F-QUASIGROUPS ISOTOPIC TO GROUPS

TOMÁŠ KEPKA*, MICHAEL K. KINYON, AND J. D. PHILLIPS

Abstract. In [5] we showed that every loop isotopic to an F-quasigroup is a Moufang loop. Here we characterize, via two simple identities, the class of F-quasigroups which are isotopic to groups. We call these quasigroups FG-quasigroups. We show that FG-quasigroups are linear over groups. We then use this fact to describe their structure. This gives us, for instance, a complete description of the simple FG-quasigroups. Finally, we show an equivalence of equational classes between pointed FG-quasigroups and central generalized modules over a particular ring.

1. Introduction

Let Q be a non-empty set equipped with a binary operation (denoted multiplicatively throughout the paper). For each $a \in Q$, the left and right translations L_a and R_a are defined by $L_a x = ax$ and $R_a x = xa$ for all $x \in Q$. The structure $(Q, \cdot)$ is called a *quasigroup* if all of the right and left translations are permutations of Q [2, 8].

In a quasigroup $(Q, \cdot)$, there exist transformations $\alpha, \beta : Q \to Q$ such that $x\alpha(x) = x = \beta(x)x$ for all $x \in Q$. A quasigroup Q is called a *left F-quasigroup* if

$$x \cdot yz = xy \cdot \alpha(x)z \qquad (F_l)$$

for all $x, y, z \in Q$. Dually, Q is called a *right F-quasigroup* if

$$zy \cdot x = z\beta(x) \cdot yx \qquad (F_r)$$

for all $x, y, z \in Q$. If Q is both a left F- and right F-quasigroup, then Q is called a (two-sided) *F-quasigroup* [1, 3, 4, 5, 6, 7, 9].

Recall that for a quasigroup $(Q, \cdot)$ and for fixed $a, b \in Q$, the structure $(Q, +)$ consisting of the set Q endowed with the binary operation $+ : Q \times Q \to Q$ defined by $x + y = R_b^{-1}x \cdot L_a^{-1}y$ is called a *principal isotope* of $(Q, +)$. Here $(Q, +)$ is a quasigroup with neutral element $0 = ab$, that is, $(Q, +)$ is a *loop* [2]. (Throughout this paper, we will use additive notation for loops, including groups, even if the operation is not commutative.)

Date: January 4, 2006.

1991 *Mathematics Subject Classification.* 20N05.

Key words and phrases. F-quasigroup, Moufang loop, generalized modules.

*Partially supported by the institutional grant MSM 113200007 and by the Grant Agency of Charles University, grant #269/2001/B-MAT/MFF.

To study any particular class of quasigroups, it is useful to understand the loops isotopic to the quasigroups in the class. In [5], we have shown that every loop isotopic to an F-quasigroup is a Moufang loop. In this paper, which is in some sense a prequel to [5], we study the structure of a particular subclass of F-quasigroups, namely those which are isotopic to groups. An F-quasigroup isotopic to a group will be called an *FG-quasigroup* in the sequel.

A quasigroup Q is called *medial* if $xa \cdot by = xb \cdot ay$ for all $x, y, a, b \in Q$. We see that (F_l) and (F_r) are generalizations of the medial identity. The main result of §2 is that the class of FG-quasigroups is axiomatized by two stronger generalizations the medial identity. In particular, we will show (Theorem 2.8) that a quasigroup is an FG-quasigroup if and only if

$$xy \cdot \alpha(u)v = x\alpha(u) \cdot yv \tag{A}$$

and

$$xy \cdot \beta(u)v = x\beta(u) \cdot yv \tag{B}$$

hold for all x, y, u, v.

In §4, we will show that FG-quasigroups are more than just isotopic to groups; they are, in fact, linear over groups. A quasigroup Q is said to be *linear* over a group $(Q, +)$ if there exist $f, g \in \mathcal{A}ut(Q, +)$ and $e \in Q$ such that $xy = f(x) + e + g(y)$ for all $x, y \in Q$. In §3, we give necessary and sufficient conditions in terms of f, g, and e for a quasigroup Q linear over a group $(Q, +)$ to be an FG-quasigroup.

In §5, we will use the linearity of FG-quasigroups to describe their structure. For a quasigroup Q, set $M(Q) = \{a \in Q : xa \cdot yx = xy \cdot ax \ \forall x, y \in Q\}$. We will show (Proposition 5.6) that in an FG-quasigroup Q, $M(Q)$ is a medial, normal subquasigroup and $Q/M(Q)$ is a group. In particular, this gives us a complete description of simple FG-quasigroups (Corollary 5.7) up to an understanding of simple groups.

In §6 we codify the relationship between FG-quasigroups and groups by introducing the notion of *arithmetic form* for an FG-quasigroup (Definition 6.1). This enables us to show an equivalence of equational classes between (pointed) FG-quasigroups and certain types of groups with operators (Theorem 6.4 and Lemma 6.5). Finally, motivated by this equivalence, we introduce in §7 a notion of *central generalized module* over an associative ring, and we show an equivalence of equational classes between (pointed) FG-quasigroups and central generalized modules over a particular ring (Theorem 7.1). In [6], which is the sequel to [5], we will examine the more general situation for arbitrary F-quasigroups and introduce a correspondingly generalized notion of module.

