FINITE SPECIAL MOUFCANG SETS OF ODD CHARACTERISTIC

YOAV SEGEV

ABSTRACT. In this paper we classify finite special Moufang sets $M(U, \tau)$ of odd characteristic. The characteristic 2 case was handled in another paper by De Medts and the author. We prove, using elementary means that $U$ is elementary abelian. Then we show that $M(U, \tau)$ is the unique Moufang set whose little projective group is $\text{PSL}_2(|U|)$. The emphasis of this paper is on obtaining elementary proofs. Section 3 deals with root subgroups in any Moufang set and may be of independent interest.

INTRODUCTION

Our notation and terminology follow [DS1]. Let $M(U, \tau)$ be a finite special Moufang set, and for a prime power $q$, let $M(q)$ be the unique Moufang set whose little projective group is $\text{PSL}_2(q)$. In [DS2] we gave a short proof to the result that says that if $|U|$ is even, then $|U| = 2^k$ and $M(U, \tau) \cong M(2^k)$, for some integer $k \geq 1$.

This paper deals with the case when $|U|$ is odd. The news in our first theorem is that its proof does not require the Feit-Thompson odd order theorem and relies on basic group theory.

**Theorem 1.** Let $M(U, \tau)$ be a finite special Moufang set, with $|U|$ odd. Then $U$ is an elementary abelian $p$-group, for some prime $p$.

The proof of our second theorem requires the Feit-Thompson theorem, and Glauberman’s $Z^*-\text{Theorem}$, but unlike existing proofs, it is short, and requires no further results from the classification of finite simple groups.

**Theorem 2.** Let $M = M(U, \tau)$ be a finite special Moufang set with $|U| = q \equiv 3 \pmod{4}$. Then $M = M(q)$, the unique Moufang set whose little projective group is $\text{PSL}_2(q)$.

Our third theorem has four parts. Part (1) is proved using elementary means. For part (2) we use section 6 (p. 448–452) of [HKSe]. This section 6 is elementary (though by no means easy) and we were not able to find a shorter proof. The proof of part (3) is based only on the Feit-Thompson theorem,


\textbf{2000 Mathematics Subject Classification.} Primary: 17C60, 20E42; Secondary: 17C30.

\textbf{Key words and phrases.} Moufang set, root group.

\textsuperscript{1}Partially supported by BSF grant no. 2004-083.
it is short and, unlike earlier proofs, does not require other classification results. For part (4) we quote [H], and this is least satisfactory part.

**Theorem 3.** Let $\mathcal{M} = \mathcal{M}(U, \tau)$ be a finite special Moufang set with $|U| = q \equiv 1 \pmod{4}$. Let $G$ be the little projective group of $\mathcal{M}$ and let $S \in \text{Syl}_2(G)$, then

1. for any $x \in U^*$, $\mu_x$ fixes exactly two points;
2. any involution in $G$ fixes exactly two points, and it follows that $S$ is dihedral or semidihedral;
3. if $S$ is dihedral then $\mathcal{M} \cong \mathcal{M}(q)$;
4. ([H]) $S$ is not semidihedral.

We were not able to find a shorter more elementary proof to part (4), and we hope that this will be done some day. We note that in Theorem 3 if $S$ is semidihedral, then it is easy to see that $G$ is triply transitive, and this should somehow help to eliminate this case.

In §3 we obtain some results on root subgroups which apply to any Moufang set and in §4 we prove a proposition on the fixed points of the $\mu$-maps in special (but not necessarily finite) Moufang sets. These sections may be of independent interest.

**Acknowledgment.** The author would like to thank Tom De Medts for detailed remarks which improved the exposition of this paper.

1. **Notation, definitions and preliminaries**

In this section we describe our notation and give a few preliminary lemmas. In particular, Lemma 1.4 gives some basic results about Moufang sets that are used implicitly throughout this paper.

**Notation 1.1** (Notation for groups). Let $G$ be a group and $p$ a prime. In addition to [DS2, Notation 1.1] we introduce the following notation.

1. Given an integer $k > 0$, $E_{p^k}$ denotes an elementary abelian group of order $p^k$.
2. For $A \subseteq G$, $\langle A \rangle$ is the subgroup generated by $A$, and for $\mathcal{H}, \mathcal{K} \leq G$, $[\mathcal{H}, \mathcal{K}] := \langle [h, k] \mid h \in \mathcal{H}, k \in \mathcal{K} \rangle$.
3. For an integer $n$, $n_p = p^k$ means that $p^k$ divides $n$ but $p^{k+1}$ does not, thus $n_p$ is the $p$-part of $n$. For a set $A$ we let $|A|$ be the cardinality of $A$. Thus if $\mathcal{G}$ is a finite group $|\mathcal{G}|_p$ is the $p$-part of $|\mathcal{G}|$.
4. If $\mathcal{G}$ is finite, $\pi(\mathcal{G})$ is the set of primes dividing $|\mathcal{G}|$.
5. For an element $g \in \mathcal{G}$, $|g|$ denotes the order of $\mathcal{G}$ and $|g|_p$ is the $p$-part of $|g|$.

**Notation 1.2** (Notation for permutation groups). Let $\mathcal{G}$ be a permutation group on a set $\Omega$, and let $Y \subseteq \Omega$ be a nonempty subset. In addition to [DS2, Notation 1.2] we introduce the following notation.

1. If $Y = \{y_1, \ldots, y_n\}$, we sometimes write $\mathcal{G}_{y_1, \ldots, y_n}$ instead of $\mathcal{G}_Y$. 
(2) If $L \leq G(Y)$, then $L^Y \cong L/L_Y$ denotes the permutation group on $Y$ induced by $L$.

**Notation 1.3** (Notation for Moufang sets). Our notation for Moufang sets follows [DS1]. Thus the notation $M(U, \tau)$ is explained there, as well as $\alpha_u, \mu_u, u \in U^*$. Let $M := M(U, \tau)$ be a Moufang set. In addition to [DS2, Notation 1.3] we introduce the following notation.

1. If $M$ is special with abelian root groups, then $U$ is a vector space over $\mathbb{F}_p$, for some prime $p$, or over $\mathbb{Q}$. $\textsf{F}$ always denotes $\mathbb{F}_p$ or $\mathbb{Q}$ and we let $\text{char}(U) = p$ or $0$ in the respective cases.

2. We reader should be warned that although we use additive notation for $U$ we are of course not assuming that $U$ is abelian.

The next lemma collects several basic properties of Moufang sets which are used repeatedly throughout this paper without further reference.

**Lemma 1.4.** Let $M := M(U, \tau)$ be a Moufang set and let $\rho \in \text{Sym}(X)$ with $M(U, \rho) = M(U, \tau) = M(U, \rho^{-1})$. Let also $h \in H$ and $x, y \in U^*$. Then

1. $\tau \mu x \in \text{Aut}(U)$, and $H \leq \text{Aut}(U)$;
2. $\mu_x = \mu_{-x^h}, \mu_{x^h} = \mu_x$ and $\alpha_x = \alpha_{x^h}$;
3. assume that $M$ is special then
   (i) if $x \mu y = -x$, then $y = \pm x$;
   (ii) if $\mu_x = \mu_y$, then $y = \pm x$;
   (iii) for $\eta \in \{\rho, h\}$, if $[\mu_x, \eta] = 1$, then $x \eta = \pm x$, so $x \eta^2 = x$. In particular, if $|h|$ is odd, $x h = x$.
   (iv) if $x \mu y = x$, then $y \mu x = y$;
   (v) if in addition $U$ is abelian then $\mu_z$ is an involution, for all $z \in U^*$.

**Proof.** Part (1) is [DW, Theorem 3.2]. Part (2) is [DS1, Prop. 3.9(2)]. (3i) is [DST, Lemma 7.7] and (3i) follows from (3i) because $x \mu_x = -x$. To prove part (3iii), suppose $\mu_x = \mu_y = \mu_{\pm x^h}$. Then $x \eta = \pm x$ and (3iii) follows. Part (3iv) is [DST, Prop. 7.8] and (3v) is [DS1, Lemma 5.1].

The following lemma is a slight generalization of [DST, Lemma 5.2(4)] which we will use in this paper.

