****
BANACH CENTER PUBLICATIONS, VOLUME **
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 202*

MOUFANG PERMUTATIONS OVER SMALL ABELIAN GROUPS

DYLENE AGDA SOUZA DE BARROS

Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia-MG, Brazil
ORCID: 0000-0001-9300-5182 E-mail: dylene@ufu.br

PETR VOJTĚCHOVSKÝ

Dept. of Mathematics, University of Denver, 2390 S. York St., Denver, CO 80208, USA
ORCID: 0000-0003-3085-6611 E-mail: petr@math.du.edu

Abstract. Moufang permutations are certain permutations on an abelian group X that differ from an automorphism of X by a symmetric alternating biadditive mapping. It is known that every finite split abelian-by-cyclic 3-divisible Moufang loop is obtained from a Moufang permutation of the abelian normal subgroup. In this paper we investigate Moufang permutations for small abelian groups. We prove that a finite abelian group X possesses non-automorphic Moufang permutations if and only if the 2-primary component of X is of order more than four and is not cyclic. The automorphism group of X acts by conjugation on the set of Moufang permutations of X and the orbits of this action provide a partial answer to the corresponding isomorphism problem. We explicitly find all Moufang permutations for small abelian groups, including small elementary abelian 2-groups.

1. Introduction. A *loop* is a nonempty set Q with a binary operation $\cdot$ and a neutral element $1 \in Q$ such that for every $a, b \in Q$ the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$, respectively. Given a loop Q, we say that a subset $H \subseteq Q$ is a *subgroup* of Q if H is an associative subloop of Q.

A loop Q is a *Moufang loop* if $((xz)x)y = x(z(xy))$ holds for every $x, y, z \in Q$. By Moufang's Theorem [7], if three elements of a Moufang loop Q associate (in some order) then they generate a subgroup of Q. In particular, Moufang loops are diassociative, that is, any two elements generate a subgroup.

In [2], the authors started a systematic study of *abelian-by-cyclic* Moufang loops, that is, Moufang loops Q with an abelian normal subgroup X such that $C = Q/X$ is cyclic.

2020 *Mathematics Subject Classification*: 20N02.
Key words and phrases: Abelian-by-cyclic Moufang loop, semidirect product, Moufang permutation.
The paper is in final form and no version of it will be published elsewhere.

A systematic survey of related literature can be found in the introduction of [2]. Here we wish to highlight at least the papers [1, 3, 5, 6].

The following concept is key for the study of abelian-by-cyclic Moufang loops.

DEFINITION 1.1 (Definition 1.2,[2]). Let $(X,+)$ be an abelian group. A permutation f on X is a *Moufang permutation* on $(X,+)$ if the mapping $\beta : X \times X \to X$ defined by

$$\beta(x,y) = f^{-1}(f(x)+f(y)) - x - y \tag{1}$$

is (symmetric) alternating and biadditive,

$$\beta(\beta(x,y),z) = 0 \tag{2}$$

holds for all all $x,y,z \in X$, and

$$\beta(f(x),f(y)) = f(\beta(f^3(x),y)) \tag{3}$$

holds for all $x,y \in X$.

When f is a Moufang permutation and β is defined by (1), we call β the biadditive mapping *associated* with f and the tuple (f,β) a *Moufang pair*. We denote by $\mathrm{Mfp}(X,+)$ the set of all Moufang permutations on $(X,+)$.

Note that condition (2) is equivalent to the fact that the image of the symmetric alternating biadditive mapping β is contained in the radical

$$\mathrm{Rad}(\beta) = \{x \in X : \beta(x,y) = 0 \text{ for all } y \in X\}$$

of β. Also note that $\mathrm{Rad}(\beta)$ is a subgroup of $(X,+)$.

Denote by $\mathrm{Aut}(X,+)$ the automorphism group of $(X,+)$. One can easily see from Definition 1.1 that every $f \in \mathrm{Aut}(X,+)$ is a Moufang permutation on $(X,+)$ (with zero associated biadditive mapping) and thus $\mathrm{Aut}(X,+) \subseteq \mathrm{Mfp}(X,+)$. We call a Moufang permutation on $(X,+)$ *proper* if it is not an automorphism of $(X,+)$. Here is a characterization of improper Moufang permutations:

LEMMA 1.2. *Let (f,β) be a Moufang pair on the abelian group $(X,+)$. The following conditions are equivalent:*

(i) $f \in \mathrm{Aut}(X,+)$,
(ii) $\mathrm{Img}(\beta) = 0$,
(iii) $\mathrm{Rad}(\beta) = X$.

Proof. If $f \in \mathrm{Aut}(X,+)$ then $\beta(x,y) = f^{-1}(f(x)+f(y)) - x - y = 0$ for all $x,y \in X$ and hence $\mathrm{Img}(\beta) = 0$. If $\mathrm{Img}(\beta) = 0$ then certainly $\mathrm{Rad}(\beta) = X$. Finally, if $\mathrm{Rad}(\beta) = X$ then $0 = \beta(x,y) = f^{-1}(f(x)+f(y)) - x - y$ for all $x,y \in X$ and hence $f \in \mathrm{Aut}(X,+)$. ∎

In Section 2 we characterize all finite abelian groups that possess proper Moufang permutations.

The connections between Moufang permutations and abelian-by-cyclic Moufang loops are as follows (see [2] for more details).

Let X be an abelian normal subgroup of a Moufang loop $(Q,\cdot)$ and let us denote the operation $(X,\cdot)$ also by $(X,+)$. For $a \in Q$, let f be the restriction of the "conjugation" $x \mapsto a^{-1}xa$ to X. Then f is a Moufang permutation on $(X,+)$.

For $i, j \in \mathbb{Z}$ let

$$I(i,j) = \begin{cases} \emptyset, & \text{if } i = j, \\ \{i, i+1, \ldots, j-1\}, & \text{if } i < j, \\ \{j, j+1, \ldots, i-1\}, & \text{if } j < i. \end{cases}$$

If $(X,+)$ is an abelian group, (f,β) a Moufang pair on $(X,+)$ and $C = \langle b \rangle$ a cyclic group, then the formula

$$(b^i, x) \cdot (b^j, y) = \Big(b^{i+j}, f^{-3j}(x) + y + \sum_{k \in I(i+j,-j)} f^{-3k}(\beta(x,y)) \Big) \tag{4}$$

correctly defines a multiplication on $C \times X$ if and only if

$$\begin{array}{l} \text{either } C \text{ is infinite,} \\ \text{or } C \text{ is finite, } |f^3| \text{ divides } |C| \text{ and } \sum_{0 \le k < |C|} f^{3k}(x) \in \mathrm{Rad}(\beta) \text{ for all } x \in X. \end{array} \tag{5}$$

(The last part of condition (5) holds for instance when C is finite, $|f^3|$ divides $|C|$ and $\mathrm{Rad}(\beta)$ has no elements of order 3.) In that case the resulting groupoid is in fact a Moufang loop, denoted by

$$Q = C \ltimes_{(f^3,\beta)} X \quad \text{or} \quad Q = C \ltimes_f X$$

that contains the normal abelian subgroup $1 \times X$ such that $Q/(1 \times X)$ is isomorphic to C.

All abelian-by-cyclic Moufang loops $Q = CX$ in which both C and X are 3-divisible are homomorphic images of the loops $C \ltimes_{(f^3,\beta)} X$. If Q is also split, it is isomorphic to $C \ltimes_{(f^3,\beta)} X$ for a suitable Moufang permutation f of $(X,+)$.

In Section 3 we construct all Moufang permutations on small abelian groups $(X,+)$. We show that if two Moufang permutations on $(X,+)$ are conjugate by an automorphism of $(X,+)$ and if C is fixed, then the corresponding Moufang loops are isomorphic. It therefore suffices to consider Moufang permutations $\mathrm{Mfp}(X,+)$ up to the conjugation action of the group $\mathrm{Aut}(X,+)$.

