Innovations in Incidence Geometry
Volume 9 (2009), Pages 79–122
ISSN 1781-6475

A course on Moufang sets

Tom De Medts* Yoav Segev†

Abstract

A Moufang set is essentially a doubly transitive permutation group such that the point stabilizer contains a normal subgroup which is regular on the remaining points. These regular normal subgroups are called the *root groups* and they are assumed to be conjugate and to generate the whole group.

Moufang sets play an significant role in the theory of buildings, they provide a tool to study linear algebraic groups of relative rank one, and they have (surprising) connections with other algebraic structures.

In these course notes we try to present the current approach to Moufang sets. We include examples, connections with related areas of mathematics and some proofs where we think it is instructive and within the scope of these notes.

Keywords: Moufang sets, BN-pairs, rank one groups, algebraic groups, Jordan algebras
MSC 2000: 20E42, 51E24, 17C30, 20G15, 20B22

Contents

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

†Partially supported by the research group “Incidence Geometry” of Ghent University and by BSF grant no. 2004-083.

Introduction

A Moufang set is essentially a doubly transitive permutation group G such that the point stabilizer contains a normal subgroup which is regular on the remaining points. These regular normal subgroups are called the *root groups* and they are assumed to be conjugate and to generate G. (The root groups are *not* assumed to be nilpotent.)

J. Tits introduced this notion in the context of twin buildings, but it is in fact a tool to study absolutely simple algebraic groups of relative rank one; the Moufang sets are precisely the Moufang buildings of rank one. It turns out that this notion is related to other algebraic structures as well.

In these notes, we try to give the reader a sense of the "modern" approach to Moufang sets. We include examples and connections to related areas of mathematics; we provide detailed proofs where we think they could offer more insight into the theory, but for the same reason, we have omitted many details that can be found elsewhere and which are beyond the scope of this manuscript.

These notes have been used for a mini-course given by both authors, on the conference "Buildings and Groups" which took place in Ghent (Belgium), May 20–26, 2007. Our references for the material in this mini-course are [DS], [DS2], [DST], [DW], [S] and [SW] (we give more precise references at the beginning of the relevant sections).

We thank Pierre-Emmanuel Caprace, Shripad Garge, Max Horn, Guy Rousseau and Richard Weiss for valuable comments on an earlier version of this manuscript.

1 Definition of a Moufang set

1.1 Notation

We start by fixing some standard notation.

Notation 1.1.1. Let G be a group and p a prime.

(1) For $x, y \in G$, $x^y := y^{-1}xy$ and $[x, y] := x^{-1}y^{-1}xy$.

(2) When we write an inequality sign $H \leq G$, we always mean that H is a *subgroup* of G (while $S \subseteq G$ means that S is a *subset* of G).

(3) For $S \subseteq G$, $\langle S \rangle$ is the subgroup generated by S.

(4) For a set S we let $|S|$ be the cardinality of S.

(5) For an element $g \in G$, $|g|$ denotes the order of G.

(6) G^* denotes the set of nontrivial elements of G.

(7) $\mathrm{Inv}(G)$ denotes the set of involutions of G (so $1 \notin \mathrm{Inv}(G)$).

Let G be a permutation group on a set Ω, let $Y \subseteq \Omega$ and let $x_1, \ldots, x_n \in \Omega$.

(8) We write G_Y for the pointwise stabilizer of Y in G and we write $G_{\{Y\}}$ for the global stabilizer of Y in G. However when the elements of Y are given, e.g. when $Y = \{x_1, \ldots, x_n\}$, then we write $G_{x_1,\ldots,x_n}$ for G_Y and $G_{\{x_1,\ldots,x_n\}}$ for $G_{\{Y\}}$.

(9) We apply permutations on the right, i.e. for $x \in \Omega$ and $g \in G$, we write xg for the image of x under g; moreover, for $g \in G_{\{Y\}}$ we write $C_Y(g) := \{y \in Y \mid yg = y\}$.

1.2 Definition of a Moufang set

A Moufang set is a set X (with $|X| \geq 3$) together with a collection of groups $\{U_x \mid x \in X\}$ satisfying the following two properties.

$\mathbb{M}_1$. For each $x \in X$, $U_x \leq \mathrm{Sym}(X)$ fixes x and acts regularly (i.e. sharply transitively) on $X \setminus \{x\}$.

$\mathbb{M}_2$. For all $x \in X$, U_x permutes the set $\{U_y \mid y \in X\}$ by conjugation.

The Moufang set is then denoted $\mathbb{M} = (X, (U_x)_{x\in X})$; the groups U_x are called the *root groups* of $\mathbb{M}$, and the group $G := \langle U_x \mid x \in X\rangle$ is called the *little projective group* of $\mathbb{M}$.

Note that this implies that G acts doubly transitively on X, and that $U_x^\varphi = U_{x\varphi}$ for all $x \in X$ and all $\varphi \in G$.

2 Motivation and situation

2.1 Connection with BN-pairs of rank one

There are several equivalent definitions of a split BN-pair of rank one. The one we choose is the most common. We refer to Definition 2.3.1 below for a definition of a BN-pair of arbitrary rank.

Definition 2.1.1. A *BN-pair of rank one* in a group G is a system (B, N) consisting of two subgroups B and N such that

BN_1. $G = \langle B, N\rangle$.

BN_2. $H := B \cap N \trianglelefteq N$.

BN$_3$. There is an element $\omega \in N \setminus H$ with $\omega^2 \in H$ such that $N = \langle H, \omega \rangle$, $G = B \cup B\omega B$ and $\omega B \omega \neq B$.

The BN-pair is called *split*, if in addition the following axiom holds.

BN$_4$. There exists a normal subgroup[1] $U \trianglelefteq B$ such that $B = U \rtimes H$.

Any BN-pair (possibly non-split) is called *saturated*, if it also satisfies the following axiom. Note that we always have $H \leq B \cap B^\omega$.

BN$_5$. $H = B \cap B^\omega$.

Remark 2.1.2. If a BN-pair (B, N) for G is not saturated, then $(B, N(B \cap B^\omega))$ is a saturated BN-pair. However, if (B, N) is split but not saturated, then its saturation $(B, N(B \cap B^\omega))$ might be non-split.

Proposition 2.1.3. *Let G be a group with a saturated split BN-pair of rank one, and let B, N, H, U and ω be as in Definition 2.1.1. Let*

$$X := \{U^g \mid g \in G\}$$

be the set of conjugates of U in G. For any $x \in X$, denote the corresponding subgroup of G (which is just x itself!) by V_x. Then $(X, (V_x)_{x \in X})$ is a Moufang set.

Proof. It is clear that each V_x acts on X by conjugation. We have to check whether the defining conditions $\mathbb{M}_1$ and $\mathbb{M}_2$ are satisfied. Condition $\mathbb{M}_2$ is clear, since each conjugate of U is mapped, by conjugation, to some conjugate of U.

We claim that $N_G(U) = B$. Indeed, by BN$_4$, B normalizes U. So suppose that $U^g = U$ for some $g \in G \setminus B$. Then by BN$_3$, $g = a\omega b$ for some $a, b \in B$, and hence $U^{a\omega b} = U$, implying $U^\omega = U$. But since ω normalizes H, this would imply $B^\omega = B$, contradicting the last statement of BN$_3$.

We now proceed to show property $\mathbb{M}_1$. Let $x \in X$ be arbitrary, and write $V_x = x = U^g$. It is obvious that each V_x fixes x (i.e. itself) by conjugation. Assume that some element $v \in V_x$ fixes some $y \in X$, say $y = U^h$. Write $v = g^{-1}ug$ with $u \in U$; then $c := hg^{-1}ugh^{-1}$ normalizes U, i.e. $c \in B$, and hence $c \in B \cap U^{gh^{-1}}$. Suppose that $y \neq x$, i.e. $gh^{-1} \notin B$, and use BN$_3$ to write $gh^{-1} = a\omega b$ with $a, b \in B$. Then $B \cap U^{gh^{-1}} \neq 1$ implies $B^\omega \cap U \neq 1$. But by BN$_5$, this would yield $U \cap H \neq 1$, contradicting BN$_4$. We conclude that V_x acts semi-regularly on $X \setminus \{x\}$.

Observe that $U^\omega \neq U$ implies $U \neq 1$; let $u \in U^*$. Then the three groups U, U^ω and $U^{\omega u}$ are pairwise distinct; hence $|X| \geq 3$.

[1] Some authors also require this subgroup to be *nilpotent* as part of the definition.

We now claim that

$$G = B \cup B\omega U\,. \tag{2.1}$$

Indeed, we have $H^\omega = H$ and hence $H = H^\omega \leq B^\omega$. It follows that $\omega H \subseteq B\omega$ and therefore $B\omega HU \subseteq B\omega U$. Since $HU = B$, we get $B\omega B = B\omega U$, and the claim follows.

It remains to show that V_x is transitive on $X \setminus \{x\}$. Since G is transitive by conjugation on X it suffices to show that U is transitive via conjugation on $X \setminus \{U\}$. It thus suffices to show that $X \setminus \{U\} = \{U^{\omega u} \mid u \in U\}$, but this is immediate from (2.1). □

Remark 2.1.4. The group G might be a non-trivial extension of the little projective group of the Moufang set. For example, if $G = \mathsf{SL}_2(k)$, then the little projective group of the corresponding Moufang set will be $\mathsf{PSL}_2(k)$. The crucial observation here is that, even though the groups U^g act faithfully on X and $G = \langle U^g \mid g \in G\rangle$, it might be that G does not act faithfully. In other words, if ψ_x is the natural injection from V_x into $\mathrm{Sym}(X)$ for each $x \in X$, then the induced map ψ from G to $\mathrm{Sym}(X)$ might not be injective.

We now consider the converse.

Proposition 2.1.5. *Let $\mathbb{M} = (X, (U_x)_{x\in X})$ be an arbitrary Moufang set, with little projective group G. Let $0, \infty$ be two arbitrary elements of X, let $B := G_\infty$, $N := G_{\{0,\infty\}}$, $H := G_{0,\infty}$ and $U := U_\infty$ (i.e. the root group corresponding to ∞), and let ω an element of G interchanging 0 and ∞. (Such elements ω always exist because G is doubly transitive.) Then B, N, ω and U satisfy all the axioms of a saturated split BN-pair of rank one.*

Proof. It is straightforward to check conditions BN_1, BN_2, BN_4 and BN_5. To prove BN_3, let $g \in G \setminus B$ be arbitrary, and let $x := \infty g \neq \infty$. Let u be the unique element of U_∞ mapping 0 to x, and let $b := gu^{-1}\omega^{-1}$. Then $\infty b = \infty$, hence $b \in B$ and $g = b\omega u \in B\omega B$. Moreover, $\omega B\omega = B^\omega = G_0 \neq B$. □

2.2 Connection with abstract rank one groups

The notion of abstract rank one groups was introduced by Franz Timmesfeld [Tim].

Definition 2.2.1. A group G is called an *abstract rank one group* with *unipotent subgroups* U and V, if $G = \langle U, V\rangle$, U and V are two distinct nilpotent subgroups of G, and

$(*)$ for each $u \in U^*$, there exists an element $v \in V^*$ such that $U^v = V^u$, and vice-versa.

Every Moufang set with nilpotent root groups gives rise in a natural way to an abstract rank one group:

Proposition 2.2.2. *Let $\mathbb{M} = (X, (U_x)_{x \in X})$ be a Moufang set with little projective group G, and assume that the root groups U_x are nilpotent. Let $0, \infty \in X$ be two arbitrary elements. Then $G = \langle U_\infty, U_0 \rangle$ is an abstract rank one group with unipotent subgroups U_∞ and U_0.*

Proof. Let $a \in U_\infty^*$ be arbitrary, and let $x := 0a \neq 0$. Then by $\mathbb{M}_2$, $U_0^a = U_{0a} = U_x$. Let b be the (unique) element of U_0 mapping ∞ to x. Then $U_\infty^b = U_x = U_0^a$. Of course, a similar argument holds if we interchange 0 and ∞, and it is obvious that $U_\infty \neq U_0$. Also, since U_∞ is transitive on $X \setminus \{\infty\}$ and since $U_0^\alpha = U_{0\alpha}$, for any $\alpha \in U_\infty$, it follows that $\langle U_\infty, U_0 \rangle$ contains all the root groups U_x, $x \in X$, so $G = \langle U_\infty, U_0 \rangle$. It follows that G is an abstract rank one group with unipotent subgroups U_∞ and U_0. □

Conversely, every abstract rank one group gives rise to a Moufang set. We will show how it gives rise to a saturated split BN-pair of rank one, and hence, by Proposition 2.1.3, to a Moufang set.

