$ and $h \in Mul(G)$ are such that $fh = gh$, then $f = g$.

Proof. Let $h = S_{1,a_1}\dots S_{n,a_n}$. Now, we shall proceed by induction on M.

First, let $n = 1, a_1 = a, S_1 = L$ (the other case, $S_1 = R$, being similar). Further, let $f', g' \in Mul(G)$ be such that $f'(xy) = f(y)f(x)$ and $g'(xy) = g(y)g(x)$ $(f'(xy) = f(x)f(y)$ and $g'(xy) = g(x)g(y))$ for all $x, y \in G$ (see 4.1). Now, $f(aa) = fh(a) = gh(a) = g(aa)$ and $f(aa)f(xy) = f'(xy \cdot aa) = f'(ay \cdot ax) = f(ax)f(ay) = fh(x)fh(y) = gh(x)gh(y) = g(aa)g(xy) = f(aa)g(xy)$, so that $f(xy) = g(xy)$ and, since $G = GG$, we have $f = g$.

Now, let $n \geq 2$ and $k = S_{1,a_1}\dots S_{n-1,a_{n-1}}$. Then either $fk, gk \in N$ or $fk, gk \in M$ and $fkS_{n,a_n} = gkS_{n,a_n}$. According to the preceding part of the proof, we have $fk = gk$, and hence $f = g$ by the induction hypothesis.

4.5 Lemma. If $G = GG$, then M is a left uniform cancellative semigroup.

Proof. M is cancellative by 4.4 and it follows easily from the proof of 4.2 that M is left uniform.

4.6 Corollary. If $G = GG$ and $M = Mul(G)$, then $Mul(G)$ is a left uniform cancellative semigroup.

4.7 Proposition. If $G = GG$ and $M \cap N = \varnothing$, then $Mul(G)$ is a left uniform cancellative semigroup.

Proof. We have to show that $Mul(G)$ is right cancellative. Let $f, g, h \in Mul(G)$ be such that $fh = gh$. With respect to 4.4, we can assume that $f \in M$ and $g \in N$. If $h \in M$, then $fh \in M$, $gh \in N$ and $fh = gh \in M \cap N = \varnothing$, a contradiction. Similarly, if $h \in N$.

4.8 Remark. Let $f \in M \cap N, f = S_{1,a_1}\dots S_{n,a_n} = T_{1,b_1}\dots T_{m,b_m}$, n even and m odd. Put $g = \overline{S}_{1,c_1}\dots\overline{S}_{n,c_n}$ and $h = \overline{T}_{1,d_1}\dots\overline{T}_{m,d_m}$, $c_i = a_i^2$ and $d_i = b_i^2$. Then $g(xy) = f(x)f(y)$ and $h(xy) = f(y)f(x)$ for all $x, y \in G$. Consequently, $hg(xy) = f^2(y)f^2(x) = gh(xy)$ and $g^2(xy) = f^2(x)f^2(y) = h^2(xy)$. In particular, if $G = GG$, then $hg = gh$ and $h^2 = g^2$. Moreover, $g(x^2) = h(x^2)$. Finally, if $o_G(G) = G$, then $g = h$, and hence $g(xy) = g(yx)$ for all $x, y \in G$. Since g is an injective transformation, it follows that the groupoid G is commutative.

4.9 Theorem. Suppose that $o_G(G) = G$. Then:

(i) Either $M \cap N = \varnothing$ or G is commutative.

(ii) $Mul(G)$ is a left uniform cancellative semigroup.

Proof. (i) See 4.8.

(ii) The assertion is proved in 4.7 for $M \cap N = \varnothing$. However, if G is commutative, then we can proceed similarly as in the proof of 4.4.

4.10 Lemma. Let H be a subgroupoid of G and $K = [H]_{G,c} = \{a \in G; f(a) \in H$ for some $f \in Mul(G, H)\}$. Then:

(i) $H \subseteq K$ and K is a subgroupoid of G.

(ii) If $a, b \in G, ab \in K$ and $a \in K(b \in K)$, then $b \in K(a \in K)$.

(iii) If G is a quasigroup, then K is a quasigroup.

Proof. (i) Let $a, b \in K$ and $f, g \in Mul(G, H)$ be such that $f(a), g(b) \in H$. We have $q = hf = kg$ for suitable $h, k \in Mul(G, H), q(a), q(b) \in H$ and we can assume that $q \in M$. Now, $q'(ab) = q(a)q(b) \in H$.

