Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra 317 (2007) 435–461

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

The structure of F-quasigroups ☆

Tomáš Kepka [a], Michael K. Kinyon [b,*], J.D. Phillips [c]

[a] *Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic*
[b] *Department of Mathematics, University of Denver, Denver, CO 80208, USA*
[c] *Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933, USA*

Received 14 October 2005

Available online 18 May 2007

Communicated by Efim Zelmanov

Abstract

We solve a problem of Belousov which has been open since 1967: to characterize the loop isotopes of F-quasigroups. We show that every F-quasigroup has a Moufang loop isotope which is a central product of its nucleus and Moufang center. We then use the loop to reveal the structure of the associated F-quasigroup.

Keywords: F-quasigroup; Moufang loop

1. Introduction

A *quasigroup* $(Q, \cdot)$ is a set Q together with a binary operation $\cdot : Q \times Q \to Q$ such that for each $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$. Equivalently, we may consider a quasigroup $(Q, \cdot, \backslash, /)$ to be a set Q together with three binary operations $\cdot, \backslash, / : Q \times Q \to Q$ such that the equations $x\backslash(xy) = y$, $(xy)/y = x$, $x(x\backslash y) = y$, and $(x/y)y = x$ hold

☆ This work is a part of the research project MSM 0021620839 financed by MSMT and partly supported by the grant agency of the Czech Republic, grant #201/05/0002.

* Corresponding author.
E-mail addresses: kepka@karlin.mff.cuni.cz (T. Kepka), mkinyon@math.du.edu (M.K. Kinyon), phillipj@wabash.edu (J.D. Phillips).
URLs: http://www.math.du.edu/~mkinyon (M.K. Kinyon), http://persweb.wabash.edu/facstaff/phillipj/ (J.D. Phillips).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.05.007

for all $x, y \in Q$. A quasigroup with a neutral element is called a *loop*. For the basic theory of quasigroups and loops, we refer to the standard texts [3,6,18].

Because we will be dealing extensively with sets which possess both a quasigroup structure and a loop structure, we will use additive notation for loops, even though the loop may not necessarily be commutative. Thus the neutral element of a loop $(Q, +)$ is denoted by 0.

Among the earliest studied varieties of quasigroups are *F-quasigroups*. These were introduced by Murdoch in 1939 [16]. F-quasigroups are defined by the equations

$$x \cdot yz = xy \cdot (x\backslash x)z, \tag{F_l}$$

$$zy \cdot x = z(x/x) \cdot yx. \tag{F_r}$$

A quasigroup satisfying (F_l) (respectively (F_r)) is said to be a *left* (respectively *right*) *F-quasigroup*. Murdoch did not actually name this particular variety. The earliest use of the term "F-quasigroup" we can find is in a paper of Belousov [1].

Quasigroups $(Q, \cdot)$ and $(\tilde{Q}, \tilde{\cdot})$ are said to be *isotopic* if there are bijections $f, g, h : Q \to \tilde{Q}$ such that $f(x) \,\tilde{\cdot}\, g(y) = h(x \cdot y)$ for all $x, y \in Q$. If $Q = \tilde{Q}$ and $h = \mathrm{id}_Q$, then $(Q, \cdot)$ and $(\tilde{Q}, \tilde{\cdot})$ are said to be *principally isotopic*. Every quasigroup $(Q, \cdot, \backslash, /)$ is principally isotopic to a loop $(Q, +)$: fix $a, b \in Q$, and set $0 = ba$ and $x + y = (x/a)(b\backslash y)$ for all $x, y \in Q$.

One of the key issues in the study of any variety of quasigroups is to characterize those loops to which quasigroups in the variety are isotopic. The exemplar of results of this type is the (weak form of the) Toyoda–Bruck theorem: every medial quasigroup is isotopic to an abelian group [5, 20]. This result was later generalized to distributive quasigroups [2], trimedial quasigroups [10], and semimedial quasigroups [11,12].

In the very first of the problems (задачи) in Belousov's 1967 book [3, p. 216], we find the following question, which has remained open until now:

1. ... Каким лупат изотопны двусторонние F-квазигруппы...?

1. ... To which loops are two-sided F-quasigroups isotopic...? (our translation)

In 1979, one of us [13] implicitly conjectured the following answer to Belousov's question.

Every loop $(Q, +)$ isotopic to a given F-quasigroup $(Q, \cdot)$ is a Moufang loop.

Recall that *Moufang loops* $(Q, +)$ are defined by any of the equivalent identities

$$x + \big(y + (x + z)\big) = \big((x + y) + x\big) + z, \qquad x + \big((y + z) + x\big) = (x + y) + (z + x),$$
$$\big((z + x) + y\big) + x = z + \big(x + (y + x)\big), \qquad \big(x + (y + z)\big) + x = (x + y) + (z + x)$$

for all $x, y \in Q$ [3,6,18]. Moufang loops are isotopically invariant, that is, every loop isotopic to a Moufang loop is a Moufang loop. In view of this, the conjecture can be stated more concisely:

Every F-quasigroup is isotopic to a Moufang loop.

In [13], it was shown that if a given F-quasigroup is isotopic to a Moufang loop, then at least one of the loop isotopes has additional structure. This will be seen below in the statement of our main result, but first, we need additional notation.

Recall that the *nucleus* of a loop $(Q,+)$ is defined by

$$N(Q)=\big\{a\in Q\colon\ (a+x)+y=a+(x+y),\ (x+a)+y=x+(a+y),\ \text{and}\\ x+(y+a)=(x+y)+a,\ \forall x,y\in Q\big\}.$$

In a Moufang loop $(Q,+)$, $N(Q)$ is a normal associative subloop of $(Q,+)$ [3,6,18]. The *Moufang center* of a loop is

$$K(Q)=\big\{a\in Q\colon\ (a+a)+(x+y)=(a+x)+(a+y),\ \forall x,y\in Q\big\}\\ =\big\{a\in Q\colon\ (x+y)+(a+a)=(x+a)+(y+a),\ \forall x,y\in Q\big\}.$$

In any loop, the Moufang center is a commutative Moufang subloop [6, p. 94].

Definition 1.1. An *NK-loop* is a loop $(Q,+)$ satisfying $Q=N(Q)+K(Q)$, that is, for each $a\in Q$, there exists $n\in N(Q)$, $k\in K(Q)$ such that $a=n+k$.

In Section 5, we will study NK-loops in some detail. In particular, every NK-loop is Moufang (Theorem 5.4).

With these notions in hand, here is one of our main results.

Theorem 1.2. *For a quasigroup $(Q,\cdot)$, the following are equivalent*:

(1) *$(Q,\cdot)$ is an F-quasigroup.*
(2) *There exist a Moufang NK-loop $(Q,+)$, $f,g\in \mathrm{Aut}(Q,+)$, and $e\in N(Q,+)$ such that*

$$x\cdot y=f(x)+e+g(y)$$

for all $x,y\in Q$, $fg=gf$, and $x+f(x),x+g(x)\in N(Q,+)$, $-x+f(x),-x+g(x)\in K(Q,+)$ for all $x\in Q$.

Theorem 1.2 not only confirms the conjecture of [13], but also characterizes those Moufang loops that can occur as loop isotopes of F-quasigroups. In addition, the theorem generalizes the corresponding results in the distributive [2] and trimedial [10] cases.

In the aforementioned Open Problem, Belousov also asked the same question regarding loop isotopes for the one-sided case of left F-quasigroups. An answer of sorts was found by Golovko, who showed that every left F-quasigroup is isotopic to a *left M-loop* [7]. (It would take us too far afield to include the definition here.) This result was later included by Belousov in his lecture notes [4], which are not easily accessible. In a differential geometric context, the relationship between left F-quasigroups and left M-loops was used by Sabinin and his students to study transsymmetric spaces. See [19] and the complete bibliography therein for this particular line of inquiry. This book also has the most easily accessible proof of Golovko's result.

It turns out that the notion of M-loop is of no help in dealing with the case of two-sided F-quasigroups. Although it follows from Golovko's work that every F-quasigroup is isotopic to a loop which is both a left and right M-loop, that information does not seem to be sufficient to characterize the loop isotopes, nor does the M-loop structure seem to help in establishing Theorem 1.2.

We conclude this introduction with an outline of the sequel. In Section 2, we recite general preliminary results on quasigroups and loops which will be used later in the paper. In Section 4,

we state necessary well-known results about Moufang loops, and also present a few technical lemmas needed later. In Section 3, we present basic facts about (left) F-quasigroups. In Section 5, we examine the structure of NK-loops and show that they are Moufang (Theorem 5.4). We also give a sufficient condition for a loop to be NK (Theorem 5.2), and this turns out to be the main tool in showing that F-quasigroups are isotopic to NK-loops.

Our proof of Theorem 1.2 is really split up into the harder implication (1) $\Rightarrow$ (2) in Theorem 6.13 and the easier converse in Proposition 7.1. The former is in Section 6 and the latter is in Section 7. In the remainder of Section 7 as well as Section 8, we study the structure of F-quasigroups by using their representations in terms of NK-loops. In Section 9, we formalize the relationship between (pointed) F-quasigroups and NK-loops with additional data (which we call arithmetic forms) and show an appropriate equivalence of equational classes (and categories) in Theorem 9.4. Finally, in Section 10, we reap the rewards of this equivalence and our work in Sections 7 and 8 by presenting a summary of the structure of F-quasigroups.

This paper redevelops some of the main results of [9,13], as they are necessary to give a complete proof of Theorem 1.2 and its consequences. Wherever possible, we try to give shorter, clearer proofs.

2. Preliminaries

In a quasigroup $(Q, \cdot, \backslash, /)$, it is useful to introduce notation for local right and left neutral elements. Here we adopt the following:

$$\alpha(x) = x\backslash x, \qquad \beta(x) = x/x,$$

that is $x \cdot \alpha(x) = x$ and $\beta(x) \cdot x = x$.

For $a \in Q$, left and right translations $L_a, R_a : Q \to Q$ are defined by $L_a(x) = ax$ and $R_a(x) = xa$ for $x \in Q$. The *multiplication group* of Q is the group generated by all translations: $\mathcal{M}(Q) = \langle L_a, R_a \colon a \in Q \rangle$.

If $(Q, +)$ is a loop, then the stabilizer of the neutral element $0 \in Q$ is called the *inner mapping group* of Q and is denoted by $\mathrm{I}(Q)$. A loop is called an *A-loop* if $\mathrm{I}(Q) \subseteq \mathrm{Aut}(Q, +)$.

In Section 1, we have already defined the nucleus and Moufang center of a loop, which are subloops. The *commutant* or *semicenter* of a loop $(Q, +)$ is the set

$$C(Q) = \{a \in Q \colon a + x = x + a \ \forall x \in Q\}.$$

The commutant is not necessarily a subloop. Finally, the *center* of a loop $(Q, +)$ is defined by

$$Z(Q) = N(Q) \cap C(Q).$$

Lemma 2.1. *In a loop $(Q, +)$,*

(1) $K(Q) \subseteq C(Q)$.
(2) $C(Q)$ *is a characteristic subset.*
(3) $K(Q)$ *is a characteristic subloop.*
(4) $N(Q)$ *is a characteristic subgroup.*
(5) $Z(Q) = N(Q) \cap K(Q)$.
(6) $Z(Q)$ *is a normal abelian subgroup.*

Proof. For (1): If $a \in K(Q)$, then for all $x \in Q$, $a + (a + x) = (a + 0) + (a + x) = 2a + x = (a + x) + (a + 0) = (a + x) + a$. Replacing $a + x$ with x, we have the desired result. The rest are clear or can be found in the standard references [3,6,18]. □

Lemma 2.2. *Let $(Q, +)$ be an A-loop.*

(1) *Every characteristic subloop is normal.*
(2) *$N(Q)$ is a normal subloop.*
(3) *$K(Q)$ is a normal subloop.*

Proof. Recall that a subloop is normal if and only if it is invariant under the action of $\mathrm{I}(Q)$. Then (1) follows immediately, and (2) and (3) follow from 2.1. □

For a quasigroup $(Q, \cdot)$, we define

$$M(Q) = \{a \in Q\colon\ xa \cdot yx = xy \cdot ax\ \forall x, y \in Q\}.$$

Lemma 2.3. *For a loop $(Q, +)$,*

(1) $M(Q) \subseteq C(Q)$.
(2) $Z(Q) = N(Q) \cap M(Q)$.

