Finite Zassenhaus Moufang Sets with root groups of even order

Barbara Baumeister, Matthias Grüninger
Freie Universität Berlin
Institut für Mathematik
Arnimallee 3
14195 Berlin
E-Mail:baumeist@mi.fu-berlin.de, matgruen@zedat.fu-berlin.de

February 12, 2010

Abstract

Keywords: Moufang sets, rank one groups, rank one BN-pairs

1 Introdution

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

Moufang sets have been introduced by Tits in order to describe the absolutely simple algebraic groups of relative rank one [**?**]. The concept of a Moufang set is strongly related to the concept of a split BN-pair of rank one. Notice that it is also closely related to the concept of an abstract rank one group due to Timmesfeld [**?**].

As usual we choose two different elements in X, denote them by ∞ and 0 and set $U := U_\infty$. Then the Moufang set is completely determined by U and some element τ in $G^\dagger$ which interchanges ∞ and 0. Therefore, we denote the Moufang set also by $M(U, \tau)$.

The finite Moufang sets have already been studied since long time using a different language. More precisely the finite Moufang sets have already been classified by Hering, Kantor and Seitz [**?**]. Their classification uses difficult and long papers as [**?**] and [**?**]. It seems to us that the concept of a Moufang set is the appropiate language to carry out the determination of these groups.

De Medts and Segev gave a new proof using this language under the further condition that the Moufang set is special – for the definition of special see

the next section. Our goal of this paper is to extend their proof to the finite Zassenhaus Moufang sets and thereby giving a partial answer to Question 3 posed by Segev in [**?**]. A Moufang set is *Zassenhaus* if $G^\dagger$ is a Zassenhaus group, i.e. if in $G^\dagger$ there is a non-identy element which fixes two elements in X, but only the identity fixes three elements.

The finite Zassenhaus Moufang sets had been determined by Feit ([**?**]), Ito [**?**] and Suzuki [**?**] in a long proof. There are two families of examples:

$M(q)$: This Moufang set is just the projective line and its little projective group is $PSL(2,q)$ with q a prime power.

$MSuz(q)$: This Moufang set is the natural domain for the Suzuki group $Suz(q)$ with $q = 2^{2n+1}, n \in \mathbb{N}$. In this paper we give an elementary and short proof of

the classification of the finite Zassenhaus Moufang sets with root groups of even order. The latter implies that U contains some involution. We distinguish the two cases that U contains a special involution or not.

Theorem 1.1 *Let $M(U,\tau)$ be a finite Zassenhaus Moufang set such that U is of even order. If there is special involution in U, then $M(U,\tau) = M(q)$ and $G^\dagger \cong PSL_2(q)$ with $q = |U| = 2^m$ for some m in $\mathbb{N}$.*

Theorem 1.2 *Let $M(U,\tau)$ be a finite Zassenhaus Moufang set such that U is of even order. If there is no special involution in U, then $M(U,\tau) = MSuz(q)$ with $q^2 = |U|$, q an odd power of 2.*

As a corollary we obtain

Corollary 1.3 *Let $M(U,\tau)$ be a finite Zassenhaus Moufang sets such that U is of even order. Then one of the following holds:*

(a) U is abelian, $M(U,\tau) = M(q)$ and $G^\dagger \cong PSL_2(q)$ for some even prime power q.

(b) U is a Suzuki 2-group, $M(U,\tau) = MSuz(q)$ and $G^\dagger = Suz(q)$ with q an odd power of 2.

Notice that this is one of the first papers discussing not only special but also non-special Moufang sets.

Notice also that the distinction we make in our main theorems has in fact also be made by Suzuki without using the language of Moufang sets. Our proof differs heavily from Suzuki's - in particular in the case that there is a special involution in U. There is also some hope that some of our arguments can be extended to the case of infinite Zassenhaus Moufang sets.

The proof of Theorem **??** only uses the language of Moufang sets. The aim is to show that U is an elementary abelian 2-group and then to quote [**?**] or [**?**].

The proof of Theorem **??** is at some places a translation of the proof of Suzuki in the language of Moufang sets. We had some difficulties to prove that U is p-group. There we quote parts of the proof given by Feit [**?**] and presented

in [**?**]. Moreover, we have to refer to the classification of Suzuki 2-groups in [**?**]. The rest of the proof is pure Moufang set theory. At some parts it is shorter and more lucid than the original proof of Suzuki in [**?**]. For example, in **??** we don't have to compute the class number of the group which turns out to be the Suzuki group.

The paper is organized as follows:

2 Notation

We start with the basic notation. If $M(U,\tau)$ is a Moufang set, then we can recover X by setting

$$X := U \cup \{\infty\}.$$

Our notation is fairly standard and can for instance be found in [**?**].

(a) For $a \in U$ let α_a be the map in $\mathrm{Sym}(X)$ defined by $\infty\alpha_a = \infty$ and $b\alpha_a = b + a$ for $b \in U$.

(b) Set $U_\infty = \{\alpha_a \mid a \in U\}$ and for $a \in U$: $U_a := U_\infty^{\tau\alpha_a}$

(c) For $a \in U^\# := U \setminus \{0\}$, let μ_a be the unique element in $U_0\alpha_a U_0$ with $\infty\mu_a = 0$ and $0\mu_a = \infty$. One has $\mu_a^{-1} = \mu_{-a}$ and, if $M(U,\tau) = M(U,\tau^{-1})$, then $\mu_{a\tau} = \mu_{-a}^\tau$ for all $a \in U^\#$. Especially, one has $\mu_{a\mu_b} = \mu_{-a}^{\mu_b}$ for $b \in U^\#$ ([**?**], 4.3.1). . .

(d) Set $H := \langle \mu_a\mu_b \mid a,b \in U^\# \rangle$ (the Hua subgroup of $M(U,\tau)$). Then $H = G^\dagger_{0,\infty}$, the stabilizer of 0 and ∞ in $G^\dagger$.

As τ interchanges 0 and ∞, it acts on $U^\#$. Therefore, the following definition makes sense.

(e) For $a \in U^\#$ set $\sim a := (-a\tau^{-1})\tau$. One easily computes $\sim(\sim a) = a$. By 3.10 in [**?**] one has $\sim a = -(-a)\mu_a$. Especially, the element $\sim a$ doesn't depend on the choice of τ.

3 Preliminary observations

In the following section, $M(U,\tau)$ is an arbitrary, not necessarily finite Moufang set. We will repeatedly use the following equations (see [**?**], 6.1.1)

(3.1) If $a,b \in U^\#$ with $a \neq b$, then the element $c := (a\tau^{-1} - b\tau^{-1})\tau$ doesn't depend on τ. More precisely, $c = (a-b)\mu_b + \sim b$.

(3.2) One has $\mu_c = \mu_{-b}\mu_{b-a}\mu_a$.

3.1 Some properties of involutions in a root group

Lemma 3.1 *If a is an involution in $U^{\#}$, then:*

(a) One has $\mu_a^{\alpha_{-\sim a}} = \alpha_a^{\mu_a}$. Especially, μ_a is an involution conjugate to α_a.

(b) The element $\sim a$ is the unique fixed point of μ_a.

(c) It is $\sim - \sim a = - \sim a$.

Proof.

(a) By 4.3.1 in [**?**] one has $\mu_a = \alpha_{-\sim a}\mu_a\alpha_a\mu_a\alpha_{\sim a} = \alpha_a^{\mu_a\alpha_{\sim a}}$.

(b) Since ∞ is the unique fixed point of α_a, $\infty^{\mu_a\alpha_{\sim a}} = \sim a$ is the unique fixed point of $\mu_a = \alpha_a^{\mu_a \sim a}$.

(c) By definition, $\sim(- \sim a) = -(\sim a)\mu_{\sim a} = -(\sim a)\mu_a = - \sim a$.

□

Lemma 3.2 *If $a, b \in U$ are involutions with $\mu_a = \mu_b$, then $a = b$.*

Proof. If $\mu_a = \mu_b$, then by **??** $\sim a = \sim b$ and thus $a = b$. □

Lemma 3.3 *Let $M(U, \tau)$ be a Moufang set such that U has finite even order. Then $\mu_a\mu_b$ has odd order for all involutions $a, b \in U$. Hence all involutions in U are H-conjugate.*

Proof. We prove the first statement by induction on $|U|$. Suppose $a, b \in U$ are involutions in U such that $\mu_a\mu_b$ has even order n. Set $t := (\mu_a\mu_b)^{\frac{n}{2}}$. Then $t \in H$ and t centralizes μ_a and μ_b. It follows that t centralizes a and b as well. Hence $a, b \in V := C_U(t)$ which is a root group of U ([**?**], 6.2.3). By 6.2.2 of the same paper on can choose τ in a such way that $M(V, \rho)$ is a Moufang set and ρ is the restriction of τ on $V \cup \{\infty\}$. Since $t \neq 1$, V is a proper subgroup of U and hence we can apply induction. Hence there is an odd number k such that $(\mu_a\mu_b)^k$ centralizes V. Thus there is a power h of $\mu_a\mu_b$ such that $h^2|V = \mu_a\mu_b|V$. Therefore $\mu_a h^2|V^{\#} = \mu_a^h|V^{\#} = \mu_b|V^{\#}$. Using **??** for $M(V, \rho)$, this implies $a^h = b$. But then we get $\mu_a^h = \mu_{a^h} = \mu_b$ and thus $h^{-2}\mu_a\mu_b = \mu_a^h\mu_b = 1$. Therefore $h^2 = \mu_a\mu_b$. Since h is a power of $\mu_a\mu_b$, the element $\mu_a\mu_b$ must have odd order, a contradiction. Hence we have proved the first statement. The second follows immediately since we have shown that μ_a and μ_b are H-conjugate for all involutions $a, b \in U$ which together with **??** implies that a and b are H-conjugate as well. □

We remark here that in the infinite case it is possible that there is more than one H-orbit of involutions in a root group. This happens for example in $\mathbb{M}(K)$ if $charK = 2$, K not perfect, or in $MSuz(K, L, \theta)$ for θ not surjective (see Section 6).

