Maximal subloops of finite simple Moufang loops

Alexander N. Grishkov a,b,1, Andrei V. Zavarnitsine a,c,*2

a Departamento de Matemática, Universidade de São Paulo, Caixa Postal 66281, São Paulo-SP, 05311-970, Brazil
b Omsk State University, pr. Mira 55-a, 644077, Russia
c Sobolev Institute of Mathematics, pr. Koptyuga 4, Novosibirsk 630090, Russia

Received 1 April 2004
Available online 19 May 2006
Communicated by Efim Zelmanov
In memoriam: Our teacher Georgy P. Kukin

Abstract

We classify the maximal subloops of finite simple non-associative Moufang loops up to conjugacy with respect to automorphisms.
© 2006 Elsevier Inc. All rights reserved.

Keywords: Moufang loop; Group with triality; Cayley algebra; Maximal subloop

1. Introduction

In this paper we continue the study started in [1] of the properties of Moufang loops using their relation to groups with triality. Our main purpose now is to give a classification of the maximal subloops of the unique finite simple non-associative Moufang loops $M(q)$. It was shown in [1] that there exists a correspondence between the subloops of $M(q)$ and certain subgroups of the simple group with triality $P\Omega_8^{+}(q)$. This correspondence becomes more natural when we bring into consideration the simple alternative algebra $O(q)$ and its automorphism group $G_2(q)$. As a corollary to our results, we have the following description:

* Corresponding author.
E-mail addresses: grishkov@ime.usp.br (A.N. Grishkov), zavarn@ime.usp.br (A.V. Zavarnitsine).
2 Supported by FAPESP, Brazil, Proc. 01/14611-4.

0021-8693/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2006.02.038
Theorem A. The maximal subloops of the simple Moufang loop $M(q)$, $q = p^n$, are as follows:

(i) $q^2 : \operatorname{PSL}_2(q)$, $q$ arbitrary;
(ii) $M(\operatorname{PSL}_2(q), 2)$, $q \neq 3$;
(iii) $M(q_0)$, $q = q_0^2$, $k$ prime, $(q, k) \neq (\text{odd}, 2)$;
(iv) $\operatorname{PGL}(\mathbb{O}(q_0))$, $q = q_0^2$ odd;
(v) $M(2)$, $q = p$ odd.

Moreover, all isomorphic maximal subloops of $M(q)$ are conjugate by the group of inner automorphisms $\operatorname{Inn}(M(q))$.

The symbolic notation that we used in Theorem A for each type (i)–(v) of maximal subloops gives hint of their structure and is explained in detail in Section 7. The group of inner automorphisms of a loop is defined in Section 3.

The paper is organized as follows. The next section introduces some notation and basic definitions. In Section 3, we give a brief background on Moufang loops and describe the general relation between Moufang loops and groups with triality. In addition, we recall the classification of the subgroups of $\operatorname{PGL}_2(q)$ that correspond to certain important subloops of $M(q)$ including all maximal ones. In Section 4, we state some necessary facts about the Cayley algebra $\mathbb{O}(q)$ and the loops and groups associated with it. Section 5 contains a description of the full automorphism group $\operatorname{Aut}(\mathbb{O}(q))$ and some characterization of its elements. The geometry of triality related to the algebra $\mathbb{O}(q)$ is introduced in Section 6. We use this geometry to define explicitly the triality automorphisms of $\operatorname{PGL}_2(q)$. The last section contains a description of the maximal subloops of $M(q)$, the statement of the main result, which is included in Table 5, and a proof of the main theorem of this article. This theorem implies, in particular, the above Theorem A.

As another corollary to our results, we determine the structure of the normalizer in $\operatorname{Inn}(M(q)) \cong G_2(q)$ of each maximal subloop of $M(q)$ and the explicit number subloops of each type (see Table 5).

2. Preliminaries

We mostly use standard notation. $F = F_q$ denotes the field of $q = p^n$ elements, $p$ prime, and $F^*$ is the multiplicative group of $F$. Throughout put $d = (2, q − 1)$. For elements $x, y$ in a group $G$, we put $[x, y] = x^{-1}y^{-1}xy$, $x^y = y^{-1}xy$, $x^{-y} = (x^{-1})^y$. If $\varphi$ is an automorphism of $G$ and $x \in G$ then $x^\varphi$ is the image of $x$ under $\varphi$. Expressions like $x\varphi, [x, \varphi]$, etc., are to be regarded in the semidirect product $G : \operatorname{Aut}(G)$. In particular, $x^\varphi = \varphi^{-1}x\varphi$. The commutator subgroup and the center of $G$ are $G'$ and $Z(G)$, respectively. If $G$ acts by permutations on a set $X$ then $x^G$ denotes the $G$-orbit of an $x \in X$ and we say that the elements of $x^G$ are $G$-conjugate to $x$. If $X_0 \subseteq X$ then $N_G(X_0) = \{g \in G \mid X_0g = X_0\}$.

A vector space $V$ over $F$ equipped with a quadratic form $Q : V \to F$ is called an orthogonal space. The form $Q$ is called non-degenerate if the set

$$\{v \in V \mid f_Q(v, w) = 0 \text{ for all } w \in V\} \cap \{v \in V \mid Q(v) = 0\}$$

contains only the zero vector of $V$, where $f_Q$ is the bilinear form associated with $Q$, i.e., $f_Q(v, w) = Q(v + w) − Q(v) − Q(w)$. For $v \in V$, we call $Q(v)$ the norm of $v$ and say that $v$ is (non-)singular if it has a (non-)zero norm. If $X \subseteq V$ then $X^\perp = \{v \in V \mid f_Q(v, x) = 0 \text{ for all } x \in X\}$.
all \( x \in X \). A set of vectors \( v_1, \ldots, v_n \) of \( V \) satisfying \( f_Q(v_i, v_j) = 0 \) for all \( i \neq j \) is called \( f_Q \)-orthonormal (\( Q \)-orthonormal) if \( f_Q(v_i, v_i) = 1 \) \((Q(v_i) = 1)\) for all \( i \). A subspace \( W \subseteq V \) is called non-degenerate if \( Q|_W \) is a non-degenerate quadratic form on \( W \) and totally singular (t.s.) if \( Q \) vanishes on \( W \). A non-degenerate orthogonal space \((V, Q)\) of even dimension \( 2m \) is said to have type ‘+’ or ‘−’ if all maximal t.s. subspaces of \( V \) have dimension \( m \) or \( m - 1 \), respectively. By definition, an \( m \)-subspace of \( V \) is a subspace of dimension \( m \). If \( m \) is even then an \( \epsilon m \)-subspace \( W \) of \( V \), where \( \epsilon = \pm \), is a non-degenerate \( m \)-subspace such that \((W, Q|_W)\) is an orthogonal space of type \( \epsilon \). For \( q \) odd, a +1-subspace (−1-subspace) is the 1-subspace spanned by an element of \( V \) whose norm is a square (non-square) in \( F^* \). For \( q \) even, a +1-subspace is an arbitrary non-degenerate 1-subspace. A decomposition \( V = \bigoplus_i V_i \) of \( V \) into the orthogonal sum of \( \epsilon m \)-subspaces \( V_i \) is called an \( \epsilon m \)-decomposition.

An involution \( a \mapsto \tilde{a} \) of a ring \( A \) is an anti-automorphism of \( A \) satisfying \( \tilde{a} = a \) for all \( a \in A \). Let \( V \) be a left \( A \)-module, where \( A \) is a commutative ring with involution. A transformation \( f : V \rightarrow V \) is called \( A \)-semilinear if it is additive and \( f(\alpha v) = \tilde{\alpha} f(v) \) for all \( v \in V \), \( \alpha \in A \). A form \( k : V \times V \rightarrow A \) is called \( A \)-sesquilinear if it is \( A \)-linear in the first argument and \( k(v, w) = k(w, v) \) for all \( v, w \in V \). In particular, \( k \) is \( A \)-semilinear in the second argument. The form \( k \) is called non-degenerate if \( k(v, w) = 0 \) for all \( w \in V \) implies \( v = 0 \). An \( A \)-linear \( m \)-form \( f : V \times \cdots \times V \rightarrow A \) is called alternating if \( f(v_1, \ldots, v_m) = 0 \) whenever \( v_i = v_j \) for some \( 1 \leq i < j \leq m \).

All groups (loops) we consider are finite. All vector spaces have finite dimension. The sub-
group (subspace) generated by a set \( X \) is denoted by \( \langle X \rangle \). When a field \( F \) is to be specified, we write \( \langle X \rangle_F \). The inverse transpose of a matrix \( A \) is \( A^{-T} \). The cyclic and dihedral groups of order \( n \) are \( \mathbb{Z}_n \) and \( \mathbb{D}_n \).

A reference of form “(8.iv)” means “item (iv) of Lemma 8.”

3. Groups with triality and Moufang loops

A set \( M \) with a binary operation \( M \times M \ni (x, y) \mapsto xy \in M \) is called a loop if the following two conditions hold:

1. for every \( a \in M \), the mappings \( L_a : x \mapsto ax \) and \( R_a : x \mapsto xa \) are bijections of \( M \),
2. there exists an identity \( e \in M \) satisfying \( ex = xe = x \) for all \( x \in M \).

An associative subloop of a loop \( M \) is called a subgroup. A subloop \( H \) of \( M \) is normal if

\[
  xH = Hx, \quad (Hx)y = H(xy), \quad y(xH) = (yx)H
\]

for all \( x, y \in M \). A loop is called simple if it does not have proper normal subloops or, equivalently, does not have proper homomorphic images (see in [7, p. 60]).

If \( M \) is a loop then the multiplication group \( \text{Mlt}(M) \) is the group of permutations of \( M \) generated by the operators \( L_x \) and \( R_x \) of left and right multiplication by \( x \) in \( M \), the inner mapping group \( \text{Inn}(M) \) is the stabilizer in \( \text{Mlt}(M) \) of the identity \( e \in M \), and \( \text{Inn}(M) = \text{I}(M) \cap \text{Aut}(M) \) is the group of inner automorphisms of \( M \).

A loop \( M \) is called a Moufang loop if, for all \( x, y, z \in M \), one (hence, any) of the following identities hold:

\[
  (xy)(zx) = (x(yz))x, \quad ((xy)x)z = x(y(xz)), \quad x(y(zy)) = ((xy)z)y.
\]
A group $G$ possessing automorphisms $\rho$ and $\sigma$ that satisfy $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ is called a group with triality (relative to $\rho$ and $\sigma$) if the following relation holds for every $x$ in $G$:

$$[x, \sigma] \cdot [x, \sigma]^\rho \cdot [x, \sigma]^\sigma = 1.$$  \hfill (3.1)

Denote $S = \langle \rho, \sigma \rangle$. The triality is called non-trivial if $S \neq 1$. Relation (3.1) does not depend on the particular choice of the generators $\rho$ and $\sigma$ of $S$ (see [3]) and we will thus speak of a group with triality $S$.

Let $G$ be a group with triality $S = \langle \rho, \sigma \rangle$. Put

$$M = \{[x, \sigma] | x \in G\}, \quad H = C_G(\sigma).$$ \hfill (3.2)

It was shown in [1] that $M$ endowed with the multiplication

$$m \cdot n = m^{-\rho} nm^{-\rho^2} \quad \text{for all} \ m, n \in M \hfill (3.3)$$

becomes a Moufang loop of order $|G : H|$ which is isomorphic to the loop previously considered by Doro [3]. We denote by $\mathcal{M}(G)$ the loop $(M, \cdot)$ constructed in this way from a group $G$ with triality.

**Lemma 1.** In the above notation, we have

(i) $M^{\rho^2}$ is both left and right transversal of $H$ in $G$,
(ii) for every $g \in G$, we have $g = \eta(g)\xi(g)^{\rho^2}$, where $\eta(g) = gg^{-\rho \sigma}g^{\rho^2} \in H$ and $\xi(g) = [g, \sigma] \in M$,
(iii) for every $m \in M$, the elements $m$, $m^\rho$, $m^{\rho^2}$ pairwise commute,
(iv) for every $m, n \in M$, we have $m^{-\rho} nm^{-\rho^2} = n^{-\rho^2} mn^{-\rho}$.

**Proof.** See Lemma 2 in [1] and [3]. \hfill $\square$

If $G_0 \leq G$ is an $S$-invariant subgroup of $G$ (in brief, $S$-subgroup) then $\mathcal{M}(G_0)$ is a subloop of $\mathcal{M}(G)$. The reverse correspondence is expressed in the following lemma.

**Lemma 2.** Let $G$ be a group with triality $S$. Then, for every subloop $M_0 \leq \mathcal{M}(G)$, there exist uniquely defined $S$-subgroups $G_0^{\min}$ and $G_0^{\max}$ of $G$ such that $\mathcal{M}(G_0^{\min}) = \mathcal{M}(G_0^{\max}) = M_0$ and, for every $S$-subgroup $G_0 \leq G$ with $\mathcal{M}(G_0) = M_0$, we have $G_0^{\min} \leq G_0 \leq G_0^{\max}$.

**Proof.** Denote $G_0^{\min} = \langle M_0, M_0^\rho, M_0^{\rho^2} \rangle$. Clearly, $G_0^{\min}$ is an $S$-subgroup and it is known that $\mathcal{M}(G_0^{\min}) = M_0$ (see proof of Theorem 1 in [1]). Observe that, for every $S$-subgroup $G_0$ with $\mathcal{M}(G_0) = M_0$, we have $G_0^{\min} = [G_0, S]$. Indeed, the sets $[G_0, \sigma]$, $[G_0, \rho \sigma]$, $[G_0, \sigma \rho]$ coincide with $M_0$, $M_0^\rho$, $M_0^{\rho^2}$, respectively. Moreover, $[G_0, \rho] = [G_0, \rho^2]^\rho$. Thus, it suffices to show that $[G_0, \rho^2] \subseteq G_0^{\min}$. For $g \in G_0$, we have $g^{-1}g^{\rho^2} = (g^{-1}g^\sigma)(g^{\rho \sigma})^{-1}(g^{\rho \sigma})^\rho \in M_0M_0^\rho$. Thus, $G_0^{\min} = [G_0, S] \subseteq G_0$.

Now show that any $S$-subgroups $G_1$ and $G_2$ with $\mathcal{M}(G_1) = \mathcal{M}(G_2) = M_0$ satisfy $\mathcal{M}(\langle G_1, G_2 \rangle) = M_0$. This will imply that $G_0^{\max}$ is the subgroup generated by all $S$-subgroups.
$G_0$ with $\mathcal{M}(G_0) = M_0$. It suffices to prove that $[g_1g_2, \sigma] \in M_0$ for all $g_1 \in G_1$ and $g_2 \in G_2$. Put $m_1 = [g_1, \sigma]$ and $m_2 = [g_2, \sigma]$. Then $m_1, m_2 \in M_0$. Write $g_2 = hm_2^\rho$, where $h = \eta(g_2) \in G_2 \cap H$ (see Lemma 1). Using (3.1), (3.3), and Lemma 1, we have

$$[g_1g_2, \sigma] = m_1^{\rho_2}m_2 = m_2^{-\rho^2}h^{-1}m_1hm_2^{\rho_2}m_2 = m_2^{-\rho^2}m_0m_2^{-\rho}, \quad (3.4)$$

where $m_0 = m_1^\rho$. Note that $M_0^h = M_0$, since $M_0 = \{[\sigma, g] \mid g \in G_2\}$ and $h \in G_2 \cap H$. In particular, $m_0 \in M_0$. Then (3.4) and (1.iv) imply that $[g_1g_2, \sigma] = m_0, m_2 \in M_0$. $\square$

A subgroup of $G$ is called $S$-maximal if it is maximal among the $S$-subgroups of $G$. We obtain the following obvious corollary to Lemma 2.

**Corollary 3.** If $G_1 \neq G_2$ are $S$-maximal subgroups of $G$ then $\mathcal{M}(G_1) \neq \mathcal{M}(G_2)$.

It is well known that the finite simple group $G = P\Omega_8^+(q)$ is a group with triality relative to its group of graph automorphisms $S \cong S_3$ and the corresponding Moufang loop $\mathcal{M}(G)$ is a simple loop (see also Lemma 16 below). We will denote by $M(q)$ an abstract Moufang loop isomorphic to $\mathcal{M}(P\Omega_8^+(q))$. As was shown by Liebeck [5], the loops $M(q)$ for $q = p^n$ are the only simple non-associative Moufang loops and $P\Omega_8^+(q)$ are the only (finite) simple groups with triality. Namely, the following result holds:

**Lemma 4.** If $G$ is a finite non-abelian simple group with non-trivial triality $S = \langle \rho, \sigma \rangle$ then $G = P\Omega_8^+(q)$ and $S$ is conjugate in $\text{Aut}(G)$ to the group of graph automorphisms of $G$ which is isomorphic to $S_3$. If this is the case then $\mathcal{M}(G)$ is isomorphic to $M(q)$.

**Proof.** See [5] and Lemma 4 in [1]. $\square$

In [1], all $S$-maximal subgroups $G_0$ of $G = P\Omega_8^+(q)$ were determined up to conjugacy and, for each conjugacy class, the orders of the corresponding subloops in $M(q)$ were found. We reproduce these subgroups here in Table 1. Column I lists representatives of the conjugacy classes in $G$ that contain $S$-maximal subgroups. The notation here is carried over from [6]. The structure of the subgroups will be explained later in detail (see proof Theorem 1 below). Column II tells for which $q$ (with “–” meaning “for all $q$”) the corresponding subgroup is defined and is $S$-maximal. Column III shows “✓” (“–”) if $G_0$ is always (never) maximal in $G$, or indicates the specific values of $q$ for which it is maximal. Columns IV and V give the orders of $G_0$ and the corresponding subloop $\mathcal{M}(G_0)$. It was proven in [1] that the latter order does not depend on the choice of an $S$-maximal representative in the conjugacy class of $G_0$.

A subgroup of $G$ that is $G$-conjugate to $S$ is called a triality $S_3$-complement. An involution in $G$ is called a triality involution if it lies in a triality $S_3$-complement.

**Lemma 5.** For every $S$-maximal subgroup $G_0 \leq G$, the number of triality $S_3$-complements in $G_0S$ is equal to $|\mathcal{M}(G_0)|^2$.

**Proof.** When considering each type of $S$-maximal subgroups $G_0 \leq G$ in the proof of Theorem 2 in [1], we showed that all triality involutions in $G_0(\sigma)$ are $G_0$-conjugate and, in particular, there are exactly $|\mathcal{M}(G_0)|$ of them in each of the cosets $G_0\sigma$, $G_0\sigma\rho$, $G_0\rho\sigma$. Moreover, every pair of
Table 1

| I   | II Restrictions on q | III Maximal in $PΩ_8^+(q)$ | IV $|G_0|$ | V $|\mathcal{M}(G_0)|$ |
|-----|----------------------|-----------------------------|----------|-----------------|
| 1.  | $P_2$                | -                           | $\frac{1}{d^2}q^{12}(q-1)^4(q+1)$ | $\frac{1}{d}q^3(q-1)$ |
| 2.  | $R_{12}$            | -                           | $\frac{1}{d^2}q^{12}(q-1)^4(q+1)^3$ | $\frac{1}{d}q^3(q^2-1)$ |
| 3.  | $N_1$               | -                           | $\frac{2}{d^2}q^3(q^3+1)(q+1)^3(q-1)$ | $\frac{1}{d}q^3(q+1)$ |
| 4.  | $N_2$               | $q \geq 4$                 | $\frac{2}{d^2}q^3(q^3-1)(q+1)^3(q+1)$ | $\frac{1}{d}q^3(q-1)$ |
| 5.  | $N_4^4$             | $q = p \geq 3$             | $\frac{1}{d}q^{12} \cdot 3 \cdot 7$ | 8 |
| 6.  | $I_+2$              | $q \geq 7$                 | $\frac{1}{d^2}q^{12}(q-1)^4$ | $\frac{1}{d}q^3(q-1)$ |
| 7.  | $L_\perp$           | $q \neq 3$                 | $\frac{1}{d^2}q^{12}(q+1)^4$ | $\frac{4}{d}q^3(q+1)$ |
| 8.  | $L_+4$              | $q \geq 3$                 | $\frac{1}{d^2}q^3(q^2-1)^4$ | $\frac{2}{d}q^3(q^2-1)$ |
| 9.  | $G_2^1$             | -                           | $q^6(q^6-1)(q^2-1)$ | 1 |
| 10. | $PΩ_8^+(2)$         | $q = p \geq 3$             | $\frac{1}{d^2}q^{12} \cdot 3 \cdot 5 \cdot 7 \cdot 7$ | 120 |
| 11. | $PΩ_8^+(q_0)$       | $q = q_0^k$, $k$ prime,   | $\frac{1}{d^2}q_0^12(q_0^2-1)(q_0^4-1)(q_0^6-1)$ | $\frac{1}{d^2}q_0^3(q_0^4-1)$ |
| 12. | $PΩ_8^+(q_0).2^2$  | $q = q_0^2$ odd             | $q^6(q-1)(q^2-1)^2(q^3-1)$ | $q_0^3(q_0^4-1)$ |

Triality involutions from different cosets in $G_0S : G_0$ generates a triality $S_3$ complement, as was explained in the proof of Lemma 6 in [1]. The claim follows from these remarks. □

Let $D = C_G(S)$. By Proposition 3.1.1 in [6], we have $D \cong G_2(q)$. It is clear form (3.2) and (3.3) that the loop $\mathcal{M}(G)$ is $D$-invariant and $D$ acts by automorphisms on $\mathcal{M}(G)$.

Denote by $[G_0]$ the $G$-conjugacy class of $G_0 \leq G$. Note that if $G_0$ is $S$-maximal then so is every $S$-subgroup in $[G_0]$. Moreover, $N_G(G_0) = G_0$ for every $S$-maximal $G_0$.

**Lemma 6.** Let $G_0$ be an $S$-maximal subgroup of $G = PΩ_8^+(q)$. Then the following conditions are equivalent:

(i) for all $S$-subgroups $P \in [G_0]$, the subloops $\mathcal{M}(P) \leq \mathcal{M}(G)$ are conjugate by automorphisms in $D$, and hence are isomorphic,

(ii) all $S$-subgroups in $[G_0]$ are $D$-conjugate,

(iii) $|D : G_0 \cap D|$ is the number of $S$-subgroups in $[G_0]$.

(iv) all triality $S_3$-complements in $G_0S$ are $G_0$-conjugate,

(v) $|G_0 : G_0 \cap D| = |\mathcal{M}(G_0)|^2$.

**Proof.** Let $P_1, P_2 \in [G_0]$ be $S$-subgroups. If $P_1 = P_2^g$ for some $g \in D$ then $\mathcal{M}(P_1) = \mathcal{M}(P_2)^g$, since, for every $p_1 \in P_1$, we have $[p_1, \sigma] = [p_2^g, \sigma] = [p_2, \sigma]^g$ for a suitable $p_2 \in P_2$. Conversely, let $\mathcal{M}(P_1) = \mathcal{M}(P_2)^g$ and put $P_0 = P_2^g$. Then $P_0$ is $S$-maximal and, by the above, $\mathcal{M}(P_0) = \mathcal{M}(P_2)^g = \mathcal{M}(P_1)$. Corollary 3 now implies $P_0 = P_1$. This shows equivalence of (i) and (ii). Clearly, (iii) is equivalent to (ii). Equivalence of (iv) and (v) follows from Lemma 5. Show that (ii) and (iv) are equivalent. Let (ii) hold. If $S_0$ is a triality $S_3$-complement in $G_0S$ then $S_0^{gh} = S$ for some $g \in G$ and $G_0^h$ is an $S$-subgroup in $[G_0]$. By (ii), $G_0^{gh} = G_0$ for some $h \in D$. But then $gh \in G_0$, since $N_G(G_0) = G_0$, and $S_0^{gh} = S^h = S$. Now let (iv) hold. If $P \in [G_0]$ is
S-invariant and $P^g = G_0$ for suitable $g \in G$ then $G_0$ is $S^g$-invariant. By (iv), $S^{gh} = S$ for some $h \in G_0$. But then $gh \in D$ and $P^{gh} = G_0^h = G_0$. □

We intend to study in detail what subloops of $M(q)$ arise from $S$-maximal subgroups of $G$ and determine which of them are maximal. Using Lemma 6 we will show that all such subloops are isomorphic and conjugate by automorphisms for every type of $S$-maximal subgroups of $G$. To do this we will need to know explicitly the action of the triality automorphisms on $G$. For this reason we invoke the Cayley algebra.

4. The split Cayley algebra

An algebra $A$ is called alternative if $(xx)y = x(xy)$ and $(yx)x = y(xx)$ for all $x, y \in A$. These identities imply $(xy)x = x(yx)$, which allows us to write $xyx$ without ambiguity. For every $x \in A$, introduce linear transformations $U_x, L_x, R_x$ of $A$ as follows:

$$yU_x = xyx, \quad yL_x = xy, \quad yR_x = yx \quad \text{for all } y \in A. \quad (4.1)$$

**Lemma 7.** Let $A$ be an alternative algebra. Then, for all $x, y, z \in A$, we have:

(i) $(xy)(zx) = x(yz)x$ or, equivalently, $L_yU_x = R_xL_{xy}$, or $R_yU_x = L_xR_{yx}$.

(ii) $z(xy)x = ((yz)x)y$ or, equivalently, $U_{xy} = L_yU_xR_y$.

(iii) $z((xy)x) = ((zx)y)x$ or, equivalently, $R_{xy} = R_xU_yL_x$.

(iv) $(xy)z(xy) = (x(yz)x)y$ or, equivalently, $U_{xy} = L_xLyL_x$.

(v) $(xy)z(xy) = x((yz)x)y$ or, equivalently, $U_{xy} = R_xU_yL_x$.

**Proof.** The identities (i)–(iii) are well known (see, e.g., Lemma 2.7 in [4]). For (iv) and (v), see relation (8) in [8]. □

Given a group $Z$, a decomposition $A = \bigoplus_{z \in Z} A_z$ is called a $Z$-grading of $A$ if $A_{z_1}A_{z_2} \subseteq A_{z_1z_2}$ for all $z_1, z_2 \in Z$. Given an algebra $A$ over a field $F$ with involution, denote by $A^\circ$ the Cayley–Dickson duplication of $A$, which is the vector $F$-space $A \oplus A$ with multiplication

$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - b_2b_1, b_2a_1 + b_1a_2). \quad (4.2)$$

Then $A^\circ$ is an algebra with involution $(a, b) = (\bar{a}, -b)$.

Let $O = O(q)$ be the 8-dimensional Cayley algebra over $F$. This algebra can be defined as set of all Zorn matrices

$$\begin{pmatrix} a & v \\ w & b \end{pmatrix}, \quad a, b \in F, \; v, w \in F^3 \quad (4.3)$$

with the natural structure of a vector space over $F$ and multiplication given by the rule

$$\begin{pmatrix} a_1 & v_1 \\ w_1 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & v_2 \\ w_2 & b_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + v_1 \cdot w_2 & a_1v_2 + b_2v_1 \\ a_2w_1 + b_1w_2 & w_1 \cdot v_2 + b_1b_2 \end{pmatrix} + \begin{pmatrix} 0 & -w_1 \times w_2 \\ v_1 \times v_2 & 0 \end{pmatrix}, \quad (4.4)$$
where, for \( \mathbf{v} = (v_1, v_2, v_3) \) and \( \mathbf{w} = (w_1, w_2, w_3) \) in \( F^3 \), we denoted

\[
\mathbf{v} \cdot \mathbf{w} = v_1 w_1 + v_2 w_2 + v_3 w_3 \in F,
\]

\[
\mathbf{v} \times \mathbf{w} = (v_2 w_3 - v_3 w_2, v_3 w_1 - v_1 w_3, v_1 w_2 - v_2 w_1) \in F^3.
\]

We choose the standard basis \((e_1, \ldots, e_4, f_1, \ldots, f_4)\) of \( \mathcal{O} \) as follows

\[
e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ i \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ j \\ 0 \end{pmatrix}, \quad e_4 = \begin{pmatrix} 0 \\ k \\ 0 \end{pmatrix},
\]

\[
f_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 0 \\ 0 \\ -i \end{pmatrix}, \quad f_3 = \begin{pmatrix} 0 \\ 0 \\ -j \end{pmatrix}, \quad f_4 = \begin{pmatrix} 0 \\ 0 \\ -k \end{pmatrix},
\]

(4.5)

where \( \mathbf{0} = (0, 0, 0), \mathbf{i} = (1, 0, 0), \mathbf{j} = (0, 1, 0), \mathbf{k} = (0, 0, 1) \). Then \( 1 = e_1 + f_1 \) is the unit of \( \mathcal{O} \).

We identify \( F \) with \( \langle 1 \rangle \). The basis elements of \( \mathcal{O} \) multiply as shown in Table 2.

For \( x \in \mathcal{O} \) define its conjugate \( \bar{x} \) by

\[
\begin{pmatrix} a \\ v \\ w \\ b \end{pmatrix} \mapsto \begin{pmatrix} b \\ -v \\ -w \\ a \end{pmatrix}.
\]

Then conjugation is an involution of \( \mathcal{O} \). Introduce a quadratic form \( Q: \mathcal{O} \to F \) as follows:

\[
\begin{pmatrix} a \\ v \end{pmatrix} \mathcal{O} \mapsto ab - \mathbf{v} \cdot \mathbf{w},
\]

and denote by \((,\)\) the associated bilinear form \( f_Q \). Then (4.5) is a standard basis for these forms, i.e.,

\[
(e_i, f_j) = 1, \quad Q(e_i) = Q(f_j) = (e_i, e_j) = (e_i, f_j) = (f_i, f_j) = 0 \quad \text{for } 1 \leq i \neq j \leq 4.
\]

In particular, the norm of an arbitrary element of \( \mathcal{O} \) is

\[
Q(a_1 e_1 + \cdots + a_4 e_4 + b_1 f_1 + \cdots + b_4 f_4) = a_1 b_1 + \cdots + a_4 b_4.
\]

If the characteristic of \( F \) is not 2 then \( \mathcal{O} \) possesses another equally useful basis. Namely, suppose for the moment that \( q \) is odd and let \( a, b \in F \) satisfy \( a^2 + b^2 = -1 \). Then the elements

<table>
<thead>
<tr>
<th>Table 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplication table of the algebra ( \mathcal{O} )</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>( e_1 )</td>
</tr>
<tr>
<td>( e_1 )</td>
</tr>
<tr>
<td>( e_2 )</td>
</tr>
<tr>
<td>( e_3 )</td>
</tr>
<tr>
<td>( e_4 )</td>
</tr>
<tr>
<td>( f_1 )</td>
</tr>
<tr>
<td>( f_2 )</td>
</tr>
<tr>
<td>( f_3 )</td>
</tr>
<tr>
<td>( f_4 )</td>
</tr>
</tbody>
</table>
An alternative multiplication table of $O$ in odd characteristic

<table>
<thead>
<tr>
<th></th>
<th>$\varepsilon_1$</th>
<th>$\varepsilon_2$</th>
<th>$\varepsilon_3$</th>
<th>$\varepsilon_4$</th>
<th>$\varepsilon_5$</th>
<th>$\varepsilon_6$</th>
<th>$\varepsilon_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varepsilon_1$</td>
<td>$-1$</td>
<td>$\varepsilon_4$</td>
<td>$\varepsilon_7$</td>
<td>$-\varepsilon_2$</td>
<td>$\varepsilon_6$</td>
<td>$-\varepsilon_5$</td>
<td>$-\varepsilon_3$</td>
</tr>
<tr>
<td>$\varepsilon_2$</td>
<td>$-\varepsilon_4$</td>
<td>$-1$</td>
<td>$\varepsilon_5$</td>
<td>$\varepsilon_1$</td>
<td>$-\varepsilon_3$</td>
<td>$\varepsilon_7$</td>
<td>$-\varepsilon_6$</td>
</tr>
<tr>
<td>$\varepsilon_3$</td>
<td>$-\varepsilon_7$</td>
<td>$-\varepsilon_5$</td>
<td>$-1$</td>
<td>$\varepsilon_6$</td>
<td>$\varepsilon_2$</td>
<td>$-\varepsilon_4$</td>
<td>$\varepsilon_1$</td>
</tr>
<tr>
<td>$\varepsilon_4$</td>
<td>$\varepsilon_2$</td>
<td>$-\varepsilon_1$</td>
<td>$-\varepsilon_6$</td>
<td>$-1$</td>
<td>$\varepsilon_7$</td>
<td>$\varepsilon_3$</td>
<td>$-\varepsilon_5$</td>
</tr>
<tr>
<td>$\varepsilon_5$</td>
<td>$-\varepsilon_6$</td>
<td>$\varepsilon_3$</td>
<td>$-\varepsilon_2$</td>
<td>$-\varepsilon_7$</td>
<td>$-1$</td>
<td>$\varepsilon_1$</td>
<td>$\varepsilon_4$</td>
</tr>
<tr>
<td>$\varepsilon_6$</td>
<td>$\varepsilon_5$</td>
<td>$-\varepsilon_7$</td>
<td>$\varepsilon_4$</td>
<td>$-\varepsilon_3$</td>
<td>$-\varepsilon_1$</td>
<td>$-1$</td>
<td>$\varepsilon_2$</td>
</tr>
<tr>
<td>$\varepsilon_7$</td>
<td>$\varepsilon_3$</td>
<td>$\varepsilon_6$</td>
<td>$-\varepsilon_1$</td>
<td>$\varepsilon_5$</td>
<td>$-\varepsilon_4$</td>
<td>$-\varepsilon_2$</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

$\varepsilon_1 = e_2 + f_2, \quad \varepsilon_2 = e_3 + f_3, \quad \varepsilon_3 = a(e_1 - f_1) + b(e_2 - f_2),

\begin{align*}
\varepsilon_4 &= \varepsilon_1 \varepsilon_2, \\
\varepsilon_5 &= \varepsilon_2 \varepsilon_3, \\
\varepsilon_6 &= \varepsilon_3 \varepsilon_4, \\
\varepsilon_7 &= \varepsilon_4 \varepsilon_5.
\end{align*}

(4.6)
together with $1$, form a basis of $O$ and multiply as shown in Table 3. This table is uniquely restored from the relations

\begin{align*}
\varepsilon_2^2 &= -1, \\
\varepsilon_{r+1} \varepsilon_{r+3} &= \varepsilon_{r+2} \varepsilon_{r+6} = \varepsilon_{r+4} \varepsilon_{r+5} = \varepsilon_r, \\
\varepsilon_{r+3} \varepsilon_{r+1} &= \varepsilon_{r+6} \varepsilon_{r+2} = \varepsilon_{r+5} \varepsilon_{r+4} = -\varepsilon_r, \\
\varepsilon_{r+7} &= \varepsilon_r,
\end{align*}

(4.7)

where $1 \leq r \leq 7$. This new basis is $Q$-orthonormal and satisfies

\begin{align*}
\overline{\varepsilon_0} &= \varepsilon_0, \\
\overline{\varepsilon_i} &= -\varepsilon_i \quad \text{for } 1 \leq i \leq 7,
\end{align*}

(4.8)

where we denoted $\varepsilon_0 = 1$. In particular, for any $a_0, \ldots, a_7 \in F$,

\begin{align*}
Q(a_0 \varepsilon_0 + a_1 \varepsilon_1 + \cdots + a_7 \varepsilon_7) &= a_0^2 + a_1^2 + \cdots + a_7^2.
\end{align*}

(4.9)

Let $q$ be arbitrary. The following properties of the Cayley algebra $O$ are well known.

