The maximal subloops of the simple Moufang loop of order 1080

A. N. Grichkov*
M. L. Merlini Giuliani†
A. V. Zavarnitsine‡

Abstract

We prove that the maximal subloops of the simple Moufang Loop of order 1080 have orders 120 and 108 and are unique up to isomorphism.

1 Introduction

Let $\mathcal{Z}(q)$ be an alternative 8-dimensional simple algebra over a finite field $\mathbf{F}_q$, $q = p^n$. In [2], M.Liebeck proved that every finite simple non-associative loop is isomorphic to loop $PSL(\mathcal{Z}(q))$, where, for any algebra A with multiplicative norm $N : A \to K$, K a field, we denote by $PSL(A)$ the loop

$$PSL(A) = \{x \in A \mid N(x) = 1\}/C(A^*),$$

where $C(A^*)$ is the center of A^*.

The loop $PSL(\mathcal{Z}(2))$ has order 120 and is the minimal non-associative finite simple Moufang loop. This loop contains two classes of maximal subloops [9]: $M(S_3, 2)$ and $M(A_4, 2)$. We use the standard notation: S_3 (A_4) is the group of (even) permutations on 3 (4) symbols, for any non-abelian group

*supported by FAPESP and CNPq, Brazil
†supported by FAPERGS, Brazil, Proc. 01/0295.2
‡supported by FAPESP, Brazil, Proc. 01/14811.4, and RAS, Russia, grant N7, 6th competition for young scientists

G, $M(G,2) = G \cup Gx$, $x^2 = 1$ and $xgx = g^{-1}$, for any $g \in G$, is the Chein's duplication of G (see [6]).

The main result of this paper is a description of all maximal subloops in the simple Moufang loop $PSL(\mathcal{Z}(3))$, which we denote by L. It is well known that L contain a subloop $PSL(\mathcal{Z}(2))$ [1]. On the other hand, the algebra $\mathcal{Z}(3)$ contains a maximal 6-dimensional subalgebra $A = M_2(\mathbf{F}_3) \oplus V$, where $V \cdot V = 0$ and V is an alternative $M_2(\mathbf{F}_3)$-bimodule. The corresponding subloop $PSL(A)$ is a non-associative loop with 108 elements. We denote this loop by M_{108}. Now we can formulate the main result of this paper:

Theorem 1.1 *The subloops $PSL(\mathcal{Z}(2))$ and M_{108} are the unique, up to isomorphism, maximal subloops of the simple Moufang loop $PSL(\mathcal{Z}(3))$.*

The proof of this theorem consists of two parts. In the first part, we prove that every maximal subloop M of L has one of the order 108, 120, 24, or 8. For showing this, we use the connection between the groups with triality and Moufang loops discovered by G.Glauberman [3] and S.Doro [4].

A group G possessing automorphisms ρ and σ such that $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ is called a *group with triality (relative to ρ and σ)* if the following relation holds for every x in G:

$$[x, \sigma] \cdot [x, \sigma]^{\rho} \cdot [x, \sigma]^{\rho^2} = 1, \qquad (1.1)$$

where $[x, y] = x^{-1}y^{-1}xy$. We denote $S = \langle \rho, \sigma \rangle$. The triality is called *non-trivial* if $S \neq 1$. The most interesting situation is when S is isomorphic to the symmetric group S_3 in which case the relation (1.1) does not depend on the particular choice of the generators ρ and σ of S (see [4]) and we will thus speak of a group with triality S.

Let G be an arbitrary group with triality. Then the set $M = \{[x, \sigma\rho] \mid x \in G\}$ is a section of the left coset space $G : C_G(\sigma)$ and the composition $m_1 \cdot m_2 = \pi(m_1 m_2)$, where π is the projection onto M parallel to $C_G(\sigma)$, endows M with the structure of a Moufang loop (see [4]). We denote this loop by $M(G)$ and note that $|M(G)| = |G : C_G(\sigma)|$.

It is well known [2] that, for the Moufang loop L=$PSL(\mathcal{Z}(3))$, the corresponding simple group with triality is $O_8^+(3) = G$.