**Lemma 1.5.** Let $M(U, \tau)$ be a special Moufang set with $M(U, \tau) = M(U, \tau^{-1})$. Then

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

**Proof.** Part (1) is [DS1, Lemma 4.4(2)]. We have

\[
(a + b) \tau = (a \tau^{-1} + b \tau^{-1}) \tau \equiv (a \tau + b \tau) \mu_{-b} + b \tau \\
\equiv (a \tau + b \tau) \tau^{-1} \mu_b \tau + b \tau \equiv (a \mu_b - b) \tau + b \tau.
\]
where the equality (*) above comes from Lemma 1.4(2), and the equality (***) follows since $\tau^{-1} \mu_b \in \text{Aut}(U)$. The other equality of (2) follows similarly from the second equality in (1). \[\blacksquare\]

The final lemma of this section will be needed in §6.

**Lemma 1.6.** Let $p, q$ be odd primes and let $P$ be a nontrivial finite $p$-group acting faithfully on a nontrivial finite elementary abelian $q$-group $E$. Assume that for each characteristic subgroup $C$ of $P$,

(i) $C_E(z) = 0$, for all $1 \neq z \in Z(C)$.

(ii) If $C$ is nonabelian, then $C_C(e) \neq 1$, for each $e \in E^*$.

(iii) There are integers $m(C) \geq s(C) \geq 0$ such that for each $e \in E^*$,

$$|C_C(e)| \in \{p^{m(C)}, p^{s(C)}\}.$$ 

Then $P$ is cyclic, and hence $C_P(e) = 1$, for all $e \in E^*$.

**Proof.** Notice that if $P$ is cyclic, then, by (i), $C_P(e) = 1$, for all $e \in E^*$. Hence it suffices to show that $P$ is cyclic.

Assume toward a contradiction that $P$ is not cyclic and choose $P$ with $|P|$ minimal. Clearly, by hypothesis (i), $P$ is nonabelian. Notice that every characteristic subgroup of $P$ satisfies the hypotheses of the lemma and hence all proper characteristic subgroups of $P$ satisfy the conclusion of the lemma. In particular, $P$ contains no noncyclic abelian characteristic subgroups, that is $P$ is of symplectic type. By [A, (23.9)], $P$ is a central product of a cyclic group $R$ and an extraspecial group $M$.

Since $P$ is not cyclic, $M \neq 1$, so by [A, (23.12)], $\Omega_1(M)$ is not cyclic and it is of exponent $p$. Since all proper characteristic subgroups of $P$ are cyclic, $P = \Omega_1(P)$. Thus $P = M$ and

\[(1.1) \quad P \text{ is extraspecial of exponent } p.\]

Let $s = s(P)$. Notice that if $s = 0$, then by hypothesis (ii) (applied to $P$), $P$ is abelian, a contradiction.

Hence we may assume that $s > 0$. Let

$$S := \{e \in E^* \mid |C_P(e)| = p^s\},$$

and let $e_1 \in S$ and $r_1 \in P^*$ such that $[e_1, r_1] = 0$ and consider the subgroup

$$R := \langle r_1, Z(P) \rangle \cong E_{p^s},$$

of $P$. By (1.1) $R \trianglelefteq P$. Let

$$\{T_1, \ldots, T_p\} \text{ be the subgroups of order } p \text{ of } R \text{ distinct from }$$

$Z(P)$, with $r_1 \in T_1$, and let $E_i = C_E(T_i)$, $i = 1, \ldots, p$.

Notice that (see [P2, Lemme, Appendice X, bottom p. 282] for the argument below)

\[(1.2) \quad E = E_1 \oplus \cdots \oplus E_p.\]
Indeed, $E = \sum_{i=1}^{p} E_i$ (cf. Exercise 8.1 in [A]). We show that this sum is direct. Suppose the sum $\sum_{i=1}^{k-1} E_i$ is direct and let $x \in E_k \cap \sum_{i=1}^{k-1} E_i$. Write $x = x_1 + \cdots + x_{k-1}, x_j \in E_j$, and let $t \in T_k$. Then $E_j t = E_j$, for all $j$ and $x_1 + \cdots + x_k = x = xt = x_1 t + \cdots + x_k t$.

Hence, for $j \in \{1, \ldots, k - 1\}, x_j \in C_E(T_k)$, so $x_j \in C_E(T, T_k) = C_E(R)$. But by hypothesis (i), as $Z(P) \leq R$, $C_E(R) = 0$, so $x = 0$, and (1.2) holds.

Since $T_1 = \langle r_1 \rangle, e_1 \in E_1$. Let $e_2 \in E_2^*$. Notice that since $P$ permutes $\{E_i \mid 1 \leq i \leq p\}$, $C_P(e_1 + e_2) = C_P(e_1) \cap C_P(e_2)$, and it follows from hypothesis (iii) that $C_P(e_1) = C_P(e_1 + e_2) \subseteq C_P(e_2)$. But then $T_1 \subseteq C_P(e_1) \subseteq C_P(e_2)$. This is a contradiction since $T_1$ does not centralize $e_2$. \hfill \square

**Definition 1.7.** We will say that a finite special Moufang set $\mathbb{M}(U, \tau)$ is a minimal counter example to Theorem 2 or 3, if $\mathbb{M}(U, \tau) \not\equiv \mathbb{M}(|U|)$, but for any finite special Moufang set $\mathbb{M} := \mathbb{M}(V, \rho)$, with $|V| < |U|$, and $|V| \equiv |U|$ (mod 4), $\mathbb{M} = \mathbb{M}(|V|)$.

## 2. $U$ IS ABELIAN

In this section we assume that $\mathbb{M}(U, \tau)$ is a special Moufang set with $U$ finite and our goal is to prove that $U$ is abelian. We thus assume that $\mathbb{M}(U, \tau)$ is a counterexample with $|U|$ minimal. Since $U$ is not abelian, $|U|$ is odd, by [DST, Theorem 3]. Further, by [DST, Theorem 4], there exists $a \in U^*$ such that $\mu_a$ is not an involution. Also, by [DS1, Prop. 4.10(5)], $\mu_a = 1$, for each $x \in U^*$.

**Lemma 2.1.**

1. Let $h \in H^*$. Then $C_U(h)$ is an elementary abelian $p$-group, for some prime $p$;
2. for each $x \in U^*$, $|x|$ is an odd prime number;
3. let $x \in U^*$, then $C_U(x)$ is a $p$-group for some prime $p$;
4. $U$ is a perfect group.

**Proof.** Set $V := C_U(h)$. If $V = 0$, then there is nothing to prove. So assume $V \neq 0$ and pick $x \in V^*$. By [DST, Cor. 1.8] if we let $\rho := \mu_x \mid V \cup \{\infty\}$, then $\mathbb{M}(V, \rho)$ is a special Moufang set. Thus, by induction, $V$ is abelian and hence an elementary abelian $p$-group (cf. [DS1, Prop. 4.6]). This shows (1).

(2) follows by [DS1, Prop. 4.6(4)], and (3) follows from [DST, Prop. 5.3].

Since $[U, U]$ is an $H$-invariant subgroup of $U$, Theorem 1.2 of [SW] implies that either $U$ is perfect or $U$ is abelian, so (4) holds. \hfill \square

We start with

**A. The case when $|\pi(U)| \geq 4$.**

**Lemma 2.2.** $H$ contains no elementary abelian subgroup of order 4.

**Proof.** Assume the contrary and let $E \leq H$ be an elementary abelian subgroup of order 4. Let $p$ be a prime dividing $|U|$. Since $|\text{Syl}_p(U)|$ is odd and
since $E$ acts on $\text{Syl}_p(U)$, $E$ normalizes a $p$-Sylow subgroup $P$ of $U$. Hence (cf. Exercise 8.1 in [A]) $P = \langle C_P(e) : e \in E^* \rangle$, so $C_P(e) \neq 1$, for some $e \in E^*$. In particular, since $|\pi(U)| > 3 = |E^*|$, there will be two distinct primes $p, q \in \pi(G)$ and $e \in E^*$ such that $|C_U(e)|_p \neq 1 \neq |C_U(e)|_q$, contrary to Lemma 2.1(1).

\begin{lemma}
There exists a unique prime $p$ such that if $a \in U^*$ and $\mu^2_a \neq 1$, then $|a| = p$.
\end{lemma}

\begin{proof}
By Lemma 2.2 a 2-Sylow subgroup of $H$ contains a unique involution, because if $T \in \text{Syl}_2(H)$, then $Z(T)$ contains an involution $z$, and then, by Lemma 2.2, $\{z\} = \text{Inv}(T)$. (In fact Lemma 2.2 implies that $T$ is either cyclic or a generalized quaternion group, but we do not need this fact.) In particular, by Sylow’s theorem, all involutions in $H$ are conjugate. Assume that $a \in U^*$ is such that $\mu_a^2 \neq 1$. Then, by [DS1, Prop. 4.10(5)] $\mu_a$ has order 4 so $\mu_a^2 \in \text{Inv}(H)$. Let also $b \in U^*$ such that $\mu_b^2 \in \text{Inv}(H)$. Then there exists $h \in H$ such that $\mu_b^2 = (\mu_a^2)^h = \mu_{ab}$. Set $g := \mu_a^2$. Then both $b$ and $ah$ are fixed by $g$, so by Lemma 2.1(1) $b$ and $ah$ and hence $b$ and $a$ have the same order.