**Lemma 8.** We have

(i) $O$ is an alternative algebra,

(ii) the space $(O, Q)$ is a non-degenerate orthogonal space of type ‘+.’

For all $x, y, z, w \in O$ we have

(iii) $Q(xy) = Q(x)Q(y),$

(iv) $\overline{x} = x, \quad \overline{xy} = \overline{y} \overline{x},$

(v) $Q(x) = x \overline{x} = \overline{x} x,$

(vi) $(x, y) = x \overline{y} + y \overline{x},$

(vii) $\overline{x(xy)} = (yx) \overline{x} = Q(x)y,$

(viii) $(zx, y) = (x, \overline{zy}), \quad (xz, y) = (x, y \overline{z}),$

(ix) $(x, y)(z, w) = (xz, yw) + (xw, zy).$
Proof. See Chapter 2 in [4]. 

Introduce some important subalgebras of $\mathcal{O}$. Let $s \in F$ be such that $t^2 - st + 1$ is an irreducible polynomial in $F[t]$. Define

$$
\mathbb{M} = \langle e_1, e_2, f_1, f_2 \rangle, \quad \mathbb{F} = \langle 1, e_2 + f_2 + sf_1 \rangle, \quad \mathbb{P} = \langle e_1, f_1 \rangle.
$$

These are subalgebras of $\mathcal{O}$ with involution induced from $\mathcal{O}$. The mapping

$$
\left( \begin{array}{cc} a_1 & (a_2, 0, 0) \\ (a_3, 0, 0) & a_4 \end{array} \right) \mapsto \left( \begin{array}{cc} a_1 & a_2 \\ a_3 & a_4 \end{array} \right)
$$

is an isomorphism between $\mathbb{M}$ and the algebra $M_2(F)$ of $2 \times 2$-matrices over $F$ with involution

$$
\left( \begin{array}{cc} a_1 & a_2 \\ a_3 & a_4 \end{array} \right) = \left( \begin{array}{cc} a_4 & -a_2 \\ -a_3 & a_1 \end{array} \right).
$$

Moreover, $\mathbb{F}$ is isomorphic to $F_{q^2}$ whose involution is the Frobenius automorphism $\bar{a} = a^q$ and $\mathbb{P}$ is isomorphic to $F \oplus F$ whose involution is $(a, b) = (b, a)$.

Denote

$$
wi = ei + fi, \quad i = 1, \ldots, 4, \quad \mathfrak{w} = \{w_1, \ldots, w_4\}.
$$

Observe that $\mathfrak{w}$ is a $Q$-orthonormal set. It is directly verified that

$$
\mathcal{O} = \mathbb{M} \oplus \mathbb{M}w_3, \quad \mathbb{M} = \mathbb{F} \oplus \mathbb{F}w_2, \quad \mathbb{M} = \mathbb{P} \oplus \mathbb{P}w_2,
$$

and, for every triple $(A, B, w) \in \{(\mathcal{O}, \mathbb{M}, w_3), (\mathbb{M}, \mathbb{F}, w_2), (\mathbb{M}, \mathbb{P}, w_2)\}$, the mapping

$$
A \ni a = b_1 + b_2w \mapsto (b_1, b_2) \in B \oplus B
$$

is an algebra isomorphism preserving involution, where the multiplication in $B \oplus B$ is as in (4.2). In other words, $\mathcal{O} \cong M^\circ$, $\mathbb{M} \cong F^\circ$, and $\mathbb{M} \cong P^\circ$. Hence, we have the decompositions

$$
\mathcal{O} = Fw_1 \oplus Fw_2 \oplus Fw_3 \oplus Fw_4,
$$

$$
\mathbb{O} = Pw_1 \oplus Pw_2 \oplus Pw_3 \oplus Pw_4.
$$

Lemma 9. Let $A$ be a subalgebra of $\mathcal{O}$ that contains 1. Then

(i) $AA^\perp \subseteq A^\perp$, $A^\perp A \subseteq A^\perp$.

For all $a, b \in A$, $v, w \in A^\perp$, we have

(ii) $\bar{v} = -v$, $va = \bar{av}$,
(iii) $a(bv) = (ba)v$, $(vb)a = v(ab)$,
(iv) $(av)w = (vw)a$, $w(va) = a(wv)$.
Proof. (i)–(iii) See Lemma 6 in Chapter 2 of [4].
(iv) For every \( c \in A \), we have by (ii) and (8.viii–ix)
\[
((av)w - (vw)a, c) = (av, c\overline{w}) - (vw, c\overline{a}) = (va, c\overline{w}) + (v\overline{w}, c\overline{a}) = (v, c)(\overline{a}, \overline{w}) = 0,
\]
since \( \overline{a} \in A \) and \( \overline{w} \in A^\perp \). By non-degeneracy of \((\cdot,\cdot)\), we obtain the first relation in (iv). The second one is obtained by conjugating. \( \Box \)

This lemma implies that
\[
O = M \oplus Mw_3 \tag{4.13}
\]
is a \( \mathbb{Z}_2 \)-grading of \( O \) and the decompositions (4.12) are \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)-gradings of \( O \).

Introduce the projective space \( PG(O) = \{ \langle x \rangle \mid x \in O \} \). By analogy with the standard notation, we put
\[
GL(O) = \{ x \in O \mid Q(x) \neq 0 \},
\]
\[
PGL(O) = \{ \langle x \rangle \in PG(O) \mid Q(x) \neq 0 \},
\]
\[
SL(O) = \{ x \in O \mid Q(x) = 1 \},
\]
\[
PSL(O) = \{ \langle x \rangle \in PG(O) \mid Q(x) \in (F^*)^2 \}. \tag{4.14}
\]
In particular, \( PSL(O) \) is the set of all \(+1\)-subspaces of \( O \). By (8.i) and (7.i), we see that \( GL(O) \), \( SL(O) \), \( PGL(O) \), and \( PSL(O) \) are Moufang loops with multiplication induced from \( O \). Note that \( \{ \pm 1 \} \) is a normal subgroup of \( SL(O) \) and \( SL(O)/\{ \pm 1 \} \cong PSL(O) \). Similarly, \( GL(O)/\{1\} \cong PGL(O) \). It is easy to see that
\[
|GL(O)| = (q^4 - q^3)(q^4 - 1), \quad |PSL(O)| = \frac{1}{d}q^3(q^4 - 1),
\]
\[
|PGL(O)| = |SL(O)| = q^3(q^4 - 1).
\]

Let \( GO(O) \) be the group of all linear transformations of \( O \) that preserve the quadratic form \( Q \). We also introduce the groups
\[
SO(O) = \{ g \in GO(O) \mid \det g = 1 \}, \quad \Omega(O) = GO(O)',
\]
\[
PGO(O) = GO(O)/Z(GO(O)), \quad P\Omega(O) = PGO(O)'.
\]
Then \( P\Omega(O) \) is a finite simple group isomorphic to \( P\Omega_8^+(q) \). We denote the image in \( PGO(O) \) of an element \( g \in GO(O) \) by \( \hat{g} \).

A reflection \( r_v \) in a non-singular vector \( v \in O \) is the linear transformation of \( O \) given by
\[
x r_v = x - \frac{(x, v)}{Q(v)}v \quad \text{for all } x \in O. \tag{4.15}
\]

**Lemma 10.** Let \( v, w \in O \) be non-singular. Then we have
(i) \( r_v \) is an involution in \( GO(\mathfrak{O}) \) and \( \det r_v = -1 \),
(ii) \( r_v = r_w \iff \langle v \rangle = \langle w \rangle \),
(iii) \( (r_v)^g = r_{vg} \) for every \( g \in GO(\mathfrak{O}) \),
(iv) \( g \in GO(\mathfrak{O}) \) centralizes \( r_v \) if and only if \( \langle v \rangle g = \langle v \rangle \).

**Proof.** Straightforward. \( \square \)

Using (8.vi–vii), we can rewrite
\[ x r_v = x - \frac{(x \bar{v}) v + (v \bar{x}) v}{Q(v)} = -\frac{1}{Q(v)} v \bar{x} v. \] (4.16)

This expression is fundamental in that it relates the action of \( GO(\mathfrak{O}) \) (which is generated by reflections) with the multiplication in \( \mathfrak{O} \). In particular, the conjugation in \( \mathfrak{O} \) is the map \( -r_1 \). The projective action of generators of \( PGO(\mathfrak{O}) \) on \( PG(\mathfrak{O}) \) is then written as
\[ \langle x \rangle \tilde{r}_v = \langle v \bar{x} v \rangle \quad \text{for all } x \in \mathfrak{O}. \] (4.17)

We also introduce, for every \( \langle v \rangle \in PG(\mathfrak{O}) \), the projective analogs \( U_{\langle v \rangle} \), \( L_{\langle v \rangle} \), \( R_{\langle v \rangle} \) of the operators (4.1) as follows:
\[ \langle x \rangle U_{\langle v \rangle} = \langle vxv \rangle, \quad \langle x \rangle L_{\langle v \rangle} = \langle vx \rangle, \quad \langle x \rangle R_{\langle v \rangle} = \langle xv \rangle \quad \text{for all } \langle x \rangle \in PG(\mathfrak{O}). \]

Note that
\[ U_{\langle v \rangle} \in PGO(\mathfrak{O}) \iff \langle v \rangle \in PGL(\mathfrak{O}), \]
[\[ L_{\langle v \rangle}, R_{\langle v \rangle} \in PGO(\mathfrak{O}) \iff \langle v \rangle \in PSL(\mathfrak{O}). \]

In fact, whenever \( \langle v \rangle \in PGL(\mathfrak{O}) \), we have \( U_{\langle v \rangle} = \tilde{r}_1 \tilde{r}_v \) by (4.17), which implies \( U_{\langle v \rangle} \in PSO(\mathfrak{O}) \). Therefore, \( U_{\langle v \rangle} \in P\Omega(\mathfrak{O}) \) iff \( \langle v \rangle \in PSL(\mathfrak{O}) \) and we will show later (6.7) that the same is true for \( L_{\langle v \rangle} \) and \( R_{\langle v \rangle} \).

The following lemma will be very useful.

**Lemma 11.** Let \( x, y \in \mathfrak{O} \) be non-zero singular elements. Then

(i) \( x \mathfrak{O} \) and \( \mathfrak{O} x \) are t.s. 4-subspaces of \( \mathfrak{O} \),
(ii) every t.s. 4-subspace of \( \mathfrak{O} \) has form \( x \mathfrak{O} \) or \( \mathfrak{O} x \) for some \( x \),
(iii) \( \langle x \rangle = \langle y \rangle \iff x \mathfrak{O} = y \mathfrak{O} \iff \mathfrak{O} x = \mathfrak{O} y \),
(iv) \( a \in x \mathfrak{O} \iff \bar{x} a = 0 \), and \( a \in \mathfrak{O} x \iff a \bar{x} = 0 \),
(v) \( \langle x, y \rangle \neq 0 \iff \dim(x \mathfrak{O} \cap y \mathfrak{O}) = 0 \),
(vi) \( \langle x, y \rangle = 0 \) and \( \langle x \rangle \neq \langle y \rangle \) if and only if \( \dim(x \mathfrak{O} \cap y \mathfrak{O}) = 2 \),

in which case \( x \mathfrak{O} \cap y \mathfrak{O} = x(\bar{y} \mathfrak{O}) = y(\bar{x} \mathfrak{O}) \),

(vii) \( xy = 0 \iff \dim(x \mathfrak{O} \cap y \mathfrak{O}) = 3 \),
(viii) \( xy \neq 0 \iff \dim(x \mathfrak{O} \cap y \mathfrak{O}) = 1 \).
Proof. These properties are well known. For a proof, see, e.g., [11, §2]. □

This lemma shows that all t.s. 4-subspaces of $O$ are naturally divided in two equal families: those of form $xO$ and $Ox$, any two members belonging to the same family iff they intersect in a subspace of even dimension.

5. Automorphisms of the Cayley algebra

Every $x \in O$ satisfies the quadratic equation $x^2 - (\bar{x} + x)x + \bar{x}x = 0$, where $\bar{x} + x$ and $\bar{x}x = Q(x)$ are in $F$. Clearly, if $x \notin F$ then the coefficients of a monic quadratic equation satisfied by $x$ are uniquely determined. Therefore, every automorphism $f$ of $O$ must preserve the form $Q$, since $1f = 1$ also holds. These requirements however are not sufficient to characterize the automorphisms $O$. We obtain certain sufficient conditions for a linear transformation of $O$ to be an automorphism.

Let $A \in \{F, P\}$ be a commutative subalgebra of $O$ defined by (4.10). By Lemma 9 and (4.12), $O$ is a 4-dimensional left and right $A$-module with basis $w$ (4.11). Every left $A$-(semi)linear transformation $f$ of $A^\perp$ is also right $A$-(semi)linear, since by (9.i)

\[(va)f = (\bar{a}v)f = (\bar{a}\tau)(vf) = (vf)(a\tau) \quad (5.1)\]

holds for every $v \in A^\perp$ and $a \in A$, where $\tau$ is the identity mapping or the involution of $A$ according as $f$ is $A$-linear or $A$-semilinear. Put

\[
\lambda = \begin{cases} 
  e_2 + f_2 + sf_1, & \text{if } A = F, \\
  te_1 + t^{-1}f_1, & \text{if } A = P,
\end{cases} \quad (5.2)
\]

where $s, t \in F$ are such that $x^2 - sx + 1$ is irreducible in $F[x]$ with roots of order $q + 1$ and $t$ generates $F^*$. Then $\lambda$ has order $q + 1$ and $q - 1$ in the respective cases $A = F$ and $A = P$. Note that $\lambda - \bar{\lambda}$ is invertible in $A$ unless $A = P$ and $q = 2, 3$. We will assume that $q \geq 4$ in this case.

For arbitrary $x, y \in O$, define

\[k_A(x, y) = \frac{\lambda(x, y) - (x, \lambda y)}{\lambda - \bar{\lambda}}. \quad (5.3)\]

Lemma 12. We have

(i) $k_A$ is an $A$-sesquilinear form on $O$,
(ii) $k_A(x, x) = Q(x)$,
(iii) $w$ is a $k_A$-orthonormal $A$-basis of $O$.
(iv) $k_A$ is non-degenerate.

Proof. (i) Let $x, y \in O$. Additivity of $k_A$ in both arguments is obvious. By (8.vii–viii),

\[
\lambda k_A(x, y)(\lambda - \bar{\lambda}) = \lambda^2(x, y) - \lambda(x, \lambda y),
\]

\[
k_A(\lambda x, y)(\lambda - \bar{\lambda}) = \lambda(\lambda x, y) - (\lambda x, \lambda y) = \lambda(x, \bar{\lambda}y) - \bar{\lambda}\lambda(x, y).
\]

Subtracting the right-hand sides, we obtain
\[ \lambda^2(x, y) - \lambda(x, (\lambda + \bar{\lambda})y) + \lambda \bar{\lambda}(x, y) = (\lambda^2 - \lambda(\lambda + \bar{\lambda}) + \lambda \bar{\lambda})(x, y) = 0. \]

Hence, \( k_A(\lambda x, y) = \lambda k_A(x, y) \). Also,

\[ k_A(y, x)(\lambda - \bar{\lambda}) = \lambda(y, x) - (x, \lambda y) = \lambda(x, y) - (\lambda x, y), \]

\[ k_A(x, y)(\bar{\lambda} - \lambda) = \bar{\lambda}(x, y) - (x, \bar{\lambda} y) = \bar{\lambda}(x, y) - (\bar{\lambda} x, y). \]

Summing the right-hand sides, we obtain \((\lambda + \bar{\lambda})(x, y) - ((\lambda + \bar{\lambda})x, y) = 0\). Hence, \( k_A(x, y) = k_A(y, x) \). These remarks imply that \( k_A \) is \( A \)-sesquilinear.

