Commentationes Mathematicae Universitatis Carolinae

Petr Němec

Commutative Moufang loops corresponding to linear quasigroups

Commentationes Mathematicae Universitatis Carolinae, Vol. 29 (1988), No. 2, 303--308

Persistent URL: http://dml.cz/dmlcz/106641

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
29,2 (1988)

COMMUTATIVE MOUFANG LOOPS CORRESPONDING TO LINEAR QUASIGROUPS

Petr NĚMEC

Abstract: Suppose that $Q(+)$ and $Q(\oplus)$ are commutative Moufang loops with the same underlying set, f and g are automorphisms of $Q(+)$, p and q are automorphisms of $Q(\oplus)$ and $a,b \in Q$ are such that $xy=(f(x)+g(y))+a=(p(x) \oplus q(y)) \oplus b$ for all $x,y \in Q$. Necessary and sufficient conditions are investigated, under which there is an isomorphism $h:Q(\oplus) \to Q(+)$ with $hp=fh$.

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

Classification: 20N05

The class of linear quasigroups, introduced in [4] and [5], can be viewed as a common generalization of several important classes of quasigroups, as e.g. medial, distributive or trimedial quasigroups (see e.g. [6],[2],[3]). A quasigroup is said to be linear if there is a commutative Moufang loop $Q(+)$ with the same underlying set, its automorphisms f, g and an element $a \in Q$ such that $xy=(f(x)+g(y))+a$ for all $x,y \in Q$; in this case, the quadruple $(Q(+),f,g,a)$ is called arithmetical form of Q.

This paper is closely related to [5]. Whence the main aim of [5] is to determine, roughly speaking, the number of possible arithmetical forms of a linear quasigroup, the present paper deals with the structure of the corresponding commutative Moufang loops. Namely, several conditions are investigated, under which the commutative Moufang loops occurring in different arithmetical forms of a linear quasigroup are canonically isomorphic.

1. Auxiliary results I. Throughout this section, let $Q(+)$ be a commutative Moufang loop. For all $x,u,v \in Q$ we define $[x,u,v]_{Q(+)}=((x+u)+v)-(x+(u+v))$, $i_{u,v}(x)=((x+u)+v)-(u+v)$ and $C(Q(+))$ to be the set of all $a \in Q$ such that $[a,u,v]_{Q(+)}=0$ for all $u,v \in Q$. It is well known that $i_{u,v}(x)=x+[x,u,v]_{Q(+)}$ and $i_{u,v}$ is an automorphism of $Q(+)$ (see e.g. [1]).

Further, let f be an endomorphism of $Q(+)$ and $a,c,o \in Q$. For all $x,y \in Q$, put $x \oplus y=(x+y)-o$ and $p(x)=(f(x)+c)+a$ (cf. Section 4 of [5]). Then $Q(\oplus)$ is a commutative Moufang loop with neutral element o. By [5], Lemma 4.1, p is an endomorphism of $Q(\oplus)$ if and only if

$$o=(f(o)+c)+a. \tag{1}$$

From now on we shall suppose that (1) holds and we shall find some necessary and sufficient conditions for the existence of an isomorphism $h:Q(\oplus) \to Q(+)$ such that $hp=fh$.

Clearly, $hp=fh$ if and only if, for every $x \in Q$,

$$h((f(x)+c)+a)=fh(x). \tag{2}$$

This implies $h(c+a)=fh(0)$.

Now, let $h:Q(\oplus) \to Q(+)$ be an arbitrary isomorphism and put $k(x)=h(x)-h(0)$ for every $x \in Q$. Then $h(o)=0$ and, for all $x,y \in Q$, we clearly have $h((x+y)-o)=h(x)+h(y)$, hence $h(x-o)=h(x)+h(o)$ and consequently $h(x+y)+h(o)=h(x)+h(y)$. Adding $-2h(o)$ to both sides of this equality, we see that k is an automorphism of $Q(+)$. Moreover, $h(x)=k(x)-e$, where $e=-h(0)$. Obviously, $e=k(o)$ and (since $o=(f(o)+c)+a$) we also have

$$e=(kf(o)+k(c))+k(a). \tag{3}$$

1.1. Lemma. $hp=fh$ if and only if, for every $x \in Q$,

$$(kf(x)+k(c))+k(a)=(fk(x)-f(e))+e. \tag{4}$$

In this case, $k(c+a)=-f(e)+e$.

Proof. Use (2) and the fact that $h(x)=k(x)-e$.