Proof. For $a \in M(Q)$, $(x + a) + (y + x) = (x + y) + (a + x)$ for all $x, y \in Q$. Take $x = 0$ to obtain (1). Then (2) is clear. □

A quasigroup $(Q, \cdot)$ is called

- *medial* if $xa \cdot by = xb \cdot ay$ for all $x, y, a, b \in Q$;
- *monomedial* (*dimedial*, *trimedial*, respectively) if every (at most) one-generated (two-generated, three-generated, respectively) subquasigroup of Q is medial;
- *distributive* if $x \cdot yz = xy \cdot xz$ and $zy \cdot x = zx \cdot yx$ for all $x, y, z \in Q$;
- *symmetric* if $xy = yx$ and $x \cdot xy = y$ for all $x, y \in Q$.

Proposition 2.4. *(See [5,20].) For a quasigroup $(Q, \cdot)$, the following are equivalent*:

(1) *$(Q, \cdot)$ is medial.*
(2) *There exist an abelian group $(Q, +)$, $f, g \in \mathrm{Aut}(Q, +)$, and $e \in Q$ such that $x \cdot y = f(x) + e + g(y)$ for all $x, y \in Q$, and $fg = gf$.*

Proposition 2.5. *(See [10].) For a quasigroup $(Q, \cdot)$, the following are equivalent*:

(1) *$(Q, \cdot)$ is trimedial.*
(2) *There exist a commutative Moufang loop $(Q, +)$, $f, g \in \mathrm{Aut}(Q, +)$, and $e \in Z(Q, +)$ such that $x \cdot y = f(x) + e + g(y)$ for all $x, y \in Q$, $fg = gf$, and $x + f(x), x + g(x) \in Z(Q, +)$ for all $x \in Q$.*

Proposition 2.6. *(See [2].) For a quasigroup $(Q,\cdot)$, the following are equivalent*:

(1) $(Q,\cdot)$ *is symmetric and distributive.*
(2) *There exists a commutative Moufang loop $(Q,+)$ of exponent 3 such that $x\cdot y=-x-y$ for all $x,y\in Q$.*

Proposition 2.7. *(See [2].) For a quasigroup $(Q,\cdot)$, the following are equivalent*:

(1) $(Q,\cdot)$ *is distributive.*
(2) *There exist a commutative Moufang loop $(Q,+)$, $f\in \mathrm{Aut}(Q,+)$ such that $x\cdot y=f(x)+y-f(y)$ for all $x,y\in Q$, $x\mapsto x-f(x)$ is a permutation of Q, and $x+f(x)\in Z(Q,+)$ for all $x\in Q$.*

We conclude this section by introducing some useful groups of pairs of mappings. For a quasigroup $(Q,\cdot)$, define

$$\mathcal{A}(Q)=\big\{(p,q)\colon\ Q\times Q\to Q\times Q \mid p(xy)=q(x)y\ \forall x,y\in Q\big\},$$
$$\mathcal{B}(Q)=\big\{(p,q)\colon\ Q\times Q\to Q\times Q \mid p(xy)=xq(y)\ \forall x,y\in Q\big\},$$
$$\mathcal{C}(Q)=\big\{(p,q)\colon\ Q\times Q\to Q\times Q \mid p(x)y=xq(y)\ \forall x,y\in Q\big\}.$$

Let

$$\mathcal{A}_l(Q)=\big\{p\colon\ (p,q)\in\mathcal{A}(Q)\big\}\quad\text{and}\quad \mathcal{A}_r(Q)=\big\{q\colon\ (p,q)\in\mathcal{A}(Q)\big\}$$

and similarly define $\mathcal{B}_l(Q)$, $\mathcal{B}_r(Q)$, $\mathcal{C}_l(Q)$, and $\mathcal{C}_r(Q)$. It is easy to see that every mapping from $\mathcal{A}_l(Q)\cup\mathcal{A}_r(Q)\cup\mathcal{B}_l(Q)\cup\mathcal{B}_r(Q)\cup\mathcal{C}_l(Q)\cup\mathcal{C}_r(Q)$ is a permutation of Q. These mappings are known as *regular permutations* of the quasigroup Q. In addition, $\mathcal{A}_l(Q)\cong\mathcal{A}_r(Q)$, $\mathcal{B}_l(Q)\cong\mathcal{B}_r(Q)$, $\mathcal{C}_l(Q)\cong\mathcal{C}_r(Q)$ are permutation groups.

3. F-quasigroups

For convenience, we repeat here the basic definitions of Section 1, using the notational conventions of Section 2. A quasigroup $(Q,\cdot)$ is said to be a *left F-quasigroup* if it satisfies the identity

$$x\cdot yz=xy\cdot\alpha(x)z \tag{F_l}$$

for all $x,y,z\in Q$. $(Q,\cdot)$ is said to be a *right F-quasigroup* if it satisfies

$$zy\cdot x=z\beta(x)\cdot yx \tag{F_r}$$

for all $x,y,z\in Q$. If $(Q,\cdot)$ is both a left F-quasigroup and a right F-quasigroup, then $(Q,\cdot)$ is called a (two-sided) F-quasigroup.

Lemma 3.1. *The following conditions are equivalent for a quasigroup $(Q,\cdot)$.*

(1) $(Q,\cdot)$ *is a left F-quasigroup.*

(2) $L_x y \cdot L_{\alpha(x)} z = L_x(yz)$, $\forall x, y, z \in Q$.
(3) $L_x L_y = L_{xy} L_{\alpha(x)}$, $\forall x, y \in Q$.
(4) $L(x, y) = L_{\alpha(x)}$, $\forall x, y \in Q$.
(5) $L(x, y) = L(x, z)$, $\forall x, y, z \in Q$.
(6) $L_x R_z = R_{\alpha(x)z} L_x$, $\forall x, z \in Q$.

Proof. These are all just different ways of rewriting the definition of left F-quasigroup. □

Lemma 3.2. *Let $(Q, \cdot)$ be a left F-quasigroup. Then*

(1) *$\alpha\beta = \beta\alpha$ and $\alpha \in \mathrm{End}(Q, \cdot)$.*
(2) *$R_a L_b = L_b R_a$ for $a, b \in Q$ if and only if $\alpha(b) = \beta(a)$.*
(3) *$R_{\alpha(a)} L_{\beta(a)} = L_{\beta(a)} R_{\alpha(a)}$.*

Proof. (i) We compute

$$x \cdot \alpha\beta(x)\alpha(x) = \beta(x)x \cdot \alpha\beta(x)\alpha(x) = \beta(x) \cdot x\alpha(x) = \beta(x)x = x = x\alpha(x).$$

Canceling x and then dividing on the right by $\alpha(x)$, we obtain $\alpha\beta(x) = \beta\alpha(x)$, as claimed. Further, $xy \cdot \alpha(x)\alpha(y) = x \cdot y\alpha(y) = xy = xy \cdot \alpha(xy)$ and so $\alpha(x)\alpha(y) = \alpha(xy)$ for all $x, y \in Q$.

(ii) Observe that

$$b \cdot xa = bx \cdot \alpha(b)a \quad \text{and} \quad bx \cdot a = bx \cdot \beta(a)a,$$

for all $x, a, b \in Q$. The desired result follows immediately.

Finally, (iii) follows from (i) and (ii). □

Corollary 3.3. *If $(Q, \cdot)$ is an F-quasigroup, then α and β are commuting endomorphisms of Q.*

Lemma 3.4. *A loop $(Q, +)$ is a left (right, two-sided) F-loop if and only if it is a group.*

Proof. This is immediate from (F_l). □

Remark 3.5. By Lemma 3.4, every group is an F-quasigroup. In addition, it is clear from definitions that every trimedial quasigroup is an F-quasigroup. Thus we observe that the variety of F-quasigroups is strictly larger than the variety of trimedial quasigroups.

Again just by comparing definitions, we have the following.

Proposition 3.6. *For a quasigroup $(Q, \cdot)$, the following are equivalent*:

(1) *$(Q, \cdot)$ is distributive.*
(2) *$(Q, \cdot)$ is idempotent and trimedial.*
(3) *$(Q, \cdot)$ is an idempotent F-quasigroup.*

4. Moufang loops

We begin by reciting some basic results, most of which are in the literature.

Proposition 4.1. *Let $(Q,+)$ be a Moufang loop. Then*

(1) $(Q,+)$ *is* diassociative*, that is, for each $x, y \in Q$, $\langle x, y\rangle$ is a group.*
(2) *$N(Q)$ is a normal subloop.*
(3) *$K(Q) = C(Q) = M(Q)$ is a characteristic subloop.*
(4) *If $K(Q)$ is a normal subloop, then for each $x \in Q$, the subloop generated by $\{x\} \cup K(Q)$ is commutative.*

Proof. Most of these are standard facts; see, for instance, [3,6,18]. The only perhaps unfamiliar assertions are the second equality of (3) and (4).

For (3): For $a \in C(Q)$, $x, y \in Q$, note that $(x + a) + (y + x) = (x + (a + y)) + x = (x + (y + a)) + x = (x + y) + (a + x)$. Thus $c \in M(Q)$. The other inclusion follows from Lemma 2.3(1).

For (4): Let $P = \langle x, K(Q)\rangle$. Then $K(Q) \subseteq K(P)$, and it suffices to show that $x \in K(P)$. Fix $y \in P$ and set $R = \langle x, y\rangle$. Then R is a group and $R/(R \cap K(Q))$ is isomorphic to a subgroup of the cyclic group $P/K(Q)$. Thus $R/Z(R)$ is cyclic, so $R = Z(R)$, that is, R is abelian and $x + y = y + x$. □

Recall that a permutation $f : Q \to Q$ of a loop $(Q,+)$ is a left *pseudoautomorphism* with left *companion* $c \in Q$ if $c + f(x + y) = (c + f(x)) + f(y)$ for all $x, y \in Q$. Right pseudoautomorphisms with their right companions are defined similarly.