We proved that, for every subloop $L_0 \subset L$ there exist an S_3-invariant subgroup $G_0 \subset G$ such that $M(G_0)$=L_0. This implies that, for any maximal subloop $L_0 \subset L$, there exists a maximal S_3-invariant subgroup $G_0 \subset G$.

Then we use the classification of maximal S_3-invariant subgroups obtained by P.Kleidman [5]. The study of maximal S_3-invariant subgroups of G and calculation of the order of the corresponding Moufang loop gives the following result:

Proposition 1.2 *Let L_0 be a maximal subloop of $L = PSL(\mathcal{Z}(3))$. Then the order $|L_0|$ of L_0 is one of the numbers* 120, 108, 24, *or* 8.

In the second part, we prove the following proposition:

Proposition 1.3 *1.Every subloop L_0 of L of order 8 is isomorphic to the group $Z_2 \times Z_2 \times Z_2$ and can be embedded in some subloop $M(A_4, 2) \subset L$ of order* 24.

2.Every subloop L_0 of L of order 24 *is isomorphic to the (nonassociative) Moufang loop $M(A_4, 2)$ and can be embedded in some subloop M_{120} of order* 120.

It is clear that Theorem 1.1 follows from Proposition 1.2 and 1.3.

2 Proof of Proposition 1.2.

By definition, $G = O_8^+(3) \cong \Omega_8^+(3)/C(\Omega_8^+(3))$, where $\Omega_8^+(3) = GO_8^+(3)'$ and $GO_8^+(3)$ is the group of 8×8 matrices which preserve a nondegenerate quadratic form Q with discriminant $D(Q) = 1$ (see[5], definition (2.5.14)). G is isomorphic to the group of Lie type $D_4(3)$, which is a group with triality with respect to its graph automorphism group isomorphic to S_3. The corresponding Moufang loop $L = PSL(\mathcal{Z}(3))$ has order 1080 [2].

If $G_0 \subset G$ is an S_3-invariant subgroup in G then the corresponding Moufang loop $M(G_0)$ is a subloop of L and the order of $M(G_0)$ is equal to $| G_0 : C_{G_0}(\sigma) |$. If $L_0 \subset L$ is some maximal subloop of L then there exists a maximal S_3-invariant subgroup in G_0 such that $M(G_0) = L_0$ (see [10]).

Let G_0 be a maximal S_3-invariant subgroup in $G = O_8^+(3)$. Then the semidirect product $G_0 \cdot S_3$ is a maximal subgroup of $G \cdot S_3$. In [5], P.Kleidman classified all such subgroups. We give a list of all maximal S_3-invariant subgroup in G in the notation of [5].

1. P_2, 2. R_{s2}, 3. G_2^1, 4. N_1, 5. N_4, 6. I_+4, 7. $\Omega_8^+(2)$. $(\star)$

If a subgroup $P_i, i \in \{1, ..., 7\}$ in this list is a group with triality, we denote by M_i the corresponding Moufang loop. Then Proposition 1.2 is a corollary of the following assertion:

Proposition 2.1 *The Moufang loops $M_1, M_2, ..., M_7$ have the following orders:* $|M_1| = 27,\quad |M_2| = 108,\quad |M_3| = 1,\quad |M_4 = 2\quad |M_5| = 8,\quad |M_6| = 24,\quad |M_7| = 120.$

Proof. For reader's convenience we present here a proof of this proposition, because the main theorem in [10] simplifies significantly in the case $q = 3$.

