Special abelian Moufang sets of finite Morley rank

Tom De Medts* Katrin Tent

August 13, 2007

Abstract

Moufang sets are split doubly transitive permutation groups, or equivalently, groups with a split BN-pair of rank one. In this paper, we study so-called special Moufang sets with abelian root groups, under the model-theoretic restriction that the groups have finite Morley rank. These groups have a natural base field, and we classify them under the additional assumption that the base field is infinite. The result is that the group is isomorphic to $\mathsf{PSL}_2(K)$ over some algebraically closed field K.

`MSC-2000` : *primary:* 03C45, 20E42 ; *secondary:* 03C60

`keywords` : Moufang sets, BN-pairs, split doubly transitive groups, finite Morley rank

1 Introduction

Groups of finite Morley rank have received a lot of attention during the last decades, because of their strong connections to algebraic groups. In fact, the famous Cherlin-Zil'ber Conjecture states that any simple group of finite Morley rank is isomorphic, as an abstract group, to an algebraic group over an algebraically closed field. Excellent progress has been made for groups of even type (see the forthcoming work in [ABC]), but the situation in the other cases is much less clear, mainly because of the lack of Sylow-p-theory for primes $p \neq 2$.

In analogy with the classification of finite simple groups, a natural class of groups to start investigating is the class of rank one groups, i.e. the groups with a split BN-pair of rank one. An equivalent description of these groups uses the notion of a Moufang set, introduced by J. Tits [T].

*The first author is a Postdoctoral Fellow of the Research Foundation - Flanders (Belgium) (F.W.O.-Vlaanderen).

Definition 1.1. A *Moufang set* is a set X together with a collection of subgroups $(U_x)_{x \in X}$, such that each U_x is a subgroup of $\mathrm{Sym}(X)$ fixing x and acting regularly (i.e. sharply transitively) on $X \setminus \{x\}$, and such that each U_x permutes the set $\{U_y \mid y \in X\}$ by conjugation. The group $G := \langle U_x \mid x \in X \rangle$ is called the *little projective group* of the Moufang set; the groups U_x are called *root groups*.

This point of view turns out to be very powerful, and has already led to several deep results as well as connections with the theory of Jordan algebras [DW, DS, DST]. We point out that each Moufang set can be constructed only starting from one abstract group U (usually written additively, even though U can be non-abelian), together with one additional permutation $\tau \in \mathrm{Sym}(U^*)$. (Here and elsewhere, we write U^* for $U \setminus \{0\}$.) The corresponding Moufang set is denoted by $\mathbb{M}(U, \tau)$; we refer to [DW] for more details.

It turns out that it is possible to make more progress in the theory of Moufang sets by assuming that the Moufang set is special.

Definition 1.2. A Moufang set $\mathbb{M}(U, \tau)$ is called *special* if $(-a)\tau = -(a\tau)$ for all $a \in U^*$.

The fact that this is a natural assumption, is illustrated by the fact that it was considered independently by Timmesfeld [Tim, p.2] in the context of abstract rank one groups, and by Borovik and Nesin [BN, p.221–222] in the context of groups with a split BN-pair of rank one (where it is precisely the condition that "α inverts U").

Despite some good progress, the classification of special Moufang sets with abelian root groups is still open.

Conjecture 1.3. *Let $\mathbb{M} = \mathbb{M}(U, \tau)$ be a special Moufang set with U abelian. Then $\mathbb{M} \cong \mathbb{M}(J)$ for some quadratic Jordan division algebra J, where $\mathbb{M}(J)$ is defined in a very natural way as described in [DW].*

The following conjecture that we are dealing with in this paper, is the intersection of Conjecture 1.3 and the Cherlin-Zil'ber Conjecture.

Conjecture 1.4. *Let $\mathbb{M} = \mathbb{M}(U, \tau)$ be an infinite special Moufang set of finite Morley rank, with U abelian. Then $\mathbb{M} \cong \mathbb{M}(K)$ for some algebraically closed field K, where $\mathbb{M}(K)$ is the Moufang set whose little projective group is $\mathsf{PSL}_2(K)$.*

If $\mathbb{M}(U, \tau)$ is a special Moufang set with abelian root groups, then it is known that U is a vector group, i.e. it is the additive group of a vector space Moreover, if $\mathrm{char}(U) \neq 2$, then H, the two point stabilizer of G, acts irreducibly on U, and hence by Schur's Lemma, $K := C_{\mathrm{End}(U)}(H)$ is a division ring. If the Moufang set has finite Morley rank, then this division ring is definable, and hence it is either a finite field or an algebraically closed field. In this paper, we prove Conjecture 1.4 in the case where K is an algebraically closed field. In particular, this gives a complete classification of special Moufang sets of finite Morley rank with U abelian and $\mathrm{char}(U) = 0$.