Lemma 4.2. *Let $(Q,+)$ be a Moufang loop.*

(1) *A permutation f of Q is a left pseudoautomorphism with left companion $c \in Q$, iff f is a right pseudoautomorphism with right companion $-c \in Q$.*
(2) *Every inner mapping is a (left and right) pseudoautomorphism.*
(3) *If f is a pseudoautomorphism, then for each $a \in N(Q)$ and all $x \in Q$, $f(a + x) = f(a) + f(x)$, $f(x + a) = f(x) + f(a)$, and $f(a) \in N(Q)$.*
(4) *A pseudoautomorphism f with companion c is an automorphism if and only if $c \in N(Q)$.*

Proof. We prove (1) and leave (2) and (3) to the references, noting that (4) is clear. If f is a left pseudoautomorphism with left companion c, then

$$\begin{aligned} f(x+y) - c &= -\big[c - f(x+y)\big] = -\big[c + f(-y-x)\big] = -\big[\big(c + f(-y)\big) + f(-x)\big] \\ &= f(x) - \big(c + f(-y)\big) = f(x) + \big(f(y) - c\big) \end{aligned}$$

for $x, y \in Q$. □

Lemma 4.3. *Let $(Q,+)$ be a Moufang A-loop. Then*

(1) *$K(Q)$ is a normal subloop.*
(2) *For each $x \in Q$, $3x \in N(Q)$.*

Proof. (1) is from Lemma 2.2. For (2), just note that the inner mapping $y \mapsto x + (y - x)$ is both a pseudoautomorphism with companion $3x$ (since Q is Moufang) and an automorphism (since Q is an A-loop), and apply Lemma 4.2(4). □

Lemma 4.4. *In a Moufang loop $(Q, +)$, the following conditions are equivalent for an automorphism f of Q:*

(1) $-x + f(x) \in C(Q)$, $\forall x \in Q$.
(2) $f(x) - x \in C(Q)$, $\forall x \in Q$.
(3) $-x + f(x) = f(x) - x \in C(Q)$, $\forall x \in Q$.
(4) $-x + f^{-1}(x) \in C(Q)$, $\forall x \in Q$.
(5) $f^{-1}(x) - x \in C(Q)$, $\forall x \in Q$.
(6) $-x + f^{-1}(x) = f^{-1}(x) - x \in C(Q)$, $\forall x \in Q$.

Proof. Trivially, (3) implies (1) and (2). If (1) holds, then $f(x) = x + (-x + f(x)) = (-x + f(x)) + x$, so that $f(x) - x = x - f(x)$, i.e., (3) holds. Similarly, (2) implies (3). The equivalence of (4), (5), and (6) follows from replacing f with f^{-1}. Finally, apply f^{-1} to (3) and replace x with $-x$ to get (6), using that $C(Q)$ is a characteristic subloop. Similarly, (6) implies (3). □

Lemma 4.5. *In a Moufang loop $(Q, +)$, the following conditions are equivalent for an automorphism f of Q and for a fixed $i \in \{0, 1\}$:*

(1) $(-1)^i x + f(x) \in N(Q)$, $\forall x \in Q$.
(2) $f(x) + (-1)^i x \in N(Q)$, $\forall x \in Q$.
(3) $(-1)^i x + f^{-1}(x) \in N(Q)$, $\forall x \in Q$.
(4) $f^{-1}(x) + (-1)^i x \in N(Q)$, $\forall x \in Q$.

Proof. If $a + b \in N(Q)$, which is a normal subloop, then $b + a = -a + (a + b) + a \in N(Q)$. Thus (1) is equivalent to (2), and (3) is equivalent to (4). Apply f^{-1} to (1), and if $i = 1$, replace x with $-x$ to get (4), and conversely, (4) implies (1). □

Lemma 4.6. *In a Moufang loop $(Q, +)$, the following conditions are equivalent for an automorphism f of Q:*

(1) $-x + f(2x) \in N(Q)$, $\forall x \in Q$.
(2) $f(2x) - x \in N(Q)$, $\forall x \in Q$.
(3) $-2x + f^{-1}(x) \in N(Q)$, $\forall x \in Q$.
(4) $f^{-1}(x) - 2x \in N(Q)$, $\forall x \in Q$.

Moreover, if $(Q, +)$ is also an A-loop, then these conditions are equivalent to the conditions of Lemma 4.5 with $i = 0$.

Proof. The equivalence of the conditions is proven similarly to Lemma 4.5. Now if $(Q, +)$ is an A-loop, then $3x \in N(Q)$ for all $x \in Q$. Thus if the conditions hold, $x + f(x) = x + f(-2x) + f(3x) \in N(Q)$, using (1) and the fact that $N(Q)$ is a characteristic subloop. But then condition (1) of Lemma 4.5 holds. The converse is similar. □

5. NK-loops

Lemma 5.1 *(Pflugfelder's theorem). Let $(Q,+)$ be a loop and $A: Q \to Q$ a mapping. The following are equivalent.*

(1) $(x+y)+(z+A(x)) = x+((y+z)+A(x))$ *for all* $x, y, z \in Q$,
(2) $(x+y)+(z+A(x)) = (x+(y+z))+A(x)$ *for all* $x, y, z \in Q$,
(3) $(Q,+)$ *is a Moufang loop and* $-x+A(x) \in N(Q)$ *for all* $x \in Q$.

Moreover, if any (and hence all) of these conditions hold, then the subloop $\langle x, A(x), y\rangle$ is a group for each $x, y \in Q$. In addition,

$$K(Q) = \big\{a \in Q\colon\ (x+a)+\big(y+A(x)\big) = (x+y)+\big(a+A(x)\big)\ \forall x, y \in Q\big\}.$$

Proof. Everything except the final assertion can be found in [17]. Now if $a \in K(Q)$, then $(x+a)+(y+A(x)) = x+((a+y)+A(x)) = x+((y+a)+A(x)) = (x+y)+(a+A(x))$. Conversely, if $a \in Q$ is such that $(x+a)+(y+A(x)) = (x+y)+(a+A(x))$ holds for all $x, y \in Q$, then taking $x = 0$, we have $a+(y+A(0)) = y+(a+A(0))$. But $A(0) = -0+A(0) \in N(Q)$, and so we may cancel to obtain $a+y = y+a$, that is, $a \in K(Q)$. □

Theorem 5.2. *Let $(Q,+)$ be a loop and $A: Q \to Q$ a mapping. The following are equivalent.*

(1) $(x+A(x))+(y+z) = (x+y)+(A(x)+z)$ *for all* $x, y, z \in Q$,
(2) $(Q,+)$ *is a Moufang loop, and* $A(x) \in K(Q)$, $-x+A(x) \in N(Q)$ *for all* $x \in Q$.

Moreover, if either (and hence both) of these conditions hold, $(Q,+)$ is an NK-loop.

Proof. (1) ⇒ (2): We let $-x$ denote the right inverse of x in Q, that is, $x+(-x) = 0$. Taking $y = 0$ in (1), we have $(x+A(x))+y = x+(A(x)+y)$. Thus $x+(A(x)+(y+z)) = (x+y)+(A(x)+z)$. Taking $z = -A(x)$ and canceling, we obtain $A(x)+(y+(-A(x))) = y$. Replace y with $A(x)+y$ and cancel to get

$$\big(A(x)+y\big)+\big(-A(x)\big) = y. \tag{5.1}$$

Next,

$$\begin{aligned}
&\big[(x+y)+A(x+y)\big]+\big[A(x)+\big(-A(x+y)\big)\big]\\
&\quad = (x+y)+A(x) = (x+y)+\big(A(x)+0\big) = \big(x+A(x)\big)+y\\
&\quad = \big(x+A(x)\big)+\big[\big(A(x+y)+y\big)+\big(-A(x+y)\big)\big]\\
&\quad = \big[x+\big(A(x+y)+y\big)\big]+\big[A(x)+\big(-A(x+y)\big)\big]
\end{aligned}$$

using (1) twice, then (5.1), and then (1) again. Canceling, we obtain

$$\begin{aligned}
(x+y)+A(x+y) &= x+\big(A(x+y)+y\big) = \big[(x+y)+u\big]+\big(A(x+y)+y\big)\\
&= \big[(x+y)+A(x+y)\big]+(u+y),
\end{aligned}$$

where $u = u(x, y)$ satisfies $(x + y) + u = x$. Canceling, we have $0 = u + y$, whence u is independent of x and $y = -u$. Thus $(x + (-u)) + u = x$ for all $x, u \in Q$. Now adding $A(x)$ on the right of (5.1), we obtain $A(x) + y = y + A(x)$, i.e., $A(x) \in C(Q)$ for all $x \in Q$. Finally,

$$\begin{aligned} x + \big((y + z) + A(x)\big) &= x + \big(A(x) + (y + z)\big) = \big(x + A(x)\big) + (y + z) \\ &= (x + y) + \big(A(x) + z\big) = (x + y) + \big(z + A(x)\big). \end{aligned}$$

Applying Lemma 5.1, we have that $(Q, +)$ is Moufang and $-x + A(x) \in N(Q)$. Since $K(Q) = C(Q)$ in Moufang loops, the proof is complete.

(2) $\Rightarrow$ (1): Using Lemma 5.1 and $A(x) \in K(Q) = C(Q)$, $(x + y) + (A(x) + z) = (x + y) + (z + A(x)) = x + ((y + z) + A(x)) = x + (A(x) + (y + z))$. Since $\langle x, A(x), y + z\rangle$ is a group, $(x + y) + (A(x) + z) = (x + A(x)) + (y + z)$.

Proof of "moreover": $x = A(x) - (-x + A(x))$. □

Lemma 5.3. *Let $(Q, +)$ be an NK-loop. Then the mapping $N(Q) \times K(Q) \to Q$; $(n, k) \mapsto n + k$ is an epimorphism of loops.*

Proof. For $n_1, n_2 \in N(Q)$, $k_1, k_2 \in K(Q)$, $(n_1 + k_1) + (n_2 + k_2) = n_1 + (k_1 + (n_2 + k_2)) = n_1 + ((n_2 + k_2) + k_1) = (n_1 + n_2) + (k_2 + k_1) = (n_1 + n_2) + (k_1 + k_2)$. □

Theorem 5.4. *Every NK-loop is a Moufang A-loop.*

Proof. The class of Moufang A-loops is a variety (i.e., equational class), and hence is closed under direct products and homomorphic images. Obviously groups are Moufang A-loops, and commutative Moufang loops are also A-loops [6, Lemma VII.3.3, p. 116]. Thus if Q is an NK-loop, then $N(Q) \times K(Q)$ is a Moufang A-loop, and by Lemma 5.3, so is Q. □

Corollary 5.5. *A loop $(Q, +)$ is an NK-loop if and only if there exists a mapping $A : Q \to Q$ such that $(x + A(x)) + (y + z) = (x + y) + (A(x) + z)$ for all $x, y, z \in Q$.*

Proof. If $(Q, +)$ is an NK-loop, then $(Q, +)$ is a Moufang loop (Theorem 5.4), and there exists a mapping $A : Q \to Q$ such that $A(x) \in K(Q)$ and $-x + A(x) \in N(Q)$ for all $x \in Q$. We may then apply Theorem 5.2. The converse follows directly from that same theorem. □

Corollary 5.6. *Let Q be an NK-loop.*

(1) $Z(Q) = Z(N(Q)) = Z(K(Q))$.
(2) *$N(Q)$ is a normal subgroup of Q, $Q/N(Q)$ is a commutative Moufang loop of exponent* 3, *and $Q/N(Q) \cong K(Q)/Z(Q)$.*
(3) *$K(Q)$ is a normal commutative subloop of Q, $Q/K(Q)$ is a group, and $Q/K(Q) \cong N(Q)/Z(Q)$.*

Remark 5.7. Suppose $(Q, \cdot)$ is an NK-loop and set $P = N(Q) \times K(Q)$. As noted in the proof of Theorem 5.4, P is an NK-loop. In addition, $N(P) = N(Q) \times Z(K(Q))$, $K(P) = Z(N(Q)) \times K(Q)$, and $Z(P) = Z(N(Q)) \times Z(K(Q))$. The epimorphism $\pi : P \to Q$; $(n, k) \mapsto nk$ (Lemma 5.3) has kernel $\ker\pi = \{(x, x^{-1})\colon\ x \in Z(Q)\} \subseteq Z(P)$. Now $P \cong Q$ iff

$\ker\pi = \{(1,1)\}$ iff $Z(Q) = \{1\}$. But then $Z(P) = \{1\}$, and conversely, if $Z(P) = \{1\}$, $P \cong Q$. In this case, $N(Q)$ is a group with trivial center and $K(Q)$ is a commutative Moufang loop with trivial center. Note that by the Bruck–Slaby theorem, it follows that $K(Q)$ must be infinitely generated [6, Chapter VIII].