By definition, a subgroup $S' \simeq S_3$ of $G \cdot S$ is called a triality complement of G if $G \cdot S \cong G \cdot S'$ and G is a group with triality with respect to S'. An involution $\tau \in G \cdot S \setminus G$ is triality involution if it lies in some triality complement of G. By [2], all triality complements are conjugated. In particular, all triality involutions are conjugated in $G_1 \overset{df}{=} G\langle\sigma\rangle$. Let V be an 8-dimensional $\mathbf{F}_3$-space equipped with a non-degenerated quadratic form Q with discriminant 1. For a vector $v \in V$ with $Q(v) \neq 0$, denote by r_v the reflection in the hyperplane $V_v = \{w \in V \mid (v, w) = 0\}$, where $(\cdot, \cdot)$ is the bilinear form associated with Q. Then $\bar{r}_v$ is a triality involution (see p.182 in [5]), where $\bar{a}$ for $a \in GO_8^+(3)$ denotes the image of a in $PGO_8^+(3)$. Note that $G_1 \setminus G$ has two classes of involutions with representatives $\bar{r}_v$ and $\tau = r_{v_1} r_{v_2} r_{v_3}$, where $(v_i, v_j) = \delta_{ij}$, $i, j = 1, 2, 3$. Since $|C_G(\bar{r}_v)| \neq |C_G(\tau)|$, it follows that that all triality-involutions have the form $\bar{r}_v$ for some reflection r_v in a vector v such that $Q(v)$ is a square in $\mathbf{F}_3^*$.

Let G_0 be one of the groups from the list ($\star$). If $N = N_{GS}(G_0)$ contains a triality involution $\sigma = \bar{r}_v$, then the order of the corresponding loop is $|G_0 : C_{G_0}(\sigma)| = |\widehat{G}_0 : C_{\widehat{G}_0}(r_v)|$, where $\widehat{G}_0$ is the preimage of G_0 in $GO_8^+(3)$.

Now we consider all the possibilities for G_0 case by case.

1. G_0=P_2. In this case, G_0 is a parabolic subgroup which normalizes three totally singular (t.s.) subspaces $U, R, T \subseteq V$ such that $U \subseteq R \cap T$, $\dim U = 1$, $\dim R = \dim T = 4$, $\dim R \cap T = 3$. Every t.s. 3-dimensional subspace lies in exactly two t.s. 4-dimensional subspaces which are permuted by a reflection r_v $GO_8^+(3)$. Hence, $N = N_{GS}(G_0)$ contains triality-involution $\bar{r_v}$. Note that the index $t = |\widehat{G_0} : C_{\widehat{G_0}}(r_v)|$ is equal to the number of involutions in $\widehat{G}_0\langle r_v\rangle$ conjugate to r_v.

Since $\widehat{G}_0 = N_{\Omega_8^+(3)}(G_0)(U, R \cap T)$, we have $r_v \in N_{GS}(G_0)$ if and only if $v \in U^\perp \cap (R \cap T)^\perp$=$(R \cap T)^\perp$. Hence, $t = |\{v \in (R \cap T)^\perp \mid Q(v) = 1\}|$ is the number of nonsingular $+1$-subspaces of $(R \cap T)^\perp$, i.e. 1-dimensional subspaces spanned by vectors v such that $Q(v)$ is a square in $\mathbf{F}_3^*$. Choose a standard basis in V: $\{e_1, ...e_4; f_1, ...f_4\}$ such that (e_i, e_j)=(f_i, f_j)=0, (e_i, f_j)=δ_{ij}; $i, j = 1, ...4$. Without lost of generality we can take $R = \langle e_1, ..., e_4\rangle$ and $T = \langle e_1, e_2, e_3, f_4\rangle$. Then $(R \cap T)^\perp = \langle e_1, ..., e_4, f_4\rangle$ and, given a $v \in (R \cap T)^\perp$, we have $Q(v) = \alpha\beta$ if $v = \alpha e_4 + \beta f_4 + v_0$, $v_0 \in \langle e_1, e_2, e_3 \rangle$. Then the number of non-singular vectors in $(R \cap T)^{\perp}$ is equal to 108, number of non-singular 1-subspaces is 54 and $t = 27$.

2. $G_0 = R_{s2}$. In this case, G_0 is a parabolic subgroup which normalizes a t.s. 2-subspace U. We may assume that $U = \langle e_1, e_2 \rangle$. Since $v = e_3 + f_3 \in U^{\perp}$ and $Q(v) = 1$, it follows that $N = N_{GS}(G_0)$ contains the triality-involution $\bar{r}_v$. As in the case (1), the order of $M(G_0)$ is equal to number of non-singular +1-subspaces in $U^{\perp}$. For a vector $v \in U^{\perp}$, which we write as $v = ae_3 + bf_3 + \alpha e_4 + \beta f_4 + v_0$, with $v_0 \in \langle e_1, e_2 \rangle$, we have $Q(v) = ab + \alpha\beta$ Therefore, in this case, the number of non-singular +1-subspaces in $U^{\perp}$ is equal to 108.