It is rather difficult to calculate the sets $\mathrm{Mfp}(X,+)$ even for small abelian groups $(X,+)$. Let V be a vector space over the two-element field. In Section 4 we develop a mini-theory of symmetric alternating biadditive mappings $\beta : V \times V \to V$ satisfying $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$ in order to push the calculation of Moufang permutations little bit further in the case of elementary abelian 2-groups.

2. Groups with proper Moufang permutations. Our goal here is to characterize all finite abelian groups $(X,+)$ with proper Moufang permutations. Throughout this section, let $(X,+)$ be an abelian group and C_n a cyclic group of order n.

We note in passing that $\mathrm{Mfp}(X,+)$ does not have to be a subgroup of the symmetric group on X. For instance, there are two Moufang permutations on $X = C_2^4$ whose product is not a Moufang permutation on X.

We start by recalling the following result of [2]:

LEMMA 2.1 (Lemma 9.1,[2]). *Let $(X,+)$ be an abelian group, (f,β) a Moufang pair on $(X,+)$ and i an integer. Then:*

(i) $f(0) = 0$, $f(2x) = 2f(x)$ *and* $f(-x) = -f(x)$ *for all* $x \in X$,
(ii) $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$, $2X \subseteq \mathrm{Rad}(\beta)$ *and* $2\mathrm{Img}(\beta) = 0$,
(iii) f^i *permutes both* $\mathrm{Rad}(\beta)$ *and* $\mathrm{Img}(\beta)$,
(iv) $f^i(x+y) = f^i(x) + f^i(y)$ *whenever* $\{x, y\} \cap \mathrm{Rad}(\beta) \neq \emptyset$,
(v) f^i *restricts to an automorphism of* $\mathrm{Rad}(\beta)$.

Corollary 2.2. *Let* $(X, +)$ *be an abelian group of odd order. Then every Moufang permutation on* X *is an automorphism of* X.

Proof. Let f be a Moufang permutation on X. Since X has odd order, the mapping $x \mapsto 2x$ is a bijection of X. Hence $X = 2X \subseteq \mathrm{Rad}(\beta)$ by Lemma 2.1. Then $f \in \mathrm{Aut}(X, +)$ by Lemma 1.2. ∎

Lemma 2.3. *Let* (f, β) *be a Moufang pair on a nontrivial abelian group* $(X, +)$. *Then* $\mathrm{Rad}(\beta) \neq 0$.

Proof. If $\mathrm{Rad}(\beta) = 0$ then $\mathrm{Img}(\beta) = 0$ since $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$ by Lemma 2.1. Then $X = \mathrm{Rad}(\beta) = 0$ by Lemma 1.2, a contradiction. ∎

Given a subgroup H of a group G, let $[G : H]$ be the index of H in G.

Lemma 2.4. *Let* (f, β) *be a Moufang pair on* $(X, +)$ *with* $[X : \mathrm{Rad}(\beta)] \leq 2$. *Then* $\mathrm{Rad}(\beta) = X$ *and* $f \in \mathrm{Aut}(X, +)$.

Proof. Set $R = \mathrm{Rad}(\beta)$. If $[X : R] = 1$ then $X = R$ and, by Lemma 1.2, $f \in \mathrm{Aut}(X, +)$. If $[X : R] = 2$ then $X = R \cup (a + R)$ for some $a \in X \backslash R$. Let $x, y \in X$. If $\{x, y\} \cap R \neq \emptyset$, Lemma 2.1 implies that $f(x + y) = f(x) + f(y)$. Suppose that both x and y are in the coset $a + R$ and write $x = a + x_1$ and $y = a + y_1$ for some $x_1, y_1 \in R$. By Lemma 2.1, we get $f(x + y) = f(2a + x_1 + y_1) = f(2a) + f(x_1 + y_1) = 2f(a) + f(x_1) + f(y_1) = (f(a) + f(x_1)) + (f(a) + f(y_1)) = f(a + x_1) + f(a + y_1) = f(x) + f(y)$, where in the second step we used $2X \subseteq \mathrm{Rad}(\beta)$. Therefore $f \in \mathrm{Aut}(X, +)$. ∎

Lemma 2.5. *Let* $(X, +)$, $(Y, +)$ *be abelian groups,* (f, β_f) *a Moufang pair on* $(X, +)$ *and* (g, β_g) *a Moufang pair on* $(Y, +)$. *Define* $h : X \times Y \to X \times Y$ *by* $h(x, y) = (f(x), g(y))$. *Then* h *is a Moufang permutation on* $X \times Y$ *and the associated biadditive mapping* β_h *satisfies* $\beta_h((x_1, y_1), (x_2, y_2)) = (\beta_f(x_1, x_2), \beta_g(y_1, y_2))$ *for all* $x_i \in X$, $y_i \in Y$. *Moreover,* $h \in \mathrm{Aut}(X \times Y)$ *if and only if* $f \in \mathrm{Aut}(X)$ *and* $g \in \mathrm{Aut}(Y)$.

Proof. This is straightforward but here are the details. Clearly, h is a permutation of $X \times Y$ with $h^{-1}(x, y) = (f^{-1}(x), g^{-1}(y))$. Now,

$$\begin{aligned}
\beta_h((x_1, y_1), (x_2, y_2)) &= h^{-1}(h(x_1, y_1) + h(x_2, y_2)) - (x_1 + x_2, y_1 + y_2) \\
&= h^{-1}((f(x_1), g(y_1)) + (f(x_2), g(y_2))) - (x_1 + x_2, y_1 + y_2) \\
&= h^{-1}((f(x_1) + f(x_2), g(y_1) + g(y_2))) - (x_1 + x_2, y_1 + y_2) \\
&= (f^{-1}(f(x_1) + f(x_2)) - (x_1 + x_2), g^{-1}(g(y_1) + g(y_2)) - (y_1 + y_2)) \\
&= (\beta_f(x_1, x_2), \beta_g(y_1, y_2)),
\end{aligned}$$

and then it is straightforward to check that β_h is alternating and biadditive. For all $x_i \in X$ and $y_i \in Y$, $\beta_h(\beta_h((x_1, y_1), (x_2, y_2)), (x_3, y_3)) = \beta_h((\beta_f(x_1, x_2), \beta_g(y_1, y_2)), (x_3, y_3)) =$

$(\beta_f(\beta_f(x_1,x_2),x_3),\beta_g(\beta_g(y_1,y_2),y_3))=(0,0)$, so (2) holds for β_h. Finally,

$$\begin{aligned}\beta_h(h(x_1,y_1),h(x_2,y_2)) &= \beta_h((f(x_1),g(y_1)),(f(x_2),g(y_2)))\\ &= (\beta_f(f(x_1),f(x_2)),\beta_g(g(y_1),g(y_2)))\\ &= (f(\beta_f(f^3(x_1),x_2)),g(\beta_g(g^3(y_1),y_2)))\\ &= h(\beta_f(f^3(x_1),x_2),\beta_g(g^3(y_1),y_2))\\ &= h(\beta_h((f^3(x_1),g^3(y_1)),(x_2,y_2)))\\ &= h(\beta_h(h^3(x_1,y_1),(x_2,y_2))),\end{aligned}$$

so (3) holds for β_h. Therefore (h,β_h) is a Moufang pair on $X\times Y$. The last assertion is clear. ∎

Denote the order of an element $x\in(X,+)$ by $|x|$. In the finite case, for a prime p, let $X_p=\{x\in X : |x|=p^k \text{ for some } k\}$ be the p-primary component of X, and note that $X=\bigoplus_p X_p$ and $\mathrm{Aut}(X)\cong\bigoplus_p \mathrm{Aut}(X_p)$.