Lemma 3.4 *Let $M(U,\tau)$ be a Moufang set with Hua subgroup H and let V be a subgroup of U. Suppose that*

(a) there is an abelian subgroup K of H such that all elements in $V^\#$ are K-conjugate.

(b) $h^{\mu_a} = h^{-1}$ for all $a \in V^\#, h \in K$.

Then $\mu_{b-a} = \mu_{a\mu_{-a}-b\mu_{-b}}$ for all $a, b \in V^\#$ with $a \neq b$.

Proof. There exist elements $g, h \in K$ with $ah = b, ag = b - a$. One computes

$$(a\mu_{-a}-b\mu_{-b})\mu_a = (a\mu_{-a}-ah\mu_{-ah})\mu_a = (a\mu_{-a}-ah\mu_{-a}^h)\mu_a = (a\mu_{-a}-ah^{-1}\mu_{-a})\mu_a =$$

$$(a-ah^{-1})\mu_{ah^{-1}} + \sim ah^{-1} = (a-ah^{-1})h\mu_a h^{-1} + \sim ah^{-1} = ((ah-a)\mu_a + \sim a)h^{-1}$$

$$= (ag\mu_a + \sim a)h^{-1} = (a\mu_a g^{-1} + \sim a)h^{-1} = (a\mu_a + \sim ag)g^{-1}h^{-1}.$$

By (3.2), one has

$$\mu_{a\mu_a+\sim ag} = \mu^{gh}_{(a\mu_a+\sim ag)g^{-1}h^{-1}} = (\mu_{(a\mu_{-a}-ah^{-1}\mu_{-a})\mu_a})^{gh} = (\mu_{-ah^{-1}}\mu_{ah^{-1}-a}\mu_a)^{gh}.$$

Hence $\mu_{a\mu_a+\sim ag}$ inverts every element in K. We get

$$hg^2h\mu_{a\mu_a+\sim ag} = hg\mu_{a\mu_a+\sim ag}g^{-1}h^{-1} = \mu_{(a\mu_a+\sim ag)g^{-1}h^{-1}} = \mu_{(a\mu_a-ah^{-1}\mu_a)\mu_a}$$

$$= \mu_{-ah^{-1}}\mu_{ah^{-1}-a}\mu_a = h\mu_{-a}h^{-1}\mu_{-agh^{-1}}\mu_a = h^2\mu_{-a}hg^{-1}\mu_{-a}gh^{-1}\mu_a =$$

$$h^2\mu_{-a}h^2g^{-2}\mu_{-a}\mu_a = g^2\mu_{-a},$$

and so

$$\mu_{-a} = h^2\mu_{a\mu_a+\sim ag} = \mu_{(a\mu_a+\sim ag)h^{-1}} = \mu^g_{(a\mu_a+\sim ag)h^{-1}g^{-1}} =$$

$$\mu^g_{(a\mu_{-a}-b\mu_{-b})\mu_a} = \mu^{\mu_a g}_{b\mu_{-b}-a\mu_{-a}} = \mu^{g^{-1}\mu_a}_{a\mu_{-a}-b\mu_{-b}}.$$

This implies finally

$$\mu_{b\mu_{-b}-a\mu_{-a}} = \mu^{\mu_a g}_{-a} = \mu^g_{-a} = \mu_{-ag} = \mu_{a-b.}$$

Hence we get $\mu_{a\mu_{-a}-b\mu_{-b}} = \mu_{b-a}$. □

3.2 Some properties of special elements

In this section we prove facts on Moufang sets whose root group contains a special element.

Definition 3.5 *(a) A Moufang set $M(U,\tau)$ is called special if $(-a)\tau = -(a\tau)$ for all $a \in U^\#$ holds.*

(b) An element $a \in U^\#$ is called special if $(-a)\tau^{-1} = -(a\tau^{-1})$.

It is very easy to see that $M(U,\tau)$ is special iff all elements in $U^{\#}$ are special: If $M(U,\tau)$ is special and $a \in U^{\tau}$, then

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

and thus a is special. If all elements in $U^{\#}$ are special, then for $a \in U^{\#}$ one gets

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

and hence $M(U,\tau)$ is special.

It might surprise that we demand $(-a)\tau^{-1} = -(a\tau^{-1})$ and not $(-a)\tau = -(a\tau)$ for the definition of a special element. But it may happen that $M(U,\tau) = M(U,\rho)$ and $a \in U^{\#}$ with $(-a)\tau = -a\tau$ but $(-a)\rho \neq -a\rho$. This happens for example in the Ree-Tits Moufang sets. Moreover, $(-a)\tau = -(a\tau)$ is in general not equivalent to one of the statements in the following lemma.

Lemma 3.6 *For $a \in U^{\#}$ the following statements are equivalent.*

(a) *a is special.*

(b) *$\sim a = -a$.*

(c) *$(-a)\mu_a = a$.*

(d) *$a\mu_{-a} = -a$.*

(e) *If $M(U,\tau) = M(U,\rho)$, then $(-a)\rho^{-1} = -(a\rho^{-1})$.*

(f) *There is an element $\rho \in SymX$ with $M(U,\rho) = M(U,\tau)$ such that $-(a\rho^{-1}) = (-a)\rho^{-1}$.*

(g) *$(-a)\mu_a = -(a\mu_a)$.*

Proof.

"$(a) \to (b)$" By definition, one has $\sim a = (-(a\tau^{-1})\tau = ((-a)\tau^{-1})\tau = -a$.

"$(b) \to (c)$" By 4.3.1.(6) in [**?**], one has $-a = \sim a = -(-a)\mu_a$ and hence $a = (-a)\mu_a$.

"$(c) \leftrightarrow (d)$" This is clear since $\mu_a^{-1} = \mu_{-a}$.

"$(c) \to (e)$" By 3.5 and 4.4.1 (1) in [**?**] $\mu_a\rho^{-1}$ induces and automorphism of U. One has $a\rho^{-1} = (-a)\mu_a\rho^{-1}$ and thus $-a\rho^{-1} = a\mu_a\rho^{-1} = (-a)\rho^{-1}$.

"$(e) \to (f)$" This is trivial.

"$(f) \to (g)$" Again by 3.5 and 4.4.1 (1) in [**?**] $\rho\mu_a$ induces an automorphism of U. Therefore, one has $(-a)\mu_a = (-a)\rho^{-1}\rho\mu_a = ((-a)\rho^{-1})\rho\mu_a = (-a\rho^{-1})\rho\mu_a = -(a\rho^{-1})\rho\mu_a = -(a\mu_a)$.

"$(g) \to (a)$" By 4.3.1 (1) in [**?**], $\mu_a = \tau^{-1}h_a$ where h_a is the Hua map associated to a and hence induces an automorphism on U. Thus $-(a\tau^{-1}) = -a(\mu_a h_a^{-1}) = (-(a\mu_a))h_a^{-1} = (-a)\mu_a h_a^{-1} = (-a)\tau^{-1}$.

□

Lemma 3.7 *(a) An element $a \in U^\#$ is special if and only if $-a$ is special.*

(b) If $a \in U$ is an involution, then a is special if and only if $a\tau^{-1}$ is again an involution.

(c) If $a \in Z(U)^\#$ is special, then $a\rho^{-1} \in Z(U)$ for all $\rho \in SymX$ with $0\rho = \infty, \infty\rho = 0$ and $M(U,\tau) = M(U,\rho)$.

Proof. The first statement follows from the fact that (c) and (d) are equivalent, the second is true by definiton. If $a \in Z(U)^\#$ is special and ρ as above, then $\mu_a\rho^{-1}$ induces an automorphism of U. Since $a = (-a)\mu_a$ one gets $a\rho^{-1} = (-a)\mu_a\rho^{-1} \in Z(U)$. □

Lemma 3.8 *If $a \in U^\#$ is special, then $a\mu_a = -a = a\mu_{-a}$.*

Proof. By **??** (c) and (g) $-(a\mu_a) = (-a)\mu_a = a$ and thus $a\mu_a = -a$. The second equation holds since $-a$ is again special. □

It is not clear if $a\mu_a = -a$ implies that a is special.

The following lemma implies that if the Moufang set is not special, then H is "linear" in two ways on U.

Lemma 3.9 *For all $a \in U^\#$ and all $h \in H$, one has $\sim (ah) = (\sim a)h$.*

Proof. By 4.3.1(6) in [**?**], $\sim (ah) = -(-ah)\mu_{ah} = -(-ah)\mu_a^h$. By 4.3.1(4) of [**?**] the latter equals $-(-ah)h^{-1}\mu_a h = -(-a)\mu_a h = (\sim a)h$. □

.