2. Characterizations of FG-quasigroups

Proposition 2.1. *Let Q be a left F-quasigroup. Then*

1. $\alpha\beta = \beta\alpha$ *and* α *is an endomorphism of* Q.
2. $R_a L_b = L_b R_a$ *for* $a, b \in Q$ *if and only if* $\alpha(b) = \beta(a)$.

3. $R_{\alpha(a)}L_{\beta(a)} = L_{\beta(a)}R_{\alpha(a)}$ *for every* $a \in Q$.

Proof. For (1): $x \cdot \alpha\beta(x)\alpha(x) = \beta(x)x \cdot \alpha\beta(x)\alpha(x) = \beta(x) \cdot x\alpha(x) = \beta(x)x = x = x\alpha(x)$ and so $\alpha\beta(x) = \beta\alpha(x)$. Further, $xy \cdot \alpha(x)\alpha(y) = x \cdot y\alpha(x) = xy = xy \cdot \alpha(xy)$ and $\alpha(x)\alpha(y) = \alpha(xy)$.

For (2): If $R_aL_b = L_bR_a$, then $ba = R_aL_b\alpha(b) = L_bR_a\alpha(b) = b \cdot \alpha(b)a, a = \alpha(b)a$ and $\beta(a) = \alpha(b)$.

Conversely, if $\beta(a) = \alpha(b)$ then $b \cdot xa = bx \cdot \alpha(b)a = bx \cdot \beta(a)a = bx \cdot a$.

Finally (3), follows from (1) and (2). □

Corollary 2.2. *If Q is an F-quasigroup, then α and β are endomorphisms of Q, and $\alpha\beta = \beta\alpha$.*

For a quasigroup $(Q, \cdot)$, if the loop isotope $(Q, +)$ given by $x + y = L_b^{-1}x \cdot R_a^{-1}y$ for all $x, y \in Q$ is a associative (*i.e.*, a group), then $L_b^{-1}x \cdot R_a^{-1}(L_b^{-1}y \cdot R_a^{-1}z) = L_b^{-1}(L_b^{-1}x \cdot R_a^{-1}y) \cdot R_a^{-1}z$ for all $x, y, z \in Q$. Replacing x with L_bx and z with R_az, we have that associativity of $(Q, \circ)$ is characterized by the equation

$$x \cdot L_b^{-1}(R_a^{-1}y \cdot z) = R_a^{-1}(x \cdot L_b^{-1}y) \cdot z \tag{2.1}$$

for all $x, y, z \in Q$, or equivalently,

$$L_xL_b^{-1}R_zR_a^{-1} = R_zR_a^{-1}L_xL_b^{-1} \tag{2.2}$$

for all $x, zinQ$.

Lemma 2.3. *Let Q be a quasigroup. The following are equivalent:*

1. *Every loop isotopic to Q is a group.*
2. *Some loop isotopic to Q is a group.*
3. *For all $x, y, z, a, b \in Q$, (2.1) holds.*
4. *There exist $a, b \in Q$ such that (2.1) holds for all $x, y, z \in Q$.*

Proof. The equivalence of (1) and (2) is well known [2]. (3) and (4) simply express (1) and (2), respectively, in the form of equations. □

Lemma 2.4. *Let Q be an F-quasigroup. The following are equivalent:*

1. *Q is an FG-quasigroup,*
2. $x\beta(a) \cdot (L_b^{-1}R_a^{-1}y \cdot z) = (x \cdot R_a^{-1}L_b^{-1}y) \cdot \alpha(b)z$ *for all* $x, y, z \in Q$.

Proof. Starting with Lemma 2.3, observe that (F_r) and (F_l) give $R_a^{-1}(uv) = R_{\beta(a)}^{-1}u \cdot R_a^{-1}v$ and $L_b^{-1}(uv) = L_b^{-1}u \cdot L_{\alpha(b)}^{-1}v$ for all $u, v, \in Q$. Replace x with $x\beta(a)$ and replace z with $\alpha(b)z$. The result follows. □

Lemma 2.5. *Let Q be an F-quasigroup and let $a, b \in Q$ be such that $\alpha(b) = \beta(a)$. Then Q is an FG-quasigroup if and only if $x\beta(a) \cdot yz = xy \cdot \alpha(b)z$ for all $x, y, z \in Q$.*

Proof. By Proposition 2.1(2), $R_aL_b = L_bR_a$ and so $R_a^{-1}L_b = L_bR_a^{-1}$. The result follows from Lemma 2.4 upon replacing y with R_aL_by. □

Proposition 2.6. *The following conditions are equivalent for an F-quasigroup Q:*

1. *Q is an FG-quasigroup,*
2. *$x\alpha\beta(w) \cdot yz = xy \cdot \alpha\beta(w)z$ for all $x, y, z, w \in Q$.*
3. *There exists $w \in Q$ such that $x\alpha\beta(w) \cdot yz = xy \cdot \alpha\beta(w)z$ for all $x, y, z \in Q$.*

Proof. For given $w \in Q$, set $a = \alpha(w)$ and $b = \beta(w)$. By Corollary 2.2, $\alpha(b) = \beta(a)$, and so the result follows from Lemma 2.5. □

The preceding results characterize FG-quasigroups among F-quasigroups. Thus the F-quasigroup laws together with Proposition 2.6(2) form an axiom base for FG-quasigroups. Now we turn to the main result of this section, a two axiom base for FG-quasigroups.