LEMMA 2.6. *If (f,β) is a Moufang pair on a finite abelian group $(X,+)$ then $|f(x)|=|x|$ for every $x\in X$.*

Proof. Set $X=X_2\oplus Y$, where $Y=\bigoplus_{p>2}X_p$. As Y has odd order, $Y=2Y\subseteq 2X\subseteq \mathrm{Rad}(\beta)$ by Lemma 2.1. Since f restricts to an automorphism of $\mathrm{Rad}(\beta)$, we conclude that $|f(y)|=|y|$, for every $y\in Y$. This implies that $f(Y)=Y$. If $x\in X_2$ then $|x|=2^k$ for some k. By Lemma 2.1, we have $0=f(2^kx)=2^kf(x)$ and thus $|f(x)|=2^j$ for some $j\le k$. On the other hand, $0=2^jf(x)=f(2^jx)$ and then $2^jx=0$, which implies $k\le j$ and $|f(x)|=|x|$. In particular, $f(X_2)=X_2$. Now, for every $z\in X$ there are unique elements $x\in X_2$ and $y\in Y$ such that $z=x+y$. In addition, if $|x|=2^k$ and $|y|=n$ (with n odd) then $|z|=2^kn$. Since $Y\subseteq\mathrm{Rad}(\beta)$, we get $f(z)=f(x+y)=f(x)+f(y)$ with $|f(x)|=|x|=2^k$ and $|f(y)|=|y|=n$. Therefore $|f(z)|=2^kn=|z|$. ∎

PROPOSITION 2.7. *Let (f,β) be a Moufang pair on a finite abelian group $(X,+)$. Then f restricts to a Moufang permutation on X_2 and to an automorphism of $Y=\bigoplus_{p>2}X_p$. In particular, f decomposes into a sum of a Moufang permutation of X_2 and an automorphism of Y.*

Proof. It follows from Lemma 2.6 that $f(X_2)=X_2$ and $f(Y)=Y$. Since X_2 and Y are subgroups of X, it is straightforward to see that f restricts to a Moufang permutation on these subgroups. As Y has odd order, f restricts to an automorphism of Y by Corollary 2.2. Also, for every $z\in X$, $z=x+y$ for some unique $x\in X_2$ and $y\in Y$. Since $Y\subseteq\mathrm{Rad}(\beta)$, $f(z)=f(x)+f(y)$, and the proof is complete. ∎

We now prove that if $(X,+)$ is a (not necessarily finite) cyclic group, then every Moufang permutation on X is an automorphism of X.

PROPOSITION 2.8. *Let $(X,+)$ be a cyclic group and let (f,β) be a Moufang pair on $(X,+)$. Then f is an automorphism of $(X,+)$.*

Proof. First, suppose that $|X|$ is finite. If X has odd order, then the result follows from Corollary 2.2. Let us suppose that X is a cyclic group of order 2^mn, where $m\ge 1$ and n is odd. Let a and b be elements of X with $|a|=2^m$ and $|b|=n$. Since b has odd

order, $b \in 2X$, and we obtain the cyclic subgroup $D = \langle 2a, b\rangle \subseteq 2X \subseteq \mathrm{Rad}(\beta)$ satisfying $2 = [X : D] \geq [X : \mathrm{Rad}(\beta)]$. By Lemma 2.4, $f \in \mathrm{Aut}(X, +)$.

Now let $X = \mathbb{Z}$. We again have $2\mathbb{Z} \subseteq \mathrm{Rad}(\beta)$, $2 = [\mathbb{Z} : 2\mathbb{Z}] \geq [\mathbb{Z} : \mathrm{Rad}(\beta)]$, and therefore $f \in \mathrm{Aut}(\mathbb{Z}, +)$ by Lemma 2.4. ∎

Example 2.9. Let $X = C_2 \times C_2$. We have $\mathrm{Aut}(X) \cong S_3$. If $f \in \mathrm{Mfp}(X)$ then $f(0) = 0$ by Lemma 2.1. Hence $|\mathrm{Mfp}(X)| \leq 6$, $\mathrm{Mfp}(X) = \mathrm{Aut}(X)$, and there are no proper Moufang permutations on X.

Next we present a general construction of proper Moufang permutations.

Proposition 2.10. *Let $(Z, +)$ be an abelian group and let $h \in \mathrm{Aut}(Z, +)$ be such that $|h| = 2$ and $h(2x) = 2x$ for all $x \in Z$. Let $(A, +)$ be an abelian group with a subgroup S of index 2. Let $X = A \times Z$. Then $f : X \to X$ defined by*

$$f(a, x) = \begin{cases} (a, x), & \text{if } a \in S, \\ (a, h(x)), & \text{otherwise,} \end{cases}$$

is a proper Moufang permutation of X and $|f| = 2$.

Proof. It is easy to see that f is a permutation of X. If $a \in S$, we have $f^{-1}(a, x) = (a, x)$. If $a \in A \setminus S$, we have $f^{-1}(a, x) = (a, h^{-1}(x)) = (a, h(x))$. Hence $f^{-1} = f$ and $|f| = 2$ follows from $h \neq 1$.

For all $(a, x), (b, y) \in X$, we have $\beta((a, x), (b, y)) = f^{-1}(f(a, x)+f(b, y))-(a+b, x+y)$. Since X is an abelian group, β is symmetric.

If $a, b \in S$ then, since $a + b \in S$,

$$\begin{aligned} \beta((a, x), (b, y)) &= f^{-1}(f(a, x) + f(b, y)) - (a + b, x + y) \\ &= f^{-1}((a, x) + (b, y)) - (a + b, x + y) \\ &= f^{-1}(a + b, x + y) - (a + b, x + y) \\ &= (a + b, x + y) - (a + b, x + y) \\ &= (0, 0). \end{aligned}$$

If $a \in S$ and $b \notin S$ then, since $a + b \notin S$ and $h^2 = 1$,

$$\begin{aligned} \beta((a, x), (b, y)) &= f^{-1}(f(a, x) + f(b, y)) - (a + b, x + y) \\ &= f^{-1}((a, x) + (b, h(y))) - (a + b, x + y) \\ &= f^{-1}(a + b, x + h(y)) - (a + b, x + y) \\ &= (a + b, h(x + h(y))) - (a + b, x + y) \\ &= (0, h(x) - x). \end{aligned}$$

If $a, b \notin S$ then, since $a + b \in S$,

$$\begin{aligned} \beta((a, x), (b, y)) &= f^{-1}(f(a, x) + f(b, y)) - (a + b, x + y) \\ &= f^{-1}((a, h(x)) + (b, h(y))) - (a + b, x + y) \\ &= f^{-1}(a + b, h(x + y)) - (a + b, x + y) \\ &= (a + b, h(x + y)) - (a + b, x + y) \\ &= (0, h(x + y) - (x + y)). \end{aligned}$$

To show that β is alternating, note that if $a \in S$ then $\beta((a,x),(a,x)) = (0,0)$, and if $a \notin S$ then $\beta((a,x),(a,x)) = (0, h(2x) - 2x) = (0, 2x - 2x) = (0,0)$.

For biadditivity, consider $\beta((a,x)+(b,y),(c,z)) = \beta((a+b,x+y),(c,z)) = (0,\ell)$ and $\beta((a,x),(c,z)) + \beta((b,y),(c,z)) = (0,r)$. If $a,b,c \in S$ then $\ell = 0$ and $r = 0+0$. If $a,b \in S$ and $c \notin S$ then $\ell = h(x+y) - (x+y)$ and $r = h(x) - x + h(y) - y$. If $a \in S$, $b \notin S$ and $c \in S$ then $\ell = h(z) - z$ and $r = 0 + h(z) - z$. If $a \in S$ and $b,c \notin S$ then $\ell = h(x+y+z) - (x+y+z)$ and $r = h(x) - x + h(y+z) - (y+z)$. If $a,b \notin S$ and $c \in S$ then $\ell = 0$ and $r = h(z) - z + h(z) - z = 2h(z) - 2z = h(2z) - 2z = 2z - 2z = 0$. Finally, if $a,b,c \notin S$ then $\ell = h(x+y) - (x+y)$ and $r = h(x+z) - (x+z) + h(y+z) - (y+z) = h(x+y) - (x+y) + 2h(z) - 2z = h(x+y) - (x+y)$. Hence β is biadditive.