Acknowledgment

This paper was written during a longer visit of the first author at the University of Bielefeld, supported by a travel grant from the Research Foundation in Flanders (Belgium) (F.W.O.-Vlaanderen). The support from both institutions is gratefully acknowledged.

2 Setup

Let $\mathbb{M} := \mathbb{M}(U, \tau)$ be a special Moufang set with U abelian. Then either U is an elementary abelian p-group, in which case we put $\mathrm{char}(U) = p$, or U is a torsion-free uniquely divisible group, in which case we put $\mathrm{char}(U) = 0$; see [DS, Prop. 4.6(5)]. By the main result of [SW], either $\mathrm{char}(U) = 2$, or H acts irreducibly on U, and hence by Schur's Lemma, the ring $K := C_{\mathrm{End}(U)}(H)$ is a division ring.

We now assume in addition that $\mathbb{M}$ is of finite Morley rank (in the language of permutation groups). In particular, X, U and G are definable, and so is the Hua subgroup $H := G_{0,\infty}$, the pointwise stabilizer of 0 and ∞. Moreover, G is connected because it is a simple group [DST, Theorem 1.11], and then U is connected since the connected group G acts transitively on $X = U \cup \{\infty\}$.

By [MP, Theorem 1.2(b)], K is definable, and then by [Ch], K is a commutative field; by Macintyre's theorem [M], it then follows that K is either finite or algebraically closed; see also [BN, Thm 8.10].

In this paper, we assume in addition that K is not finite. We will show the following theorem.

Theorem 2.1. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set of finite Morley rank, with U abelian and $\mathrm{char}(U) \neq 2$. Assume that the field $K := C_{\mathrm{End}(U)}(H)$ is infinite. Then $\mathbb{M}(U, \tau) \cong \mathbb{M}(K)$, the unique Moufang set whose little projective group is $\mathsf{PSL}_2(K)$.*

We start with a proposition which we will use later, but which is interesting in its own right. The proof is identical to the argument used in [BN, Theorem 11.89], but the result is slightly more general since we do not assume the existence of involutions in H (but we do assume that the Moufang set is special).

Proposition 2.2. *Let $\mathbb{M}(U, \tau)$ be a special Moufang set of finite Morley rank, with U* not necessarily *abelian, and assume that each $h \in H^*$ has no fixpoints in U^* (equivalently, G is a split special Zassenhaus group). Then $G \cong \mathsf{PSL}_2(K)$ and $\mathbb{M} \cong \mathbb{M}(K)$ for some algebraically closed field K.*

Proof. Let $a \in U^*$ be arbitrary; then the map $h \mapsto ah$ is a bijection from H to aH, and hence $\mathrm{RM}(H) = \mathrm{RM}(aH)$ for each $a \in U^*$. On the other hand, the map $\pm b \mapsto \mu_a \mu_b$ is an injection from the quotient space $U/\{\pm 1\}$ into H, and hence $\mathrm{RM}(H) \geq \mathrm{RM}(U)$. Therefore $\mathrm{RM}(aH) = \mathrm{RM}(U)$ for all $a \in U^*$, i.e. each orbit aH is generic in U. But U is connected, so it follows that there is only one orbit, i.e. H is transitive on U^*. Since each $h \in H^*$ acts freely, this implies that H is regular on U^*, and hence G is sharply 3-transitive. But then $G \cong \mathsf{PSL}_2(K)$ and hence $\mathbb{M} \cong \mathbb{M}(K)$ for some algebraically closed field K (see, for example, [BN, Thm. 11.88]; alternatively, see [BN, Thm. 8.5]). □

We now make an easy but important observation.

