Prace Naukowe Wyższej Szkoły Pedagogicznej w Częstochowie
Matematyka IV, Częstochowa 1998

Some classes of linear quasigroups

Petr Němec

Several important classes of quasigroups can be characterized by means of certain linear constructions (see e.g. [3], [4], [7], [8]). The first to investigate such linear quasigroups seems to be Toyoda [8] as early as in 1941, who showed that a quasigroup Q is medial iff there is an Abelian group $Q(+)$, two automorphisms f, g of Q and an element $a \in Q$ such that $fg = gf$ and $xy = f(x) + g(y) + a$ for all $x, y \in Q$. Further, Belousov [1] (and independently Soublin [7] showed that a quasigroup Q is distributive iff there is a commutative Moufang loop $Q(+)$ and an automorphism f of $Q(+)$ such that $1 - f$ is an automorphism, $f(x) + x \in C(Q(+))$ and $xy = f(x) + (1 - f)(y)$ for all $x, y \in Q$. As a further generalization in this direction, Kepka [3] proved that a quasigroup is trimedial (i.e., each subquasigroup generated by at most three elements is medial) iff there is a commutative Moufang loop $Q(+)$, two automorphisms f, g of $Q(+)$ and an element $a \in C(Q(+))$ such that $fg = gf$ and $xy = f(x) + g(y) + a$ for all $x, y \in Q$.

These results naturally suggest an idea of defining an *arithmetical form* of a quasigroup Q as a quadruple $(Q(+), f, g, a)$ such that $Q(+)$ is a commutative Moufang loop, f, g are automorphisms of $Q(+)$, $a \in Q$ and $xy = (f(x) + g(y)) + a$ for all $x, y \in Q$. We shall say that Q is a *linear quasigroup* if it has at least one arithmetical form. All possible arithmetical forms of a linear quasigroup were characterized in [5] and the structure of commutative Moufang loops occurring in different arithmetical forms of a linear quasigroup was investigated in [6]. This contribution is devoted to the description of some particular classes of linear quasigroups.

1 Preliminaries

Let Q be a groupoid. For each $a \in Q$ define transformations L_a and R_a of the set Q by $L_a(x) = ax$, $R_a(x) = xa$ for all $x \in Q$. These mappings are called *left translation (by a)* and *right translation (by a)*, respectively. We shall say that Q is

- *cancellable* if all left and right translations are injective,
- *divisible* if all left and right translations are projective,
- a *quasigroup* if all left and right translations are bijective (i.e., permutations of the set Q),
- a *loop* if Q is a quasigroup with neutral element (denoted by 1),
- *idempotent* if it satisfies the identity $\mathbf{xx} = \mathbf{x}$,
- *left distributive* if it satisfies the identity $\mathbf{x} \cdot \mathbf{y} = \mathbf{xy} \cdot \mathbf{xz}$,
- *right distributive* if it satisfies the identity $\mathbf{yz} \cdot \mathbf{x} = \mathbf{yx} \cdot \mathbf{zx}$,
- *distributive* if it is both left and right distributive,
- *left semimedial* if it satisfies the identity $\mathbf{xx} \cdot \mathbf{yz} = \mathbf{xy} \cdot \mathbf{xz}$,
- *right semimedial* if it satisfies the identity $\mathbf{yz} \cdot \mathbf{xx} = \mathbf{yx} \cdot \mathbf{zx}$,
- *semimedial* if it is both left and right semimedial,
- *medial* if it satisfies the identity $\mathbf{xy} \cdot \mathbf{uv} = \mathbf{xu} \cdot \mathbf{yv}$,
- *trimedial* if every subgroupoid of Q generated by at most 3 elements is medial.

Every left semimedial loop is commutative (the identity implies $xy \cdot x = xx \cdot y = x \cdot xy$ for all $x, y \in Q$ and the commutativity follows) and is called a *commutative Moufang loop*. The operation in a commutative Moufang loop Q will usually be denoted additively and in this case 0 will denote the neutral element of the loop $Q(+)$ and the element b such that $a + b = 0$ will be denoted by $-a$.

