Tomáš Kepka

$F$-quasigroups isotopic to Moufang loops


Persistent URL: [http://dml.cz/dmlcz/101579](http://dml.cz/dmlcz/101579)

**Terms of use:**

© Institute of Mathematics AS CR, 1979

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project **DML-CZ: The Czech Digital Mathematics Library** [http://dml.cz](http://dml.cz)
One of the oldest tasks of the theory of quasigroups is to study generalizations of groups. One of the oldest examples of generalized groups is the class of F-quasigroups (the first article on this subject has appeared in 1939). The main aim of the present paper is to describe F-quasigroups isotopic to Moufang loops. It is shown that these quasigroups consist of three basic classes, namely groups, medial quasigroups and distributive Steiner quasigroups. Unfortunately, the author does not know whether there are any F-quasigroups not isotopic to a Moufang loop.

1. PRELIMINARIES

Some details concerning quasigroups and loops may be found in [1] and [2].

Let \( Q \) be a quasigroup and \( a \in Q \). We denote by \( e(a) \) and \( f(a) \) the right and left local unit of \( a \), respectively. Hence \( f(a) \ a = a = a \ e(a) \) and \( e, f \) are mappings of \( Q \) into \( Q \). Further we define two mappings \( L_a, R_a \) of \( Q \) into \( Q \) by \( L_a(b) = ab \) and \( R_a(b) = ba \) for every \( b \in Q \). We denote by \( \mathcal{M}(Q) \) the group generated by all these permutations \( L_a, R_a, a \in Q \) and we put \( \mathcal{F}(Q, a) = \{ g \in \mathcal{M}(Q) \mid g(a) = a \} \). Further we put \( S(a, b) = L_b^{-1}L_a^{-1}L_{ab}, T(a, b) = R_a^{-1}R_b^{-1}R_{ab} \) and \( V(a) = R_a^{-1}L_a \) for all \( a, b \in Q \).

Let \( Q \) be a left (right) loop. The left (right) unit of \( Q \) will be denoted by \( j \). Further, if \( a \in Q \) then \( a^{-1} = b \) and \( -1a = c \), where \( ab = j = ca \). The following result is well known (see [1], Theorem 4.4).

1.1. Lemma. Let \( Q \) be a loop. Then the group \( \mathcal{F}(Q, j) \) is generated by the permutations \( S(a, b), T(a, b), V(a), a, b \in Q \).

A congruence \( r \) of a quasigroup \( Q \) is said to be normal if the factor \( Q/r \) is a quasigroup. A subquasigroup \( P \) of \( Q \) is said to be normal if \( P \) is a class of a normal congruence. The following result is classical (see [1], Theorem 4.5).
1.2. Lemma. A subloop $P$ of a loop $Q$ is normal iff $g(a) \in P$ for all $a \in P$ and $g \in \mathcal{F}(Q, j)$.

Let $Q$ be a quasigroup. We put

$$A(Q) = \{a \in Q \mid ba \cdot cd = bc \cdot ad \text{ for all } b, c, d \in Q\},$$

$$B_1(Q) = \{a \in Q \mid ab \cdot cd = ac \cdot bd \text{ for all } b, c, d \in Q\},$$

$$B_2(Q) = \{a \in Q \mid bc \cdot da = bd \cdot ca \text{ for all } b, c, d \in Q\},$$

$$M(Q) = \{a \in Q \mid ba \cdot cb = bc \cdot ab \text{ for all } b, c \in Q\},$$

$$D(Q) = \{a \in Q \mid ab \cdot ca = ac \cdot ba \text{ for all } b, c \in Q\},$$

$$N_1(Q) = \{a \in Q \mid a \cdot bc = ab \cdot c \text{ for all } b, c \in Q\},$$

$$N_2(Q) = \{a \in Q \mid bc \cdot a = b \cdot ca \text{ for all } b, c \in Q\},$$

$$N_3(Q) = \{a \in Q \mid ba \cdot c = b \cdot ac \text{ for all } b, c \in Q\},$$

$$N(Q) = N_1(Q) \cap N_2(Q) \cap N_3(Q),$$

$$K(Q) = \{a \in Q \mid ab = ba \text{ for every } b \in Q\},$$

$$C(Q) = N(Q) \cap K(Q),$$

$$\text{Id } Q = \{a \in Q \mid a = aa\}.$$ 

Moreover, we denote by $\text{Aut } Q$ the automorphism group of $Q$.

1.3. Lemma. Let $Q$ be a quasigroup. Then:

(i) $N_1(Q) (N_2(Q))$ is non-empty iff $Q$ is a left (right) loop. In this case, $N_1(Q)$ ($N_2(Q)$) is a subgroup of $Q$.

(ii) $N(Q)$ is non-empty iff $Q$ is a loop. In this case, $N(Q)$ is a subgroup of $Q$.

(iii) $C(Q)$ is non-empty iff $Q$ is a loop. In this case, $C(Q)$ is an abelian subgroup of $Q$.

Proof. See [1], Theorem 1.1.

A quasigroup $Q$ is called an S-quasigroup if $S(a, b)$ is an automorphism for all $a, b \in Q$. Similarly we define T-quasigroups, V-quasigroups, ST-quasigroups, STV-quasigroups. STV-loops are called also A-loops. The following lemma is clear from the definitions of $S(a, b)$, $T(a, b)$ and $V(a)$.

1.4. Lemma. Let $Q$ be a quasigroup. Then:

(i) $ab \cdot c = a \cdot bS(a, b)(c)$ and $c \cdot ab = T(a, b)(c) a \cdot b$ for all $a, b, c \in Q$.

(ii) $K(Q) = \{a \in Q \mid V(a) = 1\}$ and $K(Q) = \{a \in Q \mid V(b)(a) = a \text{ for every } b \in Q\}$. 

63
1.5. Lemma. Let $Q$ be an $A$-loop. Then:

(i) If $P$ is a subloop of $Q$ and $g(P) \subseteq P$ for every $g \in \text{Aut } Q$ then $P$ is normal.

(ii) $N(Q)$ and $C(Q)$ are normal subgroups of $Q$.

(iii) $K(Q)$ is a normal commutative subloop of $Q$.

Proof. (i) follows from 1.1 and 1.2, (ii) follows from (i) and 1.3 and (iii) follows from (i) and 1.4(ii).

A quasigroup $Q$ is called an LIP-quasigroup (RIP-quasigroup) if there is a mapping $p(q)$ of $Q$ into $Q$ such that $p(a) \cdot ab = b \cdot q(a) = b$ for all $a, b \in Q$. Further, $Q$ is called an IP-quasigroup if it is both LIP-quasigroup and RIP-quasigroup.

The following results are proved in [1], Chapter 5.

1.6. Lemma. Let $Q$ be an LIP-quasigroup. Then $p^2 = 1$, $pf = f$, $p(a) a = e(a)$, $a \cdot p(a) = e(a)$ and $a \cdot p(a) b = b$ for all $a, b \in Q$. Moreover, if $Q$ is a right loop then $a^{-1} = p(a) = a^{-1}$ for every $a \in Q$.

1.7. Lemma. Let $Q$ be an IP-quasigroup. Then $p(ab) = q(b) q(a)$ and $q(ab) = = p(b) p(a)$ for all $a, b \in Q$.

1.8. Lemma. Let $Q$ be an IP-quasigroup. Then:

(i) If $Q$ is commutative then $p = q \in \text{Aut } Q$.

(ii) If $Q$ is a loop then $p(a) = a^{-1} = q(a)$ and $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in Q$.

A quasigroup $Q$ is called medial if $A(Q) = Q$. Further, $Q$ is called monomedical (dimedial, trimedial) if each of its subquasigroups generated by one (two, three) element(s) is medial.

A quasigroup $Q$ is called a WM-quasigroup if $aa \cdot bc = ab \cdot ac$ and $bc \cdot aa = = ba \cdot ca$ for all $a, b, c \in Q$.

A quasigroup $Q$ is called unipotent if $aa = bb$ for all $a, b \in Q$.

A quasigroup $Q$ is called idempotent if $\text{Id } Q = Q$.

A quasigroup $Q$ is called distributive if $a \cdot bc = ab \cdot ac$ and $bc \cdot a = ba \cdot ca$ for all $a, b, c \in Q$.

A quasigroup $Q$ is called a Steiner quasigroup if it is commutative idempotent and $a \cdot ab = b$ for all $a, b \in Q$.

A mapping $g$ of a quasigroup $Q$ into itself is said to be (left) regular if there exists a mapping $h$ such that $g(ab) = h(a) b$ for all $a, b \in Q$.

Remark. The notation $e(a), f(a), L_a, S(a, b)$, etc., will be used only if the basic operation is written multiplicatively. We shall write $e^*(a), f^*(a), L^*_a, S(a, b, *)$, when another symbol (say $*$) is used.
2. PSEUDOAUTOMORPHISMS

All results of this section are auxiliary and their proofs are only sketched. However, almost each of the following assertions is either implicitly or explicitly contained in [1] and [2].

Let \( g \) be a permutation of a quasigroup \( Q \) and \( x \in Q \) an element. We say that \( g \) is a left pseudomorphism with a left companion \( x \) of the quasigroup \( Q \) if \( x g(ab) = x g(a) \cdot g(b) \) for all \( a, b \in Q \). Dually we define right pseudomorphisms.

2.1. Lemma. Let a quasigroup \( Q \) possess a left pseudomorphism \( g \) with a left companion \( x \). Then:

(i) \( Q \) is a left loop and \( g(j) = e(x) \).
(ii) If \( Q \) is a loop then \( g(j) = j \).
(iii) If \( Q \) is an RIP-quasigroup then \( g(a^{-1}) = g(a)^{-1} \) for every \( a \in Q \).
(iv) If \( Q \) is an IP-loop then \( g \) is a right pseudomorphism and \( x^{-1} \) is its right companion.

Proof. (i) \( x \cdot g(g^{-1} e(x) a) = x g(a) \) for every \( a \in Q \).
(ii) follows from (i).
(iii) \( x = x g(aa^{-1}) = x g(a) \cdot g(a^{-1}) \) and \( x g(a^{-1})^{-1} = x g(a) \) for every \( a \in Q \).
(iv) \( g(b^{-1}a^{-1}) x^{-1} = g(ab)^{-1} \cdot x^{-1} = (x g(a) \cdot g(b))^{-1} = g(b^{-1}) \cdot g(a^{-1}) x^{-1} \) for all \( a, b \in Q \).

2.2. Lemma. Let \( g, h \) be two left pseudomorphisms of a left loop \( Q \) and let \( x, y \) be their respective left companions. Then \( gh \) is a left pseudomorphism and \( x g(y) \) is its left companion.

Proof. \( x g(y) \cdot g(h(ab)) = x g(y h(ab)) = x g(y h(a)) \cdot g(h(b)) = (x g(y) \cdot g(h(a))) \cdot g(h(b)) \) for all \( a, b \in Q \).

2.3. Lemma. Let \( g \) with a left companion \( x \) be a left pseudomorphism of a left loop \( Q \). Then \( g^{-1} \) is a left pseudomorphism and \( g^{-1}(x^{-1}) \) is its left companion.

Proof. \( x g(g^{-1}(x^{-1}) g^{-1}(a)) = a \) and \( x g(g^{-1}(x^{-1}) g^{-1}(ab)) = ab = (x g(g^{-1}(x^{-1}) g^{-1}(a))) g g^{-1}(b) = x g(g^{-1}(x^{-1}) g^{-1}(a) \cdot g^{-1}(b)) \) for all \( a, b \in Q \).

2.4. Lemma. Let \( Q \) be a left loop, \( g \) a permutation of \( Q \) and \( x \in Q \). The following conditions are equivalent:

(i) \( g \in \text{Aut} \ Q \) and \( x \in N_1(Q) \).
(ii) \( g \) is a left pseudomorphism, \( x \) is its left companion and \( x \in N_1(Q) \).
(iii) \( g \in \text{Aut} \ Q \) and \( g \) is a left pseudomorphism with a left companion \( x \).
Proof. Easy.

2.5. Corollary. Let \( Q \) be a left loop. Then every automorphism is a left pseudoautomorphism and left pseudoautomorphisms form a group.

2.6. Lemma. Let \( g \) with a companion \( x \) be a pseudoautomorphism of a commutative loop \( Q \). Then \( g \) is an automorphism and \( x \) belongs to \( N(Q) \).

Proof. \( x g(ab) = x g(a) \cdot g(b) = x g(ba) = x g(b) \cdot g(a) \) for all \( a, b \in Q \). Hence \( x \in N(Q) \) and the rest is clear.

2.7. Lemma. Let \( Q \) be a left loop and \( ab^{-1} \in N_1(Q) \) for some \( a, b \in Q \). Then \( a = ab^{-1} \cdot b \).

Proof. \( e(ab^{-1}) = j \) since \( N_1(Q) \) is a subgroup, and hence \( ab^{-1} = ab^{-1} \cdot bb^{-1} = (ab^{-1} \cdot b) b^{-1} \).

2.8. Lemma. Let \( Q \) be a left loop and \( g \) a left pseudoautomorphism with a left companion \( x \). The following conditions are equivalent for any \( y \in Q \):

(i) \( y \) is a left companion of \( g \).
(ii) \( yx^{-1} \in N_1(Q) \).
(iii) \( y = ax \) for some \( a \in N_1(Q) \).

Proof. (i) implies (ii). By 2.2 and 2.3, \( yx^{-1} = ygg^{-1}(x^{-1}) \) is a left companion of \( gg^{-1} = 1 \).

(ii) implies (iii) by 2.7 and (iii) implies (i) trivially.

2.9. Lemma. Let \( g, h \) be two left pseudoautomorphisms of a left loop \( Q \). The following conditions are equivalent:

(i) \( g \) and \( h \) have a common left companion.
(ii) \( g \) and \( h \) have the same left companions.
(iii) \( g^{-1}h \) is an automorphism.

Proof. (i) implies (ii) by 2.8.

(ii) implies (iii). Let \( x \) be a left companion of both \( g \) and \( h \). Then \( g^{-1}(x^{-1}) g^{-1}(x) \) is a left companion of \( g^{-1}h \). But \( x = xg(g^{-1}(x^{-1}) g^{-1}(x)) \), and so \( g^{-1}(x^{-1}) \cdot g^{-1}(x) = j \).

(iii) implies (i). Let \( x \) be a left companion of \( g \). Then \( x = xg(j) = x e(x) \) is a left companion of \( gg^{-1}h = h \).

2.10. Lemma. Let \( Q \) be a left loop and \( g \) a left pseudoautomorphism with a left companion \( x \). Put \( a \ast b = R_j^{-1}(a) b \) for all \( a, b \in Q \) and suppose that \( g(j) = j \).
Then $Q(*)$ is a loop, $g$ is a left pseudoautomorphism of $Q(*)$ and $x$ is its left companion.

Proof. $x \ast g(aj \ast b) = x \ast g(ab) = (x \ast g(a))j \ast g(b)$, and hence $x \ast g(aj) = (x \ast g(a))j$ and $x \ast g(aj \ast b) = (x \ast g(aj)) \ast g(b)$ for all $a, b \in Q$.

3. MOUFANG LOOPS

Details concerning Moufang loops may be found in [1] and [2].

3.1. Lemma. Let $Q$ be a Moufang loop. Then $K(Q) = M(Q)$ is a commutative subloop of $Q$.

Proof. Let $x, y \in K(Q)$ and $a \in Q$. Then $x(a \ast xy) = (xa \ast x)y = y(xa \ast x) = y(x \ast ax) = (yx \ast a)x = x(yx \ast a) = x(xy \ast a)$. Hence $a \ast xy = xy \ast a$ and $xy \in K(Q)$. Further, $ax^{-1} = x^{-1}ax^{-1} = x^{-1}axx^{-1} = x^{-1}a$ and we have proved that $K(Q)$ is a subloop of $Q$. If $x \in K(Q)$ and $a, b \in Q$ then $ax \ast ba = (a \ast xb)a = (a \ast bx)a = ab \ast xa$ and $x$ is contained in $M(Q)$. Similarly we can show that $M(Q)$ is a subset of $K(Q)$.

3.2. Lemma. Let $Q$ be a Moufang ST-loop. Then $K(Q)$ is a normal subloop.

Proof. Clearly, $g(K(Q))$ is a subset of $K(Q)$ for every automorphism $g$ of $Q$. Further, $V(a)(x) = x$ for all $a \in Q$ and $x \in K(Q)$. The rest is clear from 1.1 and 1.2.

3.3. Lemma. Let $Q$ be a Moufang loop, $K(Q)$ a normal subloop and $a \in Q$. Then the subloop generated by $\{a\} \cup K(Q)$ is commutative.

Proof. Let $P$ be the subloop generated by $K(Q) \cup \{a\}$. Then $K(Q)$ is contained in $K(P)$ and it suffices to show that $a \in K(P)$. Let $b \in P$ and let $G$ be the subloop generated by $\{a, b\}$. Then $G$ is a group and $G/G \cap K(Q)$ is a subgroup of $P/K(Q)$. However, $P/K(Q)$ is a cyclic Moufang loop, hence a group, and therefore $G/G \cap K(Q)$ is cyclic. On the other hand, $G \cap K(Q) \subseteq C(G)$ and consequently $G/C(G)$ is cyclic. Thus $G$ is commutative and $ab = ba$.

3.4. Lemma. Let $Q$ be a Moufang loop. Then every mapping from $\mathcal{S}(Q, j)$ is a pseudoautomorphism of $Q$.

Proof. See [1], Theorem 6.4.

3.5. Lemma. Let $Q$ be a Moufang loop. Then:

(i) If $Q$ is commutative then $Q$ is an A-loop.
(ii) If $Q$ is a V-loop then $a^3 \in N(Q)$ for every $a \in Q$. 

67
Proof. (i) follows from 3.4 and 2.6, (ii) follows from 3.4, 2.4 and [1], Corollary 6.4.1.

3.6. Lemma. Let \( g \) be a pseudoautomorphism of a Moufang loop \( Q \). Then \( g(ax) = g(a)g(x), g(xa) = g(x)g(a) \) and \( g(x) \in N(Q) \) for all \( a \in Q \) and \( x \in N(Q) \).

Proof. See [1], Lemma 6.2 and its proof.

3.7. Lemma. Let \( Q \) be a Moufang loop. Then \( N(Q) \) is a normal subloop of \( Q \).

Proof. Apply 3.4, 3.6 and 1.2.

Let \( Q \) be a loop. We shall say that \( Q \) satisfies the condition \( \text{NK} \) if for every \( a \in Q \) there exist \( b \in N(Q) \) and \( c \in K(Q) \) such that \( a = bc \).

3.8. Lemma. Let \( Q \) be a loop, \( a, c \in N(Q) \) and \( b, d \in K(Q) \). Then \( ab \cdot cd = ac \cdot bd \).

Proof. \( ab \cdot cd = a(b \cdot cd) = a(cd \cdot b) = a(c \cdot db) = ac \cdot db = ac \cdot bd \).

3.9. Lemma. Let \( Q \) be a Moufang loop satisfying \( \text{NK} \). Then \( Q \) is a homomorphic image of the cartesian product \( N(Q) \times K(Q) \).

Proof. Define \( g(a, b) = ab \) for all \( a \in N(Q) \) and \( b \in K(Q) \). According to 3.8, \( g \) is a homomorphism. However, \( Q \) satisfies \( \text{NK} \), and hence \( g \) is onto \( Q \).

3.10. Lemma. Every Moufang loop satisfying \( \text{NK} \) is an \( A \)-loop.

Proof. Every group is an \( A \)-loop and every commutative Moufang loop is an \( A \)-loop. On the other hand, as is easy to see, \( A \)-loops form a quasigroup variety. In particular, \( A \)-loops are closed under homomorphic images and we can apply 3.9.

3.11. Lemma. Let \( Q \) be a Moufang loop satisfying \( \text{NK} \). Then \( N(K(Q)) \) is contained in \( C(Q) \).

Proof. There is a homomorphism \( g \) of \( N(Q) \times K(Q) \) onto \( Q \). If \( a \in N(K(Q)) \) then \( (j, a) \in C(N(Q) \times K(Q)) \), and therefore \( a = g(j, a) \in C(Q) \).

3.12. Lemma. Let \( Q \) be a Moufang loop satisfying \( \text{NK} \). Then every pseudoautomorphism of \( Q \) is an automorphism.

Proof. Let \( g \) with a companion \( x \) be a pseudoautomorphism. Then \( x = yz \) for some \( y \in N(Q), z \in K(Q) \) and \( z \) is a companion of \( g \). Let \( a, b \in K(Q) \) and \( c \in N(Q) \). Then \( g^{-1}(c) \in N(Q) \) and \( g(a) c = g(a) g^{-1}(c) = g(ag^{-1}(c)) = g(g^{-1}(c) a) = c g(a) \) by 3.6. Further, \( g(a) \cdot cb = g(a) c \cdot b = c g(a) \cdot b = c \cdot b g(a) = cb \cdot g(a) \). However, \( Q \) satisfies \( \text{NK} \) and it is evident that \( g(a) \in K(Q) \). Similarly \( g^{-1}(a) \in K(Q) \) and \( g \) with a companion \( z \) is a pseudoautomorphism of \( K(Q) \). By 2.6 and 3.11, \( z \in C(Q) \), and hence \( g \) is an automorphism of \( Q \).
3.13. Lemma. Let \( Q \) be a Moufang loop satisfying NK. Then:

(i) \( K(Q) \) is a normal subloop of \( Q \) and \( Q/K(Q) \) is a group.

(ii) If \( a \in Q \) then the subloop generated by \( \{a\} \cup K(Q) \) is commutative.

Proof. (i) \( K(Q) \) is normal by 3.10,3.2 and \( Q/K(Q) \) is a group since \( Q \) is generated by \( K(Q) \cup N(Q) \).

(ii) Use (i) and 3.3.

A Moufang loop \( Q \) is called primitive if \( Q \) is commutative and \( a^3 = e \) for every \( a \in Q \).

3.14. Lemma. Let \( Q \) be a Moufang loop satisfying NK. Then:

(i) \( N(Q) \) is a normal subloop and \( Q/N(Q) \) is a primitive Moufang loop.

(ii) If \( a, b \in Q \) then the subloop generated by \( \{a, b\} \cup N(Q) \) is a group.

Proof. (i) \( N(Q) \) is normal by 3.7, \( Q/N(Q) \) is commutative since \( Q \) is generated by \( N(Q) \cup K(Q) \), and \( Q/N(Q) \) is primitive by 3.5(ii).

(ii) With respect to 3.9, we can assume that \( Q \) is either a group or a commutative loop. The first case is obvious. If \( Q \) is commutative then \( N(Q) = C(Q) \) and the assertion follows from the fact that \( Q \) is diassociative.

3.15. Lemma. Let \( Q \) be a Moufang loop satisfying NK. Suppose that \( Q \) is isotopic to a commutative quasigroup. Then \( Q \) is commutative.

Proof. There are two permutations \( g, h \) of \( \beta \) such that \( g(a)h(b) = h(b)g(a) \) for all \( a, b \in Q \). Then \( xa . b = xb . a \) for all \( a, b \in Q \), where \( x = h^{-1}(j) \). However, \( x = yz \), \( y \in N(Q) \), \( z \in K(Q) \) and \( y(az . b) = y(za . b) = (y . za) b = (yz . a) b = (yz . b) a = y(zb . a) = y(a . zb) \) for all \( a, b \in K(Q) \). Hence \( z \in N(K(Q)) \) and \( z \in C(Q) \) by 3.11. It is easy to see that \( x \in N(Q) \). Consequently \( x . ab = xa . b = xb . a = x . ba \) for all \( a, b \in Q \).

3.16. Lemma. Let \( Q \) be a loop and \( g \) a mapping of \( Q \) into \( Q \). The following conditions are equivalent:

(i) \( ab . c g(a) = (a . bc) g(a) \) for all \( a, b, c \in Q \).

(ii) \( Q \) is a Moufang loop and \( a^{-1} . g(a) \in N(Q) \) for every \( a \in Q \).

Proof. See [11], Theorem 1.

3.17. Lemma. Let \( Q \) be a Moufang loop and \( g \) a mapping of \( Q \) into \( Q \). The following conditions are equivalent:

(i) \( a g(a) . b c = ab . g(a) c \) for all \( a, b, c \in Q \).

(ii) \( g(a) \in K(Q) \) and \( a^{-1} . g(a) \in N(Q) \) for every \( a \in Q \).
Proof. (i) implies (ii). \( a \cdot g(a) \ b = a \cdot g(a) \ b = a \cdot g(a) \ b \), and hence \( a \cdot g(a) = a \cdot b \ g(a) \) by Moufang’s theorem. Then \( a \cdot b \ g(a) = ab \cdot g(a) = ab \cdot g(a) \ b = a \cdot g(a) \ b \) yields \( g(a) \in K(Q) \). Now \( ab \cdot c \ g(a) = ab \cdot g(a) \ c = a \ g(a) \ . b = (a \ . b) (g(a) \ j) = (a \ . b) g(a) \) and we can apply 3.16.

(ii) implies (i.) \( (ab \cdot c \ g(a)) \ (g(a)\ ^{-1} \ . a) = ab \cdot c a = (a \ . b) g(a) \) \( \ . (g(a)\ ^{-1} \ . a) \), and therefore \( ab \cdot c \ g(a) = (a \ . b) g(a) \) \( \ . g(a)\ ^{-1} \ . a \) \( \). In particular, \( a \ g(a) \ . c \ g(a) = (a \ . g(a) \ . c) g(a) = (a \ . c \ g(a)) g(a) \) for all \( a, c \in Q \). Thus \( a \ g(a) \ . b = ab \ . g(a) \) and \( a \ g(a) \ . b = (a \ . b) g(a) = ab \ . c \ g(a) = ab \ . g(a) \ c \) for all \( a, b, c \in Q \).

3.18. Lemma. Let \( Q \) be a Moufang loop such that \( a \ g(a) \ . b = ab \ . g(a) \ c \) for all \( a, b, c \in Q \) and a mapping \( g \). Then \( Q \) satisfies NK.

Proof. We have \( a = g(a)^{-1} \ a \ . g(a) \) and \( g(a) \in K(Q) \), \( g(a)^{-1} \ a \in N(Q) \) by 3.17.

3.19. Lemma. Let \( Q \) be a Moufang loop and let \( g \in \text{Aut} \ Q \) be such that \( g^{-1}(a^{-1}) \ . a \in K(Q) \) for every \( a \in Q \). Then \( a^{-1} \ . g(a) \in K(Q) \).

Proof. It is enough to take into account that \( K(Q) \) is a subloop and \( g(a^{-1}) = g(a)^{-1} \).

3.20. Lemma. Let \( g \) be an automorphism of a Moufang loop \( Q \). The following conditions are equivalent:

(i) \( a^{-2} \ . g^{-1}(a) \in N(Q) \) for every \( a \in Q \).
(ii) \( a^{-1} \ . g(a^2) \in N(Q) \) for every \( a \in Q \).
(iii) \( g^{-1}(a) \ . a^{-2} \in N(Q) \) for every \( a \in Q \).
(iv) \( g(a^2) \ . a^{-1} \in N(Q) \) for every \( a \in Q \).

Proof. Similar to that of 3.19.

Let \( Q \) be a Moufang loop and \( g, h \) two automorphisms of \( Q \). We shall say that \( g, h \) satisfy the condition (F) if \( gh = hg, a^{-1} \ . g(a), a^{-1} \ . h(a) \in K(Q) \) and \( a^{-1} \ . g(a^2), a^{-1} \ . h(a^2) \in N(Q) \) for every \( a \in Q \).

3.21. Lemma. Let \( Q \) be a Moufang loop and let \( g, h \in \text{Aut} \ Q \) satisfy (F). Then:

(i) \( a \ . bc = (g(a) \ b) \ (g(a)^{-1} \ a \ . c) \) for all \( a, b, c \in Q \).
(ii) \( bc \ . a = (b \ . a \ h(a^{-1})) \ (c \ h(a)) \) for all \( a, b, c \in Q \).
(iii) \( K(Q) = \{ a \in Q \mid g^2(b) \ a \ . c \ h^2(b) = g^2(b) \ c \ . a \ h^2(b) \) for all \( b, c \in Q \} \).
(iv) \( Q \) satisfies NK.

Proof. (i) Put \( k(a) = a^{-1} \ . g^{-1}(a) \) for every \( a \in Q \). It is easy to see that \( k(a) \in K(Q) \) and \( a^{-1} \ . k(a) \in N(Q) \) for every \( a \in Q \). According to 3.17, \( a k(a) \ . bc = ab \ . k(a) \ c \) for all \( a, b, c \in Q \). The rest is clear.
(ii) is similar to (i).

(iii) Since \( a^{-1} \cdot h(a^2) \), \( a^{-2} \cdot g^{-1}(a) \in N(Q) \) for every \( a \in Q \), \( h(a^{-2}) \cdot h g^{-1}(a) \) and \( a^{-1} \cdot h g^{-1}(a) \) belong to \( N(Q) \). Hence \( h g^{-1}(a^{-1}) \cdot h^2 g^{-2}(a) \) and \( a^{-1} \cdot h^2 g^{-2}(a) \) are contained in \( N(Q) \). By 3.16, \( ax \cdot bh^2 g^{-2}(a) = (a \cdot xb) h^2 g^{-2}(a) = (a \cdot bx) h^2 g^{-2}(a) = ab \cdot x h^2 g^{-2}(a) \) for all \( x \in K(Q) \) and \( a, b \in Q \). Conversely, if \( g^2(a) b \cdot x h^2(a) = g^2(a) x \cdot b h^2(a) \) for all \( a, b \in Q \) then the substitution \( a = j \) yields \( x \in K(Q) \).

(iv) \( a = a^{-1} g(a^2) \cdot g(a^{-2}) a^2 \) for every \( a \in Q \).

3.22. Lemma. Let \( Q \) be a Moufang loop and let \( g \in \text{Aut} Q \) be such that \( a^{-2} \cdot g(a) \in N(Q) \) for every \( a \in Q \). Then a \( g(a) \in N(Q) \), provided \( Q \) is a V-loop.

**Proof.** Apply 3.5(ii).

4. BASIC PROPERTIES OF F-QUASIGROUPS

A quasigroup \( Q \) is called an LF-quasigroup (RF-quasigroup) if \( a \cdot bc = ab \cdot e(a) c \) (\( cb \cdot a = c f(a) \cdot ba \)) for all \( a, b, c \in Q \). If \( Q \) is both an LF and an RF-quasigroup then we shall say that \( Q \) is an F-quasigroup.

4.1. Lemma. The following conditions are equivalent for a quasigroup \( Q \):

(i) \( Q \) is an LF-quasigroup.

(ii) \( L_a(b) \cdot L_{e(a)}(c) = L_a(bc) \) for all \( a, b, c \in Q \).

(iii) \( L_a^{-1}(b) \cdot L_{e(a)}^{-1}(c) = L_a^{-1}(bc) \) for all \( a, b, c \in Q \).

(iv) \( S(a, b) = L_{e(a)}^{-1} \) for all \( a, b \in Q \).

(v) \( S(a, b) = S(a, c) \) for all \( a, b, c \in Q \).

**Proof.** The equivalence of (i), (ii), (iii) and the implication (iv) implies (v) are obvious.

(i) implies (iv). We have \( L_{ab}(c) = ab \cdot c = ab \cdot L_{e(a)} L_{e(a)}^{-1}(c) = a \cdot b L_{e(a)}^{-1}(c) = a L_b L_{e(a)}^{-1}(c) \). Hence \( S(a, b) = L_{e(a)}^{-1} \).

(v) implies (iv). \( S(a, b) = S(a, e(a)) = L_{e(a)}^{-1} L_a^{-1} L_{e(a)} = L_{e(a)}^{-1} \).

(iv) implies (i). \( a \cdot bc = L_a L_b(c) = L_a S(a, b) L_b^{-1}(c) = L_a S(a, e(a)) L_b e(a) = ab \cdot e(a) c \) for all \( a, b, c \in Q \).

4.2. Lemma. Let \( Q \) be an LF-quasigroup. Then \( ef = fe \) and \( e \) is an endomorphism of \( Q \).

**Proof.** \( a \cdot e f(a) e(a) = f(a) a \cdot e f(a) e(a) = f(a) \cdot a e(a) = a = a e(a) \) for every \( a \in Q \). Further, \( ab \cdot e(a) e(b) = a \cdot b e(b) = ab \) for all \( a, b \in Q \).
4.3. Lemma. Let $Q$ be an LF-quasigroup and $a, b \in Q$. Then $L_aR_a = R_aL_a$ iff $e(b) = f(a)$.

Proof. If $L_a$ and $R_a$ commute then $ba = R_aL_b e(b) = L_aR_a e(b)$ and $a = e(b) a$. Conversely, if $e(b) = f(a)$ then $b . ca = bc . e(b) a = bc . a$ for every $c \in Q$.

4.4. Lemma. Let $Q$ be an LF-quasigroup and $a \in Q$. Then $L_{f(a)}R_{e(a)} = R_{e(a)}L_{f(a)}$ and $eL_a = L_{e(a)}e$.

Proof. The former equality follows from 4.3 and 4.2, the latter from the fact that $e$ is an endomorphism of $Q$.

4.5. Lemma. Let $Q$ be an LF-quasigroup and $j \in \text{Id} \; Q$. Then $L_j$ is an automorphism, $L_jR_j = R_jL_j$, $L_je = eL_j$ and $L_jf = fL_j$.

Proof. Use 4.1(ii), 4.3, 4.4 and the fact that $ja = jf(a) \cdot ja$.

4.6. Proposition. A quasigroup is a group iff it is an LF-quasigroup (or an RF-quasigroup) and a loop.

Proof. Easy.

4.7. Proposition. Let $Q$ be an LF-quasigroup, $j \in \text{Id} \; Q$, $K = \{a \in Q \mid e(a) = j\}$, $H = \{a \in Q \mid f(a) = j\}$ and $G = H \cap K$. Then $K$ is a normal subquasigroup and a right loop, $H$ is a subquasigroup and a left loop and $G$ is a subgroup of $Q$. Moreover, if $Q$ is an F-quasigroup then $G$ is a normal subgroup.

Proof. By 4.2, $e$ is an endomorphism of $Q$ and $K$ is one of classes of the corresponding normal congruence. However, $j$ is an idempotent and consequently $K$ is a normal subquasigroup. Further, $L_j$ is an automorphism and $H = \{a \mid L_j(a) = a\}$. Hence $H$ is a subquasigroup. Now it is evident that $G$ is a subgroup, and therefore a subgroup by 4.6. If $Q$ is an F-quasigroup then $H$ is normal, and so $G$ is normal as well.

4.8. Lemma. Let $Q$ be an LF-quasigroup, $x \in Q$, $j = e(x)$ and $a * b = a \cdot L_j^{-1}(b)$ for all $a, b \in Q$. Then $Q(*)$ is a left loop, $j$ is its left unit and $Q(*)$ is an LF-quasigroup.

Proof. Clearly, $j * a = j \cdot L_j^{-1}(a) = a$ for every $a \in Q$. Further, $a * j e(a) = a$, $j e(a) = e^*(a)$ and $a * (b * c) = a \cdot L_j^{-1}(b L_j^{-1}(c)) = a L_j^{-1}(b) \cdot L_j^{-1}(c) = (a L_j^{-1}(b)) (e(a) \cdot L_j^{-1}(c)) = a L_j^{-1}(b) \cdot L_j^{-1}(j e(a) \cdot L_j^{-1}(c)) = (a * b) * (e^*(a) * * c)$ for all $a, b, c \in Q$. 

72
5. PSEUDOAUTOMORPHISMS OF F-QUASIGROUPS

In the following four lemmas we shall assume that \( Q \) is an LF-quasigroup with a left unit \( j \). These lemmas are implicitly contained in [1].

5.1. Lemma. Let \( a \in Q \). Then \( L_{e(a)} \) is a left pseudoautomorphism of \( Q \) and \( aj \) is its left companion.

Proof. \( aj(e(a), bc) = a(j . bc) = a . bc = ab . e(a) c = (aj . e(a) b) . e(a) c \) for all \( b, c \in Q \).

5.2. Lemma. Let \( a, b \in Q \). The left pseudoautomorphisms \( L_{e(a)}L_{e(b)} \) and \( L_{e(R_j^{-1}(a.bj))} \) have the same left companions.

Proof. By 5.1 and 2.2, \( (aj)(e(a), bj) = a . bj \) is a left companion of \( L_{e(a)}L_{e(b)} \). On the other hand, \( R_j(R_j^{-1}(a . bj)) = a . bj \) is a left companion of the other pseudoautomorphism.

5.3. Lemma. Let \( a, b \in Q \). Then \( L_{e(b)}^{-1}L_{e(a)}^{-1}L_{e(R_j^{-1}(a.bj))} \) is an automorphism of \( Q \).

Proof. Apply 5.2 and 2.9.

5.4. Lemma. Let \( a \circ b = R_j^{-1}(a) \circ b \) for all \( a, b \in Q \). Then \( Q(\circ) \) is an S-loop.

Proof. We can write \( R_j(R_j(a) \circ b) \circ c = ab . c = a . b L_{e(a)}^{-1}(c) = R_j(a) \circ (R_j(b) \circ L_{e(a)}^{-1}(c)) \) for all \( a, b, c \in Q \). Hence \( R_j(a \circ b) \circ c = a \circ (R_j(b) \circ L_{e(a)}^{-1}(c)) \), where \( g(a) = eR_j^{-1}(a) \). In particular, \( R_j(a) \circ c = a \circ L_{g(a)}^{-1}(c) \) for all \( a, c \in Q \), and hence \( R_j(a \circ b) \circ c = (a \circ b) \circ L_{g(a)g(b)}^{-1}(c) \) and \( R_j(b) \circ L_{g(a)}^{-1}(c) = b \circ L_{g(b)g(a)}^{-1}(c) \) for all \( a, b, c \in Q \). This implies the equalities \( a \circ (R_j(b) \circ L_{g(a)}^{-1}(c)) = (a \circ b) \circ L_{g(a)g(b)}^{-1}(c) \) and \( (a \circ b) \circ c = a \circ (b \circ L_{g(b)g(a)}^{-1}(c)) \) for all \( a, b, c \in Q \). It is evident that \( S(a, b, c) = = L_{g(b)g(a)}^{-1}(c)g(a)g(b) \) for all \( a, b \in Q \). Let \( a, b \in Q \), \( c = R_j^{-1}(a) \), \( d = R_j^{-1}(b) \) and \( h = = S(a, b, c) \). Then \( h = L_{g(c)}^{-1}L_{g(d)}^{-1}L_{g(R_j^{-1}(c.d))} \) is an automorphism of \( Q \) by 5.3. Hence \( h(j) = j = hR_j = R_jh \) and \( hR_j^{-1} = R_j^{-1}h \). Finally, \( h(x \circ y) = h_j^{-1}(x) . h(y) = = R_j^{-1}h(x) . h(y) = h(x) \circ h(y) \) for all \( x, y \in Q \).

5.5. Proposition. Let \( Q \) be an F-quasigroup, \( x \in Q \) and \( y = ef(x) \). Put \( a \circ b = = R_y^{-1}(a) . L_y^{-1}(b) \) for all \( a, b \in Q \). Then \( Q(\circ) \) is an ST-loop, provided \( y \in Id Q \).

Proof. Let \( a \ast b = a . L_y^{-1}(b) \) for all \( a, b \in Q \). Then \( Q(\ast) \) is an LF-quasigroup and a left loop with left unit \( y \) (see 4.8). Further, \( a \circ b = R_y^{-1}(a) \ast b = (R_y)^{-1}(a) \ast b \) for all \( a, b \in Q \). By 5.4, \( Q(\circ) \) is an S-loop. On the other hand, \( y = f e(x) \) and we can use the right hand forms of 4.8 and 5.4 to prove that \( Q(\circ) \) is a T-loop.

5.6. Corollary. Every F-quasigroup with non-empty \( Id Q \) is isotopic to \( na \) ST-loop.
6.1. Proposition. Let $Q$ be a WM-quasigroup. Then $D(Q) = Q$.

Proof. See [9], Corollary 2.

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

(i) $Q$ is a WM-quasigroup and an LF-quasigroup.

(ii) $Q$ is a WM-quasigroup and an RF-quasigroup.

(iii) $Q$ is an $F$-quasigroup and there exists $x \in Q$ such that $f(x) a \cdot b e^2(x) = f(x) b \cdot a e^2(x)$ for all $a, b \in Q$.

(iv) $Q$ is an $F$-quasigroup and there exists $x \in Q$ such that $f^2(x) a \cdot b e(x) = f^2(x) b \cdot a e(x)$ for all $a, b \in Q$.

(v) $Q$ is a trimedial quasigroup.

(vi) There are a commutative Moufang loop $Q(s)$, $g, h \in \text{Aut } Q(s)$ and $x \in N(Q(s))$ such that $gh = hg$, $a \circ g(a)$, $a \circ h(a) \in N(Q(s))$ and $ab = g(a) \circ h(b) \circ x$ for all $a, b \in Q$.

Proof. Apply 6.1 and [7], Theorem 2.

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

(i) $Q$ is an idempotent WM-quasigroup.

(ii) $Q$ is a distributive quasigroup.

(iii) $Q$ is an idempotent $F$-quasigroup.

Proof. Obvious.

6.4. Proposition. Every distributive quasigroup is trimedial.

Proof. See [1], Corollary 8.6.1.

6.5. Proposition. Every commutative $F$-quasigroup is trimedial.

Proof. See [7], Corollary 6.

6.6. Proposition. Let $Q$ be a trimedial quasigroup. Then there is a normal congruence $r$ of $Q$ such that every class of $r$ is a medial subquasigroup of $Q$ and $Q/r$ is a distributive Steiner quasigroup.

Proof. See [7], Theorem 3.

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

(i) $Q$ is an $F$-quasigroup and $A(Q)$ is non-empty.
(ii) $Q$ is an F-quasigroup and $Q$ is isotopic to a group.

(iii) There are a group $Q(o)$, $g, h \in \text{Aut } Q(o)$ and $x \in C(Q(o))$ such that $gh = hg$, $a^{-1} \circ g(a), a^{-1} \circ h(a) \in C(Q(o))$ and $ab = g(a) \circ h(b) \circ x$ for all $a, b \in Q$.

Proof. See [6], Theorem 3.2.

6.8. Proposition. Let $Q$ be an F-quasigroup isotopic to a group. Then $A(Q)$ is a normal subquasigroup of $Q$ and $Q/A(Q)$ is a group.

Proof See [6], Theorem 3.4.

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

(i) $Q$ is an LF-quasigroup and a right loop.
(ii) There is an element $j \in Q$ such that $a . bc = ab . jc$ for all $a, b, c \in Q$.
(iii) $Q$ is a right loop and $A(Q)$ is non-empty.
(iv) There are a group $Q(o)$ and $h \in \text{Aut } Q(o)$ such that $ab = a \circ h(b)$ for all $a, b \in Q$.

Proof. The implications (i) implies (ii) and (iv) implies (i) are easy.

(ii) implies (iii). We have $a = a . j e^2(a), e(a) = j \cdot e^2(a)$ and $j = e(a)$ for every $a \in Q$. Hence $j$ is a right unit and $aj = a \cdot bc = ab \cdot jc$ for all $a, b, c \in Q$.

(iii) implies (iv). By Theorem 1.1 from [6] there are a group $Q(o)$ and $g, h \in \text{Aut } Q(o)$ such that $ab = g(a) \circ h(b)$ for all $a, b \in Q$ and $j$ is the unit of $Q(o)$. Now $a = aj = g(a) \circ h(j) = g(a)$ and $g = 1$.

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

(i) $Q$ is an F-quasigroup and a right loop.
(ii) There are a group $Q(o)$ and $h \in \text{Aut } Q(o)$ such that $a^{-1} \circ h(a) \in C(Q(o))$ and $ab = a \circ h(b)$ for all $a, b \in Q$.

Proof. Apply 6.7 and 6.9.

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

(i) $Q$ is an F-quasigroup and $B_i(Q)$ is non-empty.
(ii) $Q$ is an F-quasigroup and $B_i(Q)$ is non-empty.
(iii) $Q$ is a medial quasigroup.
(iv) $Q$ is an F-quasigroup and $Q$ is isotopic to an abelian group.
(v) There are an abelian group $Q(+), g, h \in \text{Aut } Q(+)$ and $x \in Q$ such that $gh = hg$ and $ab = g(a) + h(b) + x$ for all $a, b \in Q$.

Proof. Apply 6.7, [1], Theorem 2.10 and [6], Theorem 3.6.
6.12. Proposition. The following conditions are equivalent for a quasigroup Q:

(i) Q is an ST-quasigroup and an LF-quasigroup.
(ii) Q is an ST-quasigroup and an RF-quasigroup.
(iii) Q is an F-quasigroup and e(Q), f(Q) Í Id Q.
(iv) Id Q is a normal distributive subquasigroup of Q, Q/Id Q is a group and Q is isomorphic to the cartesian product Id Q × Q/Id Q.

Proof. See [5], Theorem 12.

6.13. Proposition. Let Q be an IP-quasigroup and an LF-quasigroup. Then Q is isotopic to a Moufang loop.

Proof. See [3], Theorem 1.

6.14. Lemma. Let an F-quasigroup Q be isotopic to a Moufang loop. Then every loop isotopic to Q is a Moufang loop.

Proof. It is well known that Moufang loops are closed under loop isotopies.

7. SEVERAL LEMMAS ON F-QUASIGROUPS

Throughout this section, let Q be an F-quasigroup and let x, y Í Q be such that R_xL_y = L_yR_x. Further put g = R_x, h = L_y, j = yx, u = e(y) x, v = yf(x), k = gR_f(x) g^{-1}, t = hL_e(y) h^{-1}, z = g(j) = yx . x, w = h(j) = y . yx, m = geh^{-1}, n = hgh^{-1} and a Ï b = g^{-1}(a) . h^{-1}(b) for all a, b Í Q. As is easy to see, Q is a loop and f is its unit.

7.1. Lemma. g(a Ï b) = k(a) Ï g(b) and h(a Ï b) = h(a) Ï t(b) for all a, b Í Q.

Proof. g(g(a) Ï h(b)) Ï h(c) = ab . c = a f(c) . bc = g(g(a) Ï h(f(c))) Ï h(g(b) Ï h(c)) for all a, b, c Í Q. Hence g(a Ï b Ï c = g(a Ï hgh^{-1}(c)) Ï h(g^{-1}(b) Ï c) for all a, b, c Í Q. If c = j then g(a Ï b) = g(a Ï hgh^{-1}(j)) Ï g(b). However, hgh^{-1}(j) = hfx = v and g(a Ï v) = g(g^{-1}(a) . h^{-1}(v)) = gR_{f(x)} g^{-1}(a) = k(a). The latter identity can be proved in a similar way.

7.2. Lemma. a Ï (b Ï c) = (k(a) Ï b) Ï (m(a) Ï c). (a Ï mk^{-1}(a)) Ï (b Ï c) = (a Ï b) Ï (mk^{-1}(a) Ï c), (b Ï c) Ï a = (b Ï n(a)) Ï (c Ï t(a)) and (b Ï c) Ï (nt^{-1}(a) Ï a) = = (b Ï nt^{-1}(a)) Ï (c Ï a) for all a, b, c Í Q.

Proof. We have g(g(a) Ï h g(b) Ï t h(c)) = a . bc = ab . e(a) c = (k g(a) Ï g(h(b))) Ï (hg e(a) Ï t h(c)) for all a, b, c Í Q. Hence a Ï (b Ï c) = (k(a) Ï b) Ï (m(a) Ï c) for all a, b, c Í Q. In particular, a = k(a) Ï m(a) and the rest is clear.

76
7.3. Lemma. $g(a) = k(a) \circ z$ for every $a \in Q$ and $k$ is a right pseudoautomorphism with a right companion $z$ of the loop $Q(\circ)$.

Proof. The equality $g(a) = k(a) \circ z$ is an immediate consequence of 7.1. Further, $k(a \circ b) \circ z = g(a \circ b) = k(a) \circ g(b) = k(a) \circ (k(b) \circ z)$ for all $a, b \in Q$.

7.4. Lemma. $h(a) = w \circ t(a)$ for every $a \in Q$ and $t$ is a left pseudoautomorphism with a left companion $w$ of the loop $Q(\circ)$.

Proof. Similar to that of 7.3.

In the remaining part of this section we shall assume that $Q(\circ)$ is a Moufang loop.

7.5. Lemma. $m k^{-1}(a), n t^{-1}(a) \in K(Q(\circ)), a^{-1} \circ m k^{-1}(a), n t^{-1}(a) \circ a^{-1}$ belong to $N(Q(\circ))$ for every $a \in Q$. Moreover, $Q(\circ)$ satisfies NK.

Proof. Apply 7.2, 3.17 (and its right hand form) and 3.18.

7.6. Lemma. $a^{-1} \circ k(a), a^{-1} \circ t(a), gh e(a), gh f(a) \in K(Q(\circ))$ for every $a \in Q$.

Proof. $m k^{-1}(a) = gheR_{f(\circ)}^{-1}(a) \in K(Q(\circ))$ for every $a \in Q$. However, $k^{-1}$ and $R_{f(\circ)} k^{-1}$ are permutations. Hence $m(a)$ and $gh e(a)$ belong to $K(Q(\circ))$. Further, $a = k(a) \circ m(a)$ (see 7.2), and hence $k(a^{-1}) \circ a \in K(Q(\circ))$. Now we can use 7.5, 3.12, 7.3 and 3.19.

7.7. Lemma. $k, t \in \text{Aut } Q(\circ)$ and $z, w \in N(Q(\circ))$.

Proof. Apply 7.3, 7.4, 7.5 and 3.12, 2.4.

7.8. Lemma. $a^{-1} \circ k(a^2), a^{-1} \circ t(a^2) \in N(Q(\circ))$ for every $a \in Q$.

Proof. $a^{-1} \circ m k^{-1}(a) = a^{-2} \circ k^{-1}(a)$ and $n t^{-1}(a) \circ a^{-1} = t^{-1}(a) \circ a^{-2}$ belong to $N(Q(\circ))$ and we can use 3.20.

7.9. Lemma. Let $z \in K(Q(\circ))$. Then $z \in C(Q(\circ))$ and $k t = t k$.

Proof. We can write $k(w) \circ k(t(a) \circ z = g h(a) = h g(a) = w \circ t k(a) \circ t(z)$. Consequently $k(w) \circ z = w \circ t(z)$. Moreover, $z \in N(Q(\circ)) \cap K(Q(\circ)) = C(Q(\circ))$, and therefore $k(w) \circ z \circ k(t(a) = w \circ t(z) \circ t k(a)$. Thus $k t(a) = t k(a)$.

7.10. Lemma. Let $x = e(p)$ and $y = e(q)$ for some $p, q \in Q$. Then $e(Q) \subseteq K(Q(\circ))$ and $z \in C(Q(\circ))$.

Proof. $gh e(a) = e(q \cdot a) e(p) = e(qa \cdot p) \in K(Q(\circ))$ for every $a \in Q$. However, $R_p L_q$ is a permutation. Finally, $z = g(j) = yx \cdot x = e(qp \cdot p)$ and we can use 7.9.
7.11. Lemma. Let \( x = f(p) \) and \( y = f(q) \) for some \( p, q \in Q \). Then \( f(Q) \subseteq K(Q(\circ)) \) and \( w \in C(Q(\circ)) \).

Proof. Similar to that of 7.10.

7.12. Lemma. Let \( z \in K(Q(\circ)) \) (or \( w \in K(Q(\circ)) \)). Then \( k, t \) satisfy \( (F) \).

Proof. Apply 7.6, 7.7 and 7.9, 7.8.

7.13. Lemma. Let \( x = e f(p) \) and \( y = e f(q) \) for some \( p, q \in Q \). Then \( z, w, z \circ w \in C(Q(\circ)) \) and \( k, t \) satisfy \( (F) \). Moreover, \( ab = k(a) \circ t(b) \circ z \circ w \) for all \( a, b \in Q \).

Proof. Apply 7.12, 7.10 and 7.11.

8. QUASIGROUPS LINEAR OVER MOUFANG LOOPS

In this section, let \( Q(\circ) \) be a Moufang loop, let \( k, t \in \text{Aut} \ Q(\circ) \) satisfy \( (F) \) and \( q \in C(Q(\circ)) \). By 3.21, the loop \( Q(\circ) \) satisfies the condition NK. We put \( ab = k(a) \circ t(b) \circ q \) for all \( a, b \in Q \). As is easy to see, \( Q \) is a quasigroup.

8.1. Lemma. \( Q \) is an \( F \)-quasigroup.

Proof. We can write \( a \cdot bc = (k(a) \circ (kt(b) \circ t^2(c)) \circ q \circ t(q) = ((k^2(a) \circ k t(b)) \circ ((k^2(a^{-1}) \circ k(a)) \circ t^2(c)) \circ q \circ t(q) \) for all \( a, b, c \in Q \) (use 3.21). Hence \( a \cdot bc = k(k(a) \circ t(b) \circ q) \circ t(k t^{-1}(k(a^{-1}) \circ a \circ q^{-1}) \circ t(c) \circ q) \circ q = ab \cdot e \) since \( k(a) \circ t(k t^{-1}(k(a^{-1}) \circ a \circ q^{-1}) \circ q = a \). Similarly we can show that \( Q \) is an RF-quasigroup.

8.2. Lemma. If \( Q(\circ) \) is commutative then \( Q \) is trimedial.

Proof. By 3.22, \( a \circ k(a), a \circ t(a) \in N(Q(\circ)) \) for every \( a \in Q \) and we can use 6.2.

8.3. Lemma. Let \( P(\circ) \subseteq Q(\circ) \) be a subloop such that \( K(Q(\circ)) \subseteq P(\circ) \). Then \( P \) is a subquasigroup of \( Q \). Furthermore, if \( P(\circ) \) is a normal subloop then \( P \) is a normal subquasigroup and the corresponding normal congruences coincide.

Proof. Since \( a^{-1} \circ k(a), a^{-1} \circ k^{-1}(a), a^{-1} \circ t(a), a^{-1} \circ t^{-1}(a) \) belong to \( K(Q(\circ)) \subseteq P \) for every \( a \in Q \), we see that \( k(P) = P = t(P) \). Further, \( q \in P \) and it is evident that \( P \) is a subquasigroup of \( Q \). Let \( r \) be a normal congruence of \( Q(\circ) \) such that \( P(\circ) \) is one of its classes. If \( arb \) then \( a \circ b^{-1} \in P \), \( k(a \circ b^{-1}) = k(a) \circ k(b^{-1}) \in P \) and \( k(a) \circ r(k(b)) \). Hence \( ac = k(a) \circ t(c) \circ q \) and \( bc \) are in \( r \). The rest is similar.

8.4. Lemma. \( M(Q) = K(Q(\circ)) = M(Q(\circ)) \).

Proof. Let \( x \in M(Q) \). Then \( (k^2(a) \circ k t(x) \circ q) \circ (k t(b) \circ t^2(a) \circ q) \circ q = ax \) . \( ba = ab \cdot xa = (k^2(a) \circ k t(b) \circ q) \circ (k t(x) \circ t^2(a) \circ q) \circ q \) for all \( a, b \in Q \). Hence
\( (k^2(a) \circ k \, t(x)) \circ (b \circ t^2(a)) = (k^2(a) \circ b) \circ (k \, t(x) \circ t^2(a)) \) for all \( a, b \in Q \) and \( k \, t(x) \in K(Q(\varnothing)) \) by 3.21(iii). But \( K(Q(\varnothing)) \) is invariant under automorphisms, and therefore \( x \in K(Q(\varnothing)) \). If \( x \in K(Q(\varnothing)) \) then \( x \in M(Q) \), as one can show proceeding conversely. Finally \( M(Q(\varnothing)) = K(Q(\varnothing)) \) by 3.1.

8.5. Lemma. \( e(Q), f(Q) \subseteq M(Q) \).

Proof. We have \( e(a) = t^{-1}(k(a^{-1}) \circ a \circ q^{-1}) \) and \( k(a^{-1}) \circ a \in K(Q(\varnothing)) \) for every \( a \in Q \). Hence \( e(a) \in K(Q(\varnothing)) = M(Q) \). The rest is similar.

8.6. Lemma. \( M(Q) \) is a normal subquasigroup of \( Q \) and \( Q/M(Q) \) is a group.

Proof. \( M(Q) \) is a normal subquasigroup by 8.3, 8.4, 3.13, and \( Q/M(Q) \) is a group by 8.5 and 4.6.

8.7. Lemma. Let \( a \in Q \). Then the subquasigroup generated by \( \{a\} \cup M(Q) \) is trimedial.

Proof. Apply 8.3, 3.13(ii), 8.4 and 8.2.

8.8. Lemma. Let \( P(\varnothing) \subseteq Q(\varnothing) \) be a subloop such that \( N(Q(\varnothing)) \subseteq P \). Then \( P \) is a subquasigroup of \( Q \). Furthermore, if \( P(\varnothing) \) is a normal subloop then \( P \) is a normal subquasigroup and the corresponding normal congruences coincide.

Proof. Similar to that of 8.3 (use 3.22 and the fact that \( q \) is contained in \( N(Q(\varnothing)) \)). In the sequel, let \( H \) denote the nucleus \( N(Q(\varnothing)) \).

8.9. Lemma. \( H \) is a normal subquasigroup of \( Q \) and \( Q/H \) is a distributive Steiner quasigroup.

Proof. \( H \) is normal by 8.8 and 3.7. Let \( r \) be the corresponding normal congruence \( (r \) is a congruence of both \( Q(\varnothing) \) and \( Q \)). If \( a, b \in Q \) then \( c = a \cdot ab = k(a) \circ (k \, t(a) \circ t^2(b)) \circ q \circ t(q) \). Since \( q \circ t(q) \in C(Q(\varnothing)) \subseteq H \), we have \( c \, r \, k(a) \circ (k \, t(a) \circ t^2(b)) \). Further, \( a^{-1} \circ k(a^{-1}) \in H \) by 3.22, and consequently \( c \, r \, a^{-1} \circ (k \, t(a) \circ t^2(b)) \). Finally, \( k \, t(a^{-1}) \circ k(a^{-1}), k(a) \circ a, t(b^{-1}) \circ t^2(b^{-1}), b \circ t(b) \) are contained in \( H \), and hence \( k \, t(a^{-1}) \circ a \in H, c \, r \, t^2(b), c \, r \, t(b^{-1}) \) and \( c \, r \, b \). From this we see that \( x \cdot xy = y \) for all \( x, y \in Q/H \). Similarly we can show that \( ab \, r \, a^{-1} \circ b^{-1} \) and \( ba \, r \, b^{-1} \circ a^{-1} \) for all \( a, b \in Q \). But \( Q(\varnothing)/H(\varnothing) \) is commutative by 3.14, and therefore \( b^{-1} \circ a^{-1} \circ r \, a^{-1} \circ b^{-1} \) and \( ab \, r \, ba \). Thus \( Q/H \) is commutative. Finally, \( aa = k(a) \circ t(a) \circ q \circ a^{-2} \circ r \, a \), since \( a^3 \) is contained in \( H \) by 3.5, and it is seen that \( Q/H \) is idempotent. An application of 6.3 completes the proof.

8.10. Lemma. Let \( a, b \in Q \). Then the subquasigroup generated by \( \{a, b\} \cup H \) is isotopic to a group.

79
Proof. Apply 8.8 and 3.14(ii).

8.11. Lemma. Let a, c ∈ H, b ∈ M(Q) and d ∈ Q. Then ab . cd = ac . bd.

Proof. a, c ∈ N(Q(σ)), b ∈ K(Q(σ)), and therefore ab . cd = (k^2(a) ○ k t(b) ○ k(q)) ○ (k t(c) ○ t^2(d) ○ t(q)) q = (k^2(a) ○ ((k t(b) ○ k t(c)) ○ t^2(d)) ○ k(q) ○ t(q)) q = (k^2(a) ○ ((k t(c) ○ k t(b)) ○ t^2(d)) ○ k(q) ○ t(q)) ○ q = (k^2(a) ○ k t(c) ○ k(q)) ○ (k t(b) ○ t^2(d) ○ t(q)) q = ac . bd.