Proposition 2.2.3. *Let $G = \langle U, V \rangle$ be an abstract rank one group with unipotent subgroups U and V. Then G has a saturated split BN-pair of rank one.*

Proof. Let $B := N_G(U)$ and let $H := N_G(U) \cap N_G(V)$. Observe that

$$\begin{aligned}\Omega := \{U^g \mid g \in G\} = \{V^g \mid g \in G\} \\ = \{U^v \mid v \in V\} \cup \{V\} = \{V^u \mid u \in U\} \cup \{U\}\,.\end{aligned}$$

This follows easily from condition $(*)$ in Definition 2.2.1. Notice that condition $(*)$ also implies that $N_G(U) \cap V = 1$, so $\mid \Omega \mid \geq 3$. Hence the above observation implies that G is doubly transitive by conjugation on Ω. Let ω be an arbitrary element of G conjugating U to V and V to U, and set $N := \langle H, \omega \rangle$.

If b is an arbitrary element of B, then $V^b \neq U$, hence $V^b = V^u$ for some $u \in U$. Of course, we also have $U^b = U^u$; hence $bu^{-1} \in H$, i.e. $b \in UH$. Also $U \cap H = 1$, since $U \cap N_G(V) = 1$. Hence BN_4 holds.

BN_2 is immediate. To show BN_1, observe that U and ω are contained in $\langle B, N \rangle$, and since $G = \langle U, V \rangle = \langle U, U^\omega \rangle$, we get $G = \langle B, N \rangle$.

Also, $\omega B \omega = B^\omega = N_G(V)$, so if $\omega B \omega = B$ then we would have $B = H$, contradicting BN_4. Now let $g \in G \setminus B$ be arbitrary; then $U^g \neq U$, and hence

$U^g = V^u = U^{\omega u}$ for some $u \in U$. It follows that $\omega u g^{-1} = b$ for some $b \in B = N_G(U)$, and hence $g = b^{-1}\omega u \in B\omega B$.

Finally, we have $B \cap B^\omega = N_G(U) \cap N_G(U^\omega) = H$, which shows that BN_5 holds, i.e. the BN-pair (B, N) is saturated. □

Remark 2.2.4. If $G = \langle U, V \rangle$ is an abstract rank one group with unipotent subgroups U and V, then the corresponding Moufang set is given by defining $X := \{U^g \mid g \in G\}$, i.e. X is the set of all conjugates of U in G. The root groups are precisely the elements of X (seen as subgroups of G), and the action is given by conjugation; this is very similar to the approach in Proposition 2.1.3.

2.3 Connection with higher rank groups

This subsection is not self-contained and the reader should consult one of the other lectures of this conference for more information about buildings.

Let Δ be a spherical building with chamber set $\mathcal{C}$. There exist several definitions of the Moufang property for spherical buildings, which are all equivalent in rank ≥ 2, but they do not all make sense in rank one. The following definition is due to B. Mühlherr [M].

A *Moufang structure* on Δ is a family of groups $(U_c)_{c \in \mathcal{C}}$ such that

- $U_c \leq \mathrm{Stab}_{\mathrm{Aut}(\Delta)}(c)$, and U_c is transitive on c^{op}, the set of chambers opposite c;
- for all $\alpha \in U_c$ and all $d \in \mathcal{C}$, we have $U_d^\alpha = U_{d\alpha}$;
- let $c \in \mathcal{C}$, let P be a panel containing c, let d be a chamber in $P \setminus \{c\}$, and let $\alpha \in U_c$ with $d\alpha = d$; then $\alpha \in U_x$ for all $x \in P$.

If Δ is thick and its diagram has no isolated nodes, then Γ admits at most one Moufang structure. The building Δ is said to satisfy the *Moufang property* if it admits a Moufang structure.

It is clear from this definition that in this sense, the Moufang buildings of rank one are precisely the Moufang sets. Moreover, every rank one residue of a higher rank Moufang spherical building is a Moufang set.

Also the notion of a (split) BN-pair of rank one has a generalization to higher rank. Our definition is taken from [T74, 3.2.1].

Definition 2.3.1. A *BN-pair* in a group G is a system (B, N) consisting of two subgroups B and N such that

BN_1. $G = \langle B, N \rangle$;

BN$_2$. $H := B \cap N \trianglelefteq N$;

BN$_3$. The group $W := N/H$ has a generating set R of involutions such that the following two relations hold for any $r \in R$ and any $w \in W$:

- $rBwB \subseteq BwB \cup BrwB$;
- $rBr \neq B$.

The group W is called the *Weyl group* of the BN-pair.

The BN-pair is called *split*, if there exists a normal subgroup[2] $U \trianglelefteq B$ such that $B = U \rtimes H$. It is called *saturated* if $H = \bigcap_{w \in W} B^w$.

Any group with a BN-pair has a natural associated building on which it acts strongly transitively (i.e. transitive on the pairs consisting of an apartment and a chamber contained in it). In fact, a saturated BN-pair for a group G is equivalent to a building on which G acts strongly transitively. See, for example, [T74, Theorem 3.2.6 and Proposition 3.11].

2.4 Connection with linear algebraic groups of relative rank one

This subsection is not self-contained and requires knowledge about linear algebraic groups. The sole purpose of this subsection is to mention, very briefly and without proofs, one of the most important motivations for the study of Moufang sets.

Let $\mathbf{G}$ be an absolutely simple algebraic group defined over a field k, of k-rank one. Let X denote the set of all k-parabolic subgroups of $\mathbf{G}$. Note that, since $\mathbf{G}$ has k-rank one, all elements of X are conjugate under $\mathbf{G}(k)$. For each element $x \in X$, we let U_x be the root subgroup of the k-parabolic subgroup x (which coincides with the k-unipotent radical of x). Let $\mathbf{G}^+(k)$ be the group generated by all these root subgroups. Then $(X, (U_x)_{x \in X})$ is a Moufang set, on which $\mathbf{G}^+(k)$ modulo its center acts faithfully; we will denote it by $\mathbb{M}(\mathbf{G}, k)$.

The pairs of elements of X are in one-to-one correspondence with the maximal k-split tori of $\mathbf{G}$. More precisely, for each k-split torus there are precisely two k-parabolic subgroups containing it, and every two k-parabolics contain a common k-split torus. If S is such a maximal k-split torus, then $N(S)/Z(S)$ (which is the relative Weyl group of $\mathbf{G}$ over k) is a group of order 2.

Many of the exceptional algebraic groups of relative rank one are still poorly understood. It is our hope that the study of Moufang sets will eventually provide more insight into these groups.

[2] Some authors also require this subgroup to be *nilpotent* as part of the definition.

2.5 Finite Moufang sets

Finite Moufang sets have already been studied and classified a long time before the notion of a Moufang set existed, as part of the classification of the finite simple groups, and more precisely in the study of finite split BN-pairs of rank one. Their classification was carried out by Suzuki [Su], Shult [Sh] and Peterfalvi [P] when the degree is odd, and by Hering, Kantor and Seitz [HKSe] when the degree is even. Some of these papers are hard and rely, in addition to the Feit-Thompson odd order theorem, on many other deep results in finite group theory.

It turns out that any finite Moufang set is either sharply two-transitive, or it is $\mathsf{PSL}_2(q)$, $\mathsf{PSU}_3(q)$, $\mathsf{Sz}(q) \cong {}^2\mathsf{B}_2(q)$ or $\mathsf{Re}(q) \cong {}^2\mathsf{G}_2(q)$ for appropriate prime powers q.

In subsection 7.7, we will outline an elementary proof for the classification when the Moufang set is *special*, in which case the only possibility is $\mathsf{PSL}_2(q)$.

3 Main construction

Here we will describe how to construct an arbitrary Moufang set starting with a group U and one permutation of the set U^*. The material of this section is taken from [DW].

Let U be a group with composition $+$ and identity 0. (The operation $+$ is not necessarily commutative. It will become clear in the examples why we have nevertheless chosen an additive notation.) Let X denote the disjoint union of U with $\{\infty\}$, where ∞ is a new symbol. For each $a \in U$, we denote

$$\mathrm{Sym}(X) \ni \alpha_a \colon \begin{cases} \infty \mapsto \infty \\ x \mapsto x + a \quad \text{for all } a \in U\,. \end{cases} \tag{3.1}$$

Thus the map $a \mapsto \alpha_a$ is essentially the right regular representation of the group U. Let

$$U_\infty := \{\alpha_a \mid a \in U\}\,.$$

Now let τ be a permutation of U^*. We extend τ to an element of $\mathrm{Sym}(X)$ (which we also denote by τ) by setting $0^\tau = \infty$ and $\infty^\tau = 0$. Next we set

$$U_0 := U_\infty^\tau \text{ and } U_a := U_0^{\alpha_a} \tag{3.2}$$

for all $a \in U$. Let

$$\mathbb{M}(U, \tau) := (X, (U_x)_{x \in X}) \tag{3.3}$$

and let

$$G := \langle U_\infty, U_0 \rangle = \langle U_x \mid x \in X \rangle .$$

Of course, this construction does not always give rise to a Moufang set, but every Moufang set can be obtained in this way, and we can tell exactly when this construction does indeed give rise to a Moufang set; see Theorem 3.5 below.

Remark 3.1. Let $\rho \in \mathrm{Sym}(X)$ be a permutation interchanging 0 and ∞. Then $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau)$ if and only if $U_\infty^\tau = U_\infty^\rho$. In particular τ is *not* determined by the Moufang set and can be chosen in a variety of different ways.

Remark 3.2. In view of equation (3.1), it makes sense to use the convention that $a + \infty = \infty + a = \infty$ for all $a \in U$.

Definition 3.3. For each $a \in U$, we define $\gamma_a := \alpha_a^\tau$, i.e. $x\gamma_a = (x\tau^{-1} + a)\tau$ for all $x \in X$. Consequently, $U_0 = \{\gamma_a \mid a \in U\}$.

We will now give an ad-hoc definition of the so-called *Hua maps* of a Moufang set; it will become clear in section 4 how these maps arise. These maps can be defined for any datum $\mathbb{M}(U, \tau)$ as defined in equation (3.3) above.

Definition 3.4. For each $a \in U^*$, we define

$$h_a := \tau\alpha_a\tau^{-1}\alpha_{-(a\tau^{-1})}\tau\alpha_{-(-(a\tau^{-1}))\tau} \in \mathrm{Sym}(X) ;$$

if we use the convention of Remark 3.2, then we can write this explicitly as

$$h_a \colon X \to X \colon x \mapsto \big((x\tau + a)\tau^{-1} - a\tau^{-1}\big)\tau - \big(-(a\tau^{-1})\big)\tau .$$

Observe that each h_a fixes the elements 0 and ∞.

Theorem 3.5 ([DW])**.** *$\mathbb{M}(U, \tau)$ is a Moufang set if and only if the restriction of each Hua map to U is contained in $\mathrm{Aut}(U)$, i.e. if $(a + b)h_c = ah_c + bh_c$ for all $a, b \in U$ and all $c \in U^*$.*

Proof. See [DW] for the general case. We give an easier proof here for the case that $\tau \in G$ and τ^2 normalizes U_∞.

We claim that the restriction of h_a to U is additive if and only if h_a normalizes U_∞. Indeed, h_a normalizes U_∞ if and only if $\alpha_b^{h_a} \in U_\infty$ for all $b \in U$. Note that $0\alpha_b^{h_a} = 0h_a^{-1}\alpha_b h_a = bh_a$, and hence h_a normalizes U_∞ if and only if $\alpha_b^{h_a} = \alpha_{bh_a}$ for all $b \in U$. Since h_a is a permutation of U, we have $U = \{ch_a \mid c \in U\}$, and hence this is equivalent to

$$(ch_a)\alpha_b^{h_a} = (ch_a)\alpha_{bh_a}$$

for all $b, c \in U$, which can be rewritten as $(c+b)h_a = ch_a + bh_a$ for all $b, c \in U$, proving the claim.

Assume first that $\mathbb{M}(U, \tau)$ is a Moufang set (with $\tau \in G$). Then each $h_a \in G$, and hence $U_\infty^{h_a} = U_{\infty h_a} = U_\infty$, i.e. each h_a normalizes U_∞.

Conversely, assume that each h_a normalizes U_∞. Since $\alpha_{(-(a\tau^{-1}))\tau}\tau^{-2}$ normalizes U_∞, it follows that $\tau\alpha_a\tau^{-1}\alpha_{-(a\tau^{-1})}\tau^{-1}$ normalizes U_∞ as well, i.e. $U_\infty^{\tau\alpha_a\tau^{-1}} = U_\infty^{\tau\alpha_{a\tau^{-1}}}$. By the definition of the groups U_a in equation (3.2), this can be rewritten as $U_a^{\tau^{-1}} = U_{a\tau^{-1}}$, for all $a \in U^*$, and this clearly also holds for $a \in \{0, \infty\}$. Also, again by the definition of the groups U_a, we have $U_a^{\alpha_b} = U_{a\alpha_b}$ for all $a \in X$ and all $b \in U$. Since $G = \langle U_\infty, \tau^{-1}\rangle$, we conclude that $U_a^\varphi = U_{a\varphi}$ for all $a \in X$ and all $\varphi \in G$, which proves that $\mathbb{M}(U, \tau)$ is a Moufang set. □

Lemma 3.6. *Let $\mathbb{M}(U, \tau)$ be a Moufang set. Then $\mathbb{M}(U, \tau^{-1})$ is a Moufang set; furthermore $g_a = h_{a\tau}^{-1}$, where g_a is the Hua map of $\mathbb{M}(U, \tau^{-1})$ corresponding to a.*

Proof. For a permutation $\varphi \in \mathrm{Sym}(X)$ that fixes ∞ let

$$\varphi^{(0)} = \varphi \cdot \alpha_{-(0\varphi)}\,.$$

First we claim that

($*$) If ξ and η are two permutations of X that fix ∞ and ξ normalizes U_∞, then $(\eta\xi)^{(0)} = \eta^{(0)}\xi^{(0)}$.

Indeed,

$$\eta^{(0)}\xi^{(0)} = \eta\alpha_{-(0\eta)}\xi\alpha_{-(0\xi)} = \eta\xi(\alpha_{-(0\eta)})^\xi\alpha_{-(0\xi)} \in \eta\xi U_\infty\,.$$

But $(\eta\xi)^{(0)}$ is the unique element in $\eta\xi U_\infty$ that fixes 0, so $(*)$ holds.

Let $a \in U^*$ and let

$$\varphi_a := \tau\alpha_a\tau^{-1}\alpha_{-a\tau^{-1}}\tau, \qquad \psi_a := \tau^{-1}\alpha_a\tau\alpha_{-a\tau}\tau^{-1}.$$

Notice that $h_a = \varphi_a^{(0)}$ and $g_a = \psi_a^{(0)}$. Also,

$$\psi_a\varphi_{a\tau} = \mathrm{id}_X.$$

From $(*)$ we get $g_a h_{a\tau} = \mathrm{id}_X^{(0)} = \mathrm{id}_X$. This shows that $g_a = h_{a\tau}^{-1}$. In particular $g_a \in \mathrm{Aut}(U)$, so by Theorem 3.5, $\mathbb{M}(U, \tau^{-1})$ is a Moufang set. □

Remark 3.7. Notice that although it is *not* made explicit in the notation h_a, the Hua-maps h_a depend on τ; see Remark 3.1.

4 First properties of Moufang sets

From now on we assume that $\mathbb{M} = \mathbb{M}(U, \tau)$ is a Moufang set; in particular, by Theorem 3.5(i), the Hua maps h_a act on U as automorphisms. The material of subsections 4.1 and 4.2 can be found in [DW] and of subsections 4.3 and 4.4 in [DS].

4.1 The μ-maps

We start by introducing certain permutations of X which interchange the elements 0 and ∞. These maps play a central role in the analysis of Moufang sets.

Proposition 4.1.1. *For each $a \in U^*$, there is a unique permutation $\mu_a \in U_0^* \alpha_a U_0^*$ interchanging 0 and ∞. This permutation will be denoted by μ_a; we have*

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

Proof. Let $\rho \in U_0 \alpha_a U_0$ and assume that $0\rho = \infty$ and $\infty\rho = 0$. Write $\rho = \gamma_x \alpha_a \gamma_y$, with $\gamma_x, \gamma_y \in U_0$ as in Definition 3.3. 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 $x = (-a)\tau^{-1}$. □

Since the μ-maps of Proposition 4.1.1 are permutations interchanging 0 and ∞, any of them can take the role of the permutation τ:

Lemma 4.1.2. *For each $a \in U^*$, we have $\mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_a)$.*

Proof. This follows from the fact that $\mu_a \in G$, μ_a interchanges 0 and ∞, and Remark 3.1. □

Remark 4.1.3. It follows from Proposition 4.1.1 that, unlike the Hua-maps, the μ-maps are independent of the choice of τ.

Remark 4.1.4. If Δ is an arbitrary Moufang spherical building, then each group $X_\alpha = \langle U_\alpha, U_{-\alpha} \rangle$ generated by two opposite root groups is an abstract rank one group and therefore induces a Moufang set. The μ-maps of this Moufang set are elements of X_α, and hence act on all of Δ. It turns out that these μ-maps play an important role in the theory of Moufang buildings in general. For the rank two case (i.e. the case of Moufang polygons), see [TW, Chapter 6].

4.2 The Hua subgroup

We start with the definition of the Hua subgroup:

Definition 4.2.1. We define the *Hua subgroup* of $\mathbb{M}$ by

$$H := \langle \mu_a \mu_b \mid a, b \in U^* \rangle .$$

Notice that $H \leq G_{0,\infty}$.

In light of Lemma 4.1.2, Theorem 3.5 and Proposition 4.3.1(2) below, we see that $\mu_a \mu_b \in \mathrm{Aut}(U)$, for all $a, b \in U^*$. Thus the Hua subgroup H consists of automorphisms of U.

Lemma 4.2.2 ([DW, Theorem 3.1(ii)])**.** $H = G_{0,\infty}$.

Proof. By Lemma 4.1.2, we may and we will assume that $\tau = \mu_e$ for some $e \in U^*$. Let $K := U_0 H \leq G_0$, and let $Q := K\tau \cup KU_\infty$. Note that $G = \langle U_\infty, \tau \rangle$; we want to show that $Q\langle U_\infty, \tau \rangle \subseteq Q$, which will imply that $Q = G$. Since only the trivial element in $\{\tau\} \cup U_\infty$ fixes 0, this will imply that $G_0 = K$, and then $G_{0,\infty} = K_\infty = H$.

So it remains to show that $QU_\infty \subseteq Q$ and $Q\tau \subseteq Q$. We have $K\tau U_\infty = K\tau U_0^\tau = KU_0\tau = K\tau$, which proves that $QU_\infty \subseteq Q$. Clearly $(K\tau)\tau = K\tau^2 \subseteq KH = K$. Observe that $KH = K$ implies $K\tau = K\mu_a$ for all $a \in U^*$ (because $\mu_a^{-1} = \mu_{-a}$ for all $a \in U^*$, see Proposition 4.3.1(1) below), and hence by Proposition 4.1.1 and the fact that $KU_0 = K$, we have $K\tau = K\mu_{a\tau} = K\alpha_{a\tau}\alpha_{-a}^\tau$ for all $a \in U^*$. It follows that

$$K\alpha_a\tau = K\tau \cdot \alpha_a^\tau = K\alpha_{a\tau} \subseteq KU_\infty$$

for all $a \in U^*$, which proves that $Q\tau \subseteq Q$. □

Corollary 4.2.3. *The following are equivalent:*

(i) *G is sharply two-transitive;*

(ii) *$H = 1$;*

(iii) *$\mu_a = \mu_b$ for all $a, b \in U^*$.*

Proof. Since G is always two-transitive, the equivalence between (i) and (ii) follows immediately from Lemma 4.2.2. The equivalence between (ii) and (iii) is immediate from the definition of H and from Proposition 4.3.1(1) below. □

Remark 4.2.4. Because of Corollary 4.2.3, the sharply two-transitive groups have a completely different behavior than the other Moufang sets. For that

reason, Moufang sets whose little projective group is not sharply two-transitive, are sometimes called *proper* Moufang sets. Nevertheless, it seems interesting to study these sharply two-transitive groups from the point of view of Moufang sets. For a good introduction (from the classical point of view) to sharply two-transitive groups, we refer to [BN, Section 11.4].

4.3 Properties of the μ-maps

In this subsection, we list various elementary properties of the μ-maps.

Proposition 4.3.1. *Let $a, b \in U^*$ and let $\sim a = (-a\tau^{-1})\tau$, then*

(1) $\mu_{-a} = \mu_a^{-1}$;

(2) $\mu_a = \tau^{-1} h_a$;

(3) *if $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$, then $\mu_{a\tau} = \mu_{-a}^{\tau}$; in particular, $\mu_{a\mu_b} = \mu_{-a}^{\mu_b}$;*

(4) $\mu_{ah} = \mu_a^h$, *for all $h \in H$;*

(5) *if $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$, then $\mu_a = \alpha_a \alpha_{-a\tau^{-1}}^{\tau} \alpha_{-\sim a}$;*

(6) $\sim a = -(-a)\mu_a$;

(7) *$\sim a$ is independent of the choice of τ, i.e. $\sim a = (-a\rho^{-1})\rho$ for all ρ with $\mathbb{M}(U,\tau) = \mathbb{M}(U,\rho)$;*

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

Proof. (1) Notice that $\mu_a^{-1} \in U_0^* \alpha_{-a} U_0^*$ and μ_a^{-1} interchanges 0 and ∞, so by Proposition 4.1.1, part (1) holds.

(2) We have

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

where g_a is as in Lemma 3.6 and the last equality comes from Lemma 3.6. Therefore, by (1), we have that $\mu_a = \mu_{-a}^{-1} = \tau^{-1}h_a$.

(3) Assume that $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$. Then we can apply (2) to the maps g_a. Note that by Remark 4.1.3, the maps μ_a are independent of τ. Therefore, taking in (2) 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 by Lemma 3.6, $g_a = h_{a\tau}^{-1}$, and hence

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

which shows the first part of (3). The second part follows by replacing τ by μ_b recalling that $\mathbb{M}(U,\tau) = \mathbb{M}(U,\mu_b)$.

(4) Applying (3) twice we get that for $h = \mu_x\mu_y$, the statement holds, where $x, y \in U^*$. The general result now follows from Definition 4.2.1.

(5) Notice that by (1) and by the definition of μ_a in Proposition 4.1.1,

$$\mu_{a\tau} = \alpha^{\tau}_{(-a\tau)\tau^{-1}} \cdot \alpha_{a\tau} \cdot \alpha^{\tau}_{-a}\,.$$

Using (1) and (3) we have $\mu_a^{-1} = \mu_{a\tau}^{\tau^{-1}} = \alpha_{(-a\tau)\tau^{-1}} \cdot \alpha_{a\tau}^{\tau^{-1}} \cdot \alpha_{-a}$. Hence $\mu_a = \alpha_a \cdot \alpha^{\tau^{-1}}_{-a\tau} \cdot \alpha_{-((-a\tau)\tau^{-1})}$. 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}, which is precisely the statement in (5).

(6) This is obtained from (5) by applying both sides of the equality in (5) to the element $-a$.

(7) This follows from (6) since μ_a is independent of τ by Remark 4.1.3.

(8) Since statement (8) is independent of τ, using Proposition 4.1.2 we may assume that $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$ by replacing τ by some μ_x. By part (5) with τ replaced by τ^{-1}, we have that

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

and hence

$$\alpha_{-a}\mu_a\alpha_{\sim a} = \tau\alpha_{-a\tau}\tau^{-1}\,;$$

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

$$\alpha_{-a}\mu_a\alpha_{\sim a} = \mu_x\alpha_{-a\mu_x}\mu_{-x}\,,$$

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

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

4.4 Connection between the μ-maps and the Hua maps

The Hua-maps and the μ-maps are intimately connected by the equation

$$\mu_a = \tau^{-1}h_a\,.$$

The advantage of the μ-maps is that they are an invariant of the Moufang set and are not dependent on τ. The advantage of the Hua-maps is that they are

in $\mathrm{Aut}(U)$. As we will see in section 6, the identity in Proposition 4.3.1(3) translates to an identity which very much resembles the *fundamental identity of quadratic Jordan algebras*; see QJ_3 on page 98 below. Further, when dealing with the so called "special" Moufang sets with abelian root groups, the Hua maps should play the role of the structure maps of the underlying quadratic Jordan division algebra. Also, when dealing with finite Moufang sets the Hua maps help define a multiplication on U which turns U into a field.

The properties of the μ-maps in Proposition 4.3.1 translate to the following properties of the Hua-maps.

Proposition 4.4.1. *Let $a, b \in U^*$, then*

(1) $h_a = \tau\mu_a$;

(2) *If $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$, then $h_{a\tau} = \tau^{-1}h_{-a}\tau$;*

(3) $h_{ah_b} = h_{-b}h_{a\tau}^{-1}h_b$;

(4) *if τ is an involution, then $h_{a\tau} = h_a^{-1}$;*

(5) *if μ_a is an involution, then $h_a = h_{-a}$;*

(6) *if τ and μ_b are involutions, then $h_{ah_b} = h_b h_a h_b$.*

Proof. (1) This is Proposition 4.3.1(2).

(2) By (1) and Proposition 4.3.1(3),

$$h_{a\tau} = \tau\mu_{a\tau} = \mu_a^{-1}\tau = \tau^{-1}(\tau\mu_{-a})\tau = \tau^{-1}h_{-a}\tau\,.$$

(3) Again by (1) and Proposition 4.3.1(3),

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

(4) By (1) and by Proposition 4.3.1(3), $h_{a\tau} = \tau\mu_{a\tau} = \mu_{-a}\tau = h_a^{-1}$.

(5) By (1) and Proposition 4.3.1(1), $h_a = \tau\mu_a = \tau\mu_{-a} = h_{-a}$.

(6) This follows from (3) using (4) and (5). As we will see later, this identity is closely related to quadratic Jordan algebras; see subsection 5.3 below. □

5 Examples of Moufang sets

5.1 $\mathbb{M}(k)$, k a commutative field

We start by describing the easiest class of Moufang sets, namely those that arise from a commutative field k. The corresponding little projective group will turn

out to be $\mathsf{PSL}_2(k)$, and in this way, it makes sense to think about Moufang sets as (albeit very broad) generalizations of $\mathsf{PSL}_2(k)$.

So let k be an arbitrary commutative field, of arbitrary characteristic. Let $U = (k, +)$ be the additive group of k, and let

$$\tau\colon U^* \to U^*\colon x \mapsto -x^{-1}\,. \tag{5.1}$$

We will use the convention that $0^{-1} = \infty$. Then the Hua maps are given by

$$xh_a = a - \Big(a^{-1} - \big(a - x^{-1}\big)^{-1}\Big)^{-1}$$

for all $a \in U^*$ and all $x \in X$ (here $X = k \cup \{\infty\}$). The classical *Hua identity* states precisely that the right hand side of this expression is equal to a^2x, and so it is clear that the restriction of each h_a to U is in $\mathrm{Aut}(U)$. Hence by Theorem 3.5, $\mathbb{M}(U, \tau)$ is a Moufang set. We will denote this Moufang set by $\mathbb{M}(k)$; it is sometimes called the *projective Moufang set over* k, since the underlying set $X = k \cup \{\infty\}$ can be seen as the projective line $\mathsf{PG}(1, k)$.

The little projective group of $\mathbb{M}(k)$ is $\mathsf{PSL}_2(k)$; just for this example, we will make the isomorphism explicit. Let Y be the set of vector lines in $V(2, k)$, i.e. $Y := \{k(0, 1)\} \cup \{k(1, x) \mid x \in k\}$. Let $*\colon \mathsf{SL}_2(k) \to \mathsf{PSL}_2(k)$ be the canonical map. We act by $\mathsf{PSL}_2(k)$ on the right on Y, and we let

$$V_\infty := \left\{ \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)^* \,\middle|\, a \in k \right\},$$

$$V_0 := \left\{ \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)^* \,\middle|\, a \in k \right\},$$

$$\sigma := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^*.$$

Now let $\beta\colon Y \to X$ be the bijection which maps $k(0, 1)$ to ∞ and each $k(1, x)$ to x for all $x \in k$. Then β induces an isomorphism

$$\varphi\colon \mathrm{Sym}(Y) \to \mathrm{Sym}(X)\colon \rho \mapsto \beta^{-1}\rho\beta\,.$$

The restriction of φ to $\mathsf{PSL}_2(k)$ is then an isomorphism between $\mathsf{PSL}_2(k)$ and the little projective group of $\mathbb{M}(U, \tau)$ such that $V_\infty\varphi = U_\infty$ ($\varphi\colon \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)^* \mapsto \alpha_a$), $V_0\varphi = U_0$ ($\varphi\colon \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)^* \mapsto \gamma_a$) and $\sigma\varphi = \tau$.

Remark 5.1.1. The minus-sign in equation (5.1) is actually not needed; even if omitted, the corresponding Hua-maps will still induce automorphisms on U. However, the map τ will then in general no longer be an element of the little projective group G, as can be seen from the isomorphism above. Indeed, τ would then be represented by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^*$, which is not an element of $\mathsf{PSL}_2(k)$ in general.

Remark 5.1.2. From the formula $xh_a = a^2x$, it is clear that $H \cong (k^*)^2$. In particular, H is abelian.

5.2 $\mathbb{M}(D)$, D a skew field or an octonion division algebra

We will now generalize the previous example to so-called *alternative division rings*. These include all skew-fields, and in addition a family of non-associative division rings called *octonion division algebras* or *Cayley-Dickson algebras*.

Definition 5.2.1. A (not necessarily associative) ring $(D, +, \cdot)$ is called an *alternative division ring* if, for each $a \in D^*$, there exists some element $a^{-1} \in D^*$ such that $a \cdot a^{-1}b = b = ba^{-1} \cdot a$ for all $b \in D$.

Even though this is a seemingly very weak associativity law, it turns out that almost all alternative division rings are skew fields:

Theorem 5.2.2. *Let D be an alternative division ring which is not a skew field. Then D is 8-dimensional over its center k. It is a so-called octonion division algebra or Cayley-Dickson algebra. Its automorphism group is an anisotropic algebraic group of type G_2 defined over k.*

Proof. The fact that D is a Cayley-Dickson algebra is due to Bruck and Kleinfeld [BrKl] when $\mathrm{char}(D) \neq 2$, and then completed by Kleinfeld [Kl] for the case where $\mathrm{char}(D) = 2$. See, for example, [TW] for a characteristic-free proof. For the fact about the automorphism group in general characteristic, see [SV]. □

So let D be an arbitrary alternative division ring. It can be shown that every subring generated by two elements is associative; in particular, the expression aba with $a, b \in D$ makes sense. Let $U := (D, +)$, the additive group of D, and as in the previous example, let

$$\tau \colon U^* \to U^* \colon x \mapsto -x^{-1}\,. \tag{5.2}$$

Then the Hua maps are again given by

$$xh_a = a - \left(a^{-1} - \left(a - x^{-1}\right)^{-1}\right)^{-1}$$

for all $a \in U^*$ and all $x \in X$. The *Hua identity* now states that the right hand side of this expression is equal to axa, and again it is clear that the restriction of each h_a to U is in $\mathrm{Aut}(U)$. Hence by Theorem 3.5, $\mathbb{M}(U, \tau)$ is a Moufang set. We will denote this Moufang set by $\mathbb{M}(D)$; it is sometimes called the *projective Moufang set over D*, and its little projective group is denoted by $\mathsf{PSL}_2(D)$.

5.3 $\mathbb{M}(J)$, J a quadratic Jordan division algebra

All known examples of Moufang sets with abelian root groups (including the previous two examples) arise in the fashion which we will now describe.

We first recall the definition of quadratic Jordan algebras, as introduced by K. McCrimmon [Mc1]. We will use the notation W_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 $W_x \in \mathrm{End}_k(J)$, and assume that the map $W\colon J \to \mathrm{End}(J)\colon x \mapsto W_x$ is quadratic, i.e.

$$W_{xt} = W_x t^2 \text{ for all } t \in k, \text{ and}$$
$$\text{the map } (x,y) \mapsto W_{x,y} \text{ is } k\text{-bilinear},$$

(note that we multiply scalars on the right) where

$$W_{x,y} := W_{x+y} - W_x - W_y$$

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

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

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

QJ$_1$. $W_1 = \mathrm{id}_J$;

QJ$_2$. $W_x V_{x,y} = V_{y,x} W_x$;

QJ$_3$. $W_{yW_x} = W_x W_y W_x$ ["the fundamental identity"]

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

$$yW_x = x \quad \text{and} \quad 1W_yW_x = 1.$$

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 W_x is invertible; we then have $W_x^{-1} = W_{x^{-1}}$. In particular,

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

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

Now assume that $(J, W, 1)$ is an arbitrary quadratic Jordan division algebra. We will now construct a Moufang set $\mathbb{M}(J)$, in the same way as we did in the

previous two examples. So let $U := (J, +)$, the additive group of the vector space J, and let

$$\tau\colon U^* \to U^*\colon x \mapsto -x^{-1}\,. \tag{5.3}$$

Then the Hua maps are once again given by

$$xh_a = a - \left(a^{-1} - \left(a - x^{-1}\right)^{-1}\right)^{-1}$$

for all $a \in U^*$ and all $x \in X$. The *Hua identity for Jordan algebras* now states that the right hand side of this expression is precisely equal to xW_a, and again it is clear that the restriction of each h_a to U is in $\mathrm{Aut}(U)$. Hence by Theorem 3.5, $\mathbb{M}(U, \tau)$ is a Moufang set. We will denote this Moufang set by $\mathbb{M}(J)$, and it makes sense to denote its little projective group by $\mathsf{PSL}_2(J)$.

Remark 5.3.1. In the theory of Jordan algebras, there is the important notion of the *structure group* for J, which is the group of isomorphisms from J to an arbitrary *isotope* of J. The group $\langle W_x \mid x \in J^* \rangle$ is known as the *inner structure group* of J, and plays an important role in understanding the structure of J. Since $h_a = W_a$ in our case, we see that the inner structure group is precisely the Hua subgroup H of $\mathbb{M}(J)$, and this illustrates once more that this group H ought to be very important in the theory of Moufang sets in general.

Remark 5.3.2. Quadratic Jordan division algebras have been classified by K. McCrimmon and E. Zel'manov [McZ]. We give a very brief overview of the outcome of this classification, and we refer to [McZ] for more details. Every quadratic Jordan division algebra belongs to one of the following (non-disjoint) classes:

(a) an algebra D^+ for some associative division algebra D, defined by $bW_a = aba$ for all $a, b \in D$;

(b) a hermitian algebra $H(A, *) = \{x \in A \mid x^* = x\} \subset A^+$ for some associative algebra A with involution $*$, or more generally, an ample subspace $H_0(A, *)$ of $H(A, *)$;

(c) a Jordan Clifford algebra associated to a non-degenerate anisotropic quadratic form q with basepoint ϵ (which lives inside the classical Clifford algebra with basepoint $C(q, \epsilon)$);

(d) an ample outer ideal of a "small" Jordan Clifford algebra;

(e) an Albert division algebra, i.e. an exceptional 27-dimensional Jordan division algebra.

5.4 Examples of Moufang sets with non-abelian root groups

We will now briefly describe two different examples of Moufang sets with non-abelian root groups. There are many more interesting examples, but it is out of the scope of this course to go into more detail.

Example 5.4.1. Let k be an arbitrary commutative field, and let A be either a separable quadratic extension field of k, a quaternion division algebra over k, or an octonion division algebra over k. Let σ be the standard involution of A/k, and let $N(a) := aa^\sigma$ and $T(a) := a + a^\sigma$ (for all $a \in A$) be the norm map and the trace map of A/k, respectively. Let

$$U := \{(a, b) \in A \times A \mid N(a) + T(b) = 0\}.$$

Then we can make U into a (non-abelian) group by defining the group "addition"

$$(a, b) + (c, d) := (a + c, b + d - c^\sigma a)$$

for all $(a, b), (c, d) \in U$; it is easily checked that this is indeed a group, with neutral element $(0, 0)$ and with the inverse given by $-(a, b) = (-a, b^\sigma)$. Now we define a permutation τ on U^*, by setting

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

for all $(a, b) \in U^*$. Then $\mathbb{M}(U, \tau)$ is a Moufang set.

Remark 5.4.2. When $k = \mathsf{GF}(2)$ and $A = \mathsf{GF}(4)$, this gives the smallest example of a Moufang set with non-abelian root groups. It has $U \cong Q_8$, and hence $|X| = 9$, and $G \cong \mathsf{PSU}_3(2)$.

Example 5.4.3. Let k be an arbitrary commutative field with $\mathrm{char}(k) = 3$ and admitting a Tits endomorphism θ, i.e. an endomorphism such that $(x^\theta)^\theta = x^3$ for all $x \in k$. Let

$$U := \{(a, b, c) \mid a, b, c \in k\}.$$

Then we can turn U into a (non-abelian) group by defining the group "addition"

$$(a, a', a'') + (b, b', b'') = (a + b, a' + b' + ab^\theta, a'' + b'' + ab' - a'b - ab^{1+\theta})$$

for all $a, a', a'', b, b', b'' \in k$. We define a "norm" function on U by setting

$$N(a, a', a'') := -a^{4+2\theta} - aa''^\theta + a^{1+\theta}a'^\theta + a''^2 + a'^{1+\theta} - a'a^{3+\theta} - a^2a'^2$$

for all $a, a', a'' \in k$. We also set

$$T_1(a, a', a'') = -a^{3+2\theta} - a''^\theta + a^\theta a'^\theta + a'a'' + aa'^2,$$
$$T_2(a, a', a'') = -a^{3+\theta} + a'^\theta - aa'' + a^2a',$$

for all $a, a', a'' \in k$. Now let

$$\tau\colon U^* \to U^*\colon (a, a', a'') \mapsto \left(\frac{-T_1(a, a', a'')}{N(a, a', a'')}, \frac{-T_2(a, a', a'')}{N(a, a', a'')}, \frac{-a''}{N(a, a', a'')} \right).$$

Then $\mathbb{M}(U, \tau)$ is a Moufang set. These are the so-called *Ree-Tits Moufang sets*. The corresponding little projective groups are the *Ree groups of type* ${}^2\mathsf{G}_2$; in the finite case, these groups are sometimes considered to be the most complicated infinite class of finite simple groups.

Remark 5.4.4. A more natural but less direct way to describe these Moufang sets, is as the action of a certain subgroup of the centralizer of a polarity of a mixed Moufang hexagon $H(k, k^\theta)$ on the corresponding set of absolute points; see, for example, [DW2].

Remark 5.4.5. In example 5.4.1, the root groups have nilpotency class 2, and in example 5.4.3, they have nilpotency class 3. There is only one known other class of Moufang sets with root groups of nilpotency class 3, namely those arising from a polarity of a Moufang quadrangle of type F_4; see [MV]. All other known examples of proper[3] Moufang sets with non-abelian root groups have root groups of nilpotency class 2. On the other hand, it is not known whether there exist examples with non-nilpotent root groups, or with nilpotent root groups of higher nilpotency class.

5.5 Connection with algebraic groups

As we briefly explained in subsection 2.4, the theory of Moufang sets is motivated by its connection to linear algebraic groups of relative rank one. We point out (without going into detail) which of the previous examples arise from algebraic groups, and which do not.

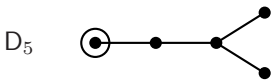
The examples $\mathbb{M}(k)$, where k is a commutative field, all arise from algebraic groups; in fact, they are the only examples arising from a split algebraic group of rank one defined over k, i.e. they arise from $\mathbf{G} = \mathsf{A}_1$.

The examples $\mathbb{M}(D)$, where D is a skew field, arise from an algebraic group if and only if D is finite-dimensional over its center k. In that case, they arise from a group with index

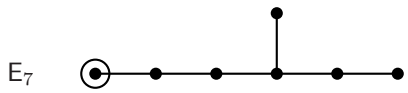
A_{2d-1} 

[3] See Remark 4.2.4.

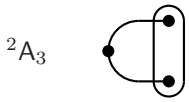
where $d = \sqrt{\dim_k(D)}$. If D is an octonion division algebra, then the Moufang set also arises from an algebraic group. Even though the octonions are exceptional algebraic structures, the corresponding Moufang set is still classical, because its structure is in fact completely determined by its norm form, which is an 8-dimensional quadratic form. The algebraic group has the following index.

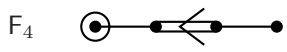


As for the Moufang set $\mathbb{M}(J)$ where J is a Jordan division algebra, we only mention that a necessary condition for it to arise from an algebraic group is that J has to be finite-dimensional over k, but even then, there exist examples which do not arise from algebraic groups, such as, for example, the so-called amply sandwiched Jordan division algebras. Let us mention, however, that the Moufang sets $\mathbb{M}(J)$ where J is an exceptional Jordan division algebra, do arise from algebraic groups of the following index.



We now turn to the examples with non-abelian root groups. All Moufang sets arising from algebraic groups have root groups that are either abelian, or nilpotent of class 2. In particular, the example of the previous subsection of nilpotency class 3 does not arise from algebraic groups. The examples of nilpotency class 2 of the previous subsection do arise from algebraic groups. Depending on whether A is a quadratic field extension, a quaternion division algebra or an octonion division algebra, the corresponding indices are as follows.





6 More advanced properties of Moufang sets

In Proposition 4.4.1(6) we saw that the identity

$$h_{ah_b} = h_b h_a h_b, \text{ if } \tau \text{ and } \mu_b \text{ are involutions}, \tag{6.1}$$

holds in any Moufang set. As we discussed earlier, this is the so-called *fundamental identity* in the area of quadratic Jordan algebras. As we will see, when $\mathbb{M}(U,\tau)$ is special and U is abelian, μ_b is an involution, for all $b \in U^*$, and (of course) we can, in this case, choose τ to be an involution, so that equation (6.1) holds for all $a, b \in U^*$.

In subsection 6.1, we will deduce a second important identity that holds in any Moufang set. We will see later how this identity relates to the axiom QJ_2 of quadratic Jordan algebras discussed in the previous subsection 5.3.

Subsection 6.2 is devoted to the notion of a "root subgroup", an important and useful notion in the theory of Moufang sets. Subsection 6.1 comes from [DS] and 6.2 from [S].

6.1 Identities in Moufang sets

Proposition 6.1.1. *Let $a, b \in U^*$ with $a \neq b$, then*

(1) *the element $(a\tau^{-1} - b\tau^{-1})\tau$ is independent of τ; more precisely,*

$$(a\tau^{-1} - b\tau^{-1})\tau = (a-b)\mu_b + (\sim b)\,.$$

(2) $\mu_{(a\tau^{-1}-b\tau^{-1})\tau} = \mu_{-b}\mu_{b-a}\mu_a$.

Proof. (1) Let

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

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 4.3.1(2) and Theorem 3.5, $\tau\mu_x^{-1} \in \mathrm{Aut}(U)$, hence the first statement of (1) holds. Since for $x \in U^*$, $\mathbb{M}(U,\tau) = \mathbb{M}(U,\mu_x)$, we may again assume that $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$ by replacing τ by some μ_x. Notice that $c = a\gamma_{-b\tau^{-1}}$, so by Proposition 4.3.1(5), we have $c = a\alpha_{-b}\mu_b\alpha_{\sim b}$, or

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

and (1) holds.

(2) We have that $\sim c = (b\tau^{-1} - a\tau^{-1})\tau$. By interchanging a and b in (1) we get

$$\sim c = (b-a)\mu_a + (\sim a)\,. \tag{6.2}$$

Since c is independent of the choice of τ, we have

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

Notice that since $\sim b = (-(b\tau))\tau^{-1}$, $b\tau = -((\sim b)\tau)$. Also, $\sim(\sim b) = b$ and by Proposition 4.3.1(1 and 3), $\mu_{\sim b} = \mu_{-b}$. From Proposition 4.3.1(5) (with a replaced by $\sim b$ and τ by τ^{-1}) it now follows that

$$\tau\alpha_{b\tau}\tau^{-1} = \alpha_{-(\sim b)}\mu_{-b}\alpha_b\,. \tag{6.3}$$

Thus, by a repeated use of Proposition 4.3.1(5) and equation (6.3), we get

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

It follows that

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

and using (1), 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 (6.3) (with μ_b in place of τ and $(a-b)$ in place of b) and Proposition 4.3.1(5) (with μ_a^{-1} in place of τ and $(b-a)$ in place of a), 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 Proposition 4.3.1(8) with $a-b$ in place of a. □

6.2 Root subgroups and the fixpoints of the Hua maps

Given a Moufang set $\mathbb{M}(U,\tau)$ a *root subgroup* of U is roughly a τ-invariant subgroup $V \leq U$ so that $\mathbb{M}(V,\tau)$ is a Moufang set. More precisely:

Definition 6.2.1 (Root subgroup)**.** A *root subgroup* of U is a subgroup $V \leq U$ such that there exists some $a \in V^*$ with $V^*\mu_a = V^*$.

Lemma 6.2.2. *Let $V \leq U$ be a root subgroup of U. Then*

(1) $\mathbb{M}(V, \rho)$ *is a Moufang set, where* $\rho := \mu_a \restriction V \cup \{\infty\}$*;*

(2) $V^*\mu_v = V^*$*, for all* $v \in V^*$.

Proof. (1) Since $\mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_a)$, we may assume that $\tau = \mu_a$. By the definition of the Hua-maps we now see that the Hua-maps of $\mathbb{M}(V, \rho)$ are the restriction of Hua-maps of $\mathbb{M}(U, \mu_a)$ to V, and hence they belong to $\mathrm{Aut}(V)$. By Theorem 3.5, $\mathbb{M}(V, \rho)$ is a Moufang set.

(2) This follows from the definition of the μ-maps in Proposition 4.1.1. □

One important place where root subgroups appear and where they turn out to be useful, is the following:

Lemma 6.2.3. *For any* $h \in H$*, then* $C_U(h)$ *is a root subgroup.*

Proof. Set $V := C_U(h)$ and let $v, w \in V$. Then, by Proposition 4.3.1(4), we have $v\mu_w h = vh\mu_{wh} = v\mu_w \in V$, hence $V^*\mu_w = V^*$ and by definition V is a root subgroup. □

We will see that the notion of a root subgroups and Lemma 6.2.3 had already been used successfully for finite Moufang sets and for the "special if and only if abelian root groups" conjecture.

Notation 6.2.4. Let $0 \neq V \leq U$ be a root subgroup and let $x \in V^*$.

(1) We let $V_\infty := \{\alpha_v \mid v \in V\}$, $V_0 := V_\infty^{\mu_x}$, and for $w \in V$, $V_w := V_0^{\alpha_w}$. Notice that, since $\alpha_v^{\mu_x\mu_y} = \alpha_{v\mu_x\mu_y} \in V_\infty$ for all $v \in V$ and all $x, y \in V^*$, the definition of V_y, $y \in V \cup \{\infty\}$ is independent of the choice of x.

(2) We let $G(V) := \langle \alpha_v, \mu_v \mid v \in V^* \rangle$, $N(V) := \langle \mu_v \mid v \in V^* \rangle$, $H(V) := \langle \mu_v\mu_w \mid v, w \in V^* \rangle$ and $X(V) := V \cup \{\infty\}$.

Definition 6.2.5. A group G is called a *generalized abstract rank one group* with *unipotent subgroups* A and B, if $G = \langle A, B \rangle$, A and B are two different subgroups of G, and for each $a \in A^*$, there exists an element $b \in B^*$ such that $A^b = B^a$, and conversely. Note that the only difference with Timmesfeld's definition of an abstract rank one group (as given in Definition 2.2.1) is that we do *not* require A and B to be nilpotent.

Lemma 6.2.6. *Let* $0 \neq V \leq U$ *be root subgroup, set* $\mathcal{X} := X(V)$ *and let* $\mathcal{G} := G_{\{\mathcal{X}\}}$ *and* $\mathfrak{G} := G(V)$*. Then*

(1) $\mathfrak{G}$ *is a generalized rank one group with unipotent subgroups* V_∞ *and* V_0*;*

(2) $\mathfrak{G} \trianglelefteq \mathcal{G}$ *and* $\mathcal{G} = \mathfrak{G}H_{\{V\}}$*;*

(3) $G_{\mathcal{X}} = H_{\mathcal{X}}$ *and* $[G_{\mathcal{X}}, \mathfrak{G}] = 1$*, in particular,* $\mathfrak{G}_{\mathcal{X}} = Z(\mathfrak{G})$.

Proof. The proof is omitted; see [S, Section 3]. □

7 Special Moufang sets

In this last section, we will concentrate on the so-called *special* Moufang sets. This is the class of Moufang sets that has been studied the most so far, and despite some significant progress, there are some very intriguing questions in this area which are still unsolved. The material of subsection 7.4 comes from [SW] and of subsection 7.7 from [DS2] and [S]. The results of the other subsections can be found in [DS] and [DST].

7.1 Definition of special Moufang sets

Definition 7.1.1. A Moufang set $\mathbb{M}(U, \tau)$ is called *special* if the condition

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

holds.

Remark 7.1.2. The notion of "special" abstract rank one group is due to Timmesfeld. In his book [Tim] Timmesfeld defines an abstract rank one group Y with unipotent subgroups A and B to be special if and only if for each $a \in A$ there exists $b \in B$ with $a^b = (b^{-1})^a$ and vice versa. It can be shown that this condition is equivalent to condition $(*)$ in the case where Y is a Moufang set.

There are several reasons for singling out the "special" property.

(a) In [Tim, Remark, p. 26] Franz Timmesfeld writes: "I believe that each special rank one group with abelian unipotent subgroups is either quasisimple or isomorphic to $\mathsf{SL}_2(2)$ or $(\mathsf{P})\mathsf{SL}_2(3)$. If one could prove this, it would quite simplify the proofs of simplicity for classical and Lie type groups".

The following theorem in [DST] shows that the the above assertion of Timmesfeld about special rank one groups holds:

Theorem 7.1.3. (1) *Let $\mathbb{M}(U, \tau)$ be a special Moufang set, let G be its little projective group and let $H = G_{0,\infty}$ be its Hua-subgroup. Assume that $|U| > 3$, then $[U_\infty, H] = U_\infty$, and hence G is perfect.*

(2) *Let Y be a special abstract rank one group with unipotent subgroups A and B and let $K = N_Y(A) \cap N_Y(B)$. Then A is abelian, and either $Y \cong \mathsf{SL}_2(2)$ or $(\mathsf{P})\mathsf{SL}_2(3)$, or $[A, K] = A$ and hence Y is quasisimple.*

(b) It is clear that the structure of a Moufang set $\mathbb{M}(U,\tau)$ and its little projective group is related to the structure of U. So it is only natural to start investigating the simplest case, i.e., the case where U is abelian. Conjectures 7.2.1 and 7.2.6 assert that $\mathbb{M}(U,\tau)$ is special if and only if U is abelian.

(c) The "special" property can be used efficiently to further restrict the structure of U, $\mathbb{M}(U,\tau)$ and G.

We now start our investigation of special Moufang sets.

Lemma 7.1.4. *Let $\mathbb{M}(U,\tau)$ be a Moufang set. Then the following are equivalent:*

(i) *$\mathbb{M}(U,\tau)$ is special;*

(ii) *$\sim a = -a$, for all $a \in U^*$, where $\sim a = (-a\tau^{-1})\tau$;*

(iii) *$(*)$ of Definition 7.1.1 holds with μ_x in place of τ, for some $x \in U^*$;*

(iv) *$(*)$ of Definition 7.1.1 holds with μ_x in place of τ, for all $x \in U^*$;*

(v) *$(-a)\mu_a = a$, for all $a \in U^*$.*

Proof. (i)$\Leftrightarrow$(ii). Notice that by definition, (ii) means that $\mathbb{M}(U,\tau^{-1})$ is special. Assume that $\mathbb{M}(U,\tau)$ is special. Then replacing a with $a\tau^{-1}$ in $(*)$ we get $(-(a\tau^{-1}))\tau = -a = (-a)\tau^{-1}\tau$, so $(-a)\tau^{-1} = -(a\tau^{-1})$. Conversely the same argument shows that if $\mathbb{M}(U,\tau^{-1})$ is special then $\mathbb{M}(U,\tau)$ is special.

(i)$\Rightarrow$(iv). Let $a, x \in U^*$. By Proposition 4.3.1(2), $\mu_x\tau^{-1} \in \mathrm{Aut}(U)$. Hence $(-a)\mu_x\tau^{-1} = -(a\mu_x\tau^{-1})$, so

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

(iv)$\Rightarrow$(iii). This is trivial.

(iii)$\Rightarrow$(i). Assume (iii) holds, then for $a \in U^*$ we have

$$(-a)\tau = (-a)\tau\mu_x\mu_{-x} = (-(a\tau\mu_x))\mu_{-x} = -(a\tau)\,,$$

and hence (i) holds.

(ii)$\Leftrightarrow$(v). By Lemma 4.3.1(6), $\sim a = -(-a)\mu_a$, so (ii) and (v) are equivalent. □

7.2 The structure of the root groups

We will assume from now on, and until the end of these notes, that $\mathbb{M}(U,\tau)$ is a special Moufang set. The main conjecture here is:

Conjecture 7.2.1. *Let $\mathbb{M}(U,\tau)$ be a special Moufang set. Then U is abelian.*

At the moment we cannot prove Conjecture 7.2.1, but we can impose severe restrictions on the structure of U:

Proposition 7.2.2. *Let $a \in U^*$, $n \geq 1$ be a positive integer such that $a \cdot n \neq 0$, and $\rho \in \mathrm{Sym}(X)$ 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 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. We will prove only (1) and (2), the rest can be found in [DS] and [DST]. Let $n \geq 1$ be a positive integer. Assume that the equality

$$(a \cdot n)\mu_{-a} \cdot n = -a \text{ for all } a \in U^* \text{ such that } a \cdot n \neq 0 \tag{7.1}$$

holds. We claim that then (1) and (2) hold for n. First, by Proposition 7.3.1(2) below, $a\rho = (-a)\mu_{-a}\rho$. Now $\mu_{-a}\rho$ is the inverse of the map $\rho^{-1}\mu_a$ which, by Proposition 4.3.1(2), is a Hua map corresponding to ρ^{-1}, so $\mu_{-a}\rho \in \mathrm{Aut}(U)$. It follows that

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

Also, the equality

$$(a \cdot n)\rho \cdot n = a\rho \text{ for all } a \in U^* \text{ such that } a \cdot n \neq 0\,, \tag{7.2}$$

holds. This is because

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

since $\mu_a\rho \in \mathrm{Aut}(U)$. 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 (7.2) (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 (7.1). The proof is by induction on n. For $n = 1$, this is Proposition 7.3.1(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 $a \cdot n \neq 0$; hence by the induction hypothesis, equations (7.1), (7.2) and parts (1) and (2) hold for n. 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) (which holds for n), $a \cdot n = -a$, which is false. Hence $a \cdot (n+1) \cdot \frac{1}{n}$ makes sense.

By Proposition 4.3.1(8) and Lemma 7.1.4(v), $\mu_{-a} = \alpha_a\mu_{-a}\alpha_a\mu_{-a}\alpha_a$. Hence, using equation (7.2) (which holds for n by induction) we get

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

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

Remark 7.2.3. The statement in Proposition 7.2.2(5) is equivalent to stating that U is a vector space over some field $\mathbb{F}$, where $\mathbb{F}$ can be chosen to be either a finite field $\mathsf{GF}(p)$ or the field of rationals $\mathbb{Q}$. This field $\mathbb{F}$ is called the *prime field* of U, and such a group U is sometimes called a *vector group*.

Remark 7.2.4. Notice that Proposition 7.2.2 says that the order of any element in U^* is either a prime or ∞ and that U has very interesting unique divisibility properties, i.e., if $a \in U^*$ is such that $a \cdot n \neq 0$, then $(a\rho^{-1} \cdot n)\rho$ is the unique n-th root of a in U.

The next lemma shows that the structure of centralizers in U is very restricted.

Lemma 7.2.5. (1) *If $a \in U^*$ is an element whose order is a prime p, then $C_U(a)$ is a group of exponent p;*

(2) *if $a \in U^*$ is of infinite order, then $C_U(a)$ is a torsion-free uniquely divisible group.*

Proof. (1) Let $b \in C_U(a)$ and assume that the order of b is not p. Then the order of $a + b$ is not p and by (1) we have

$$\left((a+b) \cdot \tfrac{1}{p} - b \cdot \tfrac{1}{p}\right) \cdot p = a,$$

contradicting the fact that a has no p-root in U (by Proposition 7.2.2(4)).

(2) Follows from (1), because by (1) each element in $C_U(a)$ has infinite order, and by Proposition 7.2.2(1), $C_U(a)$ is uniquely divisible. □

It is also conjectured that the converse of Conjecture 7.2.1 holds:

Conjecture 7.2.6. *Let $\mathbb{M}(U,\tau)$ be a Moufang set such that U is abelian. Then either $H = 1$ or $\mathbb{M}(U,\tau)$ is special.*

Conjecture 7.2.6 is, at the moment, wide open[4].

7.3 The μ-maps in special Moufang sets

When $\mathbb{M}(U,\tau)$ is special, we can say more than just Proposition 4.3.1 about the μ-maps. This turns out very useful for making progress towards the main conjectures about special Moufang sets.

Proposition 7.3.1. *Let $a, b \in U^*$, and let $k, m, n \in \mathbb{Z}$. Then:*

(1) *if $\mathbb{M}(U,\tau) = \mathbb{M}(U,\tau^{-1})$, then $\mu_a = \alpha_a \alpha^{\tau}_{-a\tau^{-1}} \alpha_a$;*

(2) *$a\mu_a = -a$ and $(-a)\mu_a = a$;*

(3) *$\mu_a = \alpha_a \alpha_a^{\mu_a} \alpha_a$;*

(4) *if $a \cdot n \neq 0$, then $(a \cdot n)\mu_b = (a\mu_b) \cdot \frac{1}{n}$;*

(5) *if $a + b \neq 0$, then $a\mu_{a+b} = -b - a + a\mu_b - b$;*

(6) *if $a\mu_b = -a$, then $b = \pm a$;*

(7) *if $\mu_a = \mu_b$, then $b = \pm a$;*

(8) *$(a \cdot k)\mu_{a\cdot m} = -a \cdot \frac{m^2}{k}$ and $\mu_{a\cdot k}^{\mu_{a\cdot m}} = \mu_{a\cdot \frac{m^2}{k}}$;*

(9) *if $a \cdot 2 \neq 0$, then $\mu^2_{a\cdot 2} = \mu^2_a$ and if $t \in \mathbb{Z}$ is such that $a \cdot t \neq 0$, then $\mu^2_{a\cdot t^2} = \mu^2_a$;*

(10) *if $|a| = 2$, then μ_a is conjugate to α_a; in particular, $\mu_a^2 = 1$;*

(11) *if $|a|$ is finite, then $\mu_a^4 = 1$;*

(12) *if U is abelian then $\mu_a^2 = 1$.*

Proof. The parts of the proof that we omit can be found in [DS] and [DST].

(1) This comes from Proposition 4.3.1(3).

(2) By (1), $a\mu_{-a} = a\alpha_{-a}\gamma_{a\tau^{-1}}\alpha_{-a} = 0\gamma_{a\tau^{-1}}\alpha_{-a} = -a$. Using Lemma 7.1.4(iv) it follows that $a = (-a)\mu_a = -(a\mu_a)$.

[4]Note added in proof: this conjecture has now been proved in [S2].

(3) This follows from (1) using (2) and taking $\tau = \mu_a$.

(4) This is Proposition 7.2.2(2) with μ_b in place of ρ.

(5) Set $c := (a\tau^{-1} - b\tau^{-1})\tau$. By Proposition 6.1.1(1), $c = (a-b)\mu_b - b$. Notice that

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

so

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

Hence we get that

$$(a-b)\mu_b - b = a + (a-b)\mu_a. \tag{7.3}$$

Replacing a with $a+b$ in (7.3) we get $a\mu_b - b = a + b + a\mu_{a+b}$.

(6) This is crucial, but we have to omit the proof.

(7) This is an immediate consequence of (6), because if $\mu_a = \mu_b$, then also $a\mu_b = -a$.

(8) By Proposition 7.2.2(2), $(a \cdot k)\mu_{a\cdot m} = (a\mu_{a\cdot m}) \cdot \frac{1}{k}$. Also, by (2) and Proposition 7.2.2(2),

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

(9) We omit the proof of this fact.

(10) This is an immediate consequence of (3).

(11) Let $a \in U^*$ be an element of finite order p and note that p is a prime by Proposition 7.2.2(4). If $p = 2$, the $\mu_a^2 = 1$, by (10). 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 (11) follows. The case when -1 is a non-square modulo p, is more elaborate and we omit the details.

(12) Since μ_a is independent of τ we may use (1) to get $\mu_a = \alpha_a\tau^{-1}\alpha_{a\tau^{-1}}^{-1}\tau\alpha_a$, and hence

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

for all x. We then get that

$$\begin{aligned} (-x)\mu_{-a} &= (-(x+a)\tau^{-1} + a\tau^{-1})\tau - a \\ &= -((x+a)\tau^{-1} - a\tau^{-1})\tau - a \\ &= -x\mu_a\,. \end{aligned}$$

It follows that $x\mu_{-a} = x\mu_a$ for all x, and hence $\mu_a^{-1} = \mu_{-a} = \mu_a$. □

Remark 7.3.2. In Theorem 7.5.2 below, we will see that (12) is actually equivalent to the assertion that U is abelian.

7.4 The action of the Hua subgroup on the root groups

The following structural theorem turns out to be very useful in proving various results about special Moufang sets.

Theorem 7.4.1 ([SW])**.** *Let $W \leq U$ be a nontrivial H-invariant subgroup. Then either U is an elementary abelian 2-group, or $W = U$.*

Sketch of proof. Let W be an H-invariant subgroup of U. First we notice that

$$W^*\mu_u = W^* \text{ for all } u \in U^*. \tag{7.4}$$

This is because $w\mu_u = (-w)\mu_w\mu_u$, for all $w \in W^*$.

Step 1. Let $a \in W^*$ and $b \in U$. If $b + a + b \in W$, then $b \cdot n + a + b \cdot n \in W$ for all $n \in \mathbb{Z}$.

Step 2. As a corollary we get:
Let $a \in W^*$ and $b \in U^*$. If $a + b \neq 0$, then $b \cdot n + a\mu_{a+b} + b \cdot n \in W$ for all $n \in \mathbb{Z}$.

Proof of Step 2. As $a \in W^*$, equation (7.4) says that $a\mu_b$ and $a\mu_{a+b}$ are also in W, so $-a + a\mu_b \in W$. Then, by Proposition 7.3.1(5), $b + a\mu_{a+b} + b = -a + a\mu_b \in W$, so Step 2 follows from Step 1. □

Step 3. Assume W is normal in U. Then either U is an elementary abelian 2-group or $W = U$.

Proof of Step 3. We repeatedly use the fact that for $x \in U^*$, $W^*\mu_x = W^*$ (and hence if $u \in U \setminus W$, then $u\mu_x \notin W$). We assume that $W \neq U$ and we show that U is an elementary abelian 2-group.

First we show that

$$\text{if } w \in W \text{ and } w \cdot 2 \neq 0, \text{ then } w \cdot \tfrac{1}{2} \in W. \tag{i}$$

Let $w \in W$ such that $w \cdot 2 \neq 0$. Then, by Proposition 7.2.2(2), with $\rho = \mu_w$, we have $w \cdot \frac{1}{2} = ((-w) \cdot 2)\mu_w$. Hence $w \cdot \frac{1}{2} \in W$. Next we claim that

$$\text{if } u \in U \text{ and } u \cdot 2 \neq 0, \text{ then } u \in W. \tag{ii}$$

Let $u \in U$ with $u \cdot 2 \neq 0$ and choose $w \in W^*$ such that $u + w \neq 0$. We have $w\mu_{w+u} = -u - w + w\mu_u - u$. Notice however that $w, w\mu_{w+u}, w\mu_u \in W$, and since W is normal in U it follows that $w\mu_{w+u}$ conjugated by u is in W. Hence $-u \cdot 2 = (-u + w\mu_{w+u} + u) - (-w + w\mu_u) \in W$. But $u \cdot 4 \neq 0$, since there are no elements of order 4 in U. It follows from (i) that $u = (u \cdot 2) \cdot \frac{1}{2} \in W$.

Our next step is to show that

$$\text{if } u \in U \setminus W, \text{ then } u \text{ inverts } W; \text{ in particular } W \text{ is abelian.} \qquad \text{(iii)}$$

By (ii) we see that all elements in $U \setminus W$ are involutions. It follows that any involution $u \in U \setminus W$ inverts W, because $w + u \notin W$ for $w \in W$, and then $w + u$ is an involution, so u inverts w.

Next we claim

$$W \text{ is an elementary abelian 2-group, and hence so is } U. \qquad \text{(iv)}$$

If W is an elementary abelian 2-group, then, since by (ii), all elements in $U \setminus W$ are involutions, we see that U is also an elementary abelian 2-group and we are done.

So assume that W is not an elementary abelian 2-group. Let $x, y \in U \setminus W$. Since x and y invert W, $x + y$ centralizes W. But if $x + y \notin W$, then $x + y$ inverts W. It follows that $x + y \in W$ and thus W has index 2 in U. Let now $x, y \in U \setminus W$ be elements such that $x + y \neq 0$. Then, $-x\mu_{x+y} - y - x + x\mu_y - y = 0$. However, $x, y, x\mu_y, x\mu_{x+y} \notin W$, so we get that 0 is the sum of an odd number of elements which are not in W. This contradicts the fact that U/W has order two. Hence (iv) holds and the proof of Step 3 is complete. □

Step 4. If $W \neq U$, then W is of exponent 2.

Sketch of proof of step 4. We now drop the assumption that W is normal in U. We show that $V := \langle w \cdot 2 \mid w \in W \rangle$ is a normal subgroup of U. Since it is characteristic in W, it is H-invariant, so by Step 3, either $V = 0$ or $V = U$ (in which case $W = U$ as well). Hence if $W \neq U$, $V = 0$ and it follows that W is of exponent 2. □

Step 5. If $W \neq U$, then U is of exponent 2.

Sketch of proof of step 5. Assume $W \neq U$; we show that all elements in $U \setminus W$ are involutions, by Step 4 it will then follow that W is of exponent 2. For that we show first that if $a \in W^*$ (which is an involution by step 4) and if $b \in U \setminus W$ is not an involution, then

(I) $a\mu_{a+b}$ inverts b;

(II) $b\mu_{b+a}$ centralizes a;

(III) if b centralizes a, then $b\mu_a$ centralizes a.

Now choose $a \in W^*$ and let $b \in U \setminus W$ such that b is not an involution. By (II), $b\mu_{b+a}$ centralizes a. Since the order of $b\mu_{b+a}$ is distinct from 2, we can apply (III) with $b\mu_{b+a}$ in place of b. Thus, by (III), $b\mu_{b+a}\mu_a$ centralizes a. Since $\mu_{b+a}\mu_a \in \mathrm{Aut}(U)$, we get that $a\mu_a^{-1}\mu_{-(b+a)}$ centralizes b, i.e. $a\mu_{a-b}$ centralizes b. But by (I), $a\mu_{a-b}$ inverts b, so b must be an involution. This contradicts our hypothesis that b is not an involution and completes the proof of Theorem 7.4.1. □

7.5 The "special implies abelian" conjecture

As we indicated above the main conjecture regarding the structure of the root groups of a special Moufang set is Conjecture 7.2.1 which asserts that they must be abelian. In addition to Proposition 7.2.2, the best results we have toward this conjecture are the following two results.

Theorem 7.5.1. *If a root group of a special Moufang set contains involutions then it is (abelian) of exponent* 2*.*

Theorem 7.5.2. *The root groups of a special Moufang set are abelian if and only if its μ-maps are involutions.*

We only present the proof of Theorem 7.5.1.

Proof of Theorem 7.5.1.

Step 1. Let $a, b \in U^*$, such that $a \in \mathrm{Inv}(U)$ and a inverts b. Then a centralizes b and hence $b \in \mathrm{Inv}(U)$.

Proof of Step 1. First note that

$$\text{if } a, b \in \mathrm{Inv}(U) \text{ then } a \text{ commutes with } a\mu_b. \tag{$*$}$$

Indeed, $a\mu_{a+b} = b + a + a\mu_b + b$, so $a + a\mu_b$ is an involution and $(*)$ follows. Notice that by Lemma 7.2.5(1),

$$C_U(t) \text{ is a group of exponent } 2, \text{ for all } t \in \mathrm{Inv}(U). \tag{$**$}$$

Let $a \in \mathrm{Inv}(U)$ and let $b \in U^*$ be an element inverted by a. We will show that $b \in C_U(a)$. If $b \in \mathrm{Inv}(U)$, then we are done. So we may assume that $b \notin \mathrm{Inv}(U)$.

Consider the equality

$$a\mu_{a+b} = -b + a + a\mu_b - b = a + b + a\mu_b - b\,.$$

Since $a + b \in \mathrm{Inv}(U)$ (because a inverts b), it follows from $(*)$ that a commutes with $a\mu_{a+b}$ so a commutes with $b + a\mu_b - b$. Conjugating by b we see that $a\mu_b$ commutes with $-b + a + b$, hence

$$\text{if } a \text{ inverts } x \in U^* \setminus \mathrm{Inv}(U), \text{ then } a\mu_x \text{ commutes with } -x + a + x. \tag{7.5}$$

In what follows we will use the following facts from Proposition 7.3.1(8):

$$(b \cdot \gamma)\mu_{b\cdot\delta} = -b \cdot \frac{\delta^2}{\gamma}, \qquad \mu_{b\cdot\gamma}^{\mu_{b\cdot\delta}} = \mu_{b\frac{\delta^2}{\gamma}} \tag{7.6}$$

for all $\gamma, \delta \in \mathbb{Q}$ such that $b \cdot \gamma$, $b \cdot \delta$ are well defined. Notice that the uniqueness of roots in U implies that a inverts $b \cdot \gamma$, for every $\gamma \in \mathbb{Q}$ for which $b \cdot \gamma$ is well defined. Let now $\alpha, \beta \in \mathbb{Q}$ such that $b \cdot \alpha$ and $b \cdot \beta$ are well defined. From equation (7.5) we get

$$a\mu_{b\cdot\alpha} \text{ commutes with } -b \cdot \alpha + a + b \cdot \alpha\,. \tag{7.7}$$

Applying $\mu_{-b\cdot\alpha}\mu_{b\cdot\beta} \in \mathrm{Aut}(U)$ to equation (7.7) we get

$$a\mu_{b\cdot\beta} \text{ commutes with } -b \cdot \frac{\beta^2}{\alpha} + a\mu_{-b\cdot\alpha}\mu_{b\cdot\beta} + b \cdot \frac{\beta^2}{\alpha}\,.$$

Replacing in this last equality β with α and α with $-\beta$ we get

$$a\mu_{b\cdot\alpha} \text{ commutes with } b \cdot \frac{\alpha^2}{\beta} + a\mu_{b\cdot\beta}\mu_{b\cdot\alpha} - b \cdot \frac{\alpha^2}{\beta}\,. \tag{7.8}$$

From equations (7.7) and (7.8) using $(**)$ we see that

$$-b \cdot \alpha + a + b \cdot \alpha \text{ commutes with } b \cdot \frac{\alpha^2}{\beta} + a\mu_{b\beta}\mu_{b\alpha} - b \cdot \frac{\alpha^2}{\beta}$$

and after conjugating by $-b\alpha$ we get

$$a \text{ commutes with } a\mu_{b\cdot\beta}\mu_{b\cdot\alpha} - b \cdot (\alpha + \tfrac{\alpha^2}{\beta}) \cdot 2\,. \tag{7.9}$$

Notice that we have used (7.6) which implies that $a\mu_{b\cdot\beta}\mu_{b\cdot\alpha}$ inverts b (because $\mu_{b\cdot\beta}\mu_{b\cdot\alpha} \in \mathrm{Aut}(U)$). Since a and $a\mu_{b\beta}\mu_{b\alpha}$ invert b, $a + a\mu_{b\cdot\beta}\mu_{b\cdot\alpha}$ centralizes b. But by equation (7.9), a commutes with $c := a + a\mu_{b\cdot\beta}\mu_{b\cdot\alpha} - b \cdot (\alpha + \frac{\alpha^2}{\beta}) \cdot 2$ and c commutes with b. Hence, if $c \neq 0$, then, by $(**)$, c is an involution, and hence b is an involution. We have thus shown that

$$a\mu_{b\cdot\beta}\mu_{b\cdot\alpha} = a + b \cdot (\alpha + \frac{\alpha^2}{\beta}) \cdot 2\,. \tag{7.10}$$

Taking in equation (7.10) $\alpha = \beta = -1$ we get

$$a\mu_{-b}^2 = a - b \cdot 4\,. \tag{7.11}$$

But taking in equation (7.10) $\beta = -1$ and $\alpha = 2$ we also get

$$a\mu_{-b}\mu_{b\cdot 2} = a - b \cdot 4\,. \tag{7.12}$$

Hence $a\mu_{-b}^2 = a\mu_{-b}\mu_{b\cdot 2}$. Applying μ_b on both sides of this equality and using equation (7.6) we obtain $a\mu_{-b} = a\mu_{b\cdot\frac{1}{2}}$ or

$$a = a\mu_{b\cdot\frac{1}{2}}\mu_b \tag{7.13}$$

But from equations (7.10) and (7.13) we get

$$a = a\mu_{b\cdot\frac{1}{2}}\mu_b = a + b \cdot 6\,.$$

so $b \cdot 6 = 0$. Since the order of b is a prime (see Proposition 7.2.2(4)) and $b \notin \mathrm{Inv}(U)$, we see that $b \cdot 3 = 0$. But then, by Proposition 7.3.1(11), $\mu_b^2 = \mu_{-b}^2$. However, by equation (7.10), $a\mu_b^2 = a + b\cdot 4$ whereas $a\mu_{-b}^2 = a - b\cdot 4$, so $b\cdot 8 = 0$. This is a contradiction and the proof this step is complete. □

Step 2. Let $b \in U^*$. We will show that $b \in \mathrm{Inv}(U)$. Assume not and let $a \in \mathrm{Inv}(U)$, then $a\mu_{a+b} = -b + a + a\mu_b - b$, and conjugating by b we get that $-b \cdot 2 + a + a\mu_b \in \mathrm{Inv}(U)$. Thus $a\mu_b$ inverts $-b \cdot 2 + a$, so, by Step 1, $-b \cdot 2 + a$ is an involution. It follows that a inverts $-b \cdot 2$ and hence a inverts b. But then, by Step 1, b is an involution, a contradiction. This completes the proof of Theorem 7.5.1. □

7.6 The "special abelian implies Jordan algebra" conjecture

In this section we assume that U is abelian. Hence, by Proposition 7.3.1(13),

$$\mu_a^2 = 1\,, \text{ for all } a \in U^*\,.$$

We assume that $\tau = \mu_e$ for some $e \in U^*$, but occasionally e may vary. Recall that by Remark 7.2.3, U is a vector space over a prime field $\mathbb{F}$. Recall also that by Theorem 3.5, h_a is an invertible $\mathbb{F}$-linear transformation of U, for all $a \in U^*$.

The main conjecture here is:

Conjecture 7.6.1. *There exists a field extension $\mathbb{K}/\mathbb{F}$ such that*

(1) *U is a vector space over $\mathbb{K}$;*

(2) *$h_a \in \mathrm{End}_{\mathbb{K}}(U)$, for all $a \in U^*$;*

(3) $\mathcal{U}_e := (U, \mathcal{H}, e)$ *is a quadratic Jordan division algebra, where* $\mathcal{H}\colon x \mapsto h_x := \mu_e\mu_x$, *for* $x \in U$.

Notice that since quadratic Jordan division algebras have been classified (see Remark 5.3.2), this will yield a complete classification of special Moufang sets with abelian root groups.

One possible candidate for the field $\mathbb{K}$ of Conjecture 7.6.1 is

$$\mathbb{K} := Z\big(C_{\mathrm{End}_{\mathbb{F}}(U)}(H)\big), \quad \text{if } \mathrm{char}(\mathbb{F}) \neq 2.$$

Notice that since H acts irreducibly on U, $\mathbb{K}$ is a commutative field. Note that any quadratic Jordan algebra over $\mathbb{K}$ is also a quadratic Jordan algebra over $\mathbb{F}$, so another possibility is just to take $\mathbb{K} = \mathbb{F}$.

Of course $\mathcal{U}_e$ depends on the choice of e, because the Hua-maps $h_a = \mu_e\mu_a$ depend on e. Inspired by the theory of Jordan algebras, it makes sense to call $\mathcal{U}_e$ an *isotope*.

We define

$$h_{a,b} := h_{a+b} - h_a - h_b$$

for all $a, b \in U$, with the convention that h_0 is the zero map. Recall that $(U, \mathcal{H}, e)$ is a quadratic Jordan division algebra if and only if

(Quadratic) $\mathcal{H}$ is quadratic, i.e.

(i) $h_{xt} = h_x t^2$ for all $t \in \mathbb{K}$;

(ii) the map $(x, y) \mapsto h_{x,y}$ is k-bilinear.

(QJ axioms) The following identities hold *strictly*:

QJ$_1$. $h_e = \mathrm{id}_U$;

QJ$_2$. $ah_{c,b}h_a = ch_{a,bh_a}$, for all $a, b, c \in U$;

QJ$_3$. $h_{bh_a} = h_a h_b h_a$, for all $a, b \in U$.

Notice that axiom QJ$_2$ actually says that $h_a V_{a,c} = V_{c,a} h_a$, where $bV_{a,c} = ch_{a,b}$, hence $bh_a V_{a,c} = ch_{a,bh_a}$ and $bV_{c,a}h_a = ah_{c,b}h_a$.

Of course, QJ$_1$ obviously holds. Also, QJ$_3$ is Proposition 4.4.1(6), and $h_{a\cdot s} = h_a \cdot s^2$ for all $a \in U^*$ and $s \in \mathbb{F}$. So we can see that some of the axioms defining a quadratic Jordan division algebra already hold. What is actually missing is:

Missing axioms: The biadditivity of $(x, y) \mapsto h_{x,y}$ *and* QJ$_2$.

Our first observation is the following.

Proposition 7.6.2. *If* $\mathrm{char}(U) \notin \{2,3\}$*, then* $\mathcal{U}$ *is a quadratic Jordan division algebra if and only if condition* QJ_2 *is satisfied.*

Proof. This is [DS, Proposition 5.4]. □

In other words, QJ_2 implies the biadditivity of $(x,y) \to h_{x,y}$. Our next observation shows that it is enough to require that QJ_2 holds for a being *the identity element* but *in each isotope* $\mathcal{U}_e$.

Proposition 7.6.3. *If* QJ_2 *holds for* $a = e$*, but in each isotope* $\mathcal{U}_e$*, i.e., if the identity*

$$eh_{b,c} = ch_{b,e}, \quad \text{for all } b,c \in U^* \tag{7.14}$$

holds in each isotope $\mathcal{U}_e$*,* $e \in U^*$*, then the stronger identity* QJ_2 *holds for each isotope* $\mathcal{U}_e$*,* $e \in U^*$*.*

Proof. This is [DS, Corollary 5.6]. □

As we noted in subsection 6.1, the identity in Proposition 6.1.1(2), i.e, the identity

$$\mu_{(a\tau^{-1}-b\tau^{-1})\tau} = \mu_{-b}\mu_{a+b}\mu_a\,, \tag{7.15}$$

is closely related to QJ_2. Indeed, one can show that

(7.15) implies (7.14) with $b = c$, i.e., $eh_{b,b} = bh_{b,e}$, for all $b \in U^*$.

Finally, the following theorem brings us back to biadditivity and shows that (in characteristic different from 2 and 3) it is enough to require even less then the biadditivity of the map $(x,y) \mapsto h_{x,y}$ to show that $\mathcal{U}_e$ is a quadratic Jordan division algebra.

Theorem 7.6.4. *Assume that* $\mathrm{char}(U) \notin \{2,3\}$*, 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* QJ_2*. It follows that* $\mathcal{U}$ *is a quadratic Jordan division algebra. In particular if the map* $(x,y) \mapsto h_{x,y}$ *is biadditive, then* $\mathcal{U}$ *is a quadratic Jordan division algebra.*

Proof. In the proof we show that (i) and (ii) imply (7.14), for each isotope $\mathcal{U}_e$. See [DS, Theorem 5.11] for more details. □

7.7 Finite special Moufang sets

The techniques that were introduced above are useful to give a short and direct proof for the (known) classification of finite special Moufang sets.

Notation 7.7.1. For any prime power q, we write $\mathbb{M}(q) := \mathbb{M}(\mathsf{GF}(q))$, where $\mathbb{M}(k)$ is the projective Moufang set over the commutative field k as defined in subsection 5.1.

The proof of the following Theorem uses the Feit-Thompson "Odd Order Theorem" and Glauberman's Z^*-Theorem. Otherwise, it is self contained. We will only sketch the proof very briefly, and we refer to [DS2] for more details.

Theorem 7.7.2. *Let $\mathbb{M}(U, \tau)$ be a finite special Moufang set such that $|U| = q$ is even. Then q is a power of 2, U is elementary abelian and $\mathbb{M}(U, \tau) \cong \mathbb{M}(q)$.*

Sketch of proof.

Step 1. By Theorem 7.5.1, U is elementary abelian.

Step 2. $|H|$ is odd and H is transitive on U^*.

Sketch of proof of Step 2. Let

$$\mathcal{I} := \bigcup_{x \in X} U_x^* .$$

First we show that

$$\mathcal{I} \text{ is a conjugacy class of involutions in } G. \tag{7.16}$$

From (7.16) it follows that H is transitive on U^*, and therefore, by Proposition 4.3.1(4) and Proposition 7.3.1(7),

$$\{\mu_a \mid a \in U^*\} \text{ is a conjugacy class of involutions in } N. \tag{7.17}$$

Notice however that for $a, b \in U^*$ with $a \neq b$, $[\mu_a, \mu_b] \neq 1$, because $\mu_a^{\mu_b} = \mu_{a\mu_b}$, so if $\mu_{a\mu_b} = \mu_a$, $a\mu_b = a$, but b is the unique fixed point of μ_b, because μ_b is conjugate to α_b.

By (7.16) and Glauberman's Z^*-Theorem, $\mu_a\mu_b \in O_{2'}(N)$, for all $a, b \in U^*$, where $O_{2'}(N)$ is the largest normal subgroup of odd order of N. However, $H = \langle \mu_a\mu_b \mid a, b \in U^* \rangle$, so $H \leq O_{2'}(N)$ and hence $|H|$ is odd. □

Step 3. H is cyclic.

Proof of Step 3. We use the following very useful Lemma of Peterfalvi:

Lemma (Peterfalvi [P2])**.** *Let p be an odd prime, and suppose that P is a p-group acting faithfully on U with $C_U(P) = 0$. If $|C_P(a)| = |C_P(b)|$ for all $a, b \in U^*$, then P is cyclic.*

Now by Step 2, H is solvable and since H is transitive on U^*,

$$|C_{O_p(H)}(e)| = |C_{O_p(H)}(f)|, \quad \text{for all primes } p \text{ and all } e, f \in U^*.$$

Hence by Peterfalvi's Lemma, $O_p(H)$ is cyclic for all primes p, so the Fitting subgroup $F(H) = \prod_{p \text{ prime}} O_p(H)$ is cyclic and hence $\langle h \rangle \trianglelefteq H$, for all $h \in F(H)^*$. Since H is transitive on U^*,

$$C_U(h) = 0, \text{ for all } h \in F(H)^*.$$

This implies $C_{F(H)}(\mu_x) = 1$ for all $x \in U^*$ (because $\mu_x = \mu_x^h = \mu_{xh}$ would imply $x = xh$). Hence $H = \langle \mu_x \mu_y \rangle \leq C_H(F(H)) \leq F(H)$, so H is cyclic. □

Step 4. $\mathbb{M}(U, \tau) \cong \mathbb{M}(q)$, where $q = |U|$.

Sketch of proof of Step 4. We pick $e \in U^*$ and we let $\tau = \mu_e$. We show that $H = \{h_a \mid a \in U^*\}$, so $|H| = q - 1$. We then define

$$a \cdot b = a h_b^{q/2},$$

and we show that $(U, +, \cdot, e)$ is a field and that τ is the inverse map of this field. □

This completes the proof of Theorem 7.7.2. □

In the case where $|U|$ is odd a theorem similar to Theorem 7.7.2 holds, we state it but omit the (more involved) discussion on it.

Theorem 7.7.3. *Let $\mathbb{M}(U, \tau)$ be a finite special Moufang set such that $|U| = q$ is odd. Then q is a power of a prime p, U is elementary abelian and $\mathbb{M}(U, \tau) \cong \mathbb{M}(q)$.*

Proof. See [S]. □

References

[BN] **A. Borovik** and **A. Nesin**, *Groups of finite Morley rank*, Oxford university press, London, 1994.

[BrKl] **R. H. Bruck** and **E. Kleinfeld**, The structure of alternative division rings, *Proc. Amer. Math. Soc.* **2** (1951), 878–890.

[DS] **T. De Medts** and **Y. Segev**, Identities in Moufang sets, *Trans. Amer. Math. Soc.* **360** (2008), 5831–5852.

[DS2] ———, Finite special Moufang sets of even characteristic, *Commun. Contemp. Math.* **10** (2008), no. 3, 449–454.

[DST] **T. De Medts**, **Y. Segev** and **K. Tent**, Special Moufang sets, their root groups, and their μ-maps, *Proc. London Math. Soc.* **96** (2008), no. 3, 767–791.

[DW] **T. De Medts** and **R. M. Weiss**, Moufang sets and Jordan division algebras, *Math. Ann.* **335** (2006), no. 2, 415–433.

[DW2] ———, The norm of a Ree group, *Nagoya Math. J.*, to appear.

[HKSe] **C. Hering**, **W. M. Kantor** and **G. M. Seitz**, Finite groups with a split BN-pair of rank 1, I, *J. Algebra* **20** (1972), 435–475.

[Kl] **E. Kleinfeld**, Alternative division rings of characteristic 2, *Proc. Natl. Acad. Sci. USA* **37** (1951), 818–820.

[Mc1] **K. McCrimmon**, A general theory of Jordan rings, *Proc. Natl. Acad. Sci. USA* **56** (1966), 1072–1079.

[Mc2] ———, *A taste of Jordan algebras*, Springer-Verlag, Berlin, Heidelberg, New York, 2004.

[McZ] **K. McCrimmon** and **E. Zel'manov**, The structure of strongly prime quadratic Jordan algebras, *Adv. Math.* **69** (1988), no. 2, 133–222.

[M] **B. Mühlherr**, *Some contributions to the theory of buildings based on the gate property*, Ph.D. thesis, Tübingen, 1994.

[MV] **B. Mühlherr** and **H. Van Maldeghem**, Moufang sets from groups of mixed type, *J. Algebra* **300** (2006), no. 2, 820–833.

[P] **T. Peterfalvi**, Sur les BN-paires scindées de rang 1, de degré impair, *Comm. Algebra* **18** (1990), no. 7, 2281–2292.

[P2] _____, Le théoréme de Bender-Suzuki II, **in** *Révision dans les groupes finis. Groupes du type de Lie de rang* 1*, Astérisque* **143** (1986), 235–295.

[S] **Y. Segev**, Finite special Moufang sets of odd characteristic, *Commun. Contemp. Math.* **10** (2008), no. 3, 455–475.

[S2] _____, Proper Moufang sets with abelian root groups are special, *J. Amer. Math. Soc.* **22** (2009), 889–908.

[SW] **Y. Segev** and **R. M. Weiss**, On the action of the Hua subgroups in special Moufang sets, *Math. Proc. Cambridge Philos. Soc.* **144** (2008), 77–84.

[Sh] **E. Shult**, On a class of doubly transitive groups, *Illinois J. Math.* **16** (1972), 434–445.

[SV] **T. A. Springer** and **F. Veldkamp**, *Octonions, Jordan algebras and exceptional groups*, Springer Monogr. Math., Springer-Verlag, Berlin, 2000. viii+208 pp.

[Su] **M. Suzuki**, On a class of doubly transitive groups II, *Ann. of Math.* (2) **79** (1964), 514–589.

[Tim] **F. Timmesfeld**, *Abstract root subgroups and simple groups of Lie-type*, Birkhäuser-Verlag, Monogr. Math., vol. **95**, Basel, Berlin, Boston, 2001.

[T74] **J. Tits**, *Buildings of spherical type and finite BN-pairs*, Lecture Notes in Math., vol. **386**, Springer-Verlag, New York, Heidelberg, Berlin, 1974.

[T] _____, Twin buildings and groups of Kac-Moody type, in *Groups, combinatorics & geometry (Durham, 1990)*, 249–286, London Math. Soc. Lecture Note Ser. **165**, Cambridge University Press, Cambridge, 1992.

[TW] **J. Tits** and **R. Weiss**, *Moufang Polygons*, Springer Monogr. Math., Springer-Verlag, Berlin, Heidelberg, New York, 2002.

Tom De Medts

Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, S22, B-9000 Gent, Belgium

e-mail: tdemedts@cage.UGent.be

Yoav Segev

Department of Mathematics, Ben-Gurion University, Beer-Sheva 84105, Israel

e-mail: yoavs@math.bgu.ac.il