From now on, let $Q(+)$ be an additively written commutative Moufang loop. For all $a, b, c \in Q$, we define an element

$$[a, b, c] = ((a + b) + c) - (a + (b + c)),$$

so called *associator* of the elements a, b, c. Further, we define

$$C(Q(+)) = \{ a \in Q \mid [a, x, y] = 0 \text{ for all } x, y \in Q \}.$$

The set $C(Q(+))$ is called *center* of the loop $Q(+)$. It is well known (see e.g. [1] or [2]) that the subloop generated by any two elements of Q is a group, $C(Q(+))$ is a normal subloop of $Q(+)$ invariant under every automorphism of $Q(+)$, every congruence of $Q(+)$ is normal and $3x \in C(Q(+))$ for every

$x \in Q$. If $a, b, c \in Q$ then $[a, b, c] = -[b, a, c] = [b, c, a] = -[c, b, a] = [c, a, b] = -[a, c, b] = [a, a+b, c]$ and if $[a, b, c] = 0$ then the subloop of $Q(+)$ generated by the set $\{a, b, c\}$ is a group.

1.1 LEMMA. *Let $Q(+)$ be a commutative Moufang loop and $a, b, c, d \in Q$. The following conditions are equivalent:*

(i) $(a + b) + (c + d) = (a + c) + (b + d)$.

(ii) $[a - b, c - b, d - b] = 0$.

(iii) $[a - c, b - c, d - c] = 0$.

(iv) $[a - d, b - d, c - d] = 0$.

(v) $[b - a, c - a, d - a] = 0$.

PROOF. If (i) holds then, adding $-2b$ to both sides, we get $a+((c+d)-b) = ((a + c) - b) + d$ and, adding $-2b$ once more, we have $(a - b) + (((c + d) - b) - b)) = (((a+c) - b) - b) + (d - b)$. Since $((c+d) - b) - b = (c+d) - 2b = (c - b) + (d - b)$ and $((a + c) - b) - b = (a - b) + (c - b)$, this implies $(a-b)+((c-b)+(d-b)) = ((a-b)+(c-b)+(d-b)$ and hence (ii) holds. The converse implication can be proved by adding $2b$ twice and the rest is similar. □

1.2 COROLLARY. *Let $Q(+)$ be a commutative Moufang loop and $a, b, c, d \in Q$ be such that $(a + b) + (c + d) = (a + c) + (b + d)$. Then $(x + y) + (u + v) = (x + u) + (y + v)$ for all $x, y, u, v \in \{a, b, c, d\}$.* □

1.3 COROLLARY.. *Let $Q(+)$ be a commutative Moufang loop and $a, b \in Q$. The following conditions are equivalent:*

(i) $(a + b) + (x + y) = (a + x) + (b + y)$ *for all* $x, y \in Q$.

(ii) $(a + x) + (b + y) = (a + y) + (b + x)$ *for all* $x, y \in Q$.

(iii) $a - b \in C(Q(+))$. □

Let $m \in \mathbf{Z}$. A mapping $f : Q \longrightarrow Q$ is said to be *m-central* if $f(x) + mx \in C(Q(+))$ for every $x \in Q$. Further, we shall say that a transformation f of the set Q is *central* if it is k-central for some $k \in \mathbf{Z}$.

1.4 LEMMA. *Let $Q(+)$ be a commutative Moufang loop and $n \in \mathbf{Z}$, $n = 3k + m$, $m \in \{0, 1, 2\}$ and f be a transformation of the set Q. Then:*

(i) If f is n-central then f is m-central.

(ii) The mapping $x \to nx$ is a $(-m)$-central endomorphism of $Q(+)$.

(iii) If f is central and Q is not associative then there is exactly one $r \in \{0,1,2\}$ such that f is r-central.

PROOF. The assertion (i) follows from the fact that $3x \in C(Q(+))$ for every $x \in Q$ and (ii), (iii) are clear. □

1.5 LEMMA. *Let $Q(+)$ be a commutative Moufang loop, $m, n \in \mathbf{Z}$ and f, g be endomorphisms of the loop $Q(+)$ such that f is m-central and g is n-central. Then:*
(i) The endomorphism fg is $(-mn)$-central.
(ii) The mapping $f+g$, defined by $(f+g)(x) = f(x)+g(x)$ for every $x \in Q$, is an $(m+n)$-central endomorphism.
(iii) If f is an automorphism then f^{-1} is an m-central automorphism.

