RT-MAT 2004-04

MAXIMAL SUBLOOPS OF SIMPLE MOUFANG LOOPS

Alexander N. Grishkov and
Andrei V. Zavarnitsine

Fevereiro 2004

Maximal subloops of simple Moufang loops

Alexander N. Grishkov[*]

Departamento de Matemática, Universidade de São Paulo,
Caixa Postal 66281, São Paulo-SP, 05311-970, Brasil,
and Omsk State University, pr. Mira 55-a, 644077, Russia
e-mail: grishkov@ime.usp.br

Andrei V. Zavarnitsine[†]

Sobolev Institute of Mathematics,
pr. Koptyuga 4, Novosibirsk, 630090, Russia
and Departamento de Matemática, Universidade de São Paulo,
Caixa Postal 66281, São Paulo-SP, 05311-970, Brasil
e-mail: zavarn@ime.usp.br

Abstract

We classify the maximal subloops of finite simple non-associative Moufang loops up to conjugacy with respect to automorphisms.

[*] supported by FAPESP and CNPq, Brazil

[†] supported by FAPESP, Brazil, Proc. 01/14611-4

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 $\mathbb{O}(q)$ and its automorphism group $G_2(q)$. As a corollary to our results, we have the following description:

Theorem A *The maximal subloops of the simple Moufang loop $M(q)$, $q = p^n$, are as follows:*

(i) $q^2 : PSL_2(q)$, maximal parabolic;

(ii) $(PSL_2(q), 2)$, $q \neq 3$;

(iii) $M(q_0)$, $q = q_0^k$, k prime, $(q, k) \neq (odd, 2)$;

(iv) $PGL(\mathbb{O}(q_0))$, $q = q_0^2$ odd;

(v) $M(2)$, $q = p$ odd.

Moreover, all isomorphic maximal subloops of $M(q)$ are conjugate in $Aut(M(q))$.

The paper is organized as follows. The next section explains the notation and basic definitions. In Section 3, we describe the general relation between Moufang loops and groups with triality, and a classification of the subgroups of $P\Omega_8^+(q)$ that correspond to certain important subloops of $M(q)$ including all maximal subloops. 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 automorphism group $Aut(\mathbb{O}(q))$ and some characterization of its elements. The geometry of triality related to the algebra $\mathbb{O}(q)$ is introduced in Section 6. We use it to define explicitly the triality automorphisms of $P\Omega_8^+(q)$. 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.

2 Preliminaries

We mostly use standard notation. $\boldsymbol{F} = \boldsymbol{F}_q$ denotes the field of $q = p^n$ elements, p prime, and $\boldsymbol{F}^*$ is the multiplicative group of $\boldsymbol{F}$. 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 φ is an automorphism of G and $x \in G$ then x^φ is the image of x under φ. Expressions like $x\varphi$, $[x,\varphi]$, etc. are to be regarded in the semidirect product $G : \mathrm{Aut}(G)$. In particular, $x^\varphi = \varphi^{-1}x\varphi$. The commutator subgroup and the center of G are G' and $Z(G)$. 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 $N_G(X_0) = \{g \in G \mid X_0 g = X_0\}$.

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

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

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 $X^\perp = \{v \in V \mid f_Q(v,x) = 0 \text{ for all } x \in X\}$. 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 $W \leqslant V$ 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 *ϵm-subspace* W of V, where $\epsilon = \pm$, is a non-degenerate m-subspace such that $(W, Q|_W)$ is an orthogonal space of type ϵ. 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 $\boldsymbol{F}^*$. 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 ϵm-subspaces V_i is called an ϵm-decomposition.

An *involution* $a \mapsto \bar{a}$ of a ring A is an anti-automorphism of A satisfying $\bar{\bar{a}} = a$ for all $a \in A$. Let V be a left A-module, where A is a commutative ring with involution. A transformation $f : V \to V$ is called *A-semilinear* if it is additive and $f(av) = \bar{a}f(v)$ for all $v \in V$, $a \in A$. A form $k : V \times V \to A$ is called *A-sesquilinear* if it is A-linear in the first argument and $k(v, w) = \overline{k(w, v)}$ 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 $f : V \times \ldots \times V \to A$ is called *alternating* if $f(v_1, \ldots, v_m) = 0$ whenever $v_i = v_j$ for some $1 \leqslant i < j \leqslant m$.

