BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(54), 2007, Pages 101–106
ISSN 1024–7696

Crossed-inverse-property groupoids

V. Izbash, N. Labo

Abstract. The (right, left) crossed-inverse-property in groupoids is investigated. It is shown that the class of all crossed-inverse-property groupoids is a variety of quasigroups. Some properties of the right-crossed-property groupoids are established.

Mathematics subject classification: 20N05,20N15.
Keywords and phrases: CI-groupoid, quasigroup, variety.

In this paper we investigate (right, left) crossed-inverse-property groupoids. We concentrate on the problem of proving whether the right-crossed-inverse-property groupoid is a quasigroup. We establish in this paper several results that bring nearer the solution of this problem. For quasigroups these notions are considered, for example, in [1–3].

Let $(Q, \cdot)$ be a groupoid (i.e. a non-empty set together with a binary operation " $\cdot$ ").

Definition 1. *A groupoid $(Q, \cdot)$ is called:*

(i) a right crossed-inverse-property groupoid (RCIP-groupoid) if for each $x \in Q$, there exists an element $x' \in Q$ such that $(xy)x' = y$ for all $y \in Q$;

(ii) a left crossed-inverse-property groupoid (LCIP-groupoid) if for each $x \in Q$, there exists an element $x'' \in Q$ such that $x''(yx) = y$ for all $y \in Q$;

(iii) a crossed-inverse-property groupoid (CIP-groupoid) if it satisfies (i) and (ii).

Note that in Definition 1 the uniqueness of the elements $x', x'' \in Q$ is not requested. Nevertheless we have the following assertion.

Proposition 1. *The elements x', x'' from Definition 1 are unique for every $x \in Q$.*

Proof. Let be $u, v \in Q$ and $(xy)u = y = (xy)v$. Then $u = ((xy)u)(xy)' = ((xy)v)(xy)' = v$. The same is valid for $x'' \in Q$.

For a groupoid $(Q, \cdot)$ from Definition 1 denote by I_r, I_l the mappings $x \to x'$, $x \to x''$ respectively. Thus from Proposition 1 the mappings I_r, I_l are unique if exist. So the considered groupoids can be defined as follows.

Definition 2. *A groupoid $(Q,\cdot)$ is called:*

(i) a right crossed-inverse-property groupoid (RCIP-groupoid) if there exists a mapping I_r of Q such that

$$(xy)I_r x = y \tag{1}$$

for all $x, y \in Q$, that is shortly denoted by $(Q,\cdot,I_r)$;

(ii) a left crossed-inverse-property groupoid (LCIP-groupoid) if there exists a mapping I_l of Q such that

$$I_l x(yx) = y \tag{2}$$

for all $x, y \in Q$, that is shortly denoted by $(Q,\cdot,I_l)$;

(iii) a crossed-inverse-property groupoid (CIP-groupoid) if it satisfies (i) and (ii), , that is shortly denoted by $(Q,\cdot,I_r,I_l)$.

Let $L_a x = ax$ $(R_a x = xa)$ be the left (right) translation by element x in $(Q,\cdot)$.

Proposition 2. *(i) If $(Q,\cdot,I_r)$ is a RCIP-groupoid, then it is a left cancellable groupoid, (i. e. $(ax = ay) \Rightarrow (x = y)$ for all $a, x, y \in Q$, or, equivalently, L_a is injective for any $a \in Q$);*

(ii) If $(Q,\cdot,I_l)$ is a LCIP-groupoid, then it is a right cancellable groupoid, i. e. $(xa = ya) \Rightarrow (x = y)$ for all $a, x, y \in Q$, or, equivalently, R_a is injective for any $a \in Q$);

(iii) If $(Q,\cdot,I_r,I_l)$ is a CIP-groupoid, then it is a cancellable groupoid;

Proof. (i) Let be $a, x_1, x_2 \in Q$ such that $ax_1 = ax_2$. Then $(ax_1)I_r a = (ax_2)I_r a$, so $x_1 = x_2$ by Definition 2. Similarly for (ii) and (iii).

Proposition 3. *Let be φ, ψ arbitrary mappings and χ bijection on the set Q:*

(i) If $\varphi\psi = \chi$ then ψ is injective and φ is surjective;

(ii)If $\varphi\psi = \chi$ and φ is injective, then φ, ψ are bijections on Q.