Lemma 3.10 *If $a \in U$ is special and $h \in H$, then ah is special.*

Proof. If a is special, then $\sim (ah) = (\sim a)h = (-a)h = -ah$, hence ah is special. □

Lemma 3.11 *An element $a \in U^\#$ is special if and only if there is an element $b \in U_0$ such that $\mu_a = b\alpha_a b$.*

Proof. There exist uniquely determined elements $b', b'' \in U_0$ such $\mu_a = b'\alpha_a b''$. By 4.1.1 in [**?**], these elements are $b' = \alpha^\tau_{(-a)\tau^{-1}}$ and $b'' = \alpha^\tau_{-(a\tau^{-1})}$. Thus a is special if and only if these elements are equal. □

For all $a \in U^\#$, we set

$$V_a := \{b \in U^\# \mid \mu_a = \mu_b\}.$$

Then $U^\#$ is a disjoint union of the sets V_a where a runs through $U^\#$. Notice that $-\sim a$ and $\sim -a$ are in V_a for all $a \in U^\#$: by **??**(c) $\mu_{-\sim a} = \mu_{(-a)\mu_a} = \mu_a^{\mu_a} = \mu_a$, so $\mu_{-\sim a} = \mu_a$. In this equation replace a by $\sim a$ and get $\mu_{-a} = \mu_{\sim a}$ (clearly, $\sim\sim a = a$). If we replace a by $-a$ in the latter equation, then we get $\mu_a = \mu_{\sim -a}$.

We will frequently use the following lemma.

Lemma 3.12 *If μ_a is an involution, then $\sim - \sim a = - \sim -a$.*

Proof. By 2.3 in [**?**], one has $a\mu_a = \sim - \sim a$ and $a\mu_{-a} = - \sim -a$. Thus the claim follows. □

The following lemma collects some useful information about V_a for a special central element a. We will need only part (a)-(d), but the other parts are interesting too.

Lemma 3.13 *Suppose that $a \in Z(U)^\#$ is special, that $\mu_a = \mu_{-a} = \mu_a^{-1}$ and that $b \in V_a \setminus \{a, -a\}$. Then the follwing holds.*

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

(b) $-(a-b)\mu_a + (b-a)\mu_a = b + a \cdot 2$.

(c) $-a \cdot 3 = \sim -b - \sim b + b = - \sim b + b + \sim -b = b - \sim b + \sim -b$.

(d) $-((-a)\tau^{-1} - (-b)\tau^{-1})\tau + (a\tau^{-1} - b\tau^{-1})\tau = a$ *and* $(a\tau^{-1} - b\tau^{-1})\tau - ((-a)\tau^{-1} - (-b)\tau^{-1})\tau = a$.

(e) $(a-b)\tau - (-a - \sim b)\tau = a\tau$.

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

(g) $-(-a-b)\tau + (\sim b - a)\tau = - \sim (b\tau) - a\tau$.

(h) $-(-a-b)\mu_a + (\sim b - a)\mu_a = \sim b + a$.

(i) *a and $-a$ are the only special elements in V_a.*

Proof. (a) We have by (3.1)

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

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

hence

$$(*) \quad -(a + \sim b)\mu_a + (a-b)\mu_a = a - \sim b.$$

Furthermore

$$(**)\ (\sim b + a)\mu_a = (-(-b)\mu_a + (-a)\mu_a)\mu_a = ((-a)\mu_a - (-b)\mu_a)\mu_a =$$

$$(b-a)\mu_a + \sim -b = -[- \sim -b - (b-a)\mu_a].$$

If we set $(**)$ in $(*)$, the claim follows.

(b) This is similar to (a): We have again by (3.1)

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

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

hence

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

Furthermore

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

Thus the claim follows.

(c) By (a) and (b),

$$\sim -b + a- \sim b = -a \cdot 2 - b.$$

Hence

$$\sim -b- \sim b + b = -a \cdot 3.$$

We get the other equations if we conjugate by $- \sim -b$ and b.

(d) We have

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

By part (a), we get

$$\sim -b + a- \sim b = -(-a-(-b))\mu_a + (a-b)\mu_a =$$

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

Therefore, we get the first equation. The second follows since a is central and we can conjugate with $-(a\tau^{-1} - b\tau^{-1})\tau$.

(e) follows by (d) and by replacing b with $b\tau$ and a with $a\tau$.

(f) We have

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

and

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

Subtracting yields the result.

(g) follows by taking $a\tau$ instead a and $b\tau$ of b.

(h) follows by taking $\tau = \mu_a$ and by

$$- \sim (b\mu_a) = - \sim - \sim -b = \sim - \sim \sim -b = \sim b$$

by **??**.

(i) If b is special, then $\sim b = -b$ and hence $a = b$ by (g). □

Proposition 3.14 *If a and b are as in* **??**, *then $\mu_a = \mu_{a-b}\mu_{a\cdot 5+b}\mu_{a-b}$. Especially, if a is an involution, then $\mu_a = \mu_{a+b}$.*

Proof. Set $x := a\mu_a - b\mu_a$ and $y := -a\mu_a - (-b)\mu_a$. Then $\mu_{a-b} = \mu_x$ and $\mu_y = \mu_{-a+b} = \mu_{a-b}^{-1}$ by [**?**], 2.6. Furthermore, (3.2) tells us

$$\mu_c = \mu_{-y}\mu_{y-x}\mu_x$$

with $c = (x\mu_a - y\mu_a)\mu_a$. We have $c = a\mu_a = -a$ by **??** (d) with $\tau = \mu_a$, and

$$y - x = -a\mu_a - (-b)\mu_a - a\mu_a + b\mu_a = a+ \sim b + a- \sim -b =$$

$$a \cdot 2 - (\sim -b- \sim b) = a \cdot 2 - (-a \cdot 3 - b) = a \cdot 5 + b$$

by **??** (c). Hence $\mu_a = \mu_{a-b}\mu_{a\cdot 5+b}\mu_{a-b}$. If a is an involution, then $a - b = -(a + b)$ and hence $\mu_a = \mu_{a-b}\mu_{a+b}\mu_{a+b}^{-1} = \mu_{a-b}$. As μ_a is an involution by **??**(a), it follows that $\mu_a = \mu_{a-b} = \mu_{a+b}$ □

Lemma 3.15 *If $a \in Z(U)^\#$ is a special involution and $x \in U^\#$ with $\mu_{x+a} = \mu_x = \mu_{-x}$, then $\mu_x = \mu_a$.*

Proof. We have $((x + a)\tau^{-1} - x\tau^{-1})\tau = a\mu_x+ \sim x$ and thus

$$\mu_{a\mu_x} = \mu_x\mu_a\mu_x = \mu_x\mu_a\mu_{x+a} = \mu_{a\mu_x+\sim x}.$$

Now $a\mu_x = a\mu_a\mu_x$ is again a special involution in $Z(U)$. Thus by **??**

$$\mu_{a\mu_x} = \mu_{a\mu_x+\sim x+a\mu_x} = \mu_{\sim x} = \mu_x.$$

Hence $\mu_x\mu_a\mu_x = \mu_x$ and therefore $\mu_a = \mu_x$. □

4 Zassenhaus Moufang sets

Definition 4.1 *A proper Moufang set $M(U, \tau)$ is called a Zassenhaus Moufang set if $G^\dagger_{0,\infty,a} = 1$ for all $a \in U^\#$, or equivalently, if $C_U(h) = 1$ for all $h \in H^*$.*

From now on, we assume that $M(U, \tau)$ is a Zassenhaus Moufang set such that the order of U is finite.

Lemma 4.2 *(a) The root group U is nilpotent.*

(b) If U is abelian, then $M(U, \tau) \cong M(\mathbb{F}_q)$ for $q = |U|$ and hence $G^\dagger \cong PSL_2(q)$.

(c) $G^\dagger$ is simple.

Proof.

(a) Since $M(U,\tau)$ is proper, $H \neq 1$. Thus UH is a Frobenius group with Frobenius kernel U. By Thompson's theorem, U is nilpotent.

(b) By the main theorem of [**?**], $M(U,\tau)$ is special. Thus the claim follows by [**?**] and [**?**].

(c) Suppose $1 < M$ is a normal subgroup of $G^\dagger$. Since $G^\dagger$ acts primitively on X, M is transitive on X and thus on the set of root groups. By definition $G^\dagger$ is generated by the root groups and hence one has $G^\dagger = MU_\infty$ and $G^\dagger/M \cong U_\infty/(M \cap U_\infty)$. If $M < G^\dagger$, then U_∞ is not contained in $(G^\dagger)'$ since $U/(U \cap M)$ is nilpotent. But since H acts without fixed point on U, one has $U = [U,H] \leq (G^\dagger)'$. It follows $G^\dagger = M$.

□

Lemma 4.3 *If H has even order, then $M(U,\tau) \cong M(\mathbb{F}_q)$.*

Proof. If H has even order, then H contains an involution t. Since t has no fixed points on U, t must invert every element in U. This implies U abelian and hence $M(U,\tau) \cong M(\mathbb{F}_q)$. □

Lemma 4.4 *If $|U| \equiv 1 \ mod\ 4$, then $M(U,\tau) \cong M(\mathbb{F}_q)$ for $q = |U|$.*

Proof. If $|U| \equiv 1 \ mod\ 4$ and H has odd order, then $|G^\dagger| = (|U|+1)|U||H| \equiv 2 \ mod\ 4$. Hence $G^\dagger$ possesses a normal subgroup L of index 2. Since $|L|$ is odd, L cannot act transitively on X. But this is a contradiction since $G^\dagger$ acts 2-transitively and therefore primitively on X. □

Lemma 4.5 *If H is odd, then there is an unique conjugacy class of involutions in $G^\dagger$.*

Proof. Let t be an involution. Since $G^\dagger$ acts 2-transitively on X, we can assume $t \in N$. For every $a \in U^\#$, the element $t\mu_a \in H$ has odd order. Hence t and μ_a are conjugate. □

4.1 Zassenhaus Moufang sets with $|U|$ even

From now on, we assume that the order of U is even.

