

IDENTITIES IN MOUFANG SETS

TOM DE MEDTS¹ AND YOAV SEGEV²

ABSTRACT. Moufang sets were introduced by Jacques Tits as an axiomatization of the buildings of rank one that arise from simple algebraic groups of relative rank one. These fascinating objects have a simple definition and yet their structure is rich, while it is rigid enough to allow for (at least partial) classification. In this paper we obtain two identities that hold in *any* Moufang set. These identities are closely related to the axioms that define a quadratic Jordan algebra. We apply them in the case when the Moufang set is so-called special and has abelian root groups. In addition we push forward the theory of special Moufang sets.

1. INTRODUCTION

During the last few years, there has been a growing interest in Moufang sets, which were introduced in 1990 by Jacques Tits in [Ti]. The notion of a Moufang set is equivalent to that of a group with a split BN -pair of rank one. Another essentially equivalent concept is that of (an abstract) rank one group, as introduced by F. Timmesfeld in [T]. (The latter requires the root groups to be nilpotent; this is not required for Moufang sets.)

Moufang sets are of great importance: On the one hand for purely group-theoretical purposes (and in particular, for classification purposes of both simple algebraic groups and finite simple groups). On the other hand, there are many deep connections with algebraic structures (octonion algebras, Jordan algebras, Albert algebras, quadratic forms, hermitian forms as well as other structures).

The first systematic study of Moufang sets was begun only recently by T. De Medts and R. Weiss in [DW]. The paper [DW] had set the path along which the current paper follows and both papers show that it may be possible to classify at least certain classes of Moufang sets (e.g. the so-called special ones, see Definition 4.1).

In order to make the statements of our results accessible we first need to give some definitions. A *Moufang set* is a permutation group G^\dagger on a set X together with a conjugacy class of subgroups $\{U_x \mid x \in X\}$ which generate

Date: August 30, 2005.

2000 Mathematics Subject Classification. Primary: 17C60, 20E42 ; Secondary: 17C30.

Key words and phrases. Moufang set, special, rank one group, Jordan algebra.

¹Postdoctoral Fellow of the Research Foundation - Flanders (Belgium) (F.W.O.-Vlaanderen).

²Partially supported by BSF grant no. 2004-083.

G^\dagger , such that for every $x \in X$, U_x fixes x , acts regularly on $X \setminus \{x\}$, and $U_x^\varphi = U_{x\varphi}$, for all $\varphi \in G^\dagger$. In particular, G^\dagger is a doubly transitive permutation group. The group G^\dagger is called the *little projective group* of the Moufang set, and the subgroups $\{U_x \mid x \in X\}$ are called the *root groups* of the Moufang set.

Any Moufang set can be constructed as follows (see [DW]). Start with a group U and let ∞ be a new symbol (not in U). Let X denote the set $X := U \cup \{\infty\}$. We write U in *additive notation* even though we do not assume that U is commutative. For $a \in U^* := U \setminus \{0\}$, we let $\alpha_a \in \text{Sym}(X)$ be the permutation which fixes ∞ and maps x to $x + a$ for every $x \in U$. Suppose that $\tau \in \text{Sym}(X)$ with $0\tau = \infty$ and $\infty\tau = 0$, and let

$$U_\infty = \{\alpha_a \mid a \in U\}, U_0 = U_\infty^\tau, \text{ and } U_a = U_0^{\alpha_a} \text{ for all } a \in U^*.$$

Then $G^\dagger := \langle U_x \mid x \in X \rangle$ and the subgroups $\{U_x \mid x \in X\}$ are candidates for being a Moufang set. These ‘‘candidates’’ are encoded by the notation $\mathbb{M}(U, \tau)$. For $a \in U^*$, let

$$\mu_a := \alpha_{(-a)\tau^{-1}}^\tau \alpha_a \alpha_{-(a\tau^{-1})}^\tau,$$

where for group elements g, h , $g^h = h^{-1}gh$. These complicated looking permutations μ_a play an important role in the analysis of Moufang sets. It can be easily shown that μ_a interchanges 0 and ∞ , for all $a \in U^*$. In particular, for $a \in U^*$, $\tau\mu_a$ fixes 0 and ∞ and hence acts as a permutation on the set U . In the main theorem (Theorem 2) of [DW] it is proved that the fact that $\mathbb{M}(U, \tau)$ is a Moufang set is equivalent to the fact that $\tau\mu_a \in \text{Aut}(U)$, for all $a \in U^*$.

The permutations μ_a , $a \in U^*$ are invariants of $\mathbb{M}(U, \tau)$ in the following sense: From the definition of $\mathbb{M}(U, \tau)$ it follows that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \rho)$ for every permutation $\rho \in \text{Sym}(X)$ that interchanges 0 and ∞ and satisfies $U_\infty^\rho = U_\infty^\tau = U_0$. Although the permutations μ_a appear to depend on τ , once it is established that $\mathbb{M}(U, \tau)$ is a Moufang set, it turns out that μ_a depends only on the subgroups U_0 and U_∞ : it is the unique element in $U_0\alpha_aU_0$ that interchanges 0 and ∞ (see Lemma 3.3(2)).

This paper shows that some of the connections between special Moufang sets and quadratic Jordan division algebras discovered in [DW], actually exist in a more general context: We prove

Theorem 1.1. *Assume $\mathbb{M}(U, \tau)$ is a Moufang set. Then*

- (1) $\mu_{a\mu_b} = \mu_b^{-1}\mu_a^{-1}\mu_b$, for all $a, b \in U \setminus \{0\}$;
- (2) $\mu_{(a\tau^{-1}-b\tau^{-1})\tau} = \mu_{-b}\mu_{b-a}\mu_a$, for all $a, b \in U \setminus \{0\}$ with $a \neq b$.

It turns out that in the case when U is abelian and $\mathbb{M}(U, \tau)$ is a special Moufang set, identity (1) of Theorem 1.1 is equivalent to the ‘‘fundamental identity’’ in the theory of quadratic Jordan algebras (axiom (QJ3) in §2), while identity (2) of Theorem 1.1 is closely related to axiom (QJ2).

The exact way the identities of Theorem 1.1 translate to identities in the theory of quadratic Jordan division algebras becomes more transparent once

the *Hua maps* (relative to τ) are introduced. These maps come from [DW], see Notation 3.2. They are given by

$$h_a = \tau\mu_a.$$

A word of caution is needed here: though τ does not appear in the notation h_a , nevertheless h_a does depend on τ .

We now discuss the application of Theorem 1.1 to special Moufang sets with abelian root groups. By [T, Thm. 5.2(a), p. 55], if $\mathbb{M}(U, \tau)$ is a special Moufang set such that U is abelian, then U is a vector space over \mathbb{Q} or over $\text{GF}(p)$ for some prime p (see also Proposition 4.6(5) below). Thus U has a natural characteristic. The following theorem generalizes Theorem 7 of [DW]. We refer the reader to §2 for the definition of a quadratic Jordan division algebra.

Theorem 1.2. *Assume that $\mathbb{M}(U, \tau)$ is a special Moufang set and that U is abelian of characteristic distinct from 2 and 3. Fix $e \in U^*$ and let $h_a := \mu_e\mu_a$ be the Hua maps relative to μ_e , $a \in U^*$. Let $\mathcal{H}: U \rightarrow \text{Aut}(U)$ be the map $\mathcal{H}: x \mapsto h_x$, and suppose that the map $(x, y) \mapsto h_{x+y} - h_x - h_y$, from $U \times U$ to $\text{End}(U)$ is biadditive.*

Then (U, \mathcal{H}, e) is a quadratic Jordan division algebra.

In §5 there are additional results related to special Moufang sets with abelian root groups: In Propositions 5.5 and Corollary 5.6 we show some interesting conditions which are equivalent to axiom (QJ2) in the context of Moufang sets.

Section 4 is devoted to special Moufang sets: In Lemma 4.3 we deduce a variety of identities involving the permutations μ_a and α_a , $a \in U^*$. Proposition 4.6 shows that if U is torsion free, then U is a uniquely divisible group (and there are results also in the case when U contains torsion). Proposition 4.9 shows that two μ -maps μ_a and μ_b can only be equal if $b = \pm a$ and Proposition 4.10(5) shows that if $a \in U^*$ has finite order then $\mu_a^4 = 1$. There are various additional results in this paper. We note that some of the results of §4 were applied in [SW].

ACKNOWLEDGMENT: Both authors are grateful to Richard Weiss for his careful reading of the paper which resulted in valuable comments.

2. QUADRATIC JORDAN ALGEBRAS

Throughout this paper we compose maps *from left to right* and we apply maps on the *right side* of the variable. For a set X containing a zero element, X^* will denote $X \setminus \{0\}$.

We first recall the definition of quadratic Jordan algebras, as introduced by K. McCrimmon [Mc1]. Note that we will use the notation J_x in place of the more common notation U_x , to avoid confusion with our notation for the root groups.

Let k be an arbitrary commutative field, let J be a vector space over k of arbitrary dimension, and let $1 \in J^*$ be a distinguished element. For each

$x \in J$, let $J_x \in \text{End}_k(J)$, and assume that the map $\mathcal{J}: x \mapsto J_x$ from J to $\text{End}(J)$ is quadratic, i.e.

$$J_{xt} = J_x t^2 \text{ for all } t \in k, \text{ and}$$

$$\text{the map } (x, y) \mapsto J_{x,y} \text{ is } k\text{-bilinear,}$$

(note that we multiply scalars on the right) where

$$J_{x,y} := J_{x+y} - J_x - J_y$$

for all $x, y \in J$. Let

$$zV_{x,y} := yJ_{x,z}$$

for all $x, y, z \in J$. Then the triple $(J, \mathcal{J}, 1)$ is a *quadratic Jordan algebra* if the identities

$$\begin{aligned} \text{(QJ1)} \quad & J_1 = \text{id}_J; \\ \text{(QJ2)} \quad & J_x V_{x,y} = V_{y,x} J_x; \\ \text{(QJ3)} \quad & J_y J_x = J_x J_y J_x \end{aligned}$$

hold *strictly*, i.e. if they continue to hold in all scalar extensions of J . (It suffices for them to hold in the polynomial extension $J_{k[t]}$ and this is automatically true if the base field k has at least 4 elements.)

Any element $e \in J$ such that $J_e = \text{id}_J$ is called an *identity element*. An element $x \in J$ is called *invertible* if there exists $y \in J$ such that

$$yJ_x = x \quad \text{and} \quad 1J_y J_x = 1.$$

In this case y is called the *inverse* of x and is denoted $y = x^{-1}$. By [Mc2, 6.1.2], an element $x \in J$ is invertible if and only if J_x is invertible; we then have $J_x^{-1} = J_{x^{-1}}$. In particular,

$$(x^{-1})^{-1} = x \quad \text{and} \quad x^{-1} = xJ_x^{-1}.$$

If all elements in J^* are invertible, then $(J, \mathcal{J}, 1)$ is called a quadratic Jordan *division algebra*.

3. MOUFANG SETS

For a permutation group $H \leq \text{Sym}(X)$ and elements $x, y \in X$ we denote by H_x the stabilizer in H of x , by $H_{x,y} := H_x \cap H_y$, and by $H_{\{x,y\}}$ the stabilizer of the set $\{x, y\}$ in H . Also, for any group G , elements $x, y \in G$ and a subgroup $H \leq G$, $x^y = y^{-1}xy$ and $H^y = y^{-1}Hy$.

