SIMPLE PARAMEDIAL GROUPOIDS

JUNG R. CHO, Pusan, JAROSLAV JEŽEK and TOMÁŠ KEPKA, Praha

(Received September 27, 1996)

The present note is a free continuation of [1] and [2] and its purpose is to initiate the study of simple paramedial groupoids—a small contribution to the task of describing simple algebras satisfying strong linear indentities.

A reader is referred to [1] for notation and various prerequisities.[1]

1. BASIC PROPERTIES OF SIMPLE PARAMEDIAL GROUPOIDS

1.1 Theorem. *Let G be a (non-trivial) simple paramedial groupoid. Then exactly one of the following three cases takes place:*

(1) *o_G is an injective transformation of G.*

(2) *G is a finite unipotent medial quasigroup.*

(3) *G is zeropotent.*

Proof. By [1, 2.1(iii)], $r = \ker(o_G)$ is a congruence of G, and hence either $r = \mathrm{id}_G$ or $r = G \times G$.

If $r = \mathrm{id}_G$, then o_G is injective, and hence we will assume that $r = G \times G$. Then G is unipotent, i.e., $xx = e = yy$ for all $x, y \in G$. By [1, 2.9(i)], $s = \ker(L_e R_e)$ is a congruence of G. Again, we have either $s = \mathrm{id}_G$ or $s = G \times G$.

First, let $s = \mathrm{id}_G$. Then $L_e R_e = R_e L_e$ is an injective endomorphism of G and consequently both L_e and R_e are injective transformations of G. By [1, 2.9(ii)], G is a cancellative medial groupoid. However, it is proved in [3] that every simple cancellative medial groupoid is a finite quasigroup.

Now, let $s = G \times G$. Then $e \cdot xe = e \cdot ye$ for all $x, y \in G$ and it follows that $e \cdot xe = e = ex \cdot e$. Further, by [1, 2.6(i)], $t = \ker(L_e^2)$ is a congruence of G. If

[1] While working on this paper, the first author was supported by the Basic Science Research Institute Program, Ministry of Education, Korea 1966, No. BSRI-96-1433 and the second one by the Grant Agency of the Czech Republic, Grant # 201/96/0312

$t = \mathrm{id}_G$, then both L_e and R_e are injective and G is cancellative ([1, 2.6(ii), 2.9(ii)]). But $e \cdot xe = e \cdot ye$ implies $x = y$ for all $x, y \in G$, which is a contradiction. Thus $t = G \times G$ and we have $e \cdot ex = e = xe \cdot e$ for every $x \in G$.

Put $I = \{a \in G;\ ae = e = ea\}$. Clearly, $e \in I$ and if $a \in I$ and $x \in G$, then $e \cdot ax = xe \cdot ae = xe \cdot e = e$, $ax \cdot e = ex \cdot ea = ex \cdot e = e$, $e \cdot xa = ae \cdot xe = e \cdot xe = e$ and $xa \cdot e = ea \cdot ex = e \cdot ex = e$, so that $ax, xa \in I$. We have proved that I is an ideal of G. But then $w = (I \times I) \cup \mathrm{id}_G$ is a congruence of G and if $w = G \times G$, then $I = G$ and G is zeropotent. If $w = \mathrm{id}_G$, then $I = \{e\}$, e is an absorbing element of G and G is again zeropotent (in fact, $I = \{e\}$ is not possible). □

1.2 Lemma. *Let G be a non-trivial finite idempotent medial groupoid and let f be an antiautomorphism of G such that id_G and $G \times G$ are the only congruences of G which are invariant under f. Then exactly one of the following three cases takes place:*

(1) *G is a quasigroup.*
(2) *G is a semilattice.*
(3) *G is a rectangular band.*

Proof. First, let r denote the intersection of all cancellative congruences of G. Then r is the smallest cancellative congruence of G and, if we define a relation r_1 on G by $(a, b) \in r_1$ iff $(f(a), f(b)) \in r_1$, we get a cancellative congruence r_1, so that $r \subseteq r_1$. This shows that r is invariant under f.

If $r = \mathrm{id}_G$, then G is cancellative and, since G is finite, it is a quasigroup. Now, we will assume that $r = G \times G$, i.e., no proper homomorphic image of G is cancellative.