Lemma 4.6 *(a) Every involution in U is contained in $Z(U)$.*

(b) For every $a \in U^\#$ there is exactly one involution $b \in U$ with $\mu_a = \mu_b$.

(c) H is cyclic.

Proof. (a) This is clear since U is nilpotent and all involutions are H-conjugate by **??**.

(b) This follows since $|H| = |\{\mu_x \mid x \in U^\#, x \text{ involution }\}| \leq |\{\mu_x \mid x \in U^\#\}| \leq |N| - |H| = |H|$.

(c) If a is an involution, then **??** and **??** imply that N contains exactly $|H|$ conjugates of μ_a. Thus $C_H(\mu_a) = 1$ and therefore H is abelian. Since H acts freely on U, this means that H is cyclic. □

Since all involutions in U are H-conjugate, either all involutions are special or no involution is special. We first treat the case that all involutions are special and show that this implies $M(U,\tau)$ special and hence $G^\dagger \cong (P)SL_2(q)$ with $q = |U|$ a power of 2.

Proof of Theorem ?? We show that U is an elementary-abelian 2-group, as this then implies that $M(U,\tau)$ is special, see [**?**]. Since H is cyclic by **??** (c), the main theorem in [**?**] then yields that $M(U,\tau) \cong M(\mathbb{F}_q)$ with $q = |U|$ (alternatively, we can apply [**?**]).

We first note that U contains more than one involution since H acts regularly on the set of involutions and $H \neq 1$ since $M(U,\tau)$ is proper.

By assumption U contains a special involution. By **??**(a) a is contained in $Z(U)$ and by **??** every involution in U is contained in $Z(U)$ and is conjugate to a under H. Suppose U contains an element b of order 4. Let a be the unique involution with $\mu_a = \mu_b$. Then $\mu_b = \mu_{-b} = \mu_{b+b\cdot 2}$, hence $a = b \cdot 2$ by **??**. If t is an involution distinct from a, then again $(b+t)\cdot 2 = b \cdot 2 = a$, as t is in $Z(U)$, hence $\mu_{b+t} = \mu_a = \mu_b$ and so $\mu_a = \mu_b = \mu_t$ by **??** and $a = t$ by **??**, a contradiction. Hence if V is the unique Sylow 2-subgroup of U, then V is elementary abelian.

If $U \neq V$, then there is an element $b \in Z(U) \setminus V$. Let a be the unique involution in V_b. By **??**, $a = - \sim b+ \sim -b + b$ and hence $a - b = - \sim b+ \sim -b = (-b)\mu_a - b\mu_a$ by 4.3.1 (6) of [**?**]. Hence by [**?**], 2.5 (1) and **??**

$$\mu_{b\cdot 2} = \mu_{-b\cdot 2} = \mu_{(-b)\mu_a - b\mu_a} = \mu_{a-b} = \mu_b.$$

But again, if $t \in U$ is an involution distinct from a, then $\mu_{b+t} = \mu_{(b+t)\cdot 2} = \mu_{b\cdot 2} = \mu_b$, hence $\mu_a = \mu_b = \mu_t$ By **??**, this is a contradiction. □

5 Suzuki Moufang Sets

5.1 Suzuki 2-Groups

Definition 5.1 (compare [?], p. 299) *A finite group G is called a Suzuki 2-group if the following hold:*

(a) G is a nonabelian 2-group.

(b) G has more than one involution.

(c) There is a soluble subgroup of AutG which permutes the involutions transitively.

By **??** the Sylow 2-group of the root group U a Zassenhaus Moufang set of finite even order is either abelian or a Suzuki 2-group.

Example 5.2 *et K be a field of characteristic 2 and let θ be a non-zero endomorphism of K. Set $k = K^\theta$ and let L be a k-subvectorspace of K with $1 \in L$ and $K = k[L]$. Set $A(K, L, \theta) := L \times L$ with addition $(a, b) + (c, d) := (a + c, b + d + ac^\theta)$. One sees easily that $(A(K, L, \theta), +)$ with this addition is a group. If $K = \mathbb{F}_{2^n}$ is finite then $L = K = k$ and we will call this group $A(n, \theta)$. If θ is not the identity, then $A(K, L, \theta)$ is non-abelian and the center consists of all elements with first coordinate zero. If $a^\theta \neq a^{-1}$ for all $a \in L$ these are exactly the elements of order at most 2. In the finite case this condition holds if and only if the order of θ is odd. Finally, if θ is a* Tits endomorphism*, that means θ^2 is the Frobenius endomorphism, then $[(a^{-1}, 0), (a^\theta, 0)] = (0, a+1)$ and thus the center equals the derived subgroup.*
Suppose that $\lambda \mapsto \lambda^{1+\theta}$ is a bijection of L. For every $\lambda \in K^\#$ with $\lambda L = L$ the map $h_\lambda : A(K, L, \theta) \to A(K, L, \theta) : (a, b) \mapsto (\lambda a, \lambda^{1+\theta} b)$ is an automorphism of $A(K, L, \theta)$ and the map $\lambda \mapsto h_\lambda$ is an injective homomorphism from $K^\#$ to $AutA(K, L, \theta)$ whose image we call Λ. Suppose that $K = \mathbb{F}_{2^n}$ and that the order of θ is odd.. Then Λ acts regularly on the set of involutions of $A(K, L, \theta)$. Thus $A(n, \theta)$ Suzuki 2-group. A set $X \subseteq A(n, \theta)$ is a system of representative for $A(n, \theta)/Z(A(n, \theta))$ if and only if the map $a \mapsto a \cdot 2$ maps X bijectively on $Z(A(n, \theta))$.

Theorem 5.3 *If G is a Suzuki 2-group, then the exponent of G is 4 and either $G \cong A(n, \theta)$ with $o(\theta)$ odd or $|G| = |Z(G)|^3$.*

Proof. See [**?**], Theorem VIII.7.9. □

Theorem 5.4 *If $U = A(n, \theta)$ with $o(\theta)$ odd and if $K \leq AutU$ is cyclic of order $2^n - 1$, then $K \leq C\Lambda$ with $C = C_{AutU}(U/Z(U)) \cap C_{AutU}(Z(U))$.*

Proof. This follows from [**?**], VII. 6.8. □

Definition 5.5 *Let K, θ, k and L as above. Moreover, suppose that θ is a Tits endomorphism. Note that $K^2 \subseteq k$ and that $a^{-1} = a^{-2}a \in L$ for all $a \in L^\#$. If K is a finite field of order 2^n this implies n odd. For $a, b \in K$ set $N(a, b) := a^{2+\theta} + ab + b^\theta$. Since $N(a, b) = (\frac{b}{a})^{1+\theta} + (a^\theta + \frac{b}{a})^{1+\theta}$ for $a \neq 0$, one easily see that $N(a, b) = 0$ implies $a = b = 0$. Set $U := A(K, L, \theta)$. Let τ be the permutation on $U^\#$ defined by $(a, b)\tau = (\frac{b}{N(a,b)}, \frac{a}{N(a,b)})$. We first check that $(a, b)\tau$ is in U. This is easily seen if $a = 0$ or $b = 0$, so suppose both elements are not zero. One has $aN(a, b) = a^{2+\theta}a + a^2b + b^\theta a \in L$ since $a^{2+\theta}, a^2, b^\theta \in k$, thus $a^{-1}N(a, b) = a^{-2}aN(a, b)$ and $aN(a, b)^{-1}$ are again in L.*

Also $bN(a,b) = a^{2+\theta}b + b^2a + b^\theta b \in L$ *since* $a^{2+\theta}, b^2, b^\theta \in L$. *Thus* $b^{-1}N(a,b)$ *and* $bN(a,b)^{-1}$ *are in* L.

One can see that $M(U,\tau)$ *defines a Moufang set which we will call* $MSuz(K,L,\theta)$ *or for* $K = \mathbb{F}_{2^n}$ *just* $MSuz(2^n)$. *These Moufang sets are also called* (generalized) Suzuki Moufang sets. *The little projective group correspondig to such a Moufang set is called* generalized Suzuki group *or* $Suz(K,L,\theta)$ *(*$Suz(2^n)$ *if* $K = \mathbb{F}_{2^n}$*)..*
An easy but tedious computation shows that $\tau^2 = 1$ *and* $\tau\mu_{(a,b)}$ *induces the automorphism* $h_{N(a,b)^{2-\theta}}$ *on* U *(see [?] where a matrix representation for* $Suz(K,L,\theta)$ *is given). Especially* $MSuz(K,L,\theta)$ *is Zassenhaus and* $\mu_{(a,b)} = \mu_{(c,d)}$ *iff* $N(a,b) = N(c,d)$.

5.2 The Case where no involution is special

From now on we assume that no involution of U is special.

Theorem 5.6 *U is a p-group*

Proof. This was proven by Feit [**?**]. His proof with some improvement by Bender is contained in [**?**]. More precisely the assertion follows from 4.1, 6.3, 6.5, 6.6 and 5.7 of [**?**] together with □

We know that U is either an abelian 2-group or a Suzuki 2-group. If U is abelian, then $M(U,\tau)$ is special by [**?**], so U must be a Suzuki 2-group. From now on, let $q := |Z(U)|$. Then q is a power of 2 and $|H| = q - 1$. Moreover, $|U| = q^2$ or $|U| = q^3$ by **??**. Since $M(U,\tau)$ is proper, $q > 2$.