For the sake of being orderly we repeat (and expand) here some of the definitions and notation given in the introduction. A Moufang set is a set X together with a permutation group

$$G^\dagger \leq \text{Sym}(X),$$

and a collection of subgroups

$$\{U_x \mid x \in X\},$$

satisfying the following properties:

$$\text{(MFS1)} \quad G^\dagger = \langle U_x \rangle;$$

- (MFS2) $U_x \leq G_x^\dagger$ and U_x is regular on $X \setminus \{x\}$, for all $x \in X$ (in particular, G^\dagger is doubly transitive);
- (MFS3) for all $x \in X$, we have that $U_x^\varphi = U_{x\varphi}$ for all $\varphi \in G^\dagger$. In particular, U_x is weakly closed in G_x^\dagger with respect to G^\dagger .

The subgroups U_x are called the *root (sub)groups* of the Moufang set; the group G^\dagger is called its *little projective group*.

Notation 3.1. (1) Throughout this paper U denotes a group which is *not necessarily commutative* but *written in additive notation*.

- (2) Throughout ∞ is a new symbol (not in U) and X denotes the set

$$X := U \cup \{\infty\}.$$

- (3) For $a \in U^*$ we let $\alpha_a \in \text{Sym}(X)$ be the permutation

$$x\alpha_a := \begin{cases} x + a & \text{if } x \in U; \\ \infty & \text{if } x = \infty. \end{cases}$$

- (4) Suppose that $\tau \in \text{Sym}(X)$ with $0^\tau = \infty$ and $\infty^\tau = 0$, then we denote $U_\infty = \{\alpha_a \mid a \in U\}$, $U_0 = U_\infty^\tau$, and $U_a = U_0^{\alpha_a}$ for all $a \in U^*$.

Notation 3.2. Let $a \in U^*$; following [DW] we denote

- (1) $\gamma_a := \alpha_a^\tau$;
- (2) $\mu_a := \gamma_{(-a)\tau^{-1}}\alpha_a\gamma_{a\tau^{-1}}^{-1}$;
- (3) $h_a := \tau\alpha_a\tau^{-1}\alpha_{a\tau^{-1}}^{-1}\tau\alpha_{(-a\tau^{-1})}^{-1}$; these maps h_a are called the *Hua maps* corresponding to τ .
- (4) It will be convenient to define $\mu_0 := 0$ and $h_0 := 0$.

Lemma 3.3. *Let $a \in U^*$, then*

- (1) $\mu_{-a} = \mu_a^{-1}$;
- (2) μ_a is the unique element in $U_0\alpha_aU_0$ interchanging 0 and ∞ .

Proof. (1) is immediate from the definition of μ_a .

To show (2), let $\rho \in U_0\alpha_aU_0$ and assume that $0\rho = \infty$ and $\infty\rho = 0$. Write $\rho = \gamma_x\alpha_a\gamma_y$, with $\gamma_x, \gamma_y \in U_0$. Then $\infty = 0\rho = a\gamma_y = ((a\tau^{-1}) + y)\tau$. Hence $a\tau^{-1} + y = \infty\tau^{-1} = 0$, so $y = -(a\tau^{-1})$. Also,

$$0 = \infty\rho = \infty\gamma_x\alpha_a\gamma_y = \infty\tau^{-1}\alpha_{x\tau}\alpha_a\gamma_y = x\tau\alpha_a\gamma_y = (x\tau + a)\gamma_y.$$

It follows that $x\tau + a = 0\gamma_y^{-1} = 0$, so $x = (-a)\tau^{-1}$. \square

Notation 3.4. (1) Let X be a set. Suppose that for each $x \in X$ we are given a subgroup $U_x \leq \text{Sym}(X)$ that fixes x . We denote this situation by $(X, (U_x)_{x \in X})$.

- (2) $\mathbb{M}(U, \tau) := (X, (U_x)_{x \in X})$, where $X = U \cup \{\infty\}$ and τ, U_x are as in Notation 3.1(2) and 3.1(4).

Theorem 3.5 ([DW], Thm. 2). *$\mathbb{M}(U, \tau)$ is a Moufang set if and only if the map h_a restricted to U is an automorphism of U , for all $a \in U^*$.*

Notation 3.6. Let $\Lambda \subset \text{Sym}(X)$ be the set of all permutations $\lambda \in \text{Sym}(X)$ such that $0\lambda = \infty$ and $\infty\lambda = 0$. Then we can define $\mathbb{M}(U, \lambda)$, for $\lambda \in \Lambda$, where $\mathbb{M}(U, \lambda)$ is as in Notation 3.4(2), with τ replaced by λ . We let $\mathfrak{M} \subset \Lambda$ be the smallest subset satisfying the following properties: (i) $\tau \in \mathfrak{M}$; (ii) if $\rho \in \mathfrak{M}$, then $\rho^{-1} \in \mathfrak{M}$; (iii) if $\lambda \in \Lambda$ is such that $U_\infty^\lambda = U_\infty^\rho$, for some $\rho \in \mathfrak{M}$, then $\lambda \in \mathfrak{M}$.

Lemma 3.7. *Let \mathfrak{M} be as in Notation 3.6 and suppose $\mathbb{M}(U, \tau)$ is a Moufang set. Then*

- (1) $\mathbb{M}(U, \rho)$ is a Moufang set for each $\rho \in \mathfrak{M}$;
- (2) the permutation $\mu_{x, \rho} := \alpha_{(-x)\rho^{-1}}^\rho \alpha_x \alpha_{-(x\rho^{-1})}^\rho$ belongs to \mathfrak{M} for each $\rho \in \mathfrak{M}$ and $x \in U^*$. Furthermore $\mathbb{M}(U, \mu_{x, \rho}) = \mathbb{M}(U, \rho) = \mathbb{M}(U, \mu_{x, \rho}^{-1})$;
- (3) given $\rho, \sigma \in \mathfrak{M}$, $\mathbb{M}(U, \rho) = \mathbb{M}(U, \sigma)$ if and only if $U_\infty^\rho = U_\infty^\sigma$.

Proof. First notice that (3) is immediate from the definitions. Then by (3) to show (1) it suffices to show that if for some $\lambda \in \Lambda$, $\mathbb{M}(U, \lambda)$ is a Moufang set, then also $\mathbb{M}(U, \lambda^{-1})$ is a Moufang set. We show this for τ ; so we must show that $\mathbb{M}(U, \tau^{-1})$ is a Moufang set. For $a \in U^*$ consider the permutation $g_a := \tau^{-1} \alpha_a \tau \alpha_{a\tau}^{-1} \tau^{-1} \alpha_{-(a\tau)}^{-1} \in \text{Sym}(X)$. Notice that g_a is the Hua map corresponding to τ^{-1} (see Notation 3.2(3)). By [DW, Lemma 8(i)], $g_a = h_{a\tau}^{-1}$, so in particular, $g_a \in \text{Aut}(U)$. It follows by Theorem 3.5 that $\mathbb{M}(U, \tau^{-1})$ is a Moufang set.

It remains to prove (2). Note that the map $\mu_{x, \rho}$ is the “ μ -map” as defined in Notation 3.2(1) and 3.2(2), with τ replaced by ρ . Now by (1), $\mathbb{M}(U, \rho)$ is a Moufang set and, by definition, $\mu_{x, \rho}$ is in the little projective group corresponding to the Moufang set $\mathbb{M}(U, \rho)$. Furthermore, by Lemma 3.3(2), $\mu_{x, \rho} \in \Lambda$. Thus (2) follows from the fact that $\mathbb{M}(U, \rho)$ is a Moufang set (in particular from axiom (MFS3)), using (3). \square

Proposition 3.8. *Assume that $\mathbb{M}(U, \tau)$ is a Moufang set. Then*

- (1) $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau)$ for any $\rho \in \text{Sym}(X)$ which interchanges 0 and ∞ and satisfies $U_\infty^\rho = U_0$; in particular, this holds for $\rho = \mu_a$, where a is an arbitrary element in U^* ;
- (2) $G_{0, \infty}^\dagger = \langle \mu_a \mu_b \mid a, b \in U^* \rangle$ and $G_{\{0, \infty\}}^\dagger = \langle \mu_a \mid a \in U^* \rangle$;
- (3) $G_{0, \infty}^\dagger \leq \text{Aut}(U)$.

Proof. (1) This follows from Lemma 3.7(3) and 3.7(2).

(2) The first part of (2) is [DW, Thm. 1(ii)]. The second part follows from the first and from Lemma 3.3(2).

(3) By (2) it suffices to show that $\mu_a \mu_b \in \text{Aut}(U)$. But replacing τ with μ_a and using (1), we get from Proposition 3.9(1) below that the corresponding Hua maps are $\mu_a \mu_b$ and by Theorem 3.5, these maps are in $\text{Aut}(U)$. \square

Proposition 3.9. *Assume $\mathbb{M}(U, \tau)$ is a Moufang set, let $a, b \in U^*$ and let $\Lambda \subset \text{Sym}(X)$ be the set of permutations that interchange 0 and ∞ . Then*

- (1) $\mu_a = \tau^{-1}h_a$;
- (2) if $\rho \in \Lambda$ is such that $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau) = \mathbb{M}(U, \rho^{-1})$, then $\mu_{a\rho} = \rho^{-1}\mu_a^{-1}\rho$, it follows that $\mu_{ag} = g^{-1}\mu_ag$, for every $g \in G_{0, \infty}^\dagger$;
- (3) if $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$, then $h_{a\tau} = \tau^{-1}h_{-a}\tau$ and $h_{ah_b} = h_{-b}h_{a\tau}^{-1}h_b$.

Proof. (1) By [DW, Lemma 8.1(ii)], we have that $\mu_a = h_{-a}^{-1}\tau$. Therefore, by Lemma 3.3(1), we have that $\mu_a = \mu_{-a}^{-1} = \tau^{-1}h_a$.

(2) Assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$. We first prove (2) for $\rho = \tau$. Following [DW], we define the maps $g_a := \tau^{-1}\alpha_a\tau\alpha_{a\tau}^{-1}\tau^{-1}\alpha_{(-a\tau)}^{-1}$ for all $a \in U^*$. Then by definition, the maps g_a are the Hua maps corresponding to τ^{-1} . Since we are assuming that $\mathbb{M}(U, \tau^{-1}) = \mathbb{M}(U, \tau)$, we can apply (1) to the maps g_a . Note that by Lemma 3.3(2), the maps μ_a are independent of τ . Therefore, taking in (1) g_a in place of h_a and τ^{-1} in place of τ we have

$$\mu_a = \tau g_a.$$

On the other hand, we know from [DW, Lemma 8(i)] that $g_a = h_{a\tau}^{-1}$, and hence

$$\mu_{a\tau} = \tau^{-1}h_{a\tau} = \tau^{-1}g_a^{-1} = \tau^{-1}\mu_a^{-1}\tau,$$

which shows (2) for $\rho = \tau$. Now if $\rho \in \Lambda$ is such that $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau) = \mathbb{M}(U, \rho^{-1})$, just replace τ by ρ in the above argument, so the first part of (2) holds. The second part of (2) is a consequence of the first, noticing that by Proposition 3.8(1), $\mathbb{M}(U, \mu_x) = \mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_x^{-1})$, for each $x \in U^*$, and using Proposition 3.8(2).