Proof. (i) For $x, y \in Q$ we have $(\psi x = \psi y) \Rightarrow (\varphi(\psi x) = \varphi(\psi y)) \Rightarrow (\chi x = \chi y) \Rightarrow (x = y)$. So ψ is injective. Since $\varphi\psi = \chi$ then $\varphi\psi y = \chi y$ and $\varphi\psi\chi^{-1}y = y$ for every $y \in Q$, hence φ is surjective.

(ii) By (i) φ is surjective, so it is a bijection. Then ψ is a bijection by $\varphi\psi = \chi$.

Proposition 4. *(i) The mapping I_r of a RCIP-groupoid $(Q,\cdot,I_r)$ is an endomorphism of $(Q,\cdot)$ and*

$$yI_r(xy) = I_r x \tag{3}$$

for all $x, y \in Q$;

(ii) The mapping I_l of a LCIP-groupoid $(Q,\cdot,I_l)$ is an endomorphism of $(Q,\cdot)$ and

$$I_l(yx)y = I_l x \tag{4}$$

for all $x, y \in Q$*;*

(iii) The image $I_r(Q)$ *of a* $RCIP$*-groupoid* $(Q, \cdot, I_r)$ *is a concellable* $RCIP$*-groupoid. In the groupoid* $(I_r(Q), \cdot, I_r)$ *the translations* $L_x, R_{I_r x}$ *are bijections for all* $x \in I_r(Q)$*,* I_r *is injective and*

$$y(xI_r y) = x \tag{5}$$

holds for all $x, y \in I_r(Q)$*;*

(iv) The image $I_l(Q)$ *of* $LCIP$*-groupoid* $(Q, \cdot, I_l)$ *is a cancellable* $LCIP$*-groupoid. In the groupoid* $(I_l(Q), \cdot, I_l)$ *the translations* $R_x, L_{I_l x}$ *are bijections for all* $x \in I_l(Q)$*,* I_l *is injective and*

$$(I_l yx)y = x \tag{6}$$

holds for all $x, y \in I_l(Q)$*;*

Proof. (i). From (1), we have $((xy)I_r x)I_r(xy) = yI_r(xy)$, that is $yI_r(xy) = I_r x$, by (1). Then $(yI_r(xy))I_r y = I_r x I_r y$, so $I_r(xy) = I_r x I_r y$ i. e. I_r is an endomorphism.

(ii). The proof is similar to that of (i).

(iv). The homomorphic image of a groupoid is a groupoid. For any $x \in I_l(Q)$ it holds $I_l(x) \in I_l(Q)$. Thus $(I_l(Q), \cdot, I_l)$ is a $LCIP$-groupoid.

If elements $a, b, x \in Q$ and $xa = b$ then $x = I_l a \cdot b$ by (2). Now suppose $a, b, c \in Q$ such that $(I_l a \cdot b)a = c$. Then by (2) we have $I_l a \cdot b = I_l a \cdot c = d$ for some $d \in Q$ and $I_l b \cdot d = I_l a = I_l c \cdot d$ from which $I_l b = I_l c$ by the right cancellability in the groupoid $(Q, \cdot)$.

The following implications

$$((I_l a \cdot b)a = c) \Rightarrow (I_l((I_l a \cdot b)a)) = I_l c) \Rightarrow ((I_l^2 a \cdot I_l b)I_l a = I_l c) \Rightarrow ((I_l^2 a \cdot I_l b)I_l a = I_l b)$$

are valued for all $a, b \in Q$, thus (6) is proved. From (2) and (6) we get $L_{I_l x} R_x = \varepsilon = R_x L_{I_l x}$, so $R_x, L_{I_l x}$ are bijections for any $x \in I_l(Q)$ by Proposition 3.

Let be $x_1, x_2 \in I_l(Q)$ such that $I_l x_1 = I_l x_2$. Then $L_{I_l x_1} = L_{I_l x_2}$ and $I_l x_1(yx_1) = y = I_l x_2(yx_2)$, for all $y \in I_l(Q)$. Put here $y = I_l a$ for an arbitrary fixed $a \in I_l(Q)$. We obtain $I_l x_1(I_l a \cdot x_1) = I_l a = I_l x_2(I_l a \cdot x_2)$, or $L_{I_l x_1} L_{I_l a} x_1 = L_{I_l x_2} L_{I_l a} x_2$. Thus $x_1 = x_2$ and I_l is injective.