Lemma 2.7. *Let Q be an FG-quasigroup. For all $x, y, u, v \in Q$, $L_x L_y^{-1} R_v^{-1} R_u = R_v^{-1} R_u L_x L_y^{-1}$.*

Proof. Another expression for (F_r) is $R_v^{-1} R_u = R_{\beta(u)} R^{-1}_{R_u^{-1} v}$, and so the result follows from (2.2). □

Theorem 2.8. *A quasigroup Q is an FG-quasigroup if and only if the identities (A) and (B) hold.*

Proof. Suppose first that Q is an FG-quasigroup. We first verify the following special case of (A): for all $x, y, u, v \in Q$,

$$\alpha(x)y \cdot \alpha(u)v = \alpha(x)\alpha(u) \cdot yv \tag{2.3}$$

Indeed, (F_l) implies $y = L_u^{-1} R^{-1}_{\alpha(u)v} R_{yv} u$. Using this and Lemma 2.7, we compute

$$\alpha(x)y \cdot \alpha(u)v = R_{\alpha(u)v} L_{\alpha(x)} L_u^{-1} R^{-1}_{\alpha(u)v} R_{yv} u = R_{yv} L_{\alpha(x)} L_u^{-1} u = \alpha(x)\alpha(u) \cdot yv$$

as claimed.

Next we verify (B). For all $x, y, u, v \in Q$,

$$\begin{aligned} x\beta(\alpha(u)y) \cdot (u \cdot vy) &= x\beta(\alpha(u)y) \cdot (uv \cdot \alpha(u)y) && \text{by } (F_l) \\ &= (x \cdot uv) \cdot \alpha(u)y && \text{by } (F_r) \\ &= (xu \cdot \alpha(x)v) \cdot \alpha(u)y && \text{by } (F_l) \\ &= (xu \cdot \beta(\alpha(u)y)) \cdot (\alpha(x)v \cdot \alpha(u)y) && \text{by } (F_r) \\ &= (xu \cdot \beta(\alpha(u)y)) \cdot (\alpha(x)\alpha(u) \cdot vy) && \text{by } (2.3) \\ &= xu \cdot (\beta(\alpha(u)y) \cdot vy) && \text{by } (F_l) \end{aligned}$$

where we have also used Corollary 2.2 in the last step. Replacing v with $R_y^{-1} v$ and then y with $L_{\alpha u}^{-1} y$, we have (B). The proof of (A) is similar.

Conversely, suppose Q satisfies (A) and (B). Obviously, (A) implies (F_l) and (B) implies (F_r), and so we may apply Proposition 2.6 to get that Q is an FG-quasigroup. □

3. Quasigroups linear over groups

Throughout this section, let Q be a quasigroup and $(Q,+)$ a group, possibly noncommutative, but with the same underlying set as Q. Assume that Q is linear over $(Q,+)$, that is, there exist $f, g \in \mathcal{A}ut(Q,+)$, $e \in Q$ such that $xy = f(x) + e + g(y)$ for all $x, y \in Q$.

Let $\Phi \in \mathcal{A}ut(Q,+)$ be given by $\Phi(x) = -e + x + e$ for all $x \in Q$. If we define a multiplication on Q by $x \cdot_1 y = f(x) + g(y) + e$ for all $x, y \in Q$, then $x \cdot_1 y = f(x) + e - e + g(y) + e = f(x) + e + \Phi g(y)$. On the other hand, if we define a multiplication on Q by $x \cdot_2 y = e + f(x) + g(y)$ for all $x, y \in Q$, then $x \cdot_2 y = \Phi^{-1} f(x) + e + g(y)$. In particular, there is nothing special about our convention for quasigroups linear over groups; we could have used $(Q, \cdot_1)$ or $(Q, \cdot_2)$ instead.

Lemma 3.1. *With the notation conventions of this section,*

1. *Q is a left F-quasigroup if and only if $fg = gf$ and $-x + f(x) \in Z(Q,+)$ for all $x \in Q$,*
2. *Q is a right F-quasigroup if and only if $fg = gf$ and $-x + g(x) \in Z(Q,+)$ for all $x \in Q$,*
3. *Q is an F-quasigroup if and only if $fg = gf$ and $-x + f(x), -x + g(x) \in Z(Q,+)$ for all $x \in Q$.*

Proof. First, note that $\alpha(u) = -g^{-1}(e) - g^{-1}f(u) + g^{-1}(u)$ and $\beta(u) = f^{-1}(u) - f^{-1}g(u) - f^{-1}(e)$ for all $u \in Q$.