We can now obtain a contradiction under the hypothesis that $|\pi(U)| \geq 4$. Let $p$ be the prime of Lemma 2.3. We claim that

\begin{align}
(2.1) \quad N_U(\mathcal{P}) \text{ is a } p\text{-group for each nontrivial } p\text{-subgroup } \mathcal{P} \leq U.
\end{align}

Let $\mathcal{P}$ be a nontrivial $p$-subgroup of $U$ and assume that there exists $y \in N_U(\mathcal{P})$ with $|y| = q \neq p$. Note that by Lemma 2.3, if $b \in U^*$ is an element of order $q$, then $\mu_b$ is an involution. Let $x \in \mathcal{P}$. We claim that

\begin{align*}
y, \quad -x + y + x, \quad y + x \text{ and } -y + x \text{ have order } q.
\end{align*}

Of course this is true for $y$ and $-x + y + x$. Next, since $y$ normalizes $\mathcal{P}$, the order of $y + x$ in $\mathcal{P}(y)$ is divisible by $q$, and hence, by Lemma 2.1(2) is equal to $q$. The same argument shows that $-y + x = q$. But now

\begin{align*}
\mu_y, \quad \mu_{-x+y+x}, \quad \mu_{y+x} \text{ and } \mu_{-y+x} \text{ are all involutions},
\end{align*}

so by [DST, Theorem 4], $x$ and $y$ commute. But this contradicts the fact that $C_U(y)$ is a $q$-group (see Lemma 2.1(3)). Hence the assertion in equation (2.1) holds. But now, by the Frobenius normal $p$-complement theorem (cf. [A, 39.4]), $U$ has a normal $p$-complement. In particular $U$ is not perfect, contradicting Lemma 2.1(4).

In view of the contradiction obtained in subsection A, and since $U$ is a perfect group, we may assume that $|\pi(U)| = 3$ (since if $|\pi(U)| = 1$ or 2, $U$ is solvable).
B. The case where $|\pi(U)| = 3$.

In this subsection we assume that $|\pi(U)| = 3$. Further, if the 2-rank of $H$ is one (i.e. if $H$ contains no elementary abelian subgroup of order 4) then the contradiction obtained in subsection A is also obtained in the case when $|\pi(U)| = 3$. Thus we may pick $E \leq H$ an elementary abelian 2-subgroup of order 4. We let $\pi(U) = \{p, q, r\}$ and we let $P \in \text{Syl}_p(U)$, $Q \in \text{Syl}_q(U)$ and $R \in \text{Syl}_r(U)$ be subgroups normalized by $E$.

**Step 1.** For each $e \in E$ there exists a prime $p(e) \in \pi(U)$ such that $C_U(e)$ is a nontrivial $p(e)$-group, furthermore if $e, f \in E$ are distinct, then $p(e) \neq p(f)$.

Let $e \in E$. Since $U$ is not abelian, $U$ is not inverted by $e$, so $C_U(e) \neq 0$. Then, by Lemma 2.1(3), there exists $p(e) \in \pi(U)$ such that $C_U(e)$ is a $p(e)$-group.

Assume that $e, f$ are distinct elements of $E$ such that $p(e) = p(f) = p$. Since $Q = C_U(v) \mid v \in E^*$, and since $C_U(e)$ and $C_U(f)$ are $p$-groups, we see that $Q = C_U(w)$ where $\{w\} = E^* \setminus \{e, f\}$. But the same argument shows that $R = C_U(w)$. This contradicts the fact that $C_U(w)$ is an $\ell$-group, for some prime $\ell$.

We let $e_p, e_q, e_r$ be an involution in $E$ such that $C_U(e_\ell)$ is an $\ell$-group $\ell = p, q, r$ respectively.

**Step 2.** $P$ is elementary abelian, $P = C_U(e_p)$ and there exists $x \in N_U(P)$ of order $q$ or $r$ such that $xe_p = -x$.

Since $e_q$ normalizes $P$, but $C_P(e_q) = 1$, $e_q$ inverts $P$, so in particular $P$ is abelian of exponent $p$ so $P$ is elementary abelian. Similarly $e_r$ inverts $P$ so $e_p = e_q e_r$ centralizes $P$. Next, by the Burnside normal $p$-complement theorem (cf. [A, 39.1]), $N_U(P) \neq P$. Hence we may assume without loss that $|N_U(P)|_q \neq 1$. Since $E$ normalizes $P$, $E$ normalizes $N_U(P)$, so $E$ normalizes a $q$-Sylow subgroup $Q$ of $N_U(P)$. Since $C_Q(e_p) = 1$, we see that $e_p$ inverts $Q$.

We can now reach a contradiction in the case where $|\pi(U)| = 3$. Let $x \in N_U(P)$ of order $q$ be an element inverted by $e_p$. Then $e_p$ normalizes $P\langle x \rangle$ and acts on $P\langle x \rangle$ by $(y + x \cdot t)e_p = y - x \cdot t$, $y \in P$. Thus, for $y \in P^*$ we have

$((y + x) \cdot 2)e_p = (y + x + y - x + x \cdot 2)e_p = y + x + y - x - x \cdot 2 = y + x + y - x \cdot 3$,

and also

$((y + x) \cdot 2)e_p = y - x + y - x$.

Thus $y + x + y - x \cdot 3 = y - x + y - x$ or $x \cdot 2 + y - x \cdot 2 = y$, and we see that $x \cdot 2$ centralizes $y$, a contradiction since by Lemma 2.1(3) $C_U(y)$ is a $p$-group.
With this contradiction, we conclude that such a minimal counterexample cannot exist, and hence $U$ is abelian. By [DS1, Prop. 4.6], $U$ is an elementary abelian $p$-group, for some prime $p$. This completes the proof of Theorem 1.

3. Root subgroups

In this section $\mathcal{M}(U, \tau)$ is any Moufang set (not necessarily special and not necessarily finite).

Definitions and notation 3.1.  
(1) A root subgroup of $U$ is a subgroup $V \leq U$ such that $V^*\mu_x = V^*$, for all $v \in V^*$. Recall from [DST, Lemma 1.7] that if we pick $x \in V^*$ and we let $\rho := \mu_x \restriction (V \cup \{\infty\})$, then $\mathcal{M}(V, \rho)$ is a Moufang set.

(2) Given a root subgroup $0 \neq V \leq U$ and $x \in V^*$, we let $V_\infty := \{\alpha_v \mid v \in V\}$, $V_0 := V_\infty^\alpha$, and for $w \in V$, $V_w := V_0^{\alpha_w}$. Notice that by Lemma 1.4(2), the definition of $V_\infty$ is independent of the choice of $\mu_x$.

(3) Given a root subgroup $0 \neq V \leq U$, we let $G(V) := \langle \alpha_v, \mu_v \mid v \in V^* \rangle$, $N(V) := \langle \mu_v \mid v \in V^* \rangle$, $H(V) := \langle \mu_v \mu_w \mid v, w \in V^* \rangle$ and $X(V) := V \cup \{\infty\}$.

(4) A generalized rank one group with unipotent subgroups $A$ and $B$ is a generalization of a rank one group according to Timmesfeld ([Ti, p. 1]): It is a group generated by its distinct subgroups $A$ and $B$ (but, unlike [Ti], we do not require that $A$ and $B$ are nilpotent) such that for all $a \in A^*$ there exists $b \in B^*$ with $A^b = B^a$ and vice versa.

(5) A generalized rank one group with unipotent subgroups $A$ and $B$ is special if for each $a \in A$ there exists $b \in B$ with $a^b = (b^{-1})^a$ (cf. [DST, Prop. 1.10(5)]).

Lemma 3.2. Let $0 \neq V \leq U$ be root subgroup, set $X := X(V)$ and let $G := G(X)$ and $\mathfrak{G} := G(V)$. Then

(1) $\mathfrak{G}$ is a generalized rank one group with unipotent subgroups $V_\infty$ and $V_0$; furthermore, if $\mathcal{M}(U, \tau)$ is special, then $\mathfrak{G}$ is special.

