Acta Universitatis Carolinae. Mathematica et Physica

Tomáš Kepka; P. Němec

Quasigroups whose regular mappings are automorphisms

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 20 (1979), No. 1, 61--71

Persistent URL: http://dml.cz/dmlcz/142432

1979 ACTA UNIVERSITATIS CAROLINAE – MATHEMATICA ET PHYSICA VOL. 20, NO. 1, Pag. 61–71

Quasigroups Whose Regular Mappings Are Automorphisms

T. KEPKA and P. NĚMEC
Department of Mathematics, Charles University, Prague*)

Received 6 June 1978

The paper deals with regular mappings of quasigroups. First, several conditions are presented, under which all groups of regular mappings coincide. Further, quasigroups isotopic to a group (so called transitive quasigroups) are investigated and quasigroups which are left (right) linear over a group are characterized via regular mappings. For example, it is shown that a quasigroup is linear over an Abelian group iff it is transitive and all groups of regular mappings coincide. The main emphasis is on transitive quasigroups such that some of their regular mappings are automorphisms. Several classes of such quasigroups are decsribed via groups and their automorphisms. It is also shown that if all regular mappings of Q are automorphisms then Q is medial. The class of such quasigroups having at least one idempotent coincicdes with the class of idempotent medial quasigroups.

В статье изучены регулярные подстановки квазигрупп. Приведены некоторые условия, при выполнении которых все группы регулярных подстановок совпадают. Исследуются тоже транзитивные квазигруппы, т. е. квазигруппы изотопные группам. Показано например, что квазигруппа линейна над абелевой группой тогда и только тогда, если она транзитивна и все группы регулярных подстановок совпадают. Главной частью работы является изучение транзитивных квазигрупп, для которых некоторые регулярные подстановки являются автоморфизмами. Некоторые классы таких квазигрупп описаны при помощи групп и их автоморфизмов. Доказывается тоже, что если все регулярные достановки являются автоморфизмами, то квазигруппа уже медиальна. Класс таких квазигрупп содержащих по крайней мере один идемпотент совпадает с классом всех медиальных идемпотентных квазигрупп.

Článek se zabývá studiem regulárních zobrazení kvazigrup a podmínek, za nichž všechny grupy regulárních zobrazení dané kvazigrupy splývají. Kvazigrupy, které jsou zleva (zprava) lineární nad grupou, jsou popsány pomocí regulárních zobrazení. Vyšetřují se rovněž kvazigrupy, jejichž regulární zobrazení jsou automorfismy. Je dokázáno například, že každá tranzitivní kvazigrupa taková, že všechna regulární zobrazení jsou automorfismy, je už nutně mediální. Třída těchto kvazigrup obsahujících aspoň jeden idempotent je totožná s třídou všech idempotentních mediálních kvazigrup.

*) 186 00 Praha 8, Sokolovská 83, Czechoslovakia

1. Introduction

If M is a set then $P(M)$ (resp. $S(M)$) denotes the semigroup (resp. group) of all mappings (resp. bijective mappings) of M into M.

Let Q be a quasigroup and $a \in Q$. We put $L_a(b) = ab$ and $R_a(b) = ba$ for every $b \in Q$. Then $L_a, R_a \in S(M)$ and the group generated by all permutations L_a (resp. R_a), $a \in Q$, will be denoted by $G_l(Q)$ (resp. $G_r(Q)$). The group generated by $G_l(Q) \cup G_r(Q)$ will be denoted by $G(Q)$ and the automorphism group of Q by Aut Q. In case the operation on Q is written additively, we shall use symbols L_a^+, R_a^+, $G_l(Q(+))$ etc. Further we put

$$\begin{aligned}
L(Q) &= \{(f, g) \mid f, g \in P(Q),\ \ f(ab) = g(a)b \ \text{ for all } \ a, b \in Q\}\,,\\
R(Q) &= \{(f, g) \mid f, g \in P(Q),\ \ f(ab) = ag(b) \ \text{ for all } \ a, b \in Q\}\,,\\
M(Q) &= \{(f, g) \mid f, g \in P(Q),\ \ f(a)b = ag(b) \ \text{ for all } \ a, b \in Q\}\,,\\
L_l(Q) &= \{f \in P(Q) \mid \text{ there is } g \in P(Q) \text{ such that } (f, g) \in L(Q)\}\,,\\
L_r(Q) &= \{g \in P(Q) \mid \text{ there is } f \in P(Q) \text{ such that } (f, g) \in L(Q)\}\,.
\end{aligned}$$

Similarly we define $R_l(Q)$, $R_r(Q)$, $M_l(Q)$, $M_r(Q)$. We shall say that Q satisfies condition (C) if $L_l(Q) = L_r(Q) = R_l(Q) = R_r(Q) = M_l(Q) = M_r(Q)$.