- (3) First, by (1) and (2), $h_{a\tau} = \tau\mu_{a\tau} = \mu_a^{-1}\tau = \tau^{-1}(\tau\mu_{-a})\tau = \tau^{-1}h_{-a}\tau$. Next, again by (1) and (2),

$$h_{ah_b} = \tau\mu_{a\tau}\mu_b = \tau\mu_b^{-1}\mu_{a\tau}^{-1}\mu_b = \tau\mu_{-b}\mu_{a\tau}^{-1}\tau^{-1}\tau\mu_b = h_{-b}h_{a\tau}^{-1}h_b.$$

□

Proposition 3.10. *Assume $\mathbb{M}(U, \tau)$ is a Moufang set. Let $a \in U^*$ and set $\sim a := (-a\tau^{-1})\tau$. Then*

- (1) \sim is independent of τ , i.e., $\sim a = (-a\rho^{-1})\rho$, for every $\rho \in \text{Sym}(X)$ that interchanges 0 and ∞ and satisfies $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau)$;
- (2) if $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$, then $\mu_a = \alpha_a\gamma_{-a\tau^{-1}}\alpha_{-(\sim a)}$;
- (3) $\sim a = -((-a)\mu_a)$;
- (4) $\mu_{-a} = \alpha_{-(\sim a)}\mu_{-a}\alpha_a\mu_{-a}\alpha_{\sim(-a)}$;
- (5) let $c := a\gamma_{-(b\tau^{-1})} = (a\tau^{-1} - b\tau^{-1})\tau$, then c is independent of the choice of τ , and $\mu_b\mu_c\mu_{-a} = \mu_{b-a}$.

Proof. (1) Let $x \in U^*$, then $\sim a = (-a\tau^{-1})\tau\mu_{-x}\mu_x = (-a\mu_x^{-1})\mu_x$, because $\tau\mu_{-x} \in \text{Aut}(U)$. By Lemma 3.3(2), μ_x is independent of τ , and hence the same equalities hold with ρ in place of τ , which implies (1).

- (2) Notice that by (1) and by the definition of μ_a in Notation 3.2(2),

$$\mu_{a\tau} = \gamma_{\sim a} \alpha_{a\tau} \gamma_{-a}.$$

Using Lemma 3.3(1) and Proposition 3.9(2) we have $\mu_a^{-1} = \mu_{a\tau}^{\tau^{-1}} = \alpha_{\sim a} \alpha_{a\tau}^{\tau^{-1}} \alpha_{-a}$. Hence $\mu_a = \alpha_a \alpha_{-a\tau}^{\tau^{-1}} \alpha_{-(\sim a)}$. Since $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$ and since μ_a is independent of τ , this last equality holds with τ replaced by τ^{-1} .

- (3) By (2) we have

$$\begin{aligned} -((-a)\mu_a) &= -(-a)\alpha_a \tau^{-1} \alpha_{a\tau^{-1}}^{-1} \tau \alpha_{-(a\tau^{-1})}^{-1} \\ &= -(\infty) \alpha_{a\tau^{-1}}^{-1} \tau \alpha_{-(a\tau^{-1})}^{-1} \\ &= -(a\tau^{-1})\tau = \sim a. \end{aligned}$$

- (4) Since statement (4) is independent of τ , using Proposition 3.8(1) we may (and we will) assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$ by replacing τ by some μ_x . By part (2) with τ replaced by τ^{-1} , we have that

$$\mu_a = \alpha_a \tau \alpha_{-a\tau} \tau^{-1} \alpha_{-(\sim a)}$$

and hence

$$\alpha_{-a} \mu_a \alpha_{\sim a} = \tau \alpha_{-a\tau} \tau^{-1}; \quad (3.1)$$

since the left hand side is independent of τ , we can replace τ by any μ_x , and therefore

$$\alpha_{-a} \mu_a \alpha_{\sim a} = \mu_x \alpha_{-a\mu_x} \mu_{-x}, \quad (3.2)$$

for all $x \in U^*$. In particular, if we put $x = -a$, then we get, using the identity in part (3), that

$$\alpha_{-a} \mu_a \alpha_{\sim a} = \mu_{-a} \alpha_{\sim(-a)} \mu_a$$

which can be rewritten as

$$\alpha_{-(\sim a)} \mu_{-a} \alpha_a \mu_{-a} \alpha_{\sim(-a)} = \mu_{-a}.$$

- (5) First notice that, for all $x \in U^*$,

$$c = (a\tau^{-1} - b\tau^{-1})\tau \mu_x^{-1} \mu_x = (a\mu_x^{-1} - b\mu_x^{-1})\mu_x,$$

because, by Proposition 3.9(1), $\tau \mu_x^{-1} \in \text{Aut}(U)$. Hence, using Proposition 3.8(1), we may (and we will) again assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$ by replacing τ by some μ_x .

We have that $\sim c = (b\tau^{-1} - a\tau^{-1})\tau$. Note that $c = a\gamma_{-b\tau^{-1}}$, so by part (2), $c = a\alpha_{-b}\mu_b\alpha_{\sim b}$, or

$$c = (a - b)\mu_b + (\sim b); \quad (3.3)$$

by interchanging a and b we get

$$\sim c = (b - a)\mu_a + (\sim a). \quad (3.4)$$

In particular, c is independent of the choice of τ , and hence we have that

$$c = (a\tau^{-1} - b\tau^{-1})\tau = (a\tau - b\tau)\tau^{-1}.$$

Notice that since $\sim b = (-b\tau)\tau^{-1}$, $b\tau = -((\sim b)\tau)$. Also, $\sim(\sim b) = b$ and by Proposition 3.9(2) and Lemma 3.3(1), $\mu_{\sim b} = \mu_{-b}$. From equation (3.1) (with a replaced by $\sim b$) it now follows that

$$\tau\alpha_{b\tau}\tau^{-1} = \alpha_{-(\sim b)}\mu_{-b}\alpha_b. \quad (3.5)$$

Thus, by a repeated use of (3.1), we get that

$$\begin{aligned} \alpha_{-c}\mu_c\alpha_{\sim c} &= \tau\alpha_{-c\tau}\tau^{-1} \\ &= \tau\alpha_{b\tau-a\tau}\tau^{-1} \\ &= \tau\alpha_{b\tau}\tau^{-1}\tau\alpha_{-a\tau}\tau^{-1} \\ &= \alpha_{-(\sim b)}\mu_{-b}\alpha_b\alpha_{-a}\mu_a\alpha_{\sim a}. \end{aligned}$$

It follows that

$$\mu_c = \alpha_{c-(\sim b)}\mu_{-b}\alpha_b\alpha_{-a}\mu_a\alpha_{(\sim a)-(\sim c)},$$

and using (3.3) and (3.4), we can write this as

$$\mu_c = \alpha_{(a-b)\mu_b}\mu_{-b}\alpha_{b-a}\mu_a\alpha_{-(b-a)\mu_a}.$$

Therefore

$$\mu_b\mu_c\mu_{-a} = \mu_b\alpha_{(a-b)\mu_b}\mu_{-b} \cdot \alpha_{b-a} \cdot \mu_a\alpha_{-(b-a)\mu_a}\mu_{-a}.$$

We now apply equation (3.5) (with μ_b in place of τ and $(a-b)$ in place of b) and equation (3.2), and we get that

$$\begin{aligned} \mu_b\mu_c\mu_{-a} &= \alpha_{-\sim(a-b)}\mu_{b-a}\alpha_{a-b} \cdot \alpha_{b-a} \cdot \alpha_{a-b}\mu_{b-a}\alpha_{\sim(b-a)} \\ &= \alpha_{-\sim(a-b)}\mu_{b-a}\alpha_{a-b}\mu_{b-a}\alpha_{\sim(b-a)} \\ &= \mu_{b-a} \end{aligned}$$

where we have used part (4) with $a-b$ in place of a . □

4. SPECIAL MOUFANG SETS

In this section $\mathbb{M}(U, \tau)$ is a special Moufang set. We start by defining this notion, which has been introduced by F. Timmesfeld [T] in the context of (abstract) rank one groups.

Definition 4.1. A Moufang set $\mathbb{M}(U, \tau)$ is called *special* if the condition

$$(-a)\tau = -(a\tau) \text{ for all } a \in U^* \quad (*)$$

holds.

Lemma 4.2. *Let \mathfrak{M} be as in Notation 3.6. Then $(-a)\rho = -(a\rho)$, for each $\rho \in \mathfrak{M}$ and each $a \in U^*$. In particular, $(-a)\tau^{-1} = -(a\tau^{-1})$ and $(-a)\mu_x = -(a\mu_x)$, for all $a, x \in U^*$.*

Proof. We first show that $(-a)\mu_x = -(a\mu_x)$, for all $a, x \in U^*$. By Proposition 3.9(1) and Theorem 3.5, $\mu_x\tau^{-1} \in \text{Aut}(U)$. Hence $(-a)\mu_x\tau^{-1} = -(a\mu_x\tau^{-1})$, so

$$(-a)\mu_x = (-a)\mu_x\tau^{-1}\tau = (-(a\mu_x\tau^{-1}))\tau = -(a\mu_x\tau^{-1}\tau) = -(a\mu_x).$$

Let now $\rho \in \mathfrak{M}$ and assume first that $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau)$. Then by Proposition 3.9(1) (with ρ replacing τ), $\rho\mu_x \in \text{Aut}(U)$, where x is an arbitrary element in U^* . Then $(-a)\rho = (-a)\rho\mu_x\mu_{-x} = (-(a\rho\mu_x))\mu_{-x} = -(a\rho)$, using the first paragraph of the proof.

Finally, using the previous paragraph of the proof and the definition of \mathfrak{M} , to prove the lemma, it remains to show that $(-a)\tau^{-1} = -(a\tau^{-1})$. Notice that $(-(a\tau^{-1}))\tau = -a = (-a)\tau^{-1}\tau$, so $(-a)\tau^{-1} = -(a\tau^{-1})$. \square

Lemma 4.3. *Assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$. Let $a \in U^*$ then,*

- (1) $\mu_a = \alpha_a\gamma_{-a\tau^{-1}}\alpha_a$;
- (2) $a\mu_a = -a = a\mu_{-a}$;
- (3) $\mu_a = \alpha_a\alpha_a^{\mu_a^\epsilon}\alpha_a$, where $\epsilon \in \{+, -\}$;
- (4) μ_a^2 centralizes α_a and $\mu_a^4 = (\alpha_a\mu_a)^3$, in particular, if μ_a is an involution, then $(\alpha_a\mu_a)^3 = 1$;
- (5) if $a + a = 0$, then α_a is an involution, μ_a is conjugate to α_a , so μ_a is an involution as well and $\langle \alpha_a, \mu_a \rangle \cong \text{Sym}_3$.

Proof. (1) Notice that since $\mathbb{M}(U, \tau)$ is special, $\sim a := (-(a\tau^{-1}))\tau = -a$.

Hence (1) follows from Lemma 3.10(2).

(2) By part (1), $a\mu_{-a} = a\alpha_{-a}\gamma_{a\tau^{-1}}\alpha_{-a} = 0\gamma_{a\tau^{-1}}\alpha_{-a} = -a$. Using Lemma 4.2 it follows that $a = (-a)\mu_a = -(a\mu_a)$.

(3) By Proposition 3.8(1), Lemma 3.10(2) holds with $\mu_{\epsilon a}$ in place of τ . so (3) follows from (2).