(2) $\mathfrak{G} \leq G$ and $G = \mathfrak{G}H(V)$;

(3) $G_X = H_X$ and $[G_X, \mathfrak{G}] = 1$, in particular, $G_X = Z(\mathfrak{G})$;

(4) if $|V| > 3$ and $\mathcal{M}(U, \tau)$ is special then $\mathfrak{G}$ is a perfect group.

Proof. (1): Fix $x \in V^*$. We claim that

$$V_\infty^{\alpha_c^x} = V_0^{\alpha_c^{\mu_x}}, \quad \text{for all } c \in V^*.$$ 

Since $\alpha_c^{\mu_x}$, $c \in V^*$ is an arbitrary element in $V^*$ and $\alpha_c^{\mu_x}$ is an arbitrary element in $V_0^*$, the first part of (1) will follow.

Now $V_0^{\alpha_c^{\mu_x}} = V_\infty^{\alpha_c^{\mu_x}}$, so we must show that

$$\delta_c := \mu_x^{-1}\alpha_c^{\mu_x}\alpha_{-c^{\mu_x}}\mu_x^{-1} \text{ normalizes } V_\infty.$$ 

(3.1)
Now, by [DS1, Prop. 3.10(2&3)],
\[ \alpha_c h x \alpha_{-c} h x^{-1} = \mu_c \alpha_{-((-c) \mu_c)} \]
so
\[ \delta_c = \mu_{-c} \alpha_{-((-c) \mu_c)}. \]
It follows that for \( v \in V^* \),
\[ \alpha_v^\delta_c = \alpha_v^\mu_{-c} \alpha_{-((-c) \mu_c)} = \alpha_{v \mu_{-c} \mu_{-c}} \alpha_{-((-c) \mu_c)} \]
\[ = \alpha_{(-c) \mu_c + v \mu_{-c} \mu_{-c} - ((-c) \mu_c)}. \]
Now the restriction of \( \mu_{-c} \mu_{-c} \) to \( V \) is an automorphism of \( V \), and conjugation by \( (-c) \mu_c \) is also an automorphism of \( V \), so (3.1) holds and the first part of (1) is proved.

For the second part of (1) suppose \( M(U, \tau) \) is special let \( v \in V^* \) and let \( \alpha := \alpha_c \in V_\infty \). We claim that \( \beta := \alpha^{\mu_{-c}} \) satisfies \( \alpha \beta = \beta \alpha \). For that we use [DS1, Lemma 4.3(3)] which implies that
\[ \mu_{-c} = \alpha_{-c} \mu_{-c} \alpha_{-c} \mu_{-c}. \]
Hence
\[ \alpha_c^{\mu_{-c} \alpha_c} = (\alpha_c)^{\mu_{-c}} \iff \alpha_c = (\alpha_c)^{\mu_{-c} \alpha_{-c} \mu_{-c}} \iff \alpha_c = (\alpha_c)^{\mu_{-c} \alpha_{-c} \mu_{-c}} \iff \alpha_c = (\alpha_c)^{\alpha_c \mu_{-c}} \iff \alpha_c = \alpha_c, \]
where we have used the fact that \( \mu^2_{-c} \in Aut(U) \) and \( c \mu^2_{-c} = c \).

(2): Let \( g \in \mathcal{G} \); since \( \mathcal{G} \) is doubly transitive on \( X \) (by (1)), there exists \( g \in \mathcal{G} \) such that \( \mathcal{G} g \in H \), so \( \mathcal{G} = \mathcal{G} H(V) \). Since for each \( h \in H(V) \) and each \( v \in V^* \), \( \alpha_v^h = \alpha_v h \) and \( \mu_v^h = \mu_v h \), \( H(V) \) normalizes \( \mathcal{G} \) and we see that \( \mathcal{G} \leq \mathcal{G} \).

(3): Clearly \( G_X \leq H \), so \( G_X = H_X \) and since \( H_X \) centralizes \( \alpha_v \) and \( \mu_{-c} \), for all \( v \in V^* \), \( [H_X, \mathcal{G}] = 1 \). Thus \( [G_X, \mathcal{G}] = 1 \), and it follows that \( \mathcal{G} \leq Z(\mathcal{G}) \). Since \( \mathcal{G} \) is doubly transitive on \( X \), it follows that \( Z(\mathcal{G}) \leq G_X \).

(4): Assume the hypotheses of (4) and set \( \mathcal{H} := H(V) = \langle \mu_v \mu_w \mid v, w \in V^* \rangle \). Notice that \( \mathcal{H}^X \) is the little projective group of \( M(V, \rho) \) (where \( \rho = \mu_{-c} \upharpoonright X \) and \( x \in V^* \); see Definition 3.1(1)). By [DST, Lemma 1.7], \( M(V, \rho) \) is special. Since \( \mathcal{H}^X \) is the Hua subgroup of \( M(V, \rho) \), [DST, Theorem 1(1)] implies that
\[ [\mathcal{H}^X, V^X] = V^X_\infty. \]
We show that (3.2) implies that \( [\mathcal{H}, V_\infty] = V_\infty \). Since \( \mathcal{G} \) is generated by the conjugates of \( V_\infty \), this will imply that \( \mathcal{G} \) is perfect.
Clearly $V_{\infty} \cap \Phi_X = 1$, so if $W_{\infty}$ is a proper subgroup of $V_{\infty}$, then $W_{\infty}^X$ is a proper subgroup of $V_{\infty}^X$. Notice now that $\mathcal{H}$ normalizes $V_{\infty}$. Suppose $W_{\infty} := [\mathcal{H}, V_{\infty}]$ is a proper subgroup of $V_{\infty}$, then $[\mathcal{H}^X, V_{\infty}^X]$ is a proper subgroup of $V_{\infty}^X$, contradicting (3.2). Hence $[\mathcal{H}, V_{\infty}] = V_{\infty}$ and part (4) is proved. 

**Lemma 3.3.** Let $0 \neq V \leq U$ be a subgroup of $U$ and let $\rho \in \text{Sym}(X)$ with $M(U, \rho) = M(U, \tau) = M(U, \rho^{-1})$. Assume that $V^*\rho = V^*$, then

1. if $M(U, \rho)$ is special, then $V$ is a root subgroup of $U$;
2. if $V$ is a root subgroup of $U$, then $\rho$ normalizes $G(V)$.

**Proof.** The proof of (1) is exactly as in the proof of [DST, Cor. 1.8(2)], for completeness we include it.

Let $v, w \in V$ with $w \neq -v$, then by Lemma 1.5(2),

$$(v + w)\rho = (v\mu_w - w)\rho + w\rho,$$

by our hypothesis, $(v + w)\rho, w\rho \in V$, so $(v\mu_w - w)\rho \in V$ and applying $\rho^{-1}$ shows that also $v\mu_w - w \in V$, so $v\mu_w \in V$, and $V$ is a root subgroup of $U$.

To prove (2), we have $\mu_i^* = \mu_{-i}^*$, for all $v \in V^*$, so $\mu_i^* \in G(V)$. It thus remains to show that $\alpha_0^0 \in G(V)$. By [DS1, Prop. 3.10(2, 3)], taking $a = (-v)\rho$ we get

$$\mu_a = \alpha_a^0 \alpha_{(-a)\mu_a}^0, \quad a = (-v)\rho.$$

Hence $\alpha_0^0 = \alpha_{-a}^0 \alpha_{(-a)\mu_a}^0$. Notice that $a \in V$ and since $V$ is a root subgroup, also $(-a)\mu_a \in V$. Thus $\alpha_0^0 \in G(V)$ as asserted. 

**Lemma 3.4.**

1. if $V \leq U$ is a root subgroup, and $g \in N$, then $V := V^* g \cup \{0\}$ is also a root subgroup of $U$;
2. if $\{V_i \mid i \in I\}$ are root subgroups of $U$, then $\bigcap_{i \in I} V_i$ is a root subgroup of $U$;
3. let $K \leq H$, then $C_U(K)$ is a root subgroup of $U$.

**Proof.** (1): Let $v \in V$. If $g \notin H$, set $h := \mu_v g$, while if $g \in H$, set $h := g$. Then $h \in H$ and since $V^* \mu_v = V^*, V^* g \cup \{0\} = V h$, so $V$ is a subgroup of $U$. Then, for $u g, v g \in V^*$, we have $(u g) \mu_{vg} = (u g)^{-1} \mu_{vg} g = u \mu_{vg} g \in V$, since $u \mu_{vg} \in V$, so $V$ is a root subgroup.