1.1 Lemma. Let Q be a quasigroup, $a \in Q$ and $f, g \in P(Q)$. Then

(i) if $(f, g) \in L(Q)$ then $f = L_{g(a)}L_a^{-1}$, $g = R_a^{-1}fR_a$;

(ii) if $(f, g) \in R(Q)$ then $f = R_{g(a)}R_a^{-1}$, $g = L_a^{-1}fL_a$;

(iii) if $(f, g) \in M(Q)$ then $f = R_{g(a)}R_a^{-1}$, $g = L_a^{-1}L_{f(a)}$;

(iv) $L(Q)$, $R(Q)$ are subgroups of $S(Q)$ and $M(Q)$ is a subgroup of $S(Q) \times S(Q)^o$, where $S(Q)^o$ is the opposite group of $S(Q)$;

(v) if $(f, g) \in L(Q) \cup R(Q) \cup M(Q)$ then each of f, g uniquely determines the other;

(vi) $L_l(Q) \cong L_r(Q)$, $R_l(Q) \cong R_r(Q)$, $M_l(Q) \cong M_r(Q)$;

(vii) if either $f \in L_l(Q)$, $g \in R_l(Q)$ or $f \in L_r(Q)$, $g \in M_l(Q)$ or $f \in R_r(Q)$, $g \in M_r(Q)$ then $fg = gf$.

Proof. (i) – (iv) follow immediately from the definitions, (v) is a consequence of (i)–(iii) and (vi) follows from (iv), (v). (vii) If $f \in L_l(Q)$, $g \in R_l(Q)$ then there are $h, k \in S(Q)$ such that $(f, h) \in L(Q)$, $(g, k) \in R(Q)$. Hence for all $x, y \in Q$, $fg(xy) = f(xk(y)) = h(x)k(y) = g(h(x)y) = gf(xy)$. The rest is similar.

1.2 Lemma. Let Q be a quasigroup and $f, g, h \in P(Q)$. Then

(i) if $(f, g) \in L(Q)$ then $(f, h) \in R(Q)$ iff $(g, h) \in M(Q)$;

(ii) if $(f, g) \in R(Q)$ then $(f, h) \in L(Q)$ iff $(h, g) \in M(Q)$;

(iii) if $(f, g) \in M(Q)$ then $(h, f) \in L(Q)$ iff $(h, g) \in R(Q)$.

Proof. Obvious.

1.3 Corollary. Let Q be a quasigroup. Then

(i) $L_l(Q) \subseteq R_l(Q)$ iff $L_r(Q) \subseteq M_l(Q)$;
(ii) $R_l(Q) \subseteq L_l(Q)$ iff $R_r(Q) \subseteq M_r(Q)$;
(iii) $M_l(Q) \subseteq L_r(Q)$ iff $M_r(Q) \subseteq R_r(Q)$.

1.4 Corollary. A quasigroup Q satisfies (C) iff $L_l(Q) = R_l(Q) = L_r(Q)$ and $M_l(Q) = M_r(Q) \subseteq L_r(Q)$.

1.5 Lemma. Let Q be a quasigroup. Then
(i) if Q is commutative then $L_l(Q) = R_l(Q)$ and $L_r(Q) = R_r(Q) \subseteq M_l(Q) = M_r(Q)$;
(ii) if Q is a left loop then $R_l(Q) = R_r(Q)$;
(iii) if Q is a right loop then $L_l(Q) = L_r(Q)$;
(iv) if Q is a loop then $M_l(Q) = M_r(Q)$;
(v) if Q is an IP-quasigroup then $L_l(Q) = L_r(Q) = M_r(Q)$ and $R_l(Q) = M_l(Q) = R_r(Q)$;
(vi) if Q is unipotent then $M_l(Q) = M_r(Q)$.

Proof. The assertions (i)–(iv) are obvious and (v) follows from [4], Lemma 2.13
(vi) If Q is unipotent and $(f, g) \in M(Q)$ then for every $x \in Q$, $xx = f(x)f(x) = xgf(x)$, and hence $f = g^{-1}$.