For (1): Fix $u, v, w \in Q$ and set $x = f(u)$ and $y = gf(v)$. We have

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

and

$$uv \cdot \alpha(u)w = f^2(u) + f(e) + fg(v) + e - gfg^{-1}(e) - gfg^{-1}f(u) + gfg^{-1}(u) + g(e) + g^2(w).$$

Thus (F_l) holds if and only if

$$x + e + y = f(x) + f(e) + fgf^{-1}g^{-1}(y) + e - gfg^{-1}(e) - gfg^{-1}(x) + gfg^{-1}f^{-1}(x) \quad (3.1)$$

for all $x, y \in Q$.

Suppose (F_l) holds. Then setting $x = 0$ in (3.1) yields $e + y = f(e) + fgf^{-1}g^{-1}(y) + e - gfg^{-1}(e)$ and $x = 0 = y$ yields $-f(e) + e = e - gfg^{-1}(e)$. Thus $-f(e) + e + y = fgf^{-1}g^{-1}(y) - f(e) + e$ and $x + e + y = f(x) + e + y - gfg^{-1}(x) + gfg^{-1}f^{-1}(x)$. Setting $y = -e$ in the latter equality, we get $-f(x) + x = -gfg^{-1}(x) + gfg^{-1}f^{-1}(x)$ and hence $-f(x) + x + e + y = e + y - f(x) + x$. Consequently, $-f(x) + x \in Z(Q,+)$ for all $x \in Q$ and looking again at the already derived equalities, we conclude that $fg = gf$.

For the converse, suppose $fg = gf$. Then (3.1), after some rearranging, becomes

$$(-f(x) + x) + e + y = f(e) + y + (e - f(e)) + (-f(x) + x).$$

If we also suppose $-x + f(x) \in Z(Q,+)$ for all $x \in Q$, then the latter equation reduces to a triviality, and so (F_l) holds.

The proof of (2) is dual to that of (1), and (3) follows from (1) and (2). □

It is straightforward to characterize F-quasigroups among quasigroups linear over groups for the alternative definitions $(Q, \cdot_1)$ and $(Q, \cdot_2)$ above. Recalling that $\Phi(x) = e + x - e$, observe that if $-z + f(z) \in Z(Q, +)$ for all $z \in Q$, then $fg = gf$ if and only if $f\Phi g = \Phi gf$. Using this observation and Lemma 3.1(3), we get the following assertion: $(Q, \cdot_1)$ is an F-quasigroup if and only if $fg = gf$ and $-x+f(x), -x+\Phi g(x) \in Z(Q, +)$ for all $x \in Q$. Similarly, $(Q, \cdot_2)$ is an F-quasigroup if and only if $fg = gf$ and $-x + \Phi^{-1} f(x), -x + g(x) \in Z(Q, +)$ for all $x \in Q$.

4. FG-quasigroups are linear over groups

Let h and k be permutations of a group $(Q, +)$. Define a multiplication on Q by $xy = h(x) + k(y)$ for all $x, y \in Q$. Clearly, Q is a quasigroup.

Lemma 4.1. *Assume that Q is a right F-quasigroup. Then:*

1. $h(x + y) = h(x) - h(0) + h(y)$ *for all* $x, y \in Q$.
2. *The transformations* $x \mapsto h(x) - h(0)$ *and* $x \mapsto -h(0) + h(x)$ *are automorphisms of* $(Q, +)$.

Proof. We have $\beta(u) = h^{-1}(u - k(u))$ and $h(h(w) + k(v)) + k(u) = wv \cdot u = w\beta(u) \cdot vu = h(h(w) + kh^{-1}(u - k(u))) + k(h(v) + k(u))$ for all $u, v, w \in Q$. Then $h(x+y)+z = h(x+kh^{-1}(k^{-1}(z)-z))+k(hk^{-1}(y)+z)$ for all $x, y, z \in Q$. Setting $z = 0$ we get $h(x + y) = h(x + t) + khk^{-1}(y)$ where $t = kh^{-1}k^{-1}(0)$. Consequently, $h(y) = h(t) + khk^{-1}(y)$ and $khk^{-1}(y) = -h(t) + h(y)$. Similarly, $h(x) = h(x + t) + khk^{-1}(0) = h(x + t) - h(t) + h(0), h(x + t) = h(x) - h(0) + h(t)$. Thus, $h(x + y) = h(x) - h(0) + h(t) - h(t) + h(y) = h(x) - h(0) + h(y)$. This establishes (1). (2) follows immediately from (1). □

Lemma 4.2. *Assume that Q is a left F-quasigroup. Then:*

1. $k(x + y) = k(x) - k(0) + k(y)$ *for all* $x, y \in Q$.
2. *The transformations* $x \mapsto k(x) - k(0)$ *and* $x \mapsto -k(0) + k(x)$ *are automorphisms of* $(Q, +)$.