For (2), observe that we always have $\beta((a,x),(b,y)) = (0, h(u) - u)$ for some $u \in A$. If $c \in S$ then $\beta(\beta((a,x),(b,y)),(c,z)) = \beta((0,h(u)-u),(c,z)) = (0,0)$. If $c \notin S$, then $\beta(\beta((a,x),(b,y)),(c,z)) = \beta((0,h(u)-u),(c,z)) = (0, h(h(u)-u) - (h(u)-u)) = (0, 2u - 2h(u)) = (0,0)$. Hence (2) holds for β.

For (3), we need to check $f(\beta(f^3(a,x),(b,y))) = \beta(f(a,x),f(b,y))$. Since $|f| = 2$, we have $f^3 = f$. Also, $\mathrm{Img}(\beta) \subseteq 0 \times X$ and $f(0,x) = (0,x)$, so all we need to check is $\beta(f(a,x),(b,y)) = \beta(f(a,x),f(b,y))$. By biadditivity, it is clear that this is the same as $\beta(f(a,x), f(b,y) - (b,y)) = (0,0)$. But $f(b,y) - (b,y)$ either vanishes or it is equal to $(0, h(y) - y)$. We already showed above that $\beta((c,z),(0,h(y)-y)) = (0,0)$.

Hence (f,β) is a Moufang pair on $(X,+)$. Since $\mathrm{Img}(\beta) \neq 0$, f is not an automorphism of $(X,+)$, by Lemma 1.2. ∎

COROLLARY 2.11. *Let $(X,+)$ be a noncyclic abelian 2-group. Then there exist a proper Moufang permutation on X if and only if $|X| \geq 2^3$.*

Proof. The only noncyclic abelian 2-group of order less than 8 is $C_2 \times C_2$, which has no proper Moufang permutations by Example 2.9. Suppose that $|X| \geq 2^3$. We will use Proposition (2.10). Note that any nontrivial abelian 2-group contains a subgroup of index 2.

Suppose that X is elementary abelian, say $X = A \times C_2^2$. Then the mapping h that flips the two coordinates of C_2^2 clearly satisfies all the assumptions of Proposition 2.10.

Suppose that X is not elementary abelian, say $X = A \times C_{2m}$ for some positive even integer m. We claim that the mapping $h : C_{2m} \to C_{2m}$ defined by $h(x) = (m+1)x$ satisfies all assumptions of Proposition 2.10. Since $\gcd(m+1, 2m) = 1$, it is an automorphism of C_{2m}. Since $h(1) = m+1 \neq 1$, it is nontrivial. We have $h^2(x) = (m+1)^2 x = (m^2 + 2m + 1)x = x$ because m^2 is divisible by $2m$ (as $m > 0$ is even). Finally, $h(2x) = (m+1)(2x) = 2mx + 2x = 2x$. ∎

THEOREM 2.12. *Let $(X,+)$ be a finite abelian group and let X_2 be the 2-primary component of X. Then $\mathrm{Mfp}(X) = \mathrm{Aut}(X)$ if and only if either X_2 is cyclic or $X_2 = C_2 \times C_2$.*

Proof. Suppose that f is a Moufang permutation on X. By Proposition 2.7, f decomposes into a sum of a Moufang permutation on X_2 and an automorphism of $Y = \bigoplus_{p>2} X_p$. Conversely, Lemma 2.5 shows how to build a Moufang permutation of X from Moufang permutations of X_2 and Y. In view of Corollary 2.2, it remains to discuss the case of abelian 2-groups.

If $X = X_2$ is cyclic or $X = C_2 \times C_2$ then every Moufang permutation on X is an automorphism of X, by Proposition 2.8 and Example 2.9. If X is not cyclic and $|X_2| \geq 2^3$, Corollary 2.11 furnishes a proper Moufang permutation on X. ∎

3. Moufang permutations up to conjugation and the corresponding Moufang loops. It seems to be a difficult problem to calculate $\mathrm{Mfp}(X, +)$ even for small abelian groups. A naive approach is to consider all permutations of X and check each one against Definition 1.1. (Since $\mathrm{Mfp}(X, +)$ is not a subgroup under composition, it does not suffice to find generators.)

A better approach is to take advantage of some of the properties of Moufang permutations established in Lemma 2.1, such as $f(0) = 0$, $f(2x) = 2f(x)$ and $f(-x) = -f(x)$. It therefore suffices to consider (minimal) subsets S of $(X, +)$ from which $(X, +)$ is obtained by iterated applications of the operations $x \mapsto 2x$ and $x \mapsto -x$. This works well for some groups (such as groups containing elements of large odd orders) but fails completely for other groups (such as elementary abelian 2-groups, where one has to take $S = X$).

Given a Moufang permutation $f \in \mathrm{Mfp}(X, +)$ and a cyclic group C of order coprime to 3 such that $|f^3|$ divides $|C|$, the multiplication formula (4) yields the abelian-by-cyclic Moufang loop $C \ltimes_f X$. As usual, from the point of view of the isomorphism types of the resulting Moufang loops, it suffices to consider Moufang permutations up to conjugation by $\mathrm{Aut}(X)$. Here are the details:

LEMMA 3.1. *Let (f, β) be a Moufang pair on the abelian group $(X, +)$. Let g be an automorphism of X. Then $f^g = g^{-1}fg$ is a Moufang permutation on X with associated biadditive mapping given by $\beta^g(x, y) = g^{-1}\beta(g(x), g(y))$. Moreover,* $\mathrm{Rad}(\beta^g) = g^{-1}(\mathrm{Rad}(\beta))$.

Proof. We have

$$\begin{aligned}\beta^g(x, y) &= (f^g)^{-1}(f^g(x) + f^g(y)) - (x + y)\\ &= g^{-1}f^{-1}g(g^{-1}fg(x) + g^{-1}fg(y)) - (x + y)\\ &= g^{-1}f^{-1}(fg(x) + fg(y)) - (x + y)\\ &= g^{-1}[f^{-1}(fg(x) + fg(y)) - (g(x) + g(y))] = g^{-1}\beta(g(x), g(y)).\end{aligned}$$

Since $g \in \mathrm{Aut}(X)$ and β is symmetric, alternating and biadditive, we immediately see that β^g is also symmetric, alternating and biadditive.

Let us establish (2) for β^g. For x, y and $z \in X$,

$$\begin{aligned}\beta^g(\beta^g(x, y), z) &= \beta^g(g^{-1}\beta(g(x), g(y)), z)\\ &= g^{-1}\beta(g(g^{-1}\beta(g(x), g(y))), g(z))\\ &= g^{-1}\beta(\beta(g(x), g(y)), g(z)) = 0,\end{aligned}$$

where the last equality comes from the fact that β satisfies (2).

We now establish (3). On the one hand, we have

$$\begin{aligned}\beta^g(f^g(x),f^g(y)) &= g^{-1}\beta(g(f^g(x)),g(f^g(y)))\\ &= g^{-1}\beta(gg^{-1}fg(x),gg^{-1}fg(y))\\ &= g^{-1}\beta(fg(x),fg(y))\\ &= g^{-1}f\beta(f^3g(x),g(y)),\end{aligned}$$

where the last equality follows by (3) for (f,β). On the other hand,

$$\begin{aligned}f^g\beta^g((f^g)^3(x),y) &= f^gg^{-1}\beta(g(f^g)^3(x),g(y))\\ &= f^gg^{-1}\beta(gg^{-1}f^3g(x),g(y))\\ &= g^{-1}fgg^{-1}\beta(f^3g(x),g(y))\\ &= g^{-1}f\beta(f^3g(x),g(y)).\end{aligned}$$

Hence (3) holds and (f^g,β^g) is a Moufang pair on $(X,+)$.