1.6 Corollary. A commutative quasigroup Q satisfies (C) iff $L_l(Q) = L_r(Q)$ and $M_l(Q) \subseteq L_r(Q)$.

1.7 Corollary. A loop Q satisfies (C) iff $L_l(Q) = R_l(Q)$ and $M_l(Q) \subseteq L_l(Q)$.

1.8 Corollary. A commutative loop Q satisfies (C) iff $M_l(Q) \subseteq L_l(Q)$.

1.9 Corollary. An IP-quasigroup Q satisfies (C), provided at least one of the following conditions holds:
(i) $M_r(Q) = M_l(Q)$.
(ii) $L_l(Q) = R_l(Q)$.
(iii) Q is commutative.
(iv) Q is unipotent.

1.10 Proposition. Every WA-quasigroup satisfies condition (C).

Proof. See [3].

1.11 Lemma. Let Q be a quasigroup and $f, g, \in P(Q)$. Then
(i) if $(f, g) \in L(Q)$ and $f \in \operatorname{Aut} Q$ then $(gf^{-1}, f) \in M(Q)$;
(ii) if $(f, g) \in L(Q)$ and $g \in \operatorname{Aut} Q$ then $(f^{-1}g, g) \in R(Q)$;
(iii) if $(f, g) \in R(Q)$ and $f \in \operatorname{Aut} Q$ then $(f, gf^{-1}) \in M(Q)$;
(iv) if $(f, g) \in R(Q)$ and $g \in \operatorname{Aut} Q$ then $(f^{-1}g, g) \in L(Q)$;
(v) if $(f, g) \in M(Q)$ and $f \in \operatorname{Aut} Q$ then $(f, gf) \in R(Q)$;
(vi) if $(f, g) \in M(Q)$ and $g \in \operatorname{Aut} Q$ then $(g, fg) \in L(Q)$.

Proof. (i) For all $a, b \in Q$, $af(b) = ff^{-1}(a)f(b) = f(f^{-1}(a)\, b) = gf^{-1}(a)\, b$.
(ii) For all $a, b \in Q$, $f(ag(b)) = g(a)g(b) = g(ab)$ and hence $f^{-1}g(ab) = ag(b)$.
The rest is similar.

1.12 Corollary. Let Q be a quasigroup. Then $L_1(Q) \cap \text{Aut } Q = M_r(Q) \cap \cap \text{Aut } Q$, $L_r(Q) \cap \text{Aut } Q = R_r(Q) \cap \text{Aut } Q$ and $R_1(Q) \cap \text{Aut } Q = M_1(Q) \cap \cap \text{Aut } Q$.

We shall say that a quasigroup Q satisfies condition (L1A) if $L_1(Q) \subseteq \text{Aut } Q$, and similarly (LrA), etc. Further, we shall say that Q satisfies (A) if it satisfies all six conditions (L1A), (LrA), (R1A), (RrA), (M1A), (MrA).

1.13 Lemma. If Q satisfies (A) then $L_1(Q) = M_r(Q)$, $L_r(Q) = R_r(Q)$ and $R_1(Q) = M_1(Q)$.

Proof. The assertion is an immediate consequence of 1.12.

1.14 Corollary. Let Q be a quasigroup satisfying (A). Then Q satisfies (C), provided at least one of the following conditions holds:

(i) $L_1(Q) = R_1(Q)$ and $M_1(Q) \subseteq L_r(Q)$.
(ii) Q is commutative and $M_1(Q) \subseteq L_r(Q)$.
(iii) Q is unipotent and $M_1(Q) \subseteq L_r(Q)$.
(iv) Q is a loop.
(v) Q is an IP-quasigroup.

A quasigroup Q is called left (right) distributive if $a(bc) = (ab)(ac)$ ($(bc)a = = (ba)(ca)$) for all $a, b, c \in Q$.

1.15 Lemma. Let Q be a quasigroup. Then

(i) if Q is left distributive then Q satisfies (L1A) and (MrA);
(ii) if Q is right distributive then Q satisfies (R1A) and (M1A);
(iii) if Q is distributive then Q satisfies (A).

Proof. Obviously, if Q is left (right) distributive then $G_1(Q) \subseteq \text{Aut } Q$ ($G_r(Q) \subseteq \text{Aut } Q$). Now it suffices to use 1.1.

In the following five lemmas we suppose that $Q(+)$ is a group with unit element 0 and $u \in S(Q)$. Further, we denote $G_1 = G_1(Q)+))$ and $G_r = G_r(Q(+))$.