PROOF. Let $x, y \in Q$ be arbitrary elements.
(i) As $fg(x) + mg(x) \in C(Q(+))$ and $-g(mx) - nmx \in C(Q(+))$, we immediately get $fg(x) - nm(x) \in C(Q(+))$.
(ii) Put $a = -f(x) - mx$, $b = -g(x) - nx$, $c = -f(y) - my$, $d = -g(y) - ny$. Then $a, b, c, d \in C(Q(+))$ and $((f(x)+g(x))+(f(y)+(g(y)))+(a+b+c+d) = -mx-nx-my-ny = ((f(x)+f(y))+(g(x)+g(y)))+(a+b+c+d)$, so that $(f+g)(x)+(f+g)(y) = (f+g)(x+y)$. Further, $((f(x)+g(x))+(m+n)x)+(a+b) = 0$, however $a+b \in C(Q(+))$ and so $(f+g)(x)+(m+n)x \in C(Q(+))$.
(iii) With respect to 1.4(i), we can assume that $m \in \{0,1,2\}$. If $m = 0$ then $Q(+)$ is associative and there is nothing to prove. For $m = 1$ we have $f^{-1}(x) + x = f(f^{-1}(x)) + f^{-1}(x) \in C(Q(+))$, and if $m = 2$ then $x + 2f^{-1}(x) \in C(Q(+))$, hence $-x + f^{-1}(x) \in C(Q(+))$ and so $f^{-1} + 2x \in C(Q(+))$. □

2 Basic properties of linear quasigroups

An *arithmetical form* of a groupoid Q is a quadruple $(Q(+), f, g, a)$, where $Q(+)$ is a commutative Moufang loop (with the same underlying set as the groupoid Q), f, g are automorphisms of the loop $Q(+)$, $a \in Q$ and

$$xy = (f(x) + g(y)) + a$$

for all $x, y \in Q$. Obviously, a groupoid having at least one arithmetical form is a quasigroup and it is called *linear quasigroup*.

2.1 LEMMA. *Let $(Q(+), f, g, a)$ be an arithmetical form of a linear quasigroup Q. Then:*

(i) $a = 0 \cdot 0$, $f = R_{g^{-1}(a)}$, $g = L_{f^{-1}(a)}$.
(ii) $(x+y)+a = R^{-1}_{g^{-1}(a)}(x) \cdot L^{-1}_{f^{-1}(a)}(y)$ *for all* $x, y \in Q$.
(iii) $xy = (f(x)+2a)+(g(y)-a) = (f(x)-a)+(g(y)+2a)$ *for all* $x, y \in Q$.

PROOF. Since $3a \in C(Q(+))$, for all $x, y \in Q$ we have $xy + 3a = (f(x) + g(y)) + 4a = (f(x) + 2a) + (g(y) + 2a)$ and hence $xy = (xy + 3a) - 3a = (f(x) - a) + (g(x) + 2a) = (f(x) + 2a) + (g(x) - a)$. The rest is clear. □

Clearly, 2.1(ii) implies that the loop $Q(+)$ is an isotope of the quasigroup Q. Consequently, every loop isotopic to a linear quasigroup is a Moufang loop.

2.2 PROPOSITION. *Let* $(Q(+), f, g, a)$ *be an arithmetical form of a linear quasigroup* Q *and* ϱ *be a relation on the set* Q. *Then* ϱ *is a normal congruence of* Q *iff* ϱ *is a congruence of* $Q(+)$ *which is invariant with respect to* f, g, f^{-1}, g^{-1}.

