Toward the abelian root groups conjecture for special Moufang sets

Yoav Segev

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

Received 25 July 2009; accepted 5 October 2009
Available online 14 October 2009
Communicated by the Managing Editors of AIM

Abstract

We prove that if a root group of a special Moufang set contains an element of order \( p \equiv 1 \pmod{4} \) then it is abelian.

© 2009 Elsevier Inc. All rights reserved.

MSC: primary 20E42; secondary 17C60

Keywords: Moufang set; Root group

1. Introduction

Moufang sets were introduced by J. Tits [11] as a tool for studying algebraic groups of relative rank one. They are essentially equivalent to split BN-pairs of rank one, and to Timmesfeld’s abstract rank one groups (see [10]).

Let us recall that a Moufang set is a doubly transitive permutation group such that the point stabilizer contains a normal subgroup which is regular on the remaining points. These regular normal subgroups are called the root groups and they are assumed to be conjugate and to generate the whole group. In [1,2,4] the notation \( M(U, \tau) \) is used for a Moufang set (and this notation is of course explained there). The group \( U \) in this notation is isomorphic to any one of the root groups of the Moufang set. Note that as in the references cited above, we use additive notation for \( U \), though \( U \) is not assumed to be abelian.
Recall that $\mathbb{M}(U, \tau)$ is special iff, $(-a)\tau = -(a\tau)$, for all $a \in U^* := U \setminus \{0\}$. This paper makes a contribution to the following conjecture.

**Abelian root groups conjecture.** Let $\mathbb{M}(U, \tau)$ be a special Moufang set. Then $U$ is abelian.

Thus the conjecture asserts that special Moufang sets have abelian root groups. In [8] we proved the converse: that proper (i.e. not sharply 2-transitive) Moufang sets with abelian root groups are special. We prove

**Theorem A.** Let $\mathbb{M}(U, \tau)$ be a special Moufang set. Suppose there exists $a \in U^*$ whose order is $p \equiv 1 \pmod{4}$. Then $U$ is abelian.

In [3, Section 5] it is shown that if $U^*$ contains involutions (i.e. elements of order 2), then $U$ is a group of exponent 2 (and hence abelian). Thus since $a \in U^*$ has order $p \equiv 1 \pmod{4}$, [1, Proposition 4.6] implies that $U$ is a uniquely 2-divisible group. Section 2 deals with such groups, in fact what we need is information on regular automorphisms of order 2 and 4 of such groups. Several of the results of Section 2 are taken from [6], but we add a little more.

2. Regular automorphisms of order 4 acting on uniquely 2-divisible groups

In this section $U$ is a uniquely 2-divisible group. This means that each element in $U$ has a unique square root. We use additive notation for $U$ although we do not assume that $U$ is abelian.

The unique square root of an element $x \in U^* := U \setminus \{0\}$ is thus denoted $x \cdot \frac{1}{2}$. Also, for $n \in \mathbb{Z}$ we write $x \cdot n$ for the $n$th power of $x$. We will use the usual notation $x^3 = -y + x + y$ and $[x, y] = -x - y + x + y$. Notice however that $x^{-y}$ denotes $y + x - y$ and not $-y + x + y = (-x)^3$.

Here are a few more words of caution. Notice that 0 is the neutral element of $U$, so for $x, y \in U^*$, $[x, y] = 0$ indicates that $x$ and $y$ commute, and that the conjugation $u^0 = u$, for $u \in U$ (of course $u \cdot 0 = 0$).

We let $\eta \in \text{Aut}(U)$ be a regular automorphism of order 4. Regular means that the implication $y\eta = y \Rightarrow y = 0$ holds for all $y \in U$ (i.e. $\eta$ is a fixed point free automorphism). Notice though that our assertions in this section with regards to automorphisms of order 2, as well as Proposition 2.3(1), do not rely on the existence of $\eta$. For any automorphism $\nu$ of $U$ of order 2 we let

$$T_\nu := C_U(\nu) \quad \text{and} \quad S_\nu := \{x \in U \mid x\nu = -x\}.$$ 

We let $S_\nu^0 := S_\nu \setminus \{0\},$

$$T := T_\eta^2 \quad \text{and} \quad S := S_\eta^2.$$ 

The following lemma comes from [6, (3.3) and (3.4), p. 281].

