

Tomáš Kepka

Quasigroups having at most three inner mappings

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 30 (1989), No. 1, 3--11

Persistent URL: <http://dml.cz/dmlcz/142599>

Terms of use:

© Univerzita Karlova v Praze, 1989

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

Quasigroups Having at most Three Inner Mappings

T. KEPKA

Department of Mathematics, Charles University, Prague

Received 2 February 1988

In the paper, the quasigroups with at most three inner mappings are described.

V článku se popisují kvazigrupy, které mají nejvýše tři vnitřní permutace.

В статье изучаются квазигруппы имеющие не более 3 внутренних подстановок.

1. Introduction

Let Q be a quasigroup. We denote by $\mathcal{M}_l(Q)$ ($\mathcal{M}_r(Q)$) the left (right) multiplication group of Q , i.e. the permutation group generated by all L_a (R_a), $a \in Q$; here, $L_a(x) = ax$ and $R_a(x) = xa$ for every $x \in Q$. Further, let $\mathcal{M}(Q)$ be the multiplication group of Q . For $a \in Q$, we put $\mathcal{I}(Q, a) = \{f \in \mathcal{M}(Q); f(a) = a\}$. Clearly, the inner mapping groups $\mathcal{I}(Q, a)$ are isomorphic and we can define $i(Q) = \text{card}(\mathcal{I}(Q, a))$.

1.1. Proposition. Let Q be a loop with $i(Q) \leq 3$. Then Q is an abelian group and $i(Q) = 1$.

Proof. For $i(Q) \leq 2$, the result is proved in [1]. Hence, assume that $i(Q) = 3$. Then $\mathcal{I}(Q, 1) = \{1, g, g^2\}$, where $g^3 = 1$. Further, assume for a moment that Q is not commutative. Then $ab \neq ba$ for some $a, b \in Q$. We have $f(b) \neq b$, where $f = R_a^{-1}L_a$. But $f(1) = 1$, $f(a) = a$, and hence either $f = g$ or $f = g^2$. Similarly, $h = R_b^{-1}L_b$ is equal either to g or to g^2 . In particular, either $f = h$ or $f = h^2$ and, anyway, $f(b) = b$, a contradiction. We have proved that Q is commutative. Put $f_{a,b} = L_b^{-1}L_a^{-1}L_{ab}$ for all $a, b \in Q$. Then $f_{a,b}(a) = a$. We have $f_{a,b} \in \{1, g, g^2\}$, and so either $f_{a,b} = 1$ or $f_{a,b} \in \{g, g^2\}$ and $g(a) = a$. Now, let $a, b, c \in Q$ be such that $a \cdot bc \neq ab \cdot c$. Then $f_{b,c}(a) \neq a$, so that $f_{b,c} \in \{g, g^2\}$, $f_{a,b} = 1$ and $a \cdot bc = ab \cdot c$, a contradiction. We have proved that Q is associative.

1.2. Corollary. Let Q be a quasigroup with $i(Q) \leq 3$. Then Q is isotopic to an abelian group.

*) Sokolovská 83, 186 00 Praha 8, Czechoslovakia

A quasigroup Q is said to be

- medial if it satisfies $xy \cdot uv = xu \cdot yv$,
- left modular if it satisfies $x \cdot yz = z \cdot yx$,
- right modular if it satisfies $xy \cdot z = zy \cdot x$,
- left permutable if it satisfies $x \cdot yz = y \cdot xz$,
- right permutable if it satisfies $xy \cdot z = xz \cdot y$,
- an LIP – quasigroup if there is a mapping f of Q into Q such that $f(x) \cdot xy = y$ for all $x, y \in Q$,
- an RIP – quasigroup if there is a mapping f of Q into Q such that $yx \cdot f(x) = y$ for all $x, y \in Q$,
- an IP – quasigroup if it is both left and right IP – quasigroup.

2. Auxiliary results

In this section, let $G(+)$ be an abelian group containing at least three elements and let g be a permutation of G such that $g \neq \text{id}_G = g^3$ and $g(0) = 0$.

Put $A = \{a \in G; g(a + x) = g(a) + x \text{ for every } x \in G\}$, $B = \{b \in G; g(b + x) = g(b) + g(x) \text{ for every } x \in G\}$ and $C = \{c \in G; g(c + x) = g(c) + g^2(x) \text{ for every } x \in G\}$.