1.16 Lemma. Let f, g, h, F, G be mappings of Q into Q such that, for all $x \in Q$, $F(x) = f(x) - f(0)$ and $G(x) = -f(0) + f(x)$. Then

(i) if $f(x + y) = g(x) + h(y)$ for all $x, y \in Q$ then F, G are endomorphisms of $Q(+)$;
(ii) if $f(x + y) = g(y) + h(x)$ for all $x, y \in Q$ then F, G are antiendomorphisms of $Q(+)$.

Proof. (i) Obviously, for every $x, y \in Q$, $f(x) = g(x) + h(0)$ and $f(y) = = g(0) + h(y)$, hence $f(x + y) = g(x) + h(0) - h(0) - g(0) + g(0) + h(y) = = f(x) - (g(0) + h(0)) + f(y) = f(x) - f(0) + f(y)$ and the assertion immediately follows.

(ii) Similarly, $f(x + y) = f(y) - f(0) + f(x)$.

1.17 Lemma. The following are equivalent:

(i) $u^{-1}G_1u = G_1$.

(ii) $u^{-1}G_1u \subseteq G_1$.

(iii) $G_1 \subseteq u^{-1}G_1u$.

(iv) There are $p \in \operatorname{Aut} Q(+)$ and $g \in Q$ such that $u^{-1} = R_g^+ p$.

(v) There are $q \in \operatorname{Aut} Q(+)$ and $h \in Q$ such that $u = R_h^+ q$.

Proof. The implications (i) $\Rightarrow$ (ii) and (i) $\Rightarrow$ (iii) are obvious. (ii) $\Rightarrow$ (iv) There is a mapping $p : Q \to Q$ such that, for every $a \in Q$, $u^{-1}L_a^+u = L_{p(a)}^+$. Hence, for all $a, b \in Q$, $u^{-1}(a + b) = p(a) + u^{-1}(b)$ and $p(a) = u^{-1}(a) - u^{-1}(0)$. Obviously, p is a permutation and $u^{-1} = R_{u^{-1}(0)}^+ p$. However $p \in \operatorname{Aut} Q(+)$ by 1.16. (iv $\Rightarrow$ (v) Since $p \in \operatorname{Aut} Q(+)$, we have $u = p^{-1}R_{u^{-1}(0)}^{+} = R_{p^{-1}u^{-1}(0)}^{+}p^{-1}$.
(v) $\Rightarrow$ (i) For each $a, b \in Q$, $u^{-1}L_a^+u(b) = q^{-1}R_h^{-1}L_a^+R_h^+q(b) = q^{-1}(a + q(b) + h - h) = q^{-1}(a) + b = L_{q^{-1}(a)}^{+}(b)$ and $L_a^+ = u^{-1}L_{q(a)}^{+}u$.
(iii) $\Rightarrow$ (i) We have already proved that (ii) implies (i) and it suffices to take u^{-1} instead of u.

1.18 Lemma. The following are equivalent:

(i) $u^{-1}G_ru = G_r$.

(ii) $u^{-1}G_ru \subseteq G_r$.

(iii) $G_r \subseteq u^{-1}G_ru$.

(iv) There are $p \in \operatorname{Aut} Q(+)$ and $g \in Q$ such that $u^{-1} = L_g^+ p$.

(v) There are $q \in \operatorname{Aut} Q(+)$ and $h \in Q$ such that $u = L_h^+ q$.

Proof. Similar to that of 1.17.

1.19 Lemma. The following are equivalent:

(i) $u^{-1}G_1u = G_r$.

(ii) $u^{-1}G_1u \subseteq G_r$.

(iii) $G_r \subseteq u^{-1}G_1u$.

(iv) There are $g \in Q$ and an antiautomorphism p of $Q(+)$ such that $u^{-1} = L_g^+ p$.

(v) There are $h \in Q$ and an antiautomorphism q of $Q(+)$ such that $u = R_h^+ q$.

Proof. The implications (i) $\Rightarrow$ (ii), (i) $\Rightarrow$ (iii), (iv) $\Rightarrow$ (v) and (v $\Rightarrow$ (i) are very easy. (ii) $\Rightarrow$ (iv) For every $a \in Q$, $u^{-1}L_a^+u = R_{p(a)}^+$. Hence, for all $a, b \in Q$, $u^{-1}(a + b) = u^{-1}(b) + p(a)$ and $u^{-1}(a) = u^{-1}(0) + p(a)$. The rest follows by 1.16.
(iii) $\Rightarrow$ (v) For all $a, b \in Q$, $R_a^+ = u^{-1}L_{q(a)}^{+}u$, hence $uR_a^+u^{-1}u(b) = L_{q(a)}^{+}u(b)$, so that $u(b + a) = p(a) + u(b)$ and $u(a) = p(a) + u(0)$. Now we can use 1.16.