Proof. Dual to the proof of Lemma 4.1. □

Now let Q be an FG-quasigroup, $a, b \in Q, h = R_a, k = L_b$ and $x + y = h^{-1}(x) \cdot k^{-1}(y)$ for all $x, y \in Q$. Then $(Q, +)$ is a group (every principal loop isotope of Q is of this form), $0 = ba$ and $xy = h(x) + k(y)$ for all $x, y \in Q$. Moreover, by Lemmas 4.1 and 4.2, the transformations $f : x \mapsto h(x) - h(0)$ and $g : x \mapsto -k(0) + k(x)$ are automorphisms of $(Q, +)$. We have $xy = f(x) + e + g(y)$ for all $x, y \in Q$ where $e = h(0) + k(0) = 0 \cdot 0 = ba \cdot ba$.

Corollary 4.3. *Every FG-quasigroup is linear over a group.*

5. Structure of FG-quasigroups

Throughout this section, let Q be an FG-quasigroup. By Corollary 4.3, Q is linear over a group $(Q, +)$, that is, there exist $f, g \in \mathcal{A}ut(Q, +)$, $e \in Q$ such that

$xy = f(x) + e + g(y)$ for all $x, y \in Q$. Recall the definition

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

Lemma 5.1. $M(Q) = Z(Q,+) - e = \{a \in Q : xa \cdot yz = xy \cdot az \ \forall x, y, z \in Q\}$.

Proof. If $a \in M(Q)$, then $f^2(x)+f(e)+fg(a)+e+fg(y)+g(e)+g^2(x) = xa \cdot yx = xy \cdot ax = f^2(x)+f(e)+fg(y)+e+fg(a)+g^2(x)$ or, equivalently, $fg(a)+e+z = z+e+fg(a)$ for all $z \in Q$. The latter equality is equivalent to the fact that $fg(a)+e \in Z(Q,+)$ or $a \in f^{-1}g^{-1}(Z(Q,+)-e) = Z(Q,+) - f^{-1}g^{-1}(e) = Z(Q,+) - e$, since $f^{-1}g^{-1}(e) - e \in Z(Q,+)$. We have shown that $M(Q) \subseteq Z(Q,+) - e$. Proceeding conversely, we show that $Z(Q,+) - e \subseteq \{a \in Q : xa \cdot yz = xy \cdot az\}$, and the latter subset is clearly contained in $M(Q)$. □

Corollary 5.2. *The following conditions are equivalent:*

1. $M(Q) = Z(Q,+)$.
2. $e \in Z(Q,+)$.
3. $0 \in M(Q)$.

Lemma 5.3. $\alpha(Q) \cup \beta(Q) \subseteq M(Q)$.

Proof. This follows from Theorem 2.8. □

Lemma 5.4. *$M(Q)$ is a medial subquasigroup of Q.*

Proof. If $u, v, w \in Z(Q,+)$ then $(u-e)\cdot(v-e) = f(u) - f(e) + e + g(v) - g(e) = w - e \in Z(Q,+) - g(e) = Z(Q,+) - e = M(Q)$. Thus $M(Q) = Z(Q,+) - e$ (Lemma 5.1) is closed under multiplication, and it is easy to see that for each $a, b \in Z(Q,+)$, the equations $(a-e)\cdot(x-e) = b-e$ and $(y-e)\cdot(a-e) = b-e$ have unique solutions $x, y \in Z(Q,+)$. We conclude that $M(Q)$ is a subquasigroup of Q. Applying Lemma 5.1 again, $M(Q)$ is medial. □

Lemma 5.5. *$M(Q)$ is a normal subquasigroup of Q, and $Q/M(Q)$ is a group.*

Proof. $Z(Q,+)$ is a normal subgroup of the group $(Q,+)$, and if ρ denotes the (normal) congruence of $(Q,+)$ corresponding to $Z(Q,+)$, it is easy to check that ρ is a normal congruence of the quasigroup Q, too. Finally, by Lemma 5.3, $Q/M(Q)$ is a loop, and hence it is a group. □

Putting together Lemmas 5.1, 5.3, 5.4, and 5.5, we have the following.

Proposition 5.6. *Let Q be an FG-quasigroup. Then $\alpha(Q) \cup \beta(Q) \subseteq M(Q) = \{a \in Q : xa \cdot yz = xy \cdot az \ \forall x, y, z \in Q\}$, $M(Q)$ is a medial, normal subquasigroup of Q, and $Q/M(Q)$ is a group.*

Corollary 5.7. *A simple FG-quasigroup is medial or is a group.*

6. Arithmetic forms of FG-quasigroups

Definition 6.1. *An ordered five-tuple $(Q, +, f, g, e)$ will be called an* arithmetic form *of a quasigroup Q if the following conditions are satisfied:*

(1) *The binary structures $(Q, +)$ and Q share the same underlying set (denoted by Q again);*
(2) *$(Q, +)$ is a (possibly noncommutative) group;*
(3) *$f, g \in \mathcal{A}ut(Q, +)$;*
(4) *$fg = gf$;*
(5) *$-x + f(x), -x + g(x) \in Z(Q, +)$ for all $x \in Q$;*
(6) *$e \in Q$;*
(7) *$xy = f(x) + e + g(y)$ for all $x, y \in Q$.*

If, moreover, $e \in Z(Q, +)$, then the arithmetic form will be called strong.