(ii) Using (8.viii), we have

\[ k_A(x, x)(\lambda - \bar{\lambda}) = \lambda(x, x) - (x, \lambda x) = 2\lambda Q(x) - (1, (\lambda x)\bar{\lambda}) = 2\lambda Q(x) - Q(1, \lambda) = Q(x)(\lambda - \bar{\lambda}). \]

(iii) Since \( Aw_i \perp Aw_j \) for \( i \neq j \), we have \( k_A(w_i, w_j) = 0 \). Also, \( k_A(w_i, w_i) = Q(w_i) = 1 \) for \( 1 \leq i \leq 4 \) by (ii). Thus, \( \mathfrak{w} \) is \( r_A \)-orthonormal.

(iv) This follows from (iii).

Although \( \lambda \) appears in the definition (5.3), the form \( k_A \) depends only on \( A \). Indeed, if \( A = \langle 1, \lambda_0 \rangle_F \) for some \( \lambda_0 = a\lambda + b \in A \) with \( a, b \in F \), \( a \neq 0 \), then substituting \( \lambda_0 \) for \( \lambda \) in (5.3) defines the same form. This remark allows one to define \( k_A \) in the excluded cases \( A = \mathbb{P} \) and \( q = 2, 3 \) as well. We will not need this, however.

Note also that \( A^\perp = \langle w_2, w_3, w_4 \rangle_A \) is a 3-dimensional \( A \)-module. For all \( u, v, w \in A^\perp \) define

\[ t_A(u, v, w) = k_A(u, vw). \]

(5.4)

Lemma 13. \( t_A \) is an alternating \( A \)-trilinear form on \( A^\perp \).

Proof. Additivity of \( t_A \) in all arguments is obvious. Take \( u, v, w \in A^\perp \). We have \( t_A(au, v, w) = at_A(u, v, w) \) for \( a \in A \), since \( k_A \) is \( A \)-linear in the first argument. Also, (9.ii) implies \( t_A(u, v, v) = k_A(u, -\bar{v}v) = -Q(v)k_A(u, 1) = 0 \). It remains to show that \( t_A(u, v, w) = t_A(v, w, u) \). By (9.vi), we obtain

\[ k_A(u, vw)(\lambda - \bar{\lambda}) = \lambda(u, vw) - (u, \lambda(vw)) = \lambda(\bar{\lambda}u, w) - (\bar{\lambda}u, \lambda vw) = -\lambda(vu, w) + (\bar{\lambda}u, \bar{\lambda}vw), \]

\[ k_A(v, wu)(\lambda - \bar{\lambda}) = \lambda(v, wu) - (v, \lambda(wu)) = \lambda(v\bar{w}, w) - (v, w(u\lambda)) = -\lambda(vu, w) - (\bar{\lambda}v, u\lambda). \]

Subtracting the right-hand sides gives

\[ (\bar{\lambda}u, \bar{\lambda}vw) + (\bar{\lambda}v, u\lambda) = (u\lambda, \bar{\lambda}vw) + (u\lambda, \bar{\lambda}vw) = (u\lambda, \bar{\lambda}vw + \bar{\lambda}vw) = (v, \bar{\lambda}u\lambda, 1) = 0, \]

since \( u\lambda \in A^\perp \). Thus, \( t_A(u, v, w) = t_A(v, w, u) \). \( \square \)
If \( V \) is an \( A \)-submodule of \( \mathcal{O} \) then the orthogonal complement \( V^\perp \) is the same whether considered with respect to \( Q \) or \( k_A \). In particular, a non-degenerate \( A \)-(semi)linear transformation \( f \) of \( \mathcal{O} \) that preserves the form \( k_A \) and leaves \( V \) invariant also leaves \( V^\perp \) invariant.

**Lemma 14.** A non-degenerate \( A \)-(semi)linear transformation \( f \) of \( \mathcal{O} \) that satisfies \( 1f = 1 \) and preserves the forms \( k_A \) and \( t_A \) is an automorphism of \( \mathcal{O} \).

**Proof.** Let \( f \) be as stated. Then both \( A \) and \( A^\perp \) are \( f \)-invariant; hence, it is correct to say that \( f \) preserves \( t_A \). For arbitrary \( x, y, z \in A^\perp \), we have

\[
k_A(xf, (yz)f) = k_A(x, yz) = t_A(x, y, z) = t_A(xf, yf, zf) = k_A(xf, (yf)(zf)).
\]

Since \( f \) is non-degenerate, \( xf \) runs through \( A^\perp \) as \( x \) does. By non-degeneracy of \( k_A \), we have \((yz)f = (yf)(zf)\). For arbitrary \( y, z \in \mathcal{O} \) the claim holds by \( A \)-(semi)linearity and by (5.1). \( \square \)

This lemma gives a sufficient condition for \( f \) to be an automorphism. However, not every automorphism of \( \mathcal{O} \) leaves \( A \) invariant. To obtain a necessary and sufficient condition, one could similarly introduce the trilinear form \( t(u, v, w) = (u, vw) \) on the 7-dimensional \( F \)-space \( F^\perp \). Then any \( F \)-linear transformation \( f \) of \( \mathcal{O} \) is an automorphism if and only if it satisfies \( 1f = 1 \) and preserves both \((\cdot, \cdot)\) and \( t \). This fact can be proved as Lemma 14 above.

The full group of automorphisms \( \text{Aut}(\mathcal{O}(q)) \) is known to be isomorphic to the Chevalley group \( G_2(q) \) of order \( q^6(q^6 - 1)(q^2 - 1) \) (see Chapter 2 in [23]). We will require an explicit form of this 8-dimensional representation of \( G_2(q) \). Introduce some basic automorphisms of \( \mathcal{O} \). For every \( C \in SL_3(q) \), define

\[
\delta_0(C) : \begin{pmatrix} a & v \\ w & b \end{pmatrix} \mapsto \begin{pmatrix} a & v \\ wC & b \end{pmatrix},
\]

and, for every \( c \in F^3 \), put

\[
\delta_1(c) : \begin{pmatrix} a & v \\ w & b \end{pmatrix} \mapsto \begin{pmatrix} a & v \\ w & b \end{pmatrix} + \begin{pmatrix} v \cdot c & w \times c \\ (b - a)c & -v \cdot c \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ -v \cdot c & 0 \end{pmatrix},
\]

\[
\delta_2(c) : \begin{pmatrix} a & v \\ w & b \end{pmatrix} \mapsto \begin{pmatrix} a & v \\ w & b \end{pmatrix} + \begin{pmatrix} w \cdot c & (a - b)c \\ -v \cdot c & w \cdot c \end{pmatrix} + \begin{pmatrix} 0 & -(w \cdot c)c \\ 0 & 0 \end{pmatrix}.
\]

Then \( \delta_0, \delta_1, \delta_2 \) are automorphisms of \( \mathcal{O} \). Note that \( \delta_1 \) and \( \delta_2 \) are the exponents (in the sense of §3 in [24]) of the following derivations of \( \mathcal{O} \):

\[
d_1(c) : \begin{pmatrix} a & v \\ w & b \end{pmatrix} \mapsto \begin{pmatrix} v \cdot c & w \times c \\ (b - a)c & -v \cdot c \end{pmatrix}, \quad d_2(c) : \begin{pmatrix} a & v \\ w & b \end{pmatrix} \mapsto \begin{pmatrix} w \cdot c & (a - b)c \\ -v \times c & w \cdot c \end{pmatrix}.
\]

Let

\[
\Phi = \{ \pm \omega_1, \pm \omega_2, \pm \omega_3, \pm (\omega_1 - \omega_2), \pm (\omega_2 - \omega_3), \pm (\omega_3 - \omega_1) \mid \omega_1 + \omega_2 + \omega_3 = 0 \}
\]

be a root system of type \( G_2 \). We may choose the following root subgroups:
We also note that the group $D = Aut(\mathfrak{O})$. Define the short and long fundamental roots to be $\alpha = \omega_2$ and $\beta = \omega_1 - \omega_2$. Then the system of positive roots of $\Phi$ is

$$\Pi = \left\{ \begin{array}{ll}
\omega_1 = \alpha + \beta, & \omega_2 = \alpha, \\
\omega_1 - \omega_3 = 3\alpha + 2\beta, & \omega_1 - \omega_2 = \beta, \\
\omega_2 - \omega_3 = 3\alpha + \beta & \end{array} \right\}. \quad (5.7)$$

In particular, the unipotent subgroup $U = \prod_{\omega \in \Pi} X_\omega(t)$ of $D$ contains $\delta_0(C)$ for all upper uniprotangular $C$. Define also the diagonal subgroup

$$H = \{ \delta_0(C) \mid C = \text{diag}(h_1, h_2, h_3) \in SL_3(q) \}. \quad (5.8)$$

(For all these notions, see [18]. See also pp. 142–143 in [15].)

The group $D = Aut(\mathfrak{O})$ lies in $\Omega(\mathfrak{O})$ and induces automorphisms of all loops (4.14) associated with $\mathfrak{O}$. We identify $D$ with its image $\tilde{D}$ in $P\Omega(\mathfrak{O})$. Note that $D$ commutes with $S$ and thus coincides with the $D = C_G(S)$ introduced after Lemma 5. Indeed, for every 0-point $\langle x \rangle$ and every $f \in D$, we have

$$\langle x \rangle f \sigma = \langle x f \rangle \sigma = \langle \overline{x f} \rangle = \langle \overline{x} f \rangle = \langle x \rangle \sigma f,$$

$$\langle x \rangle f \rho = \langle x f \rangle \rho = \langle \overline{x f} \rangle = \langle \overline{x} \rangle f = \langle x \rangle \rho f.$$  

The two actions of $D$ on $PSL(\mathfrak{O})$ and $\mathcal{M}(P\Omega(\mathfrak{O}))$ are respected by the isomorphism (6.5), since, for every $m = [g, \sigma] \in \mathcal{M}(P\Omega(\mathfrak{O}))$, we have

$$(m^f)_\theta = [g^f, \sigma]_\theta = \langle 1 \rangle f^{-1} g f = \langle 1 \rangle g f = (m\theta) f.$$  

We also note that $D$ is the group of inner automorphisms of $PSL(\mathfrak{O})$ (see Proposition 2 in [2]). As follows from [20], the full group $Aut(M(q))$ is the extension of $G_2(q)$ by its field automorphisms.

| Table 4 |
|---|---|---|
| **Type** | **Order** | **Comments** |
| $P_\alpha$ | $q^6(q^2-1)^2(q+1)$ | Parabolic, short root |
| $P_\beta$ | $q^6(q^2-1)^2(q+1)$ | Parabolic, long root |
| $(SL_2(q) \circ SL_2(q)) \cdot d$ | $q^2(q^2-1)^2$ | $q \neq 2$ |
| $2^3 \cdot PSL_3(2)$ | $8 \cdot 168$ | $q = p$ odd |
| $G_2(q_0)$ | $q_0^6(q_0^2-1)(q_0^2-1)$ | $q = q_0^k$, $k$ prime |
| $G_2(2)$ | $2^6 \cdot 3^3 \cdot 7$ | $q = p$ odd |
| $SL_3(q) : 2$ | $2q^3(q^3-1)(q^2-1)$ | $q$ arbitrary |
| $SU_3(q) : 2$ | $2q^3(q^3+1)(q^2-1)$ | $q$ arbitrary |
For our purposes, we need to know certain maximal subgroups of $G_2(q)$. Table 4 is a consequence of the papers [21,22]. The notation is mostly preserved.

6. The geometry of triality

Let $\mathfrak{P}$ be the polar geometry associated with $Q$. This geometry consists of objects of four types: all t.s. 1-subspaces $\langle x \rangle$ of $\mathbb{O}$ called 0-points of $\mathfrak{P}$, all t.s. 2-subspaces of $\mathbb{O}$ called lines of $\mathfrak{P}$, all t.s. 4-subspaces of form $x\mathbb{O}$ called $l$-points, and all t.s. 4-subspaces of form $\mathbb{O}x$ called $r$-points of $\mathfrak{P}$. The incidence between these objects is natural (the inclusion) except that an $l$-point is incident with an $r$-point iff they intersect in a 3-space.

An automorphism of $\mathfrak{P}$ is a transformation of $\mathfrak{P}$ that preserves the type of objects and the incidence relation between them. The group $P\Omega(\mathbb{O})$ acts naturally by automorphisms on $\mathfrak{P}$ and it is known that the full group $\text{Aut}(\mathfrak{P})$ is just the extension of $P\Omega(\mathbb{O})$ by its field and diagonal automorphisms (see, e.g., [9, p. 203]).

Remark 15. The group $P\Omega(\mathbb{O})$ is faithfully represented as group of permutations on each of the four types of objects of $\mathfrak{P}$. In particular, an element $g \in P\Omega(\mathbb{O})$ is identity if and only if it stabilizes all 0-points of $\mathfrak{P}$.

The remarkable property of the geometry $\mathfrak{P}$, often called triality, is that besides automorphisms it also admits transformations that preserve the incidence but permute the three types of points. These can be defined in the following way. Let $\rho$ be the transformation of $\mathfrak{P}$ that acts on the points by the rule

$$\langle x \rangle \mapsto^\rho \bar{x}\mathbb{O}, \quad x\mathbb{O} \mapsto^\rho \bar{x}\mathbb{O}, \quad \mathbb{O}x \mapsto^\rho \bar{x}\mathbb{O}, \quad \langle x, y \rangle \mapsto^\rho \langle \bar{x}, \bar{y} \rangle.$$

This action is uniquely extended to the lines of $\mathfrak{P}$ to preserve incidence: for example, if $\langle x \rangle$ and $\langle y \rangle$ are 0-points on a line $l$ then $l\rho = \bar{x}\mathbb{O} \cap \bar{y}\mathbb{O}$. We also define $\sigma = \check{r}_1 \in \text{PGO}(\mathbb{O})$, i.e., the action of $\sigma$ on all objects is induced by the conjugation:

For details, see [11,12]. Clearly, $\rho$ and $\sigma$ normalize $\text{Aut}(\mathfrak{P})$ and, in particular, its characteristic subgroup $P\Omega(\mathbb{O})$. We henceforth denote $S = \langle \rho, \sigma \rangle$, where $\rho$ and $\sigma$ are defined by (6.1) and (6.2).

Lemma 16. $P\Omega(\mathbb{O})$ is a group with triality $S$.

Proof. The fact that $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ (identical mappings of $\mathfrak{P}$) is obvious from the definitions (6.1) and (6.2). Take $g \in P\Omega(\mathbb{O})$ and let $v \in \mathbb{O}$ be such that $\langle 1 \rangle g = \langle v \rangle$. Note that $v$ is non-singular. Then $[g, \sigma] = \sigma^g\sigma = \check{r}_v\check{r}_1$ by (10.iii). Hence, for all points $\langle x \rangle, x\mathbb{O}, \mathbb{O}x$ of $\mathfrak{P}$, we have
\[
\langle x \rangle \mathcal{g}_\sigma = \langle x \rangle \mathcal{r}_1 = \langle v(x) \rangle,
\]
\[
(x \mathcal{O})[g, \sigma] = (v(x) \mathcal{O}) \mathcal{r}_1 = (v(x)) \mathcal{O},
\]
\[
(\mathcal{O} x)[g, \sigma] = (v(x)) \mathcal{r}_1 = ((v(x)) \mathcal{O}) \mathcal{r}_1 = (v(x) \mathcal{O}),
\] (6.3)

where we have used (4.17), (7.i), and the fact that \( v \) is non-singular. Then

\[
\langle x \rangle \mathcal{g}_\sigma \rho = \langle x \rangle \rho - 1 \mathcal{g}_\sigma \rho = (v(x)) \mathcal{O} \mathcal{g}_\sigma \rho = (v(x)) \mathcal{O},
\]
(6.4)

Therefore,

\[
\langle x \rangle \mathcal{g}_\sigma \rho_2 = \langle x \rangle \rho - 1 \mathcal{g}_\sigma \rho_2 = (v(x)) \mathcal{O} \mathcal{g}_\sigma \rho_2 = (v(x)) \mathcal{O}.
\] (6.5)

There are now two ways to associate the simple Moufang loop \( M(q) \) with the Cayley algebra \( \mathcal{O} \); namely, taking the loops \( \text{PSL}(\mathcal{O}) \) and \( M(\text{P}_\mathcal{O}(\mathcal{O})) \). We construct an explicit isomorphism between these loops. Define the mapping

\[
\theta : M(\text{P}_\mathcal{O}(\mathcal{O})) \rightarrow \text{PSL}(\mathcal{O})
\]
(6.5)

as follows: given an \( m = [g, \sigma] \in M(\text{P}_\mathcal{O}(\mathcal{O})) \), put \( m\theta = (1)g \). Then \( m\theta \in \text{PSL}(\mathcal{O}) \), since \( (1)g \) is a +1-subspace. Note that

\[
[g_1, \sigma] = [g_2, \sigma] \Leftrightarrow g_1 g_2^{-1} \in C_{\text{P}_\mathcal{O}(\mathcal{O})}(\sigma) \Leftrightarrow (1)g_1 = (1)g_2
\]
by (10.iv). This implies that \( \theta \) is well defined and injective. It is also surjective, since \( \text{P}_\mathcal{O}(\mathcal{O}) \) is transitive on +1-subspaces (see [10, Lemma 2.10.5]). Therefore, for every \( m \in M(\text{P}_\mathcal{O}(\mathcal{O})) \), we have

\[
m\theta = v \Leftrightarrow \langle x \rangle m = \langle v(x) \rangle \quad \text{for all 0-points} \ \langle x \rangle \in \mathcal{P}
\]
(6.6)

by the first equality in (6.3).