Lemma 2.3. *U is an n-dimensional vector space over K for some natural number n, and $H \leq \mathsf{GL}_n(K)$.*

Proof. It is clear that U is a vector space over K, and since U has finite Morley rank, this vector space is finite-dimensional. It follows from the definition of K that every element of H is a K-vector space automorphism of U. □

Notation 2.4. Let $\mathbb{F}$ be the prime field of K, i.e. if $\mathrm{char}(K) = p > 0$, then $\mathbb{F} = \mathsf{GF}(p)$, and if $\mathrm{char}(K) = 0$, then $\mathbb{F} = \mathbb{Q}$.

3 A minimal counterexample

We assume from now on, and until the end of the paper, that $\mathbb{M} = \mathbb{M}(U, \tau)$ is a minimal counterexample to Theorem 2.1, i.e. a counterexample for which $\mathrm{RM}(U)$ (the Morley rank of U) is minimal.

Note that it follows from [DW, Thm. 6.1] that for such a counterexample, H is non-abelian. Observe that this implies by Lemma 2.3 that $\dim_K U \geq 2$. We start with a lemma which gives information about the elements of H in such a counterexample.

Lemma 3.1. (i) *Let $h \in H$. Then either $h = \lambda \cdot \mathrm{id}$ for some $\lambda \in K^*$, or each eigenspace of h corresponding to an eigenvalue in $\mathbb{F}$ (if any) is one-dimensional and induces a sub-Moufang set isomorphic to $\mathbb{M}(K)$.*

(ii) *Assume that h has eigenvalues λ and $-\lambda$ for some $\lambda \in \mathbb{F}^*$, with eigenspaces V_+ and V_-, respectively. Then $a\mu_b \in V_+$ for every $a \in V_+$ and every $b \in V_+ \cup V_-$.*

Proof. (i) Assume that $h \notin K \cdot \mathrm{id}$. Let λ be any eigenvalue of h which lies in $\mathbb{F}^*$, and let V be the corresponding eigenspace; then V is a proper non-trivial definable subspace of U. In particular, V is infinite. By [S, Lemma 3.5], V is a root subgroup, i.e. it induces a sub-Moufang set. By the minimality of our counterexample, this induced sub-Moufang set is isomorphic to $\mathbb{M}(L)$ for some algebraically closed field L. Note that L contains K as an (algebraically closed) subfield. However, the additive group of L is just V, which is a finite-dimensional vector space over K. This can only happen if $L = K$, and hence V is one-dimensional over K.

(ii) This follows from [S, Lemma 3.5]. □

Notation 3.2. Let $\iota : U \to U$ be the map $a \mapsto -a$ for all $a \in U$.

Notation 3.3. Let $N := \langle \mu_a \mid a \in U^* \rangle$; then $N = G_{\{0,\infty\}}$, the setwise stabilizer of $\{0, \infty\}$. Note that H is an index two subgroup of N, and that N is a definable subgroup of G.

The main idea behind the following proposition comes from [S, Prop. 6.2].

Proposition 3.4. *Let $a, b \in U^*$ be such that $a\mu_b = a$. Then $\mu_a\mu_b = \iota$; in particular, $\iota \in H$.*

Proof. Let $a, b \in U^*$ be such that $a\mu_b = a$, and let $h := \mu_a\mu_b$; then $h^2 = \mu_a\mu_a^{\mu_b} = \mu_a\mu_{a\mu_b} = 1$. Note that $h \neq 1$ since otherwise $\mu_a = \mu_b$ and hence $b\mu_a = b\mu_b = -b \neq b$.

Assume now that $h \neq \iota$, and let $V_+ := \{x \in U \mid xh = x\}$ and $V_- := \{x \in U \mid xh = -x\}$; then by Lemma 3.1(i), both V_+ and V_- are either trivial or one-dimensional subspaces of U. But since $h^2 = 1$, the only possible eigenvalues of h are 1 and -1, and since $\dim_K U \geq 2$, it follows that neither V_+ nor V_- is trivial. Hence $U = V_+ \oplus V_-$ and $\dim_K V_+ = \dim_K V_- = 1$.

Now fix some $c \in V_+$, and observe that $a, b \in V_-$. Let $g := \mu_c\mu_a$. By Lemma 3.1(ii), both μ_c and μ_a stabilize the subsets V_+^* and V_-^*, and hence the same is true for $D := c(\mu_c, \mu_a)$, i.e. the definable closure of the subgroup of G generated by μ_c and μ_a. Note that $g \in D$.