Lemma 5.8. *Let $(Q,+)$ be a commutative Moufang loop. If f is a pseudoautomorphism with companion c, then f is an automorphism and $c \in Z(Q)$.*

Proof. We show this for f a left pseudoautomorphism, the right case being dual. For all $x, y \in Q$, $(c + f(x)) + f(y) = c + f(x+y) = c + f(y+x) = (c + f(y)) + f(x)$. But then $c \in N(Q) = Z(Q)$. □

Lemma 5.9. *Let $(Q,+)$ be an NK-loop. If f is a pseudoautomorphism with companion c, then f is an automorphism and $c \in N(Q)$.*

Proof. First write $c = a + b$ where $a \in N(Q)$, $b \in K(Q)$, and we see easily that b is a companion of f. Now for $u \in K(Q)$, $v \in N(Q)$, we use Proposition 4.1(6) to compute $f(u) + v = f(u) + f(f^{-1}(v)) = f(u + f^{-1}(v)) = f(f^{-1}(v) + u) = v + f(u)$. Since $(Q,+)$ is an NK-loop, $f(u) \in K(Q)$. Similarly, $f^{-1}(u) \in K(Q)$, and so (the restriction of) f is a pseudoautomorphism of $K(Q)$ with companion b. By Lemma 5.8 and Corollary 5.6(1), $b \in Z(K(Q)) = Z(Q)$, and so f is an automorphism of $(Q,+)$. □

Lemma 5.10. *Let $(Q,+)$ be an NK-loop. Then*:

(1) *For each $x \in Q$, the subloop $\langle x, K(Q)\rangle$ is commutative.*
(2) *For each $x, y \in Q$, the subloop $\langle x, y, N(Q)\rangle$ is a group.*

Proof. For (1): combine Corollary 5.6(3) and Proposition 4.1(4).

For (2): By Lemma 5.3, we may assume without loss that Q is commutative. But then $N(Q) = Z(Q)$, and the assertion follows from the diassociativity of Q. □

Lemma 5.11. *Let $(Q,+)$ be a Moufang loop, and let $f \in \mathrm{Aut}(Q)$ satisfy $-x + f(x) \in K(Q)$ and $-x + f(2x) \in N(Q)$ for all $x \in Q$. Then $(Q,+)$ is an NK-loop and*

$$x + (y + z) = \big(f(x) + y\big) + \big(\big(f(-x) + x\big) + z\big).$$

Proof. Set $k(x) = -x + f^{-1}(x)$. By Lemmas 4.4 and 4.6, $k(x) \in K(Q)$ and $-k(x) + x = -f^{-1}(x) + 2x \in N(Q)$. Since $x = k(x) + (-k(x) + x) \in K(Q) + N(Q)$, Q is an NK-loop. By Theorem 5.2, $(x + k(x)) + (y + z) = (x + y) + (k(x) + z)$. That is, $f^{-1}(x) + (y + z) = (x + y) + ((-x + f^{-1}(x)) + z)$, and so replacing x with $f(x)$, we have the rest of the result. □

Lemma 5.12. *Let $(Q,+)$ be a Moufang loop, and let $f, g \in \mathrm{Aut}(Q)$ satisfy $-x + f(2x)$, $-x + g(2x) \in N(Q)$ for all $x \in Q$. Then*

$$K(Q) = \big\{a \in Q\colon \big(f^2(x) + a\big) + \big(y + g^2(x)\big) = \big(f^2(x) + y\big) + \big(a + g^2(x)\big)\ \forall x, y \in Q\big\}.$$

Proof. By Lemma 4.6, $-2x + f^{-1}(x) \in N(Q)$. Since $N(Q)$ is characteristic, $g(-2x) + gf^{-1}(x) \in N(Q)$. Now $g(-2x) + gf^{-1}(x) = ((g(-2x) + x) - x) + gf^{-1}(x)$ and since $g(-2x) + x \in N(Q)$ (again by Lemma 4.6), we have $-x + gf^{-1}(x) \in N(Q)$. Thus $g(-x) + g^2 f^{-1}(x) \in N(Q)$ since $N(Q)$ is characteristic. Setting $x = f^{-1}(u)$, we have $gf^{-1}(-u) + g^2 f^{-2}(u) \in N(Q)$. Now

$$gf^{-1}(-u) + g^2 f^{-2}(u) = \big(\big(-u + gf^{-1}(u)\big)^{-1} - u\big) + g^2 f^{-2}(u),$$

and since $-u + gf^{-1}(u) \in N(Q)$ as before, we have $-u + g^2 f^{-2}(u) \in N(Q)$ for all $u \in Q$. Now Pflugfelder's theorem applies with $A = g^2 f^{-2}$ and gives that $a \in K(Q)$ if and only if $(x + a) + (y + g^2 f^{-2}(x)) = (x + y) + (a + g^2 f^{-2}(x))$ for all $x, y \in Q$. Replacing x with $f^2(x)$, we have the desired result. □

6. F-quasigroups are linear over NK-loops

Throughout this section, let $(Q, \cdot)$ be an F-quasigroup and let $a, b \in Q$ be such that $hk = kh$ where $h = R_a$ and $k = L_b$ (see Lemma 3.2). Further, put

$$f = hR_{\beta(a)}h^{-1}, \qquad g = kL_{\alpha(b)}k^{-1}, \qquad p = hk\alpha h^{-1}, \qquad q = khk\beta k^{-1} \big(= hk\beta k^{-1}\big).$$

Observe that the mappings $f, g, p, q : Q \to Q$ are permutations of Q. Finally, put

$$x + y = h^{-1}(x) \cdot k^{-1}(y)$$

for all $x, y \in Q$ and set $0 = ba$. Then $(Q, +)$ is a (possibly noncommutative) loop isotopic to $(Q, \cdot)$ and 0 is the neutral element. Our goals are to show that $(Q, +)$ is an NK-loop and that $(Q, \cdot)$ is linear over the loop. To get there, we need a sequence of lemmas.

Lemma 6.1.

(1) $h(x + y) = f(x) + h(y)$ *for all* $x, y \in Q$.
(2) $h(x) = f(x) + c$ *for all* $x \in Q$, *where* $c = h(0) = ba \cdot a$.
(3) f *is a right pseudoautomorphism with right companion* c *of* $(Q, +)$.

Proof. For (1): We have

$$h\big(h(u) + k(v)\big) + k(w) = uv \cdot w = u\beta(w) \cdot vw = h\big(h(u) + k\beta(w)\big) + k\big(h(v) + k(w)\big)$$

for all $u, v, w \in Q$ by (F_r). Setting $x = h(u)$, $y = k(v)$, and $z = k(w)$, we get

$$h(x + y) + z = h\big(x + k\beta k^{-1}(z)\big) + k\big(hk^{-1}(y) + z\big) \quad \text{for all } x, y, z \in Q.$$

In particular, for $z = 0$, we get $h(x + y) = h(x + k\beta k^{-1}(0)) + h(y)$, since $khk^{-1} = h$. Moreover, $k\beta k^{-1}(0) = k\beta k^{-1}(ba) = k\beta(a)$ and $h(x + k\beta(a)) = h(h^{-1}(x) \cdot \beta(a)) = f(x)$. Thus $h(x + y) = f(x) + h(y)$ for all $x, y \in Q$ as claimed.

(2) follows from (1) by taking $y = 0$, and (3) follows from (1) and (2). □

Lemma 6.2.

(1) $k(x+y)=k(x)+g(y)$ *for all* $x, y \in Q$.
(2) $k(y)=d+g(y)$ *for all* $x \in Q$, *where* $d=k(0)=b\cdot ba$.
(3) g *is a left pseudoautomorphism with left companion* d *of* $(Q,+)$.

Proof. (1) can be proved similarly to 6.2(1) using (F_l), and (2) and (3) follow similarly. □

Lemma 6.3.

(1) $x+(y+z)=(f(x)+y)+(p(x)+z)$ *for all* $x, y, z \in Q$.
(2) $x=f(x)+p(x)$ *for all* $x \in Q$.
(3) $(x+pf^{-1}(x))+(y+z)=(x+y)+(pf^{-1}(x)+z)$ *for all* $x, y, z \in Q$.

Proof. For (1): We have

$$\begin{aligned} h(u)+\big(kh(v)+gk(w)\big) &= h(u)+k\big(h(v)+k(w)\big) \\ &= u\cdot vw = uv\cdot\alpha(u)w \\ &= h\big(h(u)+k(v)\big)+k\big(h\alpha(u)+k(w)\big) \\ &= \big(fh(u)+hk(v)\big)+\big(hk\alpha(u)+gk(w)\big) \end{aligned}$$

for all $u, v, w \in Q$ by Lemma 6.1. Consequently, $x+(y+z)=(f(x)+y)+(p(x)+z)$ for all $x, y, z \in Q$.

(2) follows from (1) by taking $y=z=0$, and (3) follows from combining (1) and (2). □

Lemma 6.4.

(1) $(x+y)+z=(x+q(z))+(y+g(z))$ *for all* $x, y, z \in Q$.
(2) $z=q(z)+g(z)$ *for all* $z \in Q$.
(3) $(x+y)+(qg^{-1}(z)+z)=(x+qg^{-1}(z))+(y+z)$ *for all* $x, y, z \in Q$.

Proof. This is dual to Lemma 6.3. □

Theorem 6.5. $(Q,+)$ *is an NK-loop.*

Proof. This follows from Theorem 5.2 and Lemma 6.3(3) (or 6.4(3)). □

Lemma 6.6. $f, g \in \mathrm{Aut}(Q,+)$ *and* $c, d \in N(Q,+)$.

Proof. By Lemma 6.1, f is a right pseudoautomorphism with companion c. By Theorem 6.5, $(Q,+)$ is an NK-loop, so we may apply Lemma 5.9. The rest is dual. □

Lemma 6.7.

(1) $p(x), q(x) \in K(Q,+)$ *for all* $x \in Q$.
(2) $p(x)-f(x), q(x)-g(x) \in N(Q,+)$ *for all* $x \in Q$.

Proof. By Theorem 5.2, $pf^{-1}(x) \in K(Q,+)$ and $-x + pf^{-1}(x) \in N(Q,+)$ for every $x \in Q$. Since f is a permutation, $p(x) \in K(Q,+)$ and so $p(x) - f(x) = -f(x) + p(x) \in N(Q,+)$. The rest is dual. □

Lemma 6.8.

(1) $-x + f(x), -x + g(x) \in K(Q,+)$ *for all* $x \in Q$.
(2) $x + f(x), x + g(x) \in N(Q,+)$ *for all* $x \in Q$.

Proof. By Lemmas 6.3 and 6.7, $f(x) - x = (x - f(x))^{-1} = p(x)^{-1} \in K(Q,+)$ and so

$$-x + f(x) = -x + \big(f(x) - x\big) + x = f(x) - x \in K(Q,+).$$

By Lemma 6.7, $x - 2f(x) = p(x) - f(x) \in N(Q,+)$. Since $(Q,+)$ is an NK-loop, $3f(x) \in N(Q,+)$ by Corollary 5.6(2). Thus $x + f(x) = (x - 2f(x)) + 3f(x) \in N(Q,+)$. The remaining assertions are dual. □

Lemma 6.9. $hk\alpha(Q) \subseteq K(Q,+)$ *and* $hk\beta(Q) \subseteq K(Q,+)$.