PROOF. First, let ϱ be a normal congruence of Q. If $(x, y) \in \varrho$ then $(f(x), f(y)) \in \varrho$ and $(f^{-1}(x), f^{-1}(y)) \in \varrho$ and similarly for g. Further, using 2.1(ii), we have $(a + (x + z), a + (y + z)) \in \varrho$ for every $z \in Q$ and (taking $z = -2a$) also $(x - a, y - a) \in \varrho$. Since $x + z = (a + (x + z)) - a$ and $y + z = (a + (y + z)) - a$, we obtain $(x + z, y + z) \in \varrho$ for every $z \in Q$, i.e., ϱ is a congruence of $Q(+)$. The converse is straightforward. □

2.3 PROPOSITION. *The class* $\mathcal{L}$ *of all linear quasigroups is closed under cartesian products and (quasigroup) homomorphic images.*

PROOF. The fact that $\mathcal{L}$ is closed under homomorphic images follows from 2.2 and the rest is clear. □

2.4 PROPOSITION. *Let* $(Q(+), f, g, a)$ *be an arithmetical form of a linear quasigroup* Q. *Then* Q *is commutative iff* $f = g$.

PROOF. If Q is commutative then $f(x) + a = x \cdot 0 = 0 \cdot x = g(x) + a$ for every $x \in Q$ and hence $f = g$. The converse is clear. □

2.5 PROPOSITION. *Let* $(Q(+), f, g, a)$ *be an arithmetical form of a linear quasigroup* Q. *Then* Q *is idempotent iff* $a = 0$ *and* $f(x) + g(x) = x$ *for every* $x \in Q$.

PROOF. If Q is idempotent then $a = 0 \cdot 0 = 0$ and hence $f(x) + g(x) = xx = x$ for every $x \in Q$. The converse is obvious. □

2.6 PROPOSITION. *Let* $(Q(+), f, g, a)$ *be an arithmetical form of a linear quasigroup* Q. *Then* Q *is a loop iff* $f = g = \mathrm{id}_Q$. *In this case,* Q *is a commutative Moufang loop.*

PROOF. If Q is a loop with neutral element e then $g(e)+a=0\cdot e=0=e\cdot 0=f(e)+a$ and so $g(e)=f(e)=-a$. Consequently, for every $x\in Q$ we have $f(x)=f(x)+(-a+a)=(f(x)-a)+a=(f(x)+g(e))+a=xe=x=ex=(f(e)+g(x))+a=(g(x)-a)+a=g(x)$. Conversely, if $f=g=\mathrm{id}_Q$ then, for all $x,y\in Q$, we have $xy=(x+z)+a$ and hence $x\cdot(-a)=x=(-a)\cdot x$. Thus Q is a loop with neutral element $-a$ and, for all $x,y,z\in Q$, $xx\cdot yz=(((x+x)+a)+((y+z)+a))+a=(((x+x)+(y+z))+2a)+a=(((x+y)+(x+z))+2a)+a=(((x+y)+a)+((x+z)+a))+a=xy\cdot xz$. □

3 Semimedial linear quasigroups

3.1 PROPOSITION. *Let $(Q(+),f,g,a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is left semimedial.*

(ii) *Q is right semimedial.*

(iii) *Q is semimedial.*

(iv) *$fg=gf$ and fg^{-1} is a 2-central automorphism of the loop $Q(+)$.*

PROOF. For all $u,v,w\in Q$ we have

$$uu\cdot vw=(((f^2(u)+fg(U))+f(a))+((gf(v)+g^2(w))+g(a)))+a\ , \quad (1)$$

$$uv\cdot uw=(((f^2(u)+fg(v))+f(a))+((gf(u)+g^2(w))+g(a)))+a\ . \quad (2)$$

If (i) holds then, taking $u=0$, $w=-g^{-1}(a)$, we get $f(a)+gf(v)=fg(v)+f(a)$ and hence $fg=gf$. For arbitrary $x,y,z\in Q$ put $u=f^{-1}g^{-1}(x)$, $v=f^{-1}g^{-1}(y)$, $w=g^{-2}(z)$. Then

$$\begin{aligned}&((fg^{-1}(x)+x)+f(a))+((y+z)+g(a))=\\&=((fg^{-1}(x)+y)+f(a))+((x+z)+g(a)).\end{aligned} \quad (3)$$