(ii) There is $f \in Mul(G, H)$ such that $f \in M$ and $f(ab), f(a) \in H$. Now, $f'(ab) = f(a)f(b) = L_{f(a)}f(b) \in H$ and $L_{f(a)}f \in Mul(G, H)$.

4.11 Lemma. Let H be a subgroupoid of G such that $[H]_{G,c} = G$. Then every cancellative congruence of H can be extended to a cancellative congruence of G.

Proof. Let r be a cancellative congruence of H and define a relation s on G by $(a, b) \in s$ iff $(f(a), f(b)) \in r$ for some $f \in Mul(G, H)$. Using 4.1 and the fact that $Mul(G, H)$ is left uniform, it is easy to check that s is a cancellative congruence of G. Finally, since r is cancellative, we have $s \cap (H \times H) = r$.

5. Embeddings of cancellative paramedial groupoids into paramedial quasigroups

Denote by Iq the class of subgroupoids of paramedial quasigroups. It seems to be an open problem whether Iq consists of all cancellative paramedial groupoids. Some properties of the class Iq are established in this section. First, notice that Iq is closed under subgroupoids, cartesian products and cancellative homomorphic images (4.11).

5.1 Proposition. Let G be a cancellative paramedial groupoid such that o_G is an injective transformation of G. Then $G \in Iq$.

Proof. We can assume without loss of generality that $f = o_G$ is an antiautomorphism of G (see 2.2). Put $x * y = f^{-1}(xy)$ for all $x, y \in G$. By 2.4, $G(*)$ is an idempotent medial groupoid, f is an antiautomorphism of $G(*)$ and $xy = f(x)*f(y)$ for all $x, y \in G$. One also checks easily that $G(*)$ is cancellative. Now, due to [1, 5.3.1], $G(*)$ can be embedded into an idempotent medial quasigroup $Q(*)$ and the isomorphisms $f : G(*) \to G(*)^{op}$ and $f^{-1} : G(*)^{op} \to G(*)$ can be uniquely extended to isomorphisms $g : Q(*) \to Q(*)^{op}$ and $g^{-1} : Q(*)^{op} \to Q(*)$ (the embedding $G(*) \to Q(*)$ is reflexion of $G(*)$ into the category of medial quasigroups). In other words, f is extended by an antiautomorphism g of $Q(*)$. Finally, define a multiplication on Q by $xy = g(x) \cdot g(y)$. Then Q becomes a paramedial quasigroup and G is a subgroupoid of Q.

5.2 Proposition. Let G be a cancellative paramedial groupoid such that o_G is a projective transformation of G. Then $G \in Iq$.

Proof. Let H be the set of sequences $\alpha = (a_0, a_1, a_2, \dots)$ of elements from G such that $o_G(a_{i+1}) = a_i, i \geq 0$. For $\alpha = (a_i)$ and $\beta = (b_i)$ from H we define the product $\alpha\beta = (c_i)$ by $c_i = a_ib_i$ for $i \geq 0$ even and $c_i = b_ia_i$ for $i \geq 1$ odd. Then we have $\alpha\beta \in H$ and H becomes a cancellative paramedial groupoid (in fact, H is a subgroupoid of the product $G \times G^{op} \times G \times G^{op} \times \dots$). Further, the mapping $f : H \to G$ defined by $f(\alpha) = a_0$ is a projective homomorphism. Moreover, if $\alpha = (a_i) \in H$ and $\gamma = (a_0, a_1, a_2, \dots)$, then $\gamma^2 = \alpha$, so that o_H is a projective transformation of H. On the other hand, if $\alpha = (a_i)$ and $\beta = (b_i)$ are such that $\alpha^2 = \beta^2$, then $(a_0^2, a_0, a_1, a_2, \dots) = \alpha^2 = \beta^2 = (b_0^2, b_0, b_1, b_2, \dots)$, and so $\alpha = \beta$. We have thus proved that o_H is an antiautomorphism of H, and hence $H \in Iq$ by 5.1. Finally, G is a (cancellative) homomorphic image of H, and therefore $G \in Iq$.

5.3 Remark. Let A be a group given by two generators α, β and by one relation $\alpha^2 = \beta^2$ and let $R = ZA$ be the corresponding group-ring of A over the ring Z of integers. We check that $(0 : \alpha + \beta)_l = 0$ in R.