Finally, we have $x\in\mathrm{Rad}(\beta^g)$ if and only if $g^{-1}\beta(g(x),g(y))=0$ for every $y\in X$, which is equivalent to $\beta(g(x),z)=0$ for every $z\in X$. Therefore, $x\in\mathrm{Rad}(\beta^g)$ if and only if $g(x)\in\mathrm{Rad}(\beta)$. ∎

LEMMA 3.2. *Let $(X,+)$ be an abelian group, C a cyclic group, (f,β) a Moufang pair on $(X,+)$ and $g\in\mathrm{Aut}(X,+)$. Then (f,β) satisfies the condition* (5) *if and only if (f^g,β^g) satisfies the condition* (5).

Proof. It suffices to establish the direct implication. Suppose that (5) holds for (f,β). If C is infinite then (5) clearly holds for (f^g,β^g), too. Suppose that C is finite. Then f^3 divides $|C|$ and $\sum_{0\le k<|C|}f^{3k}(x)\in\mathrm{Rad}(\beta)$ for all $x\in X$. Since f^g has the same cycle structure as f, it has the same order as f and so $|(f^g)^3|$ divides $|C|$. By Lemma 3.1, we need to check that $\sum_{0\le k<|C|}(f^g)^{3k}(x)\in\mathrm{Rad}(\beta^g)=g^{-1}(\mathrm{Rad}(\beta))$ for all $x\in X$, which is the same as $g(\sum_{0\le k<|C|}g^{-1}f^{3k}g(x))\in\mathrm{Rad}(\beta)$ for all $x\in X$, that is, $\sum_{0\le k<|C|}f^{3k}g(x)\in\mathrm{Rad}(\beta)$ for all $x\in X$, which is true because g permutes X. ∎

PROPOSITION 3.3. *Let $(X,+)$ be an abelian group, let C be a cyclic group and let (f,β) be a Moufang pair on $(X,+)$ such that* (5) *holds. Let $g\in\mathrm{Aut}(X,+)$ and let (f^g,β^g) be the corresponding Moufang pair. Then (f^g,β^g) is a Moufang pair on $(X,+)$,* (5) *holds for (f^g,β^g), and the Moufang loops $C\ltimes_f X$ and $C\ltimes_{f^g}X$ are isomorphic.*

Proof. By Lemma 3.1, (f^g,β^g) is a Moufang pair on $(X,+)$. By Lemma 3.2, (5) holds for (f^g,β^g). Let $Q=C\ltimes_f X$ and $Q^g=C\ltimes_{f^g}X$. We shall prove that $\varphi:Q\to Q^g$, defined by $\varphi(b^i,x)=(b^i,g^{-1}(x))$ is an isomorphism. For every $(b^i,x),(b^j,y)\in Q$, we get

$$\begin{aligned}&\varphi(b^i,x)\varphi(b^j,y)=(b^i,g^{-1}(x))(b^j,g^{-1}(y))\\ &=(b^{i+j},g^{-1}f^{-3j}gg^{-1}(x)+g^{-1}(y)+\sum_{k\in I(i+j,-j)}g^{-1}f^{-3k}gg^{-1}\beta(gg^{-1}(x),gg^{-1}(y)))\\ &=(b^{i+j},g^{-1}(f^{-3j}(x)+y+\sum_{k\in I(i+j,-j)}f^{-3k}\beta(x,y)))=\varphi((b^i,x)(b^j,y))\end{aligned}$$

and hence φ is a homomorphism. The mapping is obviously onto and one-to-one. ∎

EXAMPLE 3.4. Let $X = C_2^3$. There are 252 Moufang permutations on X, including 168 Moufang permutations contained in $\mathrm{Aut}(X) \cong \mathrm{GL}_3(\mathbb{F}_2)$. Up to conjugation by $\mathrm{Aut}(X)$, there are 9 Moufang permutations $f_1, \ldots, f_9$, including 6 automorphisms of X. They have cycle structures 1^8, $1^6 2^1$, $1^4 2^2$, $1^2 2^3$, $1^2 2^1 4^1$, $1^2 3^2$, $1^2 6^1$, $1^1 7^1$ and (again) $1^1 7^1$, respectively. Since the multiplication formula (4) depends only on f^3, we clearly have $f_1^3 = f_6^3$ and we coincidentally also have $f_4^3 = f_7^3$, it suffices to keep $f_1, \ldots, f_5$, f_8 and f_9.

Let us construct all Moufang loops $C_2 \ltimes_f X$ up to isomorphism. In order to apply the multiplication formula (4), we can only consider $f \in \mathrm{Mfp}(X)$ such that $|f^3|$ divides $|C_2| = 2$. This eliminates f_5, f_8 and f_9, leaving $f_1, \ldots, f_4$. These four permutations happen to yield four pairwise nonisomorphic Moufang loops: the group C_2^4, the nonassociative Moufang loop `MoufangLoop(16,1)`, the group $C_2 \times D_8$, and `MoufangLoop(16,4)`, in this order. Here, `MoufangLoop(n,m)` denotes the mth Moufang loop of order n as cataloged in the `GAP` [4] package `LOOPS` [8].

REMARK 3.5. The converse of Proposition 3.3 does not hold. There are two Moufang permutations on $X = C_2 \times C_4$ (both of order 2, one is a transposition and the other is a product of three independent transpositions) that are not conjugate by an automorphism of X yet yield isomorphic Moufang loops with $C = C_2$.

$(X,+)$	m	2	4	8	10	14	16	20	22	26	28	32	34	38	40	44	46	50
$C_4 \times C_2$	3	3	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
C_2^3	3	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
$C_8 \times C_2$	6	4	3	2	4	4	2	3	4									
$C_4 \times C_2^2$	26	17	11	11	17	17	11	11	17									
$C_4 \times C_4$	10	7	3	3	7	7	3	3	7									
C_2^4	8	5	4	4	5	5	4	4	5									
$C_8 \times C_4$	38	28	21	16	28													
$C_{16} \times C_2$	12	4	7	6	4													
$C_4^2 \times C_2$	274	150	79	79	150													
$C_8 \times C_2^2$	52	36	27	22	36													
$C_4 \times C_2^3$	201	115	74	76	115													
$C_{20} \times C_2$	12	4	3	3	4													
$C_{10} \times C_2^2$	12	4	3	3	4													

Table 1. Proper Moufang permutations up to conjugation and the corresponding Moufang loops up to isomorphism.

In Table 1 we collect some computational results on Moufang permutations and the corresponding Moufang loops. In the first column we list some small abelian groups $(X,+)$. In the second column we give the number m of proper Moufang permutations on X up to the action of the automorphism group of X. In the remaining columns labeled by n, we give the number of isomorphism types of loops $C_n \ltimes_f X$, where X is the abelian group from column one and f is one of the Moufang permutations enumerated in column 2.

4. The elementary abelian case. In this section we have a look at Moufang permutations over small elementary abelian groups. In view of Theorem 2.12, the only case of interest are the groups $\mathbb{Z}_2^n$.

4.1. Symmetric alternating biadditive mappings up to equivalence. Let F be a field and $V = F^n = \langle e_1, \dots, e_n \rangle$ a vector space of dimension n over F. We start with some results concerning the classification of symmetric alternating biadditive mappings $\beta : V \times V \to V$ satisfying $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$ up to the action of $GL(V)$ given by

$$\beta^g(x, y) = g^{-1}\beta(gx, gy),$$

where $g \in GL(V)$ and $x, y \in V$. Recall that $\mathrm{Rad}(\beta^g) = g^{-1}(\mathrm{Rad}(\beta))$.