Hence (taking $x=0$) $f(a)+((y+z)+g(a))=(y+f(a))+(z+g(a))$ for all $y,z\in Q$. Since $Q(+)$ is commutative, for all $u,v\in Q$ we have $(f(a)+u)+(g(a)+v)=(f(a)+v)+(g(a)+u)$ and consequently, using 1.2,

$$(f(a)+g(a))+(u+v)=(f(a)+u)+(g(a)+v)\ . \quad (4)$$

Hence the left-hand side of 3 is equal to $(f(a)+g(a))+((fg^{-1}(x)+x)+(y+z))$ and the right-hand side to $(f(a)+g(a))+((fg^{-1}(x)+y)+(x+z))$. Now, for all $x,y,z \in Q$,

$$(fg^{-1}(x)+x)+(y+z) = (fg^{-1}(x)+y)+(x+z)\ . \tag{5}$$

By 1.2, $fg^{-1}(x)-x \in C(Q(+))$, hence $fg^{-1}(x)+2x \in C(Q(+))$ and fg^{-1} is 2-central.

If (iv) holds then $f(x)-x \in C(Q(+))$ for every $x \in Q$ and, with respect to 1.2, 5 holds for all $x,y,z \in Q$. Since $fg^{-1} = g^{-1}f$, we have $g^{-1}f(a)-a \in C(Q(+))$, hence $f(a)-g(a) \in C(Q(+))$ and so, using 1.2 again, 4 holds for all $u,v \in Q$. Adding $f(a)+g(a)$ to both sides of 5 and using 4, we conclude that 3 holds for all $x,y,z \in Q$. If $u,v,w \in Q$ are arbitrary and $x = fg(u)$, $y = fg(v)$, $z = g^2(w)$ then 3 implies 1 and 2) $uu \cdot vw = uv \cdot uw$, i.e., Q is left semimedial.

The equivalence of (ii) and (iv) is an immediate consequence of the fact that Q is right semimedial iff $Q(*)$ is left semimedial, where $x * y = yx = (g(x)+f(y))+a$ for all $x,y \in Q$ (by 1.5(iii), the mapping $gf^{-1} = (fg^{-1})^{-1}$ is 2-central iff fg^{-1} is 2-central). □

3.2 PROPOSITION. *Let $(Q(+),f,g,a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is left distributive.*

(ii) *Q is right distributive.*

(iii) *Q is distributive.*

(iv) *$a = 0$, $f(x)+g(x) = x$ for every $x \in Q$ and fg^{-1} is 2-central.*

(v) *$a = 0$, $f(x)+g(x) = x$ for every $x \in Q$ and f is 1-central.*

PROOF. The equivalence of (i) – (iv) is an immediate consequence of 2.5 and 3.1, since Q is (left, right) distributive iff it is idempotent and (left, right) semimedial. If (iv) holds then $fg = gf$, $f^{-1}g = (g^{-1}f)^{-1}$ is 2-central and $f^{-1}g(x)+2x \in C(Q(+))$ for every $x \in Q$, hence $g(x)+2f(x) = x+f(x) \in C(Q(+))$ and f is 1-central. Conversely, if (v) holds then $2x+2f(x) \in C(Q(+))$ for every $x \in Q$, hence $2x-f(x) = x+(x-f(x)) = x+g(x) \in C(Q(+))$ and g is 1-central. By 1.5(i), fg^{-1} is 2-central. □

3.3 PROPOSITION. *Let $(Q(+),f,g,a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is medial.*

(ii) $fg = gf$ *and* $Q(+)$ *is an Abelian group.*

PROOF. For all $u, v, w, t \in Q$,

$$uv \cdot wt = (((f^2(u) + fg(v)) + f(a)) + ((gf(w) + g^2(t)) + g(a))) + a \,,$$

$$uw \cdot vt = (((f^2(u) + fg(w)) + f(a)) + ((gf(v) + g^2(t)) + g(a))) + a \,,$$

and hence Q is medial iff

$$\begin{aligned} &((f^2(u) + fg(v)) + f(a)) + ((gf(w) + g^2(t)) + g(a)) = \\ &= ((f^2(u) + fg(w)) + f(a)) + ((gf(v) + g^2(t)) + g(a)) \end{aligned} \tag{6}$$

for all $u, v, w, t \in Q$.