Assume first that the order of g is either odd or infinite. Then by [BN, Exercise 1 on p.175], μ_c and μ_a are conjugate in D; say $\mu_c = \mu_a^f$ for some $f \in D$. Since N is definable and $\mu_c, \mu_a \in N$, we have $D \leq N$, and hence $\mu_a^f = \mu_{af}$ by [DS, Prop. 5.2(2)]. But now $\mu_c = \mu_{af}$, and this implies $af = c$

or $af = -c$; see [DS, Prop. 4.9(4)]. In both cases, this contradicts the fact that f stabilizes the sets V_+ and V_-.

Assume now that the order of g is $4t + 2$ for some natural number t. Then $\mu_c^{g^t}$ commutes with μ_a. Let $d := cg^t \in V_+$; then it follows that μ_d commutes with μ_a. Hence $\mu_a = \mu_{a\mu_d}$, from which it follows that $a = a\mu_d$ and similarly $d = d\mu_a$. (Note that the cases $a = -a\mu_d$ and $d = -d\mu_a$ cannot occur since either of them would imply $a = \pm d$ which is impossible since $a \in V_-$ whereas $d \in V_+$.) But since $d \in V_+$, we have $d = d\mu_a\mu_b = d\mu_b$, and therefore $b\mu_d = b$ as well. But now μ_d fixes both a and b, which contradicts [S, Prop. 4.1(3)].

Assume finally that the order of g is $4t$ for some natural number t. Let $N_\epsilon := \langle \mu_x \mid x \in V_\epsilon \rangle$ for $\epsilon \in \{+,-\}$. Then $\mu_a \in N_-$ and $\mu_c \in N_+$; moreover, μ_a and μ_c normalize both N_+ and N_-. In particular, $g^2 = [\mu_c, \mu_a] \in N_+ \cap N_-$. Now note that D is a finite dihedral group and that $D \cap H$ is a cyclic subgroup of index two, which has a unique involution, namely g^{2t}. Let $D_+ := \langle \mu_c, g^2 \rangle$ and $D_- := \langle \mu_a, g^2 \rangle$; then $D_\epsilon \leq D \cap N_\epsilon$, and g^{2t} is still the unique involution of $D_\epsilon \cap H$ for $\epsilon \in \{+,-\}$. But by the structure of $\mathbb{M}_\epsilon \cong \mathbb{M}(K)$, we know that $N_\epsilon \cap H$ has a unique involution, which inverts each element of V_ϵ. Since this involution is equal to g^{2t} for both $\epsilon \in \{+,-\}$, we conclude that $g^{2t} = \iota$. On the other hand, $h = \mu_a\mu_b \in N_- \cap H$, and therefore $h = \iota$ after all (which in fact contradicts our initial assumption that $h \neq \iota$). □

Corollary 3.5. *For each $a \in U^*$, the map μ_a has at most two fixpoints.*

Proof. Indeed, assume that $b\mu_a = b$ and $c\mu_a = c$, then it follows from Proposition 3.4 that $\mu_b\mu_a = \iota$ and $\mu_c\mu_a = \iota$, and hence $\mu_b = \mu_c$, implying $c = \pm b$. □

Proposition 3.6. (i) *H acts transitively on U^*.*

(ii) *For each $a \in U^*$, the map μ_a has precisely two fixpoints, namely $\pm a\cdot\gamma$, where $\gamma^2 = -1$ in K.*

(iii) *For each $a \in U^*$, $aK \leq U$ induces a sub-Moufang set isomorphic to $\mathbb{M}(K)$.*

Proof. Recall that we are considering a minimal counterexample to Theorem 2.1. Hence by Proposition 2.2, there is at least one element $h \in H^*$ that has fixpoints in U^*. It then follows from Lemma 3.1(i) that $\mathbb{M}$ has a proper sub-Moufang set isomorphic to $\mathbb{M}(K)$. Write

$$U = a \cdot K \oplus W ,$$

where $a \cdot K$ induces the sub-Moufang set; in particular,

$$(a \cdot s)\mu_{a \cdot t} = -a \cdot s^{-1}t^2 \tag{3.1}$$

for all $s, t \in K$. Observe that this implies that $aK^* \subseteq aH$ and hence that aH is closed under scalar multiplication by elements of K^*. Also, it follows from equation (3.1) and Corollary 3.5 that

$$\mathrm{Fix}_{U^*}(\mu_{at}) = \{a \cdot t\gamma, -a \cdot t\gamma\} \tag{3.2}$$

for each $t \in K^*$. We now claim:

$$\text{If } \mu_b \text{ fixes some element of } aK^*, \text{ then } b \in aK^*. \tag{3.3}$$

Indeed, let $b \in U^*$ be such that $(at)\mu_b = at$ for some $t \in K^*$. Then by [DST, Prop. 7.8(1)], $b\mu_{at} = b$. But by (3.2), this implies $b \in aK^*$, which proves the claim (3.3).