1.2. Lemma. If $hp=fh$ then

$$e=(k(c)+k(a))+fk(o). \tag{5}$$

Proof. This follows immediately from the second part of 1.1.

1.3. Lemma. $hp=fh$ if and only if, for every $y \in Q$,

$$((kf(y)+kf(o))+k(c))+k(a)=fk(y)+((kf(o)+k(c))+k(a)). \tag{6}$$

Proof. Using (3), the equation (4) can be written as
$((kf(x-o)+kf(o))+k(c))+k(a)=(fk(x)-fk(o))+k(o)=fk(x-o)+((kf(o)+k(c))+k(a))$.

1.4. Lemma. $hp=fh$ if and only if, for every $y \in Q$,

(7) $$((f(y)+f(o))+c)+a=k^{-1}fk(y)+o.$$

Proof. Since $o=(f(o)+c)+a$, it suffices to apply k^{-1} to both sides of (6).

2. Auxiliary results II. Throughout this section, we shall also assume, in addition to the assumptions of Section 1, that f is an automorphism of $Q(+)$.

2.1. Lemma. $hp=fh$ if and only if, for every $z \in Q$,

(8) $$((z+f(o))+c)+a=k^{-1}fkf^{-1}(z)+o.$$

Proof. This is clear from 1.4.

Now, put $i=i_{f(o),c}$ and $j=i_{f(o)+c,a}$. Then $(z+f(o))+c=i(z)+(f(o)+c)$ and, using (1), $(i(z)+(f(o)+c))+a=ji(z)+o$ for every $z \in Q$. Combining these two equations, we have

(9) $$((z+f(o))+c)+a=ji(z)+o.$$

From this, using (1), we obtain

(10) $$ji(z)=(((z+((o-a)-c))+c)+a)-o.$$

2.2. Lemma. $hp=fh$ iff $ji=k^{-1}fkf^{-1}$.

Proof. Use 2.1.

2.3. Lemma. $ji=id_Q$ (the identical mapping on Q) if and only if, for every $x \in Q$,

(11) $$((x+o)-a)-c=x+((o-a)-c).$$

Proof. Use (10).

2.4. Lemma. $ji=id_Q$ iff $y+(((o-a)-c)-a)=(y+(o-a))+(-c-a)$ for every $y \in Q$.

Proof. Adding $-2a$ to both sides of (11), we get

$$((x-a)+(o-a))-(c-a)=(x-a)+(((o-a)-c)-a).$$

2.5. Lemma. $ji=id_Q$ iff $((o-a)-c)-a=(o-a)+(-c-a)$ and $y+((o-a)+(-c-a))=(y+(o-a))+(-c-a)$.

Proof. Use 2.4.

2.6. Lemma. $ji=id_Q$ iff $[o,c,a]_{Q(+)}=0$ and $[y,o-a,c+a]_{Q(+)}=0$ for every

$y \in Q$.

Proof. This is an easy consequence of 2.5.

2.7. Lemma. $ji=id_Q$ iff $[y,o-a,c+a]_{Q(+)}=0$ for every $y \in Q$. In this case, $o-f(o)=c+a$.

Proof. If $[y,o-a,c+a]=0$ for every $y \in Q$ then, taking $y=0$, we get $[o,c,a]=0$. Then, of course, $[o,a,c]=0$ and consequently $f(o)=(o-a)-c=$ $=o-(a+c)$.

2.8. Lemma. $ji=id_Q$ iff $[y,o-a,o-f(o)]_{Q(+)}=0$ for every $y \in Q$.

Proof. The direct implication follows from 2.7. Conversely, we have $[o,a,f(o)]=0$ and (1) yields $o-f(o)=c+a$.

Now we can summarize our results (assuming that f is an automorphism of $Q(+)$ and consequently p is an automorphism of $Q(\oplus)$):

2.9. Lemma. The following conditions are equivalent:

(i) There is an isomorphism $h:Q(\oplus) \longrightarrow Q(+)$ such that $hp=fh$.

(ii) Automorphisms f and jif (of $Q(+)$) are conjugated in the group $Aut(Q(+))$.

Proof. If (i) holds then the result follows immediately from 2.2. Conversely, suppose that (ii) holds and $k \in Aut(Q(+))$ is such that $jif=k^{-1}fk$. Define $h(x)=k(x)-k(o)$ for every $x \in Q$. Since $h(x \oplus y)=((k(x)+k(y))-k(o))-k(o)=$ $=(k(x)-k(o))+(k(y)-k(o))=h(x)+h(y)$ for all $x,y \in Q$, h is an isomorphism of $Q(\oplus)$ onto $Q(+)$. Moreover, $h(0)=-k(o)$ and so $k(x)=h(x)-h(0)$ for every $x \in Q$. Now we can use 2.2.