Suppose that (i) holds and $x, y, z \in Q$ are arbitrary. By 3.1, $fg = gf$ and $f(a) - g(a) \in C(Q(+))$. Taking $u = f^{-2}(x)$, $v = 0$, $w = g^{-1}f^{-1}(y)$, $t = g^{-2}(z)$, 6 yields

$$(x + f(a)) + ((y + z) + g(a)) = ((x + y) + f(a)) + (z + g(a)). \tag{7}$$

However $f(a) - g(a) \in C(Q(+))$, and so (with respect to 1.3) $(x + f(a)) + ((y+z)+g(a)) = (x+(y+z))+(f(a)+g(a))$, $((x+y)+f(a))+(z+g(a)) = ((x + y) + z) + (f(a) + g(a))$. Now 7 implies $x + (y + z) = (x + y) + z$ and the converse implication is obvious. □

4 Linear F–quasigroups

Let Q be a quasigroup. For every $x \in Q$, there are uniquely determined elements (called *local units*) e_x, f_x such that $xe_x = f_x x = x$. The quasigroup Q is called

- an *LF–quasigroup* if $x \cdot yz = xy \cdot e_x z$ for all $x, y, z \in Q$,
- an *RF–quasigroup* if $yz \cdot x = yf_x \cdot zx$ for all $x, y, z \in Q$,
- an *LE–quasigroup* if $x \cdot yz = f_x y \cdot xz$ for all $x, y, z \in Q$,
- an *RE–quasigroup* if $yz \cdot x = yx \cdot ze_x$ for all $x, y, z \in Q$.

4.1 PROPOSITION. *Let $(Q(+), f, g, a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is an LF–quasigroup.*

(ii) $fg = gf$, $a \in C(Q(+))$ *and* f *is 1-central.*

PROOF. For every $x \in Q$ we have $x = xe_x = (f(x) + g(e_x)) + a$ and hence $e_x = g^{-1}((x-a) - f(x)) = (g^{-1}(x) - g^{-1}(a)) - g^{-1}f(x)$. In particular, $e_0 = -g^{-1}(a)$. For all $u, v, w \in Q$ we have

$$u \cdot vw = (f(u) + ((gf(v) + g^2(w)) + g(a))) + a \tag{8}$$

$$uv \cdot e_u w = ((f^2(u) + fg(v)) + f(a)) + ((gf(e_u) + g^2(w)) + g(a))) + a \tag{9}$$

If (i) holds then (taking $u = 0$, $w = -g^{-1}(a)$) we have

$$gf(v) = (fg(v) + f(a)) - gfg^{-1}(a). \tag{10}$$

Hence (for $v = 0$) $f(a) = gfg^{-1}(a)$ and 10 yields $fg = gf$. For arbitrary $x, y, z \in Q$ put $u = f^{-1}(x)$, $v = f^{-1}g^{-1}(y)$, $w = g^{-2}(z)$. Then

$$x + ((y+z) + g(a)) = ((f(x)+y) + f(a)) + ((gf(e_{f^{-1}(x)}) + z) + g(a)). \tag{11}$$

Since $gf(e_{f^{-1}(x)}) = (x - f(a)) - f(x)$, we can rewrite 11 as

$$x + ((y+z) + g(a)) = ((f(x)+y) + f(a)) + ((((x - f(a)) - f(x)) + z + g(a)). \tag{12}$$

Taking $x = 0$, $v = z - f(a)$, we conclude that, for all $u, v \in Q$,

$$g(a) + (y + (f(a) + v)) = (f(a) + y) + (v + g(a)). \tag{13}$$

In particular, for $v = -f(a)$ we have $g(a) + u = (f(a) + u) + (g(a) - f(a))$ and hence 13 yields $g(a) + (y + (f(a) + v)) = (f(a) + y((f(a) + v) + (g(a) - f(a)))$. Writing again $z = v + f(a)$, we get $(f(a) + (g(a) - f(a)) + (y + z) = (f(a) + y) + (z + (g(a) - f(a))$ for all $y, z \in Q$. By 1.3, $f(a) - (g(a) - f(a)) = 2f(a) - g(a) \in C(Q(+))$, hence $-f(a) - g(a) \in C(Q(+))$ and, adding this element to both sides of 12, we get $x + ((y+z) - f(a)) = (f(a) + (f(x) + y)) + ((((x - f(a)) - f(x)) + z) - f(a))$. Adding $3f(a)$ and writing $u = z + f(a)$, for all $x, y, u \in Q$ we have