1.20 Lemma. The following are equivalent:

(i) $G_1 = G_r$.

(ii) $G_1 \subseteq G_r$.

(iii) $G_r \subseteq G_1$.

(iv) $Q(+)$ is commutative.

Proof. Obvious.

2. Transitive Quasigroups

The following proposition is well-known (see e.g. [1], Theorem 7).

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

(i) At least one of the groups $L_l(Q), L_r(Q), R_l(Q), R_r(Q), M_l(Q), M_r(Q)$ operates transitively on Q.

(ii) Each of the groups $L_l(Q), L_r(Q), R_l(Q), R_r(Q), M_l(Q), M_r(Q)$ operates transitively on Q.

(iii) Q is isotopic to a group.

Every quasigroup satisfying the equivalent conditions of the proceding proposition is called transitive. A quasigroup Q is said to be left linear (right linear) if there are a group $Q(+)$, $f \in \operatorname{Aut} Q(+)$ and $g \in S(Q)$ such that $ab = f(a) + g(b)$ ($ab = g(a) + f(b)$) for all $a, b \in Q$. Finally, Q is called linear if it is both left and right linear.

2.2 Lemma. The following conditions for a quasigroup Q are equivalent:

(i) Q is linear.

(ii) There are a group $Q(+)$, $e \in Q$ and $f, g \in \operatorname{Aut} Q(+)$ such that $ab = f(a) + g(b) + e$ for all $a, b \in Q$.

(iii) There are a group $Q(+)$, $e \in Q$ and $f, g \in \operatorname{Aut} Q(+)$ such that $ab = f(a) + e + g(b)$ for all $a, b \in Q$.

(iv) There are a group $Q(+)$, $e \in Q$ and $f, g \in \operatorname{Aut} Q(+)$ such that $ab = e + f(a) + g(b)$ for all $a, b \in Q$.

Proof. Obvious.

2.3 Lemma. Let Q be a quasigroup, $Q(+)$ be a group, $u, v \in S(Q)$ and $a, b, c \in Q$ be such that $xy = a + u(x) + b + v(y) + c$ for all $x, y \in Q$. Then

(i) if $u \in \operatorname{Aut} Q(+)$ then Q is left linear;

(ii) if $v \in \operatorname{Aut} Q(+)$ then Q is right linear.

Proof. Obvious.

2.4 Lemma. Let Q be a quasigroup and $f, g \in S(Q)$. Let further $Q(+)$ be a group and $u, v \in S(Q)$ be such that $ab = u(a) + v(b)$ for all $a, b \in Q$. Then

(i) $(f, g) \in L(Q)$ iff there is $e \in Q$ such that $f = L_e^+$ and $g = u^{-1}L_e^+u$;

(ii) $(f, g) \in R(Q)$ iff there is $e \in Q$ such that $f = R_e^+$ and $g = v^{-1}R_e^+v$;

(iii) $(f, g) \in M(Q)$ iff there is $e \in Q$ such that $f = u^{-1}R_e^+u$ and $g = v^{-1}L_e^+v$.

Proof. (i) Let $(f, g) \in L(Q)$. Then $f(ab) = f(u(a) + v(b)) = ug(a) + v(b)$ for all $a, b \in Q$. Hence $fu(a) = ug(a)$ and $f(a + b) = f(a) + b$ for all $a, b \in Q$. Now it suffices to put $e = f(0)$. Conversely, for all $e, a, b \in Q$, $L_e^+(ab) = e + u(a) + v(b) = uu^{-1}(e + u(a)) + v(b) = u^{-1}L_e^+u(a)\, b$.

(ii) Similarly as for (i).
(iii) Let $(f, g) \in M(Q)$. Then $uf(a) + v(b) = u(a) + vg(b)$ for all $a, b \in Q$, hence $uf(a) = u(a) + e$, where $e = vgv^{-1}(0)$, and consequently $vg(b) = ufu^{-1}(0) + v(b) = e + v(b)$. Conversely, for all $e, a, b \in Q$, $u^{-1}R_e^+u(a)\, b = u(a) + e + v(b) = u(a) + vv^{-1}(e + v(b)) = av^{-1}L_e^+v(b)$.