Let s be the smallest congruence of G such that the corresponding factor is a semilattice. Again, define s_1 by $(a, b) \in s_1$ iff $(f(a), f(b)) \in s$. It is easy to check that s_1 is a congruence of G and $(x, xx) \in s_1, (xy, yx) \in s_1$ and $(x \cdot yz, xy \cdot z) \in s_1$ for all $x, y, z \in G$. Thus G/s_1 is a semilattice, $s \subseteq s_1$, s is invariant under f and we can assume that $s = G \times G$.

Now, since G is non-trivial and finite, at least one proper non-trivial factorgroupoid H of G is simple. According to our assumptions, H is neither cancellative nor a semilattice. Using the description of simple idempotent medial groupoids as given in [3] we conclude that H is either an LZ-semigroup or an RZ-semigroup. In both cases, $t \neq G \times G$, where t is the smallest congruence such that the corresponding factor is a rectangular band. As usual, t is invariant under f, and therefore $t = \mathrm{id}_G$. In other words, G is a rectangular band. □

1.3 Proposition. *Let G be a (non-trivial) finite simple paramedial groupoid such that o_G is injective. Then exactly one of the following three cases takes place:*

(1) *G is a quasigroup.*

(2) *G is commutative (and hence medial) and not cancellative.*
(3) *There exist a rectangular band $G(*)$ and an antiautomorphism f of $G(*)$ such that $xy = f(x) * f(y)$ $(= f(y * x))$ for all $x, y \in G$.*

Proof. Clearly, o_G is a permutation and, by [1, 2.4], there exist an idempotent medial groupoid $G(*)$ and an antiautomorphism f of $G(*)$ such that $xy = f(x) * f(y)$ for all $x, y \in G$. Since G is simple, id_G and $G \times G$ are the only congruences of $G(*)$ that are invariant under f. Now, we can apply 1.2.

If $G(*)$ is a quasigroup, then G is also a quasigroup.

If $G(*)$ is a semilattice, then G is commutative.

If $G(*)$ is a rectangular band, then one may check easily that G is neither cancellative nor commutative. □

1.4 Lemma. *Let G be a simple paramedial groupoid containing at most three elements. Then G is medial.*

Proof. Easy to check. □

1.5 Example. *Consider the following four-element groupoid G_1:*

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

Then G_1 is a simple zeropotent non-medial paramedial groupoid.

1.6 Example. *Consider the following four-element groupoid G_2:*

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

Then G_2 is a simple non-medial paramedial groupoid, G_2 is not cancellative, o_{G_2} is a permutation and $\mathrm{Id}(G_2) = \{0, 3\}$ is not a subgroupoid of G_2.

1.7 Example. *Consider the following four-element groupoid G_3:*

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

Then G_3 is a simple non-medial paramedial quasigroup and $\mathrm{Id}(G_3) = \{0,3\}$ is not a subgroupoid of G_3.

1.8 Example. *Consider the following four-element groupoid G_4:*

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

Then G_4 is a simple medial and paramedial groupoid (notice that G_2 and G_4 are not isomorphic).

Let G be a (non-trivial) simple paramedial groupoid. We will say that G is

- of type (I) if G is cancellative;
- of type (II) if G is zeropotent;
- of type (III) if G is commutative but neither cancellative nor zeropotent;
- of type (IV) if there exist a rectangular band $G(*)$ and an antiautomorphism f of $G(*)$ such that $xy = f(x) * f(y)$ for all $x, y \in G$;
- of type (V) if G is of none of the above types.

Clearly, every simple paramedial groupoid is of just one of these five types. Further, by 1.1 and 1.3, every simple paramedial groupoid of type (V) is infinite.

2. Antiautomorphisms of rectangular bands

2.1. Let G be a rectangular band. Define two relations α and β on G by $(a,b) \in \alpha$ iff $a = ab$ and $(c,d) \in \beta$ iff $d = cd$. Then both α and β are congruences of G, G/α is an RZ-semigroup, G/β is an LZ-semigroup and $\alpha \cap \beta = \mathrm{id}_G$. Moreover, $(a, ba) \in \alpha$ and $(b, ba) \in \beta$ for all $a, b \in G$. Now, it is clear that the mapping $\varphi\colon G \to G/\alpha \times G/\beta, \varphi(x) = (x/\alpha, x/\beta)$, is an isomorphism of G onto the cartesian product $G/\alpha \times G/\beta$.