(2): Let $V := \bigcap_{i \in I} V_i$, and let $v \in V^*$. Then $V^* \mu_v = V^*$, for all $i$, so $V^* \mu_v \leq V^*$. As this holds for $-v$ as well, $V^* \mu_v = V^*$ and $V$ is a root subgroup.

(3): By [DST, Cor. 1.8(1)], $C_U(h)$ is a root subgroup, for all $h \in H$. Hence, by (2), $C_U(K) = \bigcap_{h \in H} C_U(h)$ is a root subgroup.

**Lemma 3.5.** Assume that $M(U, \tau)$ is special and that $U$ is abelian. Let $h \in H$, and assume that $\lambda \in \mathbb{F}^*$ is an eigenvalue of $h$. Let $V_{h, \lambda} := \{x \in U \mid x h = x \cdot \lambda\}$ be the $\lambda$-eigenspace of $h$. Then

1. $V_{h, \lambda}$ is a root subgroup of $U$;
(2) if $-\lambda$ is also an eigenvalue of $h$, then for $x \in V_{h,-\lambda}^*$ we have $V_{h,\lambda}^* \mu_x = V_{h,\lambda}^*$.

Proof. Set $V := V_{h,\lambda}$, let $v \in V$ and let $w \in V^* \cup V_{h,-\lambda}^*$. Then, by [DS1, Prop. 4.6],

$$v \mu_w h = v h \mu_{wh} = (v \cdot \lambda) \mu_{w,(-\lambda)} = v \mu_w \cdot \frac{\lambda^2}{\lambda},$$

hence $v \mu_w \in V$ and so $V^* \mu_w = V^*$. This implies that $V$ is a root subgroup of $U$ and that (2) holds.

Notation 3.6. Given $1 \neq h \in H$. If $\lambda \in F^*$ is an eigenvalue of $h$, we let $V_{h,\lambda}$ be the corresponding eigenspace.

4. Fixed points of the $\mu$-maps in special Moufang sets with abelian root groups

In this section $\mathcal{M}(U, \tau)$ is a special Moufang set (not necessarily finite) with abelian root groups. If $U$ is finite, we assume that $|U|$ is odd. We let $F$ be the field as in Notation 1.3(5).

Proposition 4.1. Let $a, b \in U^*$ such that $a \mu_b = a$. Then

1. $(a \cdot s + b \cdot t) \mu_b = (a \cdot s - b \cdot t) \cdot \frac{1}{t^2 + s^2}$, for all $s, t \in F^*$ such that $t^2 + s^2 \neq 0$. In particular, $(a, b)$ is a root subgroup of $U$.

2. $\mathcal{M}(\langle a, b \rangle, \mu_b) \cong \mathcal{M}(\mathbb{K})$, where $\mathbb{K} = F$ if $\text{char}(U) \equiv 1 \pmod{4}$, and if $\mathbb{K}$ is a quadratic field extension of $F$ otherwise.

3. if $\mathcal{M}(U, \rho) = \mathcal{M}(U, \tau) = \mathcal{M}(U, \rho^{-1})$ and if $a \rho = a$, $b \rho = b$, then $(a \cdot s + b \cdot t) \rho = (a \cdot s + b \cdot t) \cdot \frac{1}{t^2 + s^2}$, for all $s, t \in F^*$ such that $t^2 + s^2 \neq 0$.

4. if $U$ is finite and $c \in U^*$ is such that $a \mu_c = a$ then $b \mu_c \neq b$.

Proof. (1): Let $s, t \in F^*$ such that $t^2 + s^2 \neq 0$. By Lemma 1.5(2) and [DS1, Prop. 4.2(2&6)],

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

$$= (a \cdot \frac{s^2}{2} - b \cdot s) \mu_b - b \cdot \frac{1}{s}$$

$$= (a \cdot s - b \cdot t) \mu_b \cdot \frac{s}{t} - b \cdot \frac{1}{s}.$$

Thus

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

(4.1)

We also have

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

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

$$= (b \cdot t - a \cdot s) \mu_b \cdot \frac{s}{t} + a \cdot \frac{1}{t}.$$
and hence
\[(4.2) \quad (a \cdot t + b \cdot s)\mu_b = (b \cdot t - a \cdot s)\mu_b \cdot \frac{1}{t} + a \cdot \frac{1}{t}.\]
Comparing (4.1) and (4.2) we obtain
\[
(a \cdot s - b \cdot t)\mu_b \cdot \frac{1}{t} - b \cdot \frac{1}{s} = (b \cdot t - a \cdot s)\mu_b \cdot \frac{1}{t} + a \cdot \frac{1}{t} \iff
\]
\[
(a \cdot s - b \cdot t)\mu_b \cdot \left(\frac{1}{t} + \frac{1}{s}\right) = a \cdot \frac{1}{t} + b \cdot \frac{1}{s} \iff
\]
\[
(a \cdot s - b \cdot t)\mu_b \cdot (t^2 + s^2) = a \cdot s + b \cdot t.
\]
Replacing \(b\) with \(-b\) proves the first part of (1). Now if \(\text{char}(U) \equiv 1 \pmod{4}\), then \(\langle a, b \rangle = \langle b \rangle\) by [DST, Proposition 7.8(4)], and \(\langle b \rangle\) is a root subgroup of \(U\). Otherwise \(t^2 + s^2 \neq 0\), for all \(s, t \in F^*\), so the “in particular” part of (1) holds as well.

(2): We thank Tom De Medts for providing the proof of this part. If \(\text{char}(U) \equiv 1 \pmod{4}\), then \(\langle a, b \rangle = \langle b \rangle\). It then follows from [DST, Lemma 7.4] that \(M(\langle a, b \rangle, \mu_b) \cong M(p)\).

So assume now that \(\text{char}(U) \equiv 3 \pmod{4}\) or \(\text{char}(U) = 0\). Then \(-1\) is a non-square in \(F\); let \(K := F[\gamma]\), where \(\gamma^2 = -1\). Then \(K = \{\gamma \cdot s + t \mid s, t \in F\}\), and observe that
\[-(\gamma \cdot s + t)^{-1} = (\gamma \cdot s - t) \cdot \frac{1}{s^2 + t^2}, \quad \text{for all } (s, t) \in (F \times F)^*.
\]
Comparing this with the formula obtained in (1), this shows that the map \(\varphi : (K, +) \to \langle a, b \rangle : \gamma \cdot s + t \mapsto a \cdot s + b \cdot t\) is an isomorphism for which \(\varphi(r)\mu_b = \varphi(-r^{-1})\), \(r \in K\), and hence \(M(\langle a, b \rangle, \mu_b) \cong M(K)\); see, for example, [DW, Example 3.1].

(3): Let \(\rho\) be as in (3) and assume that \(a \rho = a\) and \(b \rho = b\). If \(\text{char}(U) \equiv 1 \pmod{4}\), then by [DST, Prop. 7.8(4)], \(b = ea \cdot \sqrt{-1}\), with \(e \in \{1, -1\}\), and then, by [DS1, Prop. 4.6(2)], \(b \rho = -e a \sqrt{-1} = -b\), a contradiction. Hence \(\text{char}(U) \not\equiv 1 \pmod{4}\). As in the proof of (1), using Lemma 1.5(2), we get
\[
(a \cdot t + b \cdot s)\rho = ((a \cdot t)\mu_{b,s} - b \cdot s)\rho + (b \cdot s)\rho
\]
\[
= (a \cdot \frac{a^2}{t} - b \cdot s)\rho + b \cdot \frac{1}{s}
\]
\[
= (a \cdot s - b \cdot t)\rho \cdot \frac{1}{s} + b \cdot \frac{1}{s}.
\]
so
\[(4.3) \quad (a \cdot t + b \cdot s)\rho = (a \cdot s - b \cdot t)\rho \cdot \frac{1}{s} + b \cdot \frac{1}{s}.
\]
and similarly, instead of equation (4.2) we get
\[(4.4) \quad (a \cdot t + b \cdot s)\rho = (b \cdot t - a \cdot s)\rho \cdot \frac{1}{t} + a \cdot \frac{1}{t}.
\]
Comparing (4.3) and (4.4) (and replacing \(b\) with \(-b\)) we get
\[(4.5) \quad (a \cdot s + b \cdot t)\rho = (a \cdot s + b \cdot t) \cdot \frac{1}{t^2 + s^2}.
\]

(4): As in the beginning of the proof of part (3) (with \(\mu_c\) in place of \(\rho\)) we get that \(\text{char}(U) \equiv 3 \pmod{4}\). Since any element in \(F^*\) is a sum of two
squares, we may pick \( s, t \in F^* \) such that \( t^2 + s^2 = -1 \). By (3) we get that 
\[
(a \cdot s + b \cdot t)\mu_c = -(a \cdot s + b \cdot t).
\]
By [DST, ], \( c = \pm (a \cdot s + b \cdot t) \). Using [DS1, Lemma 4.4(3)] and [DS1, Lemma 4.6(2&6)], we get
\[
\mu_c = \mu_{a,s+b,t} = (a \cdot s + b \cdot t) \cdot s = \left[-(a \cdot s + b \cdot t) + (a \cdot s)\mu_{b,t} - b \cdot t \right] \cdot s
\]
But since \( a, b \) are linearly independent we see that \( \mu_c \neq a \), a contradiction.  
\[\square\]

5. The Case When \(|U| \equiv 3 \pmod{4}\)

In this section \( M(U, \tau) \) is a finite special Moufang set with \(|U| \equiv 3 \pmod{4} \). We assume that \( M(U, \tau) \) is a minimal counter example to Theorem 2, see Definition 1.7.