3. $G_0 = G_2^1$. Since $C_G(S) \simeq G_2(3)$ ([5], Proposition 3.1.1), we have $|G_0 : C_{G_0}(\sigma)| = 1$.

4. $G_0 = N_1$. Let W be a 4-dimensional space over $\mathbf{F}_9 \supset \mathbf{F}_3$ with a unitary non-degenerate form f. Choose a basis $\{w_1, ...w_4\}$ of W such that $f(w_i, w_j) = \delta_{ij}$, $1 \leq i, j \leq 4$. Denote $W_i = \langle w_i \rangle$, $i = 1, \ldots, 4$, $W_0 = W_1^{\perp} = \langle w_2, w_3, w_4 \rangle$. The space W can be regarded an 8-dimensional $\mathbf{F_3}$-space W^* with the quadratic form $Q^*(v) \stackrel{df}{=} f(v, v)$. Then (W^*, Q^*) is an orthogonal nondegenerate geometry of sign +. Since the spaces (W^*, Q^*) and (V, Q) are isometric, this gives an embedding: $\varphi : GU_4(3) \mapsto GO_8^+(3)$.

Take a subgroup of $GU_4(3)$ isomorphic to $GU_1(3) \times GU_3(3)$ and consider the image $N = \varphi(GU_1(3) \times GU_3(3))$. The space V has a basis in which the elements of N have the block diagonal form $\left(\begin{smallmatrix} A & \\ \cdot & B \end{smallmatrix} \right)$, where $A \in GU_1(3) \subseteq GO_2^-(3) = GO(W_1^*)$, $B \in GU_3(3) \subseteq GO_6^-(3) = GO(W_0^*)$. Note that $A = \varphi(GU_1(3)) \simeq Z_4$. Denote by η_1 the subgroup of order 2 in $\bar{A}$. Let $\widehat{N_1}$ be a subgroup in $\Omega_8^+(3)$ generated by $N \cap \Omega_8^+(3)$ and $\delta \stackrel{df}{=} r_{w_1} r_{w_2} r_{w_3} r_{w_4}$. Denote by N_1 the image of $\widehat{N_1}$ in G. We show that N_1 is an N_1-subgroup in the sense of the definition on page 221 in [5], i.e., that $N_1 = R \cap F$, where R is an $R_{-2} - subgroup$, F is an F_2-subgroup, and $[\eta(R), \eta(F)] = 1$ (see [5], p. 221). It is obvious that $N_1 \subseteq R \stackrel{df}{=} N_G(W_1^*)$ and $\eta(R) = \eta_1$. Moreover, $N_1 \subset F \stackrel{df}{=} N_{\Omega_8^+(3)}(\varphi(SU_4(3))$ and $\eta(F) = \overline{\varphi(C(GU_4(3))} = \eta_2$. Since $[\eta_1, \eta_2] = 1$, it follows that N_1 lies the N_1-subgroup $R \cap F$. The equality of the orders $|N_1| = |R \cap F|$ implies $N_1 = R \cap F$.

We can thus assume that G_0 is the subgroup N_1 constructed above. Since $[r_{w_1}, N] \subseteq N$, $[r_{w_1}, \Omega_8^+(3)] \subseteq \Omega_8^+(3)$, and $[r_{w_1}, \delta] = 1$, we see that $N_{GS}(G_0)$ contains the triality involution $\bar{r}_{w_1}$. We have $|\widehat{G_0} : C_{\widehat{G_0}}(r_{w_1})| = |N : C_N(r_{w_1})| =$

$|A : C_A(r_{w_1})|$. The group $A\langle r_{w_1}\rangle$ is isomorphic to the dihedral group D_8; hence, $|A : C_A(r_{w_1})| = 2$.

5. $G_0 = N_4^4$.