Let f be an antiautomorphism of G. Then $(a,b) \in \alpha$ iff $(f(a), f(b)) \in \beta$, and hence the mapping $\varrho\colon G/\alpha \to G/\beta, \varrho(x/\alpha) = f(x)/\beta$, is an antiisomorphism of G/α onto G/β; in particular, $\mathrm{card}(G/\alpha) = \mathrm{card}(G/\beta)$. Similarly, $\varsigma\colon G/\beta \to G/\alpha, \varsigma(x/\beta) = f(x)/\alpha$, is an antiisomorphism of G/β onto G/α. Setting $g(u,v) = (\varsigma(v), \varrho(u))$, $u \in G/\alpha$, $v \in G/\beta$, we get an antiautomorphism of $G/\alpha \times G/\beta$ and $\varphi f = g\varphi$.

2.2. Let A and B be an RZ-semigroup and LZ-semigroup, resp., such that $\mathrm{card}(A) = \mathrm{card}(B) \geqslant 2$. Put $G = A \times B$ and consider bijections $\varrho\colon A \to B$ and

$\varsigma\colon B \to A$. Now, define $f(a,b) = (\varsigma(b), \varrho(a))$, $a \in A$, $b \in B$. Then f is an antiautomorphism of G (by 2.1, every antiautomorphism is of this type), $\sigma = \varsigma\varrho$ is a permutation of A and $\tau = \varrho\varsigma$ is a permutation of B.

Suppose that id_G and $G \times G$ are the only congruences of G that are invariant under f.

2.2.1 Lemma. *Let $a \in A$ and $n \geqslant 2$ be such that the elements $a, \sigma(a), \dots, \sigma^{n-1}(a)$ are pair-wise different and $\sigma^n(a) = a$. Then $A = \{a, \sigma(a), \dots, \sigma^{n-1}(a)\}$, $\mathrm{card}(A) = n$ and σ is an n-cycle.*

Proof. Let $C = \{a, \sigma(a), \dots, \sigma^{n-1}(a)\}$ and $D = \varrho(C)$; we have $C \subseteq A$ and $D \subseteq B$. Moreover, put $L = \{(\sigma^i(a), \varrho\sigma^j(a))\,;\ 0 \leqslant i,j < n\} \subseteq G, K_c = \{(c, \varrho\sigma^i(a))\,;\ 0 \leqslant i < n\} \subseteq G$, $c \in A - C$, and $H_d = \{(\sigma^i(a), d)\,;\ 0 \leqslant i < n\} \subseteq G$, $d \in B - D$. Clearly, these subsets of G are pair-wise disjoint, $\mathrm{card}(L) \geqslant 2$ and $r \neq \mathrm{id}_G$, where $r = \mathrm{id}_G \cup (L \times L) \cup \bigcup(K_c \times K_c) \cup \bigcup(H_d \times H_d)$, $c \in A - C$, $d \in B - D$. Since $f(L) \subseteq L$, $f(K_c) \subseteq H_{\varrho(c)}$ and $f(H_d) \subseteq K_{\varsigma(d)}$, the relation r remains invariant under f.

Let $(u,v) \in G$. Then $(u,v)K_c = \{(c,v)\}$ and $H_d(u,v) = \{(u,d)\}$. If $u \in C$, then $K_c(u,v) \subseteq L$ and $L(u,v) \subseteq L$. If $u \notin C$, then $K_c(u,v) \subseteq K_u$ and $L(u,v) \subseteq K_u$. If $v \in D$, then $(u,v)H_d \subseteq L$ and $(u,v)L \subseteq L$. If $v \notin D$, then $(u,v)H_d \subseteq H_v$ and $(u,v)L \subseteq H_v$.

We have checked that r is a congruence of the rectangular band G. Now, $r = G \times G$ and it follows that $L = G$ and $C = A, D = B$. □

2.2.2 Lemma. *Let $a, b \in A$ be such that $a \neq b$, $\sigma(a) = a$ and $\sigma(b) = b$. Then $A = \{a, b\}$.*

Proof. Put $C = \{a,b\}$, $D = \varrho(C)$, $L = \{(a,\varrho(a)), (a,\varrho(b)), (b,\varrho(a)), (b,\varrho(b))\}$, $K_c\{(c,\varrho(a), (c,\varrho(b))\}$, $c \in C - A$, $H_d = \{(a,d), (b,d)\}$, $d \in B - D$. Then these sets are pair-wise disjoint and $r = \mathrm{id}_G \cup (L \times L) \cup \bigcup(K_c \times K_c) \cup \bigcup(H_d \times H_d)$ is an f-invariant congruence of G. Thus $r = G \times G$, $L = G$ and $C = A$. □

2.2.3 Lemma. *Precisely one of the following two cases takes place:*

(1) $\mathrm{card}(A) = \mathrm{card}(B) = 2$, $\sigma = \mathrm{id}_A$, $\tau = \mathrm{id}_B$, $\varsigma = \varrho^{-1}$ *and* $\varrho = \varsigma^{-1}$.