Lemma 5.1. Let \( V \) be a proper nontrivial root subgroup of \( U \), with \(|V| \equiv 3 \pmod{4} \), then \( G(V) \cong PSL_2(|V|) \).

Proof. Set \( \mathfrak{G} := G(V) \). Since \( U \) is abelian, Lemma 3.2(1) implies that \( \mathfrak{G} \) is a special rank one group. By [DST, Theorem 1(2)], either \( \mathfrak{G} \cong (P)SL_2(3) \) or \( \mathfrak{G} \) is perfect. By Lemma 3.2(3), \( \mathfrak{G}_V = Z(\mathfrak{G}) \), and by induction \( \mathfrak{G}_V^k \cong PSL_2(|V|) \). Since \( \mathfrak{G} \) contains non-central involutions, \( \mathfrak{G} \cong PSL_2(3) \), if \(|V| = 3 \). So suppose \(|V| > 3 \), then \( \mathfrak{G} \) is a perfect central extension of \( PSL_2(|V|) \). But the universal central extension of \( PSL_2(|V|) \) is \( SL_2(|V|) \) (cf. [Sc]). Since \( \mathfrak{G} \) contains non-central involutions, \( \mathfrak{G} \cong PSL_2(|V|) \).  
\[\square\]

Proposition 5.2. Let \( b \in U^* \). Then \( \mu_b \) has no fixed points on \( X \).

Proof. Assume that \( \alpha \mu_b = a \) for some \( a \in U^* \). Then, by Lemma 1.4(2), 
\[
(\mu_b \alpha)^2 = \mu_b \mu_a \mu_a = \mu_a^2 = 1,
\]
so \( h := \mu_b \mu_a \) is an involution.
Let \( V_+ := V_{h,1} \) and \( V_- := V_{h,-1} \) as in Notation 3.6 and set \( V := V_+ \), by Lemma 1.4(3iv), \( b \mu_a = b \), and this implies that
\[
a, b \in V_-.
\]
Assume that \( V \neq 0 \) and let
\[
X_\varepsilon := V_{\varepsilon} \cup \{\infty\}, \quad \mathfrak{G}_\varepsilon := G(V_{\varepsilon}), \quad \varepsilon \in \{+,-\}.
\]
Assume first that \( \mu_b \) has a fixed point \( c \in V^* \). Then also \( c \mu_a = c \). But then 
\[
\alpha \mu_c = a \quad \text{and} \quad \beta \mu_c = b, \quad \text{contradicting Proposition 4.1(4)}.
\]
Hence
\[
(5.1) \quad \mu_b \text{ has no fixed points on } V^*.
\]
Notice that (5.1) implies that
\[
(5.2) \quad x \mu_b \neq \pm x, \quad \text{and hence} \quad [\mu_b, \mu_x] \neq 1, \quad \text{for all } x \in V^*.
\]
Indeed, if \( x \mu_b = \pm x \), then, by (5.1), \( x \mu_b = -x \), so \( b = \pm x \), a contradiction.
Now, if \( [\mu_b, \mu_x] = 1 \), then \( \mu_{x \mu_b} = \mu_{x}^b \mu_x = \mu_x \), so \( x \mu_b = \pm x \), impossible.
Assume that $|V_-| \equiv 3 \pmod{4}$. Then, by Lemma 5.1 (and since $V_-$ is a root subgroup), $\mathfrak{S}_- \cong \text{PSL}_2(|V_-|)$. But $\mu_b$ fixes the point $a \in V_+$, which is impossible since the $\mu$-maps in the Moufang set $\mathbb{M}(|V_-|)$ have no fixed points. We conclude that

$$|V_-| \equiv 1 \pmod{4}. \tag{5.3}$$

By (5.3), $|V| \equiv 3 \pmod{4}$. Now by Lemma 3.5(2), $V^* \mu_b = V^*$, so $\mu_b$ acts on $A := \{v, -v\mid v \in V^*\}$. But since $|V| \equiv 3 \pmod{4}$, $|A| = \frac{|V|-1}{2}$ is odd, so there exists $v \in V$ such that $v \mu_b = \pm v$, contradicting (5.2).

Hence $V = 0$, i.e., $x \mu_a \mu_b = -x$, for all $x \in U^*$. Now by [DST, Theorem 1.11] $G$ is simple, so $\mu_b$ is an even permutation. Hence the number of fixed points of $\mu_b$ is $\geq 4$. Let $c \in U^*$ such that $c \neq \pm a$ and $c \mu_b = c$. Then, as above, $x \mu_c \mu_b = -x$, for all $x \in U^*$, so $\mu_c \mu_b = \mu_a \mu_b$ and hence $\mu_c = \mu_a$, contradiction Lemma 1.4(3ii). \hfill \Box

**Proposition 5.3.**

1. $|H|$ is odd;
2. $H$ is transitive on the set $\{\{a, -a\mid a \in U^*\}$.

**Proof.** We first claim that

$$|\mu_a \mu_b| \text{ is odd for } a, b \in U^* \text{ with } \mu_a \neq \mu_b, \tag{5.5}$$

else there would exists $h \in \langle \mu_a \mu_b \rangle$ satisfying: $\mu_a^h \notin \{\mu_a, \mu_b\}$ and $\mu_a^h$ commutes with either $\mu_a$ or $\mu_b$. But $\mu_a^h = \mu_{ah}$, and this contradicts (5.4).

Notice that by (5.4),

$$|\mu_a \mu_b| \text{ is odd for } a, b \in U^* \text{ with } \mu_a \neq \mu_b, \tag{5.5}$$

else there would exists $h \in \langle \mu_a \mu_b \rangle$ satisfying: $\mu_a^h \notin \{\mu_a, \mu_b\}$ and $\mu_a^h$ commutes with either $\mu_a$ or $\mu_b$. But $\mu_a^h = \mu_{ah}$, and this contradicts (5.4).

By (5.5)

$$\{\mu_a \mid a \in U^*\} \text{ is a conjugacy class of involutions in } N. \tag{5.6}$$

By (5.4) and (5.6), and by Glauberman’s $Z^*$-Theorem, $\mu_a \mu_b \in O_{2^e}(N)$, for all $a, b \in U^*$ and since $H = \langle \mu_a \mu_b \mid a, b \in U^* \rangle$ (see [DW, Theorem 3.1(ii)]), we see that $H \leq O_{2^e}(N)$ and so $|H|$ is odd.

Next, by (5.6), for $x, y \in U^*$, there exists $h \in H$, with $\mu_x h = \mu_y$. Hence, $xh = \pm y$, this shows (2). \hfill \Box

We are now in a position to prove Theorem 2.

**Proof of Theorem 2.** By 5.3(1), $|H|$ is odd, so, in particular, by the Feit-Thompson theorem $H$ is solvable. By Proposition 5.3(2),

$$|C_{O_r(H)}(e)| = |C_{O_r(H)}(f)|, \quad \text{for all primes } r \text{ and all } e, f \in U^*. \tag{5.7}$$
By (5.7) and [P2, Lemme, p. 281], $O_r(H)$ is cyclic, for all odd primes $r$ and hence

(5.8) \quad H \text{ is solvable and the Fitting group } F(H) \text{ is cyclic.}

Now by Proposition 5.3(2), $H$ acts irreducibly on $U$, so by (5.8),

(5.9) \quad C_U(h) = 0, \text{ for all } h \in F(H).

and this implies that

(5.10) \quad \text{for all } x \in U^*, C_{F(H)}(\mu_x) = 1

because if $[h, \mu_x] = 1$, for some $1 \neq h \in F(H)$, then, by Lemma 1.4(3iii), $xh = x$, contradicting (5.9).