LEMMA 4.1. *Let F be a prime field, $V = F^n = \langle e_1, \dots, e_n \rangle$ and $R = \langle e_1, \dots, e_r \rangle$ for some $0 \le r \le n$. A mapping $\beta : V \times V \to V$ is symmetric, alternating, biadditive and satisfies $\mathrm{Img}(\beta) \subseteq R \subseteq \mathrm{Rad}(\beta)$ if and only if $\beta(e_i, e_j) = \beta(e_j, e_i) \in R$ for all $1 \le i, j \le n$, $\beta(e_i, e_i) = 0$ for all $1 \le i \le n$, $\beta(e_i, e_j) = 0$ for all $1 \le i \le r$, $1 \le j \le n$, and $\beta(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j) = \sum_{1 \le i,j \le n} x_i y_j \beta(e_i, e_j)$ for all $x_i, y_i \in F$.*

Proof. The direct implication is clear. For the converse implication, everything is clear except perhaps the alternating property. With $i \ne j$ we have $x_i x_j \beta(e_i, e_j) + x_j x_i \beta(e_j, e_i) = (x_i x_j + x_j x_i)\beta(e_i, e_j) = 0$ thanks to symmetry. Hence $\beta(\sum_i x_i e_i, \sum_j x_j e_j) = = \sum_{i,j} x_i x_j \beta(e_i, e_j) = \sum_{i<j}(x_i x_j \beta(e_i, e_j) + x_j x_i \beta(e_j, e_i)) + \sum_i x_i x_i \beta(e_i, e_i) = 0 + 0 = 0$. ∎

In the situation of Lemma 4.1 we say that $R = \langle e_1, \dots, e_r \rangle$ is the *designated image and radical* of β. It can of course happen that $\mathrm{Img}(\beta)$ is properly contained in R and/or $\mathrm{Rad}(\beta)$ properly contains R, depending on the values $\beta(e_i, e_j)$ with $i, j > r$.[1]

Let $\beta : V \times V \to V$ be a symmetric alternating mapping satisfying $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$. Let r be the dimension of $\mathrm{Rad}(\beta)$. Since $GL(V)$ acts transitively on r-dimensional subspaces of V, we can assume without loss of generality that $\mathrm{Rad}(\beta) = \langle e_1, \dots, e_r \rangle$. We must have $r > 0$, else $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta) = 0$ yields $\beta = 0$ and $\mathrm{Rad}(\beta) = V$, a contradiction. We must also have $r \ne n - 1$, else $\beta(e_n, e_i) = 0$ for all $1 \le i \le n - 1$ but also $\beta(e_n, e_n) = 0$ and so $e_n \in \mathrm{Rad}(\beta)$, a contradiction. Ignoring the zero mapping (with $r = n$), we can therefore assume that $r \in \{1, \dots, n - 2\}$ and $n \ge 3$.

Let now $F = \mathbb{F}_2$ be the two-element field.

Dimension $n = 3$. We can assume that $r = 1$, $\mathrm{Rad}(\beta) = \langle e_1 \rangle$ and $\mathrm{Img}(\beta) = \langle e_1 \rangle$. Hence β is determined on the basis by

	e_1	e_2	e_3
e_1	0	0	0
e_2	0	0	a
e_3	0	a	0

for some $0 \ne a \in \mathrm{Img}(\beta)$. Since $\mathrm{Img}(\beta) = \{0, e_1\}$, we have $a = e_1$, obtaining the mapping $\beta_{3,1}$ of Table 2.

[1] Our terminology is motivated by that of coding theory, where BCH codes with designated distance d are constructed so that their distance is guaranteed to be at least d but it might exceed d.

Dimension $n = 4$. We have $r \in \{1, 2\}$. Suppose that $r = 1$ and $\mathrm{Rad}(\beta) = \langle e_1 \rangle$, so again $\mathrm{Img}(\beta) = \langle e_1 \rangle$. Then β is determined by

	e_1	e_2	e_3	e_4
e_1	0	0	0	0
e_2	0	0	a	b
e_3	0	a	0	c
e_4	0	b	c	0

If $a = b = 0$ then $e_2 \in \mathrm{Rad}(\beta)$, a contradiction. Consider the element $g \in GL(V)$ determined by $g(e_1) = e_1$, $g(e_2) = e_2$, $g(e_3) = e_4$ and $g(e_4) = e_3$. Then $\beta^g(e_2, e_3) = g^{-1}\beta(ge_2, ge_3) = g^{-1}\beta(e_2, e_4) = \beta(e_2, e_4)$ and $\mathrm{Rad}(\beta^g) = g^{-1}(\mathrm{Rad}(\beta)) = \mathrm{Rad}(\beta)$. We can therefore assume that $a = \beta(e_2, e_3) \neq 0$, so $a = e_1$. If $b = c = 0$ then $e_4 \in \mathrm{Rad}(\beta)$, a contradiction. If $b = e_1$ and $c = 0$ then $e_3 + e_4 \in \mathrm{Rad}(\beta)$, since $\beta(e_3 + e_4, e_i) = \beta(e_3, e_i) + \beta(e_4, e_i) \in \{0 + 0, e_1 + e_1\} = \{0\}$. If $b = 0$ and $c = e_1$ then $e_2 + e_4 \in \mathrm{Rad}(\beta)$. Finally, if $b = c = e_1$ then $e_2 + e_3 + e_4 \in \mathrm{Rad}(\beta)$. Hence there is no solution for $r = 1$.

Suppose that $r = 2$ and $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta) = \langle e_1, e_2 \rangle$. Then β is of the form

	e_1	e_2	e_3	e_4
e_1	0	0	0	0
e_2	0	0	0	0
e_3	0	0	0	a
e_4	0	0	a	0

for some $a \in \langle e_1, e_2 \rangle$. The group $GL(\langle e_1, e_2 \rangle) \leq GL(V)$ fixes $\langle e_1, e_2 \rangle = \mathrm{Rad}(\beta)$ and permutes nonzero elements of $\langle e_1, e_2 \rangle$. We can therefore assume that $a = e_1$, obtaining the mapping $\beta_{4,2}$ of Table 2.

Dimension $n = 5$. We have $r \in \{1, 2, 3\}$. If $r = 3$, a quick argument similar to the case $n = 4$ and $r = 2$ shows that we can take $\beta = \beta_{5,3}$ of Table 2.

Suppose that $r = 1$. We can take β of the form

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	0
e_2	0	0	a	b	c
e_3	0	a	0	d	e
e_4	0	b	a	0	f
e_5	0	c	e	f	0

for some $a, b, c, d, e, f \in \langle e_1 \rangle$. We cannot have $a = b = c = 0$ (else $e_2 \in \mathrm{Rad}(\beta)$). By permuting e_3, e_4 and e_5, we can assume that $a \neq 0$, so $a = e_1$. Further analysis by hand is certainly possible but we delegate to a computer. There are 32 possibilities for the remaining parameters. A computer search shows that the resulting mappings either violate the condition on the radical, or they are equivalent to the mapping $\beta_{5,1}$ of Table 2.

Finally suppose that $r = 2$ and $\mathrm{Rad}(\beta) = \langle e_1, e_2\rangle$. Then β is of the form

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	0
e_2	0	0	0	0	0
e_3	0	0	0	a	b
e_4	0	0	a	0	c
e_5	0	0	b	c	0

for some $a, b, c \in \langle e_1, e_2\rangle$. We cannot have $a = b = 0$, and permuting e_4, e_5 shows that we can assume $a \neq 0$. Consider an element $g \in H = GL(\langle e_1, e_2\rangle)$. Then $\beta^g(e_3, e_4) = g^{-1}\beta(ge_3, ge_4) = g^{-1}\beta(e_3, e_4) = g^{-1}(a)$. Since H acts transitively on 1-dimensional subspaces of $\langle e_1, e_2\rangle$, we can assume that $a = e_1$. There are then 16 cases to consider for b and c. A computer search shows that the resulting mappings either violate the condition on the radical, or they are equivalent to the mapping $\beta_{5,2}$ of Table 2.