**Lemma 17.** \( \theta \) is a loop isomorphism of \( M(\text{P}_\mathcal{O}(\mathcal{O})) \) and \( \text{PSL}(\mathcal{O}) \).

**Proof.** Take \( m, n \in M(\text{P}_\mathcal{O}(\mathcal{O})) \) and write \( m = [g, \sigma], \ n = [h, \sigma] \) for suitable \( g, h \in \text{P}_\mathcal{O}(\mathcal{O}) \). Let \((1)g = (v)\) and \((1)h = (w)\). Note that \( m^{-1} = [g^\sigma, \sigma] \) and

\[
(1)g^\sigma = (1)\sigma g \sigma = (1)g \sigma = (v)\sigma = (\bar{v})
\]

Therefore, using (6.3), (6.4), and (7.iv), we have
\[\langle x \rangle (m.n) = \langle x \rangle m^{-\rho} nm^{-\rho} = \left((\bar{w}(\bar{v}x\bar{w}))\bar{v}\right) = \left((\bar{v}w)x(\bar{v}w)\right)\]

for every 0-point \(x \in \mathcal{P}\). By (6.6), we have \((m.n)\theta = (vw) = (m\theta)(n\theta)\). \(\square\)

As a consequence, we have the following useful description:

**Corollary 18.** Let \(G_0\) be an arbitrary \(S\)-subgroup of \(P\Omega(\mathfrak{O})\). Then \(\mathcal{M}(G_0)\theta = \langle 1 \rangle^{G_0}\), where multiplication on the orbit \(\langle 1 \rangle^{G_0}\) is induced from \(\mathfrak{O}\).

We can also write the action of \(\rho\) on \(\mathcal{M}(P\Omega(\mathfrak{O}))\) in terms of the operators \(U_{(v)}, L_{(v)}, R_{(v)}\).

Using (6.6), (6.4), and Remark 15 we have

\[
\begin{align*}
\mathcal{M}(P\Omega(\mathfrak{O})) &= \{U_{(v)} \mid \langle v \rangle \in PSL(\mathfrak{O})\}, \\
\mathcal{M}(P\Omega(\mathfrak{O}))^\rho &= \{L_{(v)} \mid \langle v \rangle \in PSL(\mathfrak{O})\}, \\
\mathcal{M}(P\Omega(\mathfrak{O}))^{\rho^2} &= \{R_{(v)} \mid \langle v \rangle \in PSL(\mathfrak{O})\},
\end{align*}
\]

and

\[
U_{(v)} \mapsto_{\rho} L_{(v)} \mapsto_{\rho} R_{(v)} \mapsto_{\rho} U_{(v)}.
\] (6.8)

**7. The maximal subloops of \(M(q)\)**

First, we introduce 5 types of subloops of the simple loop \(PSL(\mathfrak{O}) \cong M(q)\). Then we will show that they exhaust all maximal subloops of this loop.

1. **Maximal parabolic subloop**, \(q\) arbitrary. Consider all Zorn matrices of the form

\[
\begin{pmatrix}
    a_1 \\
    (r_2, a_4, 0) \\
    a_2
\end{pmatrix}
\begin{pmatrix}
    (0, a_3, r_1) \\
    a_1
\end{pmatrix},
\quad a_1a_2 - a_3a_4 = 1.
\] (7.1)

It can be verified using (4.4) that they form a subloop of \(SL(\mathfrak{O})\) whose order is \(q^3(q^2 - 1)\). Its image \(P\) in \(PSL(\mathfrak{O})\) will be called a parabolic subloop of \(PSL(\mathfrak{O})\). Note that \(|P| = q^3(q^2 - 1)\) and \(P = q^2 : PSL_2(q)\), i.e., \(P\) has a normal elementary abelian subgroup of order \(q^2\) that corresponds to the matrices (7.1) with \(a_1 = a_2 = 1, a_3 = a_4 = 0\); extended by a subgroup isomorphic to \(PSL_2(q)\) that corresponds to the matrices (7.1) with \(r_1 = r_2 = 0\). Note that \(P\) is always nonassociative.

2. \(M(PSL_2(q), 2), q \neq 3\). Recall the process of duplication of a group introduced by Chein in Theorem 1 of [13]. Let \(H\) be a group. The set of \(2|H|\) symbols \(\{h, \tilde{h} \mid h \in H\}\) with a new multiplication ‘·’ defined by

\[
g \cdot h = gh, \quad g \cdot \tilde{h} = \tilde{h}g, \quad \tilde{g} \cdot h = gh^{-1}, \quad \tilde{g} \cdot \tilde{h} = h^{-1}g
\] (7.2)

for all \(g, h \in H\) becomes a Moufang loop. We denote it by \(M(H, 2)\). Clearly, \(H\) is embedded in \(M(H, 2)\) as a normal subgroup of index 2. Fixing an arbitrary \(u \in M(H, 2) \setminus H\), every element of \(M(H, 2)\) is uniquely written as \(h\) or \(h \cdot u\) for suitable \(h \in H\). Then, suppressing the ‘·,’ we can rewrite (7.2) as
It can be seen that $M(H, 2)$ is non-associative iff $H$ is non-abelian.

Now consider the Zorn matrices of the two types

\[
\begin{pmatrix}
a_1 \\
(a_3, 0, 0) \\
0
\end{pmatrix}, \quad a_1a_4 - a_2a_3 = 1,
\]

\[
\begin{pmatrix}
0 \quad (a_2, 0, 0) \\
(0, r_2, r_4) \\
0
\end{pmatrix}, \quad r_1r_2 + r_3r_4 = -1. 
\]

(7.4)

They form a subloop of $SL(\mathbb{O})$ which has a subgroup of index 2 isomorphic to $SL_2(q)$ formed by the matrices of the first type. It can be verified that the image of this subloop in $PSL(\mathbb{O})$ is isomorphic to the duplication $M(PSL_2(q), 2)$ of order $2q(q^2 - 1)$.

(3) Field subloop $M(q_0), q = q_0^k$ for prime $k$ and $k \neq 2$ if $q$ is odd. Clearly, $PSL(\mathbb{O})$ contains a naturally embedded copy of the loop $PSL(\mathbb{O}(q_0))$ with respect to the standard basis $\{e_1, \ldots, f_4\}$ of $\mathbb{O}$.

(4) $PGL(\mathbb{O}(q_0)), q = q_0^2$ odd. In this case, the field subloop $PSL(\mathbb{O}(q_0))$ of $PSL(\mathbb{O})$ is of index 2 in a larger subloop. Namely, consider the mapping $\varphi : GL(\mathbb{O}(q_0)) \rightarrow PSL(\mathbb{O}(q_0))$ defined by $x \mapsto \langle x \rangle_{F_q}$. It is well defined as every element in $F_{q_0}^{*}$ is a square in $F_{q}^{*}$. It is easy to see that $\varphi$ is a homomorphism of loops with kernel $\langle 1 \rangle_{F_{q_0}}$. Therefore, $PGL(\mathbb{O}(q_0))$ is embedded in $PSL(\mathbb{O}(q))$ as a subloop of order $q_0^3(q_0^4 - 1)$.

(5) $M(2), q = p$ is an odd prime. This is the most interesting case as the corresponding embedding of subloops is cross-characteristic (see Lemma 21 below). Consider the real Cayley algebra $O(\mathbb{R})$, which can be defined as an 8-dimensional algebra over $\mathbb{R}$ with a unit spanned by the elements $\{1 = \epsilon_0, \epsilon_1, \ldots, \epsilon_7\}$ that multiply as in Table 3. The quadratic form defined by (4.9) turns $O(\mathbb{R})$ into a Euclidean space. We define the conjugation on the basis by (4.8) and extend it by linearity. Then $O(\mathbb{R})$ satisfies (8.iii–vii). It was shown in [17] that $O(\mathbb{R})$ contains a certain set $\Phi$ of 240 elements of norm 1, called the units of integral Cayley numbers, which is multiplicatively closed, contains 1, and such that $\Phi = \Phi$. In other words, $\Phi$ is a loop. This set can be defined in terms of an $f_0$-orthonormal basis $\{l_1, \ldots, l_8\}$ of $O(\mathbb{R})$, where

\[
l_1 = \frac{1}{2}(\epsilon_0 + \epsilon_3), \quad l_3 = \frac{1}{2}(\epsilon_2 + \epsilon_5), \quad l_5 = \frac{1}{2}(\epsilon_1 + \epsilon_7), \quad l_7 = \frac{1}{2}(\epsilon_6 + \epsilon_4),
\]

\[
l_2 = \frac{1}{2}(\epsilon_0 - \epsilon_3), \quad l_4 = \frac{1}{2}(\epsilon_2 - \epsilon_5), \quad l_6 = \frac{1}{2}(\epsilon_1 - \epsilon_7), \quad l_8 = \frac{1}{2}(\epsilon_6 - \epsilon_4),
\]

as follows:

\[
\Phi = \left\{ \pm l_s \pm l_t; \ 1 \leq s, t \leq 8, \ s \neq t, \frac{1}{2}(i_1l_1 + i_2l_2 + \cdots + i_8l_8); \ i_s = \pm 1, \ i_1i_2 \ldots i_8 = 1 \right\}. 
\]

(7.6)

We have changed here the sign of one of Coxeter’s $l_i$’s (see [17, §10]) so that the product $i_1i_2 \ldots i_8$ in (7.6) be equal to 1. Then (7.6) coincides with the standard definition of a root system of type $E_8$. Call a subset $\Pi \subset \Phi$ a fundamental system of roots if

(1) $\Pi$ is a basis of $O(\mathbb{R})$;

(2) the coefficients of every $u \in \Phi$ in $\Pi$ are either all non-negative or all non-positive.
The standard fundamental system $\Pi$ of $\Phi$ is shown in the Dynkin diagram (7.7), in which two elements $a, b \in \Pi$ are joined iff $(a, b) = -1$ and disjoint iff $(a, b) = 0$ (for all of this, see, e.g., [18]),

\[
\begin{align*}
l_1 - l_2 & \quad l_2 - l_3 \quad l_3 - l_4 \quad l_4 - l_5 \quad l_5 - l_6 \quad l_6 + l_7 \quad -\frac{1}{2}(l_1 + \cdots + l_8) \\
l_6 - l_7
\end{align*}
\]

(7.7)

Let $W$ be the Weyl group of $\Phi$, which is by definition the group generated by the reflections $r_u$ for all $u \in \Phi$. It is known that $W$ is in fact generated by $r_u$ for $u \in \Pi$ and is isomorphic to the double cover 2. $P\Omega_8^+(2)$. (see §4 of Chapter VI in [19]). Let $W_0 = W' \cong 2. P\Omega_8^+(2)$. Note that

\[
W_0 = \langle r_u r_1 \mid u \in \Pi \rangle = \langle U_\Pi \mid u \in \Pi \rangle.
\]

(7.8)

**Lemma 19.** $W_0$ acts transitively on $\Phi$.

**Proof.** Take $u \in \Phi$. First of all, every $u$ is $W$-conjugate to a fundamental root in $\Pi$ (see [18, Proposition 2.1.8]). Let $w \in W$ be such that $uw = a \in \Pi$. If $w \notin W_0$, take $b \in \Phi$ orthogonal to $a$, e.g., a fundamental root not joined with $a$ by an edge in (7.7). Then $uwr_b = a$ and $wrb \in W_0$. Now if $a, b \in \Pi$ are joined by an edge in (7.7) then $(a, b) = -1$ and $ar_b = a - (a, b)b = a + b$. Similarly, $br_a = a + b$. Hence, $ar_br_a = b$. Since $r_ar_b \in W_0$ and (7.7) is connected, all fundamental roots are $W_0$-conjugate and the claim follows. \qed

**Lemma 20.** $W = N_{GO(O(\mathbb{R}))}(\Phi)$. In particular, $L_u, R_u \in W$ for all $u \in \Phi$.

**Proof.** Let $g \in GO(O(\mathbb{R}))$ leave $\Phi$ fixed. It is easy to see that $\Pi g$ is also a fundamental system of $\Phi$. However, all fundamental systems are $W$-conjugate by Theorem 2.2.4 in [18], i.e., $\Pi gw = \Pi$ for some $w \in W$. Since $gw$ preserves the scalar product and the diagram (7.7) has no non-trivial symmetries, $gw$ acts identically on $\Pi$, i.e., $g = w^{-1} \in W$. Clearly, $L_u, R_u \in N_{GO(O(\mathbb{R}))}(\Phi)$ for all $u \in \Phi$ and the claim follows. \qed

Note that all coefficients of every $u \in \Phi$ in the original basis $\{\varepsilon_0, \ldots, \varepsilon_7\}$ belong to $\{0, \pm 1, \pm \frac{1}{2}\}$. Moreover, it can be seen from (4.16) that all matrix coefficients of every $w \in W$ in the basis $\{\varepsilon_0, \ldots, \varepsilon_7\}$ are in $\mathbb{Z}[\frac{1}{2}]$, since $\Phi$ is multiplicatively closed and $-\Phi = \Phi$. These remarks show that $\Phi$ is a subloop of $SL(O(\mathbb{Z}[\frac{1}{2}]))$ and $W$ is a subgroup of $GO(O(\mathbb{Z}[\frac{1}{2}]))$. We can now perform the $p$-reduction $\mathbb{Z}[\frac{1}{2}] \otimes \mathbb{Z}_p \cong F_p$ to identify $\Phi$ and $W$ with their respective images in $SL(\mathcal{O})$ and $GO(\mathcal{O})$ (recall that $\mathcal{O}$ stands for $\mathcal{O}(q)$ and $q = p$ in the present case). Denote by $\Phi$ the image of $\Phi$ in $PSL(\mathcal{O})$. Clearly, it is a subloop there of order 120. It is now easy to determine its isomorphism type. Note that $\mathcal{W}_0 \cong P\Omega_8^+(2)$ is an S-subgroup of $P\Omega(\mathcal{O})$. Indeed, $\mathcal{W}_0$ is $\sigma$-invariant since $\sigma = \tilde{r}_1 \in \mathcal{W}$. It is also $\rho$-invariant by (7.8), (6.8), and Lemma 20. Finally, the Moufang loop $\mathcal{M}(\mathcal{W}_0) \cong M(2)$ is isomorphic by Corollary 18 to $\langle 1 \rangle \mathcal{W}_0 < PSL(\mathcal{O})$ which is exactly $\Phi$ by Lemma 19. In other words, we have proved the following result:
Lemma 21. The simple loop $M(2)$ of order 120 is embedded into the simple loop $M(p)$ for every odd prime $p$.

Observe that the construction given above provides an explicit embedding $M(2) \hookrightarrow M(p)$.

Our aim is to show that the above 5 types of subloops are maximal and the only maximal subloops of $M(q)$ up to isomorphism, provided the indicated restrictions on $q$ are satisfied. We will need several auxiliary lemmas.

Lemma 22. The set of element orders of the loop $M(q)$ is the set of all divisors of the numbers $\frac{1}{d}(q - 1), \frac{1}{d}(q + 1),$ and $p$.

Proof. For every pair of vectors $v, w \in F^3$, we can find a matrix $C \in SL_3(q)$ such that both $vC$ and $wC^{-1}$ are in $(i)$, where $i = (1, 0, 0)$. Then the automorphism $\delta_0(C)$ sends an arbitrary $x \in SL(\mathbb{O})$ of form (4.3) to an element of the first form in (7.4). This shows that every element of $PSL(\mathbb{O})$ is conjugate by an automorphism to an element of the subgroup $PSL_2(q) \leq PSL(\mathbb{O})$. Hence the set of element orders of $M(q)$ is equal to that of $PSL_2(q)$, which is known to consist of all divisors of the numbers $\frac{1}{d}(q - 1), \frac{1}{d}(q + 1),$ and $p$ (see [16]). \hfill \Box

Lemma 23. The subloops of $PSL(\mathbb{O}(q))$ of the types 1–5 above are not embedded into each other, provided the indicated restrictions on $q$ are satisfied.

Proof. Suppose that $M$ and $N$ are subloops of types 1–5 and $M < N$. By Lagrange’s theorem (see [1]), $|M|$ divides $|N|$. It can be seen that only the following cases are possible:

(a) $q$ is even, $N$ is parabolic, and either $M = M(PSL_2(q), 2)$ or $q = q_0^2$ and $M$ is a field subloop of order $q_0^3(q_0^4 - 1)$. Then $M$ must intersect non-trivially the normal 2-subgroup of $N$. However, $M$ itself does not have normal 2-subgroups, a contradiction.

(b) $q = p$ is an odd prime, $M \cong M(2)$, and $N$ is either $M(PSL_2(q), 2)$ or parabolic, and 120 divides $|N|$. The embedding $M < N$ is impossible, since the composition factors of $N$ are groups while $M$ is simple and non-associative.

(c) $q = q_0^3, M = M(PSL_2(q), 2)$ and $N$ is a field subloop $PSL(\mathbb{O}(q_0))$ or $PGL(\mathbb{O}(q_0))$ according as $q$ is even or odd. In both cases $PSL_2(q)$ must be a subgroup of $PSL(\mathbb{O}(q_0))$. However, the group $PSL_2(q)$ contains an element of order $\frac{1}{d}(q + 1)$ which $PSL(\mathbb{O}(q_0))$ does not by Lemma 22, a contradiction.

(d) $q = p = 5, N = M(2)$, and $M = M(PSL_2(5), 2)$. Although both $N$ and $M$ have order 120, they are non-isomorphic as the former is simple and the latter has a normal subloop of index 2. \hfill \Box

We note that when $q = 3$, the subloop $M(PSL_2(3), 2) \leq M(3)$ is isomorphic to a parabolic subloop of $M(2) \leq M(3)$ and thus is not maximal (see [14]).

Introduce some more definitions. Given a +4-decomposition $\mathcal{O} = V_0 \oplus V_1$, define

$$\mathcal{L}(V_0 \oplus V_1) = \{ l \in \mathbb{P} \mid l \subseteq V_0 \cup V_1 \}.$$ (7.9)

Given an $\epsilon 2$-decomposition $\mathcal{O} = V_1 \oplus V_2 \oplus V_3 \oplus V_4$, where $\epsilon = \pm 1$, define

$$\mathcal{L}(V_1 \oplus \cdots \oplus V_4) = \{ l \in \mathbb{P} \mid l \subseteq V_i \oplus V_j \text{ for } 1 \leq i < j \leq 4 \}.$$ (7.10)
Let \( d \) be a \( +4\)- or \( \epsilon \)2-decomposition of \( \Omega \). Then \( d \) is called \( S\)-invariant if the set of lines \( \mathcal{L}(d) \) is \( S\)-invariant.

**Lemma 24.** We have

(i) If a \( +4\)-decomposition \( \Omega = V_0 \oplus V_1 \) is a \( \mathbb{Z}_2 \)-grading then it is \( S\)-invariant.

(ii) If an \( \epsilon \)2-decomposition \( \Omega = V_1 \oplus \cdots \oplus V_4 \) is a \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)-grading then it is \( S\)-invariant.

**Proof.** (i) Let \( x \in V_i \) for \( i \in \mathbb{Z}_2 \). Write \( x = y_0 + y_1 \), where \( y_j \in V_j \). Then \( x = y_0 + y_1 \in V_0 \). Thus \( x = y_{i+1} = 0 \). In particular, if \( x \) is invertible then \( y_{i+1} = 0 \) and \( x = y_i \in V_i \). Note that \( V_i \) contains a basis consisting of invertible elements. By linearity, we have \( \mathcal{V}_i = V_i \) for \( i \in \mathbb{Z}_2 \).

Hence, \( \mathcal{L}(V_0 \oplus V_1) \) is \( \sigma \)-invariant.

Let \( l = \langle x, y \rangle \subseteq V_i \). First, suppose \( x \bar{y} \neq 0 \). By Lemma 11, if \( l \subseteq \Omega \bar{z} \) for some singular \( z \) then \( \langle z \rangle \subseteq l \bar{p} \). Moreover, \( xz = yz = 0 \); hence, \( (x, \bar{z}) = (y, \bar{z}) = 0 \) and \( \bar{z} \leq l \bar{y} = l \oplus V_{i+1} \). Write \( z = a \bar{x} + b \bar{y} + \bar{w} \), where \( a, b \in F, w \in V_{i+1} \). Then

\[
xz = bx \bar{y} + x \bar{w} = 0, \quad yz = ay \bar{x} + y \bar{w} = 0.
\]

By the first part of the proof, \( x \bar{y}, y \bar{x} \in V_0 \) and \( x \bar{w}, y \bar{w} \in V_1 \). Hence, \( bx \bar{y} = ay \bar{x} = 0 \). By assumption, \( a = b = 0 \); i.e., \( z \in V_{i+1} \) and \( \mathcal{L}(V_0 \oplus V_1) \subseteq l \).

Now, suppose \( x \bar{y} = 0 \). By Lemma 11, \( x \in \mathcal{O}_y \) and \( y \in \mathcal{O}_x \). Hence, \( l = \mathcal{O}_x \cap \mathcal{O}_y \). It follows that \( l \bar{p} = \langle \bar{x}, \bar{y} \rangle = \sigma l \subseteq (V_l) \sigma = V_i \) by the first part.

(ii) Let \( l \in \mathcal{L}(V_1 \oplus \cdots \oplus V_4) \). Then \( l \subseteq V_{i_1} \oplus V_{j_1} \) for some \( 1 \leq i_1 < j_1 \leq 4 \). Let \( \{i_2, j_2\} = \{1, 2, 3, 4\} \setminus \{i_1, j_1\} \). Put \( W_k = V_{i_k} \oplus V_{j_k} \), \( k = 1, 2 \). Clearly, \( \mathcal{O} = W_1 \oplus W_2 \) is a \( \mathbb{Z}_2 \)-grading of \( \Omega \) and \( l \in \mathcal{L}(W_1 \oplus W_2) \). By (i), \( l \subseteq \mathcal{L}(W_1 \oplus W_2) \subseteq \mathcal{L}(V_1 \oplus \cdots \oplus V_4) \) for every \( s \in \mathcal{S} \). \( \square \)

We can now describe the main result of this paper which is contained in Table 5 and proved in Theorem 1 below. We show that, for every type of \( S\)-maximal subgroups \( G_0 \) from Table 1, the corresponding subloops \( M(G_0) \) of \( M(q) \) are \( D\)-conjugate and hence isomorphic. (Recall that \( D = \text{Inn}(M(q)) \) is the subgroup of \( \text{Aut}(M(q)) \) isomorphic to \( G_2(q) \).) The isomorphism type of \( M(G_0) \) is shown in column III of Table 5. For convenience, we repeat in columns II and IV the restrictions on \( q \) and the order \( |M(G_0)| \) from Table 1. Column V shows “\( \sqrt{\ } \)” (“\( \sim \)”) if \( M(G_0) \) is always (never) maximal in \( M(q) \) or gives the specific values of \( q \) for which it is maximal. The normalizer in \( D \) of \( M(G_0) \) is given in column VI. The number of subloops of \( M(q) \) that correspond to \( S\)-maximal subgroups of a given type is shown in column VII.

In particular, all maximal subloops of \( M(q) \) are classified up to isomorphism.

Henceforth, we denote \( G = P\Omega(\Omega) \).

**Theorem 1.** Table 5 holds.

**Proof.** We proceed with a case-by-case analysis of the groups from Table 1.

1. \( G_0 \) is a \( P_2\)-subgroup. The parabolic subgroup \( P_2 \) is the normalizer in \( G \) of three totally singular subspaces \( p_0, p_l, p_r \) of \( \Omega \), where \( p_0 < p_l \cap p_r \), \( \dim p_0 = 1 \), \( \dim p_l = \dim p_r = 4 \), and \( \dim p_l \cap p_r = 3 \). By Lemma 11, \( P_2 \) has a nice interpretation in terms of the polar geometry \( \mathcal{P} \). It is exactly the normalizer of a triple \( \langle p_0, p_l, p_r \rangle \) of pairwise incident 0-, \( r\)-, and \( l\)-points of \( \mathcal{P} \). For brevity, call such a triple a *triangle*. Clearly, if a triangle is \( S\)-invariant then so is the corresponding parabolic subgroup. By (11.1\( a \)), (6.1), and (6.2), it is easy to see that a triangle is \( S\)-invariant
Table 5
The subloops of $M(q)$ associated with $S$-maximal subgroups of $\P_\Omega^+(q)$

<table>
<thead>
<tr>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
<th>VI</th>
<th>VII</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_0$</td>
<td>Restrictions on $q$</td>
<td>Isomorphism type of $M(G_0)$</td>
<td>$</td>
<td>M(G_0)</td>
<td>$</td>
<td>Maximality in $M(q)$</td>
</tr>
<tr>
<td>1.</td>
<td>$P_2$</td>
<td>–</td>
<td>Non-maximal parabolic</td>
<td>$\frac{1}{d}q^3(q-1)$</td>
<td>–</td>
<td>$P_\beta$</td>
</tr>
<tr>
<td>2.</td>
<td>$R_{s2}$</td>
<td>–</td>
<td>Maximal parabolic</td>
<td>$\frac{1}{d}q^3(q^2 - 1)$</td>
<td>✓</td>
<td>$P_\alpha$</td>
</tr>
<tr>
<td>3.</td>
<td>$N_1$</td>
<td>$q \geq 4$</td>
<td>$\mathbb{Z}_{\frac{1}{d}}(q+1)$</td>
<td>$\frac{1}{d}(q+1)$</td>
<td>–</td>
<td>$SU_3(q)$ : 2</td>
</tr>
<tr>
<td>4.</td>
<td>$N_2$</td>
<td>$q \geq 3$</td>
<td>$\mathbb{Z}_{\frac{1}{d}}(q-1)$</td>
<td>$\frac{1}{d}(q-1)$</td>
<td>–</td>
<td>$SL_3(q)$ : 2</td>
</tr>
<tr>
<td>5.</td>
<td>$N_4^4$</td>
<td>$q = p \geq 3$</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>8</td>
<td>–</td>
<td>$2^3 \cdot PSL_3(2)$</td>
</tr>
<tr>
<td>6.</td>
<td>$I_{+2}$</td>
<td>$q \geq 7$</td>
<td>$M(\mathbb{Z}_{\frac{1}{d}}(q-1), 2)$</td>
<td>$\frac{4}{d}(q-1)$</td>
<td>–</td>
<td>$(q - 1)^2 \cdot (S_3 \times 2)$</td>
</tr>
<tr>
<td>7.</td>
<td>$I_{-2}$</td>
<td>$q \neq 3$</td>
<td>$M(\mathbb{Z}_{\frac{1}{d}}(q+1), 2)$</td>
<td>$\frac{4}{d}(q+1)$</td>
<td>$q = 2$</td>
<td>$(q + 1)^2 \cdot (S_3 \times 2)$</td>
</tr>
<tr>
<td>8.</td>
<td>$I_{+4}$</td>
<td>$q \geq 3$</td>
<td>$M(PSL_2(q), 2)$</td>
<td>$\frac{2}{d}q(q^2 - 1)$</td>
<td>$q \geq 4$</td>
<td>$(SL_2(q) \circ SL_2(q)) \cdot d$</td>
</tr>
<tr>
<td>9.</td>
<td>$G_1^1$</td>
<td>–</td>
<td>(1)</td>
<td>1</td>
<td>–</td>
<td>$D$</td>
</tr>
<tr>
<td>10.</td>
<td>$\P_\Omega^+(q_0)$</td>
<td>$q = q_0^k$, $k$ prime, $(d, k) = 1$</td>
<td>$M(q_0)$</td>
<td>$\frac{1}{d}q_0^3(q_0^4 - 1)$</td>
<td>✓</td>
<td>$G_2(q_0)$</td>
</tr>
<tr>
<td>11.</td>
<td>$\P_\Omega^+(q_0), 2^2$</td>
<td>$q = q_0^2$, odd</td>
<td>$PGL(\mathbb{Z}(q_0))$</td>
<td>$q_0^3(q_0^4 - 1)$</td>
<td>✓</td>
<td>$G_2(q_0)$</td>
</tr>
<tr>
<td>12.</td>
<td>$\P_\Omega^+(2)$</td>
<td>$q = p \geq 3$</td>
<td>$M(2)$</td>
<td>120</td>
<td>✓</td>
<td>$G_2(2)$</td>
</tr>
</tbody>
</table>
iff it has the form \((x, x\mathcal{Q}, \mathcal{Q}x)\) for every non-zero \(x \in \mathcal{Q}\) satisfying \(x^2 = 0\). Now put \(x = e_4\). Then, by Table 2, we have \(p_0 = \langle e_4 \rangle\), \(p_1 = e_4\mathcal{Q} = \langle e_1, e_4, f_2, f_3 \rangle\), \(p_r = \mathcal{Q}e_4 = \langle e_4, f_1, f_2, f_3 \rangle\).

We may assume that \(G_0\) is the parabolic subgroup corresponding to this triangle. Thus, \(G_0\) is \(S\)-invariant. In the proof of Theorem 2, item 1 in [1], we showed that \(G_0\) acts transitively on the \(+1\)-subspaces in

\[(p_r \cap p_l)^+ = \langle e_1, e_4, f_1, f_2, f_3 \rangle.
\]

(7.11)

(The choice of \(G_0\) and the notation of [1] were different, but it is irrelevant.) Note that \((\mathcal{I})\) is in (7.11). By Corollary 18, the subloop \(M(G_0)\) is isomorphic to the orbit \((\mathcal{I})G_0 \leq PSL(\mathcal{Q}),\) i.e., the set of all \(+1\)-subspaces contained in (7.11). Hence, this subloop is the image in \(PSL(\mathcal{Q})\) of the subloop of \(SL(\mathcal{Q})\) consisting of all elements of (7.11) of norm 1, i.e., the Zorn matrices of the form

\[
\begin{pmatrix}
a & (0, 0, r_1) \\
(r_2, b, 0) & a^{-1}
\end{pmatrix}, \quad a, b, r_1, r_2 \in F, \ a \neq 0.
\]

(7.12)

This is obviously a subloop of (7.1). We will call this subloop non-maximal parabolic. It has the structure \(q^2 : q : (q - 1)/d\).

Show that up to isomorphism it is a unique subloop arising from \(S\)-subgroups in \([G_0]\). It is directly verified that \(e_4\) is stabilized by the following subgroups of \(D\): the positive root subgroups \(X_\omega(t)\) for \(\omega \in \Pi\) (see (5.7)), the diagonal subgroup \(H\) (see (5.8)), and the subgroup \(X_{-\beta}(t)\). In particular, the parabolic subgroup \(P_\beta = \langle U, H, X_{-\beta}(t) \rangle\) of \(D\) stabilizes the triangle \((p_0, p_1, p_r)\).

However, \(P_\beta\) is maximal in \(D\) by Table 4. Therefore, \(P_\beta = G_0 \cap D\). Since

\[
|G_0 : P_\beta| = \frac{1}{d^2}q^6(q - 1)^2(q + 1) = \frac{1}{d^2}q^6(q - 1)^2 = |\mathcal{M}(G_0)|^2,
\]

Lemma 6 and Corollary 3 imply \(D\)-conjugacy and isomorphism of all subloops arising from \(S\)-subgroups in \([G_0]\) and that the number of such subloops in \(M(q)\) is \(|D : G_0 \cap D| = (q^6 - 1)/(q - 1)\). Note that this coincides with the number of \(0\)-points \((x)\) of \(\mathcal{P}\) with \(x^2 = 0\) (the so-called absolute points of the geometry \(\mathcal{P}\)) and the above discussion enlightens the one-to-one correspondence between such points and the non-maximal parabolic subloops of \(M(q)\).

2. \(G_0\) is an \(R_{s2}\)-subgroup. The parabolic subgroup \(R_{s2}\) is the normalizer in \(G\) of a totally singular 2-subspace of \(\mathcal{Q}\), i.e., a line \(l\) of \(\mathcal{Q}\). Thus \(S\)-invariant lines of \(\mathcal{Q}\) correspond to \(S\)-invariant subgroups in \([G_0]\). Let \(l = \langle x, y \rangle\). Since \(l^\sigma = \langle \overline{x}, \overline{y} \rangle\) and \(l^\rho = \mathcal{Q}x \cap \mathcal{Q}y\), it can be seen from Lemma 11 that \(l\) is \(S\)-invariant iff \(x^2 = y^2 = xy = 0\). In particular, we may put \(l = \langle f_2, e_4 \rangle\) and \(G_0 = N_G(l)\). Then \(G_0\) is \(S\)-invariant. We showed in [1] (see item 2 of proof of Theorem 2) that \(G_0\) is transitive on \(+1\)-subspaces in \(l^\perp = \langle e_1, e_3, e_4, f_1, f_2, f_3 \rangle\). By Corollary 18, the subloop \(M(G_0) \cong (\mathcal{I})G_0\) is the image in \(PSL(\mathcal{Q})\) of the set of elements of \(l^\perp\) of norm 1, which are precisely the Zorn matrices (7.1).

As in the previous case, it is directly verified that \(l\) is normalized by the following subgroups of \(D\): all positive root subgroups \(X_\omega(t)\), the diagonal subgroup \(H\), and \(X_{-\alpha}(t)\). Since the parabolic subgroup \(P_\alpha = \langle U, H, X_{-\alpha}(t) \rangle\) is maximal in \(D\), we have \(G_0 \cap D = P_\alpha\). As above, we have \(|G_0 : P_\alpha| = |\mathcal{M}(G_0)|^2\); hence, all subloops arising from \(S\)-subgroups in \([G_0]\) are \(D\)-conjugate by Lemma 6. Corollary 3 implies that the number of maximal parabolic subloops in \(M(q)\) is
We denote this module by $G_{\epsilon}$. The set of lines $L_{\Omega}$ is the image in $G$ of the normalizer of an irreducible subgroup of $\Omega(\mathbb{O})$ isomorphic to $SU_4(q)$. Let $\epsilon = \pm 1$. By definition, an $R_{\epsilon}$-subgroup of $G$ is the normalizer $N_G(W)$ of an $\epsilon$-subspace $W$ of $\Omega$. An $F_{\epsilon}$-subgroup is an $\epsilon$-subspace consisting of the direct sum of two t.s. 4-subspaces. If $K$ is either an $R_{\epsilon}$ subgroup or an $F_{\epsilon}$-subgroup then $\eta(K)$ denotes the unique cyclic normal subgroup of $K$ of order $r$, where $r$ is the largest prime divisor of $(q - \epsilon)/d$. By definition, a subgroup $N \leq G$ is an $N_{\epsilon}$-subgroup (called $N_{\epsilon}$-subgroup for $\epsilon = +1$ and $N_{\epsilon}$-subgroup for $\epsilon = -1$) if $N = R \cap F$, with $R$ an $R_{\epsilon}$ subgroup, $F$ an $F_{\epsilon}$-subgroup, and $[\eta(R), \eta(F)] = 1$.

We explain a geometric interpretation of $F_{\epsilon}$- and $R_{\epsilon}$-subgroups of $G$. Let $A = \mathbb{F}$ if $\epsilon = -1$ and $A = \mathbb{F}$ if $\epsilon = +1$. By (4.12), $\mathbb{O}$ is a left $A$-module of dimension 4 with $A$-basis $\mathfrak{w}$ (see (4.11)). We denote this module by $W_{\epsilon l}$. Introduce a form $k_A$ on $W_{\epsilon l}$ defined by (5.3). By Lemma 12, $\mathfrak{w}$ is $k_A$-orthonormal and $k_A(w, w) = Q(w)$ for all $w \in W_{\epsilon l}$. Hence, the subgroup $G_{\epsilon l}$ of $GL(W_{\epsilon l})$ consisting of the $A$-linear maps that preserve $k_A$ is naturally embedded into $GO(\mathbb{O})$. We identify $G_{\epsilon l}$ with its image in $GO(\mathbb{O})$. Observe that $G_{-1}$ is the unitary group $GU(W_{-1}) \cong GU_4(\mathbb{F})$. Also, there is an obvious natural isomorphism between $GL(W_{+1}) \cong GL_4(\mathbb{P})$ and $GL_4(\mathbb{F}) \times GL_4(\mathbb{F})$ under which $G_{+1}$ is mapped onto the subgroup $\{(C, -C^T) \mid C \in GL_4(\mathbb{F})\} \cong GL_4(\mathbb{F})$. In brief, $G_{\epsilon l} \cong GL_4(\mathbb{F})$.

Since the involution in $A$ is induced by $-r_{\epsilon l}$, the element $\delta = -r_{\epsilon l}r_{\epsilon l}r_{\epsilon l}r_{\epsilon l}r_{\epsilon l} \in \Omega(\mathbb{O})$ normalizes $G_{\epsilon l}$ and induces in it the contragredient automorphism $C \mapsto C^{-T}$ of order 2. Let

$$L(W_{\epsilon l}) = \{ Ax \mid 0 \neq x \in W_{\epsilon l}, k_A(x, x) = 0 \}.$$ 

By (12.ii), the elements of $L(W_{\epsilon})$ are lines in $\mathfrak{P}$ and the normalizer $F_{\epsilon l} = N_G(L(W_{\epsilon l}))$ is exactly an $F_{\epsilon}$-subgroup of $G$. Indeed, $G_{\epsilon l}$ clearly normalizes $L(W_{\epsilon l})$ and so does $\delta$. However, the images in $G$ of $G_{\epsilon l} \cap \Omega(\mathbb{O})$ and $\delta$ generate an $F_{\epsilon}$-subgroup which coincides with $F_{\epsilon l}$. Note that $\eta(F_{\epsilon l})$ lies in the image in $G$ of $\langle \text{diag}_{\mathfrak{w}}(\lambda, \lambda, \lambda, \lambda) \rangle$, where $\lambda$ is defined by (5.2).

Since $\mathbb{O}$ is also a right $A$-module $W_{\epsilon r}$ with the same basis $\mathfrak{w}$, we can similarly define the set of lines $L(W_{\epsilon r})$ of form $xA$ for all non-zero singular $x \in W_{\epsilon r}$, and see that the normalizer $F_{\epsilon r} = N_G(L(W_{\epsilon r}))$ is an $F_{\epsilon}$-subgroup of $G$.

Note that $A$ is an $\epsilon$-2-subspace of $\mathbb{O}$. Hence, the normalizer $R_{\epsilon} = N_G(A)$ is an $R_{\epsilon}$-subgroup. We have $\mathbb{O} = A \oplus A^\perp$ and $A^\perp$ is an $\epsilon$-6-subspace. Observe that $\eta(R_{\epsilon})$ lies in the image in $G$ of $\langle \text{diag}_{\mathfrak{w}}(\lambda, 1, 1, 1) \rangle$, which implies $[\eta(R_{\epsilon}), \eta(F_{\epsilon l})] = 1$. Define

$$L(A^\perp) = \{ l \in \mathfrak{P} \mid l \subseteq A^\perp \}.$$ 

Clearly, $R_{\epsilon} = N_G(L(A^\perp))$, since the lines in $L(A^\perp)$ span $A^\perp$. We show that

$$R_{\epsilon} \xrightarrow{\rho} F_{\epsilon l} \xrightarrow{\rho} F_{\epsilon r} \xrightarrow{\rho} R_{\epsilon},$$

for which it suffices to show that

$$L(A^\perp) \xrightarrow{\rho} L(W_{\epsilon l}) \xrightarrow{\rho} L(W_{\epsilon r}) \xrightarrow{\rho} L(A^\perp).$$

(7.13)
Let \( l = Ax \in \mathcal{L}(W_{el}) \). Then \( l = (x, \lambda x)_F \). Since \((\lambda x)\bar{x} = x(\bar{\lambda}x) = 0\), (11.vi) gives \( \lambda x \in \mathbb{O} x \) and \( x \in \mathbb{O}(\lambda x) \), i.e., \( l = \mathbb{O} x \cap \mathbb{O}(\lambda x) \). By (6.1), we have \( l \rho = (\bar{x}, \bar{\lambda}x) = \bar{x}A \in \mathcal{L}(W_{er}) \) and \( l \rho^2 = x\mathcal{O} \cap (\lambda x)\mathcal{O} = x((\lambda x)\mathcal{O}) = (\lambda x)(\bar{x}\mathcal{O}) \) by (11.vi). Note that a line of form \( a(\bar{b}\mathcal{O}) \) is orthogonal to \( v \in \mathbb{O} \) if and only if \( b(a\mathcal{O}) = 0 \), since

\[
(a(\bar{b}\mathcal{O}), v) = (\bar{b}\mathcal{O}, a\mathcal{O}) = (\mathbb{O}, b(a\mathcal{O}))
\]

by (8.viii). Hence, we have \( l \rho^2 \perp 1 \), since \((\lambda x)(\bar{1}) = (\lambda x)\bar{x} = 0\); and also \( l \rho^2 \perp \lambda \), since \( x((\lambda x)\bar{x}) = x(Q(\lambda)\bar{x}) = Q(\lambda)Q(x) = 0 \). Thus, \( \lambda \rho^2 \perp A \) and (7.13) holds.

Denote \( N_{e1} = R_e \cap F_{el} \cap F_{er} \). The above remarks show that \( N_{e1} \) is \( \rho \)-invariant. Since \( \lambda \sigma = \overline{\lambda} A \), we have \( R_\rho^\sigma = R_\sigma \) and \( F_{el}^\sigma = R_{\rho\sigma}^\sigma = R_{\rho^2}^\sigma = F_{er} \). Hence, \( N_{e1} \) is \( \sigma \)-invariant and \( S \)-invariant. Show that \( N_{e1} = R_e \cap F_{el} \). This will imply that \( N_{e1} \) is an \( N_{e1} \)-subgroup of \( G \) in the sense of the definition given above. By triality, it suffices to show that \( F_{el} \cap F_{er} \subseteq R_e \). Every \( g \in F_{el} \cap F_{er} \) normalizes \( \mathcal{L}_0 = \mathcal{L}(W_{el}) \cap \mathcal{L}(W_{er}) \). If we show that

\[
\mathcal{L}_0 = \mathcal{L}(W_{el}) \cap \mathcal{L}(A^\perp)
\]  

(7.14)

this will imply that \( g \in N_G(\mathcal{L}_0)_F) = N_G(A^\perp) = R_e \) as is required. By triality, (7.14) is equivalent to \( \mathcal{L}(W_{el}) \cap \mathcal{L}(A^\perp) \subseteq \mathcal{L}(W_{er}) \). However, every line \( l = Ax \in A^\perp \) has form \( l = x A \) by (9.ii) and the claim follows.

Therefore, \( N_{e1} \) is an \( S \)-invariant \( N_{e1} \)-subgroup of \( G \) and we may assume that \( G_0 = N_{e1} \). It was shown in [1] (see there items 3 and 4 of the proof of Theorem 2) that the only triality involutions normalizing \( G_0 \) are those of form \( \bar{r} \), where \( (v)_F \subseteq A \) is a +1-subspace, and that all such involutions are \( G_0 \)-conjugate. By Corollary 18, \( \mathcal{M}(G_0) \cong 1)^{G_0} \) is the set of all such +1 subspaces. Clearly, \( \lambda \), which has order \( q - \epsilon \), generates the subgroup of all elements with norm 1 in \( A \). Since \( \lambda \) has the first form in (7.4), the subloop \( \mathcal{M}(G_0) \cong 1)^{G_0} \) lies in \( M(PSL_2(q), 2) \) and thus is not maximal.

We find \( G_0 \cap D \). Consider the group \( SL^e(A^\perp) \), which consists of the \( A \)-linear transformations of \( \mathbb{O} \) of determinant 1 that centralize \( A \) and preserve the form \( k_A \), and also consider \( \delta = -r_{w_1}r_{w_3}r_{w_2}r_{w_4} \), which is an \( A \)-semilinear transformation of \( \mathbb{O} \) that centralizes the \( A \)-basis \( w \).

Then the elements of \( SL^e(A^\perp) \), together with \( \delta \), preserve the alternating \( A \)-trilinear form \( t_A \) defined in (5.4). This is because for any \( A \)-(semi)linear transformation \( f \) of \( A^\perp \) with matrix \((a_{ij})_{i,j=2,3,4} \) in the basis \( \{ w_2, w_3, w_4 \} \), we have \( t_A(w_2 f, w_3 f, w_4 f) = \det(a_{ij}) \tau t_A(w_2, w_3, w_4), \) where \( \tau \) is the identity mapping or the involution of \( A \) according as \( f \) is \( A \)-linear or \( A \)-semilinear. Therefore, \( f \) preserves \( t_A \) iff \( \det(f) = \det(a_{ij}) = 1 \). By Lemma 14, the elements of \( SL^e(A^\perp) \), together with \( \delta \), are automorphisms of \( \mathbb{O} \). Hence, their images in \( G \) lie in \( G_0 \cap D \) and generate a subgroup isomorphic to \( SL^3_2(q) : 2 \). Since this group is maximal in \( D \) by Table 4, it must coincide with \( G_0 \cap D \).

We now have

\[
|G_0 : G_0 \cap D| = \frac{2^2 q^3(q^3 - \epsilon)(q^2 - 1)(q - \epsilon)^2}{2q^3(q^3 - \epsilon)(q^2 - 1)} = \frac{1}{d^2} (q - \epsilon)^2 = |\mathcal{M}(G_0)|^2.
\]

By Lemma 6, all subloops of \( M(q) \) arising from \( S \)-invariant \( N_{e1} \)-subgroups of \( G \) are \( D \)-conjugate and isomorphic. The number of such subloops is \( |D : G_0 \cap D| = \frac{1}{2} q^3(q^3 + \epsilon) \).
5. $G_0$ is an $N^4_4$-subgroup. Suppose $q = p$ is odd. Let $b = \{1 = \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_7\}$ be the basis of $\mathcal{O}$ defined by (4.6). By definition, an $N^4_4$-subgroup is conjugate in $G$ to the normalizer $N_G(P)$ of the subgroup $P$ of order 8 generated by the involutions $\tilde{z}_1, \tilde{z}_2, \tilde{z}_3$, where

\[
\begin{align*}
    z_1 &= \text{diag}_0(-1, -1, 1, -1, 1, 1, 1), \\
z_2 &= \text{diag}_0(-1, 1, -1, 1, -1, 1, 1), \\
z_3 &= \text{diag}_0(-1, 1, -1, -1, 1, -1, 1)
\end{align*}
\]

are elements of $\Omega(\mathcal{O})$. We show that $N_G(P)$ is $S$-invariant.

Since $\tilde{z}_i = \tilde{r}_e \tilde{r}_{e_i+1} \tilde{r}_{e_i+2} \tilde{r}_{e_i+3}$, for $i = 1, 2, 3$, we have $(\tilde{z}_i)\sigma = \tilde{r}_{e_0} \tilde{r}_{e_i} \tilde{r}_{e_i+1} \tilde{r}_{e_i+3} = \tilde{z}_i$ by (4.8). Hence, $\sigma$ centralizes $P$. For brevity, put $j = i + 1, k = i + 3$. Then, for every 0-point $\langle x \rangle$, (4.17) and (4.8) imply

\[
\langle x \rangle \tilde{z}_i = \langle x \rangle \tilde{r}_1 \tilde{r}_{e_i} \tilde{r}_{e_j} \tilde{r}_{e_k} = (\tilde{x}) \tilde{r}_{e_i} \tilde{r}_{e_j} \tilde{r}_{e_k} = \langle \varepsilon_i x \varepsilon_i \rangle \tilde{r}_{e_j} \tilde{r}_{e_k} = \langle \varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j \rangle \tilde{r}_{e_k} = \langle \varepsilon_k (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j) \rangle \tilde{r}_{e_k} = \varepsilon_k \varepsilon_j \varepsilon_i x \varepsilon_i \varepsilon_j \varepsilon_k.
\]

By (6.1) and (7.1), we also have

\[
\langle x \rangle (\tilde{z}_i) = \langle x \rangle \rho^{-1} \tilde{z}_i \rho = (\mathcal{O} \tilde{x}) \tilde{r}_1 \tilde{r}_{e_i} \tilde{r}_{e_j} \tilde{r}_{e_k} \rho = (\mathcal{O} \tilde{x}) \tilde{r}_{e_i} \tilde{r}_{e_j} \tilde{r}_{e_k} \rho = \mathcal{O} (\varepsilon_i \varepsilon_i \varepsilon_j \varepsilon_k) = (\varepsilon_k (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j) \rangle \tilde{r}_{e_k} \rho = \varepsilon_k (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j).
\]

Note that $(\varepsilon_i \varepsilon_j \varepsilon_k) = (\varepsilon_i \varepsilon_{i+1}) \varepsilon_{i+3} = -1$ by (4.6) for $i = 1, 2, 3$. Hence, we have

\[
\varepsilon_k = (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j) \varepsilon_k = \varepsilon_k (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j) = \varepsilon_k (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j) = \varepsilon_k (\varepsilon_j (\varepsilon_i x \varepsilon_i) \varepsilon_j).
\]

Therefore, $(\tilde{z}_i) = \tilde{z}_i$ by Remark 15; i.e., $\rho$ centralizes $P$.

Thus $S$ centralizes $P$ and so $N_G(P)$ is $S$-invariant. We may therefore assume that $G_0 = N_G(P)$. We showed that $G_0$ is transitive on the 8 basis vectors in $b$. (see item 6 of the proof of Theorem 2 in [1]). By Corollary 18, the subloop $M(G_0) \cong (\langle 1 \rangle)^{G_0}$ consists of the +1-subspaces $\langle \varepsilon_i \rangle, i = 0, \ldots, 7$. It is clearly isomorphic to the elementary abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ generated by $\langle \varepsilon_1 \rangle, \langle \varepsilon_2 \rangle, \langle \varepsilon_3 \rangle$. Returning to the original basis $\{\varepsilon_1, \ldots, f_4\}$ of $\mathcal{O}$, we see by (4.6) that $\varepsilon_1, \varepsilon_2, \varepsilon_3$ have form (7.4). Hence, $M(G_0)$ lies in the subloop $M(PSL_2(2), 2)$ of $M(G)$ and thus is not maximal.