(4) By Proposition 3.8(3), $\mu_a^2 \in \text{Aut}(U)$, so by (2), $\alpha_a^{\mu_a^2} = \alpha_a\mu_a^2 = \alpha_a$, this shows the first part of (4). Then, by Lemma 3.10(4), $\mu_{-a} = \alpha_a\mu_{-a}\alpha_a\mu_{-a}\alpha_a$, multiplying this equality by μ_a^2 on the left and by μ_a^3 on the right using the fact that μ_a^2 commutes with α_a gives the rest of (4).

(5) Clearly α_a is an involution and by Lemma 3.3(1), μ_a is an involution. Then by (3), μ_a is conjugate to α_a . The rest of (5) follows from (4). \square

Lemma 4.4. *Let $a, b \in U^*$. Then*

- (1) if $a \neq b$, then $(a\tau^{-1} - b\tau^{-1})\tau = (a - b)\mu_b - b = a + (a - b)\mu_a$;
- (2) if $a \neq -b$, then $(a\tau^{-1} + b\tau^{-1})\tau = (a + b)\mu_{-b} + b = a + (a + b)\mu_a$;
- (3) if $a \neq -b$, then $a\mu_{a+b} = -b - a + a\mu_b - b$.

Proof. We already observed in Proposition 3.10(5) that $(a\tau^{-1} - b\tau^{-1})\tau$ is independent of τ . Hence, by Proposition 3.8(1) we may (and we will) assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$. Also, (in the notation of Lemma 3.10), $\sim x = -x$, for $x \in U^*$. Now (1) follows from equations (3.3) and (3.4). Since by

Lemma 4.2 $(-x)\tau^{-1} = -(x\tau^{-1})$, (2) follows from (1) by replacing b with $-b$ in (1).

Replacing in (1) a with $a + b$ we get $a\mu_b - b = a + b + a\mu_{a+b}$, and part (3) follows. \square

Lemma 4.5. *Let \mathfrak{M} be as in Notation 3.6, $\rho \in \mathfrak{M}$ and $a \in U^*$. Then the order of a is equal to the order of $a\rho$ (and one is infinite if and only if the other is). In particular, the order of a is equal to the order of $a\tau$, $a\tau^{-1}$ and $a\mu_b$, $b \in U^*$.*

Proof. We show that the order of $a\tau$ is equal to the order of a , relying only on the fact that $\mathbb{M}(U, \tau)$ is a special Moufang set. By Lemma 3.7(1) and Lemma 4.2, $\mathbb{M}(U, \rho)$ is a special Moufang set for all $\rho \in \mathfrak{M}$, hence the lemma holds for any $\rho \in \mathfrak{M}$.

We have $a\tau = a\tau\mu_x^{-1}\mu_x$ and by Theorem 3.5 and Proposition 3.9(1), $\tau\mu_x^{-1} = \tau\mu_{-x} \in \text{Aut}(U)$, so it suffices to show (by replacing a with $a\tau\mu_x^{-1}$) that the order $a\mu_x$ is equal to the order of a . By Lemma 4.3(2), $a = (-a)\mu_a\mu_x$ and by Proposition 3.8(3), $\mu_a\mu_x \in \text{Aut}(U)$, so the lemma follows. \square

Proposition 4.6. *Let $a \in U^*$, $n \geq 1$ be a positive integer such that $a \cdot n \neq 0$, and $\rho \in \text{Sym}(X)$ such that ρ interchanges 0 and ∞ and satisfies $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau) = \mathbb{M}(U, \rho^{-1})$. Then*

- (1) *there exists a unique $b \in U^*$ such that $b \cdot n = a$, we denote $b := a \cdot \frac{1}{n}$;*
- (2) *$(a\rho) \cdot n \neq 0$; $(a \cdot n)\rho = (a\rho) \cdot \frac{1}{n}$, and hence $(a \cdot \frac{1}{n})\rho = (a\rho) \cdot n$;*
- (3) *if U is torsion free, then U is a uniquely divisible group;*
- (4) *if $b \in U^*$ has a finite order, then the order of b is a prime number;*
- (5) *([T, Thm. 5.2(a), p. 55]) if U is abelian then either U is an elementary abelian p -group, for some prime p , or U is a divisible torsion free abelian group;*
- (6) *assume U is abelian and that $U \cdot n \neq 0$ and let $s \in \{n, n^{-1}\}$. Then $x\mu_{a \cdot s} = x\mu_a \cdot s^2$, for all $x \in U^*$. It follows that $h_{a \cdot s} = h_a \cdot s^2$.*

Proof. (1&2) Let $n \geq 1$ be a positive integer. Assume that the equality

$$(a \cdot n)\mu_{-a} \cdot n = -a \text{ for all } a \in U^* \text{ such that } a \cdot n \neq 0, \quad (4.1)$$

holds. We claim that then (1) and (2) hold for n . First, by Lemma 4.3(2), $a\rho = (-a)\mu_{-a}\rho$. Now $\mu_{-a}\rho$ is the inverse of the map $\rho^{-1}\mu_a$ which, by Proposition 3.9(1), is a Hua map corresponding to ρ^{-1} , so $\mu_{-a}\rho \in \text{Aut}(U)$. It follows that

$$(a\rho) \cdot n = (-a)\mu_{-a}\rho \cdot n = ((-a) \cdot n)\mu_{-a}\rho \neq 0.$$

Also, the equality

$$(a \cdot n)\rho \cdot n = a\rho \text{ for all } a \in U^* \text{ such that } a \cdot n \neq 0, \quad (4.2)$$

holds. This is because

$$\begin{aligned} ((a \cdot n)\rho) \cdot n &= ((a \cdot n)\mu_a^{-1}\mu_a\rho) \cdot n \\ &= (((a \cdot n)\mu_a^{-1}) \cdot n)\mu_a\rho = (-a)\mu_a\rho = a\rho, \end{aligned}$$

since $\mu_a\rho \in \text{Aut}(U)$. It follows (by taking $\rho = \mu_a$) that the element $b := ((-a) \cdot n)\mu_a$ satisfies $b \cdot n = a$. Furthermore, if $c \cdot n = a$, then by (4.2) (with c in place of a and μ_a^{-1} in place of ρ),

$$((-a) \cdot n) = (a\mu_a^{-1}) \cdot n = (c \cdot n)\mu_a^{-1} \cdot n = c\mu_a^{-1},$$

so $c = b$.

It thus remains to show (4.1). The proof is by induction on n . For $n = 1$, this is Lemma 4.3(2). Assume that $a \cdot (n+1) \neq 0$. Note that if $a \cdot n = 0$, then $a \cdot (n+1)\mu_a \cdot (n+1) = a\mu_a \cdot (n+1) = -a$, so we may assume that $a \cdot n \neq 0$. Notice that also $a \cdot (n+1)n \neq 0$, because otherwise we would get $(a \cdot n) \cdot n = (-a) \cdot n$, but then, by the uniqueness in part (1) and by induction, $a \cdot n = -a$, which is false. Hence $a \cdot (n+1) \cdot \frac{1}{n}$ makes sense.

By Lemma 3.10(4), $\mu_{-a} = \alpha_a\mu_{-a}\alpha_a\mu_{-a}\alpha_a$. Notice that by induction we may assume that equation (4.2) holds. Using Lemma 4.3(2) and induction we get

$$\begin{aligned} -((a \cdot (n+1))\mu_{-a}) &= ((-a) \cdot (n+1))\mu_{-a} \\ &= ((-a) \cdot (n+1))\alpha_a\mu_{-a}\alpha_a\mu_{-a}\alpha_a \\ &= ((-a) \cdot n)\mu_{-a}\alpha_a\mu_{-a}\alpha_a \\ &\stackrel{\text{induction}}{=} (a \cdot \frac{1}{n} + a)\mu_{-a}\alpha_a \\ &= (a \cdot (n+1) \cdot \frac{1}{n})\mu_{-a}\alpha_a \stackrel{\text{induction}}{=} (a \cdot (n+1)\mu_{-a}) \cdot n + a. \end{aligned}$$

Hence, $(a \cdot (n+1))\mu_{-a} \cdot (n+1) = -a$. This completes the proof of (1) and (2).

- (3) This follows immediately from (1).
(4) Assume first that $b \in U^*$ is an element of order p^2 , where p is a prime. Then $b \cdot p \neq 0$, so, by (2), $(b \cdot p)\mu_a \cdot p = b\mu_a$. However, by Lemma 4.5, $(b \cdot p)\mu_a \cdot p = 0$, a contradiction.

Let p, q be distinct primes and assume that b has order pq . By (1), there exists a unique $x \in U^*$ such that $x \cdot p = b$. But then one easily checks that the order of x must be p^2q , so the order of $x \cdot q$ is p^2 , a contradiction. This shows (4).

- (5) If U is torsion free this follows from (3), so assume U contains torsion and let p be a prime such that $V := \{x \in U \mid x \cdot p = 0\} \neq \{0\}$. Set $U \cdot p := \{x \cdot p \mid x \in U\}$. Then V and $U \cdot p$ are subgroups of U and by (1), $U = U \cdot p \cup V$. If $U = V$, then we are done, so assume not. Then since no group is a union of two proper nontrivial subgroups, $U = U \cdot p$. Since $V \neq \{0\}$ this implies the existence of an element of order p^2 in U contradicting (4).

- (6) By Proposition 3.8(1), we may assume that $\tau = \mu_x$, for some $x \in U^*$. Then $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$ so we may apply part (2) with τ in place of ρ . We note that by Lemma 3.3(2), replacing τ by μ_x does not change the permutations μ_a , $a \in U^*$.

We first show that

$$x\gamma_{(a \cdot n)\tau^{-1}} = ((x \cdot \frac{1}{n})\gamma_{a\tau^{-1}}) \cdot n, \quad -a \cdot n \neq x \in U^*. \quad (4.3)$$

Indeed,

$$\begin{aligned} x\gamma_{(a \cdot n)\tau^{-1}} &= x\tau^{-1}\alpha_{(a \cdot n)\tau^{-1}\tau} \stackrel{(2)}{=} (x\tau^{-1} + (a\tau^{-1}) \cdot \frac{1}{n})\tau \\ &= (((x\tau^{-1}) \cdot n + a\tau^{-1}) \cdot \frac{1}{n})\tau \\ &\stackrel{(2)}{=} (((x \cdot \frac{1}{n})\tau^{-1} + a\tau^{-1})\tau) \cdot n = ((x \cdot \frac{1}{n})\gamma_{a\tau^{-1}}) \cdot n. \end{aligned}$$

It follows from Lemma 4.3(1) that,

$$\begin{aligned} x\mu_{-a \cdot n} &= (x - a \cdot n)\gamma_{(a \cdot n)\tau^{-1}}\alpha_{-a \cdot n} \stackrel{(4.3)}{=} [(x \cdot \frac{1}{n} - a)\gamma_{a\tau^{-1}}] \cdot n - a \cdot n \\ &= ([(x \cdot \frac{1}{n} - a)\gamma_{a\tau^{-1}}] - a)n = ((x \cdot \frac{1}{n})\mu_{-a}) \cdot n \stackrel{(2)}{=} (x\mu_{-a}) \cdot n^2, \end{aligned}$$

for all $x \in U^*$. Replacing $-a$ with a we get (6) for $s = n$. The case $s = n^{-1}$ follows. \square

The following two technical lemmas will be used in the proof of Proposition 4.9.