All groups (loops) we consider are finite. All vector spaces have finite dimension. The subgroup (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 $x \mapsto ax$ and $x \mapsto xa$ 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 p. 60 in [6]).

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

$$(xy)(zx) = (x(yz))x, \qquad ((xy)x)z = x(y(xz)), \qquad x(y(zy)) = ((xy)z)y.$$

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

$$[x,\sigma]\cdot[x,\sigma]^{\rho}\cdot[x,\sigma]^{\rho^2}=1, \tag{3.1}$$

Denote $S=\langle\rho,\sigma\rangle$. The triality is called *non-trivial* if $S\neq 1$. The relation (3.1) does not depend on the particular choice of the generators ρ and σ of S (see [2]) and we will thus speak of a group with triality S.

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

$$M=\{[x,\sigma]\mid x\in G\},\qquad H=C_G(\sigma). \tag{3.2}$$

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

$$m.n=m^{-\rho}nm^{-\rho^2}\ \text{ for all }\ m,n\in M \tag{3.3}$$

becomes a Moufang loop of order $|G:H|$ which is isomorphic to the loop previously considered by Doro [2]. We denote by $M(G)$ the loop $(M,.)$ constructed in this way from a group G with triality.

Lemma 1 *In the above notation, we have*

(i) M^{ρ^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
$\eta(g)=gg^{-\sigma\rho}g^{\rho^2}\in H$ and $\xi(g)=[g,\sigma]\in M$,

(iii) for every $m\in M$, the elements m, m^{ρ}, m^{ρ^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 [2]. ▲

If $G_0\leqslant G$ is an S-invariant subgroup of G (shortly, *S-subgroup*) then $M(G_0)$ is a subloop of $M(G)$. The reverse correspondence is expressed in the following lemma:

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

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 $M(G_0^{min}) = M_0$ (see proof of Theorem 1 in [1]). Observe that, for every S-subgroup G_0 with $M(G_0) = M_0$, 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, M^{ρ}, M^{ρ^2}, respectively. Moreover, $[G_0, \rho^2] = [G_0, \rho]^{\sigma}$. Thus, it suffices to show that $[G_0, \rho] \subseteq G_0^{min}$. Since $G_0 = \eta(G_0)M_0^{\rho^2}$ by (1.ii) and since $[xy, \rho] = [x, \rho]^y[y, \rho]$, we only have to show that $[\eta(G_0), \rho] \subseteq G_0^{min} = \eta(G_0^{min})M_0^{\rho^2}$. This will follow once we prove that $\eta([\eta(G_0), \rho]) \subseteq \eta(G_0^{min})$. However, for every $h \in \eta(G_0)$, we have

$$\eta([h,\rho]) = h^{-1}h^{\rho}(h^{-1}h^{\rho})^{-\rho\sigma}(h^{-1}h^{\rho})^{\rho^2} = h^{-1}h^{\rho}h^{-\sigma\rho}h^{\sigma\rho^2}h^{-\rho^2}h = 1,$$

since $h^{\sigma} = h$ by (1.ii), and the claim follows. Thus, $G_0^{min} = [G_0, S] \trianglelefteq G_0$.

Now show that any S-subgroups G_1 and G_2 with $M(G_1) = M(G_2) = M_0$ satisfy $M(\langle G_1, G_2\rangle) = M_0$. This will imply that G_0^{max} is the subgroup generated by all S-subgroups G_0 with $M(G_0) = M_0$. 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 $g_2 = hm_2^{\rho^2}$, where $h = \eta(g_2) \in G_2 \cap H$ (see Lemma 1). Using (3.1), (3.3), and Lemma 1, we have

$$[g_1g_2, \sigma] = m_1^{g_2}m_2 = m_2^{-\rho^2}h^{-1}m_1hm_2^{\rho^2}m_2 = m_2^{-\rho^2}m_0m_2^{-\rho}, \tag{3.4}$$

where $m_0 = m_1^h$. 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 Lemma 1, (iv) imply that $[g_1g_2, \sigma] = m_0.m_2 \in M_0$. ▲

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 $M(G_1) \neq M(G_2)$.*

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 $M(G)$ is a simple loop (see also Lemma 16 below). We will denote by $M(q)$ the abstract Moufang loop isomorphic to $M(P\Omega_8^+(q))$. As was shown by Liebeck (see [4]), the loops $M(q)$ for $q = p^n$ are the only simple non-associative Moufang loops and $P\Omega_8^+(q)$ are the only 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 $Aut(G)$ to the group of graph automorphisms of G which is isomorphic to S_3. If this is the case then $M(G)$ is isomorphic to $M(q)$.*

Proof. See [4] and Lemma 4 in [1]. ▲

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 [5]. 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 specific values of q for which it is maximal. Columns IV and V give the orders of G_0 and the corresponding subloop $M(G_0)$. We remark that 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 GS that is G-conjugate to S is called a *triality S_3-complement.* An involution in GS is called a *triality involution* if it lies in a triality S_3-complement.

