Commentationes Mathematicae Universitatis Carolinae

Petr Němec
Arithmetical forms of quasigroups

Commentationes Mathematicae Universitatis Carolinae, Vol. 29 (1988), No. 2, 295--302

Persistent URL: http://dml.cz/dmlcz/106640

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
29,2 (1988)

ARITHMETICAL FORMS OF QUASIGROUPS

Petr NĚMEC

Abstract: A quasigroup Q is said to be linear if there is a commutative Moufang loop Q(+), its automorphisms f, g and an element $a\in Q$ such that $xy=(f(x)+g(y))+a$ for all $x,y\in Q$; the quadruple (Q(+),f,g,a) is a so called arithmetical form of Q. All arithmetical forms of a given linear quasigroup Q are characterized.

Key words: Quasigroup, commutative Moufang loop, arithmetical form.

Classification 20N05

Several important classes of quasigroups, e.g. medial, distributive or trimedial quasigroups can be characterized by a certain type of linear construction (see e.g. [3],[4],[6],[7]). The first to investigate such "linear" constructions seems to be Toyoda [7] as early as in 1941, who showed that medial quasigroups are linear over Abelian groups. Hence it seems natural to study a common generalization of all these classes, so called linear quasigroups, introduced in [5]: A quasigroup Q is said to be linear (more precisely, linear over a commutative Moufang loop) if there is a commutative Moufang loop Q(+), its automorphisms f, g and an element $a\in Q$ such that $xy=(f(x)+g(y))+a$ for all $x,y\in Q$. The quadruple (Q(+),f,g,a) is called an arithmetical form of Q.

In [5], some important identities satisfied by such quasigroups are investigated. The present paper deals with basic properties of linear quasigroups. It is shown that an arithmetical form (Q(+),f,g,a) of a linear quasigroup Q is uniquely determined by the neutral element of Q(+) and the set of all elements of Q which can serve as such neutral elements is described.

1. Preliminaries. Let Q be a quasigroup. For every $a\in Q$, left and right translations are defined by $L_a(x)=ax$, $R_a(x)=xa$ for every $x\in Q$.

Every loop (i.e. a quasigroup with neutral element) satisfying the identity xx.yz=xy.xz is commutative (the identity implies xy.x=xx.y=x.xy and the commutativity follows) and is called a commutative Moufang loop.

Let Q(+) be an additively written commutative Moufang loop with neutral element 0 (then the defining identity has the form $(x+x)+(y+z)=(x+y)+(x+z)$). For all $a,b,c \in Q$ we put

$$[a,b,c]=[a,b,c]_{Q(+)}=((a+b)+c)-(a+(b+c)),$$

so called associator of the elements a, b, c. The centre of Q(+), denoted by C(Q(+)), is the set of all elements $a \in Q$ such that $[a,x,y]=0$ for all $x,y \in Q$. For an integer m, a mapping $f:Q \rightarrow Q$ is said to be m-central if $f(x)+mx \in C(Q(+))$ for every $x \in Q$.

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 $[a,b,c]=-[b,a,c]=[b,c,a]=-[c,b,a]=[c,a,b]=-[a,c,b]$, $[a,b,c]=[a,a+b,c]$ and if $[a,b,c]=0$ then the subloop 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 $a+((c+d)-b)=((a+c)-b)+d$. Adding $-2b$ once more, we obtain $(a-b)+(((c+d)-b)-b))=(((a+c)-b)-b)+(d-b)$. Since $((c+d)-b)-b=(c+d)-2b=(c-b)+(d-b)$ and $((a+c)-b)-b)=(a-b)+(c-b)$, we have $(a-b)+((c-b)+(d-b))=((a-b)+(c-b))+(d-b)$ and (ii) follows. The converse can be obtained by adding 2b twice and the rest is similar.

1.2. Lemma. 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) $a-b \in C(Q(+))$.

Proof. This is an immediate consequence of 1.1.

Sometimes, a commutative Moufang loop will also be denoted by $Q(\oplus)$. In this case, o denotes the neutral element, $\ominus a=x$ is an element such that

$a \oplus x = o$ and $a \ominus b = a \oplus (\ominus b)$ for all $a,b \in Q$.

2. Basic properties of arithmetical forms. An arithmetical form of a quasigroup Q is a quadruple $(Q(+),f,g,a)$ such that $Q(+)$ is a commutative Moufang loop, f and g are automorphisms of $Q(+)$, $a \in Q$ and, for all $x,y \in Q$, $xy=(f(x)+g(y))+a$. A quasigroup having at least one arithmetical form is said to be linear (more precisely, linear over a commutative Moufang loop), or LCML-quasigroup for short.

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

(i) $a=0.0$, $f=R_{g^{-1}(-a)}$, $g=L_{f^{-1}(-a)}$.