But now (5.8) and (5.10) imply that $\mu_x$ inverts $F(H)$, for all $x \in U^*$. We thus see that

$$\mu_x \mu_y \in C_H(F(H)) \leq F(H),$$

for all $x, y \in U^*$, so since $H = \langle \mu_x \mu_y \mid x, y \in U^* \rangle$, we see that $H = F(H)$ is cyclic. By [DW, Thm. 6.1], $M(U, \tau) \cong M(|U|)$, a contradiction which proves Theorem 2. \hfill \Box

6. THE CASE WHEN $|U| \equiv 1 \pmod 4$

In this section $M(U, \tau)$ is a finite special Moufang set with $|U| \equiv 1 \pmod 4$. We assume that $M(U, \tau)$ is a minimal counter example to Theorem 3, see Definition 1.7.

**Lemma 6.1.** Let $V$ be a proper nontrivial root subgroup of $U$, then $G(V) \cong PSL_2(|V|)$.

**Proof.** Set $\mathfrak{G} := G(V)$. Since $U$ is abelian, Lemma 3.2(1) implies that $\mathfrak{G}$ is a special rank one group. By Lemma 3.2(3), $\mathfrak{G}_X = Z(\mathfrak{G})$, and by [DST, Theorem 1(2)], $\mathfrak{G}$ is perfect. Hence $\mathfrak{G}$ is a perfect central extension of $\mathfrak{G}_X$. By Theorem 2, or by induction, $\mathfrak{G}_X \cong PSL_2(|V|)$.

Suppose $|V| > 9$, then the universal central extension of $PSL_2(|V|)$ is $SL_2(|V|)$ (cf. [Sc]), and since $\mathfrak{G}$ contains non-central involutions, $\mathfrak{G} \cong PSL_2(|V|)$.

So suppose $|V| = 9$. Then the Schur multiplier of $PSL_2(9) \cong A_6$ is cyclic of order 6. Suppose that $\mathfrak{G} \not\cong PSL_2(9)$, then again, since $\mathfrak{G}$ contains involutions, $Z(\mathfrak{G}) \cong Z_3$. Let $P \in \text{Syl}_3(\mathfrak{G})$, then $|P| = 27$, and hence $P = V_3 \times Z(\mathfrak{G})$. In particular $P$ splits over $Z(\mathfrak{G})$, so by Gaschütz’ theorem, $\mathfrak{G}$ splits over $Z(\mathfrak{G})$, a contradiction. Thus $\mathfrak{G} \cong PSL_2(|V|)$ in this case as well. \hfill \Box

**Proposition 6.2.** Let $a, b \in U^*$ and assume that $a \mu_b = a$. Then

1. $\mu_a \mu_b = i$, where $xi = -x$, for all $x \in U^*$;
2. $\mu_b$ has exactly 2 fixed points.
Proof. By Lemma 1.4(2), $(\mu_a\mu_b)^2 = \mu_a\mu_{a\mu_b} = \mu_a^2 = 1$, so
\[ h := \mu_a\mu_b \] is an involution.

We now prove parts (1) and (2) together. Let $V_+ := V_{h,1}$ and $V_- := V_{h,-1}$ as in Notation 3.6 and set $V := V_+$. Since $b\mu_a = b$ we have:
\[ a, b \in V_. \]

Assume that $V \neq 0$ and let
\[ X_\varepsilon := V_\varepsilon \cup \{ \infty \}, \quad \text{and} \quad \mathfrak{G}_\varepsilon := G(V_\varepsilon), \quad \varepsilon \in \{ +, - \}. \]

Notice that (5.1), (5.2) and (5.3) hold here as well (the proof there applies to our case as well).

By (5.2),
\[ |V| \equiv 1 \pmod{4}. \]

Since $V_\varepsilon$ is a root subgroup of $U$, Lemma 6.1 implies that
\[ \mathfrak{G}_\varepsilon \cong \text{PSL}_2(|V_\varepsilon|). \]

Pick
\[ c \in V^*. \]

We define $\iota_\varepsilon$ as follows:
\[ \iota_\varepsilon \text{ is the unique element in } H(V_\varepsilon) \text{ satisfying } x\iota_\varepsilon = -x, \text{ for all } x \in V_\varepsilon^*. \]

From the structure of $\mathfrak{G}_\varepsilon \cong \text{PSL}_2(|V_\varepsilon|)$ it follows that for $x, y \in V_\varepsilon^*$, with $x\mu_y = x$, we have $\mu_x\mu_y = \iota_\varepsilon$. Notice also that if for $x, y \in V_\varepsilon^*$, $\mu_x\mu_y = \iota_\varepsilon$, then $x\mu_y = x$. Finally note that by the structure of $\mathfrak{G}_\varepsilon$, if $x, y \in V_\varepsilon^*$ and $|\mu_x\mu_y|$ is even, then the center of the dihedral group $\langle \mu_x, \mu_y \rangle$ is $\iota_\varepsilon$. Consider the dihedral group
\[ D := \langle \mu_b, \iota_\varepsilon \rangle \text{ and set } g := \mu_b\mu_c. \]

Assume first that $|g|$ is odd. Then some power $g^k$ of $g$ conjugates $\mu_c$ to $\mu_b$. Thus $\mu_b = \mu_c^g = \mu_{c^g}$, and $c^g = \pm b$. Since $V^*g = V^*$ (Lemma 3.5(2)), we get that $b \in V$, a contradiction.

Assume $|g| = 2m$ with $m$ odd. Then some power $g^k$ of $g$ will conjugate $\mu_c$ to an element of $D$ commuting with $\mu_b$. Thus $x := cg^k \in V$ has the property that $|\mu_b, \mu_x| = 1$, contradicting (5.2).

Hence we may conclude that $|g|$ is divisible by 4. Observe now that by Lemma 3.5(2) and Lemma 3.3(2), $\mu_b$ normalizes $\mathfrak{G}_+$ and $\mu_c$ normalizes $\mathfrak{G}_-$, so $g^2 \in \mathfrak{G}_+ \cap \mathfrak{G}_-$. Let $\langle t \rangle$ be the center of $D$. Then $\langle t \rangle$ is the center of $\langle \mu_c, g^2 \rangle \leq \mathfrak{G}_+$ and the center of $\langle \mu_b, g^2 \rangle \leq \mathfrak{G}_-$, so $t = \iota_+ = \iota_-$. It follows that $xt = -x$, for all $x \in U^*$. Also $t = \iota_- = \mu_a\mu_b$ and (1) is proved.

To complete the proof of (2), we show that $\mu_b$ has at most two fixed points. Then, since $\mu_b$ is an even permutation (because $G$ is a simple group; see [DST, Theorem 1.11]), the proposition will follow. Let $u, v \in U^*$ be fixed points of $\mu_b$. By (1) $x\mu_u\mu_b = -x = x\mu_v\mu_b$, for all $x \in U^*$, so $\mu_u = \mu_v$, and $v = \pm u$. \qed
Lemma 6.3. (1) All involutions in $G$ fix exactly 2 points; 
(2) $i$ is the unique involution in $H$, so all involutions in $G$ are conjugate; 
(3) if $t \in \text{Inv}(N) \setminus \{i\}$, then $t = \mu_x$ for some $x \in U^*$; 
(4) let $S \in \text{Syl}_2(N)$ and set $T := S \cap H \in \text{Syl}_2(H)$. Then $T$ is either cyclic or quaternion and $S$ is either dihedral or semidihedral.

Proof. (1): We observe that the arguments in section 6 (pg. 448–452) of [HKSe] apply here. Indeed, it is easy to check that for an involution $t \in H$ that fixes more than 2 points, if $V := C_U(t)$, then $G(V) = C_0(t)$, where $C_0(t)$ is as in [HKSe, p. 442].

(2): By (1), any involution in $H$ inverts $U$ so must be equal to $i$. Then the second part of (2) is an immediate consequence of the first.

(3): Let $t \in \text{Inv}(N) \setminus \{i\}$. Let $y, -y$ be the fixed points of $t$. Let $x \in U^*$, with $x \mu_y = x$. Then, by Lemma 1.4(3iv), $y, -y$ are the fixed points of $\mu_x$. By (1) there is a unique involution in $G_{y, -y}$, so $t = \mu_x$.