2.1. Lemma. $A = \emptyset$ and $C \neq G$.

Proof. Let, on the contrary, $a \in A$. Then $0 = g(0) = g(a - a) = g(a) - a$, so that $g(a) = a$. Consequently, $g(a + x) = a + x$ for every $x \in G$, and therefore $g = \text{id}_G$, a contradiction. Proceeding similarly, we can show that $C \neq G$.

2.2. Lemma. $0 \in B$ and $B \cap C = \emptyset$.

Proof. Obvious.

2.3. Lemma. $B = G$ iff g is an automorphism of $G(+)$.

Proof. Obvious.

In the rest of this section, we shall assume that $G = B \cup C$ and $C \neq \emptyset$. Then $\emptyset \neq B \neq G$.

2.4. Lemma. $g \upharpoonright B = \text{id}_G$.

Proof. Let $b \in B$ and $c \in C$. Then $g^2(b) + g(c) = g(b + c) = g(b) + g(c)$, so that $g^2(b) = g(b)$ and $b = g(b)$.

2.5. Lemma. $g(C) \subseteq C$.

Proof. Let, on the contrary, $c \in C$ be such that $g(c) \in B$. By 2.4, $g^2(c) = g(c)$, hence $c = g(c) \in B \cap C$, a contradiction with 2.2.

2.6. Lemma. $g(c) \neq c$ for every $c \in C$.

Proof. Let, on the contrary, $g(c) = c$ for some $c \in C$. Then, for every $a \in C$, $c + g^2(a) = g(c + a) = g(a) + g^2(c) = g(a) + c$, and so $g^2(a) = g(a)$ and $g(a) = a$. We have proved $g \upharpoonright C = \text{id}_C$ and hence $g = \text{id}_G$ by 2.4, a contradiction.

2.7. Lemma. $B = \{b \in G; g(b) = b\}$.

Proof. The result follows from 2.4 and 2.6.

2.8. Lemma. Let $a, b \in B$ (resp. $a, b \in C$). Then $a + b \in B$.

Proof. If $a, b \in B$, then $g(a + b) = g(a) + g(b) = a + b$ by 2.4 and $a + b \in B$ by 2.7. Now, let $a, b \in C$. Then $g(a) \in C$ by 2.5 and we have $g(a + b) = g^2(a) + g(b) = g(g(a) + g^2(b)) = g^2(a + b)$, so that $a + b = g(a + b)$ and $a + b \in B$ by 2.7.

2.9. Lemma. B is a subgroup of index 2 in $G(+)$.

Proof. If $b \in B$, then $0 = g(b - b) = g(b) + g(-b)$, $g(-b) = -g(b) = -b$ and $-b \in B$ by 2.7. Now, from 2.8 it follows that B is a subgroup of $G(+)$. Again by 2.8, B is of index 2.

2.10. Lemma. Let $u \in C$ and $v = g(u)$. Then $v \in C$, $u \neq v$, $3u = 3v$, $C = B + u$ and $g(b + u) = b + v$ for each $b \in B$.

Proof. By 2.9 and 2.4, $C = B + u$, $g(b + u) = b + v$ for each $b \in B$. Since $g \neq \text{id}_G$, $u \neq v$. Finally, $u = g^3(u) = g^2(v) = g(g(v - u + u)) = g(2v - u) = g(2v - 2u + u) = 3v - 2u$, and hence $3u = 3v$.

2.11. Lemma. There is an element $0 \neq w \in B$ such that $3w = 0$ and $g(c) = c + w$ for every $c \in C$.

Proof. The result follows from 2.10.

3. Auxiliary results

In this section let Q be a quasigroup with $i(Q) = 3$. Suppose that Q is not a right loop. Take an element $0 \in Q$, put $g = R_z$ (where $z \in Q$ is such that $0 \cdot z = 0$), $h = L_0$ and $x + y = g^{-1}(x)h^{-1}(y)$ for all $x, y \in Q$. Then $Q(+)$ is an abelian group. Since Q is not a right loop, $g \neq \text{id}_Q$. Clearly, $g(0) = 0$, and hence $\mathcal{R}(Q, 0) = \{1, g, g^2\}$. In particular, $g^3 = \text{id}_Q$.