Assume, on the contrary, that $u(\alpha + \beta) = 0$ for some $0 \neq u \in R$, $u = k_1a_1 + \dots + k_na_n$, $k_i \in Z - \{0\}$ and $a_i \in A$ pair-wise different. Now, $0 = k_1a_1\alpha + \dots + k_na_n\alpha + k_1a_1\beta + \dots + k_na_n\beta$ and it follows that there is a permutation p of $\{1, 2, \dots, n\}$ such that $k_ia_i\alpha = -k_{p(i)}a_{p(i)}\beta$; then $k_i = -k_{p(i)}$ and $a_i\alpha = a_{p(i)}\beta$. Clearly, $p(i) \neq i$ for every i and, since p is composed from cycles, we can assume that $p(1) = 2, p(2) = 3, \dots, p(m-1) = m$ and $p(m) = 1$ for some $2 \leq m \leq n$. Then $a_2 = a_1\alpha\beta^{-1}, a_3 = a_1(\alpha\beta^{-1})^2, \dots, a_m = a_1(\alpha\beta^{-1})^{m-1}$ and $a_1 = a_1(\alpha\beta^{-1})^m$. From this, $(\alpha\beta^{-1})^m = 1$, a contradiction with the obvious fact that $\alpha\beta^{-1}$ is of infinite order in the group A.

5.4 Theorem. The following conditions are equivalent for a cancellative paramedial groupoid G:

(i) $G \in Id$.
(ii) There exists a cancellative paramedial groupoid H such that o_H is a projective transformation of H and G is a subgroupoid of H.
(iii) There exists a cancellative paramedial groupoid K such that o_K is an injective transformation of K and G is a homomorphic image of K.

Proof. (i) implies (ii). We can assume that G is a quasigroup. By 6.2, there are an abelian group $G(+)$, automorphisms f, g of $G(+)$ and an element $w \in G$ such that $f^2 = g^2$ and $xy = f(x) + g(y) + w$ for all $x, y \in G$. Now, there is a unique R-module structure on $G(+)$ such that $\alpha x = f(x)$ and $\beta x = g(x)$ ($R = ZA$ by 5.3). Let $Q(+)$ be an injective R-module containing $G(+)$. Since $(0 : \alpha + \beta)_l = 0$ in R (5.3), we have $(\alpha + \beta)Q = Q$. Defining $xy = \alpha x + \beta y + w$, we obtain a paramedial quasigroup Q such that $o_Q(Q) = Q$ and G is a subquasigroup of Q.

(ii) implies (iii). In view of the proof of 5.2, H is homomorphic image of a cancellative paramedial groupoid L such that o_L is a bijection. Now, for K we can take the inverse image of G.

(iii) implies (i). Combine 5.1 and 4.11.

5.5 Remark. Let F be a free extropic groupoid of countable infinite rank. Now, it follows easily form 5.4 that the following conditions are equivalent:

(a) Iq contains every cancellative paramedial groupoid.
(b) o_F is an injective transformation of F.

6. Linear representations of paramedial groupoids

Let G be a groupoid. By a pm-linear representation of G we mean an algebra $S(+, f, g, e)$ such that G is a subset of S, $S(+)$ is a commutative semigroup, f and

g are endomorphisms of $S(+), f^2 = g^2, e \in S^0$ and $xy = f(x) + g(y) + e$ for all $x, y \in G$. The representation is said to be exact if $S = G$.

6.1 Theorem. Let G be a paramedial groupoid such that $C(G)$ is non-empty. Then there exists an exact pm-linear representation $G(+, f, g, e)$ of G such that both f and g are automorphisms of $G(+)$, $G(+)$ posses a neutral element, $e \in G$ and e is invertible in $G(+)$.

Proof. Let $w = C(G)$, $0 = ww$ and $x + y = R_w^{-1}(x)L_w^{-1}(y)$ for all $x, y \in G$. Clearly, $x + 0 = R_w^{-1}(x)w = x$ and $0 + y = wL_w^{-1}(y)$, so that 0 is a neutral element of $G(+)$.

Now, let $x, y, u, v \in G$, $\alpha = R_w^{-1}(R_w^{-1}(x)y)L_w^{-1}(uL_w^{-1}(v))$ and $\beta = R_w^{-1}(R_w^{-1}(v)y)L_w^{-1}(uL_w^{-1}(x))$. We are going to show that $\alpha = \beta$.