2.5 Corollary. Let Q be a quasigroup, $Q\,(+)$ be a group and $u, v \in S(Q)$ be such that $ab = u(a) + v(b)$ for all $a, b \in Q$. Then $L_1(Q) = G_1(Q(+))$, $L_r(Q) = u^{-1}G_1(Q(+))\, u$, $R_1(Q) = G_r(Q(+))$, $R_r(Q) = v^{-1}G_r(Q(+))\, v$, $M_1(Q) = u^{-1}G_r(Q(+))\, u$ and $M_r(Q) = v^{-1}G_1(Q(+))\, v$.

2.6 Proposition. The following conditions are equivalent for a transitive quasigroup Q:
(i) Q is left linear.
(ii) $L_1(Q) \subseteq L_r(Q)$.
(iii) $L_r(Q) \subseteq L_1(Q)$.
(iv) $R_1(Q) \subseteq M_1(Q)$.
(v) $M_1(Q) \subseteq R_1(Q)$.

Proof. By 1.17, 1.18, 2.3 and 2.5.

2.7 Proposition. The following conditions are equivalent for a transitive quasigroup Q:
(i) Q is right linear.
(ii) $R_r(Q) \subseteq R_1(Q)$.
(iii) $R_1(Q) \subseteq R_r(Q)$.
(iv) $L_1(Q) \subseteq M_r(Q)$.
(v) $M_r(Q) \subseteq L_1(Q)$.

Proof. By 1.17, 1.18, 2.3 and 2.5.

2.8 Corollary. The following conditions are equivalent for a quasigroup Q:
(i) Q is linear.
(ii) Q is transitive and $L_1(Q) \subseteq L_r(Q) \cap M_r(Q)$.
(iii) Q is transitive and $L_r(Q) \cup M_r(Q) \subseteq L_1(Q)$.
(iv) Q is transitive and $R_1(Q) \subseteq R_r(Q) \cap M_1(Q)$.
(v) Q is transitive and $R_r(Q) \cup M_1(Q) \subseteq R_1(Q)$.

2.9 Proposition. The following conditions are equivalent for a transitive quasigroup Q:
(i) There are a group $Q(+)$, $v \in S(Q)$ and an antiautomorphism u of $Q(+)$ such that $ab = u(a) + v(b)$ for all $a, b \in Q$.
(ii) $L_r(Q) \subseteq R_1(Q)$.
(iii) $R_1(Q) \subseteq L_r(Q)$.
(iv) $L_1(Q) \subseteq M_1(Q)$.
(v) $M_1(Q) \subseteq L_1(Q)$.

Proof. It follows immediately by 1.19, 2.5 and the analogue of 2.3 for antiautomorphisms.

2.10 Proposition. The following conditions are equivalent for a transitive quasigroup Q:

(i) There are a group $Q(+)$, $u \in S(Q)$ and an antiautomorphism v of $Q(+)$ such that $ab = u(a) + v(b)$ for all $a, b \in Q$.
(ii) $L_1(Q) \subseteq R_r(Q)$. (iii) $R_r(Q) \subseteq L_1(Q)$.
(iv) $M_r(Q) \subseteq R_1(Q)$. (v) $R_1(Q) \subseteq M_r(Q)$.

Proof. Similar to that of 2.9.

A quasigroup Q is called c-transitive if it is isotopic to an Abelian group. Linear c-transitive quasigroup is called T-quasigroup. By Toyoda's theorem, every medial quasigroup, i.e. quasigroup satisfying the identity $(ab)(cd) = (ac)(bd)$, is a T-quasigroup.

2.11 Proposition. The following conditions are equivalent for a quasigroup Q:
(i) Q is c-transitive.
(ii) Q is transitive and $L_1(Q) \subseteq R_1(Q)$.
(iii) Q is transitive and $R_1(Q) \subseteq L_1(Q)$.
(iv) Q is transitive and $L_r(Q) \subseteq M_1(Q)$.
(v) Q is transitive and $M_1(Q) \subseteq L_r(Q)$.
(vi) Q is transitive and $R_r(Q) \subseteq M_r(Q)$.
(vii) Q is transitive and $M_r(Q) \subseteq R_r(Q)$.

Proof. Apply 1.20 and 2.5.

2.12 Proposition. The following conditions are equivalent for a quasigroup Q:
(i) Q is a T-quasigroup.
(ii) Q is transitive and satisfies (C).
(iii) Q is a left linear c-transitive quasigroup and $M_1(Q) \subseteq M_r(Q)$.
(iv) Q is a left linear c-transitive quasigroup and $M_r(Q) \subseteq M_1(Q)$.
(v) Q is a right linear c-transitive quasigroup and $M_1(Q) \subseteq M_r(Q)$.
(vi) Q is a right linear c-transitive quasigroup and $M_r(Q) \subseteq M_1(Q)$.