(ii) $(x+y)+a=R^{-1}_{g^{-1}(-a)}(x).L^{-1}_{f^{-1}(-a)}(y)$ for all $x,y \in Q$.

(iii) $xy=(f(x)+2a)+(g(y)-a)$ for all $x,y \in Q$.

(iv) $xy=(f(x)-a)+(g(y)+2a)$ for all $x,y \in Q$.

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

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

2.4. Proposition. Let $(Q(+),f,g,a)$ be an arithmetical form of a linear quasigroup Q and r be a relation on the set Q. Then r is a normal congruence of Q iff r is a congruence of $Q(+)$ which is invariant under f,g,f^{-1},g^{-1}.

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

2,4. Proposition. The class L of all linear quasigroups is closed under cartesian products and (quasigroup) homomorphic images.

Proof. The fact that L is closed under homomorphic images follows from

2.3 and the rest is clear.

3. Homomorphisms of linear quasigroups. Throughout this section, let Q, P be linear quasigroups with arithmetical norms $(Q(+),f,g,a)$ and $(P(\oplus),p,q,b)$, respectively. The neutral elements of $Q(+)$ and $P(\oplus)$ will be denoted by 0 and o, respectively. Suppose further that $h:P \to Q$ is a projective homomorphism.

Then, for every $x,y \in P$,

(1) $$h((p(x) \oplus q(y)) \oplus b)=(fh(x)+gh(y))+a$$

and consequently, taking $y=q^{-1}(\ominus b)$,

(2) $$hp(x)=(fh(x)+c)+a,$$

where $c=ghq^{-1}(\ominus b)$. Similarly,

(3) $$hq(y)=(gh(y)+d)+a,$$

where $d=fhp^{-1}(\ominus b)$. Consequently,

(4) $$fh(x)=(hp(x)-a)-c,\ gh(y)=(hq(y)-a)-d.$$

Combining this with (1) and writing $u=p(x)$, $v=q(y)$, we obtain

(5) $$h((u \oplus v) \oplus b)=(((h(u)-a))+(h(v)-a)-d))+a$$

for all $u,v \in P$. Since $u \oplus v=v \oplus u$, the last equality yields

$$((h(u)-a)-c)+((h(v)-a)-d)=((h(v)-a)-c)+((h(u)-a)-d)$$

for all $u,v \in P$. However, h is projective and so

(6) $$(r-c)+(s-d)=(s-c)+(r-d)$$

for all $r,s \in Q$. Therefore, by 1.2(ii), $c-d \in C(Q(+))$ and (5) yields (using 1.2(i)

(7) $$h((u \oplus v) \oplus b)=(((h(u)+h(v))-2a)-(c+d))+a$$

for all $u,v \in P$. Denote, for a moment, by w the left side of (7). Then (7) can be written as

$$(w-a)+(c+d)=(h(u)-a)+(h(v)-a)$$

and, adding 2a to both sides, we obtain

$$w+((c+d)+a)=h(u)+h(v).$$

Denoting $e=-((c+d)+a)$, we have proved that, for all $u,v \in P$,

(8) $$h((u \oplus v) \oplus b)=(h(u)+h(v))+e.$$

In particular, $h(u \oplus b)=(h(u)+h(o))+e$ and consequently

(9) $$h(u \oplus v)+h(o)=h(u)+h(v)$$

for all $u,v \in P$.

Now, put $k(u)=h(u)-h(o)$ for every $u \in P$, so that k is a projective mapping of P onto Q. Notice that, by (1) and (8), $e= -h(\ominus b)=k(b)-h(c)$.

3.1. Lemma. k is a homomorphism of $P(\oplus)$ onto $Q(+)$.

Proof. Add $-2h(o)$ to both sides of (9).

3.2. Lemma. If $b \in C(P(\oplus))$ then $(a-c)-h(o) \in C(Q(+))$ and $(a-d)-h(o) \in$ $\in C(Q(+))$.

Proof. Since $b \in C(P(\oplus))$, $h(o)-(a+(c+d))=e+h(o)=k(b) \in C(Q(+))$. However, $c-d \in C(Q(+))$ by (6), hence $h(o)-(a+2c) \in C(Q(+))$ and consequently $h(o)-(a-c) \in$ $\in C(Q(+))$. The rest is similar.

3.3. Lemma. If $a \in C(Q(+))$ and $b \in C(P(\oplus))$ then $h(o)+c \in C(Q(+))$ and $h(o)+d \in C(Q(+))$.

Proof. The result follows immediately from 3.2.

3.4. Lemma. If $Q=P$ and $h=id_Q$ (the identical mapping on Q) then $f(o)-$ $-g(o)=d-c \in C(Q(+))$.

Proof. Since $d-c \in C(Q(+))$ (see (6)), the result follows from (4).