Suppose that there is some $b \in U^* \setminus aH$, and let $g := \mu_a\mu_b$. If the order of g is odd or infinite, then as before, μ_a and μ_b are conjugate in N; hence there is an $h \in H$ such that $\mu_b = \mu_a^h = \mu_{ah}$; it follows that $b = \pm ah \in aH$, a contradiction. Hence g has order $2t$ for some natural number t.

The following claim is crucial.

$$\text{If } ag^\ell \in aK^*, \text{ then } \ell \text{ is even and } ag^{\ell/2} \in aK^*. \tag{3.4}$$

Indeed, assume that $ag^\ell = a \cdot t$ for some natural number ℓ and some $t \in K^*$. Let $\rho \in K^*$ be such that $\rho^2 = -t$; then using equation (3.1) and the fact that $g \in H$ commutes with scalar multiplication,

$$a\rho = -a \cdot t\rho^{-1} = -ag^\ell \cdot \rho^{-1} = (-a \cdot \rho^{-1})\mu_a\mu_b g^{l-1} = (a\rho)\mu_b(\mu_a\mu_b)^{l-1},$$

i.e. $\nu := \mu_b(\mu_a\mu_b)^{l-1}$ fixes $a\rho$. If ℓ is odd, say $\ell = 2s+1$, then $\nu = \mu_b^{g^s} = \mu_{bg^s}$. But then by the claim (3.3), this implies $bg^s \in aH$ and hence $b \in aH$, a contradiction. Hence ℓ is even, say $\ell = 2s$, and $\nu = \mu_a^{g^s} = \mu_{ag^s}$. Again by (3.3), this implies $ag^s \in aK^*$, proving the claim (3.4).

But g has order $2t$, hence $\mu_{ag^t} = \mu_a^{g^t} = \mu_a$, and hence $ag^t = \pm a \in aK^*$. Therefore we can start the descent argument of (3.4) and continue to divide the exponent by 2, which leads to a contradiction since ℓ is a natural number.

Hence the assumption that there is some $b \in U^* \setminus aH$ is false, and we conclude that H is transitive on U^*, proving (i).

Now let $b \in U^*$ be arbitrary; then there is an $h \in H$ with $b = ah$, so in particular $\mu_b = \mu_a^h$. It now follows from (3.2) that

$$\mathrm{Fix}_{U^*}(\mu_b) = \mathrm{Fix}_{U^*}(\mu_a^h) = \mathrm{Fix}_{U^*}(\mu_a)h = \{\pm a\gamma h\} = \{\pm b\gamma\},$$

proving (ii). Moreover,

$$(bs)\mu_{bt} = (ash)\mu_{ath} = ash\mu_{at}^h = (as)\mu_{at}h = -as^{-1}t^2h = -bs^{-1}t^2$$

for all $s, t \in K^*$, which proves (iii). $\square$

Proposition 3.7. *For all $a, b \in U^*$ and all $t \in K^*$, we have*

(i) $(a \cdot t)\mu_b = a\mu_b \cdot t^{-1}$;

(ii) $a\mu_{b \cdot t} = a\mu_b \cdot t^2$.

Proof. (i) Let $a, b \in U^*$ and $t \in K^*$. Then by Proposition 3.6(iii),

$$(at)\mu_b = (-a\mu_a)t\mu_b = (-at^{-1})\mu_a\mu_b = (-a)\mu_a\mu_b t^{-1} = a\mu_b t^{-1},$$

proving (i).

(ii) By (i) with $a + b$ in place of a, we have

$$(at + bt)\mu_b = (a + b)\mu_b \cdot t^{-1}.$$

By [DST, Lemma 5.2(4)] with $x = b$, this can be rewritten as

$$\big((at)\mu_{bt} - bt\big)\mu_b + (bt)\mu_b = (a\mu_b - b)\mu_b \cdot t^{-1} + b\mu_b \cdot t^{-1}.$$

Applying (i) again on both terms of the right hand side, we get

$$\big((at)\mu_{bt} - bt\big)\mu_b + (bt)\mu_b = (a\mu_b \cdot t - bt)\mu_b + (bt)\mu_b,$$

which simplifies to $(at)\mu_{bt} = a\mu_b \cdot t$. One final application of (i) yields $a\mu_{bt} = a\mu_b \cdot t^2$ as claimed. $\square$

Corollary 3.8. *$K^* \leq Z(H)$.*

Proof. By the definition of K, every element of $K \leq \mathrm{End}(U)$ commutes with H, so it suffices to show that $K^* \leq H$. So let $t \in K^*$ be arbitrary, and let $s \in K^*$ be such that $s^2 = t$. Then by Proposition 3.7(ii), we have $\mu_b\mu_{b \cdot s} = s^2 \cdot \mathrm{id} = t \cdot \mathrm{id}$, and hence $t \cdot \mathrm{id} \in H$ for all $t \in K^*$. $\square$

Proposition 3.7 allows us to extend Lemma 3.1 to all elements of K.

Lemma 3.9. (i) *Let $h \in H$. Then either $h = \lambda \cdot \mathrm{id}$ for some $\lambda \in K^*$, or each eigenspace of h is one-dimensional and induces a sub-Moufang set isomorphic to $\mathbb{M}(K)$.*

(ii) *Assume that h has eigenvalues λ and $-\lambda$ for some $\lambda \in K^*$, with eigenspaces V_+ and V_-, respectively. Then $a\mu_b \in V_+$ for every $a \in V_+$ and every $b \in V_+ \cup V_-$.*

Proof. Simply observe that by Proposition 3.7 above, the short proof of [S, Lemma 3.5] now holds for all elements $\lambda \in K$ (see also Lemma 3.10(i) below), and hence the proof of Lemma 3.1 extends to K without any change. $\square$

We will now start to investigate the elements of H inside $\mathsf{GL}_n(K)$. We first examine the spectrum of elements of H. The next easy lemma is crucial for this proposition.

Lemma 3.10. *Let $h \in H$, and let $\mathrm{Spec}(h)$ be the set of eigenvalues of h. Assume that $\alpha, \beta \in \mathrm{Spec}(h)$, and let $a, b \in U$ be such that $ah = a \cdot \alpha$ and $bh = b \cdot \beta$. Then $\alpha^{-1}\beta^2 \in \mathrm{Spec}(h)$ as well; more precisely, $(a\mu_b)h = (a\mu_b) \cdot \alpha^{-1}\beta^2$.*

Proof. Note that $\alpha, \beta \neq 0$ since h is invertible. Then by Proposition 3.7 and [DS, Prop. 5.2(2)], $(a\mu_b)h = ah\mu_{bh} = (a\alpha)\mu_{b\beta} = a\mu_b \cdot \alpha^{-1}\beta^2$, which proves that $a\mu_b$ is an eigenvector of h with eigenvalue $\alpha^{-1}\beta^2$. $\square$

Proposition 3.11. *Let $h \in H$, and let $\mathrm{Spec}(h)$ be the set of eigenvalues of h. Then there exists some $\lambda \in K^*$ and some natural number r such that*

$$\mathrm{Spec}(h) = \{\lambda \cdot \zeta_r^k \mid k \in \{0, 1, \dots, r-1\}\},$$

where ζ_r is a primitive r^{th} root of 1 in K. Moreover, either $r = 1$ or r is an odd prime number.

Proof. If h has only one eigenvalue, then this is clearly satisfied with $r = 1$. So assume that h has eigenvalues λ and $\lambda \cdot \xi$ for some $\lambda, \xi \in K^*$. Then by Lemma 3.10, $\lambda \cdot \xi^{-1}, \lambda \cdot \xi^2 \in \mathrm{Spec}(h)$ as well. By induction (separately for m even and m odd), we see that $\lambda \cdot \xi^m \in \mathrm{Spec}(h)$ for each integer m. Since $\mathrm{Spec}(h)$ is a finite set, this implies that ξ has finite order s, and

$$\lambda \cdot \xi \in \{\lambda \cdot \zeta_s^k \mid k \in \{0, 1, \dots, s-1\}\} \subseteq \mathrm{Spec}(h).$$

Now assume that $\lambda \cdot \rho$ is another eigenvalue of h. Then similarly, ρ has finite order t, and

$$\lambda \cdot \rho \in \{\lambda \cdot \zeta_t^k \mid k \in \{0, 1, \dots, t-1\}\} \subseteq \mathrm{Spec}(h).$$

Observe that we are free to replace ζ_s and ζ_t by any primitive s^{th} and t^{th} root of 1, respectively; we choose them in such a way that $\zeta_{st}^s = \zeta_t$ and $\zeta_{st}^t = \zeta_s$ for some primitive $(st)^{\text{th}}$ root ζ_{st} of 1. Let $\zeta' := \zeta_{st}^{\gcd(s,t)}$; then ζ' is a primitive $\mathrm{lcm}(s,t)^{\text{th}}$ root of 1.

Now write $s = 2^a s'$ and $t = 2^b t'$ with s' and t' odd; we may assume that $a \geq b$. Then $\gcd(s,t) = \gcd(2s,t)$, and hence there exist natural numbers p and q such that $2sp - tq = \gcd(s,t)$. Then by Lemma 3.10 again,

$$\mathrm{Spec}(h) \ni (\lambda \cdot \zeta_s^q)^{-1}(\lambda \cdot \zeta_t^p)^2 = \lambda \cdot \zeta_{st}^{-tq+2sp} = \lambda \cdot \zeta';$$

clearly

$$\{\lambda \cdot \xi, \lambda \cdot \rho\} \subseteq \{\lambda \cdot \zeta'^k \mid k \in \{0, 1, \ldots, \mathrm{lcm}(s,t) - 1\}\} \subseteq \mathrm{Spec}(h)\,.$$

Continuing in this way, this process will eventually end since $\mathrm{Spec}(h)$ is a finite set, and this proves that $\mathrm{Spec}(h)$ has the required form.

Now suppose that r is a composite number, say $r = s \cdot t$ for some natural number $s, t > 1$. Then h^s has at least t distinct eigenvalues, each with an eigenspace of dimension at least s over K. But this contradicts Lemma 3.9(i). It remains to exclude the case $r = 2$. So assume that $\mathrm{Spec}(h) = \{\lambda, -\lambda\}$, let $ah = a \cdot \lambda$ and $bh = -b \cdot \lambda$. Then by Lemma 3.9(ii), $a\mu_b$ is contained in the eigenspace of the eigenvalue λ, which is $a \cdot K$ by Lemma 3.9(i). Hence $a\mu_b = a \cdot \nu$ for some $\nu \in K^*$. Let ρ be a square root of ν in K; then $(a\rho)\mu_b = a\mu_b\rho^{-1} = a\nu\rho^{-1} = a\rho$. But this would contradict Proposition 3.6(ii). □

We are grateful to Pierre-Emmanuel Caprace for providing us a conceptual proof of the following lemma.

Lemma 3.12. *Let g, h be two unipotent elements in $\mathsf{GL}_n(K)$ with a one-dimensional fixpoint space. Assume that $g^2 = h^2$. Then $g = h$.*

Proof. Since g and h have a one-dimensional fixpoint space, they both have the same Jordan normal form

$$J = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix},$$

possibly with respect to a different basis. Note that J and J^2 fix a unique maximal flag $[(0, \ldots, 0, 0, *), (0, \ldots, 0, *, *), \ldots, (0, *, \ldots, *, *)]$ in the projective space $\mathsf{PG}(n, K)$. (Recall that $\mathrm{char}(K) \neq 2$.) Since $g^2 = h^2$, they fix the same unique maximal flag, but of course g and g^2 fix the same unique maximal flag, and the same is true for h and h^2. Hence g and h fix the same unique maximal flag, i.e. they lie in the same unipotent subgroup. But since $\mathrm{char}(K) \neq 2$, the unipotent subgroups are uniquely 2-divisible, and hence $g^2 = h^2$ implies $g = h$. □

The next proposition produces (too) many fixpoint free elements in H.

Proposition 3.13. *For all $a, b \in U^*$, either $\mu_a\mu_b = 1$ or $\mu_a\mu_b$ has no fixpoints in U^*.*

Proof. Assume $a, b \in U^*$ are such that $\mu_a\mu_b$ has a fixpoint $c \in U^*$. Then $c\mu_a = c\mu_b$, and hence $\mu_{c\mu_a} = \mu_{c\mu_b}$. By [DS, Prop. 5.2(2)], this implies $\mu_a\mu_c\mu_a = \mu_b\mu_c\mu_b$ and hence $(\mu_a\mu_c)^2 = (\mu_b\mu_c)^2$.

By Proposition 3.11, there exist elements $\lambda, \mu \in K^*$ and odd numbers r, s (either 1 or prime) such that

$$\begin{aligned}\mathrm{Spec}(\mu_a\mu_c) &= \{\lambda \cdot \zeta_r^k \mid k \in \{0,1,\ldots,r-1\}\}\,,\\ \mathrm{Spec}(\mu_b\mu_c) &= \{\mu \cdot \zeta_s^k \mid k \in \{0,1,\ldots,s-1\}\}\,.\end{aligned}$$

Let $g := (\mu_a\mu_c)^{rs}$ and $h := (\mu_b\mu_c)^{rs}$; then $\mathrm{Spec}(g) = \{\lambda^{rs}\}$ and $\mathrm{Spec}(h) = \{\mu^{rs}\}$. Since $g^2 = h^2$, we have $\mu^{rs} = \pm\lambda^{rs}$; let $g' := g \cdot \lambda^{-rs}$ and $h' := h \cdot \mu^{-rs}$. We still have $(g')^2 = (h')^2$, but now $\mathrm{Spec}(g') = \mathrm{Spec}(h') = \{1\}$. If $g' = 1$, then it follows from the unique 2-divisibility of a unipotent subgroup containing h' that $h' = 1$ as well. So by Lemma 3.9(i), g' and h' have a one-dimensional fixpoint space. It now follows from Lemma 3.12 that $g' = h'$, so $g = h$ or $g = -h$. Since rs is odd, this implies $\mu_a\mu_c = \mu_b\mu_c$ or $\mu_a\mu_c = -\mu_b\mu_c$, hence $\mu_a\mu_b$ is 1 or -1. But since c is a fixpoint of $\mu_a\mu_b$, we must have $\mu_a\mu_b = 1$. □

We now arrive at our final contradiction. Indeed, since $n \geq 2$, there exist two linearly independent elements $a, b \in U^*$. Consider $h = \mu_a\mu_b \in H$, and let λ be an eigenvalue of h. Let $t \in K^*$ be such that $t^2 = \lambda^{-1}$; then $\mu_a\mu_{bt} = \mu_a\mu_b \cdot \lambda^{-1}$ has 1 as an eigenvalue, i.e. it has a non-trivial fixpoint in U^*. Hence by Proposition 3.13, $\mu_a\mu_{bt} = 1$, but this would imply $a = \pm bt$, and we have reached our final contradiction. This proves Theorem 2.1.

References

[ABC] T. Altinel, A. Borovik and G. Cherlin, *Simple groups of finite Morley rank*, book in preparation.

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

[Ch] G. Cherlin, "Superstable division rings", Logic Colloquium 1977 (Proc. Conf., Wrocław, 1977), pp. 99–111, Stud. Logic Foundations Math., 96, North-Holland, Amsterdam-New York, 1978.

[DS] T. De Medts and Y. Segev, "Identities in Moufang sets", to appear in *Trans. Amer. Math. Soc.*

[DST] T. De Medts, Y. Segev and K. Tent, "Some special features of special Moufang sets", submitted.

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

[M] A. Macintyre, "On ω_1-categorical theories of fields", Fund. Math. **71** (1971), no. 1, 1–25.

[MP] D. Macpherson and A. Pillay, "Primitive permutation groups of finite Morley rank", *Proc. London Math. Soc. (3)* **70** (1995), 481–504.

[S] Y. Segev, "Finite special Moufang sets of odd characteristic", submitted.

[SW] Y. Segev, R. M. Weiss, "On the action of the Hua subgroups in special Moufang sets", to appear in *Math. Proc. Cambridge Philos. Soc.*

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

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

Tom De Medts, Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, S22, B-9000 Gent, Belgium
`tdemedts@cage.UGent.be`

Katrin Tent, Fakultät für Mathematik, Universität Bielefeld, D-33501 Bielefeld
`ktent@mathematik.uni-bielefeld.de`