**Lemma 2.1.** Let $\nu \in \text{Aut}(U)$ have order 2. Then

1. each element $x \in U$ can be written uniquely as a sum $x = t + s$, with $t \in T_\nu$ and $s \in S_\nu$; in particular,
2. each element of $U$ can be written uniquely as a sum $x = t + s$, with $t \in T$ and $s \in S$;
if \( \nu \) is regular, then \( \nu \) inverts \( U \) so \( U \) is abelian; thus,

(4) \( T \) is abelian and \( \eta \) inverts \( T \) (i.e. \( t\eta = -t \), for all \( t \in T \)).

**Proof.** (1) Let \( x \in U^* \) and suppose \( x = t + s \), with \( t \in T_\nu \) and \( s \in S_\nu \). Then

\[
x + (-x + x\nu) \cdot \frac{1}{2} = (t + s) + (-s - t + t - s) \cdot \frac{1}{2} = t + s - s = t,
\]

so \( t \) is uniquely determined by \( x \) and then \( s = -t + x \) is also uniquely determined by \( x \).

Let now \( x \in U^* \) be arbitrary. Then

\[
(x + (-x + x\nu) \cdot \frac{1}{2})\nu = x\nu + (-x\nu + x) \cdot \frac{1}{2} = x - (-x\nu + x) + (-x\nu + x) \cdot \frac{1}{2} = x - (-x\nu + x) \cdot \frac{1}{2} = x + (-x + x\nu) \cdot \frac{1}{2}.
\]

Hence \( t := x + (-x + x\nu) \cdot \frac{1}{2} \in T \) and \( s = -t + x = (-x\nu + x) \cdot \frac{1}{2} \in S \).

(2) This follows from (1) applied to \( \eta^2 \).

(3) Since \( \nu \) is regular, this means that \( T_\nu = 0 \), so by (1), \( U = S_\nu \), and (3) holds.

(4) Note that \( T \) is uniquely 2-divisible, and that the restriction of \( \eta \) to \( T \) is a regular automorphism of \( T \) of order 2, so (4) follows from (3). \( \Box \)

**Lemma 2.2.** (See (3.5) in [6], p. 281.)

(1) If \( \nu \in \text{Aut}(U) \) has order 2, then \( s^t \in S_\nu \), for all \( t \in T_\nu \) and \( s \in S_\nu \);

(2) \( \langle S \rangle \) is a normal subgroup of \( U \) and \( U/\langle S \rangle \) is abelian.

**Proof.** (1) Let \( t \in T_\nu \) and \( s \in S_\nu \), then \( (s^t)^\nu = (sv)^t = (-s)^t = -(s^t) \), and (1) holds.

(2) Set \( N := \langle S \rangle \). By Lemma 2.1(2), \( U = T + N \). By (1), \( T \) normalizes \( N \), so \( N \trianglelefteq U \). Then, since by Lemma 2.1(4) \( T \) is abelian, \( U/N \) is abelian. \( \Box \)

The following proposition generalizes some of the results in [6, (5.1), p. 287].

**Proposition 2.3.**

(1) Let \( \nu \) be any regular automorphism of \( U \). Suppose \( x, y \in U \) satisfy: \( x\nu = x^{(-y+y\nu)} \). Then \( x = 0 \).

(2) Let \( y \in U^* \). Using Lemma 2.1(2), write \( -y + y\eta = -t - s \) with \( t \in T \) and \( s \in S \). Then \( [s^t, s\eta] = 0 \).

(3) Let \( s \in S \). Then \( [s, s\eta] = 0 \).

(4) Let \( t \in T \) and \( s \in S \). Then \( [s^t, s\eta] = 0 \).

**Proof.** (1) We have \( (x^{-y})\nu = x^{-y} \), so since \( \nu \) is regular it follows that \( x^{-y} = 0 \) and then also \( x = 0 \).