Proof. This follows from $hk\alpha f^{-1} = p$, $hk\beta g^{-1} = q$, and Lemma 6.7. □

Lemma 6.10. *For all* $x \in Q$, $f(d) + fg(x) + c = d + gf(x) + g(c)$. *In particular,* $f(d) + c = d + g(c)$.

Proof. Implicitly using Lemma 6.6, we compute

$$\begin{aligned} f(d) + fg(x) + c &= fk(0) + fg(x) + h(0) = f\big(k(0) + g(x)\big) + h(0) = h\big(k(0) + g(x)\big) \\ &= hk(x) = kh(x) \\ &= k\big(f(x) + h(0)\big) = k(0) + g\big(f(x) + h(0)\big) = k(0) + gf(x) + gh(0) \\ &= d + gf(x) + g(c) \end{aligned}$$

by repeated use of Lemmas 6.1, 6.2, and 6.6. The rest follows from taking $x = 0$. □

Lemma 6.11.

(1) *If* $c \in K(Q,+)$, *then* $c \in Z(Q,+)$ *and* $fg = gf$.
(2) *If* $d \in K(Q,+)$, *then* $d \in Z(Q,+)$ *and* $fg = gf$.

Proof. The first assertion of (1) is clear from Lemma 6.6, and the rest follows from Lemma 6.10: $f(d) + c + fg(x) = d + g(c) + gf(x)$. (2) is dual to (1). □

Lemma 6.12.

(1) *If* $a \in \alpha(Q)$, *then* $c \in Z(Q,+)$.
(2) *If* $b \in \beta(Q)$, *then* $d \in Z(Q,+)$.

Proof. For (1), we have $c = ba \cdot a = hk(a) \in hk\alpha(Q) \subset K(Q,+)$, by Lemma 6.9. Putting this together with Lemma 6.6 gives the desired result. (2) is dual to (1). □

Putting all this together, we have the following.

Theorem 6.13. *Assume that $a \in \alpha(Q)$, $b \in \beta(Q)$ and $\alpha(b) = \beta(a)$ (see Lemma 3.2). Then*:

(1) $(Q,+)$ *is an NK-loop.*
(2) $f, g \in \mathrm{Aut}(Q,+)$ *and* $fg = gf$.
(3) $-x + f(x), -x + g(x) \in K(Q,+)$ *for every* $x \in Q$.
(4) $x + f(x), x + g(x) \in N(Q,+)$ *for every* $x \in Q$.
(5) $e = c + d = ba \cdot a + b \cdot ba = ba \cdot ba \in Z(Q,+)$.
(6) $xy = f(x) + g(y) + e$ *for all* $x, y \in Q$.

Proof. Combine Theorem 6.5 and Lemmas 6.6, 6.8, 6.11, and 6.12. □

Remark 6.14. For $r \in Q$, put $a = \alpha(r)$ and $b = \beta(r)$. Then $\alpha(b) = \alpha\beta(r) = \beta\alpha(r) = \beta(a)$ by Lemma 3.2, and so the hypotheses of Theorem 6.13 are satisfied in this case. Note that $0 = ba = \beta(r)\alpha(r)$ and $e = \beta(rr)\alpha(rr)$.

Lemma 6.15.

(1) *If* $a, b \in \alpha(Q)$, *then* $\alpha(Q) \subset K(Q,+)$.
(2) *If* $a, b \in \beta(Q)$, *then* $\beta(Q) \subset K(Q,+)$.
(3) *If* $a, b \in \alpha\beta(Q)$ $(= \beta\alpha(Q))$, *then* $\alpha(Q) \cup \beta(Q) \subset K(Q,+)$.

Proof. For (1): we have $a = \alpha(r)$, $b = \beta(s)$, $r, s \in Q$, and $\alpha(sx \cdot r) = b\alpha(x) \cdot a = hk\alpha(x) \in K(Q,+)$ for every $x \in Q$ by Lemma 6.9. Since $R_r L_s$ is a permutation of Q, $\alpha(Q) \subseteq K(Q,+)$.
Now (2) is dual to (1), and (3) follows from combining (1) and (2). □

7. Quasigroups linear over NK-loops

In this section, let Q be an NK-loop. We denote the underlying sets of $N(Q,+)$ and $K(Q,+)$ by just N and K, respectively.

Let $e \in N$ and let f, g be commuting automorphisms of $(Q,+)$ such that $-x + f(x)$, $-x + g(x) \in K$ and $x + f(x), x + g(x) \in N$ for all $x \in Q$. Now define a multiplication on Q by

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

for $x, y \in Q$. Denote the corresponding quasigroup by $(Q,\cdot)$.

Proposition 7.1.

(1) $(Q,\cdot)$ *is an F-quasigroup.*
(2) $\alpha(x) = -g^{-1}(e) - g^{-1}f(x) + g^{-1}(x)$ *for every* $x \in Q$.
(3) $\beta(x) = f^{-1}(x) - f^{-1}g(x) - f^{-1}(e)$ *for every* $x \in Q$.

Proof. First, $x = x\alpha(x) = f(x) + e + g\alpha(x)$, and so $\alpha(x) = -g^{-1}(e) - g^{-1}f(x) + g^{-1}(x)$. Further, by Lemma 5.11, $u + (v + w) = (f(u) + v) + ((-f(u) + u) + w)$ for all $u, v, w \in Q$. Setting $u = f(x) + e$, $v = fg(y) = gf(y)$, and $w = g(e) + g^2(z)$, we get

$$\begin{aligned}
x \cdot yz &= \big(f(x) + e\big) + \big(fg(y) + \big(g(e) + g^2(z)\big)\big) \\
&= u + (v + w) = \big(f(u) + v\big) + \big(\big(-f(u) + u\big) + w\big) \\
&= \big(f^2(x) + f(e) + fg(y)\big) + \big(\big(-f(e) - f^2(x) + f(x) + e\big) + \big(g(e) + g^2(z)\big)\big) \\
&= f\big(f(x) + e + g(y)\big) + \big(\big(e - f(e) - f^2(x) + f(x)\big) + \big(g(e) + g^2(z)\big)\big) \\
&= f(xy) + e + g\big(f\big(-g^{-1}(e) - g^{-1}f(x) + g^{-1}(x)\big) + e + g(z)\big) \\
&= f(xy) + e + g\big(f\alpha(x) + e + g(z)\big) \\
&= f(xy) + e + g\big(\alpha(x)z\big) \\
&= xy \cdot \alpha(x)z.
\end{aligned}$$

(Here we have used $-f(e) - f^2(x) + f(x) + e = e - f(e) - f^2(x) + f(x)$, since $-f^2(x) + f(x) \in K$ and $e - f(e) = -f(e) + e \in K$.) Thus we have verified (F_l), and the proof of (F_r) is dual to this. □

Lemma 7.2. *Let $(P, +)$ be a subloop of $(Q, +)$ such that $e \in P$ and $f(P) = P = g(P)$. Then*

(1) *$(P, \cdot)$ is a subquasigroup of $(Q, \cdot)$.*
(2) *If $(P, +)$ is a normal subloop, then $(P, \cdot)$ is a normal subquasigroup (and then the corresponding normal congruences coincide).*

Proof. (1) is clear. Now assume that $(P, +)$ is normal in $(Q, +)$ and denote by ρ the corresponding normal congruence of $(Q, +)$; P is a block of ρ. If $(a, b) \in \rho$, then $a - b \in P$, and so $f(a) - f(b) = f(a - b) \in P$, and so $(f(a), f(b)) \in \rho$. Consequently, $(ax, bx) = (f(a) + e + g(x), f(b) + e + g(x)) \in \rho$ for each $x \in Q$. The other cases to check are similar, and it follows that ρ is a normal congruence of the quasigroup Q, too. □

Remark 7.3. Consider the situation from Lemma 7.2 and put $(R, +) = (Q, +)/(P, +) = (Q, +)/\rho$. Then $(R, +)$ is an NK-loop and the automorphisms f, g induce automorphisms $\bar{f}, \bar{g}$ of $(R, +)$ such that $\pi f = \bar{f}\pi$, $\pi g = \bar{g}\pi$, where $\pi : Q \to R$ is the natural projection. Moreover, $\bar{e} = \pi(e) \in N(R, +)$. On the other hand, $(R, \cdot) = (Q, \cdot)/\rho$ is a factor quasigroup of $(Q, \cdot)$ and $\bar{x}\bar{y} = \bar{f}(\bar{x}) + \bar{e} + \bar{g}(\bar{y})$ for all $\bar{x}, \bar{y} \in R$.

Lemma 7.4. *Let $(P, +)$ be a subloop of $(Q, +)$ such that either $K \subseteq P$ or $N \subseteq P$. Then $f(P) = P = g(P)$.*

Proof. We have $-x + f(x), -x + f^{-1}(x), -x + g(x), -x + g^{-1}(x) \in K$ and $x + f(x)$, $x + f^{-1}(x), x + g(x), x + g^{-1}(x) \in N$. □

Throughout the rest of this section, we assume that $e \in Z(Q, +)$.

Lemma 7.5.

(1) $M = M(Q,\cdot) = K$ $(= M(Q,+)$ *by Proposition* 4.1(3)).
(2) $\alpha(Q) \cup \beta(Q) \subseteq M$.
(3) $x\alpha(z)\cdot yx = xy\cdot\alpha(z)x$ *and* $x\beta(y)\cdot zx = xz\cdot\beta(y)x$ *for all* $x, y, z \in Q$.
(4) M *is a normal subquasigroup of* $(Q,\cdot)$.
(5) *For each* $x \in Q$, *the subquasigroup* $\langle x, M\rangle$ *is trimedial.*
(6) M *is trimedial.*
(7) Q/M *is a group and in fact,* $Q/M \cong N(Q,+)/K(Q,+)$.

Proof. For (1): If $a \in M$, then

$$\big(f^2(x) + fg(a)\big) + \big(fg(y) + g^2(x)\big) + c = xa\cdot yx = xy\cdot ax = \big(f^2(x) + fg(y)\big) + \big(fg(a) + g^2(x)\big) + c,$$

where $c = f(e) + g(e) + e$. Setting $x = 0$, we get $fg(a) \in K$. Since K is characteristic, $a \in K$. We have thus shown $M \subseteq K$. Similarly, using Lemma 5.12, we may show the other inclusion.

For (2) and (3): We have $-f(x) + x \in K$, and so $\alpha(x) = g^{-1}(-e - f(x) + x) \in K$. Similarly, $\beta(x) \in K$.

For (4): Since $K(Q,+)$ is a normal subloop of $(Q,+)$ (by Corollary 5.6(3)), $(M,\cdot)$ is a normal subquasigroup by Lemmas 7.4 and 7.2.

For (5): Let $(P,+)$ be the subloop generated by $\{x, M\}$. By Lemma 5.10(1), $(P,+)$ is a commutative loop and by Lemmas 7.4 and 7.2, $(P,\cdot)$ is a subquasigroup of $(Q,\cdot)$. Now $(P,\cdot)$ is trimedial by Proposition 2.5.

(6) follows from (5).

For (7): From (2), $(Q/M,\cdot)$ is a loop, and hence a group by Lemma 3.4. Now consider the situation from Remark 7.3 where $P = M$. Since $-x + f(x) \in M$, we have $\bar f = \mathrm{Id}_{Q/M}$. Similarly, $\bar g = \mathrm{Id}_{Q/M}$ and, since $e \in M$, have $\bar e = \bar 0$ and $\bar x\bar y = \bar x + \bar y$ for all $\bar x, \bar y \in R = Q/M$. Thus $R = (Q,+)/K(Q,+) \cong N(Q,+)/(K(Q,+) \cap N(Q,+)) = N(Q,+)/Z(Q,+)$. □

Corollary 7.6. $(Q,\cdot)$ *is monomedial.*

Lemma 7.7.