$\beta_{3,1}$	e_1	e_2	e_3
e_1	0	0	0
e_2	0	0	e_1
e_3	0	e_1	0

$\beta_{4,2}$	e_1	e_2	e_3	e_4
e_1	0	0	0	0
e_2	0	0	0	0
e_3	0	0	0	e_1
e_4	0	0	e_1	0

$\beta_{5,1}$	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	0
e_2	0	0	e_1	0	0
e_3	0	e_1	0	0	0
e_4	0	0	0	0	e_1
e_5	0	0	0	e_1	0

$\beta_{5,2}$	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	0
e_2	0	0	0	0	0
e_3	0	0	0	e_1	0
e_4	0	0	e_1	0	e_2
e_5	0	0	0	e_2	0

$\beta_{5,3}$	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	0
e_2	0	0	0	0	0
e_3	0	0	0	0	0
e_4	0	0	0	0	e_1
e_5	0	0	0	e_1	0

Table 2. All nonzero symmetric alternating biadditive mappings $\beta : V \times V \to V$ satisfying $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$, up to the action of $GL(V)$, with $V = \mathbb{F}_2^n$ and $1 \leq n \leq 5$.

4.2. Moufang permutations with a prescribed biadditive mapping.

PROPOSITION 4.2. *Let p be a prime. Suppose that $F = \mathbb{F}_p$, $X = F^n = \langle e_1, \ldots, e_n\rangle$ and (f, β) is a Moufang pair on $(X, +)$. Then*

$$f(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} f(x_i e_i) - \sum_{i=1}^{n} \sum_{j=i+1}^{n} f(x_i x_j \beta(e_i, e_j)) \tag{6}$$

for every $x_i \in \mathbb{F}_p$. Moreover,

$$f(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} x_i f(e_i) - \sum_{i=1}^{n} \sum_{j=i+1}^{n} x_i x_j f\beta(e_i, e_j). \tag{7}$$

Proof. Recall that $\beta(x, y) = f^{-1}(f(x)+f(y))-(x+y)$, so $\beta(x, y)+(x+y) = f^{-1}(f(x)+f(y))$ and $f(\beta(x, y) + (x + y)) = f(x) + f(y)$. Since $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$ and $f(u + v) =$

$f(u)+f(v)$ whenever $u \in \mathrm{Rad}(\beta)$, by Lemma 2.1, we have $f\beta(x,y)+f(x+y) = f(x)+f(y)$, and thus

$$f(x+y) = f(x) + f(y) - f\beta(x,y). \tag{8}$$

Using the identity (8) repeatedly, we obtain

$$\begin{aligned} f(\sum_{i=1}^{n} x_i e_i) &= f(\sum_{i=1}^{n-1} x_i e_i + x_n e_n) = f(\sum_{i=1}^{n-1} x_i e_i) + f(x_n e_n) - f\beta(\sum_{i=1}^{n-1} x_i e_i, x_n e_n) \\ &= f(\sum_{i=1}^{n-2} x_i e_i) + f(x_{n-1} e_{n-1}) - f\beta(\sum_{i=1}^{n-2} x_i e_i, x_{n-1} e_{n-1}) \\ &\quad + f(x_n e_n) - f\beta(\sum_{i=1}^{n-1} x_i e_i, x_n e_n). \end{aligned}$$

Continuing in this fashion and using biadditivity of β, we get

$$f(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} f(x_i e_i) - \sum_{j=1}^{n-1} f(\sum_{i=1}^{j} x_i x_{j+1} \beta(e_i, e_{j+1})).$$

Since every summand $x_i x_{j+1}\beta(e_i, e_{j+1})$ is in $\mathrm{Img}(\beta) \subseteq \mathrm{Rad}(\beta)$, we have

$$\sum_{j=1}^{n-1} f(\sum_{i=1}^{j} x_i x_{j+1} \beta(e_i, e_{j+1})) = \sum_{j=1}^{n-1} \sum_{i=1}^{j} f(x_i x_{j+1} \beta(e_i, e_{j+1})).$$

To finish the proof of (6), it suffices to note that $\{(i, j+1) : 1 \le j \le n-1,\ 1 \le i \le j\} = \{(i,j) : 1 \le i \le n,\ i+1 \le j \le n\}$.

If p is odd then $f \in \mathrm{Aut}(V,+)$ by Theorem 2.12 and $f(x_i e_i) = x_i f(e_i)$. If $p = 2$, note that $f(x_i e_i) = x_i f(e_i)$ obviously holds when $x_i = 1$ and it also holds when $x_i = 0$ since $f(0) = 0$ by Lemma 2.1. ∎

LEMMA 4.3. *Let $X = \mathbb{F}_2^n = \langle e_1, \ldots, e_n \rangle$ and let (f, β) be a Moufang pair on $(X,+)$ such that $\mathrm{Rad}(\beta) = \langle e_1, \ldots, e_r \rangle$. Then $\{f(e_1), \ldots, f(e_n)\}$ is a basis of X.*

Proof. The formula (7) together with Lemma 2.1 show that the image of f if contained in $\mathrm{Rad}(\beta) + \langle f(e_1), \ldots, f(e_n) \rangle$. Since f restricts to an automorphism on $\mathrm{Rad}(\beta) = \langle e_1, \ldots, e_r \rangle$, we must have $\mathrm{Rad}(\beta) = \langle f(e_1), \ldots, f(e_r) \rangle$. Thus we conclude $X = \mathrm{Img}(f) \subseteq \langle f(e_1), \ldots, f(e_n) \rangle$. ∎

PROPOSITION 4.4. *Let $0 \le r \le n$, $X = \mathbb{F}_2^n = \langle e_1, \ldots, e_n \rangle$ and $R = \langle e_1, \ldots, e_r \rangle$. Suppose that β is a symmetric alternating biadditive map with designated image and radical R. Let $\{f(e_i) : 1 \le i \le n\}$ be chosen so that $\{f(e_1), \ldots, f(e_r)\}$ is a basis of R and $\{f(e_1), \ldots, f(e_n)\}$ is a basis of X. Suppose that $f(\sum x_i e_i)$ is defined by (7). Then f permutes X, $f(x+y) = f(x)+f(y)$ whenever $\{x,y\} \cap R \neq \emptyset$, (1) holds and (2) holds. Hence (f,β) is a Moufang pair if and only if (3) holds. In fact, (f,β) is a Moufang pair if and only if (3) holds for all $x, y \in \{e_1, \ldots, e_n\}$.*

Proof. The formula (7) with $x = 0$ yields $f(0) = 0$, and then with $x = e_k$ it yields $f(e_k) - f\beta(e_k, e_k) = f(e_k) - f(0) = f(e_k)$, so the mapping f is well-defined. Suppose that $x = \sum x_i e_i \in R$ and $y = \sum y_i e_i$. Then $f(x+y) = \sum_i (x_i + y_i) f(e_i) - \sum_{i<j} (x_i +$

$y_i)(x_j+y_j)f\beta(e_i,e_j)$, while $f(x)+f(y)=\sum_i x_i f(e_i)-\sum_{i<j}x_ix_jf\beta(e_i,e_j)+\sum_i y_if(e_i)-\sum_{i<j}y_iy_jf\beta(e_i,e_j)$. We claim that $x_iy_jf\beta(e_i,e_j)=0$ for all $i<j$. Indeed, if $i>r$ then $x_i=0$ and if $i\le r$ then $\beta(e_i,e_j)=0$ and hence $f\beta(e_i,e_j)=0$. Similarly, $x_jy_i\beta(e_i,e_j)=0$ for all $i<j$. Hence $f(x+y)=f(x)+f(y)$.

In particular, f restricts to an automorphism of R. To show that f permutes X, it suffices to prove that f is onto X. Let $z\in X$ and write $z=z'+z''$, where $z'\in R$ and $z''\in\langle e_{r+1},\dots,e_n\rangle$. Since $\{f(e_i):1\le i\le n\}$ is a basis of X, there is $x=\sum x_ie_i$ such that $\sum x_if(e_i)=z''$. Then $f(x)=z''+u$ for some $u\in R$. Now, $z'-u\in R$ and therefore $f(x+f^{-1}(z'-u))=f(x)+ff^{-1}(z'-u)=z''+u+z'-u=z$.