Remember that by **??** (a) one has $\alpha_a^{\mu_a} = \mu_a^{\alpha_{\sim a}}$. This equals Suzuki's structure equation (XI. 10.6 in [**?**]).

Lemma 5.7 *One has* $(\sim a) \cdot 2 = a$ *for all involutions* $a \in U$.

Proof. Set $D = \langle \alpha_a, \mu_a \rangle$. Then D is dihedral since α_a and μ_a are involutions. The order of $\alpha_a\mu_a$ is odd since $C_{G^\dagger}(\alpha_a) \cap C_{G^\dagger}(\mu_a) = U_\infty \cap C_{G^\dagger}(\mu_a) = 1$. Set $E = \langle \mu_a\alpha_a \rangle$. Then $\alpha_{-\sim a} \in N_G(E)$ since $D^{\alpha_{-\sim a}} = \langle \alpha_a^{\alpha_{\sim a}}, \mu_a^{\alpha_{-\sim a}} \rangle = \langle \alpha_a, \alpha_a^{\mu_a} \rangle = D$ and $E = D'$ is characteristic in D. On the other hand, $C_U(E) = 1$ since $C_{G^\dagger}(\alpha_t) \leq U_\infty$ for all $t \in U^\#$. Hence $N_{U_\infty}(E) \leq AutE$ is abelian. One easily sees that α_a is the unique involution in $N_{U_\infty}(E)$, so this group must be cyclic. Since U_∞ has exponent 4, the claim follows. □
.

Lemma 5.8 *H does not contain an element of order* 3.

Proof. Suppose otherwise. Then there are involutions $a, b \in U$ such that $\mu_a\mu_b$ has order 3. Now μ_a and α_a are conjugate, hence there is an involution $t \in G^\dagger$ such that $\alpha_a t$ has order 3. Since $C_{G^\dagger}(\alpha_a) = U_\infty$ is transitive on $X \setminus \{0\}$, we can assume that t fixes 0. Hence there is an involution $c \in U$ such that $t = \alpha_c^{\mu_a}$. Hence

$$1 = \alpha_a\mu_a\alpha_c\mu_a\alpha_a\mu_a\alpha_c\mu_a\alpha_a\mu_a\alpha_c\mu_a =$$

$$\mu_a(\alpha_a^{\mu_a})\alpha_c(\alpha_a^{\mu_a})\alpha_c(\alpha_a^{\mu_a})\alpha_c\mu_a$$
$$= \mu_a(\alpha_{\sim a}\mu_a\alpha_{-\sim a})\alpha_c(\alpha_{\sim a}\mu_a\alpha_{-\sim a})\alpha_c(\alpha_{\sim a}\mu_a\alpha_{-\sim a})\alpha_c\mu_a$$
$$= \mu_a\alpha_{\sim a}\mu_a\alpha_c\mu_a\alpha_c\mu_a\alpha_{c-\sim a}\mu_a.$$

This implies

$$1 = \alpha_{\sim a}\mu_a\alpha_c\mu_a\alpha_c\mu_a\alpha_{c-\sim a},$$

hence

$$1 = \mu_a\alpha_c\mu_a\alpha_c\mu_a\alpha_c$$

and therefore

$$\mu_a = \alpha_c^{\mu_a}\alpha_c\alpha_c^{\mu_a}.$$

Since μ_c is the unique element in $U_0\alpha_c U_0$ interchanging 0 and ∞, this implies $a = c$. Now this equation implies that a is special, a contradiction. □

Lemma 5.9 *(a) $q = 2^n$ with n odd.*

(b) The order of $\mu_a\alpha_a$ is 5.

(c) U is isomorphic to $A(n, \theta)$.

Proof. We have taken this proof from [**?**], XI.11.2.

(a) If n was even, 3 would divide $q - 1$.

(b) One computes $(\alpha_a\mu_a)^{\alpha_{\sim a}} = (\alpha_a\mu_a)^2$. Since $\sim a \cdot 2 = a$, we have $(\alpha_a\mu_a)^{-1} = (\alpha_a\mu_a)^{\alpha_a} = (\alpha_a\mu_a)^4$ and thus $(\alpha_a\mu_a)^5 = 1$..

(c) If U is not isomorphic to $A(n, \theta)$, then $|U| = q^3$ and thus $|G^\dagger| = (q^3 + 1)q^3(q + 1)$ with $q = 2^n$, n odd. Since 5 divides $|G^\dagger|$ but not q^3 and $q - 1$, 5 divides $q^3 + 1$ and thus 5 divides $q^6 - 1 = 2^{6n} - 1$. This implies $2^{6n} \equiv 1 \ mod\ 5$ and hence $4|6n$, a contradiction since n is odd.

□

We now know that $|U| = q^2$ and $|G^\dagger| = (q^2 + 1)q^2(q - 1)$ which is exactly the order of the Suzuki group $Suz(q)$.

Lemma 5.10 *The set $0 \cup \{\sim a \mid a \in Z(U)^\#\}$ is a system of representatives for $U/Z(U)$.*

Proof. By **??**, $U \cong A(n, \theta)$. Thus if $|Z(U)| = q$, then $q = |U : Z(U)|$. By **??**, $\sim a \cdot 2 = a$ for all $a \in Z(U)^\#$. Thus the claim follows since a subset X of U is a system of representatives for $U/Z(U)$ if and only if the map $x \mapsto x \cdot 2$ induces a bijection between X and $Z(U)$. □

Lemma 5.11 *If a, b are two different involutions in $Z(U)$, then $\mu_{a+b} = \mu_{-\sim a+\sim b}$.*

Proof. This follows from **??**. □

The root group U contains q elements in $Z(U)$ and each $q-1$ elements of the form $\sim a$ and $-\sim a$ with $a \in Z(U)^{\#}$. We will show that each of the remaining $q^2-q-2(q-1) = (q-2)(q-1)$ elements can be uniquely written as $-\sim a+\sim b$ with $a, b \in Z(U)^{\#}, a \neq b$. Having succeeded we know μ_a for all $a \in U$.

Lemma 5.12 *If $a, b, c \in Z(U)^{\#}$ with $a \neq b$, then $c\mu_a\mu_{a+b} = c + c\mu_a\mu_b$.*

Proof. One has

$$\sim(-\sim a+\sim b) = (-(-\sim a+\sim b)\mu_b)\mu_b = (-(a\mu_a\mu_b^2 - b\mu_b)\mu_b)\mu_b =$$

$$[-((a\mu_a\mu_b - b)\mu_b+\sim b)]\mu_b = [b\mu_b - (a\mu_a\mu_b + b)\mu_b]\mu_b =$$

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

Set $x := a\mu_a\mu_b$. Then $\mu_x = \mu_a^{\mu_a\mu_b} = \mu_a^{\mu_b}$ and $\mu_{x+b} = \mu_{x\mu_x - b\mu_b} = \mu_{a\mu_a\mu_b\mu_a^{\mu_b} - b\mu_b} = \mu_{a\mu_b - b\mu_b} = \mu_{(a\mu_b - b\mu_b)\mu_b}^{\mu_b}$. By (3.2) we get $\mu_{b+x} = (\mu_b\mu_{a+b}\mu_a)^{\mu_b} = \mu_{a+b}\mu_a\mu_b$. Since all μ-maps are involutions, this implies $\mu_{b+x} = \mu_b\mu_a\mu_{a+b}$. So $a\mu_b\mu_{b+x} = a\mu_b\mu_b\mu_a\mu_{a+b} = a\mu_a\mu_{a+b}$ and thus

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

Since $\mu_{\sim(-\sim a+\sim b)} = \mu_{-\sim a+\sim b} = \mu_{a+b}$, one gets

$$a\mu_a\mu_{a+b} + a\mu_a\mu_b + b = a + b$$

and therefore

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

Now there is an element $g \in H$ with $ag = c$. Since H is abelian, one gets

$$c\mu_a\mu_{a+b} = ag\mu_a\mu_{a+b} = a\mu_a\mu_{a+b}g = (a + a\mu_a\mu_b)g = ag + ag\mu_a\mu_b = c + c\mu_a\mu_b.$$

□

Lemma 5.13 *If $a, b, c \in Z(U)$ are involutions with $a \neq b$, then $-\sim a+\sim b \notin \{c, -\sim c, \sim c\}$.*

Proof. Since $(-\sim a)\cdot 2 = a \neq b = (-\sim b)\cdot 2$, $-\sim a$ and $-\sim b$ lie in different cosets of $U/Z(U)$, hence$-\sim a+\sim b$ cannot be in $Z(U)$. If $-\sim a+\sim b =\sim c$, then $-\sim b+\sim a = -\sim c$, so we only have to show that $-\sim a+\sim b = -\sim c$ cannot hold. Suppose otherwise. Then $\mu_c = \mu_{-\sim c} = \mu_{-\sim a+\sim b} = \mu_{a+b}$ and so $c = a + b$. One has

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

Set $g := \mu_b\mu_{a+b}$ and $h := \mu_{(a\mu_a\mu_b - b)\mu_b}$. Then we have

$$a + b = (a\mu_a\mu_{a+b}^2 - b\mu_b\mu_{a+b}^2)\mu_{a+b} = (a\mu_a\mu_{a+b}^2 - bg\mu_{a+b})\mu_{a+b} =$$

$$(a\mu_a\mu_{a+b} - bg)\mu_{bg} + \sim bg = (a\mu_a\mu_{a+b} - b)g^{-1}\mu_b g + (- \sim b)g =$$
$$((a\mu_a\mu_b - b)\mu_b + \sim b)g = (a\mu_a\mu_b - b)\mu_{a\mu_a\mu_b - b}hg + \sim bg =$$
$$(- \sim (a\mu_a\mu_b - b))hg + (\sim b)g = - \sim ((a\mu_a\mu_b - b)hg) + \sim (bg).$$