(1) $(N,\cdot)$ *is a normal subquasigroup of* $(Q,\cdot)$.
(2) $(N,\cdot)$ *is an FG-quasigroup.*
(3) *For all* $x, y \in Q$, *the subquasigroup generated by* $\{x, y\} \cup N$ *is an FG-quasigroup.*
(4) $(Q/N,\cdot)$ *is a symmetric, distributive quasigroup* (*in particular, every block of the congruence corresponding to* N *is a subquasigroup of* $(Q,\cdot)$).

Proof. For (1): Combine Lemmas 7.2 and 7.4, and Corollary 5.6(2).

For (2) and (3): The subloop generated by the set is a group.

For (4): Consider again the situation from Remark 7.3 where $P = N(Q,+)$. Since $(Q,+)$ is an NK-loop, the factor loop $(R,+) = (Q,+)/(N,+)$ is a commutative Moufang loop (Corollary 5.6). Further, $x + f(x) \in N$ so that $\bar f(\bar x) = -\bar x$. Similarly, $\bar g(\bar x) = -\bar x$ and $\bar e = \bar 0$. Thus $\bar x\bar y = -\bar x - \bar y$ for all $\bar x, \bar y \in R$ and we apply Proposition 2.6. Finally, every block of ρ is a subquasigroup, since $R = Q/\rho = Q/N$ is idempotent. □

Lemma 7.8. *Let $a, b, c, d \in Q$. Then $ab \cdot cd = ac \cdot bd$ if and only if $(a + b) + (c + d) = (a + c) + (b + d)$.*

Proof. It is easy to see that $ab \cdot cd = ac \cdot bd$ if and only if $(fg^{-1}(a) + b) + (c + gf^{-1}(d)) = (fg^{-1}(a) + c) + (b + gf^{-1}(d))$. Since $a - fg^{-1}(a) \in N$ and $-gf^{-1}(d) + d \in N$, the latter equality is equivalent to $(a + b) + (c + d) = (a + c) + (b + d)$. □

Lemma 7.9. *If $a \in N$ and $b \in M$, then $xa \cdot by = xb \cdot ay$ for all $x, y \in Q$.*

Proof. The equality follows easily from Lemma 7.8. □

Lemma 7.10. *The quasigroup $(Q, \cdot)$ is a homomorphic image of the direct product $N \times M$ of the quasigroups N and M.*

Proof. According to Lemma 7.9, the mapping $(a, b) \mapsto ab$ is a homomorphism of $N \times M$ into Q. On the other hand, if $x \in Q$, then $x = c + d$, $c \in N$, $d \in M$, and $x = f^{-1}(c) \cdot g^{-1}(d - e)$, where $f^{-1}(c) \in N$, $g^{-1}(d - e) \in M$. Thus $Q = NM$ and the homomorphism is a projection. □

Lemma 7.11. *Every (at most) three-generated subquasigroup of $(Q, \cdot)$ is an FG-quasigroup.*

Proof. F-quasigroups with the indicated property form an equational class of quasigroups, and this class contains all FG-quasigroups and all trimedial quasigroups. Our result now follows from Lemma 7.10. □

Lemma 7.12.

(1) *$Z = N \cap M$ is a normal subquasigroup of Q.*
(2) *$(Z, \cdot)$ is a medial quasigroup.*
(3) *For every $x \in Q$, the subquasigroup generated by the set $\{x\} \cup Z$ is medial.*
(4) *Q/Z is isomorphic to a subquasigroup of $Q/N \times Q/M$, which is the product of a group and a symmetric distributive quasigroup.*

Proof. This follows from Lemmas 7.5 and 7.7. □

Lemma 7.13. *The following conditions are equivalent.*

(1) *$(Q, +)$ is commutative.*
(2) *$(Q, \cdot)$ is trimedial.*
(3) *$(Q, \cdot)$ is dimedial.*
(4) *$xx \cdot yx = xy \cdot xx$ for all $x, y \in Q$.*
(5) *$xx \cdot yy = xy \cdot xy$ for all $x, y \in Q$.*
(6) *$N(Q, +)$ is an abelian group.*

Proof. (1) ⇒ (2): This follows from Proposition 2.5.

(2) ⇒ (3) and (3) ⇒ (4), (5): Trivial.

(4) ⇒ (1): By Lemma 7.8, $(x + x) + (y + x) = (x + y) + (x + x)$ for all $x, y \in Q$. By diassociativity, we may cancel to get $x + y = y + x$, i.e., $(Q, +)$ is commutative.

(5) $\Rightarrow$ (1): This is proved similarly to the previous case.

(1) $\Rightarrow$ (6): Trivial.

(6) $\Rightarrow$ (2): $(N,\cdot)$ is a trimedial quasigroup, and so is $N\times M$, and so Q is trimedial by Lemma 7.10. $\square$

Lemma 7.14. *The following conditions are equivalent.*

(1) $(Q,+)$ *is a group.*
(2) $(Q,\cdot)$ *is an FG-quasigroup.*
(3) *Every four-generated subquasigroup of* Q *is an FG-quasigroup.*
(4) $x\alpha(u)\cdot yz = xy\cdot\alpha(u)z$ *for all* $x,y,z,u\in Q$.
(5) $x\beta(u)\cdot yz = xy\cdot\beta(u)z$ *for all* $x,y,z,u\in Q$.
(6) $x\alpha(u)\cdot\beta(v)z = x\beta(v)\cdot\alpha(u)z$ *for all* $x,y,u,v\in Q$.
(7) $K(Q,+)$ *is an abelian group.*

Proof. (1) $\Leftrightarrow$ (2), (2) $\Rightarrow$ (3), (4) $\Rightarrow$ (6), and (5) $\Rightarrow$ (6) are all trivial.

(3) $\Rightarrow$ (4): Four letters occur in the equality in (4), and so we may assume without loss of generality that (2), and hence (1), hold. In view of Lemma 7.8, we have to show that $x+\alpha(u)+y+z = x+y+\alpha(u)+z$, i.e., $\alpha(u)+y = y+\alpha(u)$. However, by Lemma 7.5(2), $\alpha(u)\in K(Q,+) = Z(Q,+)$.

(6) $\Rightarrow$ (7): By Lemma 7.8, $(x+\alpha(u))+(\beta(v)+y) = (x+\beta(v))+(\alpha(u)+y)$ for all $x,y,u,v\in K$. Setting $v=0$ and taking into account that $e\in Z(K) = Z(K(Q,+))$, we get $x+(-g^{-1}f(u)+g^{-1}(u))+y = x+((-g^{-1}f(u)+g^{-1}(u))+y)$, i.e., $-g^{-1}f(u)+g^{-1}(u)\in Z(K)$ for every $u\in K$. Then $-f(u)+u\in Z(K)$ and since $u+f(u)\in Z(K)$, we get $2u\in Z(K)$. But $3u\in Z(K)$ implies $u\in Z(K)$. Thus $(K,+)$ is an abelian group.

(7) $\Rightarrow$ (1): By Corollary 5.6(1), $(Q,+)$ is an image of the product $N(Q,+)\times K(Q,+)$. This product is a group. $\square$

Lemma 7.15. *The following conditions are equivalent.*

(1) $(Q,+)$ *is an abelian group.*
(2) $(Q,\cdot)$ *is medial.*
(3) $xx\cdot yx = xy\cdot xx$ *and* $x\alpha(u)\cdot\beta(v)y = x\beta(v)\cdot\alpha(u)y$ *for all* $x,y,u,v\in Q$.
(4) $xx\cdot yy = xy\cdot xy$ *and* $x\alpha(u)\cdot\beta(v)y = x\beta(v)\cdot\alpha(u)y$ *for all* $x,y,u,v\in Q$.

Proof. Combine Lemmas 7.13 and 7.14. $\square$

Lemma 7.16. *If* $(Q,\cdot)$ *is unipotent, then* $(Q,\cdot)$ *is medial.*

Proof. According to Lemma 7.15, it is sufficient to show that $(Q,+)$ is an abelian group. We have $f(x)+g(x)+e = xx = 0\cdot 0 = e$ and so $f(x)+g(x) = x$ for every $x\in Q$. Then $f=-g$, and so the mapping $x\mapsto -x$ is an automorphism of $(Q,+)$. Hence $(Q,+)$ is commutative. Further, from Lemma 7.7(4), Q/N is both unipotent and idempotent. Then Q/N is trivial, so that $Q=N$ and $(Q,+)$ is an abelian group. $\square$

8. Quasigroups linear over NK-loops II

We continue with the notational conventions of the preceding section, and continue to assume that $e \in Z(Q,+)$.

Lemma 8.1. *Let $p, q : Q \to Q$ be mappings. Then*:

(1) $(p,q) \in \mathcal{A}(Q)$ *if and only if there exists* $r \in N(Q,+)$ *such that* $p(x) = f(r) + x$ *and* $q(x) = r + x$ *for every* $x \in Q$.
(2) $(p,q) \in \mathcal{B}(Q)$ *if and only if there exists* $r \in N(Q,+)$ *such that* $p(x) = x + g(r)$ *and* $q(x) = x + r$ *for every* $x \in Q$.
(3) $(p,q) \in \mathcal{C}(Q)$ *if and only if there exists* $r \in N(Q,+)$ *such that* $p(x) = x + r$ *and* $q(x) = g^{-1}f(r) + x$ *for every* $x \in Q$.

Proof. For (1): $(p,q) \in \mathcal{A}(Q)$ if and only if $p(f(x) + g(y) + e) = p(xy) = q(x)y = fq(x) + g(y) + e$, or equivalently, if and only if $p(x+y) = fqf^{-1}(x) + y$ for all $x, y \in Q$, that is, if and only if $(p, fqf^{-1}) \in \mathcal{A}(Q,+)$. The rest is easy.

The proofs of (2) and (3) are similar. □

Lemma 8.2.

(1) $\mathcal{A}_l(Q) = \mathcal{A}_r(Q) = \mathcal{C}_l(Q)$.
(2) $\mathcal{B}_l(Q) = \mathcal{B}_r(Q) = \mathcal{C}_r(Q)$.
(3) *The permutation groups $\mathcal{A}_l(Q)$ and $\mathcal{B}_l(Q)$ are isomorphic to the group $N(Q,+)$.*

Proof. This follows from definitions and Lemma 8.1. □

Lemma 8.3. *Let ρ be the normal congruence of $(Q,\cdot)$ (and $(Q,+)$ as well) corresponding to N (see Lemma 7.7). Then*:

(1) $(a,b) \in \rho$ *if and only if* $a = p(b)$ *for some* $p \in \mathcal{A}_l(Q)$.
(2) $(a,b) \in \rho$ *if and only if* $a = p(b)$ *for some* $p \in \mathcal{B}_l(Q)$.
(3) $Q/\rho = \{N + u\colon u \in K\} = \{Nu\colon u \in K\} = \{uN\colon u \in K\}$.

Proof. This is elementary using Lemmas 8.1, 8.2, and 7.7. □

Construction 8.4. Fix $a \in K$, $b \in N$, and set $\tau(x) = (x+b)+a$ $(= x+b+a = x+a+b = (x+a)+b)$ and $x * y = ((x-b)+y)-a$ $(= (x-b+y)-a = -a + (x-b+y))$ for all $x, y \in Q$. We have defined a new binary operation $* : Q \times Q \to Q$.