(2) By Lemma 2.1(4) we have

\[
[s^t, s\eta] \eta = [(s\eta)^{-t}, -s] = [s, (s\eta)^{-t}]^{-s} = [s^t, s\eta]^{-t-s} = [s^t, s\eta]^{(-y+y\eta)},
\]
so (2) follows from (1) with \( \eta \) in place of \( v \) and \( [s^t, s\eta] \) in place of \( x \).

(3) Set \( x := -s + s\eta \), and write \( x = -t - u \) with \( t \in T \) and \( u \in S \). By (2), \([u^t, u\eta] = 0\) . Now \( x + x\eta = -t - u + t - (u\eta) \), so \( x + x\eta \) commutes with \( u\eta \). But \( x + x\eta = (-s + s\eta) + (s\eta) - s = -s \cdot 2 \). Hence \( u\eta \) commutes with \( s \cdot 2 \), and since \( U \) is uniquely 2-divisible, \( u\eta \) commutes with \( s \). Thus \( -u = (u\eta)\eta \) commutes with \( s\eta \), and we see that \( u \) commutes with \( s\eta \).

Now \( -t = x + u = -s + (s\eta + u) \). Notice that since \( s\eta \) and \( u \) commute, \( s\eta + u \in S \). Set \( v := s\eta + u \). Then \(-t = -s + v \) and hence

\[-s + v = -t = -(t)\eta^2 = s - v.\]

It follows that \(-s \cdot 2 = -v \cdot 2 \), so by unique 2-divisibility, \( s = v \) and \( t = 0 \). It follows that \(-s + s\eta = -u \) and since \([u, s\eta] = 0\) we see that \([s, s\eta] = 0\).

(4) Let \( t \in T \) and \( s \in S \). By Lemma 2.2(1), \( s^t \in S \). By (3), \((s^t)\eta \) commutes with \( s^t \). But \((s^t)\eta = (s\eta)^{-t} \), so we see that \([s^t, s\eta] = 0\), replacing \( t \) with \( t \cdot \frac{1}{2} \), we get (4). \( \square \)

3. The proof of Theorem A

Throughout this section \( p \) is a prime such that \( p \equiv 1 \pmod{4} \). We let \( \mathbb{M}(U, \tau) \) be a special Moufang set and we assume that \( a \in U^* \) is an element of order \( p \). By [3, Section 5] and [1, Proposition 4.6], \( U \) is a uniquely 2-divisible group. Our goal is to show that \( U \) is abelian. So assume toward contradiction that \( U \) is not abelian.

We now briefly recall several facts about special Moufang sets. We always denote \( X := U \cup \{\infty\} \) and by \( G \) the little projective group of \( \mathbb{M}(U, \tau) \). The letter \( H \) is reserved for \( H := G_{0, \infty} \), and recall that \( H \leq \text{Aut}(U) \). Recall from [1, Proposition 3.9] that for all \( x, y \in U^* \) and \( h \in H \),

\[\mu_x^h = \mu_{xh}, \quad \mu_x^{\mu_y} = \mu_{-x\mu_y}, \quad \mu_{-x} = \mu_x^{-1} \quad \text{and} \quad x\mu_x = -x. \quad (3.1)\]

Here are some useful properties of \( U \). By [1, Proposition 4.6] for every element \( x \in U^* \) either \( |x| = q \), where \( q \) is an odd prime which depends on \( x \), or \( |x| = \infty \), where \( |x| \) is the order of \( x \).

Furthermore, by [3, Proposition 5.3], \( C_U(x) \) is a group of exponent \( q \) in the first case and \( C_U(x) \) is a uniquely divisible torsion free group in the second case. In particular, if \( C_U(x) \) is abelian, then \( C_U(x) \) is a vector space over \( \mathbb{F}_q \) or \( \mathbb{Q} \) respectively.