Clearly (see (2)), $kp(x)=((ph(x)+c)+a)-h(o)$ and $fk(x)=fh(x)-fh(o)$ for every $x \in P$. We see that $kp=fk$ iff

$$(r+c)+a=(r-fh(o))+h(o)$$

for every $r \in Q$. Since $fh(o)=(h(o)-a)-c$ by (4), this is equivalent to

(10) $$((r+c)+a)-h(o)=r+(c+(a-h(o)))$$

for every $r \in Q$. If (10) is satisfied then (putting $r=0$) $[h(o),a,c]_{Q(+)}=0$ and consequently

(11) $$((r+c)+a)+h(o)=(r+h(o))+(c+a)$$

for every $r \in Q$. If $b \in C(P(\oplus))$ then, by 3.2, (11) is equivalent to $r+2a=$ $=(r+(a-c))+(a+c)$ which is equivalent to $r-c=(r+(a-c))-a$ and consequently to $(r-c)+a=r+(a-c)$, i.e. $[r,a,c]_{Q(+)}=0$.

3.5. Lemma. Suppose that either $b \in C(P\oplus))$ or $h(o) \in C(Q(+))$. Then $kp=$ $=fk$ iff $[r,a,c]_{Q(+)}=0$ for every $r \in Q$.

Proof. By (10), the result is clear if $h(o) \in C(Q(+))$. Hence, let

$b \in C(P(\oplus))$. If $[r,a,c]_{Q(+)}=0$ for every $r \in Q$ then (11) implies (10) and the rest is clear.

3.6. Lemma. Let $a \in C(Q(+))$. Then $kp=fk$ and $kq=gk$, provided either $b \in C(P(\oplus))$ or $h(o) \in C(Q(+))$.

Proof. Use 3.5.

3.7. Lemma. $k(b)=a$ iff $fh(o)+gh(o)=h(o)$ iff $h(o)=2a+(c+d)$.

Proof. First, using (1), $k(b)=((fh(o)+gh(o))+a)-h(o)$. Further, by (4), $fh(o)=(h(o)-a)-c$ and $gh(o)=(h(o)-a)-d$. Hence $k(b)=a$ iff $2h(o)-2a=h(o)+(c+d)$ which is equivalent to $h(o)=2a+(c+d)$.

4. Neutral elements. Throughout this section, let $Q(+)$ be a commutative Moufang loop and $o \in Q$. For all $x,y \in Q$, put $x \oplus y=(x+y)-o$. Clearly, $Q(\oplus)$ is a commutative Moufang loop with neutral element o. Further, let f, g be endomorphisms of $Q(+)$ and $a,c,d \in Q$. Define $p(x)=(f(x)+c)+a$, $q(x)=(g(x)+d)+a$ for every $x \in Q$.

4.1. Lemma. p is an endomorphism of $Q(\oplus)$ iff $o=(f(o)+c)+a$.

Proof. For all $x,y \in Q$, $p(x \oplus y)=(((f(x)+f(y))-f(o))+c)+a$ and $p(x) \oplus p(y)=$ $=(((f(x)+f(y))+2c)+2a)-o$. Hence p is an endomorphism of $Q(\oplus)$ iff

$$((f(u)-f(o))+c)+a=((f(u)+2c)+2a)-o$$

for every $u \in Q$. Adding $-3c$ and then $-3a$ to both sides, we see that this is equivalent to

$$((f(u)-c)+(-f(o)-c))+a=((f(u)-c)+2a)-o$$

and then to

$$((f(u)-c)-a)+((-f(o)-c)-a)=((f(u)-c)-a)-o.$$

However, the last equation is obviously equivalent to $o=(f(o)+c)+a$.

4.2. Lemma. Suppose that $(f(o)+c)+a)=o=(g(o)+d)+a$. If $c-d \in C(Q(+))$ then there is $b \in Q$ such that, for all $x,y \in Q$,

$$(f(x)+g(y))+a=(p(x)\oplus q(y))\oplus b. \tag{12}$$

Moreover, $b=(f(o)+g(o))+a$.

Proof. Since

$(((p(x)+q(y))-o)+b)-o=(((((f(x)+c)+a)+((g(y)+d)+a))-o)+b)-o$, (12) is equivalent to

(13) $(f(x)+g(y))+a=(((f(x)+c)+(g(y)+d))+2a)+(b-2o)$.

However, $c-d\in C(Q(+))$ and so, using 1.2, (13) can be rewritten as

$$(f(x)+g(y))+a=(((f(x)+g(y))+a)+((c+d)+a))+(b-2o).$$

Now it suffices to put $b=2o+((-c-d)-a)$. By 4.1, $b=(f(o)+g(o))+a$.