2.10. Remark. $ji=id_Q$, provided at least one of the following conditions holds: (i) $c+a \in C(Q(+))$; (ii) $2o+f(o) \in C(Q(+))$; (iii) $o-a \in C(Q(+))$; (iv) $a \in C(Q(+))$ and $o+f(o) \in C(Q(+))$.

2.11. Remark. Suppose that $ji=id_Q$ and define $h(x)=x-o$ for every $x \in Q$. By 2.9 and its proof, h is an isomorphism of $Q(\oplus)$ onto $Q(+)$ such that $hp=fh$.

3. Isomorphism 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 (on the same underlying set Q), $a \in Q$, f and g are automorphisms of $Q(+)$ and $xy=(f(x)+g(y))+a$ for all $x,y \in Q$ (cf. [5]). A quasigroup Q having at least one arithmetical form is said to be linear (over a commutative Moufang loop).

Throughout this section, let $(Q(+),f,g,a)$ and $(Q(\oplus),p,q,b)$ be arithmetical forms of the same linear quasigroup Q (we denote by o the neutral element of $Q(\oplus)$). Then $(f(x)+g(y))+a=(p(x)\oplus q(y))\oplus b$ for all $x,y\in Q$. By [5], Proposition 5.2, its proof and Proposition 5.1, we see that, for all $x,y\in Q$, $x\oplus y=(x+y)-o$, $p(x)=(f(x)+c)+a$, $q(x)=(g(x)+d)+a$, $c=(o-a)-f(o)$ and $d=(o-a)-g(o)$. Put $i=i_{f(o),c}=i_{g(o),d}$ (since $c-d=g(o)-f(o)\in C(Q(+))$ by [5], Lemma 3.4) and $j=i_{o-a,a}$.

3.1. Proposition. Let $(Q(+),f,g,a)$ and $(Q(\oplus),p,q,b)$ be arithmetical forms of a linear quasigroup Q. Then:

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

(ii) $p(0)\ominus q(0)\in C(Q(\oplus))$.

(iii) If $[x,o,f(x)]_{Q(+)}=0$ for every $x\in Q$ (or equivalently $[x,o,g(o)]_{Q(+)}=0$) then there is an isomorphism $h:Q(\oplus)\to Q(+)$ such that $hp=fh$ and $hq=gh$.

Proof. (i) and (ii) follow immediately from [5], Proposition 5.1. As for (iii), put $h(x)=x-o$ for every $x\in Q$. Then $h(x\oplus y)=(x+y)-2o=h(x)+h(y)$ for all $x,y\in Q$ and the result easily follows.

3.2. Proposition. Let $(Q(+),f,g,a)$ and $(Q(\oplus),p,q,b)$ be arithmetical forms of a linear quasigroup Q. The following conditions are equivalent:

(i) $hp=fh$ and $hq=gh$ for an isomorphism $h:Q(\oplus)\to Q(+)$.

(ii) There is an automorphism k of $Q(+)$ such that $jif=k^{-1}fk$ and $jig=k^{-1}gk$.

Proof. By 2.9.

3.3. Remark. We have $ji(x)=((x+f(o))+c)+a)-o=(((x+f(o))+((o-a)-f(o)))+a)-o$ for every $x\in Q$. If $f(x)-g(x)\in C(Q(+))$ for every $x\in Q$ (i.e. fg^{-1} is 2-central) then $jif(x)+(g(x)-f(x))=jig(x)$. Hence 3.2 (ii) implies $k(g(x)-f(x))=gk(x)-fk(x)$ for every $x\in Q$.

References

[1] R.H. BRUCK: A survey of binary systems, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1958.

[2] T. KEPKA: Structure of triabelian quasigroups, Comment. Math. Univ. Carolinae 17(1976), 229-240.

[3] T. KEPKA: Hamiltonian quasimodules and trimedial quasigroups, Acta Univ. Carolinae Math. Phys. 26,1(1985), 11-20.

[4] P. NĚMEC: Quasigroups linear over commutative Moufang loops (to appear in Rivista Mat. Pura ed Appl.)

[5] P. NĚMEC: Arithmetical forms of quasigroups, Comment. Math. Univ. Carolinae 29(1988), 295-302.

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

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

(Oblatum 3.3. 1988)