We use the following observation which follows from [1, Proposition 4.10]:

\[\mu_x^2 = \mu_{x^{-m}}, \quad \forall x \in U^* \text{ with } |x| < \infty \text{ and all } 1 \leq m < |x|. \quad (3.2)\]

Indeed let \( |x| = q \) and in [1, Proposition 4.10(3)] take \( k \) to be a generator of the multiplicative group \( \mathbb{F}_q^* \). Then \( k \) is a nonsquare in \( \mathbb{F}_q^* \). Now in the notation of [1, Proposition 4.10(3)], take \( \ell \) such that \( k^\ell = -1 \) (in \( \mathbb{F}_q^* \)) and take \( \ell' = 0 \), so that \( N = -1 \). Then parts (3) and (5) of [1, Proposition 4.10] show that \( \mu_q^2 = \mu_{-a} = \mu_{a,k}^2 \) and [1, Proposition 4.10(4)] shows that \( \mu_{a^2}^2 = \mu_{a^{2,2}}^2 = \mu_{a,k}^2 \), for all \( t \in \mathbb{F}_q^* \), so (3.2) holds.

**Notation 3.1.** Let \( x \in U^* \). We denote

1. \( \sqrt{-1} \) is an element of the field \( \mathbb{F}_p = \{0, \ldots, p - 1\} \) whose square is \(-1\).
2. \( T_x := C_U(\mu_x^2) \).
3. \( S_x := \{y \in U \mid y\mu_x^2 = -y\} \).
If \(|x|=p\) we denote \(\eta_x = \mu_x \mu_{x, \sqrt{-1}}\).

We also let

\[
T := T_a, \quad S := S_a \quad \text{and} \quad \eta = \eta_a.
\]

The notion of a root subgroup which appears in the next lemma can be found in [7, Section 3].

**Lemma 3.2.** Let \(x \in U^* \) with \(|x|=p\). Then

1. If \(\mu_x^2 = 1\) then \(U\) is abelian, so \(\mu_x\) has order 4;
2. \(T_x\) is a root subgroup of \(U\) and \(T_x\) is an elementary abelian (possibly infinite) \(p\)-subgroup of \(U\).

**Proof.**

1. Note that given distinct \(y,z \in U^*\), the permutation action of \(G_{y,z}\) on \(X \setminus \{z\}\) is equivalent to the action of \(G_{y,z}\) on \(U_y\) via conjugation.

By [3, Proposition 7.7(4)] the only fixed points of \(\mu_x\) on \(X = U \cup \{\infty\}\) are \(x \cdot \sqrt{-1}, -x \cdot \sqrt{-1}\), and thus applying the above on \(y = x \cdot \sqrt{-1}, z = -x \cdot \sqrt{-1}\) we see that \(C_{U_y}(\mu_x) = 1\). Now \(U_y\) is a uniquely 2-divisible group. Hence if \(\mu_x^2 = 1\), then, by Lemma 2.1(3) (with \(U_y\) in place of \(U\) and conjugation by \(\mu_x\) in place of \(\nu\), \(U_y\) is abelian, and then \(U\) is abelian. Since we are assuming that \(U\) is not abelian, \(\mu_x^2 \neq 1\). By [1, Proposition 4.10(5)], \(\mu_x^4 = 1\), so (1) holds.

2. Since \(C_U(h)\) is a root subgroup for all \(h \in H\) (see [3, Corollary 1.9(1)]), it follows in particular that \(T_x = C_U(\mu_x^2)\) is a root subgroup. Now the restriction of \(\mu_x\) to \(T_x \cup \{\infty\}\) is the \(\mu\)-map corresponding to \(x\) in \(M(T_x, \mu_x)\) and since the square of this restriction is trivial, part (1) applied to \(M(T_x, \mu_x)\) shows that \(T_x\) is abelian. Then, since \(C_U(x)\) is a group of exponent \(p\), part (2) holds.

**Lemma 3.3.** Let \(x, y \in U^* \) with \(|x|=p = |y|\). Then

1. \(\eta_x^2 = \mu_x^2\);
2. \(z \eta_x = -z\), for all \(z \in T_x\);  
3. \(\eta_x \in \text{Aut}(U)\) is a regular automorphism of order 4;
4. If \(y \in T_x\), then \(T_x = T_y\). In particular either \(T_x = T_y\) or \(T_x \cap T_y = 0\).