Let $\beta = \{v_1, ...v_8\}$ be an orthonormal basis of V and let $\widehat{P}$ be the elementary abelian subgroup of $\Omega_8^+(3)$ of order 16 generated by the diagonal matrices:
$-\mathbf{1} = diag(-1, -1, -1, -1, -1, -1, -1, -1)$,
$x = diag(1, 1, 1, 1, -1, -1, -1, -1)$,
$y = diag(1, 1, -1, -1, 1, 1, -1, -1)$,
$z = diag(1, -1, 1, -1, 1, -1, 1, -1)$.
Let P be the image of $\widehat{P}$ in G. Then, by definition, an N_4^4-subgroup G_0 of G is conjugate to the normalizer of P in G. Note that $\widehat{G_0} = N_{\Omega_8^+(3)}(\widehat{P})$. Since $N_{G\Omega_8^+(3)}(\widehat{P})$ consists of monomials matrices in the basis β, and every reflection has a single eigenvalue -1, while all other eigenvalues equal to $+1$, it can be shown that the only reflections that normalize β are $r_{v_i}, v_i \in \beta$. But $\widehat{G}_0$ acts transitivly on β; hence, $|\widehat{G_0} : C_{\widehat{G_0}}(r_{v_i})| = 8$.

6. $G_0 = I_{+4}$.

Let $V = V_1 \oplus V_2$ be a decomposition of V into the sum of two $+4$-spaces V_1 and V_2. A reflection r_v normalizes this decomposition if and only if r_v normalizes each V_i, $i = 1, 2$. This means that $v \in V_1$ or $v \in V_2$. It is well known that the number of reflections r_v in $GO_4^+(3)$ corresponding to vectors v with $Q(v) = 1$ is equal to 12 and all these reflections are conjugated in $GO_8^+(3)$. Thus, the number of reflections in $GO_8^+(3)$ that normalize the decomposition $V = V_1 \oplus V_2$ is equal to 24 and all these reflections are conjugate in $\widehat{I}_4$.

7. $G_0 = \Omega_8^+(2)$. It is well known that the Moufang loop corresponding to an S_3-invariant subgroup $\Omega_8^+(2)$ is the simple Moufang loop of order 120 (see [4]).

3 Proof of Proposition 1.3.

We recall the realization of $\mathcal{Z}(q)$ as the set of Zorn matrices

$$\begin{bmatrix} \alpha & \mathbf{v} \\ \mathbf{w} & \beta \end{bmatrix}, \alpha, \beta \in \mathbf{F}_q, \mathbf{v}, \mathbf{w} \in \mathbf{F}_q^3,$$

with the following multiplication:

$$\begin{bmatrix} \alpha & \mathbf{v} \\ \mathbf{w} & \beta \end{bmatrix} \cdot \begin{bmatrix} \gamma & \mathbf{u} \\ \mathbf{r} & \tau \end{bmatrix} = \begin{bmatrix} \alpha\gamma + \mathbf{v} \cdot \mathbf{r} & \alpha\mathbf{u} + \tau\mathbf{v} - \mathbf{w} \times \mathbf{r} \\ \gamma\mathbf{w} + \beta\mathbf{r} + \mathbf{v} \times \mathbf{u} & \beta\tau + \mathbf{w} \cdot \mathbf{u} \end{bmatrix},$$

where $\mathbf{v} = (v_1, v_2, v_3)$,$\mathbf{w} = (w_1, w_2, w_3) \in \mathbf{F}_q^3$, $\mathbf{v} \cdot \mathbf{w} = v_1w_1 + v_2w_2 + v_3w_3$, $\mathbf{v} \times \mathbf{w} = (v_2w_3 - v_3w_2, v_3w_1 - v_1w_3, v_1w_2 - v_2w_1)$.

It is known that $C(\mathcal{Z}(q)) = \{E, -E\}$, where E is the identity matrix. We will use the following notation: $L = PSL(\mathcal{Z}(3))$; $x \equiv y$ if $x = y \in L$ or $x = \pm y \in \mathcal{Z}(3)$. For any $X \subseteq L$, we denote by $Alg(X)$ the subalgebra of $\mathcal{Z}(3)$ generated by the preimage of X in $\mathcal{Z}(3)$ and by $G(X)$ the subloop of L generated by X. We will identify the elements with norm 1 from $\mathcal{Z}(3)$ with their images in L. Denote $\mathbf{i} = (1, 0, 0)$, $\mathbf{j} = (0, 1, 0)$, $\mathbf{k} = (0, 0, 1)$. We note that any non-identity element of L has order 2 or 3.