(2) $\mathrm{card}(A) = \mathrm{card}(B) = n \geqslant 2$ *is finite and both* σ *and* τ *are* n*-cycles.*

Proof. In view of 2.2.1 and 2.2.2, we can assume that $\mathrm{card}(A)$ is infinite and that the elements $a, \sigma(a), \sigma^2(a), \dots$ are pair-wise different for some $a \in A$. Proceeding similarly as in the proof of 2.2.1, we can show that $A = \{a, \sigma(a), \sigma^2(a), \dots\}$. Then $a \notin \sigma(A)$, a contradiction. □

2.3. Let $n \geqslant 2$, $A = B = \{1, 2, \dots, n\}$ and let $G = A \times B$ be the corresponding rectangular band (see 2.2); we have $(i, j)(k, l) = (k, j)$. Further, choose the bijections ϱ and ς of A in such a way that $\varrho = \mathrm{id}_A$ and $\varsigma(i) = (i+1) \pmod{n}$ for every $i \in A$. Then $\sigma = \tau = \varsigma$ is an n-cycle. Finally, $f(i, j) = ((j+1) \pmod{n}, i)$.

Now, let $a, b, u, v \in A$, $1 \leqslant a < b \leqslant n$, and let r denote the smallest congruence of the rectangular band G such that r is invariant under f and r contains the pair $((a, u), (b, v))$. We have $b = \sigma^s(a)$ for a unique s, $1 \leqslant s < n$.

2.3.1 Lemma. *$((\sigma^i(a), x), (\sigma^i(b), x)) \in r$ and $((x, \sigma^i(a)), (x, \sigma^i(b))) \in r$ for all $x, i \in A$.*

Proof. First, $(a, x) = (a, x)(a, u)$ and $(b, x) = (a, x)(b, v)$, so that $((a, x), (b, x)) \in r$. Further, $(\sigma(x), a) = f(a, x)$, $(\sigma(x), b) = f(b, x)$, $(\sigma(a), \sigma(x)) = f(\sigma(x), a)$, $(\sigma(b), \sigma(x)) = f(\sigma(x), b)$, etc.

For $x \in A$, let $H_x = \{(\sigma^i(a), x)\,;\ 1 \leqslant i \leqslant n\}$ and $K_x = \{(x, \sigma^i(a))\,;\ 1 \leqslant i \leqslant n\}$. □

2.3.2 Lemma. *If the numbers n and s are relatively prime, then $r = G \times G$.*

Proof. Denote by $\oplus$ the addition modulo n on A, so that $A(\oplus)$ becomes a cyclic abelian group, where n plays the role of a neutral element.

Now, let $x \in A$ and let L_x denote the block of r such that $(a, x) \in L_x$. Put $C = \{i \in A;\ (\sigma^i(a), x) \in L_x\}$. Clearly, $n \in C$ and $s \in C$ (since $(b, x) \in r$ by 2.3.1) and, if $i \in C$, then $i \oplus s \in C$ (again by 2.3.1). Consequently, $D \subseteq C$, where D is the subgroup generated by s in A. But s and n are relatively prime, and so $D = A$ and $C = A$. We have proved that $H_x \subseteq L_x$. Since $f(H_x) = K_{\sigma(x)}$, the set $K_{\sigma(x)}$ is contained in the block of r determined by $(\sigma(x), a)$.

Let $x, y \in A$. Then $x = \sigma^j(a)$ and $y = \sigma^k(a)$ for some $j, k \in A$ and we have $(y, x) \in H_x \cap K_y$. In particular, $H_x \cap K_y$ is non-empty, which means that $H_x \cup K_y$ is contained in a block of r. Now, it is clear that $r = G \times G$. □

2.3.3 Lemma. *The following conditions are equivalent:*

(i) *n is a prime number.*

(ii) *id_G and $G \times G$ are the only f-invariant congruences of the rectangular band G.*

Proof. (i) implies (ii). Let $t \neq \mathrm{id}_G$ be an f-invariant congruence of G. There are $a, b, u, v \in A$ such that $((a, u), (b, v)) \in t$ and either $a \neq b$ or $u \neq v$; we can assume $a \neq b$, the other case being dual. Now, $t = G \times G$ by the preceding lemmas.