**Proof.**

1. We have

\[
\eta_x^2 = (\mu_x \mu_{x, \sqrt{-1}})(\mu_x \mu_{x, \sqrt{-1}}) = \mu_x^2 (\mu_{-x} \mu_{x, \sqrt{-1}} \mu_x) \mu_{x, \sqrt{-1}}
\]

\[
= \mu_x^2 \mu_{-(x, \sqrt{-1})) \mu_x} \mu_{x, \sqrt{-1}} = \mu_x^2 \mu_{-x, \sqrt{-1}} \mu_{x, \sqrt{-1}} = \mu_x^2,
\]

where we have used again the fact that \((x \cdot \sqrt{-1}) \mu_x = x \cdot \sqrt{-1}\).

2. Note first that (by (1)) \(\eta_x\) acts on \(T_x\). By Lemma 3.2(2), \(T_x\) is an abelian root subgroup of \(U\), so by [1, Proposition 4.6(6)], \(z \mu_{x, \sqrt{-1}} = -z \mu_x\), for all \(z \in T_x\). Let \(z \in T_x\), then \(z \eta_x = z \mu_x \mu_{x, \sqrt{-1}} = -(z \mu_x^2) = -z\).

3. Suppose that \(z \eta_x = z\), for some \(z \in U^*\). Then \(z \mu_x^2 = z \eta_x^2 = z\). But then \(z \in T_x\), so by (2), \(z \eta_x = -z\), a contradiction.
(4) Suppose that $y \in T_x$. Since $T_x$ is an abelian root subgroup of $U$, [1, Lemma 5.1] implies that the restriction of $\mu_2^2$ to $T_x$ is trivial, that is, $T_x \leq T_y$. By symmetry (since $x \in T_x$, $T_y \leq T_x$, so $T_x = T_y$. □

Notice that by Lemma 3.3(1), using the notation of Section 2, we have

$T = T_{\eta^2}$ and $S = S_{\eta^2}$.

We can now conclude that

**Lemma 3.4.**

(1) $\eta \in \text{Aut}(U)$ is a regular automorphism of order 4;
(2) each element $x \in U^*$ can be written uniquely in the form $x = t + s$, with $t \in T$ and $s \in S$;
(3) $U = \langle S \rangle$.

**Proof.** Part (1) follows from Lemma 3.3(3). Part (2) follows from Lemma 2.1(2). By [9], $U$ is characteristically simple, so in particular $[U, U] = U$. Hence part (3) follows from Lemma 2.2(2). □

**Proposition 3.5.** Let $s \in S^*$. Suppose that $|s| \neq p$, then

(1) $C_U(s)$ is abelian, so $C_U(s)$ is a vector space, and $C_U(s)$ is inverted by $\mu_2^a$.
(2) $C_U(s) = C_U(x)$ for all $x \in C_U(s)^*$.
(3) $T$ normalizes $C_U(s)$.

**Proof.** (1) Since $s\mu_2^a = -s$, it follows that $\mu_2^a$ acts on $C_U(s)$. Notice that $C_U(s)$ is a uniquely 2-divisible group. We show that $CC_{C_U(s)}(\mu_2^a) = 0$, then by Lemma 2.1(3) part (1) will hold. Let $0 \neq x \in CC_{C_U(s)}(\mu_2^a)$, then $x \in T$, so $|x| = p$ and $x \in C_U(s)$, so $|x| = |s|$, a contradiction.

(2) Let $x \in C_U(s)$. Then by (1), $x \in S$ and since $|x| = |s|$ we can apply (1) with $x$ in place of $s$ to get that $C_U(x)$ is abelian. Hence (2) follows.

(3) Set $W := C_U(s)$, and let $x \in U^*$. Notice that if $W \cap W^x \neq 0$, then $W = W^x$, because by (2), for $0 \neq y \in W \cap W^x$ we have $W = C_U(y) = W^x$.