Lemma 4.7. *Let $a, b \in U^*$ such that $a \cdot 2 \neq 0$. Then for all $t \in \mathbb{Q}$ such that $a \cdot t$ is defined and non-zero, we have that,*

- (1) $-b - a \cdot t + a\mu_b \cdot \frac{1}{t} - b \cdot 2 - a \cdot t = a\mu_b \cdot \frac{1}{2t} - b \cdot 2 - a \cdot 2t + a\mu_b \cdot \frac{1}{2t} - b$;
- (2) *in particular, if $a\mu_b = -a$, then*

$$a \cdot t + b \cdot 2 + a \cdot (t + \frac{1}{t}) + b = b + a \cdot (2t + \frac{1}{2t}) + b \cdot 2 + a \cdot \frac{1}{2t}.$$

Proof. First we remark that by “ $a \cdot t$ is defined” we mean the following. Write $t = \frac{m}{n}$ with $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. Then $a \cdot t$ is defined provided that either the order of a is infinite, or the order of a is the prime p and $\gcd(n, p) = 1$. Then, by Proposition 4.6(1), $a \cdot t = (a \cdot m) \cdot \frac{1}{n}$ is well defined; see also Proposition 4.6(4).

- (1) We first observe that if $b = a \cdot r$ for some $r \in \mathbb{Q}$ such that $a \cdot r$ is defined, the statement is obvious since a and b then commute. So we may assume that $b \neq a \cdot r$ for all such r ; in particular, $a + b \neq 0$ and $a \cdot 2 + b \neq 0$.

We will compute $a\mu_{a \cdot 2 + b}$ in two different ways. On the one hand, if we replace a by $a \cdot 2$ in Lemma 4.4(3), then we get, using Proposition

4.6(2), that

$$\begin{aligned}
a\mu_{a \cdot 2+b} &= (a \cdot 2)\mu_{a \cdot 2+b} \cdot 2 \\
&= (-b - a \cdot 2 + (a \cdot 2)\mu_b - b) \cdot 2 \\
&= (-b - a \cdot 2 + a\mu_b \cdot \frac{1}{2} - b) \cdot 2 \\
&= -b - a \cdot 2 + a\mu_b \cdot \frac{1}{2} - b \cdot 2 - a \cdot 2 + a\mu_b \cdot \frac{1}{2} - b.
\end{aligned}$$

On the other hand, if we replace b by $a + b$ in Lemma 4.4(3), then we get

$$\begin{aligned}
a\mu_{a \cdot 2+b} &= a\mu_{a+(a+b)} \\
&= -(a+b) - a + a\mu_{a+b} - (a+b) \\
&= -b - a \cdot 2 - b - a + a\mu_b - b \cdot 2 - a.
\end{aligned}$$

Comparing these two expressions, we get that

$$-b - a + a\mu_b - b \cdot 2 - a = a\mu_b \cdot \frac{1}{2} - b \cdot 2 - a \cdot 2 + a\mu_b \cdot \frac{1}{2} - b.$$

Now let $t \in \mathbb{Q}$ such that $a \cdot t$ is defined and non-zero, and replace a by $a \cdot t$. Then we get, using Proposition 4.6(2), that

$$-b - a \cdot t + a\mu_b \cdot \frac{1}{t} - b \cdot 2 - a \cdot t = a\mu_b \cdot \frac{1}{2t} - b \cdot 2 - a \cdot 2t + a\mu_b \cdot \frac{1}{2t} - b.$$

(2) Assume now that $a\mu_b = -a$. Then it follows that

$$-b - a \cdot t - a \cdot \frac{1}{t} - b \cdot 2 - a \cdot t = -a \cdot \frac{1}{2t} - b \cdot 2 - a \cdot 2t - a \cdot \frac{1}{2t} - b.$$

Taking the negative of both sides gives us the required identity. \square

Lemma 4.8. *Assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$ and let $a, b \in U^*$. Then*

- (1) *If $a\mu_b = -a$, then $a\mu_c = -a$, for all $c \in \{a, -a, b, -b\}$;*
- (2) *if $a\mu_b = -a$ and $b \neq -a$, then $(b+a)\tau^{-1} + (a+b)\tau^{-1} = b\tau^{-1}$;*
- (3) *if $a\mu_b = -a$ and $b\mu_a = -b$, then $a, b \in \langle (a+b)\mu_a, (b+a)\mu_a \rangle =: T$, and a, b are conjugate in T ;*
- (4) *if $a\mu_b = -a$ and $b\mu_a = -b$, then $\langle a, b \rangle$ is nilpotent of class ≤ 2 .*

Proof. (1) This is obvious.

(2) By Lemma 4.3(1),

$$-a = a\mu_b = a\alpha_b\gamma_{-b\tau^{-1}}\alpha_b = a\alpha_b\tau^{-1}\alpha_{-b\tau^{-1}}\tau\alpha_b,$$

hence

$$\begin{aligned}
(a+b)\tau^{-1} - b\tau^{-1} &= a\alpha_b\tau^{-1}\alpha_{-b\tau^{-1}} \\
&= (-a)\alpha_{-b}\tau^{-1} = (-a-b)\tau^{-1} = -(b+a)\tau^{-1}.
\end{aligned}$$

This shows (2).

(3) Let $c \in \{-a, -b\}$. Taking in (2) $\tau = \mu_c$ we see that

$$(b+a)\mu_{-c} + (a+b)\mu_{-c} = -b,$$

by symmetry also,

$$(a+b)\mu_{-c} + (b+a)\mu_{-c} = -a.$$

It follows that $a, b \in T$. Clearly $(a+b)\mu_a + (b+a)\mu_a$ is conjugate to $(b+a)\mu_a + (a+b)\mu_a$ in T , so a and b are conjugate in T .

(4) CASE 1: The order of a and b is 2.

By Lemma 4.3(5), μ_a is conjugate in G^\dagger to α_a , so μ_a has a unique fixed point. Since both a and b are fixed points of μ_a , $a = b$ and (4) holds.

CASE 2: The order of a and b is 3.

By Lemma 4.7(2), with $t = 1$ we get $a - b - a + b = b + a - b - a$. That is b commutes with $a - b - a$. Replacing a with $-a$ (using (1)) we get that b commutes with $[a, b] = -a - b + a + b$. By symmetry also a commutes with $[a, b]$ so $\langle a, b \rangle$ is nilpotent of class ≤ 2 .

CASE 3: The order of a and b is 5.

By Lemma 4.7(2), with $t = 1$ we get

$$a + b \cdot 2 + a \cdot 2 + b = b \cdot 3 + a \cdot 3.$$

Subtracting $b \cdot 3$ from both sides of the above equality we get

$$a + b \cdot 2 + a \cdot 2 - b \cdot 2 = b \cdot 3 + a \cdot 3 - b \cdot 3.$$

It follows that

$$a = (b \cdot 3 + a \cdot 3 - b \cdot 3) + (b \cdot 2 + a \cdot 3 - b \cdot 2). \quad (\text{i})$$

Set $X = b \cdot 3 + a \cdot 3 - b \cdot 3$ and $Y = b \cdot 2 + a \cdot 3 - b \cdot 2$. Then by equation (i), $a = X + Y$ and replacing a by $-a$ in equation (i) (using (1)) we get that $-a = -X - Y$. However $-a = -Y - X$, so X and Y commute. Conjugating X and Y by $b \cdot 2$ we see that $a \cdot 3$ commutes with $b + a \cdot 3 - b$, and hence also a commutes with $b + a \cdot 3 - b = (b + a - b) \cdot 3$. Thus a commutes with $b + a - b$. Replacing b with $-b$ we see again that a commutes with $[a, b]$ and by symmetry also b commutes with $[a, b]$ so $\langle a, b \rangle$ is nilpotent of class ≤ 2 .

CASE 4: a and b are of order $p \geq 7$ or of infinite order.

Let $t \in \mathbb{Z}$ such that for each $s \in \{t, t^2 - 1, t^2 + 1\}$, $a \cdot s \neq 0$.

Replacing in Lemma 4.7(2) t with $\frac{1}{t}$ we get

$$a \cdot \frac{1}{t} + b \cdot 2 + a \cdot (t + \frac{1}{t}) + b = b + a \cdot (\frac{2}{t} + \frac{t}{2}) + b \cdot 2 + a \cdot \frac{t}{2}. \quad (\text{ii})$$

Subtracting equation (ii) from the equation in Lemma 4.7(2) we get

$$a \cdot t - a \cdot \frac{1}{t} = b + a \cdot (2t + \frac{1}{2t}) + b \cdot 2 + a \cdot (\frac{1}{2t} - \frac{t}{2}) - b \cdot 2 - a \cdot (\frac{2}{t} + \frac{t}{2}) - b.$$

or

$$\begin{aligned} -b + a \cdot t - a \cdot \frac{1}{t} + b = \\ a \cdot (2t + \frac{1}{2t}) + b \cdot 2 + a \cdot (\frac{1}{2t} - \frac{t}{2}) - b \cdot 2 - a \cdot (\frac{2}{t} + \frac{t}{2}). \end{aligned} \quad (\text{iii})$$

Replacing t with $-t$ in equation (iii) we see that

$$\begin{aligned} -(-b + a \cdot t - a \cdot \frac{1}{t} + b) = \\ -a \cdot (2t + \frac{1}{2t}) + b \cdot 2 - a \cdot (\frac{1}{2t} - \frac{t}{2}) - b \cdot 2 + a \cdot (\frac{2}{t} + \frac{t}{2}). \end{aligned} \quad (\text{iv})$$

From equations (iii) and (iv) we get

$$\begin{aligned} a \cdot (2t + \frac{1}{2t}) + b \cdot 2 + a \cdot (\frac{1}{2t} - \frac{t}{2}) - b \cdot 2 - a \cdot (\frac{2}{t} + \frac{t}{2}) = \\ -a \cdot (\frac{2}{t} + \frac{t}{2}) + b \cdot 2 + a \cdot (\frac{1}{2t} - \frac{t}{2}) - b \cdot 2 + a \cdot (2t + \frac{1}{2t}). \end{aligned} \quad (\text{v})$$

Let

$$X = a \cdot ((\frac{2}{t} + \frac{t}{2}) + (2t + \frac{1}{2t})) = a \cdot \frac{5(t^2+1)}{2t}$$

and

$$Y = b \cdot 2 + a \cdot (\frac{1}{2t} - \frac{t}{2}) - b \cdot 2.$$

Then equation (v) implies $X + Y - X = Y$. So X commutes with Y and hence, by Proposition 4.6(1), a commutes with Y . By equation (iii) it follows that a commutes with $-b + a \frac{t^2-1}{t} + b = (-b + a + b) \frac{t^2-1}{t}$, and eventually, a commutes with $-b + a + b$. Again we see that a and (by symmetry) b commutes with $[a, b]$ and $\langle a, b \rangle$ is nilpotent of class ≤ 2 . The proof of the lemma is now complete. \square

Proposition 4.9. *Let $a, b \in U^*$, then*

- (1) *if $a\mu_b = -a$ and $a + b = b + a$, then $b \in \{a, -a\}$;*
- (2) *if $b \neq -a$, $a\mu_b = -a$ and $b\mu_a = -b$, then $(a + b)\mu_{b+a} = -(a + b)$ and $(b + a)\mu_{a+b} = -(b + a)$;*
- (3) *if $a\mu_b = -a$ and $b\mu_a = -b$, then $b \in \{a, -a\}$, in particular,*
- (4) *if $\mu_b = \mu_a$, then $b \in \{a, -a\}$.*

Proof. By Proposition 3.8(1) we may (and we will) assume that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \tau^{-1})$, by taking $\tau = \mu_x$, for some $x \in U^*$.