Proof. (i) $\Rightarrow$ (ii) It follows from 1.4, 2.6, 2.7 and 2.11. (ii) $\Rightarrow$ (iii) This is obvious with respect to 2.6 and 2.11. (iii) $\Rightarrow$ (i) By 2.6 and 2.11, $M_1(Q) = L_1(Q)$. Now it sufficies to use 2.7.
The rest is similar.

3. Regular Mappings and Automorphisms

3.1 Proposition. The following conditions are equivalent of a quasigroup Q:
(i) Q is transitive and satisfies (L1A).
(ii) There are a group $Q(+)$, $p \in \mathrm{Aut}\, Q(+)$ and $g \in Q$ such that $ab = a + g - p(a) + p(b)$ for all $a, b \in Q$ and the mapping $a \mapsto a + g - p(a)$ is a permutation.
(iii) Q is transitive and satisfies (MrA).

Proof. (i) $\Rightarrow$ (ii) Since Q is transitive, there are a group $Q(+)$ and $u, v \in S(Q)$ such that $ab = u(a) + v(b)$ for all $a, b \in Q$. According to (L1A) and 2.5, $a + u(b) + v(c) = u(a + b) + v(a + c)$ for all $a, b, c \in Q$. Taking $b = 0$, we have $v(a + c) = - u(a) + a + u(0) + v(c)$ and hence $p = L^{\pm}_{v(0)} v \in \text{Aut}\, Q(+)$ by 1.16. Finally, takking $b = 0$ and $c = - a$, we have $u(a) + v(0) = a + u(0) + + v(- a) = a + u(0) + v(0) - p(a)$. (ii) $\Rightarrow$ (iii) Since Q is right linear, $M_r(Q) = L_1(Q)$ by 2.7. Further, $a + bc = a + b + g + p(- b) + p(c) = a + b + g + + p(- b - a) + p(a + c) = a(+ b)(a + c)$ for all $a, b, c \in Q$ and (L1A) follows immediately by 2.5.
(iii) $\Rightarrow$ (i) By 1.12, $M_r(Q) \subseteq L_1(Q)$ and hence $M_r(Q) = L_1(Q)$ by 2.7.

3.2 Proposition. The following conditions are equivalent for a quasigroup Q:
(i) Q is transitive and satisfies (R1A).
(ii) There are a group $Q(+)$, $q \in \text{Aut}\, Q(+)$ and $h \in Q$ such that $ab = = q(a) - q(b) + h + b$ for all $a, b \in Q$ and the mapping $a \mapsto - q(a) + h + a$ is a permutation.
(iii) Q is transitive and satisfies (M1A).

Proof. Dual to that of 3.1.

3.3 Proposition. The following conditions are equivalent for a quasigroup Q:
(i) Q is transitive and satisfies (A).
(ii) Q is transitive and satisfies (L1A) and (R1A).
(iii) Q is transitive and satisfies (MrA) and (R1A).
(iv) Q is transitive and satisfies (L1A) and (RrA).
(v) Q is transitive and satisfies (MrA) and (RrA).
(vi) Q is transitive and satisfies (LrA) and (R1A).
(vii) Q is transitive and satisfies (LrA) and (M1A).
(viii) Q is transitive and satisfies (L1A) and (M1A).
(ix) Q is transitive and satisfies (M1A) and (MrA).
(x) Q is right linear and satisfies (RrA).
(xi) Q is right linear and satisfies (M1A).
(xii) Q is right linear and satisfies (R1A).
(xiii) Q is left linear and satisfies (LrA).
(xiv) Q is left linear and satisfies (MrA).
(xv) Q is left linear and satisfies (L1A).
(xvi) There are an Abelian group $Q(+)$, $p \in \text{Aut}\, Q(+)$ and $g \in Q$ such that $ab = g + (1 - p)(a) + p(b)$ for all $a, b \in Q$.
In this case, Q is medial and satisfies (C).