Let $t \in T$. By Proposition 2.3(3), $s \eta$ commutes with $s$, so $s \eta \in W$. By 2.3(4), $[s^t, s \eta] = 0$, so by (2) $s^t \in W$. It follows that $W \cap W^t \neq 0$, and hence $W^t = W$. □

**Lemma 3.6.** Let $s \in S$ such that $|s| = p$. Then

(1) $\mu_2^a$ commutes with $\mu_2^a$.
(2) $\mu_2^a$ inverts $T_s$ and $\mu_2^s$ inverts $T$.
(3) $\eta$ centralizes $\mu_2^a$, so $T_s \eta = T_s$.
(4) If $T_s = (s)$, then $s \eta = s \cdot i$, for some $i \in \{\sqrt{-1}, -\sqrt{-1}\}$.

**Proof.** (1) We have $(\mu_2^2)\mu_2^a = \mu_2^2 \mu_2^a = \mu_2^{\mu_2^2} = \mu_2^a$, where the last equality holds by Lemma 3.2(1).

(2) By (1) $\mu_2^a$ acts on $T_s$. Now $T_s \neq T$, because $s \in T_s \setminus T$. Hence, by Lemma 3.3(4), $T \cap T_s = 0$. Thus $\mu_2^a$ is a regular automorphism of $T_s$ of order 2, so $\mu_2^a$ inverts $T_s$. Further, by (1), $\mu_2^a$ acts on $T$ so the same argument shows that $\mu_2^a$ inverts $T$. 


(3) We have

\[ \eta^2 = (\mu a \mu a \sqrt{-1})^2 = \mu a \mu a (a \sqrt{-1}) \mu a^2 \]

\[ \equiv \mu - a \mu a \sqrt{-1} (\ast) = \mu a \mu a \sqrt{-1} = \eta, \]

where \((\ast)\) holds since \(\mu^2 = \mu a \sqrt{-1}\) (see Eq. (3.2)).

(4) By (3) \(\eta\) acts on \(T_a\) and since \(\eta\) has no fixed points on \(T_a\), \(s\eta \neq s\). Also \(s\eta \neq -s\), because \(s\eta^2 = s\mu^2 = -s\). Since \(\eta\) has order 4, part (4) holds. \(\square\)

**Proposition 3.7.**

1. Let \(s \in S\) and assume that \(|s| = p\) and that \(T_a = \langle a \rangle\) and \(T_s = \langle s \rangle\). Then \([a, s]\) commutes with \([a, s]\).

2. Assume that for all \(x \in U^*\) of order \(p\), \(T_x = \langle x \rangle\). Then for all \(y \in U^*,\) either \(y \in S,\) or \(|y| = p\).

3. Assume that for all \(x \in U^*\) with \(|x| = p\) we have \(T_x = \langle x \rangle\). Then \(U\) is a \(p\)-group.

4. Assume that for all \(x \in U^*\) with \(|x| = p\) we have \(T_x = \langle x \rangle\). Then \(U\) is abelian.

**Proof.** (1) By Lemma 3.6(4), \(s\eta = s \cdot i\), for some \(i \in \{\sqrt{-1}, -\sqrt{-1}\}\), and by Proposition 2.3(4), \(s\eta\) commutes with \(s^a\) and we see that \([s^a, s] = 0\). Hence \([s, a]\) commutes with \(s\). By symmetry, using Lemma 3.6(2), \([s, a]\) commutes with \(a\).

(2) Let \(y \in U^*\) and suppose that \(y \notin S\). Using Lemma 3.4(2) and the fact that \(T = \langle a \rangle\), we have \(y = a \cdot m + s,\) with \(s \in S\). Assume first that \(|s| = p\). Then, by (1), \([a, s]\) commutes with \(y\). Now if \([a, s] = 0\), then clearly \(|y| = |a|\), while otherwise \(|a| = ||a, s|| = |y|\). In either case \(|y| = p\).