We have $xy = g(x) + h(y)$ for all $x, y \in Q$. Put $h(0) = v$.

3.1. Lemma. Just one of the following three cases takes place:

- (i) $h(x) = x + v$ for every $x \in Q$.
- (ii) $h(x) = g(x) + v$ for every $x \in Q$.
- (iii) $h(x) = g^2(x) + v$ for every $x \in Q$.

Proof. Let $u \in Q$ be such that $u0 = 0$. Then $L_u \in \{1, g, g^2\}$. However, $u = g^2(-h(0)) = g^2(-v)$ and $L_u = L_{-v}^+$. The rest is clear.

Further, define the sets A, B, C similarly as in the preceding section.

3.2. Lemma. $Q = A \cup B \cup C$.

Proof. Let $a \in Q$ and $k = L_{-g(a)}^+ g L_a^+$. Then $k(0) = -g(a) + g(a) = 0$, so that $k \in \{1, g, g^2\}$. If $k = 1$, then $a \in A$; if $k = g$, then $a \in B$; if $k = g^2$, then $a \in C$.

Now, suppose that $B \neq Q$, i.e. $C \neq Q$. Then, by 2.9 and 2.11, B is a subgroup of $Q(+)$, B is of index 2, $g|B = \text{id}_B$ and there is an element $0 \neq w \in B$ such that $3w = 0$ and $g(c) = c + w$ for every $c \in C$ (then $g^2|B = \text{id}_B$ and $g^2(c) = c + 2w = c - w$).

4. Auxiliary results

In this section, let $G(+)$ be an abelian group having at least six elements, let B be a subgroup of index two, $C = G - B$, and let $0 \neq w \in B$ be such that $3w = 0$. Further, let $v \in G$ be arbitrary.

Define a multiplication on G by $bx = b + x + v$ and $cx = c + x + w + v$ for all $b \in B, c \in C, x \in G$. Then we get a groupoid which is clearly a quasigroup. We denote this quasigroup by $G = G[+, B, w, v, 1]$.

- 4.1. Lemma.** (i) For $x, y \in G$, $xy = yx$ iff either $x, y \in B$ or $x, y \in C$.
(ii) The quasigroup G is not commutative.
(iii) G is a left loop and G is not a right loop.
(iv) If $v \in B$, then $-v$ is the left unit element of G .
(v) If $v \in C$, then $-w - v$ is the left unit element of G .
(vi) $r = (B \times B) \cup (C \times C)$ is a congruence of G and G/r is a two-element group.
(vii) Q is an LIP - quasigroup and Q is not an RIP - quasigroup.
(viii) Q is left permutable and is not right permutable.

Proof. Easy.

4.2. Lemma. If $v \in B$, then the mapping $x \rightarrow x + v$ is an isomorphism of $G[+, B, w, v, 1]$ onto $G[+, B, w, 0, 1]$.

Proof. The assertion may be checked easily.

4.3. Lemma. If $v \in C$, then the mapping $x \rightarrow x + v + w$ is an isomorphism of $G[+, B, w, v, 1]$ onto $G[+, B, w, 0, 1]$.

Proof. The assertion may be checked easily.

We have proved that the quasigroups $G[+, B, w, v, 1]$ and $G[+, B, w, 0, 1]$ are isomorphic. In the rest of this section, we shall assume that $v = 0$ and we put $G = G[+, w, 0, 1]$.

4.4. Lemma. G is not medial.

Proof. Let $c \in C$. Then $c \cdot 0 \cdot c \cdot 0 = (c + w)(c + w) = 2c + 3w \neq 2c + w = (2c + w) \cdot 0 = cc \cdot 00$.

Put $g(b) = b$ and $g(c) = c + w$ for all $b \in B$, $c \in C$. Then g is a permutation of G , $g \neq \text{id}_G$ and $g^3 = \text{id}_G$. Further, let $h(b) = b + w$ and $h(c) = c$ for all $b \in B$, $c \in C$. Again, $h \neq \text{id}_G$ and $h^3 = \text{id}_G$. Clearly, $gh = hg = L_w^+$, $L_b^+g = gL_b^+$ and $L_c^+h = gL_c^+$ for all $b \in B$, $c \in C$.

4.5. Lemma. $\mathcal{M}_l(G) = \mathcal{M}(G(+)) = \{L_a^+; a \in G\}$ and $\mathcal{M}_r(G) = \mathcal{M}(G) = \{L_a^+, L_ag, L_a^+g^2; a \in G\}$.

Proof. Easy.

4.6. Lemma. $\mathcal{I}(G, 0) = \{1, g, g^2\}$, and so $i(G) = 3$.

Proof. This follows from 4.5.

Finally, let B' be a subgroup of index 2 of an abelian group $G'(+)$, let $0 \neq w' \in B'$, $3w' = 0$, and let $f: G \rightarrow G'$ be a mapping.

4.7. Lemma. The following conditions are equivalent:

- (i) f is an isomorphism of $G = G[+, B, w, 1]$ onto $G' = G'[+, B', w', 1]$.
- (ii) f is an isomorphism of $G(+)$ onto $G'(+)$, $f(B) = B'$ and $f(w) = w'$.

Proof. (i) implies (ii). Clearly, $f(0) = 0$ (f preserves left units). Further, let $b \in B$. If $f(b) \notin B'$, then $g(b) = f(b \cdot 0) = f(b) \cdot 0 = f(b) + w'$, a contradiction. Consequently, $f(B) \subseteq B'$ and, conversely, $f^{-1}(B') \subseteq B$, so that $f(B) = B'$. Now, for any $x \in G$, $f(b + x) = f(bx) = f(b)f(x) = f(b) + f(x)$. On the other hand, if $c \in C$, then $f(c + x + w) = f(cx) = f(c)f(x) = f(c) + f(x) + w'$ for every $x \in G$. In particular, $f(c + w) = f(c) + w'$ and $f(c + w + x) = f(c + w + x) = f(c + w) + f(x)$. We have proved that f is an isomorphism of $G(+)$ onto $G'(+)$. Finally, $f(w) = f(c \cdot (-c)) = f(c) - f(c) + w' = w'$. (ii) implies (i). This implication is evident.

Finally, we put $G[+, B, w, 2] = G[+, B, w, 1]^{\text{op}}$.

5. Auxiliary results

In this section, let $G(+)$ be an abelian group with at least six elements, let B be a subgroup of index two, $C = G - B$, and let $0 \neq w \in B$ be such that $3w = 0$. Further, let $v \in G$ be arbitrary.

Define a multiplication on G by $bb' = b + b' + v$, $cc' = c + c' + v - w$ and $bc = cb = b + c + w + v$ for all $b, b' \in B$, $c, c' \in C$. We get a groupoid which is a quasigroup and we denote it by $G = G[+, B, w, v, 3]$.

5.1. Lemma. (i) The quasigroup G is commutative.

- (ii) If $v \in B$, then $(-v) \cdot (-v) = -v$ and $-v$ is the only idempotent of G .
- (iii) If $v \in C$, then $(w - v)(w - v) = w - v$ and $w - v$ is the only idempotent of G .

- (iv) $r = (B \times B) \cup (C \times C)$ is a congruence of G and G/r is a two – element group.
(v) G is not an IP-quasigroup.

Proof. Easy.

5.2. Lemma. If $v \in B$, then the mapping $x \rightarrow x + v$ is an isomorphism of $G[+, B, w, v, 3]$ onto $G[+, B, w, 0, 3]$.

Proof. The assertion may be checked easily.

5.3. Lemma. If $v \in C$, then the mapping $x \rightarrow x + v - w$ is an isomorphism of $G[+, B, w, v, 3]$ onto $G[+, B, w, 0, 3]$.

Proof. The assertion may be checked easily.

We have proved that the quasigroups $G[+, B, w, v, 3]$ and $G[+, B, w, 3] = G[+, B, w, 0, 3]$ are isomorphic. In the rest of this section, we shall assume that $v = 0$.

5.4. Lemma. G is not medial.

Proof. For $c \in C, 0c \cdot 0c = (c + w)(c + w) = 2c + w \neq 2c - w = 0 \cdot (2c - w) = 00 \cdot cc$.

Put $g(b) = b$ and $g(c) = c + w$ for all $b \in B, c \in C$. Further, let $h(b) = b + w$ and $h(c) = c$. Then $L_b^+ g = g L_b^+$ and $L_c^+ h = g L_c^+$.

5.5. Lemma. $\mathcal{M}(G) = \{L_a^+, L_a^+ g, L_a^+ g^2; a \in G\}$.

Proof. Easy.

5.6. Lemma. $\mathcal{S}(G, 0) = \{1, g, g^2\}$ and $i(G) = 3$.

Proof. This follows from 4.5.

Finally, let B' be a subgroup of index 2 of an abelian group $G'(+)$, let $0 \neq w' \in B', 3w' = 0$, and let $f: G \rightarrow G'$ be a mapping.

5.7. Lemma. The following conditions are equivalent:

- (i) f is an isomorphism of $G = G[+, B, w, 3]$ onto $G' = G'[+, B', w', 3]$.
(ii) f is an isomorphism of $G(+)$ onto $G'(+)$, $f(B) = B'$ and $f(w) = w'$.

Proof. Similar to that of 4.7.

6. Auxiliary results

In this section, let $G(+)$ be an abelian group with at least six elements, let B be a subgroup of index two, $C = G - B$, and let $0 \neq w \in B$ be such that $3w = 0$. Further, let $v \in G$ be arbitrary.

Define a multiplication on G by $bb' = b + b' + v, cc' = c + c' + v, bc = b + c + v - w$ and $cb = b + c + v + w$ for all $b, b' \in B, c, c' \in C$. We get a groupoid $G = G[+, B, w, v, 4]$ which is a quasigroup.

- 6.1. Lemma.** (i) For $x, y \in G$, $xy = yx$ iff either $x, y \in B$ or $x, y \in C$.
(ii) $-v$ is the only idempotent of G .
(iii) G is neither a left nor a right loop.
(iv) $r = (B \times B) \cup (C \times C)$ is a congruence of G and G/r is a two – element group.
(v) G is neither an LIP-quasigroup nor an RIP-quasigroup.

Proof. Easy.

6.2. Lemma. Let $v \in B$. The mapping $x \rightarrow x + v$ is an isomorphism of $G[+, B, w, v, 4]$ onto $G[+, B, w, 0, 4]$.

Proof. Easy.

6.3. Lemma. Let $v \in C$. The mapping $x \rightarrow -x - v$ is an isomorphism of $G[+, B, w, v, 4]$ onto $G[+, B, w, 0, 4]$.

Proof. Easy.

In the rest of this section, we shall assume that $v = 0$.

6.4. Lemma. G is not medial.

Proof. Let $c \in C$. Then $00 \cdot cc = 0.2c = 2c - w \neq 2c - 2w = (c - w)(c - w) = 0c \cdot 0c$.

Put $g(b) = b$ and $g(c) = c + w$ for all $b \in B, c \in C$.

6.5. Lemma. $\mathcal{M}_l(G) = \mathcal{M}_r(G) = \mathcal{M}(G) = \{L_a^+, L_a^+g, L_a^+g^2; a \in G\}$.

6.6. Lemma. $\mathcal{I}(G, 0) = \{1, g, g^2\}$ and $i(G) = 3$.

Proof. See 6.5.

6.7. Lemma. The opposite quasigroup G^{op} is equal to $G[+, B, -w, 4]$. In particular G and G^{op} are isomorphic.

Proof. Obvious.

Finally, let B' be a subgroup of index 2 of an abelian group $G'(+)$, let $0 \neq w' \in B'$, $3w' = 0$, and let $f: G \rightarrow G'$ be a mapping.

6.8. Lemma. The following conditions are equivalent:

- (i) f is an isomorphism of $G = G[+, B, w, 4]$ onto $G' = G'[+, B', w', 4]$.
(ii) f is an isomorphism of $G(+)$ onto $G'(+)$, $f(B) = B'$ and $f(w) = w'$.

Proof. Similar to that of 4.7.

7. Quasigroups with $i(Q) \leq 3$

The following statements are well known.