Now for all $a, x_1, x_2, c \in I_l(Q)$ we have

$$(ax_1 = ax_2 = c) \Rightarrow (I_l x_1 \cdot c = a = I_l x_2 \cdot c) \Rightarrow (I_l x_1 = I_l x_2) \Rightarrow (x_1 = x_2)$$

by the right cancellability in the groupoid $(Q, \cdot)$ and injectivity of I_l. So $I_l(Q)$ is a cancellable $LCIP$-groupoid.

(iii). The proof is similar to that of (iv).

Definition 3. *A quasigroup* $(Q, \cdot)$ *is called a* $RCIP-$ *(*$LCIP-$*,* $CIP-$*) quasigroup if it is a* $RCIP-$ *(*$LCIP-$*,* $CIP-$*) groupoid.*

Theorem 1. *The following statements are equivalent for a groupoid $(Q, \cdot)$:*

(i) $(Q, \cdot, I_r)$ is a RCIP-groupoid and the mapping I_r is a bijection;

(ii) $(Q, \cdot, I_l)$ is a LCIP-groupoid and the mapping I_l is a bijection;

(iii) $(Q, \cdot, I_r, I_l)$ is a CIP-quasigroup.

Proof. $(iii) \Rightarrow (i)$. If $(Q, \cdot)$ is a CIP-quasigroup then L_a and R_a are bijections for all $a \in Q$. Let be $x_1, x_2 \in Q$ such that $I_r x_1 = I_r x_2$. Then $R_{I_r x_1} = R_{I_r x_2}$ and $(x_1 y)I_r x_1 = y = (x_2 y)I_r x_2$, for all $y \in Q$. Put here $y = I_r a$ for an arbitrary fixed $a \in Q$. We obtain $(x_1 I_r a)I_r x_1 = I_r a = (x_2 I_r a)I_r x_2$, or $R_{I_r x_1} R_{I_r a} x_1 = R_{I_r x_2} R_{I_r a} x_2$. Thus $x_1 = x_2$ and I_r is injective.

For all $a, b \in Q$ there exists a unique $x \in Q$ such that $(xb)a = b$. Also we have $(xb)I_r x = b$ and then $I_r x = a$ by the cancellability in the quasigroup $(Q, \cdot)$. So, the mapping I_r is a bijection.

$(iii) \Rightarrow (ii)$. The proof is similar.

$(i) \Rightarrow (iii)$. Let be $a, b \in Q$. From Proposition 2 L_a is injective for any $a \in Q$. Since I_r is a bijection then there exists $x \in Q$ such that $I_r x = b$. By (3) it hold $yI_r(xy) = I_r x = b$ for any $y \in Q$. We get $L_a I_r(xa) = aI_r(xa) = I_r x = b$ and L_a is surjective. From (1) we get $R_{I_r x} L_x = \varepsilon$. Thus R_a is a bijection for any $a \in Q$ since I_r is one. So $(Q, \cdot)$ is a $RCIP$-quasigroup. Now (3) with $y = I_r^{-1} y$ and $x = I_r^{-1} x$ gives

$$I_r^{-1} y(xy) = x \tag{7}$$

for all $x, y \in Q$. Thus $(Q, \cdot, I_r, I_l)$ is a CIP-quasigroup with $I_l = I_r^{-1}$.

$(ii) \Rightarrow (iii)$. The proof is similar.

Corollary 1. *If $(Q, \cdot, I_r, I_l)$ is a CIP-quasigroup then I_l, I_r are bijections and $I_l = I_r^{-1}$.*

Corollary 2. *A finite RCIP- (LCIP-) groupoid is a CIP-quasigroup.*

Proof. Let be $(Q, \cdot, I_r)$ a finite $RCIP$-groupoid. By Proposition 3 L_a is injective for all $a \in Q$, so it is a bijective mapping because of finiteness of Q. From $(xy)I_r x = y$ we obtain $R_{I_r x} L_x = \varepsilon$, thus $R_{I_r x}$ is a bijection for all $x \in Q$.

Similarly as in Theorem 1 we can prove that I_r is injective. Because of finiteness of Q the mapping I_r is bijective and hence R_x is a bijection for all $x \in Q$. So $(Q, \cdot)$ is a quasigroup. The proof is similar when $(Q, \cdot)$ is a left crossed-inverse-property groupoid.

Theorem 2. *Every CIP-groupoid is a CIP-quasigroup.*

Proof. By Definition 2 we have $R_{I_r x} L_x = \varepsilon$ and $L_{I_l x} R_x = \varepsilon$. Thus R_x, L_x are bijections for all $x \in Q$ by Propositions 3 and 4.