(ii) implies (i). Suppose, on the contrary, that n is not prime and let $2 \leqslant m < n$ be such that m divides n. Define a relation t on G by $((i, j), (k, l)) \in t$ iff m divides both $i - k$ and $j - l$. Then t is an f-invariant congruence of G and $((n, 1), (m, 1)) \in t$, $((n, 1), (m, 1)) \notin t$. Thus $\mathrm{id}_G \notin t \notin G \times G$. □

3. Simple paramedial groupoids of type (IV)

For every prime number $p \geqslant 2$, define a groupoid $R_p = \{(i,j)\,;\ 1 \leqslant i,j \leqslant p\}$, $(i,j)(k,l) = ((l+1) \pmod p, i)$. We have $(i,j)(k,l) = f(i,j) * f(k,l)$, where $R_p(*)$ is the rectangular band from 2.3 and f is the antiautomorphism defined also in 2.3. Now, id and $R_p^{(2)}$ are the only f-invariant congruences of R_p* (2.3.3) and it follows easily that R_p is a simple paramedial groupoid of type (IV) (if r is a congruence of R_p, then r is invariant under $o = f$ and, since R_p is finite, r is also invariant under f_{-1}; thus r is a congruence of $R_p(*)$). Notice that the groupoid R_p possesses no idempotent elements, R_p is anticommutative (i.e., $xy = yx$ for $x, y \in R_p$ only if $x = y$) and that R_p is antimedial (i.e., $xu \cdot vy = xv \cdot uy$ only if $u = v$). Finally, observe that R_p contains no proper subgroupoid.

Put $R'_2 = \{(i,j)\,;\ 1 \leqslant i,j \leqslant 2\}$ and define a multiplication on R'_2 by $(i,j)(k,l) = (l,i)$. Then R'_2 becomes a (four-element) simple paramedial groupoid of type (IV), R'_2 corresponds to 2.2.3(i) and $R'_2 \cong G_2$ (see 1.6).

3.1 Theorem. *(i) R'_2 and R_p, p running through prime numbers, are pair-wise non-isomorphic simple paramedial groupoids of type* (IV).

(ii) *Every simple paramedial groupoid of type* (IV) *is finite and isomorphic to one of the groupoids from* (i).

Proof. (ii) Let G be a simple paramedial groupoid of type (IV). There exist a rectangular band $G(*)$ and an antiautomorphism f of $G(*)$ such that $xy = f(x)*f(y)$ for all $x, y \in G$. If r is an f-invariant congruence of $G(*)$, then r is also a congruence of the paramedial groupoid G (and so either $r = \mathrm{id}_G$ or $r = G \times G$). Now, we can use the auxiliary results from the preceding section. □

4. Simple paramedial groupoids of type (III)

For $n \geqslant 1$, let $Y_n = \{a_0, a_1, \ldots, a_n\}$ and let a multiplication be defined on Y_n by $a_i a_j = a_0$ for $i \neq j$, $a_0 a_0 = a_0$ and $a_i a_i = a_k$, $k = (i+1) \pmod n$ for $i \neq 0$. Then Y_n is a simple paramedial groupoid of type (III). Further, Y_2 is a two-element semilattice and, for $n \geqslant 2$, Y_n contains just one idempotent element, namely a_0; in both cases, a_0 is an absorbing element of Y_n. Notice also that Y_n, except for the above mentioned idempotents, possesses no proper subgroupoids.

4.1 Theorem. (i) *The groupoids Y_n, $n \geqslant 1$ are pair-wise non-isomorphic simple paramedial groupoids of type* (III).

(ii) *Every simple paramedial groupoid of type* (III) *is finite and isomorphic to one of the groupoids from* (i).