Lemma 3.1 *Let* $x_1 = \begin{bmatrix} 0 & \mathbf{i} \\ -\mathbf{i} & 0 \end{bmatrix}$, $x_2 = \begin{bmatrix} 0 & \mathbf{j} \\ -\mathbf{j} & 0 \end{bmatrix}$, $x_3 = \begin{bmatrix} 0 & \mathbf{k} \\ -\mathbf{k} & 0 \end{bmatrix}$. *Then, for a given* $i \in \{1, 2, 3\}$, *the element* $z = \begin{bmatrix} \alpha & \mathbf{v} \\ \mathbf{w} & \beta \end{bmatrix} \in L$ *satisfies* $[x_i, z] \equiv 1$ *if and only if either* $z \equiv x_i$, *or* $z \equiv E$, *or* $\alpha + \beta = 0$ *and* $v_i = w_i$.

Proof. Obvious.

Lemma 3.2 *The group* $Aut(L)$ *acts transitively on the sets* $P_2 = \{x \not\equiv 1 \mid x^2 \equiv 1\}$ *and* $P_3 = \{x \not\equiv 1 \mid x^3 \equiv 1\}$. *The group* $Aut(\mathcal{Z}(3))$ *acts transitivly on the set* $\{A \mid A \simeq M_2(\mathbf{F}_3) \subseteq \mathcal{Z}(3)\}$.

Proof. These facts are well-known.

Lemma 3.3 *Let* x, y *be non-identity elements of* L *such that* $x \not\equiv y$ *and* $x^2 \equiv y^2 \equiv [x, y] \equiv 1$. *Then* $Alg(x, y) \simeq M_2(\mathbf{F}_3)$.

Proof. Since all elements of order 2 are conjugate, we may assume that $x = \begin{bmatrix} 0 & \mathbf{i} \\ -\mathbf{i} & 0 \end{bmatrix}$. By Lemma 3.1, we have $y = \begin{bmatrix} \alpha & \mathbf{v} \\ \mathbf{w} & -\alpha \end{bmatrix}$, $v_1 = w_1$. We have $xy = \begin{bmatrix} v_1 & -\alpha\mathbf{i} + \mathbf{i} \times \mathbf{w} \\ -\alpha\mathbf{i} + \mathbf{i} \times \mathbf{v} & -v_1 \end{bmatrix} = -yx$. It is clear that $A = Alg(x, y)$ has a basis $\langle E, x, y, xy \rangle$ and A is a simple 4-dimensional algebra. It is easy to see that $(-E-x-y)^2 = E+x^2+y^2+2x+2y+xy+yx = -E - x - y$ and $det(E + x + y) = 0$. Hence, A is a splitting algebra and $A \simeq M_2(\mathbf{F}_3)$.

Corollary 3.4 *Let*

$$\mathcal{A}_2 = \{(x, y) = (y, x) \mid x, y \in L,\ x^2 \equiv y^2 \equiv [x, y] \equiv 1,\ Alg(x, y) \simeq M_2(\mathbf{F}_3)\}.$$

Then $Aut(L)$ acts transitivly on the set $\mathcal{A}_2$. In particular, every pair $(x,y) \in \mathcal{A}_2$ is conjugated to the pair (x_0, y_0), where $x_0 \equiv \begin{bmatrix} 0 & \mathbf{i} \\ -\mathbf{i} & 0 \end{bmatrix}$, $y_0 \equiv \begin{bmatrix} 0 & \mathbf{j} \\ -\mathbf{j} & 0 \end{bmatrix}$.

Proof. Let (x,y) and (z,t) be two elements of $\mathcal{A}_2$. If $Alg(x,y) = Alg(z,t)$ then $PSL(Alg(x,y)) = PSL(Alg(z,t))$ and $(x,y)^\varphi = (z,t)$ for some $\varphi \in PSL(Alg(x,y)) \simeq A_4$.