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

Proof. When considering each type of S-maximal subgroups $G_0 \leqslant G$ in the proof of Theorem 2 in [1], we showed that all triality involutions in $G_0\langle\sigma\rangle$ are G_0-conjugate and, in particular, there are exactly $|M(G_0)|$ of them in each of the cosets $G_0\sigma$, $G_0\sigma\rho$, $G_0\rho\sigma$. Moreover, every pair of 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 [5], we have $D \cong G_2(q)$. It is clear form (3.2) and (3.3) that the loop $M(G)$ is D-invariant and D acts by automorphisms on $M(G)$.

Denote by $[G_0]$ the G-conjugacy class of $G_0 \leqslant G$. 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.

Table 1. S-maximal subgroups of $P\Omega_8^+(q)$

	I	II	III	IV	V
	G_0	restrictions on q	maximality in $P\Omega_8^+(q)$	$\lvert G_0\rvert$	$\lvert M(G_0)\rvert$
1.	P_2	—	—	$\frac{1}{d^2}q^{12}(q-1)^4(q+1)$	$\frac{1}{d}q^3(q-1)$
2.	R_{s2}	—	✓	$\frac{1}{d^2}q^{12}(q-1)^4(q+1)^3$	$\frac{1}{d}q^3(q^2-1)$
3.	N_1	—	—	$\frac{2}{d^2}q^3(q^3+1)(q+1)^3(q-1)$	$\frac{1}{d}(q+1)$
4.	N_2	$q \geqslant 4$	—	$\frac{2}{d^2}q^3(q^3-1)(q-1)^3(q+1)$	$\frac{1}{d}(q-1)$
5.	N_4^4	$q = p \geqslant 3$	—	$2^{12} \cdot 3 \cdot 7$	8
6.	I_{+2}	$q \geqslant 7$	$q \geqslant 7$	$\frac{192}{d^2}(q-1)^4$	$\frac{4}{d}(q-1)$
7.	I_{-2}	$q \neq 3$	$q \neq 3$	$\frac{192}{d^2}(q+1)^4$	$\frac{4}{d}(q+1)$
8.	I_{+4}	$q \geqslant 3$	$q \geqslant 3$	$\frac{4}{d^2}q^4(q^2-1)^4$	$\frac{2}{d}q(q^2-1)$
9.	G_2^1	—	—	$q^6(q^6-1)(q^2-1)$	1
10.	$P\Omega_8^+(2)$	$q = p \geqslant 3$	✓	$2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$	120
11.	$P\Omega_8^+(q_0)$	$q = q_0^k, k$ prime, $(d,k)=1$	✓	$\frac{1}{d^2}q_0^{12}(q_0^2-1)(q_0^4-1)^2(q_0^6-1)$	$\frac{1}{d}q_0^3(q_0^4-1)$
12.	$P\Omega_8^+(q_0).2^2$	$q = q_0^2$ odd	✓	$q^6(q-1)(q^2-1)^2(q^3-1)$	$q_0^3(q_0^4-1)$

Lemma 6 *Let G_0 be an S-maximal subgroup of G. Then the following conditions are equivalent:*

(i) for all S-subgroups $P \in [G_0]$, the subloops $M(P) \leqslant M(G)$ 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) $|G_0 : G_0 \cap D| = |M(G_0)|^2$.