- (1) Assume the hypotheses of (1) and that $b \neq -a$. If $b \cdot 2 \neq 0$, then by Lemma 4.8(2) and by Proposition 4.6(2),

$$(a + b)\tau^{-1} \cdot 2 = (b \cdot 2)\tau^{-1} \cdot 2.$$

By Proposition 4.6(1) we get $a + b = b \cdot 2$ so $a = b$.

If $b \cdot 2 = 0$, then from the equality $(a + b)\tau^{-1} \cdot 2 = b\tau^{-1}$, and by Lemma 4.5, we get that $(a + b)\tau^{-1} \cdot 2$ has order 2. Hence $(a + b)\tau^{-1}$ has order 4. This contradicts Proposition 4.6(4).

- (2) By Lemma 4.8(2) with $\tau = \mu_{b+a}^{-1}$ we get

$$(b+a)\mu_{b+a} + (a+b)\mu_{b+a} = b\mu_{b+a}.$$

By Lemma 4.3(2) and Lemma 4.4(3) it follows that

$$-(b+a) + (a+b)\mu_{b+a} = -a - b + b\mu_a - a = -a - b - b - a.$$

Hence $(a+b)\mu_{b+a} = -(a+b)$. By symmetry $(b+a)\mu_{a+b} = -(b+a)$.

- (3) Assume that $b \neq -a$. Set $x = (a+b)\mu_a$ and $y = (b+a)\mu_a$. Then, by (2), Proposition 3.9(2) and Lemma 4.8(1),

$$x\mu_y = (a+b)\mu_a\mu_a^{-1}\mu_{b+a}^{-1}\mu_a = (a+b)\mu_{b+a}^{-1}\mu_a = -(a+b)\mu_a = -x.$$

Similarly $y\mu_x = -y$. By Lemma 4.8(4), $\langle x, y \rangle$ is nilpotent of class ≤ 2 , and by Lemma 4.8(3), $a, b \in \langle x, y \rangle$ and a, b are conjugate in the group $\langle x, y \rangle$. But two conjugate elements in a nilpotent group of class ≤ 2 commute. Thus a and b commute, so, by (1), $b = a$.

- (4) This follows immediately from (3) because $\mu_a = \mu_b$ implies $a\mu_b = -a$ and $b\mu_a = -b$.

□

Proposition 4.10. *Let $a \in U^*$ and $k_1, k_2, m_1, m_2 \in \mathbb{Z}$ such that $0 \notin \{a \cdot k_i, a \cdot m_i\}$, for $i = 1, 2$. Set $k = \frac{k_1}{k_2}$ and $m = \frac{m_1}{m_2}$. Then*

- (1) $(a \cdot k)\mu_{a \cdot m} = -a \cdot \frac{m^2}{k}$, and hence $\mu_{a \cdot k}^{\mu_{a \cdot m}} = \mu_{a \cdot \frac{m^2}{k}}$. It follows that $(a \cdot k)\mu_{a \cdot m}^2 = a \cdot k$ and hence $\mu_{a \cdot m}^2$ centralizes $\mu_{a \cdot k}$;
- (2) if $a \cdot (k+m) \neq 0$, then $\mu_{a \cdot m^2}\mu_{a \cdot km} = \mu_{a \cdot m(k+m)}\mu_{a \cdot k(k+m)} = \mu_{a \cdot km}\mu_{a \cdot k^2}$;
- (3) if $0 \notin \{a \cdot k, a \cdot (k+1)\}$, then $\mu_a\mu_{a \cdot k} = \mu_{a \cdot N}\mu_{a \cdot kN}$ for every $N = k^\ell(k+1)^{\ell'}$ where $\ell, \ell' \in \mathbb{Z}$;
- (4) if $a \cdot 2 \neq 0$, then $\mu_{a \cdot 2}^2 = \mu_a^2$, and if $t \in \mathbb{Z}$ is such that $a \cdot t \neq 0$, then $\mu_a^2 = \mu_{a \cdot t^2}^2$;
- (5) if $a \in U^*$ is such that the order of a is finite, then $\mu_a^4 = 1$.

Proof. (1) By Proposition 4.6(2), $(a \cdot k)\mu_{a \cdot m} = (a\mu_{a \cdot m}) \cdot \frac{1}{k}$. Also, by Proposition 4.6(2) and lemma 4.3(2),

$$\begin{aligned} a\mu_{a \cdot m} &= ((a \cdot m) \cdot \frac{1}{m})\mu_{a \cdot m} \\ &= ((a \cdot m)\mu_{a \cdot m}) \cdot m = (-a \cdot m) \cdot m = -a \cdot m^2. \end{aligned}$$

This shows the first part of (1). For the second part we use Proposition 3.9(2) and lemma 3.3(1) to get

$$\mu_{a \cdot k}^{\mu_{a \cdot m}} = \mu_{(a \cdot k)\mu_{a \cdot m}}^{-1} = \mu_{-a \cdot \frac{m^2}{k}}^{-1} = \mu_{a \cdot \frac{m^2}{k}}.$$

- (2) Notice that if the order of a is finite, then, by Proposition 4.6(4), the order of a is a prime number, so by Proposition 4.6, $a \cdot k$, $a \cdot m$ are well defined as well as $a \cdot (k+m)$ and

$$a \cdot rs \neq 0 \text{ for all } r, s \in \{k, m, k+m\}.$$

By Proposition 3.10(5) we have

$$\mu_{(b\tau^{-1}-c\tau^{-1})\tau} = \mu_{-c}\mu_{c-b}\mu_b, \text{ for all } b, c \in U^*,$$

Taking $b = a \cdot k$ and $c = -a \cdot m$ and using Proposition 4.6(2), we get

$$\begin{aligned} (b\tau^{-1} - c\tau^{-1})\tau &= ((a \cdot k)\tau^{-1} + (a \cdot m)\tau^{-1})\tau \\ &= ((a\tau^{-1}) \cdot \frac{1}{k} + (a\tau^{-1}) \cdot \frac{1}{m})\tau = ((a\tau^{-1}) \cdot \frac{k+m}{km})\tau = a \cdot \frac{km}{k+m}. \end{aligned} \quad (*)$$

On the other hand, using Proposition 3.9(2) and using (1) with $k+m$ in place of k and $-m$ in place of m , we get

$$\begin{aligned} \mu_{-c}\mu_{c-b}\mu_b &= \mu_{a \cdot m}\mu_{-a(k+m)}\mu_{a \cdot k} = \mu_{(a(k+m))}\mu_{-a \cdot m}\mu_{a \cdot m}\mu_{a \cdot k} \\ &= \mu_{-a \cdot \frac{m^2}{k+m}}\mu_{a \cdot m}\mu_{a \cdot k}. \end{aligned} \quad (**)$$

By (*) and (**) we have

$$\mu_{a \cdot \frac{km}{k+m}} = \mu_{-a \cdot \frac{m^2}{k+m}}\mu_{a \cdot m}\mu_{a \cdot k},$$

or

$$\mu_{a \cdot \frac{m^2}{k+m}}\mu_{a \cdot \frac{km}{k+m}} = \mu_{a \cdot m}\mu_{a \cdot k},$$

replacing a by $a \cdot (k+m)$ we get the first equality in (2). The second equality is obtained by inverting (i.e. taking the inverses) the first equality, replacing a with $-a$ and interchanging m and k .

(3) Putting $m = 1$ in (2), we get that

$$\mu_a\mu_{a \cdot k} = \mu_{a \cdot (k+1)}\mu_{a \cdot k(k+1)} = \mu_{a \cdot k}\mu_{a \cdot k^2},$$

which shows that (iii) holds for $N = k+1$ and for $N = k$. Replacing a by $a \cdot (k+1)^{-1}$ and by $a \cdot k^{-1}$ in this equality also shows the result for $N = (k+1)^{-1}$ and for $N = k^{-1}$. The result for general $N = k^\ell(k+1)^{\ell'}$ now follows by induction.

- (4) The first equality in (4) follows from (3) by taking $k = 1$. Next, By (1) we have $\mu_a^{\mu_{a \cdot t}} = \mu_{a \cdot t^2}$. Hence since μ_a^2 centralizes $\mu_{a \cdot t}$ (by (1)), $\mu_a^2 = (\mu_a^2)^{\mu_{a \cdot t}} = \mu_{a \cdot t^2}^2$.
- (5) Let $a \in U^*$ be an element of finite order p and note that p is a prime by Proposition 4.6(4). If $p = 2$, then $\mu_a = \mu_{-a} = \mu_a^{-1}$, so $\mu_a^2 = 1$. So assume that $p > 2$.

Suppose first that -1 is a square modulo p and let $t \in \mathbb{Z}$ such that $t^2 \equiv -1 \pmod{p}$. Then, by (4), $\mu_a^2 = \mu_{a \cdot t^2}^2 = \mu_{-a}^2$ and (5) follows.

So we may assume that -1 is a non-square modulo p . Now let $t \in \text{GF}(p)$ such that t is a square in $\text{GF}(p)$, but $t+1$ is not a square. Note that since -1 is not a square in $\text{GF}(p)$, and $t+1$ is a non-square, the order of $t+1$ in the multiplicative group of $\text{GF}(p)$ must be even so there exists an $\ell_0 \in \mathbb{Z}$ such that $(t+1)^{\ell_0} = -1$ in $\text{GF}(p)$.

Taking $\ell = 0$ and $\ell' = \ell_0$ in (3), we get that

$$\mu_a\mu_{a \cdot t} = \mu_{-a}\mu_{-a \cdot t},$$

or $\mu_{-a}^2 = \mu_{a,t}^2$. Since t is a square in $\text{GF}(p)$, it follows from (4) that $\mu_{a,t}^2 = \mu_a^2$, and we conclude that $\mu_{-a}^2 = \mu_a^2$ and therefore again $\mu_a^4 = 1$. \square

5. PROVING (QJ2)

In this section we assume that $\mathbb{M}(U, \tau)$ is a special Moufang set with U an abelian group, and that $\tau = \mu_e$, $e \in U^*$ (but e will occasionally vary). Note that by Lemma 5.1 (below), τ is an involution. Also, by Lemma 3.8(1) $\mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_{e'})$, for all $e' \in U^*$.

By Theorem 3.5, $h_a \in \text{Aut}(U)$, for all $a \in U^*$; we wish to show that under certain conditions, $\mathcal{U}_e := (U, \mathcal{H}, e)$ is a quadratic Jordan division algebra, where $\mathcal{H}: x \mapsto h_x := \mu_e \mu_x$, for $x \in U$. Of course \mathcal{U}_e depends on e , because the Hua-maps $h_a = \mu_e \mu_a$ depend on e . We call \mathcal{U}_e an *isotope*.