If $Alg\langle x,y\rangle \neq Alg\langle z,t\rangle$ then, by Lemmas 3.3 and 3.2, there exists $\varphi \in \mathrm{Aut}(\mathcal{Z}(3))$ such that $Alg(x,y)^\varphi = Alg(z,t)$.

Proposition 3.5 *Every subgroup $L_0 \subseteq L$ of order 8 may be embedded in an non-associative subloop of order 24, and every non-associative subloop of L of order 24 may be embedded in some simple subloop of order 120.*

Proof. Let $\mathcal{A}_3 = \{(x,y,z)|G(x,y,z) \simeq Z_2 \times Z_2 \times Z_2\}$ and $C(x,y) = \{z \in L|(x,y,z) \in \mathcal{A}_3\}$. We shall prove that $|C(x,y)| = 12$ or 0. If $|C(x,y)| \neq 0$ then, by Corollary 3.4, we can suppose that $x = \begin{bmatrix} 0 & \mathbf{i} \\ -\mathbf{i} & 0 \end{bmatrix}$ $y = \begin{bmatrix} 0 & \mathbf{j} \\ -\mathbf{j} & 0 \end{bmatrix}$. Then $z = \begin{bmatrix} -\alpha & \mathbf{v} \\ \mathbf{w} & \alpha \end{bmatrix}$, and $\mathbf{v} = \mathbf{w}$. Indeed, by definition $[x,z] \equiv [y,z] \equiv [xy,z]$, where $xy = \begin{bmatrix} 0 & -\mathbf{k} \\ \mathbf{k} & 0 \end{bmatrix}$; hence, by Lemma 3.1, either $\mathbf{v} = \mathbf{w}$ or $z \in G(x,y)$. It is easy to see that, for every $z = \begin{bmatrix} -\alpha & \mathbf{v} \\ \mathbf{v} & \alpha \end{bmatrix} \in L$, $\mathbf{v} \neq 0$, $G = G(x,y,z) \simeq Z_2 \times Z_2 \times Z_2$. Since $|V(\mathbf{F}_3, \alpha^2 + \mathbf{v}\cdot\mathbf{v} = -1)| = 24$ and $z \equiv -z$, we have $|C(x,y)| = 12$. Therefore, $G(x,y) \subset A^*$ and $PSL(A) \simeq A_4$, where $A = Alg(x,y)$. Let $z = \begin{bmatrix} 1 & \mathbf{i} \\ -\mathbf{i} & -1 \end{bmatrix}$ and define $\varphi : A \to A$, $\varphi(a) = zaz$, then $\varphi(x) = zxz = -z^2x = x$, $\varphi(y) = y$, $\varphi(xy) = xy$, $\varphi(E) = -E$. The eight elements of order 3 of the group $PSL(A) \simeq A_4$ are represented by the elements $\begin{bmatrix} 1 & \mathbf{u} \\ -\mathbf{u} & 1 \end{bmatrix}$, where $\mathbf{u} = \pm\mathbf{i} \pm \mathbf{j} \pm \mathbf{k}$, $\quad \mathbf{u}\cdot\mathbf{u} = 0$. But $\varphi\begin{bmatrix} 1 & \mathbf{u} \\ -\mathbf{u} & 1 \end{bmatrix} = \varphi(E) + \varphi\begin{bmatrix} 0 & \mathbf{u} \\ -\mathbf{u} & 0 \end{bmatrix} = -E + \begin{bmatrix} 0 & \mathbf{u} \\ -\mathbf{u} & 0 \end{bmatrix} \equiv E + \begin{bmatrix} 0 & -\mathbf{u} \\ \mathbf{u} & 0 \end{bmatrix} = \begin{bmatrix} 1 & -\mathbf{u} \\ \mathbf{u} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{u} \\ -\mathbf{u} & 1 \end{bmatrix}^{-1}$; hence, $\varphi(a) \equiv a^{-1}$ for every $a \in A_4$. It follows that $A_4 \cup A_4 z$ is the non-associative Moufang loop $M(A_4, 2)$ of order 24 (Chein's duplication [6]). But there are 12 elements $t \in A_4 z$ such that $G(x,y,t) \simeq Z_2 \times Z_2 \times Z_2$. Therefore, $G \subseteq M(A_4, 2)$.