But $a + b \in Z(U)$, so $- \sim ((a\mu_a\mu_b - b)hg)$ and $\sim bg$ are contained in the same coset of $U/Z(U)$ This is only possible if $bg = (a\mu_a\mu_b - b)hg$, but this implies $a + b = 0$, a contradiction. □

Lemma 5.14 *Suppose $a, b \in Z(U)$ are involutions and $g, h \in H^*$. Then $- \sim a + \sim (ag) = - \sim b + \sim (bh)$ if and only if $a = b$ and $g = h$.*

Proof. If $- \sim a + \sim ag = - \sim b + \sim bh$, then also $a + ag = b + bh$. Hence

$$\sim a - \sim ag = - \sim a + \sim ag + a + ag = - \sim b + \sim bh + b + bh = \sim b - \sim bh$$

and

$$\sim ag - \sim a = -(\sim a - \sim ag) = -(\sim b - \sim bh) = \sim bh - \sim b.$$

We have

$$(\sim a - \sim ag)\mu_a = ((\sim a)\mu_a - (\sim a)\mu_a g)\mu_a = ((\sim a)\mu_a - (\sim ag^{-1})\mu_a)\mu_a =$$
$$(\sim a - \sim ag^{-1})\mu_{\sim ag^{-1}} + \sim\sim (ag^{-1}) = (\sim a - \sim ag^{-1})g\mu_a g^{-1} + ag^{-1} =$$
$$((\sim ag - \sim a)\mu_a + a)g^{-1} = ((\sim bh - \sim b)\mu_a + a)g^{-1}.$$

Similarly, one computes

$$(\sim b - \sim bh)\mu_a = (\sim b - \sim bh)\mu_b^2\mu_a = ((\sim b)\mu_b - (\sim bh^{-1})\mu_b)\mu_b^2\mu_a =$$
$$((\sim b - \sim bh^{-1})h\mu_b h^{-1} + bh^{-1})\mu_b\mu_a = ((\sim bh - \sim b)\mu_b + b)h^{-1}\mu_b\mu_a$$
$$= ((\sim bh - \sim b)\mu_a + b\mu_b\mu_a)h^{-1}.$$

Therefore $\alpha_a g^{-1} h \alpha_{b\mu_b\mu_a} \in G^\dagger_{\infty,(\sim bh - \sim b)\mu_a}$. Hence there is an element $k \in H$ with

$$\alpha_a g^{-1} h \alpha_{b\mu_b\mu_a} = \alpha_{-(\sim ag - \sim a)\mu_a} k \alpha_{(\sim bh - \sim b)\mu_a}.$$

This element lies in $G^\dagger_\infty = N_{G^\dagger}(U_\infty)$. If we regard the corresponding cosets in $G^\dagger_\infty/U_\infty$, we see that $k = g^{-1}h$. Hence

$$k\alpha_{ak + b\mu_b\mu_a} = k\alpha_{-(\sim a - \sim ag)\mu_a k + (\sim a - \sim ag)\mu_a}$$

and so

$$ak + b\mu_b\mu_a = -(\sim a - \sim g)\mu_a k + (\sim a - \sim ag)\mu_a = [(\sim a - \sim ag)\mu_a, k]^{-1}.$$

Since $ak + b\mu_b\mu_a \in Z(U)$, $(\sim a - \sim ag)\mu_a Z(U)$ is a fixed point of k in $U/Z(U)$. Suppose $k \neq 1$. Then k has no fixed point in $U/Z(U)$ and hence $(\sim a - \sim ag)\mu_a \in Z(U)$. Hence there is an involution c with $\sim a - \sim ag = - \sim c$ and so $\sim a = - \sim c + \sim ag$, a contradiction to **??**. So $k = 1$ and therefore $g = h$. Now we have $a + ag = b + bg$ and therefore $(a + b)g = a + b$. This implies $a = b$. □

Corollary 5.15 *One has the following partition on U:*

$$U = Z(U) \cup \sim Z(U)^{\#} \cup - \sim Z(U)^{\#} \cup \{- \sim a + \sim b; a, b \in Z(U)^{\#}, a \neq b\}.$$

We will call such a partition a *Suzuki partition.*

Proof. The order of the last set is by **??** exactly $(q-1)(q-2)$. By **??** these sets are disjoint.Since $|Z(U)| = q$ their union has order q^2 which is just the order of U. □

From now on, e will be a fixed involution in U and $\tau = \mu_e$.

We will frequently use the next lemma.

Lemma 5.16 *If $g, h \in H$ are different, then*

$$\sim (- \sim eg + \sim eh) = - \sim (eh^2 g^{-1} + eg) + \sim (eh^2 g^{-1} + eh).$$

Proof. Set $a := eh$ and $k := gh^{-1}$. Then with **??**

$$\sim (- \sim eh + \sim eg) = \sim (- \sim ak + \sim a) = (-(a\mu_a k - a\mu_a)\mu_a)\mu_a =$$

$$(-(ak^{-1}\mu_a - a\mu_a)\mu_a)\mu_a = [-((ak^{-1} + a)\mu_a + \sim a)]\mu_a = (a\mu_a - (ak^{-1} + a)\mu_a)\mu_a =$$

$$ak^{-1}\mu_{a+ak^{-1}} + \sim (a + ak^{-1}) = a\mu_a^2 \mu_{a+ak^{-1}} k + \sim (a + ak^{-1}) =$$

$$- \sim (a\mu_a \mu_{a+ak^{-1}})k + \sim (a + ak^{-1}) =$$

$$- \sim (a + a\mu_a k \mu_a k^{-1})k + \sim (a + ak^{-1}) = - \sim (ak + ak^{-1}) + \sim (a + ak^{-1})$$

. Hence we get

$$\sim (- \sim eg + \sim eh) = - \sim (eg + eh^2 g^{-1}) + \sim (eh + eh^2 g^{-1})$$

. □

We are now going to introduce coordinates. By **??**, U is isomorphic to $A(n, \theta)$ with $o(\theta)$ odd. We can label the elements as (a, b) with $a, b \in F := \mathbb{F}_{2^n}$. We can assume that $e = (0, 1)$. By **??** there is an automorphismus ϕ of U which centralizes $Z(U)$ and $U/Z(U)$ such that $H^\phi = \Lambda$ with Λ as in 5.2. Since ϕ centralizes $Z(U)$ and $U/Z(U)$, there is a homomorphism $f : F \to F$ with $(a, b)\phi = (a, b + \phi(a))$. Hence for every $h \in H$ there is a $\lambda \in F^{\#}$ with

$$(a, b)h = (a, b)\phi^{-1} h_\lambda \phi = (a, b + f(a))h_\lambda \phi = (a\lambda, b\lambda^{1+\theta} + f(a)(\lambda^{1+\theta} + 1).$$

Set $u(a, b) := (a, b + f(a)) = (a, b)\phi$. Then $u(a, b)h = (a, b)h_\lambda \phi = (\lambda a, \lambda^{1+\theta} b)\phi = u(\lambda a, \lambda^{1+\theta} b)$. Moreover,

$$u(a, b) + u(c, d) = (a, b + f(a)) + (c, d + f(c)) = (a + c, b + d + f(a) + f(c) + ac^\theta)$$

$$= (a + c, b + d + f(a + c) + ac^\theta) = u(a + b, b + d + ac^\theta).$$

Writing (a, b) instead of $u(a, b)$, we can therefore assume that $H = \Lambda$.

Lemma 5.17 *If $h \in H^*$, then $[\sim e, \sim eh] \neq 1$. Hence θ has no fixed point different from 0 and 1.*

Proof. Let k be the fixed field of θ and let $m \in \mathbb{N}$ such that $a^\theta = a^{2^m}$. In $A(n,\theta)$, an element of the form (x,y) with $x \in k^\#$ commutes with (x',y') if and only if $x' \in k$. Let $a = (0,u)$ and $b = (0,v)$ be involutions. Since $(\sim a)\cdot 2 = a, (\sim b)\cdot 2 = b$, we get $\sim a = (u^{(1+\theta)^{-1}}, x)$ and $\sim b = (v^{(1+\theta)^{-1}}, y)$ with $x, y \in F$. Now $\lambda \mapsto \lambda^{1+\theta}$ induces a bijection of k. Thus if $u \in k$, then $\sim a$ and $\sim b$ commute if and only if $v \in k$.
Suppose that $|k| > 2$ and that $\lambda \in k \setminus \{0,1\}$. Set $h := h_\lambda$ Then $eh = (0, \lambda^{1+\theta}) = (0,\lambda^2)$, hence $\sim e$ and $\sim eh$ commute. It is

$$(- \sim eh + \sim e)\cdot 2 = (- \sim eh)\cdot 2 + (\sim e)\cdot 2 = eh + e \sim (eh+e)\cdot 2,$$

hence $c := - \sim eh + \sim e - \sim (eh+e) \in Z(U)$. Note that $c \neq 0$ by **??**.. Now by **??**

$$(- \sim e + \sim eh)\mu_{e+eh} = - \sim -(- \sim e + \sim eh) = - \sim (- \sim eh + \sim e) =$$

$$-(- \sim (e+eh^2) + \sim (eh+eh^2)) = - \sim (eh+eh^2) + \sim (e+eh^2).$$

But $eh + eh^2 = (0, \lambda^2+\lambda^4)$ and $e + eh^2 = (0, \lambda^4+1)$, therefore
$d := - \sim (eh+eh^2) + \sim (e+eh^2) - \sim (e+eh) \in Z(U)$. Again, $d \neq 0$. Now $d = (- \sim eh + \sim e)\mu_{e+eh} - (\sim (e+eh))\mu_{e+eh}$ and
$c = (- \sim eh + \sim e) - \sim (e+eh)$. By 2.5(1) in [**?**], we get $\mu_c = \mu_d$. But since c and d are involutions, this implies $c = d$ and therefore $(- \sim e + \sim eh)\mu_{e+eh} = - \sim e + \sim eh$. But $\sim (e+eh)$ is the unique fixed point of μ_{e+eh} by **??**. Thus $\sim (e+eh) = - \sim e + \sim eh$ which contradicts **??**. Hence $k = \mathbb{F}_2$ and $C_U(\sim e) = \langle Z(U), \sim e\rangle$. □