Lemma 5.1. *Let $a \in U^*$, then $\mu_a = \mu_{-a}$ and hence μ_a is an involution.*

Proof. We use condition (*) of Definition 4.1. By Lemma 4.3(1) (and Notation 3.2(1)), $\mu_a = \alpha_a \tau^{-1} \alpha_{a\tau^{-1}}^{-1} \tau \alpha_a$, and hence

$$x\mu_a = ((x+a)\tau^{-1} - a\tau^{-1})\tau + a$$

for all x . Using condition (*), we see that $(-x)\mu_{-a} = -x\mu_a$, so by Lemma 4.2 it follows that $x\mu_{-a} = x\mu_a$ for all x , and hence $\mu_{-a} = \mu_a$. But by Lemma 3.3(1), $\mu_{-a} = \mu_a^{-1}$ so μ_a is an involution. \square

Proposition 5.2. *Let $a, b \in U^*$ and let $g \in G_{\{0, \infty\}}^\dagger$. Then*

- (1) $h_a = h_{-a}$;
- (2) $g^{-1}\mu_a g = \mu_{ag}$;
- (3) $h_{a\tau} = h_a^{-1}$;
- (4) $h_a h_b h_a = h_{bh_a}$;
- (5) $\mu_a = \mu_b$ if and only if $a \in \{b, -b\}$;
- (6) g centralizes μ_a if and only if $ag \in \{a, -a\}$.

Proof. (1) By Lemma 5.1, $\mu_a = \mu_{-a}$, and hence by Proposition 3.9(1), $h_a = \tau\mu_a = \tau\mu_{-a} = h_{-a}$.

(2) This follows from Lemma 5.1 and Proposition 3.9(2).

(3) By (2) and Proposition 3.9(1), $h_{a\tau} = \tau\mu_{a\tau} = \tau\tau\mu_a\tau = \mu_a\tau = h_a^{-1}$, because τ is an involution.

(4) By (1), (3) and Proposition 3.9(3), $h_a h_b h_a = h_{-b} h_{a\tau}^{-1} h_b = h_b h_a h_b$.

(5) Assume $\mu_a = \mu_b$. Then, by Lemma 4.3(2), $a\mu_b = a\mu_a = -a$, so $b \in \{a, -a\}$ by Lemma 4.9(1).

(6) If $ag \in \{a, -a\}$, then, by Lemma 5.1 and by part (2), $\mu_a = \mu_{ag} = g^{-1}\mu_a g$. Conversely, suppose $\mu_a = g^{-1}\mu_a g = \mu_{ag}$. Then by (5), $ag \in \{a, -a\}$. \square

Notation 5.3. By Proposition 4.6(5), U is a vector space over \mathbb{Q} or over $\text{GF}(p)$, for some prime p . In the first case we write $\text{char}(U) = 0$ and in the second $\text{char}(U) = p$. Let \mathbb{F} always denote \mathbb{Q} or $\text{GF}(p)$ in the respective cases. As usual we will multiply elements of U by scalars from \mathbb{F} on the right.

Proposition 5.4. *If $\text{char}(U) \notin \{2, 3\}$, then \mathcal{U} is a quadratic Jordan division algebra if and only if condition (QJ2) is satisfied, i.e., if and only if*

$$ah_{c,b}h_a = ch_{a,bh_a} \quad \text{for all } a, b, c \in U. \quad (5.1)$$

Proof. Recall that condition (QJ2) says

$$h_x V_{x,y} = V_{y,x} h_x,$$

where

$$h_{x,y} = h_{x+y} - h_x - h_y \quad \text{and} \quad zV_{x,y} = yh_{x,z}.$$

Hence $bh_a V_{a,c} = ch_{a,bh_a}$ and $bV_{c,a}h_a = ah_{c,b}h_a$, and therefore (QJ2) can be rewritten as the identity (5.1).

Note that by Proposition 3.9(1), $h_e = \text{id}_U$, and by Proposition 5.2(4), \mathcal{U} satisfies (QJ3). So suppose that \mathcal{U} also satisfies (QJ2). Then, replacing c by $c+d$ in equation (5.1) and using the fact that h_a and $h_{x,y}$ are endomorphisms of U , we get that $ah_{c+d,b} = ah_{c,b} + ah_{d,b}$ for all $a, b, c, d \in U$, i.e. the map $(x, y) \mapsto h_{x,y}$ is biadditive. Since $h_{a \cdot s} = h_a \cdot s^2$ for all $s \in \mathbb{F}$ by Proposition 4.6(6), this implies that the map $x \mapsto h_x$ is a quadratic map from U to $\text{End}_{\mathbb{F}}(U)$. Since the base field \mathbb{F} has at least 5 elements, the identities (QJ1), (QJ2) and (QJ3) automatically hold strictly, and hence \mathcal{U} is a quadratic Jordan algebra. Finally, by definition, every map h_a (with $a \neq 0$) is a permutation of X so it is invertible (with inverse map $h_{a\tau}$); therefore, \mathcal{U} is a quadratic Jordan division algebra. \square

The following proposition and the corollary following it give some useful identities which are equivalent to (QJ2).

Proposition 5.5. *The following statements are equivalent:*

- (i) (QJ2) holds;
- (ii) $a\tau(\mu_{b+c} - \mu_b - \mu_c)\tau\mu_a = c\tau(\mu_{a+b\tau\mu_a} - \mu_a - \mu_{b\tau\mu_a})$ for all $a, b, c \in U^*$;
- (iii) $(-a)(\mu_{b+c} - \mu_b - \mu_c) = c\mu_a(\mu_{a+b} - \mu_a - \mu_b)$ for all $a, b, c \in U^*$.

Proof. By the above, (QJ2) is equivalent to the identity (5.1), and since $h_x = \tau\mu_x$, for all $x \in U^*$, it follows that $h_{x,y} = \tau(\mu_{x+y} - \mu_x - \mu_y)$ so it is clear that (i) and (ii) are equivalent.

Let $\rho = \mu_{e'}$, for some $e' \in U^*$. Then $\rho\tau \in \text{Aut}(U)$. Replacing a by $a\rho\tau$ in (ii) and using Proposition 5.2(2), we get

$$\begin{aligned} & a\rho(\mu_{b+c} - \mu_b - \mu_c)\tau\mu_{a\rho\tau} = c\tau(\mu_{a\rho\tau+b\tau\mu_{a\rho\tau}} - \mu_{a\rho\tau} - \mu_{b\tau\mu_{a\rho\tau}}) \\ \iff & a\rho(\mu_{b+c} - \mu_b - \mu_c)\rho\mu_{a\rho\tau} = c\tau(\mu_{a\rho\tau+b\rho\mu_{a\rho\tau}} - \mu_{a\rho\tau} - \mu_{b\rho\mu_{a\rho\tau}}) \\ \iff & a\rho(\mu_{b+c} - \mu_b - \mu_c)\rho\mu_{a\rho\tau} = c\rho(\mu_{a+b\rho\mu_a} - \mu_a - \mu_{b\rho\mu_a})\rho\tau \\ \iff & a\rho(\mu_{b+c} - \mu_b - \mu_c)\rho\mu_a = c\rho(\mu_{a+b\rho\mu_a} - \mu_a - \mu_{b\rho\mu_a}), \end{aligned}$$

which is (ii) with ρ in place of τ . This implies that (ii) is independent of the choice of $e \in U^*$ (i.e. if it holds for $\tau = \mu_e$, for some $e \in U^*$, then it holds for $\tau = \mu_x$, for all $x \in U^*$). Taking $\tau = \mu_a$ in (ii) we get that (ii) implies (iii).

We now show that (iii) implies (ii). So assume that (iii) holds. Then by (iii) with $-a\tau$ in place of a , we have, using Lemma 5.1,

$$(a\tau)(\mu_{b+c} - \mu_b - \mu_c) = c\mu_{a\tau}(\mu_{-a\tau+b} - \mu_{a\tau} - \mu_b), \text{ for all } a, b, c \in U^*. \quad (5.2)$$

By Proposition 3.9(2) and since τ is an involution, we get that $\mu_{a\tau} = \tau\mu_a\tau$, and note that we also get $\mu_a\tau\mu_x\tau\mu_a = \mu_{x\tau\mu_a}$, for all $x \in U^*$. Thus by equation (5.2) and again using Lemma 5.1, we have that for all $a, b, c \in U^*$,

$$\begin{aligned} (a\tau)(\mu_{b+c} - \mu_b - \mu_c)\tau\mu_a &= c\tau\mu_a\tau(\mu_{-a\tau+b} - \mu_{a\tau} - \mu_b)\tau\mu_a \\ &= c\tau(\mu_{(-a\tau+b)\tau\mu_a} - \mu_{(a\tau)\tau\mu_a} - \mu_{b\tau\mu_a}) \\ &= c\tau(\mu_{-a\mu_a+b\tau\mu_a} - \mu_{a\mu_a} - \mu_{b\tau\mu_a}) \\ &= c\tau(\mu_{a+b\tau\mu_a} - \mu_a - \mu_{b\tau\mu_a}). \end{aligned}$$

But this is the equality (ii), so we see that (iii) implies (ii). \square

Corollary 5.6. *If the identity $eh_{b,c} = ch_{b,e}$, for all $b, c \in U^*$, holds in each isotope \mathcal{U}_e , $e \in U^*$, then the stronger identity (QJ2) holds for each isotope \mathcal{U}_e , $e \in U^*$.*

Proof. Notice that the identity $eh_{b,c} = ch_{b,e}$, is precisely the identity in (iii) of Proposition 5.5, with the letter a replaced by the letter e (and hence $\tau = \mu_a$), so the corollary holds by Proposition 5.5. \square

Lemma 5.7. *For all $a, b \in U^*$ such that $b \neq -a$, we have that*

- (1) $b\mu_{a+b} = -a \cdot 2 - b + b\mu_a$;
- (2) $b\tau h_{a,b} = -a \cdot 2$.

Proof. (1) This comes from Lemma 4.4(3), because U is abelian.

(2) Using (1) and Lemma 4.3(2), we get that

$$\begin{aligned} b\tau h_{a,b} &= b\mu_{a+b} - b\mu_a - b\mu_b \\ &= -a \cdot 2 - b + b\mu_a - b\mu_a + b \\ &= -a \cdot 2. \end{aligned}$$

\square

Proposition 5.8. *Let $a, b \in U^*$ and let $c = (a\tau + b\tau)\tau$, then*

- (1) $\mu_a \mu_{a+b} \mu_b = \mu_c = \mu_b \mu_{a+b} \mu_a$;
- (2) $h_a h_{a\tau, b\tau} h_b = h_{a,b} = h_b h_{a\tau, b\tau} h_a$;
- (3) $\mu_a \mu_b$ commutes with $\mu_a \mu_{a+b}$, so h_b commutes with h_{b+e} ;
- (4) $h_{a,a} = h_a \cdot 2$;
- (5) $ah_{a,e} = eh_{a,a}$.

Proof. (1) This follows from Proposition 3.10(5), recalling that τ and μ_x , $x \in U^*$ are involutions, that U is abelian and that $\mathbb{M}(U, \tau)$ is special.

- (2) Since the maps μ_x are involutions, the left equality of (1) can be rewritten as

$$\mu_a^{-1} \mu_{a+b} = \mu_c^{-1} \mu_b;$$

since $h_x = \tau \mu_x$ for all x , this is equivalent with

$$h_a^{-1} h_{a+b} = h_c^{-1} h_b.$$

Replacing $a \leftrightarrow a\tau$ and $b \leftrightarrow b\tau$ and using Proposition 5.2(3), we get that

$$h_a h_{a\tau+b\tau} h_b = h_{a+b}.$$

Using Proposition 5.2(3) twice more, this implies that

$$h_a h_{a\tau, b\tau} h_b = h_{a,b}.$$

The other equality of (2) is similar.