Since $w \in C(G)$, there are $a, b, c, d \in G$ such that $aw = w$, $wb = a$ and $wc = w$. Then $\alpha w = \alpha \cdot aw = (wL_w^{-1}(uL_w^{-1}(v)))(aR_w^{-1}(R_w^{-1}(x)y)) = (uL_w^{-1}(v))(aR_w^{-1}(R_w^{-1}(x)y))$, $w = aw = wb \cdot wc = cb \cdot ww$, $\alpha w \cdot w = ((uL_w^{-1}(v))(aR_w^{-1}(R_w^{-1}(x)y))(cb \cdot ww) = (ww \cdot aR_w^{-1}(R_w^{-1}(x)y))(cb \cdot uL_w^{-1}(v)) = (R_w^{-1}(x)y \cdot aw)(cb \cdot uL_w^{-1}(v)) = (uL_w^{-1}(v) \cdot aw)(cb \cdot R_w^{-1}(x)y) = (wL_w^{-1}(v) \cdot au)(cb \cdot R_w^{-1}(x)y) = (v \cdot aw)(cb \cdot R_w^{-1}(x)y)$, $w = aw = a \cdot aw = a(a \cdot wc)$ and $w(\alpha w \cdot w) = (a(a \cdot wc))((v \cdot au)(cb \cdot R_w^{-1}(x)y)) = ((cb \cdot R_w^{-1}(x)y)(a \cdot wc))((v \cdot au)a) = ((wc \cdot R_w^{-1}(x)y)(a \cdot cb))((v \cdot au)a) = ((yc \cdot R_w^{-1}(x)w)(a \cdot cb))((v \cdot au)a) = ((yc \cdot x)(a \cdot cb))((v \cdot au)a)$. Quite similarly, $w(\beta w \cdot w) = ((yc \cdot v)(a \cdot cb))((x \cdot au)a)$. However, the last term can be written as $(a(a \cdot cb))((x \cdot au)(yc \cdot v)) = (a(a \cdot cb))((v \cdot au)(yc \cdot x)) = ((yc \cdot x)(a \cdot cb))((v \cdot au)a)$. We have thus shown that $w(\alpha w \cdot w) = w(\beta w \cdot w)$. Since $w \in C(G)$, it follows that $\alpha = \beta$.

Now, it is clear that $G(+)$ is paramedial. According to 1.2, $G(+)$ is a commutative semigroup. We have $xy = xw + wy$ for all $x, y \in G$. In particular, $ww \cdot w + w \cdot aa = ww \cdot aa = aw \cdot aw = ww = 0$ (a is such that $aw = w$), and so $p = ww \cdot w$ is an invertible element of $G(+)$. Similarly, $q = w \cdot ww$ is also invertible, and hence $e = p + q = ww \cdot w + w \cdot ww = ww \cdot ww = 00$ is invertible.

Now, define two permutations f and g of G by $f(x) = xw - p$ and $g(x) = wx - q$. Then $f(x + y) = (x + y)w - p = (R_w^{-1}(x)L_w^{-1}(y))w + w \cdot ww - q - p = (R_w^{-1}(x)L_w^{-1}(y))(ww) - q - p = (wL_w^{-1}(y))(wR_w^{-1}(x)) - q - p = y(wR_w^{-1}(x)) - q - p = yw + w(w(R_w^{-1}(x)) - q - p = yw + ww \cdot w + w(wR_w^{-1}(x)) - q - 2p = yw + (ww)(wR_w^{-1}(x)) - q - 2p = yw + (R_w^{-1}(x)w)(ww) - q - 2p = yw + x \cdot ww - q - 2p = yw + xw + w \cdot ww - q - 2p = yw - p + xw - p = f(x) + f(y)$. We have shown that f is an automorphism of $G(+)$ and, similarly, the same is true for g. Further, we have $xy = xw + wy = xw - p + wy - q + e = f(x) + g(y) + e$ for all $x, y \in G$ and it remains to check that $f^2 = g^2$. But $f^2(x) + f(e) + g(e) + e = f(f(x) + g(0) + e) + g(f(0) + g(0) + e) + e = f(x0) + g(00) + e = x0 \cdot 00 = 00 \cdot 0x = g^2(x) + f(e) + g(e) + e$. The element $f(e) + g(e) + e$ is invertible in $G(+)$ and we get $f^2(x) = g^2(x)$ for every $x \in G$.

6.2 Corollary. Let Q be a paramedial quasigroup. Then Q possesses an exact pm-linear representation $Q(+, f, g, e)$ such that $Q(+)$ is an abelian group and both f and g are automorphisms of $Q(+)$.

Reference

[1] J.Ježek and T.Kepka, *Medial groupoids*, Rozpravy ČSAV **93/2** (1983).

Pusan National University, Kumjung, Pusan 609–735, Republic of Korea

Charles University, Sokolovská 83, 18600 Praha 8, Czech Republic