(i) Using $a \in K$, we get

$$\tau(x) * \tau(y) = \big((x+b+a)-b\big) + (y+b+a) - a = \big((x+b)+(y+b+a)\big) - a$$
$$= \big((x+y+b)+2a\big) - a = (x+y+b) - a = \tau(x+y)$$

for $x, y \in Q$. This $\tau : (Q,+) \to (Q,*)$ is an isomorphism of binary structures. In particular, $(Q,*)$ is an NK-loop and the neutral element of $(Q,*)$ is $a+b = b+a$.

(ii) Since τ is an isomorphism, we have $N(Q,*) = \tau(N(Q,+)) = N(Q,+) + a$ and $K(Q,*) = \tau(K(Q,+)) = K(Q,+) + b$.

(iii) The mapping $h = \tau f \tau^{-1}$ is an automorphism of $(Q,*)$; we have

$$\begin{aligned} h(x) &= \tau f\big((x-b)-a\big) = \tau\big(f(x) - f(b) - f(a)\big) = \big(f(x) - f(b) - f(a)\big) + b + a \\ &= f(x) + \big(b - f(b)\big) + \big(a - f(a)\big) \end{aligned}$$

using $b - f(b), a + f(a) \in Z(Q,+)$. Similarly, $k = \tau g \tau^{-1}$ is an automorphism of $(Q,*)$, and we have $k(x) = g(x) + (b - g(b)) + (a - g(a))$.

(iv) Now $hk\tau = h\tau g = \tau f g = \tau g f = k\tau f = kh\tau$, and so $hk = kh$.

(v) For each $x \in Q$, $\tau^{-1}(x * h(x)) = \tau^{-1}(x) + \tau^{-1}h(x) = \tau^{-1}(x) + f\tau^{-1}(x) \in N(Q,+)$, and so $x * h(x) \in \tau(N(Q,+)) = N(Q,*)$. Similarly, $x * k(x) \in N(Q,*)$.

(vi) If $\tilde{x}$ denotes the inverse of x in the loop $(Q,*)$, then $\tilde{x} * h(x) \in K(Q,*)$ and $\tilde{x} * k(x) \in K(Q,*)$.

(vii) We have

$$\begin{aligned} xy &= f(x) + g(y) + e = \big(h(x) + \big(f(a) - a\big) + \big(f(b) - b\big)\big) \\ &\quad + \big(k(y) + \big(g(a) - a\big) + \big(g(b) - b\big)\big) + e \\ &= \big(h(x) + \big(f(a) - a\big)\big) + \big(k(y) + \big(g(a) - a\big)\big) + r, \end{aligned}$$

where $r = (f(b) - b) + (g(b) - b) + e \in Z(Q,+)$. Henceforth,

$$xy = \big(\big(h(x) + k(y)\big) - a\big) + s,$$

where $s = 3a + (a + f(a)) + (a + g(a)) + r \in Z(Q,+)$. Finally, $e_1 = 2b + a + s \in N(Q,+) + a = N(Q,*)$ and $h(x) * e_1 * k(y) = (((((h(x) - b) + e_1) - a) - b) + k(y)) - a = ((h(x) + (-b + e_1 - a - b)) + k(y)) - a = ((h(x) + k(y)) - a) + s$. We have shown that $xy = h(x) * e_1 * k(y)$ for all $x, y \in Q$.

(viii) Note that $e_1 \in Z(Q,*)$ if and only if $b \in Z(Q,+)$ (or $b \in K(Q,+)$).

(ix) Put $N_1 = N + a$. By Lemma 7.7, N_1 is a block of the congruence ρ corresponding to N and N_1 is a normal subquasigroup of $(Q,\cdot)$. Now N_1 is the underlying set of $N(Q,*)$ and, by (vii), $uv = h(u) * e_1 * k(v)$ for all $u, v \in N_1$. In particular, N_1 is an FG-quasigroup isotopic to $N(Q,*)$. The groups $N(Q,+)$ and $N(Q,*)$ are isomorphic.

(x) Put $e_2 = b + s$, so that $\tau(e_2) = e_1$ and $e_2 \in N(Q,+)$. Now define a binary operation $\Delta : Q \times Q \to Q$ by $x \Delta y = f(x) + e_2 + g(y)$ for $x, y \in Q$. Then $\tau(x \Delta y) = f\tau(x) * \tau(e_2) * g\tau(y) = h\tau(x) * e_1 * k\tau(y) = \tau(x)\tau(y)$. Thus $\tau : (Q,\Delta) \to (Q,\cdot)$ is an isomorphism of quasigroups.

(xi) Put $e_3 = (e + b) + a$ so that $\tau(e) = e_3$ and $e_3 \in N(Q,*)$. Now define a binary operation $\nabla : Q \times Q \to Q$ by $x \nabla y = h(x) * e_3 * k(y)$. Then $\tau(xy) = \tau(x) \nabla \tau(y)$ and consequently, $\tau : (Q,\cdot) \to (Q,\nabla)$ is an isomorphism of quasigroups.

9. Arithmetic forms of F-quasigroups

An ordered five-tuple $(Q,+,f,g,e)$ will be called an *arithmetic form* of a quasigroup $(Q,\cdot)$ if

(1) $(Q,+)$ is an NK-loop;
(2) f, g are commuting automorphisms of $(Q,+)$;
(3) $x + f(x), x + g(x) \in N(Q,+)$ for every $x \in Q$;
(4) $-x + f(x), -x + g(x) \in K(Q,+)$ for every $x \in Q$;
(5) $e \in N(Q,+)$;
(6) $xy = f(x) + e + g(y)$ for all $x, y \in Q$.

If, moreover,

(7) $e \in Z(Q,+)$,

then the arithmetic form will be called *strong*.

Theorem 9.1. *The following conditions are equivalent for a quasigroup* $(Q,\cdot)$.

(1) $(Q,\cdot)$ *is an F-quasigroup.*
(2) $(Q,\cdot)$ *has at least one strong arithmetic form.*
(3) $(Q,\cdot)$ *has at least one arithmetic form.*

Proof. (1) $\Rightarrow$ (2): Take $r \in Q$ arbitrarily and put $a = \alpha(r)$, $b = \beta(r)$ (see Remark 6.14). Then $\alpha(b) = \beta(a)$ and, by Theorem 6.13, we get a strong arithmetic form $(Q,+,f,g,e)$ of the quasigroup $(Q,\cdot)$. Note that $0 = ba = \alpha(r)\beta(r)$ and $e = \beta(rr)\alpha(rr)$.
(2) $\Rightarrow$ (3): Trivial
(3) $\Rightarrow$ (1): This follows from Proposition 7.1. □

Lemma 9.2. *Let* $(Q,+,f,g,e_1)$ *and* $(P,+,h,k,e_2)$ *be arithmetic forms of F-quasigroups* $(Q,\cdot)$ *and* $(P,\cdot)$*, respectively. Let* $\varphi : Q \to P$ *be a mapping such that* $\varphi(0_Q) = 0_P$*. Then* φ *is a homomorphism of quasigroups if and only if* φ *is a homomorphism of loops such that* $\varphi f = h\varphi$*,* $\varphi g = k\varphi$ *and* $\varphi(e_1) = e_2$.

Proof. Assume that φ is a homomorphism of quasigroup structures, the other case being easy. Now $\varphi(f(x) + e_1 + g(y)) = \varphi(xy) = \varphi(x)\varphi(y) = h\varphi(x) + e_2 + k\varphi(y)$ for all $x, y \in Q$. Setting $x = y = 0_Q$, we get $\varphi(e_1) = e_2$. Setting $y = g^{-1}(-e_1)$, we get $\varphi f(x) = h\varphi(x) + \varphi(e_1) + k\varphi g^{-1}(-e_1)$, and hence $x = 0_Q$ yields $\varphi(e_1) + +k\varphi g^{-1}(-e_1) = 0$. Thus $\varphi f = h\varphi$, and similarly, $\varphi g = k\varphi$. From this we conclude that $\varphi(x + e_1 + y) = \varphi(x) + \varphi(e_1) + \varphi(y)$ for all $x, y \in Q$. In particular, $\varphi(e_1 + y) = \varphi(e_1) + \varphi(y)$, $\varphi(x + r) = \varphi(x) + \varphi(r)$, $r = e_1 + y$, and so $\varphi : (Q,+) \to (P,+)$ is a homomorphism. □

Lemma 9.3. *Let* $(Q,+,f_1,g_1,e_1)$ *and* $(Q,*,f_2,g_2,e_2)$ *be arithmetical forms of an F-quasigroup* $(Q,\cdot)$ *such that the loops* $(Q,+)$ *and* $(Q,*)$ *have the same neutral element* 0*. Then* $(Q,+) = (Q,*)$*,* $f_1 = f_2$*,* $g_1 = g_2$*,* $e_1 = e_2$*, i.e., the forms coincide.*

Proof. The assertion follows from Lemma 9.2 where $\varphi = \mathrm{Id}_Q$. □

Theorem 9.4. *Let* $(Q,\cdot)$ *be an F-quasigroup. Then there exists a one-to-one correspondence between* (*strong*) *arithmetic forms of the quasigroup and elements from* Q (*respectively* $M(Q)$).

More precisely, for every element $w \in Q$ ($w \in M(Q)$) there exists just one arithmetic form of Q such that w is a neutral element of the corresponding loop.

Proof. By Theorem 9.1(ii), $(Q, \cdot)$ has at least one strong arithmetic form, say $(Q, +, f, g, e)$. Now if $w \in Q$, then $w = a + b$ for some $a \in K(Q, +)$ and some $b \in N(Q, +)$. By Construction 8.4, we get an arithmetic form $(Q, *, h, k, e_1)$ of Q such that $0_{(Q,*)} = a + b = w$. (By 8.4(viii) and Lemma 7.5(1), the form is strong iff $b \in Z(Q, +)$ and hence iff $w \in M(Q)$.) Finally the uniqueness of the form $(Q, *, h, k, e_1)$ follows from Lemma 9.3. □

Denote by $\mathcal{F}_p$ the equational class (and category) of pointed F-quasigroups. That is, $\mathcal{F}_p$ consists of ordered pairs (Q, a), where Q is an F-quasigroup and $a \in Q$. If $(P, b) \in \mathcal{F}_p$, then a mapping $\varphi : Q \to P$ is a homomorphism in $\mathcal{F}_p$ if and only if φ is a homomorphism of quasigroups and $\varphi(a) = b$. Further, put $\mathcal{F}_m = \{(Q, a) \in \mathcal{F}_p\colon\ a \in M(Q)\}$. Then $\mathcal{F}_m$ is an equational subclass (and a full subcategory) of $\mathcal{F}_p$.

Denote by $\mathcal{E}$ the equational class (and category again) of algebras $(Q, +, f, g, f^{-1}, g^{-1}, e)$ where $(Q, +)$ is an NK-loop and the conditions (2), (3), (4), (5) of the definition of arithmetic form hold. If $(P, +, h, k, h^{-1}, k^{-1}, e_1) \in \mathcal{E}$, then a mapping $\varphi : Q \to P$ is a homomorphism in $\mathcal{E}$ if and only if φ is a homomorphism of loops such that $\varphi f = h\varphi$, $\varphi g = k\varphi$, and $\varphi(e) = e_1$. Further, put $\mathcal{E}_c = \{(Q, +, f, g, f^{-1}, g^{-1}, e) \in \mathcal{E}\colon\ e \in Z(Q, +)\}$. Then $\mathcal{E}_c$ is an equational subclass (and full subcategory) of $\mathcal{E}$. Let $(Q, a) \in \mathcal{F}_p$. By Theorem 9.4 (and its proof), there is just one arithmetic form $(Q, +, f, g, e)$ of $(Q, \cdot)$ such that $a = 0_{(Q,+)}$ (and $e \in Z(Q, +)$ if and only if $a \in M(Q)$). Now put $\Phi((Q, a)) = (Q, +, f, g, f^{-1}, g^{-1}, e)$.