Proof. Let $P_1, P_2 \in [G_0]$ be S-subgroups. If $P_1 = P_2^g$ for $g \in D$ then $M(P_1)$=$M(P_2)^g$, since, for every $p_1 \in P_1$, we have $[p_1, \sigma] = [p_2^g, \sigma] = [p_2, \sigma]^g$ for suitable $p_2 \in P_2$. Conversely, let $M(P_1)$=$M(P_2)^g$ and put $P_0 = P_2^g$. Then P_0 is S-maximal and, by the above, $M(P_0) =$

$M(P_2)^g = M(P_1)$. 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 $S_0^g = S$ for some $g \in G$ and G_0^g 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 and it is for this reason that 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 the linear transformations U_x, L_x, R_x of A as follows:

$$yU_x = xyx, \qquad yL_x = xy, \qquad yR_x = yx \qquad \text{for all } \; y \in A. \tag{4.1}$$

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

(i) $(xy)(zx) = x(yz)x$,

(ii) $(xyx)z = x(y(xz))$ *or, equivalently,* $L_{xyx} = L_xL_yL_x$,

(iii) $z(xyx) = ((zx)y)x$ *or, equivalently,* $R_{xyx} = R_xR_yR_x$,

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

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

Proof. The identities (i) — (iii) are well-known (see, e.g., Lemma 2.7 in [3]). For (iv) and (v), see relation (8) in [7]. ▲

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 $A^\diamond$ the Cayley-Dickson duplication of A, which is the vector F-space $A \oplus A$ with multiplication

$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - \overline{b}_2b_1, b_2a_1 + b_1\overline{a}_2). \tag{4.2}$$

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

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

$$\begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix}, \quad a, b \in F, \quad \mathbf{v}, \mathbf{w} \in F^3 \tag{4.3}$$

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

$$\begin{pmatrix} a_1 & \mathbf{v}_1 \\ \mathbf{w}_1 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & \mathbf{v}_2 \\ \mathbf{w}_2 & b_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + \mathbf{v}_1 \cdot \mathbf{w}_2 & a_1\mathbf{v}_2 + b_2\mathbf{v}_1 \\ a_2\mathbf{w}_1 + b_1\mathbf{w}_2 & \mathbf{w}_1 \cdot \mathbf{v}_2 + b_1b_2 \end{pmatrix} + \begin{pmatrix} 0 & -\mathbf{w}_1 \times \mathbf{w}_2 \\ \mathbf{v}_1 \times \mathbf{v}_2 & 0 \end{pmatrix}, \tag{4.4}$$

where, for $\mathbf{v} = (v_1, v_2, v_3)$ and $\mathbf{w} = (w_1, w_2, w_3)$ in F^3, we denoted

$$\mathbf{v} \cdot \mathbf{w} = v_1w_1 + v_2w_2 + v_3w_3 \in F,$$
$$\mathbf{v} \times \mathbf{w} = (v_2w_3 - v_3w_2, v_3w_1 - v_1w_3, v_1w_2 - v_2w_1) \in F^3.$$

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

$$e_1 = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{0} & 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 & \mathbf{j} \\ \mathbf{0} & 0 \end{pmatrix}, e_4 = \begin{pmatrix} 0 & \mathbf{k} \\ \mathbf{0} & 0 \end{pmatrix},$$
$$f_1 = \begin{pmatrix} 0 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 0 & \mathbf{0} \\ -\mathbf{i} & 0 \end{pmatrix}, f_3 = \begin{pmatrix} 0 & \mathbf{0} \\ -\mathbf{j} & 0 \end{pmatrix}, f_4 = \begin{pmatrix} 0 & \mathbf{0} \\ -\mathbf{k} & 0 \end{pmatrix}, \tag{4.5}$$

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

For $x \in \mathbb{O}$ define its *conjugate* $\overline{x}$ by

$$\overline{\begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix}} = \begin{pmatrix} b & -\mathbf{v} \\ -\mathbf{w} & a \end{pmatrix}$$

Table 2. Multiplication table of the algebra $\mathbb{O}$

	e_1	e_2	e_3	e_4	f_1	f_2	f_3	f_4
e_1	e_1	e_2	e_3	e_4	.	.	.	.
e_2	.	.	$-f_4$	f_3	e_2	$-e_1$	.	.
e_3	.	f_4	.	$-f_2$	e_3	.	$-e_1$	.
e_4	.	$-f_3$	f_2	.	e_4	.	.	$-e_1$
f_1	.	.	.	.	f_1	f_2	f_3	f_4
f_2	f_2	$-f_1$	.	.	.	.	$-e_4$	e_3
f_3	f_3	.	$-f_1$	.	.	e_4	.	$-e_2$
f_4	f_4	.	.	$-f_1$	.	$-e_3$	e_2	.

Then conjugation is an involution of $\mathbb{O}$. Introduce a quadratic form $Q : \mathbb{O} \to F$ by

$$\begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} \overset{Q}{\longmapsto} ab - \mathbf{v} \cdot \mathbf{w},$$

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

$$(e_i, f_i) = 1, \quad Q(e_i) = Q(f_i) = (e_i, f_j) = (e_i, e_j) = (f_i, f_j) = 0 \quad \text{for} \quad 1 \leqslant i \neq j \leqslant 4,$$

In particular, the norm of an arbitrary element of $\mathbb{O}$ is

$$Q(a_1 e_1 + \ldots + a_4 e_4 + b_1 f_1 + \ldots + b_4 f_4) = a_1 b_1 + \ldots + a_4 b_4.$$

If the characteristic of F is not 2 then $\mathbb{O}$ 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

$$\begin{gathered} \varepsilon_1 = e_2 + f_2, \quad \varepsilon_2 = e_3 + f_3, \quad \varepsilon_3 = a(e_1 - f_1) + b(e_2 - f_2), \\ \varepsilon_4 = \varepsilon_1 \varepsilon_2, \quad \varepsilon_5 = \varepsilon_2 \varepsilon_3, \quad \varepsilon_6 = \varepsilon_3 \varepsilon_4, \quad \varepsilon_7 = \varepsilon_4 \varepsilon_5, \end{gathered} \tag{4.6}$$

together with 1, form a basis of $\mathbb{O}$ and multiply as shown in Table 3. This table is uniquely

Table 3. An alternative multiplication table of $\mathbb{O}$ in odd characteristic.

$\mathbf{1}$	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	ε_7
ε_1	$-\mathbf{1}$	ε_4	ε_7	$-\varepsilon_2$	ε_6	$-\varepsilon_5$	$-\varepsilon_3$
ε_2	$-\varepsilon_4$	$-\mathbf{1}$	ε_5	ε_1	$-\varepsilon_3$	ε_7	$-\varepsilon_6$
ε_3	$-\varepsilon_7$	$-\varepsilon_5$	$-\mathbf{1}$	ε_6	ε_2	$-\varepsilon_4$	ε_1
ε_4	ε_2	$-\varepsilon_1$	$-\varepsilon_6$	$-\mathbf{1}$	ε_7	ε_3	$-\varepsilon_5$
ε_5	$-\varepsilon_6$	ε_3	$-\varepsilon_2$	$-\varepsilon_7$	$-\mathbf{1}$	ε_1	ε_4
ε_6	ε_5	$-\varepsilon_7$	ε_4	$-\varepsilon_3$	$-\varepsilon_1$	$-\mathbf{1}$	ε_2
ε_7	ε_3	ε_6	$-\varepsilon_1$	ε_5	$-\varepsilon_4$	$-\varepsilon_2$	$-\mathbf{1}$

restored from the relations

$$\begin{aligned} \varepsilon_r^2 = -\mathbf{1}, \qquad & \varepsilon_{r+1}\varepsilon_{r+3} = \varepsilon_{r+2}\varepsilon_{r+6} = \varepsilon_{r+4}\varepsilon_{r+5} = \varepsilon_r, \\ & \varepsilon_{r+3}\varepsilon_{r+1} = \varepsilon_{r+6}\varepsilon_{r+2} = \varepsilon_{r+5}\varepsilon_{r+4} = -\varepsilon_r, \qquad \varepsilon_{r+7} = \varepsilon_r, \end{aligned} \tag{4.7}$$

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

$$\overline{\varepsilon_0} = \varepsilon_0, \qquad \overline{\varepsilon_i} = -\varepsilon_i, \quad \text{for} \quad 1 \leqslant i \leqslant 7, \tag{4.8}$$

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

$$Q(a_0\varepsilon_0 + a_1\varepsilon_1 + \ldots + a_7\varepsilon_7) = a_0^2 + a_1^2 + \ldots + a_7^2. \tag{4.9}$$

Let q be arbitrary. The following properties of the Cayley algebra $\mathbb{O}$ are well-known.

Lemma 8 *We have*

(i) $\mathbb{O}$ is an alternative algebra.

(ii) the space $(\mathbb{O}, Q)$ is a non-degenerate orthogonal space of type '+'.

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

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

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

(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) $(zx,y) = (x,\overline{z}y)$ *and* $(xz,y) = (x,y\overline{z})$,

(ix) $(x,y)(z,w) = (xz,yw) + (xw,zy)$.