7.1. Proposition. A quasigroup Q is medial iff there exist an abelian group $Q(+)$, commuting automorphisms g, h of $Q(+)$ and an element $e \in Q$ such that $xy =$

$= g(x) + h(y) + e$ for all $x, y \in Q$. In this case:

- (i) Q is commutative iff $g = h$;
- (ii) Q is a left (right) loop iff $h = \text{id}_Q$ ($g = \text{id}_Q$).
- (iii) Q is left (right) modular iff $g = h^2$ ($h = g^2$).
- (iv) Q is modular iff $g^3 = \text{id}_Q$ and $h = g^2$.
- (v) Q is left (right) permutable iff $h = \text{id}_Q$ ($g = \text{id}_Q$).
- (vi) If $g = h$, then Q satisfies the identity $x(y \cdot uv) = v(y \cdot ux)$ iff $g^2 = \text{id}_Q$.
- (vii) If $g = h$, then $g^3 = \text{id}_Q$ iff satisfies the identity $x(y(u \cdot vw)) = w(y(u \cdot vx))$.
- (viii) If $h = \text{id}_Q$, then $g^3 = \text{id}_Q$ iff Q satisfies the identity $(xy \cdot u)v = (vy \cdot u)x$.
- (ix) Q is an LIP – quasigroup (RIP – quasigroup) iff $h^2 = \text{id}_Q$ ($g^2 = \text{id}_Q$).
- (x) $\mathcal{S}(Q, 0)$ is just the permutation group generated by g and h .

7.2. Theorem. Let Q be a quasigroup.

- (i) $i(Q) = 1$ iff Q is an abelian group.
- (ii) $i(Q) = 2$ iff Q is not an abelian group and at least one (and then just) one of the following cases takes place:
 - (a) Q is a commutative medial quasigroup satisfying the identity $x(y \cdot uv) = v(y \cdot ux)$.
 - (b) Q is left modular and right permutable (then Q is a right loop).
 - (c) Q is right modular and left permutable (then Q is a left loop).

In all these cases, Q is a medial IP – quasigroup.

Proof. See 4.1 and [1, Theorem 4.6].

7.3. Theorem. The following conditions are equivalent for a quasigroup Q :

- (i) Q is medial and $i(Q) = 3$.
- (ii) Q is not an abelian group and at least one (then just one) of the following cases takes place:
 - (a) Q is commutative and satisfies the identity $x(y(u \cdot vw)) = w(y(u \cdot vx))$.
 - (b) Q is left permutable and satisfies the identity $(xy \cdot u)v = (vy \cdot u)x$ (then Q is a left loop).
 - (c) Q is right permutable and satisfies the identity $x(y \cdot uv) = v(y \cdot ux)$ (then Q is a right loop).
 - (d) Q is modular.

Proof. Apply 4.1.

7.4. Theorem. Let Q be a quasigroup such that Q is not medial and $i(Q) = 3$. Then there exist an abelian group $Q(+)$, its subgroup B of index 2 and an element $0 \neq w \in B$, $3w = 0$, such that Q is equal to at least one (and then to exactly one) from the quasigroups $Q[+, B, w, 1]$, $Q[+, B, w, 2]$, $Q[+, B, w, 3]$, $Q[+, B, w, 4]$.

Proof. Apply the results of the preceding sections.

7.5. Proposition. Let $G(+)$ be an abelian group with at least six elements, B its subgroup of index 2 and $0 \neq w \in B$, $3w = 0$. Then:

- (i) None of the quasigroups $G_j = G[+, B, w, j]$, $1 \leq j \leq 4$, is medial and $i(G_j) = 3$.
- (ii) G_1 is a left loop, G_2 is a right loop, G_3 is commutative, $G_4 \neq G_4^{\text{op}}$ and G_4 is isomorphic to G_4^{op} .
- (iii) None of the quasigroups G_1, G_2, G_3, G_4 is simple.
- (iv) $G[+, B, w, j]$ is isomorphic to $G'[+, B', w', j']$ iff $j = j'$ there and is an isomorphism $f: G(+) \rightarrow G'(+)$ such that $f(B) = B'$ and $f(w) = w'$.

Proof. Apply the results of the preceding sections.

Reference

- [1] КЕРКА Т., Multiplication groups of some quasigroups, Colloquia Math. Soc. J. Bolyai, 29 Univ. Algebra, Esztergom 1977, 459—465.