So assume that \(|s| \neq p\). Then, by Proposition 3.5(3), \(a\) normalizes \(C_U(s)\), so in particular \(y \cdot p \in C_U(s)\). But by Proposition 3.5(1), \(\mu^2\) inverts \(C_U(s)\), so \(\mu^2\) inverts \(y \cdot p\). But if \(y \cdot p \neq 0\) then by [1, Proposition 4.6(1)], \(y \in S\). Since we are assuming that \(y \notin S\), we conclude that \(y \cdot p = 0\).

(3) Assume there exists \(y \in U^*\) with \(|y| \neq p\). Then, by (2), \(y \in S\). Let \(s \in S\). Since \(|y^a| = |y|\) we can apply (2) again to conclude that \(y^a \in S\), so

\[ s - y - s = (-s + y + s)\mu^2 = -(-s + y + s) = -s - y + s. \]

It follows that \(s \cdot 2\) and hence \(s\) commutes with \(y\). Thus \(S \leq C_U(y)\). But by Lemma 3.4(3), \(U = \langle S \rangle\), so \(y \in Z(U)\). Since \(U\) is characteristically simple we get that \(U\) is abelian, a contradiction.

(4) By (3), \(U\) is a \(p\)-group. Let \(v \in S\). Then, by Lemma 3.6(4), \(v\eta = v \cdot i\) for some \(i \in \{\sqrt{-1}, -\sqrt{-1}\}\). Also for each \(s \in S\) we have \(s\eta \in \{s \cdot i, -s \cdot i\}\). Now \(v^a \in S\) by Lemma 2.2(1), so \((v^a)\eta \in \{(v^a) \cdot i, -(v^a) \cdot i\}\).

Suppose that \((v^a)\eta = (v^a) \cdot i = (v \cdot i)^a\). Then,

\[ (v \cdot i)^a = (v^a)\eta = (v\eta)^a \eta = (v \cdot i)^{−a}, \]

and hence \([a, v] = 0\).
Suppose \((v^a)\eta = -(v^a) \cdot 1 = (-v \cdot i)^a\). Then
\[ (-v \cdot i)^a = (v^a)\eta = (v\eta)^{a\eta} = (v \cdot i)^{-a}, \]
so \(a \cdot 2\) inverts \(v\) which is impossible since \(|a \cdot 2| = p\) is odd.
Hence \(a\) centralizes each element \(v \in S\) so \(a \in Z(U)\) and since \(U\) is characteristically simple, \(U\) is abelian. \(\square\)

As a corollary we get

**Proposition 3.8.** There exists \(x \in U^*\) such that \(|x| = p\) and \(T_x \neq \langle x \rangle\). Hence we may (and we will) assume that \(T \neq \langle a \rangle\).

**Proof.** This follows since we are assuming that \(U\) is not abelian and by Proposition 3.7(4). \(\square\)

We now need the following well-known result:

**Lemma 3.9.** Let \(q\) be a prime and let \(E\) be an elementary abelian group of order \(q^2\). Suppose that \(E\) acts on a vector space \(W\). Then there exists \(e \in E^*\) such that \(C_W(e) \neq 0\).

**Proof.** This is well known and follows from \([5, \text{Theorem 2.3, p. 65}]\). \(\square\)

**Proposition 3.10.** If \(s \in S^*\), then \(|s| = p\).

**Proof.** Let \(s \in S^*\) and assume that \(|s| \neq p\). By Proposition 3.5(3), \(T\) normalizes \(C_U(s)\). Let \(E \leq T\) be a subgroup of order \(p^2\). The existence of \(E\) follows from Proposition 3.8 and Lemma 3.2(2).

Of course \(E\) is elementary abelian. Since \(E\) acts on \(C_U(s)\), Lemma 3.9 together with Proposition 3.5(1), implies that there exists \(w \in C_U(s)^*\) and \(e \in E^*\) such that \([w, e] = 0\). But then \(|s| = |w| = |e| = p\), a contradiction. \(\square\)

**Lemma 3.11.** Let \(s \in S^*\), so that by Proposition 3.10, \(|s| = p\). Assume that \(s\eta = s \cdot i\) for some \(i \in \{\sqrt{-1}, -\sqrt{-1}\}\). Then

1. \(T_{sa} = T_{s^{-a}}\).
2. \((T_{sa})\mu_\alpha^2 = T_{s^a} = (T_{s^a})\mu_\alpha^2\).
3. \([s, a] = 0\).