$$x + (u + (y + f(a))) = (f(a) + (f(x) + y)) + ((((x - f(a)) - f(x)) + f(a)) + u). \tag{14}$$

From this (taking $y = 0$ and $u = -f(a)$) $x = (f(a) + f(x)) + ((x - f(a)) - f(x))$, hence $x + (-f(a) - f(x)) = (x - f(a)) - f(x)$ and $[x, -f(a), -f(x)] = 0$. Thus the subloop of $Q(+)$ generated by the set $\{x, f(a), f(x)\}$ is associative and $[x, f(x) + f(a), f(a)] = 0$. Hence $((x - f(a)) - f(x)) + f(a) = 'x + (-f(x) - f(a))) + f(a) = x - f(x)$ and we can rewrite 12 in the form

$$x + (u + (y + f(a))) = (f(a) + (f(x) + y) + ((x - f(x)) + u). \tag{15}$$

Taking $y = -f(a)$, we have $x+u = f(x)+((x-f(x))+u)$, hence $(x+u)-f(x) = (x-f(x))+u$ and $[u, x, -f(x)] = 0$. Thus $[x, f(x0, u] = 0$ for all $x, u \in Q$. Further, taking $u = 0$ in 15, we get $x+(y+f(a)) = (f(a)+(f(x)+y))+(x-f(x))$ and hence $f(a)+(f(x)+y) = (x+(y+f(a))+(f(x)-x)$. Writing $v = y+f(a)$, 15 implies that $x+(u+v) = ((x+v)+(f(x)-x))+((x-f(x))+u)$. However $[x, f(x), x+v] = 0$, hence $(x+v)+(f(x)-x) = v+f(x)$ and $x+(u+v) = (v+f(x))+((x-f(x))+u)$. Since $u+v = v+u$, we get $(f(x)+v)+((x-f(x))+u) = (f(x)+u)+((x-f(x))+v)$. With respect to 1.3, $x-2f(x) \in C(Q(+))$, hence $x+f(x) \in C(Q(+))$ and f is 1-central. Adding central elements $-x-f(x)$ and $x+f(x)$ to both sides of 15, we get $x+(u+(y+f(a))) = (f(a)+(y-x))+(2x+u)$ and so (adding $-3x$) $(u-x)+((y+f(a))-x) = (f(a)+(y-x))+(u-x)$. Thus $(f(a)+y)-x = f(a)+(y-x)$ for all $x, y \in Q$, hence $f(a) \in C(Q(+))$ and so $a \in C(Q(+))$, since $C(Q(+))$ is invariant with respect to every automorphism of $Q(+)$.

Conversely, if (ii) holds then $(x-f(x))-f(x) \in C(Q(+))$ and (with respect to 1.3) $x+(y+z) = (f(x)+(x-f(x)))+(y+z) = (f(x)+y)+((x-f(x))+z)$. Since $f(a), g(a) \in C(Q(+))$, 12 and consequently 11 hold for all $x, y, z \in Q$. If $u, v, w \in Q$ are arbitrary and $x = f(u)$, $y = fg(v)$, $z = g^2(w)$ then 11 implies (see 9 and 8) $u \cdot vw = uv \cdot e_u w$. □

4.2 PROPOSITION. *Let $(Q(+), f, g, a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is an RF–quasigroup.*

(ii) *$fg = gf$, $a \in C(Q(+))$ and g is 1-central.*

PROOF. It suffices to use 4.1 for $Q(*)$, where $x * y = yx$ for all $x, y \in Q$. □