(4): By (1) and [G, Thm. 4.10(2)], $T$ is cyclic or quaternion. We claim that

\begin{equation}
(6.2) \quad \text{if } \mu_x \in S, \text{ then } C_S(\mu_x) = (\mu_x, i).
\end{equation}

Let $\eta \in C_S(\mu_x)$. By Lemma 1.4(3iii), $x\eta^2 = x$, but by (1), $xg \neq x$, for all $x \in U^*$ and $g \in T^*$. Thus $\eta^2 = 1$. Hence $C_S(\mu_x)$ is elementary abelian and since $C_S(\mu_x) = \mu_x \times C_T(\mu_x)$, (6.2) follows. By a result of Suzuki $S$ is dihedral or semidihedral (cf. [A, Exercise 8.6, p. 116]).

Proposition 6.4. Let $S \in \text{Syl}_2(N)$. If $S$ is dihedral then $\mathfrak{M}(U, \tau) \cong \mathfrak{M}(|U|)$.

Proof. If $S$ is dihedral, then by Lemma 6.3(2), $S \cap H$ is cyclic. Thus $H = O(H)(S \cap H)$ and by the Feit-Thompson theorem $H$ is solvable.

We claim that

\begin{equation}
(6.3) \quad H \text{ has two orbits on } U^*.
\end{equation}

Let $A \subseteq U^*$ such that $a \in A$ if and only if $-a \in A$. We claim that $\{\mu_x \mid x \in A\}$ is a conjugacy class of involutions in $N$ iff $A$ is an orbit of $H$ on $U^*$. Indeed, for $x, y \in U^*$, there exists $h \in H$ with $\mu_y = \mu_x^h = \mu_{xh}$ iff $y = \pm xh$. Since $x \tau = -x$, the claim follows. Since $S$ is dihedral, it has two classes of noncentral involutions distinct from $i$, so clearly $N$ has two classes of involutions and (6.3) holds.

Recall that by [SW, Theorem 1.2],

\begin{equation}
(6.4) \quad H \text{ acts irreducibly on } U.
\end{equation}

Our next step is to show that

\begin{equation}
(6.5) \quad \text{if } A \text{ is an abelian normal } p\text{-subgroup of } N, \text{ then } A \text{ is cyclic}.
\end{equation}
Suppose $A$ is an abelian normal $p$-subgroup, of $N$ such that $A$ is not cyclic. Replacing $A$ with $\Omega_1(A)$ we may assume that $A$ is elementary abelian. By (6.4), $C_U(A) = 0$. Let

$$\mathcal{B} := \{ B \leq A \mid [A : B] = p \text{ and } U_B := C_U(B) \neq 0 \}.$$ 

We claim that $U$ is a direct sum, $U = \bigoplus_{B \in \mathcal{B}} U_B$. The argument here is very similar to the proof of (1.2). First, by [A, Exercise 8.1, p. 115], $U = \sum_{B \in \mathcal{B}} U_B$. Suppose $U_{B_1} \oplus \cdots \oplus U_{B_{k-1}}$ is a direct sum and let $u_k \in U_{B_k} \cap \sum_{i=1}^{k-1} U_{B_i}$. Write

$$u_k = u_1 + \cdots + u_{k-1}, \quad u_i \in U_{B_i}.$$ 

Since $U_{B_i}$ is $a$-invariant, for all $a \in A$, we get for $b \in B_k$ that

$$u_1 + \cdots + u_{k-1} = u_k = u_kb = u_1b + \cdots + u_{k-1}b,$$

so $b$ fixes $u_i$, for all $i \in [1, k-1]$, and then $u_i$ is centralized by $\langle B_i, B_k \rangle = A$, so $u_i = 0$ and it follows that $u_k = 0$.

Notice now that $N$ acts on $\{ B^* \mid B \in \mathcal{B} \}$. Let $\pi_B : U \to U_B$ be the projection map, $B \in \mathcal{B}$. Suppose $|\mathcal{B}| > 2$. Then $H$ will have at least 3 orbits on $U^*$ according to $|\{ B \in \mathcal{B} \mid \pi_B(u) \neq 0 \}|$, a contradiction.

Of course $|\mathcal{B}| \neq 1$. Hence $\mathcal{B} = \{ B_1, B_2 \}$ is of size 2. Let $z \in U^*$; since $N$ acts on $\mathcal{B}$, $\mu_z$ acts on $\{ U_{B_1}^*, U_{B_2}^* \}$. By Lemma 3.4(3), for $i = 1, 2$, $U_{B_i}$ is a root subgroup of $U$, so $U_{B_i}^* \mu_z = U_{B_i}^*$, for $z \in U_{B_i}^*$, and by the above, $\mu_z$ fixes both $U_{B_1}^*$ and $U_{B_2}^*$. Let $x \in U_{B_1}^*$ and let $y \in U_{B_2}^*$, with $x\mu_y \neq x$ (i.e. by Lemma 1.4(3iv), $y$ is not one of the two fixed points of $\mu_z$). Then

$$x\mu_{x+y} = -x + x\mu_y - y \cdot 2,$$

by [DS1, Lemma 4.4(3)]. Now $-x + x\mu_y \in U_{B_1}^*$ and $-y \cdot 2 \in U_{B_2}^*$. However we just saw that $x\mu_{x+y} \in U_{B_1}^* \cup U_{B_2}^*$, a contradiction. This shows (6.5).

We can now show that

(6.6) $O_p(H)$ is cyclic for all primes $p$.

If $p = 2$, then this is because $S \cap H$ is cyclic. So suppose $p$ is odd. Let $P := O_p(H)$ and assume $P \neq 1$. We claim that $P$ and $U$ (in place of $E$) satisfy all the hypotheses of Lemma 1.6. Let $C \leq P$ be a characteristic subgroup. Then $Z(C)$ is an abelian normal subgroup of $N$, so by (6.5), $Z(C)$ is cyclic and so by (6.4) $C_U(z) = 0$, for all $0 \neq z \in Z(C)$. Hence hypothesis (i) of Lemma 1.6 holds. Hypothesis (iii) is immediate from (6.3).

Assume there exists $x \in U^*$ with $C_C(x) = 0$, then, by Lemma 1.4(3iii), since $|C|$ is odd $C_C(\mu_x) = 1$. Hence $C$ is abelian (and $\mu_x$ inverts $C$). This shows the last hypothesis (ii) of Lemma 1.6 and proves (6.6).

By (6.6), $F(H)$ is cyclic. From (6.4) it follows that $C_U(g) = 0$, for all $1 \neq g \in F(H)$. By Lemma 1.4(3iii) it follows that $C_{F(H)}(\mu_x) = \langle e \rangle$, for $x \in U^*$. This together with the fact that the 2-Sylow groups of $N$ are dihedral imply that $\mu_x$ inverts $F(H)$. We thus see that

$$\mu_x\mu_y \in C_H(F(H)) \leq F(H),$$
for all \( x, y \in U^\ast \), so since \( H = \langle \mu_x \mu_y \mid x, y \in U^\ast \rangle \) (by [DW, Theorem 3.1(ii)]), we see that \( H = F(H) \) is cyclic. Applying [DW, Theorem 6.1] we get that \( \mathcal{M}(U, \tau) \cong \mathcal{M}(|U|) \), which completes the proof of Proposition 6.4. \( \square \)

The following lemma is the only weak link in the proof of Theorem 3. Unfortunately we were not able to find a simple proof to the following, so we have to refer to [H]. We purposely phrase Proposition 6.5 below so that the reader will see what needs to be shown.

**Proposition 6.5.** Let \( S \in \text{Syl}_2(N) \), then

1. if \( S \) is semidihedral, then \( G \) is triply transitive;
2. \( S \) is dihedral.

**Proof.** Assume that \( S \) is semidihedral. Since semidihedral groups are transitive on their noncentral involutions, and since \( xi = -x \), Lemma 1.4(2) implies that \( H \) is transitive on \( U^\ast \), so (1) holds.

By [H, (3), p. 165], \( H \) is solvable, and by [H, (4), p. 171], if \( H \) is solvable, then \( G \) contains a subgroup of index 1 or 2 with a dihedral 2-Sylow subgroup. But by [DST, Theorem 1(2)], \( G \) is simple, a contradiction. Hence \( S \) is not semidihedral, so by Lemma 6.3(4), \( S \) is dihedral. \( \square \)

Notice that Propositions 6.2(2), 6.3(1& 4), 6.4 and 6.5(2) prove Theorem 3.

**References**


YOAV SEGEV, DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY, BEER-SHEVA 84105, ISRAEL

E-mail address: yoavs@math.bgu.ac.il