Proof. (xii $\Rightarrow$ (xvi) There are a group $Q(+)$, $p \in \text{Aut}\, Q(+)$ and $u \in S(Q)$ such that $ab = u(a) + p(b)$ for all $a, b \in Q$. Now (R1A) yields $u(a) + p(b) + c = = u(a + c) + p(b) + p(c)$ for all $a, b, c \in Q$. Taking $a = b = 0$, we get $u(c) = = u(0) + c - p(c)$ and hence the mapping $c \mapsto c - p(c)$ is a permutation. Further, we

have $-u(0) + u(a) + p(b) + c = -u(0) + u(a + c) + p(b) + p(c)$, consequently $a - p(a) + p(c) + c = a + c - p(a + c) + p(b) + p(c)$, so that $-p(a) + p(b) + c - p(c) = c - p(c) - p(a) + p(b)$, and therefore $c - p(c) \in C(Q(+))$ for each $c \in Q$, Thus $Q(+) = C(Q(+))$ and $Q(+)$ is commutative.
(xv) ⇒ (xvi) Similarly as in the preceding implication we can show that there are a group $Q(+)$, $q \in \mathrm{Aut}\, Q(+)$ and $v \in S(Q)$ such that $ab = q(a) - q(b) + b + v(0)$, the mapping $a \mapsto -q(a) + a$ is a permutation and $-q(a) + a$ belongs to the center of $Q(+)$ for every $a \in Q$. Now it suffices to put $p = 1 - q$.
(xvi) ⇒ (i) Since $p(1 - p) = (1 - p)\, p$, Q is medial by Toyoda's theorem, and hence Q satisfies (C) by 2.12. Finally, Q satisfies (L1A) by 3.1.
The remaining implications are obvious with respect to 2.6, 2.7, 3.1 and 3.2.

3.4 Proposition. The following conditions are equivalent for a quasigroup Q:
(i) Q is left distributive and transitive.
(ii) Q is transitive, Q satisfies (MrA) and $\mathrm{Id}\, Q \neq 0$.
(iii) Q is transitive, Q satisfies (L1A) and $\mathrm{Id}\, Q \neq 0$.
(iv) There are a group $Q(+)$ and $p \in \mathrm{Aut}\, Q(+)$ such that $ab = a - p(a) + p(b)$ for all $a, b \in Q$.

Proof. (iii) ⇒ (iv) Let $e \in \mathrm{Id}\, Q$. Define $a + b = R_e^{-1}(a) L_e^{-1}(b)$ for all $a, b \in Q$. Since Q is transitive, $Q(+)$ is a group by Albert s theorem. Further, $a + e = e + a = a$ for each $a \in Q$, since e is idempotent. Now it suffices to use 3.1 together with its proof, observing that $g = ee = e$.
The remaining implications are obvious with respect to 1.15 and 3.1.

3.5 Proposition. The following conditions are equivalent for a quasigroup Q:
(i) Q is right distributive and transitive.
(ii) Q is transitive, Q satisfies (M1A) and $\mathrm{Id}\, Q \neq \emptyset$.
(iii) Q is transitive, Q satisfies (R1A) and $\mathrm{Id}\, Q \neq \emptyset$.
(iv) There are a group $Q(+)$ and $q \in \mathrm{Aut}\, Q(+)$ such that $ab = q(a) - q(b) + b$ for all $a, b \in Q$.

Proof. The same as above, using 3.2 instead of 3.1.

3.6 Proposition. The following are equivalent for a quasigroup Q:
(i) Q is medail and idempotent.
(ii) Q is transitive, $\mathrm{Id}\, Q \neq \emptyset$ and Q satisfies (A).
(iii) Q is transitive, $\mathrm{Id}\, Q \neq \emptyset$ and Q satisfies (L1A) and (R1A).
(iv) There are an Abelian group $Q(+)$ and $p \in \mathrm{Aut}\, Q(+)$ such that $ab = (1 - p)(a) + p(b)$ for all $a, b \in Q$.

Proof. Obviously, every medial idempotent quasigroup is distributive. Thus the only nontrivial implication is (iii) ⇒ (iv). However, (iii) implies that Q is isotopic to an Abelian group by 3.3 and it suffices to apply 3.4 and Albert's theorem.

References

[1] T. KEPKA: Regular mappings of groupoids, Acta Univ. Carolinae Math. et Phys. 12, 1 (1971), 25–37.

[2] T. KEPKA: L,R-transitive groupoids, Acta Univ. Carolinae Math. et Phys. 16, 2 (1975), 71–77.

[3] T. KEPKA: Structure of weakly abelian quasigroups, Czech. Math. J. 28 (1978), 181—188.

[4] T. KEPKA, P. NĚMEC: Unipotent quasigroups, Acta Univ. Carolinae Math. et Phys. 18, 2 (1977), 13–22.