4.3. Remark. If f, g are projective then also the opposite implication is true. Indeed, if there is $b\in Q$ such that (12) holds then (13) is true, hence (using the commutativity of $Q(+)$) $(u+c)+(v+d)=(v+c)+(u+d)$ for all $u,v\in Q$ and 1.2 yields $c-d\in C(Q(+))$.

4.4. Lemma. Suppose that $(f(o)+c)+a=o=(g(o)+d)+a$. Then $c-d\in C(Q(+))$ iff $f(o)-g(o)\in C(Q(+))$.

Proof. Obviously, $c-d=((o-a)-f(o))-((o-a)-g(o))$ and the assertion easily follows (consider the factor-loop $Q(+)/C(Q(+))$).

5. Main results

5.1. Proposition. Let $(Q(+),f,g,a)$ and $(Q(\oplus),p,q,b)$ be arithmetical forms of a linear quasigroup Q. If the loops $Q(+)$ and $Q(\oplus)$ have the same neutral element 0 then $Q(+)=Q(\oplus)$, $f=p$, $g=q$ and $a=b$.

Proof. For all $x,y\in Q$,

(14) $$(f(x)+g(y))+a=(p(x)\oplus q(y))\oplus b).$$

Taking $x=y=0$, we get $a=b$. Moreover, for $x=0$ and $y\in Q$ arbitrary, $g(y)+a=q(y)\oplus a$, and similarly $f(x)+a=p(x)\oplus a$ for all $x\in Q$. Consequently, $0=p(p^{-1}(\ominus a))\oplus a=f(f^{-1}(-a))+a=p(f^{-1}(-a))\oplus a$ and hence $f^{-1}(-a)=p^{-1}(\ominus a)$. Now, setting $x=f^{-1}(-a)$ in (14), we obtain $g=q$. Similarly $f=p$ and we see that $(u+v)+a=(u\oplus v)\oplus a$ for all $u,v\in Q$. In particular, $u+a=u\oplus a$ which implies $u+v=u\oplus v$.

5.2. Proposition. Let $(Q(+),f,g,a)$ be an arithmetical form of a linear quasigroup Q and $o\in Q$. The following conditions are equivalent:

(i) There is an arithmetical form $(Q(\oplus),p,q,b)$ of the quasigroup Q such that o is the neutral element of $Q(\oplus)$.

(ii) $f(o)-g(o)\in C(Q(+))$.

Proof. If (i) holds then $f(o)-g(o)\in C(Q(+))$ by 3.4. For the converse, put $c=(o-a)-f(o)$, $d=(o-a)-g(o)$ and $x\oplus y=(x+y)-o$, $p(x)=(f(x)+c)+a$, $q(x)=(g(x)+d)+a$ for all $x,y\in Q$. The result now follows from 4.1, 4.4 and 4.2.

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

(i) fg^{-1} (or gf^{-1}, $f^{-1}g$, $g^{-1}f$) is a 2-central mapping of $Q(+)$.

(ii) For every $o \in Q$ there is an arithmetical form $(Q(\oplus),p,q,b)$ of the quasigroup Q such that o is the neutral element of $Q(\oplus)$.

5.4. Remark. Let Q be a linear quasigroup which is left semimedial, i.e. satisfies the identity $xx.yz=xy.xz$. By 5.3 and [5], Proposition 3.4, for every $o \in Q$ there is an (uniquely determined) arithmetical form with o as the neutral element of the corresponding commutative Moufang loop.

5.5. Example. Let $Q(+)$ be a commutative Moufang loop with $C(Q(+))=0$, $a \in Q$ and Q be a linear quasigroup with arithmetical form $(Q(+),-id_Q,id_Q,a)$. If $(Q(\oplus),p,q,b)$ is arbitrary arithmetical form of Q and o is the neutral element of $Q(\oplus)$ then, by 5.2, $f(o)-g(o)= -2o \in C(Q(+))$ and hence $o= -2o+3o \in C(Q(+))=0$. By 5.1, Q has exactly one arithmetical form.

References

[1] V.D. BELOUSOV: Osnovy teorii kvazigrupp 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: Quasigroups linear over commutative Moufang loops (to appear in Rivista Mat. Pura ed Apl.).

[6] J.-P. SOUBLIN: Etude algébrique de la notion de moyenne, J. Math. Pures et Appl. 50(1971), 53-264.

[7] K. TOYODA: On axioms of linear functions, Proc. Imp. Acad. Tokyo 17 (1941), 221-227.

Matematicko-fyzikální fakulta, Univerzita Karlova, Sokolovská 83, 18600 Praha 8, Czechoslovakia

(Oblatum 3.3. 1988)