Since $S$ centralizes $P$, we have $P \leq D$ (see the remarks before Table 4). The group $P$ can be characterized as the group of automorphisms of $\mathcal{O}$ that centralize the set of basis +1-subspaces $\{\varepsilon \mid \varepsilon \in b\}$. Consider the group $P_0$ of automorphisms of $\mathcal{O}$ that normalize this set. Define two transformations $\alpha_1$ and $\alpha_2$ of $\mathcal{O}$ on the basis by

\[
\begin{align*}
\text{or}_1 : i = 1, \ldots, 7, \quad \tau_1 = (1234567), \\
\text{or}_2 : i = 1, \ldots, 6, \quad \varepsilon_7 \mapsto \varepsilon_7, \quad \tau_2 = (12)(36).
\end{align*}
\]

A direct verification shows that $\alpha_1$ and $\alpha_2$ belong to $P_0$ and generate (modulo $P$) a group isomorphic to the non-split extension $2^3 : PSL_3(2)$ of order $8 \cdot 168$. Since this group is maximal in $D$ by Table 4, it must coincide with $P_0$ (see also discussion in Section 1 of [17]). Hence, we have $G_0 \cap D = N_D(P) = P_0$ and
\[ |G_0 : G_0 \cap D| = \frac{192}{d^2} (q - \epsilon)^4 / 12 (q - \epsilon)^2 = \frac{16}{d^2} (q - \epsilon)^2 = |M(G_0)|^2. \]

Hence, by Lemma 6, all subloops of \( M(q) \) arising from \( S \)-invariant \( I_{12} \)-subgroups of \( G \) are \( D \)-conjugate and isomorphic, and \( |D : G_0 \cap D| = \frac{1}{1344} q^6 (q^6 - 1)(q^2 - 1) \) is the number of such subloops.

6–7. \( G_0 \) is an \( I_{12} \)-subgroup, \( \epsilon = \pm 1 \). If \( \epsilon = +1 \) then assume that \( q \geq 7 \) and if \( \epsilon = -1 \) then assume that \( q \neq 3 \). An \( I_{12} \)-subgroup \( G_0 \) is the normalizer in \( G \) of an \( \epsilon \)-2-decomposition \( \mathbb{O} = V_1 \oplus \cdots \oplus V_4 \). Denote this decomposition by \( d \). Observe that \( G_0 \) also normalizes the set of lines \( \mathcal{L}(d) \) (see (7.10)). Conversely, suppose \( g \in G \) normalizes \( \mathcal{L}(d) \). Then \( g \) also normalizes the set of \( +4 \)-subspaces that can be represented as \( l_1 \oplus l_2 \) for \( l_1, l_2 \in \mathcal{L}(d) \). Clearly, these are the subspaces \( V_i \oplus V_j \) for \( 1 \leq i < j \leq 4 \). Since their non-trivial pairwise intersections are the components \( V_i, i = 1, \ldots, 4 \), it follows that \( g \) normalizes \( d \). In particular, if \( d \) is \( S \)-invariant then so is \( G_0 \).

Now let \( d \) be the first decomposition in (4.12) if \( \epsilon = -1 \) and the second one if \( \epsilon = +1 \). Since \( d \) is a \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)-grading, (24.ii) implies that \( d \) is \( S \)-invariant. Hence, we may assume that \( G_0 = N_G(d) \). We showed (see items 7–8 of the proof of Theorem 2 in [1]) that the only triviality involutions normalizing \( G_0 \) are those of form \( \tilde{r}_v \) where \( (v) \) runs through all \( +1 \)-subspaces in \( \bigcup_{i=1}^d V_i \) and that \( G_0 \) is transitive on such subspaces. Hence, by Corollary 18, the subloop \( M(G_0) \cong \langle 1 \rangle^{G_0} \) is exactly the set of such subspaces. Since \( V_i = A w_i, i = 1, \ldots, 4 \), where \( A = \mathbb{F} \) or \( \mathbb{P} \) according as \( \epsilon = -1 \) or \( \epsilon = +1 \), the elements of \( M(G_0) \) have form \( (\lambda^j w_i) \), where \( \lambda \) is as in (5.2). In particular, \( M(G_0) \) is generated by \( \langle \lambda \rangle, \langle w_2 \rangle \), and \( \langle w_3 \rangle \). Since \( \lambda, w_2, \) and \( w_3 \) have form (7.4), we see that \( M(G_0) \) is a subloop of \( M(\text{PSL}_2(q), 2) \) and thus is not maximal unless \( \epsilon = -1 \) and \( q = 2 \), in which case \( M(G_0) = M(\text{PSL}_2(q), 2) \). Also, it is easy to see that \( M(G_0) \) is the duplication of the dihedral group \( \mathbb{D}_{2^d(q-\epsilon)} \) generated by \( \langle \lambda \rangle \) and \( \langle w_2 \rangle \).

We find \( G_0 \cap D = N_D(d) \). Let \( g \in G_0 \cap D \). Since \( 1 g = 1 \), we have \( Ag = A \) and thus \( g \) is \( A \)-linear. Then \( g \) preserves the \( A \)-sesquilinear form (5.3) on \( \mathbb{O} \) and the \( A \)-trilinear form (5.4) on \( A^1 \). Therefore, \( \det(g) = 1 \) and \( g \in \text{SL}^e(A^1) : 2 = \text{SL}_2^e(q) : 2 \). However, the normalizer of the decomposition \( A^1 = A w_2 \oplus A w_3 \oplus A w_4 \) in \( \text{SL}^e(A^1) \) has form \( (q - \epsilon)^2 \). \( S_3 \) (see [10, Proposition 4.2.9]). Consequently, \( N_D(d) = (q - \epsilon)^2 (S_3 \times 2) \). We now have

\[ |G_0 : G_0 \cap D| = \frac{192}{d^2} (q - \epsilon)^4 / 12 (q - \epsilon)^2 = \frac{16}{d^2} (q - \epsilon)^2 = |M(G_0)|^2. \]

By Lemma 6, all subloops of \( M(q) \) arising from \( S \)-invariant \( I_{12} \)-subgroups of \( G \) are \( D \)-conjugate. The number of such subloops is \( |D : G_0 \cap D| = \frac{1}{1344} q^6 (q^6 + q^2 + 1)(q + \epsilon)^2 \).

8. \( G_0 \) is an \( I_{44} \)-subgroup. Let \( q \geq 3 \). An \( I_{44} \)-subgroup \( G_0 \) is the normalizer in \( G \) of a \( +4 \)-decomposition \( \mathbb{O} = V_0 \oplus V_1 \). Note that \( G_0 \) normalizes the set of lines \( \mathcal{L}(V_0 \oplus V_1) \) (see (7.9)). The converse is also true. Indeed, let \( g \in G \) normalize \( \mathcal{L}(V_0 \oplus V_1) \). Since \( V_i = l_1 \oplus l_2 \) for some lines \( l_1, l_2, l \in \mathcal{L}(V_0 \oplus V_1) \), it follows that both \( l_1 g \) and \( l_2 g \) are either in \( V_0 \) or in \( V_1 \) (otherwise, \( (l_1 g, l_2 g) = V_i g \) would be a t.s. 4-subspace, which it is not). As every \( x \in V_i \) has form \( x_1 + x_2 \) for \( x_j \in l_j, j = 1, 2 \), we see that the decomposition \( V_0 \oplus V_1 \) is \( g \)-invariant. In particular, if \( V_0 \oplus V_1 \) is \( S \)-invariant then so is \( G_0 \).

Now, put \( V_0 = \langle e_1, e_2, f_1, f_2 \rangle, \ V_1 = \langle e_3, e_4, f_3, f_4 \rangle \). Obviously, both \( V_0 \) and \( V_1 \) are \( +4 \)-subspaces and the decomposition \( \mathbb{O} = V_0 \oplus V_1 \) is a \( \mathbb{Z}_2 \)-grading by Table 2. By (24.i) and the above remarks, we may assume that \( G_0 \) is the normalizer of this decomposition. Thus \( G_0 \) is \( S \)-invariant. We showed that \( G_0 \) acts transitively on the \( +1 \)-subspaces in \( V_0 \cup V_1 \) (see item 9 of the proof of Theorem 2 in [1]). By Corollary 18, the subloop \( M(G_0) \cong \langle 1 \rangle^{G_0} \) is the image in
PSL(\(\mathbb{O}\)) of the set of elements of \(V_0 \cup V_1\) of norm 1, which are precisely the Zorn matrices (7.4). Hence \(M(G_0) \cong M(PSL_2(q), 2)\).

Let \(A = \langle X_{\omega_1}(t), X_{-\omega_1}(t) \rangle \leq D\) and let \(B\) consist of all \(\delta_0(C)\) (see (5.5)) with

\[
C = \begin{pmatrix}
c^{-1} & 0 & 0 \\
0 & c_{11} & c_{12} \\
0 & c_{21} & c_{22}
\end{pmatrix}, \quad (c_{ij})_{i,j=1,2} \in GL_2(q), \quad c = \det(c_{ij}).
\]

It is directly verified that \(A\) and \(B\) normalize the decomposition \(\mathbb{O} = V_0 \oplus V_1\). Moreover, by considering the action of \(A\) and \(B\) on \(V_0\) and \(V_1\), it can be seen that \(A \cong SL_2(q)\), \(B \cong GL_2(q)\), \(A \cap B\) is the diagonal subgroup of \(A\) of order \(q - 1\), and \(AB \cong (SL_2(q) \circ SL_2(q))\).

By Table 4 this subgroup is maximal in \(D\) provided \(q \geq 3\). Hence, in this case, \(G_0 \cap D = AB\) and \(|G_0 : G_0 \cap D| = \frac{q^4(q^2 - 1)^4}{d^2} = \frac{4}{d^2}q^2(q^2 - 1)^2 = |M(G_0)|^2\). By Lemma 6, all subloops of \(M(q)\) arising from \(S\)-invariant \(I_{+4}\)-subgroups of \(G\) are \(D\)-conjugate and isomorphic.

The number of such subloops is \(|D : G_0 \cap D| = q^4(q^2 + q^2 + 1)\).

9. \(G_0\) is a \(G_1^1\)-subgroup. A \(G_1^1\)-subgroup is a subgroup \(G_0\) of \(G\) isomorphic to \(G_2(q)\) and such that \(G N_{G_S}(G_0) = G_S\). Since \(D = C_G(S) \cong G_2(q)\) is \(S\)-invariant, we may put \(G_0 = D\). Thus, \(G_0\) has trivial triality relative to \(S\) and \(M(G_0) = \{1\}\) is the identity subgroup of \(M(q)\). The fact that \(G_0S\) contains no other triality \(S_3\)-complements follows from Lemma 4. By Lemma 6, \(G_0\) is the unique \(S\)-subgroup in \([G_0]; i.e., only the identity subgroup arises in this case.

10–11. \(G_0\) is a \(P \Omega^+_8(q_0)^{-}\)-subgroup. Suppose that \(q = q_0^k\), with \(k\) prime. Let \(H_0 \leq G\) and \(\mathbb{O}_0 \leq \mathbb{O}\) be the naturally embedded subgroup \(P \Omega^+_8(q_0)\) and the \(F_{q_0}\)-subalgebra \(\mathbb{O}(q_0)\) with respect to the standard basis (4.5) of \(\mathbb{O}\). Show that \(H_0\) is \(S\)-invariant. Indeed, since \(\sigma = \rho_1\) and the entries of the matrix of \(r_1\) in the standard basis are in \(\{0, \pm 1\} \subseteq F_{q_0}\), it follows that \(H_0\) is \(S\)-invariant. Note that \(H_0\) is generated by elements of the form \(U(v)\), with \((v) \in PSL(\mathbb{O}_0)\), and \(U(w_1)U(w_2)\), with \((w_1), (w_2) \in PGL(\mathbb{O}_0) \setminus PSL(\mathbb{O}_0)\). By (6.8), \(U(v) = L(\overline{v})\) and \((U(w_1)U(w_2))^\rho = L(\overline{w}_1)L(\overline{w}_2)\). Since \(L(\overline{v})L(\overline{w}_1)L(\overline{w}_2) \in H_0\), it follows that \(H_0\) is \(\rho\)-invariant.

Now, if \((q, k) \neq (odd, 2)\) then we put \(G_0 = H_0\). If \(q = q_0^2\) is odd then we put \(G_0 = NG_0(H_0) \cong \text{InnDiag}(P \Omega^+_8(q_0))\), i.e., the group of inner-diagonal automorphisms of \(P \Omega^+_8(q_0)\), see [6, Proposition 2.2.9]. By Lemma 4 we see that all triality \(S_3\)-complements in \(G_0S\) are \(G_0\)-conjugate in view of the structure of \(\text{Aut}(P \Omega^+_8(q_0))\). By (6.iv) we obtain \(D\)-conjugacy and isomorphism of all subloops \(M(P)\) for all \(S\)-subgroups \(P \in [G_0]\). Note that \(G_0 \cap D = C_{G_0}(S) = C_{H_0}(S)\), since \(G_0S/H_0 \cong S_4\) when \(q = q_0^2\) is odd. Therefore, \(G_0 \cap D \cong G_2(q_0)\) and the number of subloops is \(|G_2(q) : G_2(q_0)|\) by Lemma 6.

If \((q, k) \neq (odd, 2)\) then \(M(G_0) = M(q_0)\) by definition. Let \(q = q_0^2\) be odd. Determine the isomorphism type of \(M(G_0)\) in this case. Note that \(G_0\) is generated modulo \(H_0\) by \(\tilde{b}\) and \(\tilde{c}\), where

\[
b = \text{diag}(\mu, \mu, \mu, \mu^{-1}, \mu^{-1}, \mu^{-1}),
\]

\[
c = \text{diag}(\lambda^{-1}, 1, 1, 1, \lambda, 1, 1, 1)
\]

written in the standard basis, with \(\mu\) a non-square in \(F\) and \(\lambda = \mu^2\). Note that \(\lambda\) is a non-square in \(F_{q_0}\). By Corollary 18, \(M(G_0) \cong (\langle \mathbf{1}_F \rangle)^{G_0}\). Hence, \(M(G_0)\) is isomorphic to the extension of \(M(H_0) \cong PSL(\mathbb{O}_0)\) by \(\langle \mathbf{1}_F \rangle\tilde{b}\) and \(\langle \mathbf{1}_F \rangle\tilde{c}\). However,
\[ \langle 1 \rangle_F \bar{c} = [\lambda^{-1} e_1 + \lambda f_1]_F \in PSL(\mathbb{O}_0), \]
\[ \langle 1 \rangle_F \bar{b} = [\mu e_1 + \mu^{-1} f_1]_F = (\lambda e_1 + f_1)_F \in PGL(\mathbb{O}_0) \setminus PSL(\mathbb{O}_0). \]

Therefore, \( M(G_0) \cong PGL(\mathbb{O}_0) \).

12. \( G_0 \) is a \( P \Omega^+_8 (2) \)-subgroup. Let \( q = p \) be odd. In the beginning of this section, we explained that \( \bar{W}_0 \) is an \( S \)-subgroup of \( G \) isomorphic to \( P \Omega^+_8 (2) \), where \( W_0 \) is the commutator subgroup of the Weyl group of type \( E_8 \). Hence, we may put \( G_0 = \bar{W}_0 \). Then \( M(G_0) \cong M(2) \). Moreover, all triality \( S_3 \)-complements in \( G_0 S \) are \( G_0 \)-conjugate by Lemma 4. Therefore, all subloops of \( M(2) \) are \( D \)-conjugate by Lemma 6. We also have \( G_0 \cap D = C_{G_0}(S) \cong G_2(2) \) and \( |D : G_0 \cap D| = |G_2(q) : G_2(2)| \) is the number of subloops in this case.

We can now make the concluding remarks of the proof. Every maximal subloop of \( M(q) \) has form \( M(G_0) \) for some \( S \)-maximal subgroup \( G_0 \) of \( P \Omega^+_8 (q) \) (see [1, Corollary 1]). In view of \( D \)-conjugacy of all subloops of \( M(G_0) \), in each of the above cases, the subloops in the cases (1), (3)–(7), (9) are non-maximal unless \( q = 2 \) and \( G_0 \) is an \( I_{2,2} \)-subgroup. By Lemma 23, the subloops of \( M(G_0) \) in all of the remaining cases are maximal (unless \( q = 3 \) and \( G_0 \) is an \( I_{4,4} \)-subgroup) and thus column V of Table 5 holds. The other columns hold by the above discussion. \( \square \)

References

[21] P.B. Kleidman, The maximal subloops of the Chevalley groups \( G_2(q) \) with \( q \) odd, the Ree groups \( ^2 G_2(q) \), and their automorphism groups, J. Algebra 117 (1) (1988) 30–71.