Proposition 5. *(i) A homomorphic image of RCIP- (LCIP-, CIP-) groupoid is a RCIP- (LCIP-, CIP-) groupoid;*

(ii) A direct product of two RCIP- (LCIP-, CIP-) groupoids is a RCIP- (LCIP-, CIP-) groupoid.

Proof. (i) Let $(Q, \cdot)$ be a $RCIP$-groupoid for which $(xy)I_rx = y$ for all $x, y \in Q$, and φ is a homomorphism of $(Q, \cdot)$ on a groupoid $(G, \star)$. Then $(\varphi((xy)I_rx) = \varphi y) \Leftrightarrow ((\varphi x \star \varphi y) \star \varphi(I_rx) = \varphi y)$ for all $x, y \in Q$. So $(\varphi x \star z) \star \varphi(I_rx) = z$ for all $x \in Q, z \in G$. Hence for every $u, z \in G$ there exists an element $u^{'} \in G$ such that $(u \star z) \star u^{'} = z$ for all $u, z \in G$, that is $(G, \star)$ is a $RCIP$-groupoid by Definition 1. The proof is similar when $(Q, \cdot)$ is a $LCIP$- (CIP-) groupoid. (ii) Let $(Q, \cdot)$ and $(G, \star)$ be $RCIT$-groupoids and $(x \cdot y) \cdot I_rx = y$ for all $x, y \in Q$, where I_r is a mapping on Q, and $(x \star y) \star J_rx = y$ for all $x, y \in G$, where J_r is a mapping on G. Define the mapping $T_r : Q \times G \longrightarrow Q \times G$ by $T_r(x, u) := (I_rx, J_ru)$ for all $(x, u) \in Q \times G$. Let $(\otimes)$ be the binary operation on $Q \times G$ defined by $(x, u) \otimes (y, v) := (x \cdot y, u \star v)$ for all $(x, u), (y, v) \in Q \times G$. Then we have $((x, u)\otimes(y, v))\otimes T_r(x, u) = (x\cdot y, u\star v)\otimes(I_rx, J_ru) = ((x\cdot y)\cdot I_rx, (u\star v)\star J_ru)) = (y, v)$. Thus,$(Q \times G, \otimes)$ is a $RCIP$-groupoid. The proof is similar when $(Q, \cdot)$ and $(G, \star)$ are $LCIP$- (CIP-) groupoids.

Lemma 1. *(i)A homomorphic image of CIP-quasigroup is a CIP-quasigroup;*

(ii) A subquasigroup of a CIP-quasigroup is a CIP-quasigroup.

Proof. Let $(Q, \cdot)$ be a CIP-quasigroup for which $(xy)I_rx = y$ for all $x, y \in Q$, and φ be a homomorphism of $(Q, \cdot)$ on a groupoid $(G, \star)$.

(i) It is well known that $(G, \star)$ is a groupoid with division. By Propositions 5 and 2 $(G, \star)$ is a cancellable groupoid.

(ii) Let $(P, \cdot)$ be a subquasigroup of the CIP-quasigroup $(Q, \cdot)$. Since $(xy)I_rx = y$ for all $x, y \in P$, then $I_rx \in P$ for all $x \in P$. Thus $(P, \cdot)$ is a CIP-quasigroup by Definition 2.

Theorem 3. *The class of all CIP-quasigroups is a variety of quasigroups.*

Proof. It follows from Proposition 5 and Lemma 1.

References

[1] Artzy R. *On loops with a special property.* Proc. Amer. Math. Soc., 1955, **6**, p. 448–453.

[2] Belousov V.D., Tsurkan B.V. *Crossed inverse quasigroups (CI-quasigroups).* Izv. Vyssh. Uchebn. Zaved. Math., 1969, **3**, p. 21–27 (in Russian).

[3] Keedwell A.D. *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography.* Australas. J. Combin., 1969, **20**, p. 241–250.

[4] Izbash V., Labo N. *On crossed-inverse-property groupoids.* Abstracts. Second Conference of the Mathematical Society of the Republic of Moldova. Chisinau, 2004, August 17–19, p. 181–182.

V. Izbash
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, ND-2029 Chişinău
Moldova

E-mail: *vizb@math.md, izbas@mail.md*

Received June 25, 2007

N. Labo
Baltsy State University
Baltsy, Moldova

E-mail: *labnat@mail.ru*