The condition (1) holds if and only if $f(\beta(x,y)+x+y)=f(x)+f(y)$ for all $x,y\in X$. Since $\beta(x,y)\in R$, we need to check that $f\beta(x,y)+f(x+y)=f(x)+f(y)$. The left hand side is equal to $\sum_{i,j}x_iy_jf\beta(e_i,e_j)+\sum_i(x_i+y_i)f(e_i)-\sum_{i<j}(x_i+y_i)(x_j+y_j)f\beta(e_i,e_j)$, while the right hand side is equal to $\sum_i(x_i+y_i)f(e_i)-\sum_{i<j}(x_ix_j+y_iy_j)f\beta(e_i,e_j)$. We therefore need to check that $\sum_{i,j}x_iy_jf\beta(e_i,e_j)-\sum_{i<j}(x_iy_j+y_ix_j)f\beta(e_i,e_j)=0$, which holds since β is symmetric and alternating.

Condition (2) holds because we are assuming $\mathrm{Img}(\beta)\subseteq R\subseteq\mathrm{Rad}(\beta)$.

Suppose that (3) holds whenever $\{x,y\}\subseteq\{e_1,\dots,e_n\}$. We need to verify that it then holds for all $x,y\in X$. Let us write $f(e_i)=\sum_k f_{ik}e_k$ for suitable scalars f_{ik}. Calculating modulo R we have $f(\sum_i x_ie_i)\equiv\sum_i x_if(e_i)=\sum_i x_i\sum_k f_{ik}e_k=\sum_k(\sum_i x_if_{ik})e_k$. Reindexing, we have $f(\sum_i x_ie_i)\equiv\sum_i(\sum_k x_kf_{ki})e_i$. Then $f^2(\sum x_ie_i)\equiv f(\sum_i(\sum_k x_kf_{ki})e_i)=\sum_i(\sum_{\ell,k}x_kf_{k\ell}f_{\ell i})e_i$ and finally $f^3(\sum x_ie_i)\equiv\sum_i(\sum_{m,\ell,k}x_kf_{k\ell}f_{\ell m}f_{mi})e_i$. Thus $f\beta(f^3x,fy)=f(\sum_{i,j}\sum_{m,\ell,k}x_kf_{k\ell}f_{\ell m}f_{mi}y_j\beta(e_i,e_j))$ and the coefficient at $\beta(e_i,e_j)$ is $\sum_{m,\ell,k}x_kf_{k\ell}f_{\ell m}f_{mi}y_j$. On the other hand, by our assumption, $\beta(fx,fy)=\beta(\sum_i x_if(e_i),\sum_j y_jf(e_j))=\sum_{i,j}x_iy_j\beta(f(e_i),f(e_j))=\sum_{i,j}x_iy_jf\beta(f^3(e_i),e_j)$. Applying the above formula for $f^3(x)$ in the special case of $x=e_u$ we conclude that $f^3(e_u)\equiv\sum_{i,m,\ell}f_{u\ell}f_{\ell m}f_{mi}e_i$ and upon reindexing we obtain $f^3(e_i)\equiv\sum_{u,m,\ell}f_{i\ell}f_{\ell m}f_{mu}e_u$. Hence

$$\beta(fx,fy)=\sum_{i,j}x_iy_jf\beta(f^3(e_i),e_j)=\sum_{i,j}x_iy_jf\beta(\sum_{u,m,\ell}f_{i\ell}f_{\ell m}f_{mu}e_u,e_j)$$
$$=f(\sum_{i,j}x_iy_j\sum_{u,m,\ell}f_{i\ell}f_{\ell m}f_{mu}\beta(e_u,e_j)).$$

In this expression the coefficient at $\beta(e_u,e_j)$ is equal to $\sum_{i,m,\ell}x_if_{i\ell}f_{\ell m}f_{mu}y_j$ and this agrees with the above coefficient upon reindexing. ∎

We can now calculate $\mathrm{Mfp}(X)$ for $X=C_2^k$ somewhat efficiently. First, we find all symmetric alternating biadditive mapping $\beta:X\times X\to X$ with $\mathrm{Img}(\beta)\subseteq\mathrm{Rad}(\beta)$ up to the action of $GL_k(2)$ as in Subsection 4.1. For a given $\beta:X\times X\to X$ with $\mathrm{Img}(\beta)\subseteq\mathrm{Rad}(\beta)=\langle e_1,\dots,e_r\rangle$, we prescribe the values of f on the basis in all possible ways so that $\{f(e_1),\dots,f(e_r)\}$ is a basis of $\langle e_1,\dots,e_r\rangle$ and $\{f(e_1),\dots,f(e_n)\}$ is a basis of X. We then extend f to X according to the formula (7). By Proposition 4.4 we obtain a Moufang pair (f,β), except that we must explicitly check that the condition (3) holds on a basis.

Following this procedure, a computer search finds 16 Moufang permutations f for $\beta=\beta_{3,1}$, 224 fs for $\beta_{4,2}$, 5056 fs for $\beta_{5,1}$, 1408 fs for $\beta_{5,2}$ and 6144 fs for $\beta_{5,3}$. These

Moufang permutations can be further filtered by considering the conjugation action of the stabilizer of β.

EXAMPLE 4.5. We wish to recover the three proper Moufang permutations on $X = \mathbb{F}_2^3$ for the symmetric alternating biadditive mapping $\beta_{3,1}$ of Table 2. We have $\mathrm{Img}(\beta) = \mathrm{Rad}(\beta) = \langle e_1 \rangle$. According to (6), such Moufang permutation f must satisfy

$$f(\sum_{i=1}^{3} x_i e_i) = \sum_{i=1}^{3} x_i f(e_i) + x_2 x_3 f(e_1).$$

We must also have $f(0) = 0$, $f(e_1) = e_1$ and $\{f(e_1), f(e_2), f(e_3)\}$ must be a basis of X. There are thus $6 \cdot 4 = 24$ possible choices of $f(e_2)$ and $f(e_3)$. If we choose $f(e_2) = e_2$ and $f(e_3) = e_3$, formula (6) yields the transposition $(e_2 + e_3, e_1 + e_2 + e_3)$. If we choose $f(e_2) = e_1 + e_2$ and $f(e_3) = e_1 + e_3$, we get the permutation $(e_2, e_1 + e_2)(e_3, e_1 + e_3)(e_2 + e_3, e_1 + e_2 + e_3)$. Finally, towards the last nonconjugate Moufang permutation, we can choose $f(e_2) = e_3$ and $f(e_3) = e_2 + e_3$, obtaining $(e_2, e_3, e_2 + e_3, e_1 + e_2, e_1 + e_3, e_1 + e_2 + e_3)$.

Acknowledgments. P. Vojtěchovský supported by the Simons Foundation Mathematics and Physical Sciences Collaboration Grant for Mathematicians no. 855097.

References

[1] Aleš Drápal, *On extensions of Moufang loops by a cyclic factor that is coprime to three*, Comm. Algebra **45** (2017), no. **6**, 2350–2376.

[2] Aleš Drápal and Petr Vojtěchovský, *On abelian-by-cyclic Moufang loops*, to appear in Forum Mathematicum, `https://doi.org/10.1515/forum-2022-0391`.

[3] Stephen M. Gagola, III, *Abelian by cyclic groups resulting in Moufang loops*, J. Group Theory **15** (2012), no. **1**, 1–7.

[4] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.12.2 ; 2022, `http://www.gap-system.org`.

[5] Michael K. Kinyon and Kenneth Kunen, *The structure of extra loops*, Quasigroups Related Systems **12** (2004), 39–60.

[6] Fook Leong and Andrew Rajah, *Split extension in Moufang loops*, Publ. Math. Debrecen **52** (1998), no. **1–2**, 33–42.

[7] Ruth Moufang, *Zur Struktur von Alternativkörpen*, Math. Ann. **110** (1935), no. **1**, 416–430.

[8] Gábor P. Nagy and Petr Vojtěchovský, LOOPS, version 3.4.1, package for GAP, `https://github.com/gap-packages/loops`.