Theorem 6.2. *The following conditions are equivalent for a quasigroup Q:*

1. *Q is an FG-quasigroup.*
2. *Q has at least one strong arithmetic form.*
3. *Q has at least one arithmetic form.*

Proof. Assume (1). From Corollary 4.3 and Lemma 3.1(3), we know that for all $a, b \in Q$, Q has an arithmetic form $(Q, +, f, g, e)$ such that $0 = ba$. Further, by Lemma 5.3, $\alpha(Q) \cup \beta(Q) \subseteq M(Q)$. Now, if the elements a and b are chosen so that $ba \in \alpha(Q) \cup \beta(Q)$ (for instance, choose $a = b = \alpha\beta(c)$ for some $c \in Q$ and use Corollary 2.2), or merely that $ba \in M(Q)$, then the form is strong by Corollary 5.2. Thus (2) holds. (2) implies (3) trivially, and (3) implies (1) by Lemma 3.1(3). □

Lemma 6.3. *Let $(Q, +, f_1, g_1, e_1)$ and $(Q, *, f_2, g_2, e_2)$ be arithmetic forms of the same FG-quasigroup Q. If the groups $(Q, +)$ and $(Q, *)$ have the same neutral element 0, then $(Q, +) = (Q, *)$, $f_1 = f_2, g_1 = g_2$, and $e_1 = e_2$.*

Proof. We have $f_1(x) + e_1 + g_1(y) = xy = f_2(x) * e_2 * g_2(y)$ for all $x, y \in Q$. Setting $x = 0 = y$, we get $e_1 = e_2 = e$. Setting $x = 0$ we get $p(y) = e + g_1(y) = e_2 * g_2(y)$ and so $f_1(x) + p(y) = f_2(x) * p(y)$. But p is a permutation of Q and $p(y) = 0$ yields $f_1 = f_2$. Similarly, $g_1 = g_2$ and, finally, $(Q, +) = (Q, *)$. □

Theorem 6.4. *Let Q be an FG-quasigroup. Then there exists a biunique correspondence between arithmetic forms of Q and elements from Q. This correspondence restricts to a biunique correspondence between strong arithmetic forms of Q and elements from $M(Q)$.*

Proof. Combine Corollary 4.3, Lemma 3.1(3), and Corollary 5.2. □

Lemma 6.5. *Let Q and P be FG-quasigroups with arithmetic forms $(Q, +, f, g, e_1)$ and $(P, +, h, k, e_2)$, respectively. Let $\varphi : Q \to P$ be a mapping such that $\varphi(0) = 0$. Then φ is a homomorphism of the quasigroups if and only if φ is a homomorphism of the groups, $\varphi f = h\varphi, \varphi g = k\varphi$ and $\varphi(e_1) = e_2$.*

Proof. This generalization of Lemma 6.3 has a similar proof. □

Denote by $\mathcal{F}_{g,p}$ the equational class (and category) of pointed FG-quasigroups. That is $\mathcal{F}_{g,p}$ consists of pairs (Q,a), Q being an FG-quasigroup and $a \in Q$ a fixed element. If $(P,b) \in \mathcal{F}_{g,p}$ then a mapping $\varphi : Q \to P$ is a homomorphism in $\mathcal{F}_{g,p}$ if and only if φ is a homorphism of the quasigroups and $\varphi(a) = b$. Further, put $\mathcal{F}_{g,m} = \{(Q,a) \in \mathcal{F}_{g,p} : a \in M(Q)\}$. Clearly $\mathcal{F}_{g,m}$ is an equational subclass (and also a full subcategory) of $\mathcal{F}_{g,p}$.

Let $\varphi : Q \to P$ be a homomorphism of FG-quasigroups. For every $a \in Q$ we have $(Q, \alpha(a)), (P, \alpha\varphi(a)) \in \mathcal{F}_{g,m}$, and $\varphi\alpha(a) = \alpha\varphi(a)$. Thus φ is a homomorphism in $\mathcal{F}_{g,m}$. Similarly, $(Q, \beta(a)), (P, \beta\varphi(a)) \in \mathcal{F}_{g,m}$ and $\varphi\beta(a) = \beta\varphi(a)$.

Denote by $\mathcal{G}$ the equational class (and category) of algebras $Q(+, f, g, f^{-1}, g^{-1}, e)$ where $(Q,+)$ is a group and conditions (2)-(6) of Definition 6.1 are satisfied. If $P(+, h, k, h^{-1}, k^{-1}, e_1) \in \mathcal{G}$, then a mapping $\varphi : Q \to P$ is a homomorphism in $\mathcal{G}$ if and only if φ is a homomorphism of the groups such that $\varphi f = h\varphi, \varphi g = k\varphi$ and $\varphi(e) = e_1$. Finally, denote by $\mathcal{G}_c$ the equational subclass of $\mathcal{G}$ given by $e \in Z(Q,+)$.

It follows from Theorem 6.4 and Lemma 6.5 that the classes $\mathcal{F}_{g,p}$ and $\mathcal{G}$ are equivalent. That means that there exists a biunique correspondence $\Phi : \mathcal{F}_{g,p} \to \mathcal{G}$ such that for every algebra $A \in \mathcal{F}_{g,p}$, the algebras A and $\Phi(A)$ have the same underlying set, and if $B \in \mathcal{F}_{g,p}$, then a mapping $\varphi : A \to B$ is an $\mathcal{F}_{g,p}$-homomorphism if and only if it is a $\mathcal{G}$-homomorphism.

Corollary 6.6. *The equational classes $\mathcal{F}_{g,p}$ and $\mathcal{G}$ are equivalent. The equivalence restricts to an equivalence between $\mathcal{F}_{g,m}$ and $\mathcal{G}_c$.*

7. Generalized modules

Let $(G,+)$ be a (possibly noncommutative) group. An endomorphism $\varphi \in \mathcal{E}nd(G,+)$ will be called *central* if $\varphi(G) \subseteq Z(G,+)$. We denote by $\mathcal{ZE}nd(G,+)$ the set of central endomorphisms of $(G,+)$. Clearly, the composition of central endomorphisms is again a central endomorphism and $\mathcal{ZE}nd(G,+)$ becomes a multiplicative semigroup under the operation of composition. Furthermore, if $\varphi \in \mathcal{ZE}nd(G,+)$ and $\psi \in \mathcal{E}nd(G,+)$ then $\varphi + \psi \in \mathcal{E}nd(G,+)$ where $(\varphi+\psi)(x) = \varphi(x) + \psi(x)$ for all $x \in G$. Consequently, $\mathcal{ZE}nd(G,+)$ becomes an abelian group under pointwise addition, and, altogether, $\mathcal{ZE}nd(G(+))$ becomes an associative ring (possibly without unity).

Let R be an associative ring (with or without unity). A *central generalized (left) R-module* will be a group $(G,+)$ equipped with an R-scalar multiplication $R \times G \to G$ such that $a(x+y) = ax+ay, (a+b)x = ax+bx, a(bx) = (ab)x$ and $ax \in Z(G,+)$ for all $a, b \in R$ and $x, y \in G$.

If G is a central generalized R-module, then define the *annihilator* of G to be $\mathrm{Ann}(G) = \{a \in R : aG = 0\}$. It is easy to see that $\mathrm{Ann}(G)$ is an ideal of the ring R.

Let $\mathbf{S} = \mathbb{Z}[\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}]$ denote the polynomial ring in four commuting indeterminates $\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}$ over the ring $\mathbf{Z}$ of integers. Put $\mathbf{R} = S\mathbf{x} + S\mathbf{y} + S\mathbf{u} + S\mathbf{v}$. That is, $\mathbf{R}$ is the ideal of $\mathbf{S}$ generated by the indeterminates. On the other hand, $\mathbf{R}$ is a commutative and associative ring (without unity) freely generated by the indeterminates.

Let $\mathcal{M}$ be the equational class (and category) of central generalized $\mathbf{R}$-modules G such that $\mathbf{x}+\mathbf{u}+\mathbf{xu} \in \mathrm{Ann}(G)$ and $\mathbf{y}+\mathbf{v}+\mathbf{yv} \in \mathrm{Ann}(G)$. Further, let $\mathcal{M}_p$ be the equational class of pointed () objects from $\mathcal{M}$. That is, $\mathcal{M}_p$ consists of ordered pairs (G, e) where $G \in \mathcal{M}$ and $e \in G$. Let $\mathcal{M}_c$ denote the subclass of centrally pointed objects from $\mathcal{M}_p$, *i.e.*, $(G, e) \in \mathcal{M}_c$ iff $(G, e) \in \mathcal{M}_p$ and $e \in Z(G, +)$.

Theorem 7.1. *The equational classes $\mathcal{F}_{g,p}$ and $\mathcal{M}_p$ are equivalent. This equivalence restricts to an equivalence between $\mathcal{F}_{g,m}$ and $\mathcal{M}_c$*

Proof. Firstly, take $(Q, a) \in \mathcal{F}_{g,p}$. Let $(Q, +, f, g, e)$ be the arithmetic form of the FG-quasigroup Q, such that $a = 0$ in $(Q, +)$. Define mappings $\varphi, \mu, \psi, \nu : Q \to Q$ by $\varphi(x) = -x + f(x)$, $\mu(x) = -x + f^{-1}(x)$, $\psi(x) = -x + g(x)$ and $\nu(x) = -x + g^{-1}(x)$ for all $x \in Q$. It is straightforward to check that φ, μ, ψ, ν are central endomorphisms of $(Q, +)$, that they commute pairwise, and that $\varphi(x) + \mu(x) + \varphi\mu(x) = 0$ and $\psi(x) + \nu(x) + \psi\nu(x) = 0$ for all $x \in Q$. Consequently, these endomorphisms generate a commutative subring of the ring $\mathcal{ZE}nd(Q, +)$, and there exists a (uniquely determined) homomorphism $\lambda : \mathbf{R} \to \mathcal{ZE}nd(Q, +)$ such that $\lambda(\mathbf{x}) = \varphi$, $\lambda(\mathbf{y}) = \psi$, $\lambda(\mathbf{u}) = \mu$, and $\lambda(\mathbf{v}) = \nu$. The homomorphism λ induces an $\mathbf{R}$-scalar multiplication on the group $(Q, +)$ and the resulting central generalized $\mathbf{R}$-module will be denoted by $\bar{Q}$. We have $\lambda(\mathbf{x}+\mathbf{u}+\mathbf{xu}) = 0 = \lambda(\mathbf{y}+\mathbf{v}+\mathbf{yv})$ and so $\bar{Q} \in \mathcal{M}$. Now define $\rho : \mathcal{F}_{g,p} \to \mathcal{M}_p$ by $\rho(Q, a) = (\bar{Q}, e)$, and observe that $(\bar{Q}, e) \in \mathcal{M}_c$ if and only if $e \in Z(Q, +)$.

Next, take $(\bar{Q}, e) \in \mathcal{M}_p$ and define $f, g : Q \to Q$ by $f(x) = x + \mathbf{x}x$ and $g(x) = x+\mathbf{y}x$ for all $x \in Q$. We have $f(x+y) = x+y+\mathbf{x}x+\mathbf{x}y = x+\mathbf{x}x+y+\mathbf{x}y = f(x)+f(y)$ for all $x, y \in Q$, and so $f \in \mathcal{E}nd(Q, +)$. Similarly, $g \in \mathcal{E}nd(Q, +)$. Moreover, $fg(x) = f(x + \mathbf{y}x) = x + \mathbf{y}x + \mathbf{x}x + \mathbf{xy}x = x + \mathbf{x}x + \mathbf{y}x + \mathbf{yx}x = gf(x)$, and therefore $fg = gf$. Still further, if we define $k : Q \to Q$ by $k(x) = x + \mathbf{u}x$ for $x \in Q$, then $fk(x) = x + (\mathbf{x}+\mathbf{u}+\mathbf{xu})x = x = kf(x)$, and it follows that $k = f^{-1}$ and so $f \in \mathcal{A}ut(Q, +)$. Similarly, $g \in \mathcal{A}ut(Q, +)$. Of course, $-x + f(x) = \mathbf{x}x \in Z(Q, +)$ and $-x + g(x) \in Z(Q, +)$. Consequently, Q becomes an FG-quasigroup under the multiplication $xy = f(x) + e + g(y)$. Define $\sigma : \mathcal{M}_p \to \mathcal{F}_{g,p}$ by $\sigma(\bar{Q}, e) = (Q, 0)$. Using Theorem 6.4 and Lemma 6.5, it is easy to check that the operators ρ and σ represent an equivalence between $\mathcal{F}_{g,p}$ and $\mathcal{M}_p$. Further, $0 \in M(Q)$ if and only if $e \in Z(Q, +)$, so that the equivalence restricts to $\mathcal{F}_{g,m}$ and $\mathcal{M}_c$. □

References

[1] V. D. Belousov and I. A. Flora, On left-distributive quasigroups, *Bul. Akad. Štiince RSS Moldoven* **1965** 1965 no. 7, 3–13.
[2] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.
[3] I. A. Golovko, F-quasigroups with idempotent elements, *Mat. Issled.* **4** 1969 vyp. 2 (12), 137–143.

[4] T. Kepka, F-quasigroups isotopic to Moufang loops, *Czechoslovak Math. J.* **29(104)** (1979), no. 1, 62–83.
[5] T. Kepka, M. K. Kinyon, J. D. Phillips, The structure of F-quasigroups, `math.GR/0510298`.
[6] T. Kepka, M. K. Kinyon, J. D. Phillips, F-quasigroups and generalized modules, `math.GR/0512244`.
[7] D. C. Murdoch, Quasi-groups which satisfy certain generalized associative laws, *Amer. J. Math.* **61** (1939), 509–522.
[8] H. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Helderman-Verlag, 1990.
[9] L. L. Sabinina, On the theory of F-quasigroups, in *Webs and quasigroups*, 127–130, Kalinin. Gos. Univ., Kalinin, 1988.

Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic
E-mail address: `kepka@karlin.mff.cuni.cz`

Department of Mathematical Sciences, Indiana University South Bend, South Bend, IN 46634 USA
E-mail address: `mkinyon@iusb.edu`
URL: `http://mypage.iusb.edu/~mkinyon`

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933 USA
E-mail address: `phillipj@wabash.edu`
URL: `http://www.wabash.edu/depart/math/faculty.html#Phillips`