4.3 PROPOSITION. *Let $(Q(+), f, g, a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is an LE–quasigroup.*

(ii) *Q is an RF–quasigroup.*

(iii) *$fg = gf$, $a \in C(Q(+))$ and g is 1-central.*

PROOF. For every $x \in Q$, $x = f_x x = (f(f_x)+g(x))+a$ and so $f_x = (f^{-1}(x)-f^{-1}(a))-f^{-1}g(x)$. In particular, $f_0 = -f^{-1}(a)$. If $u, v, w \in Q$ are arbitrary then

$$u \cdot vw = (f(u)+((gf(v)+g^2(w))+g(a)))+a\,,$$

$$f_u v \cdot uw = (((f^2(f_u) + fg(v)) + f(a)) + ((gf(u) + g^2(w)) + g(a))) + a\,.$$

If (i) holds then, taking $u = 0$, $w = -g^{-1}(a)$, we immediately get $fg = gf$. For arbitrary $x, y, z \in Q$, put $u = f^{-1}(x)$, $v = f^{-1}g^{-1}(y)$, $w = g^{-2}(z)$. Then

$$x + ((y+z)+g(a)) = ((f^2(f_{f^{-1}(x)}+y)+f(a))+((g(x)+z)+g(a)). \quad (16)$$

Since $f^2(f_{f^{-1}(x)}) = (x - f(a)) - g(x)$, we can rewrite 15 in the form

$$x+((y+z)+g(a)) = ((((x-f(a))-g(x))+y)+f(a))+((g(x)+z)+g(a)). \quad (17)$$

Taking $x = 0$, we get $(y + z) + g(a) = y + (z + g(a))$ for all $y, z \in Q$, hence $g(a) \in C(Q(+))$ and $a \in C(Q(+))$. Now 16 yields

$$x+(y+z) = ((x-g(x))+g(x))+(y+z) = ((x-g(x))+y)+(g(x)+z). \quad (18)$$

By 1.3, $(x - g(x)) - g(x) = x - 2g(x) \in C(Q(+))$, hence $x + g(x) \in C(Q(+))$ for every $x \in Q$ and g is 1-central.

Conversely, if (iii) holds then $x - 2g(x) \in C(Q(+))$ and 1.3 implies that 18 holds for all $x, y, z \in Q$. As $f(a), g(a) \in C(Q(+))$, 17 and consequently 16 hold for all $x, y, z \in Q$. If $u, v, w \in Q$ are arbitrary and $x = f(u)$, $y = fg(v)$, $z = g^2(w)$ then 16 implies $u \cdot vw = f_u v \cdot uw$ and hence Q is an LE–quasigroup.

The equivalence of (ii) and (iii) is an immediate consequence of 4.2. □

4.4 PROPOSITION. *Let $(Q(+), f, g, a)$ be an arithmetical form of a linear quasigroup Q. The following conditions are equivalent:*

(i) *Q is an RE–quasigroup.*

(ii) *Q is an LF–quasigroup.*

(iii) *$gf = gf$, $a \in C(Q(+))$ and f is 1-central.*

PROOF. It suffices to use 4.3 on $Q(*)$, where $x * y = yx$ for all $x, y \in Q$. □

References

[1] V.D.Belousov, *Osnovy teorii kvazigrup i lup*, Nauka, Moskva, 1967.

[2] R.H.Bruck, *A Survey of Binary Systems*, Springer–Verlag, Berlin–Göttingen–Heidelberg, 1958.

[3] T.Kepka, *Structure of triabelian quasigroups*, Comment. Math. Univ. Carolinae **17** (1976), 229–240.

[4] T.Kepka, *Hamiltonian quasimodules and trimedial quasigroups*, Acta Univ. Carolinae Math. Phys. **26**,1 (1985), 11–20.

[5] P.Němec, *Arithmetical forms of quasigroups*, Comment. Math. Univ. Carolinae **29** (1988), 295–302.

[6] P.Němec, *Commutative Moufang loops corresponding to linear quasigroups*, Comment. Math. Univ. Carolinae **29** (1988), 303–308.

[7] J.-P.Soublin, *Etude algébrique de la notion de moyenne*, J. Math. Pures Appl. **50** (1971), 53–264.

[8] K.Toyoda, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221–227.