Lemma 5.18 *After possibly replacing θ by θ^{-1}, we can assume that $- \sim e = (1,0)$. Then we have $- \sim (0, a^{1+\theta}) = (0,a)$ and $\sim (0,a^{1+\theta}) = (a, a^{1+\theta})$ for all $a \in F^\#$.*

Proof. The first statement is Lemma XI.11.12 in [**?**]. The second holds since $(0, a^{1+\theta}) = eh_a$ and hence $- \sim (0,a^{1+\theta}) = - \sim eh_a = (a,0)$. □

Lemma 5.19 *Let $(a,b) \in U$ with $0 \notin \{a,b\}$ and $b \neq a^{1+\theta}$. Then $(a,b) = (s,0) - (t,0)$ with $t = (\frac{b}{a})^{\theta^{-1}}$ and $s = a - t$.*

Proof. By **??** there are two distinct involutions u and v with $(a,b) = - \sim u + \sim v$. Hence by **??** there are $s, t \in F^\#$ with $(a,b) = (s,0) + (t, t^{1+\theta}) = (s+t, st^\theta + t^{1+\theta})$. Thus $t^\theta = \frac{a}{b}$ and $s = a + t$. □

Lemma 5.20 *For $(a,b) \in U^\#$, set $N_0(a,b) = a^{1+\theta} + a^{\theta-\theta^{-1}} b^{\theta^{-1}} + b$ (the reduced norm of (a,b)). Then $\mu_{(0,N_0(a,b))} = \mu_{(a,b)}$.*

Proof. For $a = 0$, one has $N_0(a,b) = b$. If $a \neq 0, b = 0$ or $b = a^{1+\theta}$, then $N_0(a,b) = a^{1+\theta}$ and the claim is true since $- \sim (0, a^{1+\theta}) = (a, 0)$ and $\sim (0, a^{1+\theta}) = (a, a^{1+\theta})$. If $a \neq 0, b \neq 0, a^{1+\theta}$, then $N_0(a,b) = s^{1+\theta} + t^{1+\theta}$ with s, t as is **??**, and so this case follows by **??**. □

Lemma 5.21 *Let $g, h \in H$. Then*

$$(- \sim eg + \sim eh)\tau = - \sim ej^{-1}h^{-2} + \sim eh^{-1}$$

with $ej = eg^{-1} + eh^{-1}$.

Proof. Let $j \in H$ with $ej = eg^{-1} + eh^{-1}$. Then

$$(- \sim eg + \sim eh)\tau = (e\tau g - e\tau h)\tau = (eg^{-1}\tau - eh^{-1}\tau)\tau = (eg^{-1} + eh^{-1})h\tau h^{-1} + \sim eh^{-1} =$$

$$ej\tau h^{-2} + \sim eh^{-1} = e\tau j^{-1}h^{-2} + \sim eh^{-1} = - \sim ej^{-1}h^{-2} + \sim eh^{-1}.$$

□

Lemma 5.22 *If $a, b \in F^{\#}$ with $b \neq a^{1+\theta}$, then*

(a) $(0, a^{1+\theta})\tau = (a^{-1}, 0)$.

(b) $(a, 0)\tau = (0, a^{-1-\theta})$.

(c) $(a, a^{1+\theta}) = (a^{-1}, a^{-1-\theta})$.

(d) $(a,b)\tau = (\frac{s}{Nt} + \frac{1}{t}, \frac{1}{t^{\theta}}(\frac{s}{Nt} + \frac{1}{t}))$. *with s, t as in* **??** *and $N^{1+\theta} = N_0(a,b)$.*

Proof.

(a) This follows because of $eh_a\tau = e\tau h_a^{-1} = - \sim eh_a^{-1}$.

(b) This holds since $(- \sim e)h_a\tau = (- \sim e)\tau h_a^{-1} = eh_a^{-1}$.

(c) It is $(\sim e)h_a\tau = (\sim e)\tau h_a^{-1} = (\sim e)h_a^{-1}$.

(d) Let s, t be as in **??**. Set $g := h_s$ and $h := h_t$. Then $(a,b) = - \sim eg + \sim eh$ and hence $(a,b)\tau = - \sim ej^{-1}h^2 + \sim eh^{-1}$ with $ej = eg^{-1} + eh^{-1}$. Therefore $ej^{-1} = (0, (st)^{1+\theta}N_0(a,b)^{-1})$ and so $ej^{-1}h^{-2} = (0, s^{1+\theta}t^{-1-\theta}N_0(a,b)^{-1})$ and $- \sim (ej^{-1}h^{-2}) = (st^{-1}N^{-1}, 0)$. We get

$$(a,b)\tau = (st^{-1}N^{-1}, 0) + (t^{-1}, t^{-1-\theta}) = (\frac{s}{Nt} + \frac{1}{t}, \frac{1}{t^{\theta}}(\frac{s}{Nt} + \frac{1}{t})),$$

□

Lemma 5.23 *θ is a Tits automorphism.*

Proof. For all $h \in H^*$, one has

$$(\sim eh- \sim e)\tau = ((\sim eh^{-1})\tau - (\sim e)\tau)\tau = (\sim eh^{-1}- \sim e)\tau + e.$$

For $a \in F \setminus \{0,1\}$ and $h = h_a$, this means

$$(a+1, a(a^\theta+1))\tau = (a^{-1}+1, a^{-1}(a^{-\theta}+1))\tau + (0,1).$$

There are uniquely determined elements $s,t,u,v \in F^\#$ with $(a+1, a(a^\theta+1)) = (s,0)-(t,0)$ and $(a^{-1}+1, a^{-1}(a^{-\theta}+1)) = (u,0)-(v,0)$. One computes

$$t = a^{\theta^{-1}}(a+1)(a^{\theta^{-1}}+1)^{-1}, s = a^{-\theta^{-1}}t, v = a^{-1-\theta^{-1}}t$$

and

$$u = (a^{-1}+1) + v = a^{-1}(a+1) + a^{-1}s = a^{-1}t.$$

Set $N = (s^{1+\theta}+t^{1+\theta})^{(1+\theta)^{-1}}$ and $M = (u^{1+\theta}+v^{1+\theta})^{(1+\theta)^{-1}}$. Then $M = a^{-1}N$ and $N^{1+\theta} = (1+a^{-1-\theta^{-1}})t^{1+\theta}$. By **??**, we have

$$(sN^{-1}t^{-1}+t^{-1}, sN^{-1}t^{-1-\theta}+t^{-1-\theta}) = (uM^{-1}v^{-1}+v^{-1}, uM^{-1}v^{-1-\theta}+v^{-1-\theta}+1)$$

and hence

$$a^{-\theta^{-1}}N^{-1} + t^{-1} = a^{1+\theta^{-1}}N^{-1} + a^{1+\theta^{-1}}t^{-1}.$$

This implies

$$(a^{-\theta^{-1}} + a^{1+\theta^{-1}})t = (a^{1+\theta^{-1}}+1)N.$$

Thus

$$N = a^{-\theta^{-1}}(a^{2\theta^{-1}+1}+1)(a^{1+\theta^{-1}}+1)^{-1}t.$$

Therefore we get

$$(1+a^{-1-\theta^{-1}})t^{1+\theta} = N^{1+\theta} = a^{-1-\theta^{-1}}(a^{2\theta^{-1}+1}+1)(a^{2+\theta}+1)(a^{1+\theta^{-1}}+1)^{-1}(a^{\theta+1}+1)^{-1}t^{1+\theta}$$

and so

$$a^{1+\theta^{-1}}(1+a^{-1-\theta^{-1}})(1+a^{1+\theta^{-1}})(1+a^{1+\theta}) = (a^{2\theta^{-1}+1}+1)(a^{2+\theta}+1).$$

Hence

$$(1+a^{1+\theta^{-1}})^2(1+a^{1+\theta}) = a^{3+2\theta^{-1}+\theta} + 1 + a^{2\theta^{-1}+1} + a^{2+\theta}$$

and

$$1 + a^{2+2\theta^{-1}} + a^{1+\theta} + a^{3+2\theta^{-1}+\theta} = a^{3+2\theta^{-1}+\theta} + 1 + a^{2\theta^{-1}+1} + a^{2+\theta}.$$

We get

$$a^{2+2\theta^{-1}} + a^{1+\theta} = a^{2+\theta} + a^{2\theta^{-1}+1}$$

and so

$$a(a+1)a^{2\theta^{-1}} = a(a+1)a^\theta.$$

Since $a \neq 1$, this implies $a^{2\theta^{-1}} = a^\theta$ and hence $a^2 = a^{\theta^2}$. □