P r o o f. Every commutative paramedial groupoid is medial and our result follows from the classification of simple commutative medial groupoids given in [3]. □

5. Simple paramedial groupoids of type (II)—linear representations

5.1 Proposition. *Let G be a simple paramedial groupoid of type* (II) *(and $0 = aa$, $a \in G$). Then there exist a commutative semigroup $S(+)$ and automorphisms f, g of $S(+)$ such that the following conditions are satisfied:*

(i) *$G \subseteq S$ and $ab = f(a) + g(b)$ for all $a, b \in G$.*
(ii) *0 is an absorbing element of $S(+)$ and $f(x) + g(x) = 0$ for every $x \in S$.*
(iii) *$f^2 = g^2$.*
(iv) *$S(+)$ is either zeropotent or idempotent.*
(v) *The algebra $S(+, f, g, f^{-1}, g^{-1})$ is simple and generated by G.*

P r o o f. By [4], there exist a commutative semigroup $S(+)$ and automorphisms f, g of $S(+)$ such that the conditions (i), (ii) and (iii) are satisfied; obviously, we can assume that the algebra $\widetilde{S} = S(+, f, g, f^{-1}, g^{-1})$ is generated by G. Moreover (considering the factor $\widetilde{S}/s$, where s is a congruence of $\widetilde{S}$ maximal with respect to $s \cap (G \times G) = \mathrm{id}_G$), we can assume that $r \cap (G \times G) \neq \mathrm{id}_G$ for every non-identical congruence r of $\widetilde{S}$. Now, if r is such a congruence and $t = r \cap (G \times G)$, then t is a congruence of G, $t \neq \mathrm{id}_G$, and hence $t = G \times G \subseteq r$. Consequently, $G \subseteq A = \{x \in S;\ (0, x) \in r\}$ and $A = S$, since A is evidently a subalgebra of $\widetilde{S}$. Thus $r = S \times S$ and we have proved (v). Now, it remains to show (iv); to that purpose, we can assume that $S(+)$ is not zeropotent.

The endomorphism $x \to 2x$ of $\widetilde{S}$ is not constant, and so it is an injective endomorphism of $\widetilde{S}$. Using an obvious and standard construction, we embed $\widetilde{S}$ into a (simple) algebra $\widetilde{S}_1 = S_1(+, f_1, g_1, f_1^{-1}, g_1^{-1})$ such that $x \to 2x$ is an automorphism of $\widetilde{S}_1$. Now, proceeding similarly as in [5], we can show that $S_1(+)$ is idempotent. □

5.2 Remark. Let G be a simple paramedial groupoid of type (II). Proceeding similarly as in the proof of 5.1, we can show that there exist a commutative semigroup $S(+)$ and endomorphisms f, g of $S(+)$ such that the conditions (i), (ii), (iii) and (iv) from 5.1 are satisfied and, moreover, the following is true:

(v′) The algebra $\widehat{S} = S(+, f, g)$ is simple and generated by G.

Now, $f^2 (= g^2)$ is an endomorphism of $\widehat{S}$, and hence either $\ker(f^2) = G \times G$ or $\ker(f^2) = \mathrm{id}_G$. In the former case, we must have $\mathrm{card}(G) = 2$, and so $\ker(f^2) = \mathrm{id}_G$, provided that $\text{card}(G) \geqslant 3$. However, then f and g are injective endomorphisms of $S(+)$.

6. Simple paramedial groupoids of type (I)—linear representations

First, recall that a non-trivial cancellative groupoid G is called c-simple if id_G and $G \times G$ are the only cancellative congruences of G. Further, let A be the group given by two generators α, β and one relation $\alpha^2 = \beta^2$, and let $R = ZA$ be the corresponding group-ring over the ring Z of integers.

6.1 Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) *Q is a c-simple paramedial quasigroup.*
(ii) *There exist a simple R-module structure $Q(+, rx;\ r \in R)$ defined on Q and an element $w \in Q$ such that $ab = \alpha a + \beta b + w$ for all $a, b \in Q$.*

Proof. The result is an easy consequence of [1, 6.2]. □

6.2 Proposition. *Let G be a c-simple paramedial cancellative groupoid. Then the q-envelope of G (see* [2, 5.3]*) is a c-simple paramedial quasigroup.*

Proof. See [1, 4.11] and [2, 5.1,5.3]. □

References

[1] *J. R. Cho, J. Ježek and T. Kepka*: Paramedial groupoids. (Preprint).
[2] *J. Ježek and T. Kepka*: Equational theory of paramedial groupoids. (Preprint).
[3] *J. Ježek and T. Kepka*: Medial groupoids. Rozpravy ČSAV *93/2* (1983).
[4] *J. Ježek and T. Kepka*: Linear equational theories and semimodule representations. (Preprint).
[5] *J. Ježek and T. Kepka*: Simple semimodules over commutative semirings. Acta Sci. Math. Szeged *46* (1983), 17–27.

Authors' addresses: Jung R. Cho, Pusan National University, Kumjung, Pusan 609-735, Republic of Korea; Jaroslav Ježek and Tomáš Kepka, Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic.