

Special Moufang sets, their root groups and their μ -maps

Tom De Medts, Yoav Segev and Katrin Tent

ABSTRACT

We prove Timmesfeld’s conjecture that special abstract rank one groups are quasisimple. We give two characterizations of the root groups in special Moufang sets: a normal subgroup of the point stabilizer is a root group if it is either regular, or nilpotent and transitive. We prove that if a root group of a special Moufang set contains an involution, then it is of exponent 2. We also show that the root groups are abelian if and only if the so-called μ -maps are involutions.

Introduction

A Moufang set is a set X with $|X| \geq 3$, together with a collection of groups $(U_x)_{x \in X}$ acting on X (called root groups), such that each U_x fixes x and acts regularly on $X \setminus \{x\}$, and such that $U_x^\varphi = U_{x^\varphi}$ for each $x \in X$ and each $\varphi \in G^\dagger := \langle U_y \mid y \in X \rangle$. The group G^\dagger is called the little projective group of the Moufang set, and it is clear that this group acts doubly transitively on X .

Moufang sets were introduced by Tits [11] as a tool to study absolutely simple algebraic groups of relative rank one, but the notion is important beyond its original purpose. This notion is closely related to that of a split BN-pair of rank one, which is another important notion due to Tits. Moufang sets are thus very basic, natural objects. One additional related concept is that of an ‘abstract rank one group’, as introduced by Timmesfeld [10], who also introduced *special* rank one groups (see Definition 1.10 below). In [10, Remark, p. 26] Timmesfeld conjectured that every special rank one group with abelian unipotent subgroups is quasisimple; this conjecture is part (2) of the following.

THEOREM A (Theorem 1.12 below). (1) *Let $(X, (U_x \mid x \in X))$ be a special Moufang set with $|X| \geq 5$, and let G be its little projective group. Pick distinct $x, y \in X$ and let $H = G_x \cap G_y$. Then $[U_x, H] = U_x$, 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 and B are abelian, and either $Y \cong \mathrm{SL}_2(2)$ or $(\mathrm{P})\mathrm{SL}_2(3)$, or $[A, K] = A$, and hence Y is quasisimple.*

As noted in the abstract we characterize the root groups of a special Moufang set in terms of the permutation action and the structure of the little projective group. More precisely in §4 we prove the following theorem.

THEOREM B. *Let $\mathbb{M} = \{X, (U_x \mid x \in X)\}$ be a special Moufang set and let $x \in X$. Then (1) the root group U_x is the unique normal subgroup of G_x which is regular on $X \setminus \{x\}$;*

Received 3 November 2006; revised 17 August 2007; published online 25 January 2008.

2000 *Mathematics Subject Classification* 17C60, 20E42 (primary), 17C30 (secondary).

The first author is a Postdoctoral Fellow of the Research Foundation – Flanders (Belgium) (FWO – Vlaanderen). The second author is partially supported by BSF grant no. 2004-083. The third author is partially supported by DFG under SFB 701. Part of this work was done while the first two authors were guests of the University of Bielefeld and were also partially supported by the DFG under SFB 701.

(2) if $N_x \leq G_x$ is a normal nilpotent subgroup such that N_x is transitive on $X \setminus \{x\}$, then $N_x = U_x$.

Theorem B(2) was already known before for many classes of Moufang sets (including some non-special ones) by a case-by-case analysis; see [1].

Unlike the concept of abstract rank one group, where the root groups are assumed to be nilpotent, there is no assumption on the structure of the root groups of a Moufang set. In fact the following is probably the most challenging conjecture in this area.

ROOT GROUPS CONJECTURE. Let \mathbb{M} be a Moufang set; then the following hold.

- (1) The root groups of \mathbb{M} are nilpotent.
- (2) If \mathbb{M} is special, then the root groups of \mathbb{M} are abelian.
- (3) If the root groups of \mathbb{M} are abelian, then \mathbb{M} is special.

Part (1) of the Root Groups Conjecture (RGC) seems too hard at this point. Note that by [7, Corollary 3.2], part (1) implies part (2). However, we believe that a direct proof of RGC(2) is within reach, and a portion of this paper is devoted to it. We prove RGC(2) in the case when the root groups of \mathbb{M} contain involutions.

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

Theorem C is proved in §5. Notice that in [9], Suzuki essentially considered *finite* Moufang sets in which the root groups have even order (see [9, Theorem, p. 515]), but he did not assume that the Moufang set is special. However on page 517 lines 16–17, he writes that it is rather difficult, *even in the finite case*, to show that the root groups are 2-groups and it requires character theory.

In view of Theorem C, and to resolve RGC(2), we may assume that the root groups of \mathbb{M} do not contain involutions. By [2, Proposition 4.6] (see Proposition 1.6) U is uniquely 2-divisible. In §6 we use this fact to prove the following result which gives a natural path for proving RGC(2), namely to show that the μ -maps are involutions. The μ -maps are defined in equation (1.1) below and discussed thereafter.

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

The μ -maps play a fundamental role in the analysis of a Moufang set; see [2, 3, 7]. In Corollary 6.4 we apply Theorem D to characterize the Moufang sets associated with $\mathrm{PSL}_2(k)$, k a commutative field of characteristic $\neq 2$: these are precisely those special Moufang sets such that the two-point stabilizer is abelian (and the root groups contain no involutions).

In the course of working with our Moufang sets (and not necessarily the special ones), we encountered what we call the *opposite Moufang set* and the *mirror Moufang set*; these are introduced in §§2 and 3, respectively. Finally, §7 of this paper contains a number of results that may help in proving part (2) of the RGC.

1. Generalities on Moufang sets

Throughout this paper our notation follow [2]. We recall some facts and definitions and add some basic lemmas.

DEFINITION 1.1. A *Moufang set* is a set X with $|X| \geq 3$, together with a permutation group $G^\dagger \leq \text{Sym}(X)$ and a family of subgroups $\{U_x \mid x \in X\}$ such that:

- (1) $G^\dagger = \langle U_x \mid x \in X \rangle$;
- (2) U_x fixes x and acts regularly on $X \setminus \{x\}$, for all $x \in X$;
- (3) $\{U_x \mid x \in X\}$ is a conjugacy class of subgroups of G^\dagger .

Notice that G^\dagger is a doubly transitive permutation group. The group G^\dagger is called the *little projective group* of the Moufang set, and the subgroups $\{U_x \mid x \in X\}$ are called the *root groups* of the Moufang set.

DEFINITION 1.2. An isomorphism between two Moufang sets $(X, \{U_x \mid x \in X\})$ and $(Y, \{V_y \mid y \in Y\})$ is a bijection β from X to Y such that the map $\chi_\beta : \text{Sym}(X) \rightarrow \text{Sym}(Y) : g \mapsto \beta^{-1}g\beta$ maps each root group U_x onto the corresponding root group $V_{x\beta}$.

Here is a way to construct a Moufang set (cf. [3]). Start with a group U and let ∞ be a new symbol (not in U). Let X denote the set $X := U \cup \{\infty\}$. We write U in *additive notation* even though we do not assume that U is commutative. For $a \in U^* := U \setminus \{0\}$, we let $\alpha_a \in \text{Sym}(X)$ be the permutation which fixes ∞ and maps x to $x + a$ for every $x \in U$. Suppose that $\tau \in \text{Sym}(X)$ with $0\tau = \infty$ and $\infty\tau = 0$, and let

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

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

$$\mu_a := \alpha_{(-a)\tau^{-1}}^\tau \alpha_a \alpha_{-(a\tau^{-1})}^\tau, \tag{1.1}$$

where for group elements g, h , we denote $g^h = h^{-1}gh$. These complicated-looking permutations μ_a play an important role in the analysis of Moufang sets. It can be easily shown that μ_a interchanges 0 and ∞ , for all $a \in U^*$. In particular, for $a \in U^*$, $\tau\mu_a$ fixes 0 and ∞ and hence acts as a permutation on the set U . In the main theorem [3, Theorem 3.2] it is proved that the fact that $\mathbb{M}(U, \tau)$ is a Moufang set is equivalent to the fact that $\tau\mu_a \in \text{Aut}(U)$, for all $a \in U^*$.

The permutations $\mu_a, a \in U^*$, are invariants of $\mathbb{M}(U, \tau)$ in the following sense. First, from the definition of $\mathbb{M}(U, \tau)$ it follows that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \rho)$ for every permutation $\rho \in \text{Sym}(X)$ that interchanges 0 and ∞ and satisfies $U_\infty^\rho = U_\infty^\tau = U_0$. Now, although the permutations μ_a appear to depend on τ , once it is established that $\mathbb{M}(U, \tau)$ is a Moufang set, it turns out that μ_a depends only on the subgroups U_0 and U_∞ : it is the unique element in $U_0\alpha_aU_0$ that interchanges 0 and ∞ (see [2, Lemma 3.3(2)]). We observe that (cf. [2, Proposition 3.8(1)])

$$\mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_x) \quad \text{for all } x \in U^*. \tag{1.2}$$

When $\mathbb{M}(U, \tau)$ is a Moufang set we let

$$H := G_{0, \infty}^\dagger,$$

and we call H the *Hua subgroup* of $\mathbb{M}(U, \tau)$. The following facts will be frequently used without further reference (see [2, Lemma 3.3(1)] and [2, Proposition 3.9(2)]):

$$\mu_{-a} = \mu_a^{-1}, \quad \mu_a^{\mu_b} = \mu_{-a\mu_b}, \quad \mu_a^h = \mu_{ah} \quad \forall a, b \in U^* \quad \text{and} \quad \forall h \in H. \tag{1.3}$$

The above construction is of course the most general way to construct a Moufang set, as the following two lemmas indicate.

LEMMA 1.3. Let \mathcal{U} be a regular permutation group on the set U . Pick an element in U and denote it 0 . For each $a \in U$ let $\alpha_a \in \mathcal{U}$ be the unique permutation such that $0\alpha_a = a$. Define a binary operation (which is not necessarily commutative) on U by $a + b := a\alpha_b$, $a, b \in U$. Then $(U, +)$ is a group isomorphic to \mathcal{U} , and $a \rightarrow \alpha_a$ is the right regular representation of U on itself.

Proof. This is obvious. □

LEMMA 1.4. Let $\mathbb{M} = (X, \{U_x \mid x \in X\})$ be a Moufang set. Let $x \in X$ and denote $\infty := x$. Set

$$U := X \setminus \{\infty\},$$

pick an element in U and denote it 0 . Let $+$ be the binary operation on U as defined in Lemma 1.3 with U_∞ in place of \mathcal{U} . Let $\tau \in \text{Sym}(X)$ be any permutation interchanging 0 and ∞ such that $U_\infty^\tau = U_0$. Then $\mathbb{M} = \mathbb{M}(U, \tau)$.

Proof. Denote $\mathbb{M}(U, \tau) = (X, \{\bar{U}_x \mid x \in X\})$. By the definition of $\mathbb{M}(U, \tau)$, we have $\bar{U}_\infty = \{\alpha_a \mid a \in U\} = U_\infty$, $\bar{U}_0 = U_\infty^\tau = U_0$. Let $a \in U^*$; then $\bar{U}_a = \bar{U}_0^{\alpha_a} = U_0^{\alpha_a}$. Now since $(X, \{U_x \mid x \in X\})$ is a Moufang set, $U_0^{\alpha_a} = U_{0\alpha_a} = U_a$. Thus $\bar{U}_a = U_a$ and the lemma is proved. □

Let us recall the definition of a special Moufang set.

DEFINITION 1.5. A Moufang set $\mathbb{M}(U, \tau)$ is called *special* if the condition

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

holds.

We will frequently use the following fact without further reference (see [2, Lemma 4.3(2)]):

$$\text{If } \mathbb{M}(U, \tau) \text{ is special, then } a\mu_a = -a = a\mu_{-a} \quad \text{for all } a \in U^*. \tag{1.4}$$

The following proposition is taken from [2, Proposition 4.6] and will be used several times in this paper.

PROPOSITION 1.6. Assume that $\mathbb{M}(U, \tau)$ is a special Moufang set. Let $a \in U^*$, let $n \geq 1$ be a positive integer such that $a \cdot n \neq 0$, and let $\rho \in \text{Sym}(X)$ such that ρ interchanges 0 and ∞ and satisfies $\mathbb{M}(U, \rho) = \mathbb{M}(U, \tau) = \mathbb{M}(U, \rho^{-1})$. Then the following assertions hold.

- (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) 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 [10, Theorem 5.2(a), p. 55].
- (6) Assume that 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 $h_{a \cdot s} = h_a \cdot s^2$.

REMARK 1.7. Notice that in Proposition 1.6 and throughout this paper we multiply an element of U by an integer on the right. Note also that in view of Proposition 1.6, if $\mathbb{M}(U, \tau)$ is a special Moufang set, $a \in U^*$ and $\alpha = m/n \in \mathbb{Q}$ with $\text{gcd}(m, n) = 1$, then if a has infinite

order, then $a \cdot \alpha$ is well defined, and if $\gcd(n, p) = 1$ with $|a| = p$ (where p is a prime), then $a \cdot \alpha$ is well defined.

LEMMA 1.8. *Let $\mathbb{M}(U, \tau)$ be a Moufang set, and let $0 \neq V \leq U$ be a subgroup. Assume that $V^* \mu_v = V^*$, for all $v \in V^*$. Let $x \in V^*$ and let ρ be the restriction $\rho := \mu_x \upharpoonright V \cup \{\infty\}$. Then $\mathbb{M}(V, \rho)$ is a Moufang set. If $\mathbb{M}(U, \tau)$ is special, then $\mathbb{M}(V, \rho)$ is special.*

Proof. Since $\mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_x)$ (see [2, Proposition 3.8(1)]), we may assume that $\tau = \mu_x$. By [3, Theorem 3.2], $\mathbb{M}(V, \tau)$ is a Moufang set if and only if the Hua-maps of $\mathbb{M}(V, \tau)$ are contained in $\text{Aut}(V)$. But, by definition, the Hua-maps of $\mathbb{M}(V, \tau)$ are the restriction of the Hua-maps $\{h_a \mid a \in V^*\}$ of $\mathbb{M}(U, \tau)$ to V and, by our hypothesis, V is invariant under h_a , $a \in V^*$, because by [2, Proposition 3.9(1)] $h_a = \tau \mu_a$. Since $\mathbb{M}(U, \tau)$ is a Moufang set, the Hua-maps of $\mathbb{M}(U, \tau)$ are in $\text{Aut}(U)$, so their restrictions to V are in $\text{Aut}(V)$. It is evident that if $\mathbb{M}(U, \tau)$ is special then so is $\mathbb{M}(V, \tau)$. \square

COROLLARY 1.9. *Let $\mathbb{M}(U, \tau)$ be a Moufang set.*

(1) *For $h \in H$, let $V := \{a \in U \mid ah = a\}$ be the fixed point set of h on U . If $V \neq 0$, then $\mathbb{M}(V, \rho)$ (where $\rho = \mu_x \upharpoonright V \cup \{\infty\}$ and $x \in V^*$) is a Moufang set.*

(2) *If $\mathbb{M}(U, \tau)$ is special, $a \in U^*$ and $0 \neq V \leq U$ is a subgroup such that $V^* \mu_a = V^*$, then $V^* \mu_w = V^*$, for all $w \in V^*$, and hence $\mathbb{M}(V, \rho)$ is a special Moufang set, where $x \in V^*$ and $\rho = \mu_x \upharpoonright V \cup \{\infty\}$.*

Proof. (1) Let $v, w \in V$. Then, by equation (1.3), $v \mu_w h = v h \mu_w h = v \mu_w \in V$, and hence $V^* \mu_w = V^*$. Part (1) follows now from Lemma 1.8.

(2) Let $v, w \in V$ with $w \neq -v$; then by Lemma 5.2(4) below,

$$(v + w) \mu_a = (v \mu_w - w) \mu_a + w \mu_a;$$

by our hypothesis, $(v + w) \mu_a, w \mu_a \in V$, so $(v \mu_w - w) \mu_a \in V$ and applying μ_{-a} shows that also $v \mu_w - w \in V$, so $v \mu_w \in V$. Furthermore, by equation (1.4), $(-w) \mu_w = w \in V$. It now follows from Lemma 1.8 that $\mathbb{M}(V, \tau)$ is a special Moufang set. \square

We conclude this section by proving the perfectness of the little projective group of a special Moufang set, and we prove a conjecture of Timmesfeld; see [10, Remark, p. 26]. First we define what an abstract rank one group is.

DEFINITION 1.10 [10, pp. 1–2]. *An abstract rank one group with unipotent subgroups A and B is a group Y generated by its nilpotent subgroups A and B such that $A \neq B$ and such that*

$$\text{for each } a \in A^* \text{ there exists } b \in B^* \text{ with } A^b = B^a \text{ and vice versa} \tag{*}$$

(where $A^b = b^{-1} A b$). An abstract rank one group with unipotent subgroups A and B is called *special* if

$$\text{for each } a \in A^* \text{ and } b \in B^*, A^b = B^a \text{ implies } a^b = (b^{-1})^a. \tag{**}$$

The following facts, which appear in [10] and inside proofs there, will be used in the proof of Theorem 1.12.

PROPOSITION 1.11. *Let Y be an abstract rank one group with unipotent subgroups A and B . Let $\Omega = \{A^y \mid y \in Y\}$ and let $K = N_Y(A) \cap N_Y(B)$ be the diagonal subgroup. Let $\circ : Y \rightarrow Y/Z(Y) =: Y^\circ$ be the canonical homomorphism. Then*

- (1) Y is not nilpotent;
- (2) $Z(Y)$ is the kernel of the action of Y on Ω , and $A \cap Z(Y) = 1 = B \cap Z(Y)$;
- (3) Y° is an abstract rank one group with unipotent subgroups A° and B° and $Z(Y^\circ) = 1$;
- (4) $N_Y(A)$ is the (full) inverse image under \circ of $N_{Y^\circ}(A^\circ)$ and hence if H is the diagonal subgroup of Y° then the (full) inverse image of H under \circ is K ;
- (5) Y is special if and only if for each $a \in A^*$ there exists $b \in B^*$ with $a^b = (b^{-1})^a$ and vice versa;
- (6) if Y is special, then Y° is special;
- (7) if Y° is special, then Y° is (the little projective group of) a special Moufang set as defined in Definition 1.5.

Proof. Part (1) follows from, e.g., [10, (2.10), p. 25]. Let N be the kernel of the action of Y on Ω . By [10, (1.10), p. 13], if $N \neq Z(Y)$, then $Y = NA$. But then $A \trianglelefteq Y$, a contradiction; this shows the first part of (2). The second part of (2) follows from the fact that $N_A(B) = N_B(A) = 1$, (cf. [10, (1.2)(3), p. 2]). The first part in (3) follows from [10, Exercise (1.13)(2), p. 15] and (1). The second part of (3) is by [10, (2.1), p. 17].

To prove (4), note first that for $y \in N_Y(A)$,

$$A^\circ = (A^y)^\circ = (A^\circ)^{y^\circ},$$

so $N_Y(A)^\circ \leq N_{Y^\circ}(A^\circ)$. Conversely, let $g \in N_{Y^\circ}(A^\circ)$ and let $y \in Y$ with $y^\circ = g$. Then $(A^y)^\circ = A^\circ$. Hence $A^y \leq AZ(Y)$. But if $A^y \neq A$, then $Y = \langle A, A^y \rangle$ (because by definition $Y = \langle A, B \rangle$ and Y is doubly transitive on Ω). Thus since by (1) $Y \neq AZ(Y)$, $A^y = A$, so $y \in N_Y(A)$ and the first part of (4) is established. The second part of (4) follows from the first since the first part applies also to B in place of A .

Note that Timmesfeld’s definition of ‘special’ (as defined in Definition 1.10) is not precisely the assumption in (5). However, since $N_B(A) = 1$, the b in condition (*) of Definition 1.10 is unique. Also, since $A \cap B = 1$, the equality $a^b = (b^{-1})^a$ implies that $A^b = B^a$. This shows that (5) is equivalent to condition (**) of Definition 1.10.

Finally (6) is immediate from (5), and for (7) see [3, Remark 5.1, p. 430]. □

THEOREM 1.12. *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 the following hold.*

- (1) $[U_\infty, H] = U_\infty$, 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 $Y \cong \text{SL}_2(2)$ or $(\text{P})\text{SL}_2(3)$, or $[A, K] = A$ and hence Y is quasisimple.

Proof. (1) Let $V \subseteq U$ be the set of elements $u \in U$ such that $\alpha_u \in [U_\infty, H]$. Note that for all $u \in U$ and all $h \in H$, we have

$$[\alpha_u, h] = \alpha_{-u} \alpha_u^h = \alpha_{-u} \alpha_{uh} = \alpha_{-u+uh},$$

so

$$-u + uh \in V \quad \text{for all } u \in U \quad \text{and} \quad h \in H. \tag{1.5}$$

By (1.4) and (1.5), $-u + u\mu_u\mu_w = -u - u\mu_w \in V$, for all $u, w \in U^*$. Therefore, since $|U| > 3$, there exist $u, w \in U^*$ with $u\mu_w \neq -u$ or $w\mu_u \neq -w$ (see [2, Lemma 4.9(3)]), and hence

$$V \neq 0.$$

Assume first that U is not a group of exponent 2. Since H normalizes U_∞ , it normalizes $[U_\infty, H]$, and hence V is H -invariant. By [7, Theorem 1.2], $V = U$.

Hence we may assume that U is of exponent 2. Let $Q := U/V$, and write $u \equiv w$ for $u + V = w + V$ in Q . As we saw, taking $h = \mu_u\mu_w$ in (1.5) shows that

$$u\mu_w \equiv u \quad \text{for all } u, w \in U^*. \tag{*}$$

By (*) and [2, Lemma 4.4(3)] (see Proposition 5.2(5) below) we get for all distinct $u, w \in U^*$

$$u \equiv u\mu_{u+w} = w + u + u\mu_w + w \equiv w + u + u + w = 0.$$

Since u is arbitrary, again $V = U$. This shows that $U_\infty = [G, U_\infty]$. It follows that $U_\infty \leq [G, G]$, and since G is generated by the conjugates of U_∞ , we have $G = [G, G]$.

(2) If $|A| = 2$ or 3 , then $Y \cong \text{SL}_2(2)$ or $Y \cong (\text{P})\text{SL}_2(3)$, respectively; see for example [10, (2.10)(1), p. 25]. Hence we may assume that $|A| \geq 4$.

Let $\circ : Y \rightarrow Y/Z(Y) =: Y^\circ$ be the canonical homomorphism. By Proposition 1.11, Y° is a special Moufang set. Hence we may assume without loss that $Y^\circ = G$, $A^\circ = U_\infty$ and $B^\circ = U_0$. By definition, $A \cong U_\infty$ is nilpotent, so by [7, Corollary 3.2], A is abelian.

Now, let $\alpha_u \in U_\infty$ and $h \in H$. Let $a \in A$ with $a^\circ = \alpha_u$ and, using Proposition 1.11(4), let $y \in K$ with $y^\circ = h$. Then $[a, y] \in A$ and $[a, y]^\circ = [\alpha_u, h]$. Thus we see that $[A, K]^\circ \geq [U_\infty, H] = U_\infty$, by (1). Since $[A, K] \leq A$, and since $\circ : A \rightarrow U_\infty$ is bijective, we see that $[A, K] = A$. Thus $A \leq [Y, Y]$, and since Y is generated by the conjugates of A , Y is perfect.

Next, since G is perfect and U_∞ is abelian, Iwasawa's Lemma (cf. [6, Theorem 9.27, p. 263]) implies that G is simple. Thus Y is quasisimple. \square

2. The opposite Moufang set

For future reference we define and briefly discuss the notion of the opposite Moufang set.

LEMMA 2.1. *Let $\mathbb{M}(U, \tau)$ be a Moufang set. Let $(U^\circ, \oplus) := (U, +)^\circ$ be the opposite group, that is, as sets $U^\circ = U$ and for $a, b \in U^\circ$, we have $a \oplus b = b + a$. Let $\text{inv} : U \rightarrow U$ be the inverse map (a) $\text{inv} = -a$ and extend inv to a map $\text{inv} : X \rightarrow X$ via $(\infty) \text{inv} = \infty$. Then $\mathbb{M}(U^\circ, \tau^{\text{inv}})$ is a Moufang set, where $\tau^{\text{inv}} = \text{inv} \circ \tau \circ \text{inv}$.*

Proof. Consider $\mathbb{M}(U^\circ, \tau^{\text{inv}})$. By definition, $U_\infty^\circ = \{\alpha_a^\circ \mid a \in U^\circ\}$, where $b\alpha_a^\circ = a + b$, for $a \in U^\circ \setminus \{0\}$ and $b \in U^\circ$. Hence $U_\infty^\circ = U_\infty^{\text{inv}}$. It follows that $U_0^\circ = U_0^{\text{inv}}$ and then it is easy to check that $U_a^\circ = U_{-a}^{\text{inv}}$ for all $a \in U^*$. This implies that $\mathbb{M}(U^\circ, \tau^{\text{inv}})$ is a Moufang set. \square

NOTATION 2.2. If $\mathbb{M}(U, \tau)$ is a Moufang set, we denote by $\mathbb{M}(U^\circ, \tau^{\text{inv}})$ the opposite Moufang set as in Lemma 2.1. We use $\alpha_a^\circ, \mu_a^\circ, U_\infty^\circ, U_a^\circ$, etc. to denote the various maps and the root groups of $\mathbb{M}(U^\circ, \tau^{\text{inv}})$ as in [2, Notation 3.1 and 3.2].

LEMMA 2.3. *Let $\mathbb{M}(U, \tau)$ be a Moufang set and let $\mathbb{M}(U^\circ, \tau^{\text{inv}})$ be the opposite Moufang set. Then*

- (1) *for all $a, b \in U$, $b\alpha_a^\circ = a + b$ and $\alpha_a^{\text{inv}} = \alpha_{-a}^\circ$, thus $U_\infty^\circ = U_\infty^{\text{inv}}$;*
- (2) *let G be the little projective group of $\mathbb{M}(U, \tau)$ (and G° be the little projective group of $\mathbb{M}(U^\circ, \tau^{\text{inv}})$); then $G^\circ = G^{\text{inv}}$.*

- (3) $\mu_a^{\text{inv}} = \mu_{-a}^{\circ}$ for all $a \in U^*$;
- (4) $H = H^{\circ}$;
- (5) $\mathbb{M}(U, \tau)$ is special if and only if $\tau^{\text{inv}} = \tau$ and then $\mu_a^{\circ} = \mu_{-a}$.

Proof. (1) By definition, the statement holds.

(2) By (1), $U_{\infty}^{\circ} = U_{\infty}^{\text{inv}}$ and hence also $U_0^{\circ} = U_0^{\text{inv}}$. But by [3], $G = \langle U_0, U_{\infty} \rangle$ and similarly for G° ; so (2) holds.

(3) Since $U_0^{\text{inv}} = U_0^{\circ}$, we have $(U_0 \alpha_a U_0)^{\text{inv}} = U_0^{\circ} \alpha_a^{\circ} U_0^{\circ}$. Now by [2, Lemma 3.3(2)], for any $a \in U^*$, we have μ_a is the unique element in $U_0 \alpha_a U_0$ that interchanges 0 and ∞ and similarly for μ_a° . Since μ_a^{inv} interchanges 0 and ∞ , it follows that $\mu_a^{\text{inv}} = \mu_{-a}^{\circ}$.

(4) Since $\mathbb{M}(U, \tau)$ is a Moufang set the main theorem of [3] says that $H \leq \text{Aut}(U)$. Thus $h^{\text{inv}} = h$ for all $h \in H$, and it follows that $H^{\circ} = H$.

(5) First, by definition, $\mathbb{M}(U, \tau)$ is special if and only if $\tau^{\text{inv}} = \tau$. By [2, Lemma 4.2], $\tau^{\text{inv}} = \tau$ if and only if $\mu_a^{\text{inv}} = \mu_a$ for all $a \in U$. By [2, Lemma 3.3], $\mu_{-a} = \mu_a^{-1}$, for all $a \in U$ and hence (5) is a consequence of (3). □

REMARK 2.4. We note here that clearly $\mathbb{M}(U^{\circ}, \tau^{\text{inv}}) \cong \mathbb{M}(U, \tau)$. Indeed, the permutation $\text{inv} \in \text{Sym}(X)$ induces a Moufang set isomorphism from $\mathbb{M}(U, \tau)$ to $\mathbb{M}(U^{\circ}, \tau^{\text{inv}})$ since $U_a^{\text{inv}} = U_{(a)\text{inv}}^{\circ}$ for all $a \in X$. This certainly does not mean that the concept is useless; one could compare it to the fact that a quaternion algebra is isomorphic to (but not equal to) its opposite algebra.

3. The mirror Moufang set

In this section we start with a Moufang set $\mathbb{M}(U, \tau)$ and we switch the role of U_0 and U_{∞} . The resulting Moufang set $\mathbb{M}(U^t, \tau^{-1})$ is the same Moufang set, that is, $\mathbb{M}(U, \tau) = \mathbb{M}(U^t, \tau^{-1})$; however, we give it a different name: the mirror Moufang set. The reason is that the μ -maps and the Hua-maps of $\mathbb{M}(U^t, \tau^{-1})$ are different from those of $\mathbb{M}(U, \tau)$, and in this section we are actually interested in how they are related.

LEMMA 3.1. *Let U^t be the group with underlying set $U \setminus \{0\} \cup \{\infty\}$, and with group operation \oplus defined by $x \oplus y = (x\tau^{-1} + y\tau^{-1})\tau$. Let h_a^t denote the Hua-maps (and μ_a^t denote the μ -maps) for $\mathbb{M}(U^t, \tau^{-1})$. Then*

- (1) $\mathbb{M}(U^t, \tau^{-1}) = \mathbb{M}(U, \tau)$;
- (2) $\mu_a^t = \mu_a^{-1}$ and $h_a^t = \tau^{-1}\mu_{-a}$ for all $a \in U^*$.

Proof. Notice first that \oplus is a group operation. Note next that the neutral element of U^t is ∞ ; denote $0' := \infty$. The element that takes the role of ∞ for $\mathbb{M}(U^t, \tau^{-1})$ is 0, so denote $\infty' = 0$. For $a \in U^t \setminus \{0'\}$, let $\alpha_a^t \in \text{Sym}(X)$ be the permutation fixing ∞' and such that $\alpha_a^t : b \mapsto b \oplus a$, $b \in U^t$. Then, by definition, for each $a \in U^t$, we have $b\alpha_a^t = b\tau^{-1}\alpha_{a\tau^{-1}}\tau$, that is,

$$\alpha_a^t = \gamma_{a\tau^{-1}}$$

(recall from [2] that $\gamma_x = \tau^{-1}\alpha_x\tau \in U_0$), which implies that $U_{\infty'}^t = U_0$. Then $U_{0'}^t = (U_{\infty'}^t)^{\tau^{-1}} = U_0^{-1} = U_{\infty}$. Further, by definition, for $a \in U^t \setminus \{0'\}$ we get

$$U_a^t = (U_{0'}^t)^{\alpha_a^t} = U_{\infty}^{\gamma_{a\tau^{-1}}} = U_{\infty\gamma_{a\tau^{-1}}} = U_a.$$

We have thus shown that for each $x \in X = U \cup \{\infty\}$, we have $U_x^t = U_x$, so $\mathbb{M}(U, \tau) = \mathbb{M}(U^t, \tau^{-1})$ and (1) holds.

Let $a \in U^*$, by [2, Proposition 3.10(4)], and since $\mu_a^2 \in \text{Aut}(U)$,

$$\mu_a = \alpha_{-(\sim a)}\mu_{-a}\alpha_a\mu_a\alpha_{(\sim(-a))}\mu_a^2. \tag{3.1}$$

Notice that

$$\alpha_a^{\mu_a} = \alpha_{a\mu_a}^t,$$

since $(\alpha_{a\mu_a}^t)^{\mu_{-a}} = \alpha_{a\mu_a\tau^{-1}}^{\tau\mu_{-a}} = \alpha_a$. But by definition of the μ -maps in $\mathbb{M}(U^t, \tau^{-1})$ (where the roles of U_0 and U_∞ are interchanged), we know that $\mu_{a\mu_a}^t$ is the unique element of $U_\infty\alpha_{a\mu_a}^tU_\infty$ that swaps 0 and ∞ . Hence by equation (3.1),

$$\mu_a = \mu_{a\mu_a}^t.$$

Replacing a with $a\mu_{-a}$ and recalling (see [2, Proposition 3.9(2)]) that $\mu_{a\mu_{-a}} = \mu_{-a}$, we get $\mu_a^t = \mu_{-a}^{-1}$.

Now, by [2, Proposition 3.9(1)], and keeping in mind that $\tau^t = \tau^{-1}$, we have

$$h_a^t = \tau^t\mu_a^t = \tau^{-1}\mu_{-a},$$

which finishes the proof of this lemma. □

REMARK 3.2. For $a, b \in U^*$ with $a \neq \sim b$, let

$$a \oplus b := (a\tau^{-1} + b\tau^{-1})\tau,$$

as above. Then

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

By [2, Propositions 3.3(1), 3.9(2) and 3.10(3)], we have

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

It follows from [2, Proposition 3.10(5)], that

$$\mu_{a \oplus b} = \mu_b\mu_{\sim b-a}\mu_a.$$

Further, if $\mathbb{M}(U, \tau)$ is special, then $\sim a = -a$ and we have

$$\mu_{a \oplus b}^t = \mu_{-(a \oplus b)} = \mu_{(-b) \oplus (-a)} = \mu_{-a}\mu_{a+b}\mu_{-b}.$$

4. Uniqueness of U in special Moufang sets

In this section we continue with the notation of [2]. We let $\mathbb{M}(U, \tau)$ be a special Moufang set, G its little projective group and $H = G_{0,\infty}$ its Hua subgroup. Our aim in this section is to prove the following two characterizations of the root groups.

THEOREM 4.1. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set. Then U_∞ is the unique normal subgroup of G_∞ which is regular on U .*

THEOREM 4.2. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set. If $N_\infty \leq G_\infty$ is a normal nilpotent subgroup such that N_∞ is transitive on U , then U is abelian and $N_\infty = U_\infty$.*

We start with the proof of Theorem 4.1. We distinguish two cases according to whether U is a group of exponent 2 or not. We start with the latter case, so

until Lemma 4.8 we assume that U is not a group of exponent 2.

In particular, by the main result in [7],

$$U \text{ contains no non-trivial proper } H\text{-invariant subgroup.} \tag{*}$$

LEMMA 4.3. *Let $G \leq \text{Sym}(X)$ be a transitive permutation group on X . Then*

- (1) $C_{\text{Sym}(X)}(G)$ is semiregular;
- (2) if G is regular, then $C_{\text{Sym}(X)}(G)$ is regular;
- (3) if G is abelian and regular then $C_{\text{Sym}(X)}(G) = G$.

Proof. Let $\sigma \in C_{\text{Sym}(X)}(G)$. Since G is transitive on the fixed points of σ , it follows that $\sigma = 1$ or σ has no fixed points, so (1) holds. Condition (2) holds because the left regular representation commutes with the right regular representation and (3) is immediate from (2). □

LEMMA 4.4. *Let $W_\infty \leq G_\infty$ be a normal subgroup which is regular on U with $W_\infty \neq U_\infty$. Then*

- (1) $W_\infty = \{\alpha_a^\circ \mid a \in U\}$, where $b\alpha_a^\circ = a + b$ for all $a, b \in U$, and hence $W_\infty = U_\infty^\circ$, where $\mathbb{M}(U^\circ, \tau)$ is the opposite Moufang set of $\mathbb{M}(U, \tau)$;
- (2) the little projective group G° of $\mathbb{M}(U^\circ, \tau)$ is equal to G ;
- (3) the center of U is trivial;
- (4) $\mu_a^\circ = \mu_{-a}$ for all $a \in U$.

Proof. (1) Since $U_\infty \cap W_\infty$ is H -invariant and distinct from U_∞ , it follows from (*) that $U_\infty \cap W_\infty = 1$, and hence $[U_\infty, W_\infty] = 1$. Thus, by Lemma 4.3, W_∞ is as claimed. The rest follows from Lemma 2.3(1) and (5).

(2) Recall from Lemma 2.3(2) that $G^\circ = G^{\text{inv}}$. Now $U_\infty^\circ \leq G_\infty$ and $G_\infty = U_\infty^\circ H$. But by Lemma 2.3(4), $H^\circ = H$; so we see that $G_\infty = U_\infty^\circ H = U_\infty^\circ H^\circ \leq G^\circ$. By Lemma 2.3(5), $\mu_a \in G^\circ$ for all $a \in U^*$. Since for each $a \in U^*$, $G = \langle G_\infty, \mu_a \rangle$, we see that $G \leq G^\circ = G^{\text{inv}}$ and so $G = G^\circ$.

(3) If $Z(U) \neq 0$, then since $Z(U)$ is H -invariant, U is abelian, by (*). But then, by Lemma 4.3(3), $U_\infty^\circ = U_\infty$, a contradiction.

(4) This is Lemma 2.3(5). □

In view of Lemma 4.4(1), to prove Theorem 4.1 we may assume by contradiction that U_∞° is a normal subgroup of G_∞ . We let

$$\beta_a := \alpha_a^\circ, \quad a \in U \quad \text{where } \alpha_a^\circ \text{ as in Lemma 4.4(1).}$$

LEMMA 4.5. *Let $a \in U^*$; then*

- (1) $\alpha_a \alpha_{-a\mu_{-b}}^{\mu_b} \alpha_a = \mu_a = \beta_{-a} \beta_{a\mu_{-b}}^{\mu_b} \beta_{-a}$ for all $b \in U^*$;
- (2) $\alpha_a \alpha_a^{\mu_a} \alpha_a = \mu_a = \beta_{-a} \beta_{-a}^{\mu_a} \beta_{-a}$;
- (3) if $a \cdot 2 \neq 0$, then

$$\alpha_{a \cdot 2} \alpha_{a \cdot \frac{1}{2}}^{\mu_a} \alpha_{a \cdot 2} = \mu_{a \cdot 2} = \beta_{-a \cdot 2} \beta_{-a \cdot \frac{1}{2}}^{\mu_a} \beta_{-a \cdot 2},$$

where $a \cdot \frac{1}{2} \in U^*$ is the unique element such that $(a \cdot \frac{1}{2}) \cdot 2 = a$ (see Proposition 1.6);

- (4) $c_a := \alpha_a \beta_{-a} \in H$;
- (5) c_b commutes with μ_a , for every $b \in U$ which commutes with a ;

(6) $\mu_a^2 = c_{a \cdot 3}$.

Proof. (1) To get the first equality in (1) we apply [2, Proposition 3.10(2)] to the Moufang set $\mathbb{M}(U, \tau)$ recalling that $\mathbb{M}(U, \tau) = \mathbb{M}(U, \mu_b)$ for all $b \in U^*$. Notice that by [2, Lemma 4.2], $\sim a = -a$ where $\sim a = (-a\mu_{-b})\mu_b$, $b \in U^*$. Hence the first equality of (1) holds. The second equality is a similar application to the opposite Moufang set $\mathbb{M}(U^\circ, \tau)$, using Lemma 2.3(5).

(2) The statement follows from (1) by taking $b = a$ and recalling that $a\mu_{-a} = -a$.

(3) In (1), take $a \cdot 2$ in place of a and a in place of b . By Proposition 1.6(2), we have $(a \cdot 2)\mu_{-a} = -a \cdot \frac{1}{2}$; so (3) follows.

(4) Since $G_\infty = U_\infty H$, for each $b \in U^*$ there exists an $a \in U^*$ such that $\alpha_a \beta_b \in H$, because $\beta_b \in G_\infty$. In particular $0\alpha_a \beta_b = 0$, so $b = -a$.

(5) By [2, Proposition 3.9(2)], for $b \in C_U(a)$ we have $\mu_a^{c_b} = \mu_{ac_b} = \mu_a$; so c_b commutes with μ_a .

(6) By (4) and (5),

$$\alpha_a^{\mu_a} \beta_{-a}^{\mu_a} = \alpha_a \beta_{-a},$$

or

$$\alpha_a \alpha_a^{\mu_a} \alpha_a \alpha_{-a} \beta_a \beta_{-a} \beta_{-a}^{\mu_a} \beta_{-a} = \alpha_{a \cdot 2} \beta_{-a \cdot 2}.$$

Using (2) we get

$$\mu_a \alpha_{-a} \beta_a \mu_a = \alpha_{a \cdot 2} \beta_{-a \cdot 2};$$

so since μ_a commutes with c_{-a} , (6) follows. □

PROPOSITION 4.6. (1) *There exists no $a \in U^*$ of order 2.*

(2) *U is a group of exponent 3.*

Proof. (1) Assume that $a \in U^*$ has order 2. Then by [2, Lemma 4.3(5)], $\mu_a^2 = 1$. By Lemma 4.5(6),

$$c_a = c_{a \cdot 3} = \mu_a^2 = 1,$$

so a is in the center of U . But the center of U is trivial, which is a contradiction.

(2) Let $a \in U^*$. By (1) $a \cdot 2 \neq 0$; so by Proposition 1.6 there exists a unique element $a \cdot \frac{1}{2} \in U^*$, such that $(a \cdot \frac{1}{2}) \cdot 2 = a$. We have the following equivalent equalities:

$$\begin{aligned} (\alpha_{a \cdot \frac{1}{2}} \beta_{-a \cdot \frac{1}{2}})^{\mu_a} &= c_{a \cdot \frac{1}{2}}^{\mu_a} = c_{a \cdot \frac{1}{2}} = \alpha_{a \cdot \frac{1}{2}} \beta_{-a \cdot \frac{1}{2}} && \text{(by Lemma 4.5(5))} \\ \alpha_{a \cdot \frac{1}{2}}^{\mu_a} \beta_{-a \cdot \frac{1}{2}}^{\mu_a} &= \alpha_{a \cdot \frac{1}{2}} \beta_{-a \cdot \frac{1}{2}} \\ \alpha_{a \cdot 2} \alpha_{a \cdot \frac{1}{2}}^{\mu_a} \alpha_{a \cdot 2} \alpha_{-a \cdot 2} \beta_{a \cdot 2} \beta_{-a \cdot 2} \beta_{-a \cdot \frac{1}{2}}^{\mu_a} \beta_{-a \cdot 2} &= \alpha_{a \cdot 2 \frac{1}{2}} \beta_{-a \cdot 2 \frac{1}{2}} \\ \mu_{a \cdot 2} \alpha_{-a \cdot 2} \beta_{a \cdot 2} \mu_{a \cdot 2} &= \alpha_{a \cdot 2 \frac{1}{2}} \beta_{-a \cdot 2 \frac{1}{2}} && \text{(by Lemma 4.5(3))} \\ \mu_{a \cdot 2}^2 \alpha_{-a \cdot 2} \beta_{a \cdot 2} &= \alpha_{a \cdot 2 \frac{1}{2}} \beta_{-a \cdot 2 \frac{1}{2}} && ([c_{a \cdot 2}, \mu_{a \cdot 2}] = 1) \\ \alpha_{a \cdot 4} \beta_{-a \cdot 4} &= \alpha_{a \cdot 2 \frac{1}{2}} \beta_{-a \cdot 2 \frac{1}{2}} && (\mu_{a \cdot 2}^2 = c_{a \cdot 6}) \\ \alpha_{a \cdot 1 \frac{1}{2}} \beta_{-a \cdot 1 \frac{1}{2}} &= 1 \end{aligned}$$

Thus, if $a \cdot 3 \neq 0$, then $a \cdot 1 \frac{1}{2}$ is a non-zero element in the center of U , a contradiction. □

PROPOSITION 4.7. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set such that U is not a group of exponent 2. Then U_∞ is the unique normal subgroup of G_∞ which is regular on U .*

Proof. Otherwise $U_\infty^\circ \neq U_\infty$ is a normal subgroup of G_∞ . By Proposition 4.6, U is a group of exponent 3, so U is nilpotent (cf. [5, 12.3.5, 12.3.6]). Hence, by [7, Corollary 3.2], U is abelian, contradicting Lemma 4.4(3). \square

LEMMA 4.8. *Assume that U is of exponent 2. Then H contains no non-trivial normal subgroup of exponent 2.*

Proof. Recall that by [2, Lemma 4.3(5)], $\mu_x^2 = 1$, for all $x \in U^*$. Assume that $1 \neq E \trianglelefteq H$ is a normal subgroup of exponent 2. Let $1 \neq h \in E$; choose an element $a \in U^*$ with $a \neq ah$, and let $c := ah$. Then $b := a + c$ is a non-zero fixed point of h . Using equation (1.3) we get

$$E \ni [\mu_b \mu_a, h] = \mu_a \mu_b (\mu_b \mu_a)^h = \mu_a \mu_b \mu_{bh} \mu_{ah} = \mu_a \mu_b \mu_b \mu_c = \mu_a \mu_c,$$

so

$$1 = (\mu_a \mu_c)^2 = \mu_{c \mu_a} \mu_c.$$

It follows that $\mu_c = \mu_{c \mu_a}$. But the only fixed point of μ_x , $x \in U^*$, is x , because μ_x is conjugate in G to α_x (see [2, 4.3(5)]). Thus $c = c \mu_a$ which implies $a = c$, a contradiction. \square

LEMMA 4.9. *Assume that U is of exponent 2. Then U_∞ is the only regular normal subgroup of G_∞ .*

Proof. Let $W = W_\infty$ be a regular normal subgroup of G_∞ . Let $w \in W$; then $w = h \alpha_a$, for some $a \in U$ and $h \in H$. Since $W \trianglelefteq G_\infty$, conjugating by α_a shows that $\alpha_a h \in W$, which implies that $h^2 = h \alpha_a \alpha_a h \in W$. But W is regular and h^2 fixes 0; so $h^2 = 1$. Thus we have shown that

$$\text{if } h \alpha_a \in W, \text{ where } h \in H, \text{ then } h^2 = 1.$$

Now, let $h_1 \alpha_a, h_2 \alpha_b \in W$. Then

$$W \ni h_1 \alpha_a h_2 \alpha_b = h_1 h_2 h_2 \alpha_a h_2 \alpha_b = (h_1 h_2) \alpha_{ah_2+b}.$$

This shows that

$$E := \{h \in H \mid h \alpha_a \in W \text{ for some } a \in U\}$$

is an elementary abelian 2-subgroup of H . But if $h \in E$, then $h \alpha_a \in W$ for some $a \in U$, and then for $g \in H$ we get

$$W \ni (h \alpha_a)^g = h^g \alpha_{ag}.$$

It follows that $h^g \in E$; so E is normal in H . By Lemma 4.8, $E = 1$. Thus $W \subseteq U_\infty$, and since W is regular $W = U_\infty$ as asserted. \square

Now, note that by Proposition 4.7 and Lemma 4.9, the proof of Theorem 4.1 is complete. We now turn to the proof of Theorem 4.2.

Proof of Theorem 4.2. Set $N := N_\infty$. First suppose that U is not abelian; then by [7, Theorem 1.2] we have $U_\infty \cap N = 1$ or $U_\infty \cap N = U_\infty$. If $U_\infty \cap N = 1$, then N centralizes U_∞ ; so by Lemma 4.3 $N \cong U_\infty$, so U is nilpotent and by [7, Corollary 3.2], U is abelian, which is a contradiction.

If $U_\infty \cap N = U_\infty$, then $U_\infty \leq N$ and again U is nilpotent and hence abelian, which is a contradiction. Thus U is abelian; in particular, by [2, Lemma 5.1], $\mu_x^2 = 1$ for all $x \in U^*$.

Replacing N by NU_∞ we may assume that $U_\infty \leq N$ (notice that NU_∞ is nilpotent). Let $\mathcal{H} := N \cap H$, so $N = U_\infty \rtimes \mathcal{H}$. Since no non-trivial element of H centralizes U_∞ , we have

$Z(N) \leq U_\infty$ (because if $\alpha_a h \in Z(N)$, $h \in \mathcal{H}$, then h centralizes U_∞). Let

$$W := \{a \in U \mid \alpha_a \in Z(N)\} = \{a \in U \mid ah = a \text{ for all } h \in \mathcal{H}\}.$$

Notice that $W \neq 0$ is H -invariant; so unless U is an elementary abelian 2-group, we have $W = U$. But then any $h \in \mathcal{H}$ fixes all $a \in U$ and hence $h = 1$, that is, $N = U_\infty$.

We may thus assume that U has exponent 2 and that $\mathcal{H} \neq 1$; so $W \neq U$. Note that $\mathcal{H} \trianglelefteq H$ and that for $b \in W^*$ and $h \in \mathcal{H}$ we have $\mu_b^h = \mu_{bh} = \mu_b$. Hence

$$h^{\mu_a} = h^{\mu_b \mu_a} \in \mathcal{H} \quad \text{for all } h \in \mathcal{H}, \quad a \in U^* \quad \text{and} \quad b \in W^*.$$

Now for $h \in \mathcal{H}$ and $a \in U^*$ we have $\mathcal{H} \ni [\mu_a, h] = \mu_a \mu_{ah}$. It follows that for $b \in W^*$, $b = b\mu_a \mu_{ah}$, and so $b\mu_a = b\mu_{ah} = bh^{-1}\mu_a h = b\mu_a h$. Since $b\mu_a$ is fixed by all $h \in \mathcal{H}$, this implies that $b\mu_a \in W$. We have shown that

$$b\mu_a \in W \quad \text{for all } b \in W^* \quad \text{and} \quad a \in U^*. \tag{i}$$

We have $\mu_a = \alpha_a \alpha_a^{\mu_a} \alpha_a$, so $b\mu_a = ((b+a)\mu_a + a)\mu_a + a \in W$ for all $b \in W^*, a \in U^*$, or

$$a = b\mu_a - ((b+a)\mu_a + a)\mu_a \quad \text{for all } b \in W^* \quad \text{and} \quad a \in U^*. \tag{ii}$$

We will find $a \notin W$ and $b \in W^*$ such that $(b+a)\mu_a + a \in W$, this contradicts (i) and (ii).

Let $\alpha_a \in (Z_2(N) \cap U_\infty) \setminus Z(N)$ (so $a \in U \setminus W$). Then $[\alpha_a, h] \in Z(N)$, that is,

$$a + ah \in W \quad \text{for all } h \in \mathcal{H}. \tag{iii}$$

For some $h \in \mathcal{H}$ we have $b = a + ah \in W^*$, and so $ah = a + b \neq a$. Now $(a+b)\mu_a + a = (ah)\mu_a + a = ah^{\mu_a} + a \in W$ because $h^{\mu_a} \in \mathcal{H}$ and by (iii); this contradiction completes the proof. □

5. Special Moufang sets with $\text{Inv}(U) \neq \emptyset$ have abelian root groups

In this section $\mathbb{M}(U, \tau)$ is a special Moufang set. We continue with the notation of [2].

LEMMA 5.1. *Let $a, b \in U^*$; then the order of $a\mu_b$ equals the order of a .*

Proof. The lemma holds because $(-a)\mu_a = a$, and so $a\mu_b = (-a)\mu_a\mu_b$, and because $\mu_a\mu_b \in \text{Aut}(U)$. □

LEMMA 5.2. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set, let $a, b, x \in U^*$, and set $c = (b\mu_{-x} - a\mu_{-x})\mu_x$. Then*

- (1) $c = (-b - a\mu_{-b})\mu_b = (b\mu_{-a} + a)\mu_a$;
- (2) $\mu_{a-b} = \mu_a\mu_c\mu_{-b} = \mu_a\mu_{-b}\mu_{a\mu_{-b}+b} = \mu_{-a-b}\mu_{-a}\mu_a\mu_{-b}$;
- (3) $(a\mu_x + b\mu_x)\mu_{-x} = (a+b)\mu_{-b} + b = a + (a+b)\mu_a$;
- (4) $(a+b)\mu_x = (a\mu_b - b)\mu_x + b\mu_x = a\mu_x + (-a + b\mu_{-a})\mu_x$;
- (5) $a\mu_{a+b} = -b - a + a\mu_b - b$.

Proof. (1) Recall that $H \leq \text{Aut}(U)$; so c is independent of x (given $y \in U^*$, $c = c\mu_{-y}\mu_y = (b\mu_{-y} - a\mu_{-y})\mu_y$). Therefore (1) is obtained by choosing $x = b$ for the first equality and $x = a$ for the second.

(2) The first equality in (2) is [2, Proposition 3.10(5)]. Then, by (1) and [2, Proposition 3.9(2)],

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

For the third equality we have

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

(3) This is [2, Lemma 4.4(2)].

(4) By (3),

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

The other equality of (4) follows similarly from the second equality in (3).

(5) This is [2, Lemma 4.4(3)]. □

Parts of the following proposition are included in [4, Corollary 5, p. 412].

PROPOSITION 5.3. (1) *If $x, y \in U^*$ are such that $[x, y] = 0$ and $k \in \mathbb{Q}$ is such that $x \cdot k$ is well defined, then $[x \cdot k, y] = 0$.*

(2) *If the order of $a \in U^*$ is a prime p , then $C_U(a)$ is a group of exponent p .*

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

Proof. (1) is obvious from the unique divisibility in Proposition 1.6.

For (2) 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

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

contradicting the fact that a has no p -root in U (cf. Proposition 1.6).

Finally (3) follows from (2), because by (2) each element in $C_U(a)$ has infinite order, and by (1) and Proposition 1.6, $C_U(a)$ is uniquely divisible. □

PROPOSITION 5.4. *Let $a, b \in U^*$ such that $a \in \text{Inv}(U)$ and a inverts b . Then a centralizes b and hence $b \in \text{Inv}(U)$.*

Proof. First note that

$$\text{if } x, y \in \text{Inv}(U), \text{ then } x \text{ commutes with } x\mu_y. \tag{*}$$

Indeed, by Lemma 5.2(5), $x\mu_{x+y} = y + x + x\mu_y + y$; so by Lemma 5.1, $x + x\mu_y$ is an involution and (*) follows.

Notice that by Proposition 5.3,

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

Let $a \in \text{Inv}(U)$ and let $b \in U^*$ be an element inverted by a . We will show that $b \in C_U(a)$. If $b \in \text{Inv}(U)$, then we are done. Hence we may assume that $b \notin \text{Inv}(U)$. Consider the following equality of Lemma 5.2(5):

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

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

and hence

$$\text{if } a \text{ inverts } x \in U^* \setminus \text{Inv}(U), \text{ then } a\mu_x \text{ commutes with } -x + a + x. \tag{5.1}$$

In what follows we will use the following facts from [2, Proposition 4.10]:

$$(b \cdot \gamma)\mu_{b \cdot \delta} = -b \cdot \frac{\delta^2}{\gamma}, \quad \mu_{b \cdot \gamma}^{\mu_{b \cdot \delta}} = \mu_{b \cdot \frac{\delta^2}{\gamma}} \tag{5.2}$$

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. Now, let $\alpha, \beta \in \mathbb{Q}$ such that $b \cdot \alpha$ and $b \cdot \beta$ are well defined. From equation (5.1)

$$a\mu_{b \cdot \alpha} \text{ commutes with } -b \cdot \alpha + a + b \cdot \alpha. \tag{5.3}$$

Applying $\mu_{-b \cdot \alpha}\mu_{b \cdot \beta} \in \text{Aut}(U)$ to equation (5.3)

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

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

$$a\mu_{b \cdot \alpha} \text{ commutes with } b \cdot \frac{\alpha^2}{\beta} + a\mu_{b \cdot \beta}\mu_{b \cdot \alpha} - b \cdot \frac{\alpha^2}{\beta}. \tag{5.4}$$

From equations (5.3) and (5.4), using (**) we see that

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

and after conjugating by $-b\alpha$

$$a \text{ commutes with } a\mu_{b \cdot \beta}\mu_{b \cdot \alpha} - b \cdot (\alpha + \frac{\alpha^2}{\beta}) \cdot 2. \tag{5.5}$$

Notice that we have used (5.2) which implies that $a\mu_{b \cdot \beta}\mu_{b \cdot \alpha}$ inverts b (because $\mu_{b \cdot \beta}\mu_{b \cdot \alpha} \in \text{Aut}(U)$). Since a and $a\mu_{b \cdot \beta}\mu_{b \cdot \alpha}$ invert b , it follows that $a + a\mu_{b \cdot \beta}\mu_{b \cdot \alpha}$ centralizes b . But by equation (5.5), 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

$$a\mu_{b \cdot \beta}\mu_{b \cdot \alpha} = a + b \cdot (\alpha + \frac{\alpha^2}{\beta}) \cdot 2. \tag{5.6}$$

Taking $\alpha = \beta = -1$ in equation (5.6) we get

$$a\mu_{-b}^2 = a - b \cdot 4. \tag{5.7}$$

But taking $\beta = -1$ and $\alpha = 2$ in equation (5.6) we also get

$$a\mu_{-b}\mu_{b \cdot 2} = a - b \cdot 4. \tag{5.8}$$

Hence $a\mu_{-b}^2 = a\mu_{-b}\mu_{b \cdot 2}$. Applying μ_b on both sides of this equality and using equation (5.2) we obtain $a\mu_{-b} = a\mu_{b \cdot \frac{1}{2}}$ or

$$a = a\mu_{b \cdot \frac{1}{2}}\mu_b. \tag{5.9}$$

But from equations (5.6) and (5.9)

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

so $b \cdot 6 = 0$. Since the order of b is a prime (see Proposition 1.6(4)) and $b \notin \text{Inv}(U)$ we see that $b \cdot 3 = 0$. But then, by [2, 4.10(5)], $\mu_{-b}^4 = 1$ and, by equation (5.7), $a\mu_{-b}^2 = a - b$, so

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

This is a contradiction and the proof of the proposition is complete. □

As a corollary we get the following theorem.

THEOREM 5.5. *If $\text{Inv}(U) \neq \emptyset$, then U is a group of exponent 2.*

Proof. Let $b \in U^*$. We will show that $b \in \text{Inv}(U)$. Assume not, and let $a \in \text{Inv}(U)$; then $a\mu_{a+b} = -b + a + a\mu_b - b$, and conjugating by b we see that $-b \cdot 2 + a + a\mu_b \in \text{Inv}(U)$, by Lemma 5.1. Thus $a\mu_b$ inverts $-b \cdot 2 + a$, and so, by Proposition 5.4, we have $-b \cdot 2 + a$ is an involution. It follows that a inverts $-b \cdot 2$ and hence a inverts b . But then, by Proposition 5.4, b is an involution, a contradiction. \square

The following fact is well known, but our proof below relies only on the Feit–Thompson odd order theorem but not on further results related to the classification of finite simple groups.

COROLLARY 5.6. *Assume that $\mathbb{M}(U, \tau)$ is finite; then U is abelian.*

Proof. By Theorem 5.5, we may assume that $|U|$ is odd; so, by the Feit–Thompson theorem, U is solvable. But by [7, Theorem 1.2], U is characteristically simple, and so U is abelian. \square

6. Special Moufang sets in which the μ -maps are involutions have abelian root groups

Throughout this section $\mathbb{M}(U, \tau)$ is a special Moufang set. Furthermore we assume that $\text{Inv}(U) = \emptyset$, and hence, by Proposition 1.6, U is uniquely 2-divisible. We start with the following lemma.

LEMMA 6.1. *Let $x, y \in U^*$ with $x \neq -y$; then*

- (1) $x\mu_{y+x}^2 = x \Leftrightarrow x\mu_{y+x} = -y + x\mu_{-y} - x - y$;
- (2) if $x\mu_{y+x}^2 = x = x\mu_y^2$, then $x\mu_{y+x} = -y + x\mu_y - x - y$.

Proof. We have $x\mu_{y+x}^2 = x$ if and only if $x\mu_{y+x} = x\mu_{-x-y}$. But by Lemma 5.2(5),

$$x\mu_{-x-y} = -(-x)\mu_{-x-y} = -[y + x - x\mu_{-y} + y] = -y + x\mu_{-y} - x - y,$$

so (1) holds. If, in addition, $x\mu_{-y} = x\mu_y$, then (2) holds. \square

PROPOSITION 6.2. *Let $a, b \in U^*$; then*

- (1) if $a\mu_b^2 = a\mu_{-a+b+a}^2 = a\mu_{b+a}^2 = a\mu_{-b+a}^2 = a$, then a and b commute;
- (2) if $a\mu_{x+a} = -x + a\mu_x - a - x$, for $x \in \{b, -a + b\}$, then a and b commute.

Proof. We start with

$$a\mu_{-a+b+a} = b + a + a\mu_{b+a} - a + b + a. \tag{6.1}$$

Indeed,

$$\begin{aligned} a\mu_{-a+b+a} &= -(-a)\mu_{-a+(b+a)} \\ &= -[-a - b + a - a\mu_{b+a} - a - b] \quad (\text{by Lemma 5.2(5)}) \\ &= b + a + a\mu_{b+a} - a + b + a. \end{aligned}$$

Next we claim that

$$\text{if } a\mu_{-a+b+a}^2 = a, \text{ then } a\mu_{-b+a} = -a + b \cdot 2 + a + a\mu_{b+a} - a + b \cdot 2 + a. \tag{6.2}$$

By equation (6.1) with $-b$ in place of b we have

$$a\mu_{-a-b+a} = -b + a + a\mu_{-b+a} - a - b + a. \tag{6.3}$$

Since $a\mu_{-a+b+a}^2 = a$, we obtain from equations (6.1) and (6.3) that

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

and this shows (6.2).

Our next claim is

$$\begin{aligned} &\text{if } a\mu_b^2 = a\mu_{-a+b+a}^2 = a\mu_{b+a}^2 = a, \text{ then} \\ a\mu_{-b+a} &= -a + b \cdot 2 + a - b \cdot 2 + a\mu_{-a+b} - b \cdot 2 - a + b \cdot 2 + a. \end{aligned} \tag{6.4}$$

Using Lemma 6.1, it follows from equation (6.2) that

$$a\mu_{-b+a} = -a + b \cdot 2 + a - b + a\mu_b - a - b - a + b \cdot 2 + a. \tag{6.5}$$

However by Lemma 5.2(5),

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

so $a\mu_b - a = -b + a\mu_{-a+b} - b$, and substituting in equation (6.5) gives the equality in equation (6.4).

We can now proceed with the proof of the proposition.

(1) Set $x = -a + b \cdot 2 + a$, $y = b \cdot 2$ and $z = a\mu_{-b+a}$. Since $a\mu_{-b+a} = a\mu_{-a+b}$, equation (6.4) may be written as $z = x - y + z - y + x$, so $-x + z - x + z = -y + z - y + z$. Thus, by unique 2-divisibility, $-x + z = -y + z$, so $x = y$; that is, a commutes with $b \cdot 2$, and so, by unique 2-divisibility, a commutes with b .

(2) We claim that

$$a\mu_{-a+b+a} = b + a - b + a\mu_b - a - b - a + b + a. \tag{6.6}$$

This is because by equation (6.1) and the hypothesis in (2) for $x = b$,

$$\begin{aligned} a\mu_{-a+b+a} &= b + a + a\mu_{b+a} - a + b + a \\ &= b + a + [-b + a\mu_b - a - b] - a + b + a. \end{aligned}$$

Also

$$a\mu_{-a+b+a} = -b + a + b + a\mu_b - a + b - a - b + a, \tag{6.7}$$

because by the hypothesis in (2) for $x = -a + b$ and by Lemma 5.2(5),

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

Comparing (6.6) and (6.7) we get

$$\begin{aligned} b + a - b + [a\mu_b - a - b - a + b + a] &= [-b + a + b + a\mu_b - a] + [b - a - b + a] \\ \iff \overbrace{a\mu_b - a}^x + \overbrace{(-b - a + b \cdot 2 + a - b)}^y &= \overbrace{(b - a - b \cdot 2 + a + b)}^{-y} + \overbrace{a\mu_b - a}^x. \end{aligned} \tag{6.8}$$

Therefore, equation (6.8) says that $x + y = -y + x$, and it follows that $(x + y) \cdot 2 = x \cdot 2$. By unique 2-divisibility, $x + y = x$; so $y = 0$ or $b \cdot 2 + a = a + b \cdot 2$. It follows that a commutes with $b \cdot 2$ and hence (again by unique 2-divisibility) a commutes with b . \square

As a corollary we get Theorem D from the Introduction (note that the case where $\text{Inv}(U) \neq \emptyset$ in Theorem D was already handled in Theorem C).

THEOREM 6.3. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set. Then the following are equivalent:*

- (i) U is abelian.
- (ii) $\mu_a^2 = 1$ for all $a \in U^*$.
- (iii) $a\mu_{b+a} = -b + a\mu_b - a - b$ for all $a, b \in U^*$.

Proof. By [2, Lemma 5.1], if U is abelian, then $\mu_a^2 = 1$ for all $a \in U^*$; so (i) implies (ii) (and this is regardless of whether $\text{Inv}(U)$ is empty or not). Assume that $\mu_a^2 = 1$ for all $a \in U^*$; then (iii) follows by Lemma 6.1(2) and (i) follows by Proposition 6.2(1). Finally, by Proposition 6.2(2), we have (iii) implies (i). \square

A corollary to Theorem 6.3 is the following characterization of the Moufang set associated with $\text{PSL}_2(k)$, where k is a commutative field of characteristic $\neq 2$.

COROLLARY 6.4. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set with little projective group G^\dagger and Hua subgroup H .*

- (1) *For each $h \in Z(H) \setminus \{1\}$ we have $C_U(h) = 0$.*
- (2) *If H is abelian then U is abelian and $G^\dagger \cong \text{PSL}_2(k)$ for some commutative field k with $\text{char}(k) \neq 2$.*
- (3) *If G^\dagger is Zassenhaus then U is abelian.*

Proof. Recall that we are assuming $\text{Inv}(U) = \emptyset$ (and hence U is uniquely 2-divisible). Let $h \in Z(H) \setminus \{1\}$; now [7, Theorem 1.2] says that U has no non-trivial proper H -invariant subgroup; so since $C_U(h)$ is H -invariant, (1) holds.

Assume that H is abelian. Then for each $a \in U^*$, we have $\mu_a^2 \in Z(H)$ and $a \in C_U(\mu_a^2)$; so by (1), $\mu_a^2 = 1$. Hence by Theorem 6.3, U is abelian, and (2) is now a consequence of [3, Theorem 6.1].

Finally, if G^\dagger is Zassenhaus, then for each $a \in U^*$, the element $\mu_a^2 \in G^\dagger$ has at least three fixed points $0, \infty$ and a , and hence $\mu_a^2 = 1$ for all $a \in U^*$. By Theorem 6.3 again, U is abelian. \square

7. Toward a general proof of RGC(2)

In this section we collect some results that will hopefully become useful for the general proof of part (2) of the RGC. We assume that $\mathbb{M}(U, \tau)$ is a special Moufang set and that $\text{Inv}(U) = \emptyset$. Notice that by Proposition 1.6 this implies that U is uniquely-2-divisible. Throughout this section p denotes an odd prime.

LEMMA 7.1. *Let $a, b \in U^*$; then*

- (1) $-b \cdot 2 - a = -b + a\mu_{a+b} + b - a\mu_b$; in particular,
- (2) *if U contains elements of order p , then every element in U is the sum of two elements of order p .*

Proof. By Lemma 5.2(5), $a\mu_{a+b} = -b - a + a\mu_b - b$, so (1) holds. For (2) we choose a of order p , and then by Lemma 5.1, $-b + a\mu_{a+b} + b$ and $a\mu_b$ have order p . Since U is 2-divisible, and b is an arbitrary element of U^* , it follows that $b \cdot 2$ is an arbitrary element of U^* . Thus $-b \cdot 2 - a$ is an arbitrary element of $U \setminus \{-a\}$ and so part (2) holds. \square

LEMMA 7.2. *Let $a, b \in U^*$. Then the equality $-a + b + a = -b$ never holds in U (that is, a does not invert b).*

Proof. This follows from the unique 2-divisibility of U . Indeed, suppose that $-a + b + a = -b$. Then $b + a + b = a$ and hence $(b + a) \cdot 2 = a \cdot 2$. By the unique 2-divisibility of U we see that $b + a = a$, which is a contradiction. \square

NOTATION 7.3. Let $a \in U^*$ and let $|a|$ be the order of a . We denote $\mathbb{F}_a = \text{GF}(p)$ if $|a| = p$, where p is a prime, and $\mathbb{F}_a = \mathbb{Q}$, if $|a| = \infty$ (see Proposition 1.6(4)). We let $X_a := \langle \mu_a, \alpha_{a \cdot t} \mid t \in \mathbb{F}_a \rangle$. Observe that by Remark 1.7, $a \cdot t$ is well defined for every $t \in \mathbb{F}_a$.

LEMMA 7.4. *Let $c \in U^*$ and set $\mathbb{F} := \mathbb{F}_c$ (see Notation 7.3). Then X_c is a special rank one group with abelian unipotent subgroups (see Definition 1.10). Hence if $|c| > 3$, then X_c is a perfect central extension of $\text{PSL}_2(\mathbb{F})$, and if $|c| = p$ is a prime, then $X_c \cong (\text{P})\text{SL}_2(p)$.*

Proof. Let $X := X_c$, $A := \{\alpha_{c \cdot t} \mid t \in \mathbb{F}\}$ and $B := \{\alpha_{c \cdot t}^{\mu_c} \mid t \in \mathbb{F}\}$. Notice first that $X = \langle A, B \rangle$, because by [2, Lemma 4.3(3)], $\mu_c = \alpha_c \alpha_{c \cdot t}^{\mu_c} \alpha_c$. We claim that for each $a = \alpha_{c \cdot t} \in A^*$, the element $b = \alpha_{-c \cdot t^{-1}}^{\mu_c} \in B^*$ satisfies the equality $a^b = b^{-a}$; it will then follow by Proposition 1.11(5) that X_c is a special rank one group.

To prove the claim, we first show that

$$\alpha_{c \cdot t^{-1}}^{\mu_c} = \alpha_{c \cdot t}^{\mu_c^{-1}} \tag{7.1}$$

for all $t \in \mathbb{F}$. Indeed, we apply both sides on some arbitrary element $x \in U$:

$$\begin{aligned} (x\mu_c^{-1} + c \cdot t^{-1})\mu_c &= (x\mu_{c \cdot t}^{-1} + c \cdot t)\mu_{c \cdot t} && \iff \\ x\mu_c^{-1} + c \cdot t^{-1} &= (x\mu_{c \cdot t}^{-1} + c \cdot t)\mu_{c \cdot t}\mu_c^{-1} && \iff \\ x\mu_c^{-1} + c \cdot t^{-1} &= x\mu_c^{-1} + (c \cdot t)\mu_{c \cdot t}\mu_c^{-1}, \end{aligned}$$

where we have used the fact that $\mu_{c \cdot t}\mu_c^{-1} \in \text{Aut}(U)$. Using [2, 4.10(1)], we have

$$(c \cdot t)\mu_{c \cdot t}\mu_c^{-1} = (-c \cdot t)\mu_c^{-1} = c \cdot t^{-1},$$

which proves equation (7.1).

Now let $d = c \cdot t$; then, by equation (7.1), $b^{-1} = \alpha_d^{\mu_d}$, and so the equation $a^b = b^{-a}$ can be rewritten as

$$\alpha_d^{\left(\alpha_{-d}^{\mu_d}\right)} = \alpha_d^{\mu_d \alpha_d}.$$

This can be rewritten as

$$\mu_d^{-1} \alpha_d \mu_d \alpha_d \mu_d^{-1} \alpha_{-d} \mu_d = \alpha_{-d} \mu_d^{-1} \alpha_d \mu_d \alpha_d \iff \alpha_d \mu_d^{-1} \alpha_d \mu_d \alpha_d \mu_d^{-1} = \mu_d^{-1} \alpha_d \mu_d \alpha_d \mu_d^{-1} \alpha_d;$$

using the fact that μ_d^2 commutes with α_d , this is equivalent to

$$(\alpha_d \mu_d)^3 = \mu_d (\alpha_d \mu_d)^3 \mu_d^{-1}.$$

But by [2, Lemma 4.3(4)], we know that $(\alpha_d \mu_d)^3 = \mu_d^4$, and this finishes the proof of the first part of the lemma. The second part now follows from [10, Theorem 5.6]. \square

LEMMA 7.5. *Let the notation be as in Notation 7.3, and let $a \in U^*$ with $|a| \neq 3$. Let L_a denote $\text{PSL}_2(\mathbb{F}_a)$ if $|a| = \infty$ or $|a| < \infty$ and $\mu_a^2 = 1$, while $L_a = \text{SL}_2(\mathbb{F}_a)$ if $|a| < \infty$ and $\mu_a^2 \neq 1 = \mu_a^4$. Let $\delta_a : \text{SL}_2(\mathbb{F}_a) \rightarrow \text{PSL}_2(\mathbb{F}_a)$ be the canonical homomorphism in the first two cases, and let δ_a be the identity map on $\text{SL}_2(\mathbb{F}_a)$ in the third case. Then there exists an*

epimorphism $\varphi_a : X_a \rightarrow L_a$ such that

$$(\alpha_{a \cdot t})\varphi_a = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}^{\delta_a} \quad \text{and} \quad (\mu_a)\varphi_a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{\delta_a}.$$

Moreover, if $|a| < \infty$, then φ_a is an isomorphism. Further, we have

$$(\mu_{a \cdot t})\varphi_a = \begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix}^{\delta_a}.$$

Proof. First by [8, Theorem 10] (see also [10, (5.1), p. 54], the universal perfect central extension of $\text{PSL}_2(\mathbb{F}_a)$ is the group X generated by the symbols $a(t), b(t)$ subject to the relations:

- (A) $a(t)a(s) = a(t+s), b(t)b(s) = b(t+s), t, s \in \mathbb{F}_a;$
- (B) $a(u)^{n(t)} = b(-t^{-2}u), u \in \mathbb{F}_a, t \in \mathbb{F}_a^*, n(t) := a(-t)b(t^{-1})a(-t).$

For $u \in \mathbb{F}_a$ and $t \in \mathbb{F}_a^*$, let

$$\alpha(t) := \alpha_{a \cdot t}, \quad \beta(t) = \alpha_{-a \cdot t}^{\mu_a}, \quad \nu(t) = \mu_{-a \cdot t},$$

where $\alpha(0) = \beta(0) = 1$. Then clearly the relations (A) are satisfied by $\alpha(t)$ and $\beta(t)$. Also, by [2, 3.10(2)] with $\tau = \mu_a$ (noting that $\sim a = -a$ in a special Moufang set), we have

$$\mu_{-a \cdot t} = \alpha_{-a \cdot t} \alpha_{(a \cdot t)\mu_{-a}}^{\mu_a} \alpha_{-a \cdot t}.$$

Thus by Proposition 1.6(2),

$$\mu_{-a \cdot t} = \alpha_{-a \cdot t} \alpha_{-a \cdot t^{-1}}^{\mu_a} \alpha_{-a \cdot t},$$

and thus we see that $\nu(t) = \alpha(-t)\beta(t^{-1})\alpha(-t)$. We now check that $\alpha(u)^{\nu(t)} = \beta(-t^{-2}u)$. We have

$$\begin{aligned} \alpha(u)^{\nu(t)} = \beta(-t^{-2}u) &\iff \\ \alpha_{a \cdot u}^{\mu_{-a \cdot t}} = \alpha_{a \cdot t^{-2}u}^{\mu_a} &\iff \\ \alpha_{a \cdot u}^{\mu_{-a \cdot t}\mu_{-a}} = \alpha_{a \cdot t^{-2}u} &\iff \\ \alpha_{(a \cdot u)\mu_{-a \cdot t}\mu_{-a}} = \alpha_{a \cdot t^{-2}u} &\iff \\ \alpha_{a \cdot t^{-2}u} = \alpha_{a \cdot t^{-2}u} & \end{aligned}$$

where we have used [2, Proposition 4.10(1)] for the last equivalence above. Hence we have shown that $\alpha(t)$ and $\beta(t)$ satisfy the relations (B) as well.

Next, if we let $\circ : \text{SL}_2(\mathbb{F}_a) \rightarrow \text{PSL}_2(\mathbb{F}_a)$ be the canonical homomorphism, then

$$\mathfrak{a}(t) := \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}^\circ, \quad \mathfrak{b}(t) := \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}^\circ, \quad \mathfrak{n}(t) := \begin{pmatrix} 0 & -t \\ t^{-1} & 0 \end{pmatrix}^\circ, \quad t \in \mathbb{F}_a,$$

satisfy the Steinberg relations (A), (B) above. By the universal properties of the universal central extension of $\text{PSL}_2(\mathbb{F}_a)$ the map φ_a exists in the first two cases. Since the universal central extension of $\text{PSL}_2(p)$ is $\text{SL}_2(p)$ for an odd prime $p \neq 3$, φ_a exists also in the third case. □

Our next few lemmas investigate the fixed points of the μ -maps. Lemma 7.6 below is a useful (slight) extension of [2, Proposition 4.9(3)] and will be used in the proof of Lemma 7.7.

LEMMA 7.6. *Let $a, b \in U^*$. If $a\mu_b = -a$, then $b \in \{a, -a\}$.*

Proof. We have $\mu_a^{\mu_b} = \mu_{-a\mu_b} = \mu_a$ and hence $\mu_b = \mu_b^{\mu_a} = \mu_{-b\mu_a}$. Thus, by [2, Proposition 4.9(4)], $b\mu_a \in \{b, -b\}$. But if $b\mu_a = b$ then, by Lemma 7.7(1) below, $a\mu_b = a$, a contradiction. Thus $b\mu_a = -b$ and hence, by [2, Proposition 4.9(3)], $b \in \{a, -a\}$. \square

PROPOSITION 7.7. *Let $a, b \in U^*$ be two elements such that $a\mu_b = a$. Then*

- (1) $b\mu_a = b$;
- (2) a and b have the same order;
- (3) $\mu_a^2 = \mu_b^2$;
- (4) if $|b| < \infty$ and $|b| \equiv 1 \pmod{4}$, then $a \in \{b \cdot \sqrt{-1}, -b \cdot \sqrt{-1}\}$ (note that $\sqrt{-1} \in \mathbb{F}_b$, see Notation 7.3);
- (5) $\langle a, b \rangle$ is nilpotent of class ≤ 2 ;
- (6) if a has order 3 then a and b commute.

Proof. First we claim that

$$a\mu_{a+b} = -b \cdot 2, \tag{7.2}$$

because by Lemma 5.2(5), $a\mu_{a+b} = -b - a + a\mu_b - b = -b \cdot 2$.

- (1) Using Proposition 1.6(2) Lemma 5.2(5) we have

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

so (1) holds.

- (2) The statement follows from equation (7.2) and Lemma 5.1.
- (3) By equation (7.2) and by [2, Proposition 3.9(2)],

$$\mu_{-a}^{\mu_{a+b}} = \mu_{-b \cdot 2},$$

and hence $(\mu_{-a}^2)^{\mu_{a+b}} = \mu_{-b \cdot 2}^2$. However, by equation (1.3),

$$\mu_{a+b}^{\mu_a^2} = \mu_{(a+b)\mu_a^2} = \mu_a\mu_{a+b}^2\mu_a^2 = \mu_{a+b},$$

so μ_a^2 centralizes μ_{a+b} and, by [2, Proposition 4.10(4)], $\mu_{-b \cdot 2}^2 = \mu_{-b}^2$, so (3) holds.

- (4) By Lemma 1.6(2) we have $(a \cdot \sqrt{-1})\mu_b = a\mu_b \cdot (\sqrt{-1})^{-1} = -a \cdot \sqrt{-1}$, and so part (4) is a consequence of Lemma 7.6.

- (5) Assume now that the order of a is not 3. Note that by part (2), the order of b is not 3 either. Using Lemma 7.11(2) below we get

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

so

$$a \cdot \frac{1}{2} - b \cdot 2 - a \cdot \frac{1}{2} = -b \cdot 3 - a + b + a, \tag{7.3}$$

Let $x := a \cdot \frac{1}{2} - b \cdot 2 - a \cdot \frac{1}{2}$ and $y := -a + b + a$. Then equation (7.3) says that $x = -b \cdot 3 + y$, and replacing b with $-b$ in equation (7.3) gives $-x = b \cdot 3 - y$. Together, this implies that $b \cdot 3$ commutes with y , and by unique 3-divisibility, b commutes with y , so b commutes with $[a, b]$. By symmetry a commutes with $[a, b]$ and (5) holds.

- (6) It remains to prove the case when a and b have order 3. By (7.2),

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

multiplying by μ_{-b} on the right and by μ_{a+b} on the left gives

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

and using Lemma 5.2(2) we obtain

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

It follows that

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

By [2, Proposition 4.9(4)] we get

$$(b - a)\mu_b = \pm(a + b), \tag{7.4}$$

and applying μ_b to both sides of (7.4) gives

$$(a + b)\mu_b = \pm(b - a). \tag{7.5}$$

Using (7.4), (7.5) and Lemma 5.2(4) we obtain

$$\begin{aligned} \pm(b - a) &= (a + b)\mu_b = (a\mu_b - b)\mu_b - b \\ &= (a - b)\mu_b - b \\ &= \pm(a + b) - b, \end{aligned}$$

so

$$\pm(b - a) = \pm(a + b) - b. \tag{7.6}$$

Taking the plus sign in the RHS of (7.6) gives $\pm(b - a) = a$, which says that either $b = 0$ or $b = -a$, a contradiction. Thus we have

$$\pm(b - a) = -b - a - b. \tag{7.7}$$

Taking the minus sign in the LHS of (7.7) implies that $a = b$, which is impossible. Hence $b - a = -b - a - b$ or $-b - a = -a - b$ as asserted. \square

NOTATION 7.8. Let $a \in U^*$. We denote by G_a the following group.

- (1) If $|a| = \infty$, or $|a| < \infty$ and $\mu_a^2 = 1$, $G_a := \text{PGL}_2(\mathbb{F}_a)$.
- (2) If $|a| < \infty$ and $\mu_a^2 \neq 1 = \mu_a^4$, then we let $j \notin \mathbb{F}_a$ be an element with $j^2 = -1 \in \mathbb{F}_a$ (thus $\{1, -1, j, -j\}$ is a cyclic group of order 4) and

$$G_a := \left\{ \epsilon_g g \mid g \in \left\langle \text{SL}_2(\mathbb{F}_a), \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right\},$$

where $\epsilon_g = 1$ if $g \in \text{SL}_2(\mathbb{F}_a)$ and $\epsilon_g = j$ otherwise. Multiplication in G_a is defined by $(\epsilon_g g)(\epsilon_h h) = (\epsilon_g \epsilon_h)(gh)$.

LEMMA 7.9. Let $a, b \in U^*$ and assume that $a\mu_b = a$. Set $H := \langle X_a, \mu_b \rangle$. Then the following hold.

- (1) μ_b normalizes X_a .
- (2) If $|a| \equiv 1 \pmod{4}$, then $H = X_a$.
- (3) Suppose that $a \not\equiv 1 \pmod{4}$. Then the map $\varphi_a : X_a \rightarrow L_a$ of Lemma 7.5 extends to an epimorphism $\varphi : H \rightarrow G_a$, where G_a is as in Notation 7.8. The map φ is defined by $(\mu_b)\varphi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{\delta_a}$, if a is as in case (1) of Notation 7.8, while $(\mu_b)\varphi = j \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, otherwise. In particular, if $|a| < \infty$, then φ is an isomorphism.

Proof. (1) By [2, Lemma 4.3(1)] (with $\tau = \mu_b$) and by Lemma 1.6(2) we have

$$\mu_{a \cdot t} = \alpha_{a \cdot t} \alpha_{-a \cdot \frac{1}{t}}^{\mu_b} \alpha_{a \cdot t}, \quad t \in \mathbb{F}_a,$$

and hence

$$\alpha_{a \cdot t}^{\mu_b} = \alpha_{a \cdot \frac{1}{t}} \mu_{-a \cdot \frac{1}{t}} \alpha_{a \cdot \frac{1}{t}} \quad \text{and} \quad \mu_a^{\mu_b} = \mu_{-a}. \tag{7.8}$$

This shows that μ_b normalizes X_a .

(2) If $b \equiv 1 \pmod{4}$, then by Lemma 7.7(4), $b = a \cdot t$, for $t = \sqrt{-1} \in \mathbb{F}_a$; so $\mu_b \in X_a$ and (2) follows.

(3) Suppose that $a \not\equiv 1 \pmod{4}$. Let φ be as stated above. Then by equation (7.8),

$$(\alpha_{a \cdot t}^{\mu_b})\varphi = ((\alpha_{a \cdot t})\varphi)^{(\mu_b)\varphi}, \quad ((\mu_a)^{\mu_b})\varphi = ((\mu_a)\varphi)^{(\mu_b)\varphi}. \tag{7.9}$$

Since $\sqrt{-1} \notin \mathbb{F}_a$, this shows that $(\mu_b)\varphi \notin X_a\varphi$. It follows that $H \neq X_a$. By Lemma 7.7(3), $|H/X_a| = 2$. By equation (7.9), φ_a can be extended to a homomorphism φ as claimed. \square

We believe that our next result will eventually lead to a proof that $C_U(a)$ is abelian for all $a \in U^*$.

PROPOSITION 7.10. *Let $a \in U^*$ and assume that $C_U(a)^* \mu_a = C_U(a)^*$. Then*

- (1) $[a\mu_x, b\mu_x] = 0$ for all $b \in C_U(a)^*$ and $x \in U^*$;
- (2) $C_U(a)^* \mu_x = C_U(a)^* = C(a\mu_x)^*$ for all $x \in C_U(a)^*$ and hence $C_U(a)$ is either an abelian group of exponent p , for some prime p , or a \mathbb{Q} -vector space.

Proof. (1) Let $b \in C_U(a)^*$. By hypothesis, $b\mu_a \in C_U(a)$; so since $\mu_{-a}\mu_x \in \text{Aut}(U)$, we have

$$0 = [a\mu_{-a}\mu_x, b\mu_a\mu_{-a}\mu_x] = [-a\mu_x, b\mu_x].$$

This shows (1).

(2) Let $b, x \in C_U(a)^*$ with $b - x \neq 0$. By Lemma 5.2(4),

$$(b + x)\mu_a = (b\mu_x - x)\mu_a + x\mu_a.$$

By hypothesis $(b + x)\mu_a, x\mu_a \in C_U(a)$, hence also $(b\mu_x - x)\mu_a \in C_U(a)$. But then, by hypothesis, $b\mu_x - x = (b\mu_x - x)\mu_a\mu_{-a} \in C_U(a)$. It follows that $b\mu_x \in C_U(a)$.

We have thus shown that $C_U(a)^* \mu_x = C_U(a)^*$. Now

$$C_U(a\mu_x) = C_U((-a)\mu_a\mu_x) = C_U(a)\mu_a\mu_x = C_U(a)\mu_x = C_U(a).$$

Set $V := C_U(a)$. Then, by Lemma 1.8, $\mathbb{M}(V, \mu_a)$ is a special Moufang set. But a is in the center of V , and since $\mathbb{M}(V, \mu_a)$ is special, the center of V is either V or trivial (this follows from [7, Theorem 1.2]). Thus $V = C_U(a)$ is abelian. The rest of (2) follows from Proposition 5.3, since $\mathbb{M}(V, \mu_a)$ is a special Moufang set and V is abelian. \square

We conclude this section with a lemma that gives various relations among the elements of U .

LEMMA 7.11. *Let $a, b \in U^*$ and let $1 \leq n < |a|$. Then*

- (1) $(-b - a \cdot n + a\mu_b \cdot \frac{1}{n} - b) \cdot n = -b - a \cdot n - b - a \cdot (n - 1) - \dots - b - a + a\mu_b - b - b - a - b - a \cdot 2 - \dots - b - a \cdot (n - 1)$; in particular,
- (2) $a\mu_b \cdot \frac{1}{2} - b \cdot 2 - a \cdot 2 + a\mu_b \cdot \frac{1}{2} = -b - a + a\mu_b - b \cdot 2 - a + b$;
- (3) $a + b - a\mu_b \cdot \frac{1}{2}$ commutes with $a \cdot 2 + b \cdot 2 - a\mu_b$.

Proof. (1) Let $n < |a|$; then by Lemma 1.6(2) and Lemma 5.2(5),

$$a\mu_{a \cdot n + b} = (a \cdot n)\mu_{a \cdot n + b} \cdot n = (-b - a \cdot n + a\mu_b \cdot \frac{1}{n} - b) \cdot n.$$

On the other hand

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

Then computing $a\mu_{a \cdot (n-1) + b} = a\mu_{a + a \cdot (n-2) + b}$ as above and continuing in this manner yields (1).

(2) By (1), with $n = 2$ we have

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

This shows (2).

(3) We first prove that

$$b - a\mu_b \cdot \frac{1}{2} + a \text{ commutes with } -a + a\mu_b - b \cdot 2 - a. \quad (7.10)$$

For that we rewrite (2):

$$\begin{aligned} \overbrace{(a\mu_b \cdot \frac{1}{2} - b)}^x + \overbrace{(-b - a)}^y + \overbrace{(-a + a\mu_b \cdot \frac{1}{2})}^z \\ = -b + \overbrace{(-a + a\mu_b \cdot \frac{1}{2})}^z + \overbrace{(a\mu_b \cdot \frac{1}{2} - b)}^x + \overbrace{(-b - a)}^y + b. \end{aligned}$$

Thus

$$-z + (z + x + y) + z = -b + z + x + y + b,$$

and we see that $b - z$ commutes with $z + x + y$. This shows equation (7.10). Now conjugate the identity of (7.10) by $-a$ to get that $a + b - a\mu_b \cdot \frac{1}{2}$ commutes with $a\mu_b - b \cdot 2 - a \cdot 2$. Therefore (3) holds. \square

References

1. T. DE MEDTS, F. HAOT, R. KNOP and H. VAN MALDEGHEM, ‘On the uniqueness of the unipotent subgroups of some Moufang sets’, *Finite geometries, groups and computation* (ed. A. Hulpke, R. Liebler, T. Penttila and Á. Seress) (de Gruyter, Berlin, 2006), 43–66.
2. T. DE MEDTS and Y. SEGEV, ‘Identities in Moufang sets’, *Trans. Amer. Math. Soc.*, to appear.
3. T. DE MEDTS and R. M. WEISS, ‘Moufang sets and Jordan division algebras’, *Math. Ann.* 335 (2006) 415–433.
4. A. NESIN, ‘On split B – N pairs of rank 1’, *Compos. Math.* 76 (1990) 407–421.
5. D. J. S. ROBINSON, *A course in the theory of groups*, 2nd edn, Graduate Texts in Mathematics 80 (Springer, New York, 1996).
6. J. ROTMAN, *An introduction to the theory of groups*. 4th edn, Graduate Texts in Mathematics 148 (Springer, New York, 1995).
7. Y. SEGEV and R. M. WEISS, ‘On the action of the Hua subgroups in special Moufang sets’, *Math. Proc. Cambridge Philos. Soc.*, to appear.
8. R. STEINBERG, *Lectures on Chevalley groups*, Lecture Notes (Yale University, 1967).
9. M. SUZUKI, ‘On a class of doubly transitive groups II’, *Ann. of Math.* (2) 79 (1964) 514–589.
10. F. TIMMESFELD, *Abstract root subgroups and simple groups of Lie type*, Monographs in Mathematics 95 (Birkhäuser, Basel, 2001).
11. J. TITS, ‘Twin buildings and groups of Kac–Moody type’, *Groups, combinatorics and geometry*, Durham, 1990, London Mathematical Society Lecture Note Series 165, (Cambridge University Press, Cambridge, 1992) 249–286.

Tom De Medts
Department of Pure Mathematics and
Computer Algebra
Ghent University
Krijgslaan 281 S22
9000 Gent
Belgium

tdemedts@cage.ugent.be

Katrin Tent
Faculty for Mathematics
University of Bielefeld
Postfach 100131
D-33501 Bielefeld
Germany

ktent@math.uni-bielefeld.de

Yoav Segev
Department of Mathematics
Ben-Gurion University
Beer-Sheva 84105
Israel
yoavs@math.bgu.ac.il