**Proof.** (1) Notice first that for each \(h \in H\) and \(x \in U^*\) we have \(T_{xh} = (T_x)h\). \(\quad (3.3)\)

Indeed
\[ v \in T_{xh} \iff v\mu_{xh}^2 = v \iff vh^{-1}\mu_x^2h = v \iff vh^{-1} \in T_x. \]
Since $s^a \in S$, Lemma 3.6(3) implies that $(T_{s^a})\eta = T_{s^a}$. On the other hand, by (3.3),
\[(T_{s^a})\eta = T_{(s^a)\eta} = T_{(s-i)\eta}\]
where the last equality follows from the fact that $\mu_{s^a}^2 = \mu_{s^a}$ (see Eq. (3.2)).

(2) By (3.3), we have $(T_{s^a})\mu_{s^a}^2 = T_{(s^a)\mu_{s^a}^2} = T_{(-s^a)} = T_{s^a}$. Also, $(T_{s^a})\mu_s^2 = T_{(s^a)\mu_s^2} = T_{s^a} = T_{a}$, by (1), where we have used the fact that by Lemma 3.6(2), $a\mu_s^2 = -a$.

(3) Notice that by Lemma 3.6(1&2), $E := \langle \mu_{s^a}, \mu_s^2 \rangle$ is an elementary abelian group of order 4 and that $E^* = \{\mu_{s^a}, \mu_s^2, \mu_{a\mu_s}, \mu_{s^a}\mu_s^2 \}$, indeed, by Lemma 3.6(2) and Eq. (3.1), $\mu_{s^a}\mu_s^2 = \mu_{s^a}$ which is false. Suppose $x = a\mu_s$. Then $s^a = (s^a)\mu_{s^a}^2 = ((-s)^a)\mu_{s^a}^2 = (-s)^{-a}$. This is also impossible. Hence $s^a = (s^a)\mu_s^2 = s^{-a}$ and we see that $[a, s] = 0$. 

We can now prove Theorem A.

**Proof of Theorem A.** We assume that $U$ is not abelian. Let $s \in S^*$. By Proposition 3.10, $|s| = p$. By Lemma 3.6(3), $T_s\eta = T_s$. For $i \in \{\sqrt{-1}, \sqrt{-1}\}$, let
\[T_{s,i} := \{v \in T_s \mid v \eta = v \cdot i\}.
\]
We claim that
\[T_s = T_s,\sqrt{-1} \oplus T_s,\sqrt{-1}.
\]
Notice that $\eta \in \text{Aut}(T_s)$ is an operator of order 4 and that 1 and $-1$ are not eigenvalues of $\eta$. The fact that 1 is not an eigenvalue follows from the fact that $\eta$ is regular on $U$ and the fact that $-1$ is not an eigenvalue of $\eta$ follows from the fact that $\eta^2 = \mu_s^2$ inverts $T_s$ (see Lemma 3.6(2)). Hence $i$ and $-i$ are the only eigenvalues of $\eta$ and the claim holds.

Notice that by Lemma 3.6(2), $T_s \subseteq S$. Let now $v \in T_{s,i}$. Then, by Lemma 3.11(3), $[v, a] = 0$. It follows that $[a, T_s] = 0$ and in particular $[a, s] = 0$. Since $s \in S$ was arbitrary we see that $[a, S] = 0$. But by Lemma 3.4(3), $U = \langle S \rangle$, so $a \in Z(U)$ and since $U$ is characteristically simple, $U$ is abelian, a contradiction. 

**Acknowledgments**

It is my pleasure to thank Tom De Medts for a careful reading of the paper and for pointing out to me a number of typos. I am also grateful to the referee for sharply spotting additional typos and for a detailed reading of the paper.

**References**