- (3) By (1),

$$\mu_a \mu_b \mu_{a+b} \mu_a = \mu_{a+b} \mu_b.$$

Multiplying this equality on the left by $\mu_a \mu_{a+b}$ we get

$$(\mu_a \mu_b)^{\mu_{a+b} \mu_a} = \mu_a \mu_b.$$

This shows the first part of (3). Taking $a = e$ and using Proposition 3.9(1) gives the second part.

- (4) $h_{a,a} = h_{a \cdot 2} - h_a \cdot 2$, so (4) follows from Proposition 4.6(6).
 (5) Since $h_{a,a} = h_a \cdot 2$, and $\tau = \mu_e$ we must show that

$$a \mu_b (\mu_{a+b} - \mu_a - \mu_b) = b \mu_b \mu_a \cdot 2;$$

applying $\mu_a \mu_b$ to this equality and noticing that by (3) $\mu_a \mu_b = (\mu_b \mu_a)^{-1}$ commutes with $\mu_b \mu_{a+b}$, we must show that

$$a \mu_a \mu_{a+b} - a - a \mu_a \mu_b = b \cdot 2.$$

But by Lemma 5.7(1), $a \mu_a \mu_{a+b} = -(a \mu_{a+b}) = -(-b \cdot 2 - a + a \mu_b)$, so we get

$$a \mu_a \mu_{a+b} - a - a \mu_a \mu_b = b \cdot 2 + a - a \mu_b - a + a \mu_b = b \cdot 2.$$

□

Lemma 5.9. *Assume that $h_{-a,b} = -h_{a,b}$ for all $a, b \in U$. Then*

- (1) $h_{a,b \cdot s} = h_{a,b} \cdot s$;
- (2) $h_{a+b \cdot s} = h_a + h_{a,b} \cdot s + h_b \cdot s^2$;

for all $a, b \in U$ and all $s \in \mathbb{F}$.

Proof. We first show that

$$h_{a,a+b} = h_a \cdot 2 + h_{a,b} \quad (5.3)$$

for all $a, b \in U$. Indeed, using the fact that $h_{-a,b} = -h_{a,b}$ for all $a, b \in U$ and using Proposition 5.8(4), and Lemma 5.2(1) we get

$$\begin{aligned} h_{a,a+b} &= -h_{-a,a+b} = -h_b + h_a + h_{a+b} \\ &= -h_b + h_a + h_{a,b} + h_a + h_b = h_a \cdot 2 + h_{a,b}. \end{aligned}$$

We now show that for all $a, b \in U$ and all $n \in \mathbb{Z}$,

$$h_{a \cdot n, b} = h_{a,b} \cdot n. \quad (5.4)$$

Since $h_{-a,b} = -h_{a,b}$ for all $a, b \in U$, we may assume that $n > 0$, and we will use induction on n . The statement is obvious for $n = 1$, so assume that it holds for $n = k$ (for all $a, b \in U$). Then, using equation (5.3) and Proposition 4.6(6), we get that

$$\begin{aligned} h_{a \cdot (k+1), b} &= h_{a \cdot (k+1) + b} - h_{a \cdot (k+1)} - h_b \\ &= h_{a \cdot k + (a+b)} - h_a \cdot (k+1)^2 - h_b \\ &= h_{a \cdot k, (a+b)} + h_{a \cdot k} + h_{a+b} - h_a \cdot (k+1)^2 - h_b \\ &= h_{a, a+b} \cdot k + h_a \cdot k^2 + h_{a,b} + h_a + h_b - h_a \cdot (k+1)^2 - h_b \\ &= h_a \cdot 2k + h_{a,b} \cdot k + h_a \cdot k^2 + h_{a,b} + h_a - h_a \cdot (k+1)^2 \\ &= h_{a,b} \cdot (k+1), \end{aligned}$$

which shows the statement for $n = k + 1$. Hence equation (5.4) holds; this implies (1). It now follows from (1) and Proposition 4.6(6) that also (2) holds. \square

Lemma 5.10. *Let $a, b, c, d \in U$. Then*

- (1) $ah_{b+c,d} = ah_{b,d} + ah_{c,d} \iff ah_{b,c+d} = ah_{b,c} + ah_{b,d}$;
- (2) $ah_{b,c+a\tau} = ah_{b,c} - b \cdot 2$.

Proof. (1) Both sides can be rewritten as

$$a(h_{b+c+d} + h_b + h_c + h_d - h_{b+c} - h_{b+d} - h_{c+d}) = 0,$$

and hence they are equivalent.

- (2) This follows from (1) with $d = a\tau$ using Lemma 5.7(2). \square

Theorem 5.11. *Assume that $\text{char}(U) \notin \{2, 3\}$, and that*

- (i) $h_{-a,b} = -h_{a,b}$ for all $a, b \in U$;
- (ii) $ah_{a,b+c} = ah_{a,b} + ah_{a,c}$ for all $a, b, c \in U$.

Then \mathcal{U} satisfies (QJ2). It follows that \mathcal{U} is a quadratic Jordan division algebra.

Proof. First notice that assumption (ii) together with Lemma 5.10(1) implies that

$$ah_{a+c,b} = ah_{a,b} + ah_{c,b} \quad \text{for all } a, b, c \in U. \quad (5.5)$$

We start with the identity $h_{a+e}h_a = h_a h_{a+e}$ from Proposition 5.8(3). We substitute $a + b \cdot s$ for a in this identity, where $s \in \mathbb{F}$; using Lemma 5.9(2), we then get that

$$\begin{aligned} (h_{a+e} + h_{a+e,b} \cdot s + h_b \cdot s^2)(h_a + h_{a,b} \cdot s + h_b \cdot s^2) \\ = (h_a + h_{a,b} \cdot s + h_b \cdot s^2)(h_{a+e} + h_{a+e,b} \cdot s + h_b \cdot s^2) \end{aligned}$$

for all $a, b \in U$. Since $\text{char}(U) = 0$ or $\text{char}(U) \geq 5$, we can take at least 5 different values for s , and hence the coefficients of each power of s have to coincide (see, for example, [TW, (2.26)]). Equating the coefficients of s^1 , we get

$$h_{a+e,b}h_a + h_{a+e}h_{a,b} = h_a h_{a+e,b} + h_{a,b}h_{a+e}.$$

We now apply this identity to the element $a\tau$, and we get, using Lemma 5.7(2) and Lemma 4.3(2), that

$$a\tau h_{a+e,b}h_a + a\tau h_{a+e}h_{a,b} = -ah_{a+e,b} - bh_{a+e} \cdot 2. \quad (5.6)$$

By Lemma 5.10(2) with $a\tau$ in place of a and e in place of c , we get that

$$a\tau h_{a+e,b}h_a = a\tau h_{b,e}h_a - bh_a \cdot 2. \quad (5.7)$$

Also, using Lemma 5.7(2) and Lemma 4.3(2), we get that

$$a\tau h_{a+e}h_{a,b} = a\tau(h_a + 1 + h_{a,e})h_{a,b} = -ah_{a,b} - b \cdot 2 - eh_{a,b} \cdot 2. \quad (5.8)$$

It follows from equation (5.5) that

$$-ah_{a+e,b} = -ah_{a,b} - ah_{e,b}; \quad (5.9)$$

by definition, the equation

$$-bh_{a+e} \cdot 2 = -bh_a \cdot 2 - b \cdot 2 - bh_{a,e} \cdot 2. \quad (5.10)$$

also holds. If we plug in the equations (5.7), (5.8), (5.9) and (5.10) into (5.6), then we get that

$$a\tau h_{b,e}h_a - eh_{a,b} \cdot 2 = -ah_{e,b} - bh_{a,e} \cdot 2. \quad (5.11)$$

On the other hand, if we replace a by $a + b$ in the identity $eh_a \cdot 2 = ah_{a,e}$, which follows from Proposition 5.8(4 and 5), then we get using equation (5.5)

$$\begin{aligned} eh_{a+b} \cdot 2 &= (a + b)h_{a+b,e} \\ &= ah_{a+b,e} + bh_{a+b,e} \\ &= ah_{a,e} + ah_{b,e} + bh_{a,e} + bh_{b,e} \\ &= eh_a \cdot 2 + ah_{b,e} + bh_{a,e} + eh_b \cdot 2 \end{aligned}$$

and hence

$$eh_{a,b} \cdot 2 = ah_{b,e} + bh_{a,e}. \quad (5.12)$$

If we plug this in into equation (5.11), then we get that

$$a\tau h_{b,e}h_a = -bh_{a,e};$$

replacing a by $a\tau$ then gives

$$ah_{b,e} = -bh_{a\tau,e}h_a. \quad (5.13)$$

By Proposition 5.8(2) with $b = e$, since $e\tau = -e$ and by our assumption (i), we have that $h_{a\tau,e}h_a = -h_{a,e}$. Hence identity (5.13) becomes

$$ah_{b,e} = bh_{a,e}.$$

Together with equation (5.12) and the fact that $\text{char}(U) \neq 2$, this shows that $eh_{a,b} = bh_{a,e}$ for all a, b . By Corollary 5.6, we can conclude that (QJ2) holds, and hence, by Proposition 5.4, \mathcal{U} is a quadratic Jordan division algebra. \square

Corollary 5.12. *Assume that the map $(x, y) \mapsto h_{x,y}$ is biadditive and that $\text{char}(U) \notin \{2, 3\}$. Then \mathcal{U} is a quadratic Jordan division algebra.*

Proof. If the map $(x, y) \mapsto h_{x,y}$ is biadditive, then the conditions (i) and (ii) in Theorem 5.11 are satisfied, so the result follows from that theorem. \square

REFERENCES

- [DW] T. De Medts, R.M. Weiss, Moufang sets and Jordan division algebras, *Math. Ann.*, to appear.
- [Mc1] K. McCrimmon, A general theory of Jordan rings, *Proc. Nat. Acad. Sci. U.S.A.* **56** (1966), 1072–1079.
- [Mc2] K. McCrimmon, *A taste of Jordan algebras*, Springer-Verlag, Berlin, Heidelberg, New York, 2004.
- [SW] Y. Segev, R.M. Weiss, *On the action of the Hua subgroups in special Moufang sets*, preprint, 2005.
- [T] F. Timmesfeld, *Abstract root subgroups and simple groups of Lie type*, Birkhäuser-Verlag, *Monographs in Mathematics* **95** Basel, Berlin, Boston, 2001.
- [Ti] J. Tits, *Twin buildings and groups of Kac-Moody type*, in *Groups, combinatorics & geometry (Durham, 1990)*, 249–286, London Math. Soc. Lecture Note Ser. **165**, Cambridge Univ. Press, Cambridge, 1992.
- [TW] J. Tits, R.M. Weiss, *Moufang Polygons*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York, 2002.

TOM DE MEDTS, DEPARTMENT OF PURE MATHEMATICS AND COMPUTER ALGEBRA,
GHENT UNIVERSITY, KRIJGSLAAN 281 S22, 9000 GENT, BELGIUM
E-mail address: `tdemedts@cage.ugent.be`

YOAV SEGEV, DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY, BEER-SHEVA 84105, ISRAEL
E-mail address: `yoavs@math.bgu.ac.il`