8.12. Lemma. For every a ∈ Q there are b ∈ H and c ∈ M(Q) such that a = bc.

Proof. There are x ∈ N(Q(σ)) and y ∈ K(Q(σ)) such that a = x ○ y. Put b = k^{-1}(x) and c = t^{-1}(y ○ q^{-1}). Then b ∈ H, c ∈ M(Q) and a = bc.

8.13. Lemma. The quasigroup Q is a homomorphic image of H × M(Q).

Proof. With respect to 8.11 and 8.12, we can define a homomorphism g of H × M(Q) onto Q by g(a, b) = ab for all a ∈ H and b ∈ M(Q).

8.14. Lemma. If Q is unipotent then Q(σ) is an abelian group.

Proof. We have aa = k(a) ○ t(a) ○ q = bb = k(b) ○ t(b) ○ q for all a, b ∈ Q. Hence k(a) ○ t(a) = j, k(a) = t(a^{-1}) and the mapping a → a^{-1} is an automorphism of Q(σ). It is easy to see that Q(σ) is commutative. Further, a ○ k(a), a ○ t(a) = a ○ k(a^{-1}) and a^{-2} are contained in N(Q(σ)) (by 3.22 and 3.5). Consequently a^{-1} ∈ N(Q(σ)) and N(Q(σ)) = Q.

8.15. Lemma. Let aa . ba = ab . aa for all a, b ∈ Q. Then Q(σ) is commutative.

Proof. We have (k^2(a) ○ k t(a)) ○ (b ○ t^2(a)) = (k^2(a) ○ b) ○ (k t(a) ○ t^2(a)) for all a, b ∈ Q. However, a^{-1} ○ t^2 k^{-2}(a) ∈ N(Q(σ)) and hence (a ○ (t k^{-1}(a) ○ b)) ○ t^2 k^{-2}(a) = (a ○ (b ○ t k^{-1}(a))) ○ t^2 k^{-2}(a) = (a ○ b ○ t k^{-1}(a)) ○ t^2 k^{-2}(a) by 3.16. Thus t k^{-1}(a) ○ b = b ○ t k^{-1}(a).

8.16. Lemma. Q is an IP-quasigroup iff k^2 = 1 = t^2.

Proof. The proof is purely of technical character and hence omitted.

8.17. Lemma. Let p be a mapping of Q into Q. Then p is a regular mapping of Q iff there is x ∈ N(Q(σ)) such that p(a) = x ○ a for every a ∈ Q.

Proof. Easy.

8.18. Lemma. Define a relation r on Q by a r b iff a = p(b) for a regular mapping p of Q. Then r is a normal congruence of Q and H is one of its classes.

Proof. Apply 8.8, 8.9 and 8.17.
By an FM-quasigroup or an FG-quasigroup we mean an F-quasigroup which is isotopic to a Moufang loop or a group, respectively.

9.1. Theorem. The following statements are equivalent for every quasigroup $Q$:

(i) $Q$ is an FM-quasigroup.

(ii) There are a Moufang loop $Q(o)$, $k, t \in \text{Aut } Q(o)$ and $q \in C(Q(o))$ such that
$$kt = tk, \quad a^{-1} \circ k(a), \quad a^{-1} \circ t(a) \in K(Q(o)), \quad a^{-1} \circ k(a^2), \quad a^{-1} \circ t(a^2) \in N(Q(o))$$
and
$$ab = k(a) \circ t(b) \circ q$$
for all $a, b \in Q$.

Proof. (i) implies (ii). Let $p \in Q$, $x = f e^2(p)$, $y = ef^2(p)$, $g = R_x$, $h = L_y$, $z = yx \cdot x$, $w = y \cdot yx$, $k = gR_{f(x)}g^{-1}$, $t = hL_{e(y)}h^{-1}$ and $q = z \circ w$, where $a \circ b = g^{-1}(a) \cdot h^{-1}(b)$ for all $a, b \in Q$. Then $Q(o)$ is a Moufang loop. Further, $f(x) = e^2f^2(p) = e(y)$ and $gh = hg$ by 4.3. On the other hand, $x = ef(p)$, $y = eff(p)$ and we can apply 7.13.

(ii) implies (i). Use 8.1.

9.2. Theorem. Let $Q$ be an FM-quasigroup and $M = M(Q)$. Then:

(i) $e(Q), f(Q) \subseteq M$ and $M$ is a normal subquasigroup of $Q$.

(ii) $M$ is a trimedial quasigroup and $Q/M$ is a group.

(iii) If $a \in Q$ then the subquasigroup generated by $\{a\} \cup M$ is trimedial.

Proof. Apply 9.1, 8.5, 8.6 and 8.7.

9.3. Corollary. Let $Q$ be an FM-quasigroup. Then $e(Q)$ and $f(Q)$ are trimedial subquasigroups of $Q$.

9.4. Corollary. Every FM-quasigroup is monomedial.

9.5. Corollary. Every simple FM-quasigroup is either medial or it is a group.

Proof. Let $Q$ be a simple FM-quasigroup. By 9.2, $Q$ is either a group or a trimedial quasigroup. However, every simple trimedial quasigroup is medial (see [7], Corollary 6).

Remark. Simple medial quasigroups are completely described in [4].

9.6. Theorem. Let $Q$ be an FM-quasigroup and $a \sim b$ iff $a = p(b)$ for a regular mapping $p$ of $Q$. Then:

(i) $\sim$ is a normal congruence of $Q$.

(ii) Every class of $\sim$ is a subquasigroup of $Q$ and, moreover, an FG-quasigroup.

(iii) $Q/\sim$ is a distributive Steiner quasigroup.
(iv) If $H$ is a class of $r$ and $a, b \in Q$ then the subquasigroup generated by $\{a, b\} \cup H$ is an FG-quasigroup.

(v) If $H$ is a class of $r$ then $Q$ is a homomorphic image of the cartesian product $H \times M(Q)$.

Proof. (i) and (iii) follow from 9.1 and 8.18, 8.9. Since $Q/r$ is idempotent, every class of $r$ is a subquasigroup. Now let $H$ be a class of $r$. With respect to the proof of 9.1, we can assume that the unit of the corresponding Moufang loop $Q(\omega)$ is contained in $H$. Then $H = N(Q(\omega))$ and we can apply 8.9, 8.10 and 8.13.

9.7. Corollary. Let $Q$ be an FM-quasigroup. Then every subquasigroup generated by at most two elements is an FG-quasigroup.

9.8. Theorem. Every unipotent FM-quasigroup is medial.

Proof. Apply 9.1, 8.14 and 6.11.

9.9. Theorem. Let $Q$ be an FM-quasigroup. Then $Q$ is trimedial, provided at least one of the following conditions holds:

(i) $e$ is a mapping onto $Q$.

(ii) $e$ is a one-to-one mapping.

(iii) $f$ is a mapping onto $Q$.

(iv) $f$ is a one-to-one mapping.

(v) $Q$ is trimedial.

(vi) $Q$ is isotopic to a commutative quasigroup.

(vii) $D(Q)$ is non-empty.

(viii) $ab \cdot aa = aa \cdot ba$ for all $a, b \in Q$.

Proof. (i) and (iii) follow from 9.3, (v) and (viii) follow from 8.15 and 8.2, (vi) follows from 3.15 and 8.2.

(ii) and (iv). If $e$ is one-to-one then $e$ is an isomorphism of $Q$ onto $e(Q)$ and we can use 9.3. Similarly the other case. (vii) If $D(Q)$ is non-empty and $x \in D(Q)$ then the quasigroup $Q(*)$ where $a * b = L_x(a) \cdot R_x(b)$, is commutative and (vi) may be used.

9.10. Corollary. Every $F$-quasigroup isotopic to a commutative Moufang loop is trimedial.

9.11. Theorem. The following conditions are equivalent for a quasigroup $Q$:

(i) $Q$ is an IP-quasigroup and an $F$-quasigroup.

(ii) There are a Moufang loop $Q(\omega)$, $k, t \in \text{Aut } Q(\omega)$ and $q \in C(Q(\omega))$ such that $kt = tk$, $k^2 = 1 = t^2$, $a^{-1} \circ k(a), a^{-1} \circ t(a) \in K(Q(\omega))$, $a^{-1} \circ k(a^2), a^{-1} \circ t(a^2) \in N(Q(\omega))$ and $ab = k(a) \circ t(b) \circ q$ for all $a, b \in Q$.

References


Author’s address: 186 00 Praha 8 - Karlin, Sokolovská 83, ČSSR (Matematicko-fyzikální fakulta UK).