Proof of Theorem ?? By **??**, U is isomorpic to $A(n,\theta)$ with $|U| = 2^n$ and by **??** θ a Tits automorphism. Therefore it remains to show that $(a,b)\tau = (\frac{b}{N(a,b)}, \frac{a}{N(a,b)})$ with $N(a,b) = a^{2+\theta} + ab + b^\theta = N_0(a,b)^\theta$. If $a = 0$, then $N(0,b) = b^\theta$. By **??**, $(0,b)\tau = (b^{-(\theta+1)^{-1}}, 0) = (b^{-\theta+1}, 0) = (\frac{b}{b^\theta}, 0) = (\frac{b}{N(0,b)}, \frac{a}{N(0,b)})$. If $b = 0$, then $N(a,0) = a^{2+\theta}$ and by **??**,

$$(a,0)\tau = (0, a^{-1-\theta}) = (0, \frac{a}{a^{2+\theta}}) = (\frac{0}{N(a,b)}, \frac{a}{N(a,b)}).$$

If $b = a^{1+\theta}$, then

$$N(a,b) = a^{2+\theta} + aa^{1+\theta} + a^{\theta^2+1} = a^{2+\theta}$$

and

$$(a,b)\tau = (a^{-1}, a^{-1-\theta}) = (\frac{a^{1+\theta}}{a^{2+\theta}}, \frac{a}{a^{2+\theta}}) = (\frac{b}{N(a,b)}, \frac{a}{N(a,b)}).$$

. If $a, b \neq 0$ and $b \neq a^{1+\theta}$, then

$$(a,b)\tau = (\frac{S}{Nt} + \frac{1}{t}, \frac{1}{t^{\theta-1}}\frac{s}{Nt} + \frac{1}{t})$$

with $t = (\frac{b}{a})^{\theta^{-1}}$, $s = a + t$ and $N^{1+\theta} = N_0(a,b) = N(a,b)^{\theta^{-1}}$. Since $(1+\theta)^{-1} = 1 - \theta$, one has

$$N = (N(a,b)^{\theta^{-1}})^{\theta-1} = N(a,b)^{1-\theta^{-1}}.$$

One computes

$$st^{-1} = (a + a^{1-\theta^{-1}}b^{-\theta^{-1}})a^{\theta^{-1}}b^{-\theta^{-1}} = a^{1+\theta^{-1}}b^{-\theta^{-1}} + 1$$

and

$$N(a,b)^{\theta^{-1}}st^{-1} = (a^{1+\theta^{-1}}b^{-\theta^{-1}} + 1)(a^{1+\theta} + a^{\theta^{-1}}b^{\theta^{-1}} + b) =$$
$$a^{2+\theta+\theta^{-1}}b^{-\theta^{-1}} + a^{1+2\theta^{-1}} + a^{1+\theta^{-1}}b^{1-\theta^{-1}} + a^{1+\theta} + a^{\theta^{-1}}b^{\theta^{-1}} + b =$$
$$a^{\theta^{-1}}b^{-\theta^{-1}}(a^{2+\theta} + ab + b^{2\theta^{-1}}) + b + a^{1+\theta} + a^{1+2\theta^{-1}} = \frac{1}{t}N(a,b) + b.$$

Thus

$$\frac{s}{Nt} + \frac{1}{t} = \frac{1}{N(a,b)}(\frac{1}{t}N(a,b) + b) + \frac{1}{t} = \frac{b}{N(a,b)}$$

and

$$\frac{1}{t^\theta}(\frac{s}{Nt} + \frac{1}{t}) = \frac{a}{b}\frac{b}{N(a,b)} = \frac{a}{N(a,b)}.$$

*□

6 Generalized Suzuki Moufang sets

If $M(U,\tau)$ is a finite Suzuki Moufang set, then we have seen that the following holds:

(a) H is transitive on $Z(U)^\#$.

(b) For every $a \in U^\#$ there is a $b \in U^\#$ with $\mu_a = \mu_b$.

(c) U has a Suzuki partition, that means

$$U^\# = Z(U) \cup \sim Z(U)^\# \cup - \sim Z(U)^\# \cup \{- \sim a + \sim b; a, b \in Z(U)^\#, a \neq b\}.$$

In the infinite case, one can generalize the concept of Suzuki Moufang sets. It turns out that a generalized Suzuki Moufang set $M(K, L, \theta)$ is an 'ordinary' Suzuki Moufang set (that means θ bijective and hence $K = L = K^\theta$) if and only if one of these conditions holds in which case all of them hold.

Theorem 6.1 *Let K be a field of characteristic 2. θ a Tits endomorphism, $k = K^\theta$ and L a k-subspace of K with $1 \in L$ and $k[L] = K$. Let $M(U,\tau)$ be the generalized Suzuki Moufang set as defined in 5.5. Then the following statements are equivalent.*

(a) θ is surjective.

(b) K is perfect

(c) U has a Suzuki partition.

(d) H acts transitively on $Z(U)^\#$.

(e) For every $a \in U^\#$ there is a $b \in Z(U)^\#$ with $\mu_a = \mu_b$.

Proof. It is clear that (a) and (b) are equivalent since θ^2 is the Frobenius endomorphism. Moreover, we have $(0,x)\tau\mu_{(a,b)} = (0, N(a,b)^\theta x)$ for $a, b, x \in L, (a,b) \neq (0,0)$. Since $H = \langle \tau\mu_{(a,b)}; (a,b) \in U^\# \rangle$ one sees immediately that (d) implies (a). Since $N(0,a) = a^\theta$ and thus $(0,x)\tau\mu_{(0,a)} = (0, a^2 x)$ for $a, x \in L, a \neq 0$ we conclude that (d) follows from (b). We show (e) implies (a). Let $a \in L^\#$. Then there is $b \in L$ with $\mu_{(1,a)} = \mu_{(0,b)}$. This implies $1 + a^\theta + a = N(1,a) = N(0,b) = b^\theta$, thus $a = (b + a + 1)^\theta \in K^\theta$. Since L generates K as a ring, this implies $K = K^\theta$.

Next we show that (c) follows from (a). If $a, b \in L$ with $a \neq 0, b \neq 0, b \neq a^{1+\theta}$, then $(a,b) = - \sim (0,r) + \sim (0,s)$ with $s = (\frac{a}{b})^{\theta^{-1}}, r = a + s$.

Finally we show that (c) implies (e). We only have to show that if $(a,b) = - \sim (0,r) + \sim (0,s)$ with $r, s \neq 0, r \neq s$, then there is a $c \in L$ with $\mu_{(a,b)} = \mu_{(0,c)}$. One has $(a,b) = (r+s, (r+s)s^\theta$ and thus $N(a,b) = (r+s)^{2+\theta} + (r+s)^2 s^\theta + s^2 (r+s)^\theta = (r^2 + s^2) r^\theta + r^\theta s^2 + s^{2+\theta} = r^{2+\theta} + s^{2+\theta} = (r^{1+\theta} + s^{1+\theta})^\theta = N(0, r^{1+\theta} + s^{1+\theta})$. □

References

[1] T. De Medts, Y. Segev, Identities in Moufang Sets, Trans. Am. Math. Soc. 360, No. 11 (2008), 5831-5852.

[2] T. De Medts, Y. Segev, A course in Moufang Sets, to appear in Innovations of Incidence Geometry

[3] T. De Medts, Y. Segev, Finite special Moufang sets of even characteristic, Commun. Contempt. Math. 10, No 3, 449-454

[4] T. De Medts, Y. Segev, K. Tents, Special Moufang sets, their root groups and their μ-maps, Proc. London Math. Soc. (3) 96 (2008), 767-791

[5] T. De Medts, R. M. Weiss, Moufang sets and Jordan division algebras, Math. Ann. 335 (2006), No. 2, 415-433

[6] W. Feit, On a class of doubly transitve permutation groups, Illinois J. Math. 4, 170-186 (1960)

[7] M. Grüninger, Special Moufang Sets with Abelian Hua subgroup, Journal of Algebra 323, No. 6, 1797-1801

[8] D. Gorenstein, J. H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I, II, III, J. Algebra 2, 85-151, 218-270, 354-393 (1965).

[9] B. Huppert, N. Blackburn, Finite Groups II, Springer Verlag, Berlin Heidelberg New York, 1982

[10] B. Huppert, N. Blackburn, Finite Groups III, Springer Verlag, Berlin Heidelber New York, 1982

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

[12] Ito, N., On a class of doubly transitive permutation groups, Ill. J. Math. 6, 341-352 (1962)

[13] Y. Segev, Proper Moufang Sets with abelian Root Groups are special, J. Amer. Math. Soc. 22 (2009), 889-908.

[14] Y. Segev, Finite special Moufang sets of odd characteristic, Commun. Contemp. Math. 10, No. 3, 455-475 (2008).

[15] M. Suzuki, On a class of doubly transitive groups, Ann. of Math. 75, 104-145 (1962)

[16] M. Suzuki, On a class of doubly transitive groups II, Ann. of Math. 79, 514-589 (1964)

[17] F. G. Timmesfeld, Abstract root subgroups and simple groups of Lie-type, Birkhäuser, Monographs in Mathematics. 95, Basel, 2001

[18] J. Tits, Twin buildings and groups of Kac-Moody type, *Groups, combinatorics and geometry*, Durham, 1990, London Mathematical Society Lecture Notes Series 165, (Cambridge University Press, Cambridge 1992) 249-286

[19] H. Van Maldeghem, Moufang lines defined by (generalized) Suzuki groups, Eur. J. Comb. 28, No. 7, 1878-1889 (2007)