Let $\mathcal{Z}(\frac{1}{2}\mathbf{Z})$ be the Zorn alternative algebra over the ring $\frac{1}{2}\mathbf{Z} = \{m/2^n \mid n, m \in \mathbf{Z}\}$. In [1], Coxeter proved that $\mathcal{Z}(\frac{1}{2}\mathbf{Z})$ contains a subloop $\widetilde{M}$ of order 240 with the center $C = \{E, -E\}$ such that $\widetilde{M}/C \simeq M_{120}$ is the simple Moufang loop of order 120. For every odd prime number p, there exists a homomorphism $\varphi_p : \mathcal{Z}(\frac{1}{2}\mathbf{Z}) \mapsto \mathcal{Z}(p)$ such that $\varphi_p(\widetilde{M}) = \widetilde{M}_p$ is a subloop of order 240. Hence, the loop L contains a simple subloop M_{120} of order 120. The loop M_{120} contains a subloop M_{24} of order 24 which is isomorphic to $M(A_4, 2)$. Let A_4 be the normal subgroup in M_{24} of order 12 and let $K \subset A_4$ be the Sylow 2-subgroup of A_4, $K = G(x, y)$. We have

$$K \subset A_4 \subset M_{24} \subset M_{120}. \tag{3.2}$$

If M'_{24} is some other subloop of L of order 24, as in [9] we can prove that $M'_{24} \simeq M(A_4, 2)$, because all other Moufang loops of order 24 contain an element of order 4 or 6. Hence, for M'_{24}, we have an analog of (3.2):

$$K' \subset A'_4 \subset M'_{24}. \tag{3.3}$$

Since $K' = G(x', y'), (x', y') \in \mathcal{A}_2$, Corollary 3.4 implies that there exists $\varphi \in \mathrm{Aut}(L)$ such that $K' = K^{\varphi}$. Hence, $A_4^{\varphi} = A'_4, {M_{24}}^{\varphi} = M'_{24}$, because, for a given $(r, s) \in \mathcal{A}_2$, there exist unique subloops A''_4 and M''_{24} such that $G(r, s) \subset A''_4 \subset M''_{24}$. Then (3.2) and (3.3) give $M'_{24} \subseteq {M_{120}}^{\varphi}$.

References

[1] H.S.M. Coxeter, *Integral Cayley Numbers, Duke Mathematical Journal*, **13**, (1946).

[2] M. W. Liebeck, *The classification of finite simple Moufang loops, Math. Proc. Camb. Phil. Soc.*, **102**, (1987), 33-47.

[3] G. Glauberman, *On loops of odd order II, J. Algebra*, **8**, (1968), 393-414.

[4] S. Doro, *Simple Moufang loops, Math. Proc. Camb. Phil. Soc.*, **83**, (1978), 377-392.

[5] P. B. Kleidman, *The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups, J. Algebra*, **110**, N 1 (1987), 173–242.

[6] O. Chein, *Moufang Loops of Small Order I*, **Trans. Amer. Math. Soc.** 188 (1974), 31-51.

[7] O. Chein, *Moufang Loops of Small Order II*, **Memoirs Amer. Math. Soc. 197 (13)** (1978).

[8] L.J. Paige, *A class of simple Moufang loops, Proc. Amer. Math. Soc.*, **7** (1956), 471-482.

[9] M.L. Merlini Giuliani, F.C.Polcino Milies, *On the structure of the simple Moufang loop $GLL(F_2)$, In Nonassociative Algebra and Its Application*, the fourth international conference, Lecture Notes in Pure and Applied Mathematics **211**, edited by R. Costa, A. Grishkov, H. Guzzo Jr., L.A.Peresi; Marcel Dekker, New York, (2000)

[10] A. Grishkov, A. Zavarnitsine, *Lagrange's Theorem for Moufang Loops,* submitted.

M.L. Merlini Giuliani
Departamento de Matemática
Univ. Federal de Santa Maria
97119-105 - Santa Maria RS
Brazil
lurdinha@ccne.ufsm.br