Let $(Q, +, f, g, f^{-1}, g^{-1}, e) \in \mathcal{E}$. Then set $\Psi((Q, +, f, g, f^{-1}, g^{-1}, e)) = (Q, 0_{(Q,+)}) \in \mathcal{F}_p$, where a multiplication on Q is defined by $xy = f(x) + e + g(y)$ ($0 \in M(Q)$ if and only if $e \in Z(Q, +)$).

It follows from Theorem 9.4 that Φ and Ψ are mutually inverse, one-to-one correspondences between the classes $\mathcal{F}_p$ and $\mathcal{E}$, $\Phi : \mathcal{F}_p \to \mathcal{E}$ and $\Psi : \mathcal{E} \to \mathcal{F}_p$. If $A, B \in \mathcal{F}_p$, then a homomorphism $\varphi : A \to B$ is a homomorphism in $\mathcal{F}_p$ if and only if $\varphi : \Phi(A) \to \Phi(B)$ is a homomorphism in $\mathcal{E}$ (see Lemma 9.2). This implies that the classes $\mathcal{F}_p$ and $\mathcal{E}$ are equivalent.

Summarizing this discussion, we have the following.

Corollary 9.5. *The class $\mathcal{F}_p$ of pointed F-quasigroups is equivalent to the class $\mathcal{E}$. The equivalence restricts to an equivalence between the class $\mathcal{F}_m$ of M-pointed F-quasigroups and the class $\mathcal{E}_c$.*

Remark 9.6. Let $\varphi : Q \to P$ be a homomorphism of F-quasigroups. If $a \in \alpha(Q)$ ($a \in \beta(Q)$, respectively), then $\varphi(a) \in \alpha(P)$ ($\varphi(a) \in \beta(P)$, respectively), and $(Q, a), (P, \varphi(a)) \in \mathcal{F}_m$ and $\varphi : (Q, a) \to (P, \varphi(a))$ is a homomorphism in the class $\mathcal{E}_c$.

10. Summary of structure results on F-quasigroups

Theorem 10.1. *Let $(Q, \cdot)$ be an F-quasigroup.*

(1) *$M = M(Q)$ is a normal subquasigroup of Q.*
(2) *M is a trimedial quasigroup and Q/M is a group.*
(3) *$\alpha(Q) \cup \beta(Q) \subseteq M$.*
(4) *For each $a \in Q$, the subquasigroup generated by the set $\{a\} \cup M$ is trimedial.*

Proof. Combine Theorem 9.1 with Lemma 7.5. □

Corollary 10.2. *Let $(Q,\cdot)$ be an F-quasigroup.*

(1) *Both $\alpha(Q)$ and $\beta(Q)$ are trimedial subquasigroups. Moreover, the subquasigroup generated by $\alpha(Q)\cup\beta(Q)$ is trimedial.*
(2) *$x\alpha(z)\cdot yx = xy\cdot\alpha(z)x$ and $x\beta(z)\cdot yx = xy\cdot\beta(z)x$ for all $x,y,z\in Q$.*
(3) *$(Q,\cdot)$ is monomedial.*

Corollary 10.3. *Every one-generated F-quasigroup is medial.*

Theorem 10.4. *Let $(Q,\cdot)$ be an F-quasigroup. Define a relation ρ on Q by $(a,b)\in\rho$ if and only if $a = p(b)$ for a regular permutation p of Q. Then*:

(1) *ρ is a normal congruence of $(Q,\cdot)$.*
(2) *Every block of ρ is a normal subquasigroup of Q and an FG-quasigroup.*
(3) *Q/ρ is a symmetric distributive quasigroup.*
(4) *If N is a block of ρ and $a,b\in Q$, then the subquasigroup generated by the set $\{a,b\}\cup N$ is an FG-quasigroup.*
(5) *Every (at most) three-generated subquasigroup of $(Q,\cdot)$ is an FG-quasigroup.*

Proof. See Theorem 9.1, Lemmas 8.3 and 7.7, and Construction 8.4(ix). □

Corollary 10.5. *Every (at most) three-generated F-quasigroup is an FG-quasigroup.*

Theorem 10.6. *Let $(Q,\cdot)$ be an F-quasigroup and N a block of the normal congruence ρ (see Theorem* 10.4*). Then the mapping $(a,u)\mapsto au$, $a\in N$, $u\in M$ is a surjective homomorphism of the direct product $N\times M(Q)$ onto Q.*

Proof. See Theorem 9.1 and Lemma 7.10. □

Proposition 10.7. *The following conditions are equivalent for an F-quasigroup $(Q,\cdot)$.*

(1) *$(Q,\cdot)$ is trimedial.*
(2) *$(Q,\cdot)$ is dimedial.*
(3) *$xx\cdot yx = xy\cdot xx$ for all $x,y\in Q$.*
(4) *$xx\cdot yy = xy\cdot xy$ for all $x,y\in Q$.*
(5) *At least one of the blocks of the normal congruence ρ is a trimedial quasigroup.*

Proof. See Theorem 9.1, Lemma 7.13, and Theorem 10.6. □

Proposition 10.8. *The following conditions are equivalent for an F-quasigroup $(Q,\cdot)$.*

(1) *Q is an FG-quasigroup.*
(2) *Every four-generated subquasigroup of Q is an FG-quasigroup.*
(3) *$x\alpha(u)\cdot yz = xy\cdot\alpha(u)z$ for all $x,y,z,u\in Q$.*
(4) *$x\beta(u)\cdot yz = xy\cdot\beta(u)z$ for all $x,y,z,u\in Q$.*

(5) $x\alpha(u)\cdot\beta(v)y = x\beta(v)\cdot\alpha(u)y$ *for all* $x, y, u, v \in Q$.
(6) $M(Q)$ *is a medial quasigroup.*

Proof. See Theorem 9.1 and Lemma 7.14. □

Remark 10.9. Let $(Q,\cdot)$ be an F-quasigroup. By Corollary 10.2(1), the subquasigroup generated by $\alpha(Q)\cup\beta(Q)$ is trimedial. In particular, Q is trimedial provided that $\alpha(Q) = Q$ or $\beta(Q) = Q$. On the other hand, if α (β, respectively) is injective, then Q can be imbedded into an F-quasigroup $(P,\cdot)$ such that α (β, respectively) is a permutation of P. (This is a standard construction using the fact that α and β are endomorphisms.) But then $(P,\cdot)$ is trimedial, and hence so is $(Q,\cdot)$.

Remark 10.10. It follows immediately from Theorem 10.1 that every (congruence-)simple F-quasigroup is either a simple group or a simple trimedial quasigroup. While there are many simple groups, simple trimedial quasigroups are necessarily finite and medial, and all of them can be found in [8].

Remark 10.11. Let $(Q,\cdot)$ be an F-quasigroup and N_1, N_2 two blocks of the normal congruence ρ (see Theorem 10.4). Then both N_1 and N_2 are FG-quasigroups and it follows from Construction 8.4(ix) that these quasigroups are isotopic to isomorphic groups.

Remark 10.12. Let $(Q,+,f,g,e)$ be a strong arithmetic form of an F-quasigroup $(Q,\cdot)$. If $x\circ y = f(x)+g(y)$ for all $x, y\in Q$, then $(Q,\circ)$ is again an F-quasigroup and the neutral element 0 is an idempotent element of $(Q,\circ)$. We have $x\circ y = (xy)-e$, so that the quasigroups $(Q,\cdot)$ and $(Q,\circ)$ are isotopic. In this way, we have proved that every F-quasigroup is isotopic to an F-quasigroup containing at least one idempotent element.

Remark 10.13.

(i) Consider a finite F-quasigroup $(Q,\cdot)$ which is minimal with respect to the property of *not* being an FG-quasigroup. It follows from Theorem 10.6 that $M(Q)$ is not an FG-quasigroup, and hence $Q = M(Q)$ is trimedial. Of course, Q is not medial. Now according to [14], we have $|Q| = 81$. By [14], there exist just 35 isomorphism classes of nonmedial, trimedial quasigroups of order 81.
(ii) Consider a finite F-quasigroup $(P,\cdot)$ which is minimal with respect to the property of *not* being trimedial. It follows easily from Theorem 10.6 that P is a copy of the symmetric group on three letters, and so $|P| = 6$.

Acknowledgments

We are pleased to acknowledge the assistance of OTTER, an automated deduction tool developed by McCune [15]. OTTER found a proof of Theorem 5.2, which we then "humanized" into the form presented here.

References

[1] V.D. Belousov, About one quasigroup class, Uchenye Zapiski Beltskogo Gospedinstituta im. A. Russo 5 (1960) 29–44 (in Russian).

[2] V.D. Belousov, The structure of distributive quasigroups, Mat. Sb. (N.S.) 50 (92) (1960) 267–298 (in Russian).
[3] V.D. Belousov, Foundations of the Theory of Quasigroups and Loops, Nauka, Moscow, 1967 (in Russian).
[4] V.D. Belousov, Elements of Quasigroup Theory: A Special Course, Kishinev State University Press, Kishinev, 1981 (in Russian).
[5] R.H. Bruck, Some results in the theory of quasigroups, Trans. Amer. Math. Soc. 55 (1944) 19–52.
[6] R.H. Bruck, A Survey of Binary Systems, Springer-Verlag, 1971.
[7] I.A. Golovko, Loops that are isotopic to F-quasigroups, Bul. Akad. Štiince RSS Mold. 1970 (1970) 3–13 (in Russian).
[8] J. Ježek, T. Kepka, Medial groupoids, Rozpravy Československé Akad. Věd Řada Mat. Přírod. Věd 93 (2) (1983), 93 p.
[9] T. Kepka, Quasigroups which satisfy certain generalized forms of the abelian identity, Čas. Pěst. Mat. 100 (1975) 46–60.
[10] T. Kepka, Structure of triabelian quasigroups, Comment. Math. Univ. Carolin. 17 (1976) 229–240.
[11] T. Kepka, Structure of weakly abelian quasigroups, Czechoslovak Math. J. 28 (103) (1978) 181–188.
[12] T. Kepka, A note on WA-quasigroups, Acta Univ. Carolin. Math. Phys. 19 (1978) 61–62.
[13] T. Kepka, F-quasigroups isotopic to Moufang loops, Czechoslovak Math. J. 29 (1979) 62–83.
[14] T. Kepka, L. Bénéteau, J. Lacaze, Small finite trimedial quasigroups, Comm. Algebra 14 (1986) 1067–1090.
[15] W.W. McCune, OTTER 3.3 reference manual and guide, Technical Memorandum ANL/MCS-TM-263, Argonne National Laboratory, 2003, or see: http://www.mcs.anl.gov/AR/otter/.
[16] D.C. Murdoch, Quasi-groups which satisfy certain generalized associative laws, Amer. J. Math. 61 (1939) 509–522.
[17] H.O. Pflugfelder, A special class of Moufang loops, Proc. Amer. Math. Soc. 26 (1970) 583–586.
[18] H.O. Pflugfelder, Quasigroups and Loops: Introduction, Sigma Ser. Pure Math., vol. 8, Heldermann-Verlag, Berlin, 1990.
[19] L.V. Sabinin, Smooth Quasigroups and Loops, Math. Appl., vol. 492, Kluwer Academic Publishers, Dordrecht, 1999.
[20] K. Toyoda, On axioms of linear functions, Proc. Imp. Acad. Tokyo 17 (1941) 221–227.