Proof. See chapter 2 in [3]. ▲

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

$$\mathbb{M} = \langle e_1, e_2, f_1, f_2\rangle, \qquad \mathbb{F} = \langle 1, e_2 + f_2 + sf_1\rangle, \qquad \mathbb{P} = \langle e_1, f_1\rangle. \tag{4.10}$$

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

$$\begin{pmatrix} a_1 & (a_2,0,0) \\ (a_3,0,0) & a_4 \end{pmatrix} \longmapsto \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

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

$$\overline{\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}} = \begin{pmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{pmatrix}.$$

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

Denote $w_i = e_i + f_i$, $i = 1,\ldots,4$. Observe that $\mathfrak{w} = \{w_1,\ldots,w_4\}$ is a Q-orthonormal set. It is directly verified that

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

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

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

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

$$\begin{aligned} \mathbb{O} &= \mathbb{F}w_1 \oplus \mathbb{F}w_2 \oplus \mathbb{F}w_3 \oplus \mathbb{F}w_4, \\ \mathbb{O} &= \mathbb{P}w_1 \oplus \mathbb{P}w_2 \oplus \mathbb{P}w_3 \oplus \mathbb{P}w_4. \end{aligned} \tag{4.11}$$

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

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

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

(ii) $\overline{v} = -v, \quad va = \overline{a}v,$

(iii) $a(bv) = (ba)v, \quad (vb)a = v(ab),$

(iv) $(av)w = (vw)a, \quad w(va) = a(wv).$

Proof.

(i)–(iii) See Lemma 6 in chapter 2 of [3].

(iv) For every $c \in A$, we have by (ii) and (8.viii–ix)

$$((av)w - (vw)a, c) = (av, c\overline{w}) - (vw, c\overline{a}) = (v\overline{a}, c\overline{w}) + (v\overline{w}, c\overline{a}) = (v, c)(\overline{a}, \overline{w}) = 0,$$

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. ▲

This lemma implies that

$$\mathbb{O} = \mathbb{M} \oplus \mathbb{M}w_3 \tag{4.12}$$

is a $\mathbb{Z}_2$-grading of $\mathbb{O}$ and (4.11) are $\mathbb{Z}_2 \times \mathbb{Z}_2$-gradings of $\mathbb{O}$.

Introduce the projective space $PG(\mathbb{O}) = \{\langle x \rangle \mid x \in \mathbb{O}\}$. By analogy with the standard notation, we put

$$\begin{array}{ll} GL(\mathbb{O}) = \{x \in \mathbb{O} \mid Q(x) \neq 0\}, & PGL(\mathbb{O}) = \{\langle x \rangle \in PG(\mathbb{O}) \mid Q(x) \neq 0\}, \\ SL(\mathbb{O}) = \{x \in \mathbb{O} \mid Q(x) = 1\}, & PSL(\mathbb{O}) = \{\langle x \rangle \in PG(\mathbb{O}) \mid Q(x) \in (F^*)^2\}. \end{array} \tag{4.13}$$

In particular, $PSL(\mathbb{O})$ is the set of all $+1$-subspaces of $\mathbb{O}$. By (8.i) and (7.i), we see that $GL(\mathbb{O})$, $SL(\mathbb{O})$, $PGL(\mathbb{O})$, and $PSL(\mathbb{O})$ are Moufang loops with multiplication induced from $\mathbb{O}$. Note that $\{\pm 1\}$ is a normal subgroup of $SL(\mathbb{O})$ and $SL(\mathbb{O})/\{\pm 1\} \cong PSL(\mathbb{O})$. Similarly, $GL(\mathbb{O})/\langle 1 \rangle \cong PGO(\mathbb{O})$. It is easy to see that

$$|GL(\mathbb{O})| = (q^4 - q^3)(q^4 - 1), \qquad |PSL(\mathbb{O})| = \frac{1}{d}q^3(q^4 - 1),$$
$$|PGL(\mathbb{O})| = |SL(\mathbb{O})| = q^3(q^4 - 1).$$

Let $GO(\mathbb{O})$ be the group of all linear transformations of $\mathbb{O}$ that preserve the quadratic form Q. We also introduce the groups

$$SO(\mathbb{O}) = \{g \in GO(\mathbb{O}) \mid \det g = 1\}, \qquad \Omega(\mathbb{O}) = GO(\mathbb{O})',$$

$$PGO(\mathbb{O}) = GO(\mathbb{O})/Z(GO(\mathbb{O})), \qquad P\Omega(\mathbb{O}) = PGO(\mathbb{O})'.$$

Then $P\Omega(\mathbb{O})$ is a finite simple group isomorphic to $P\Omega_8^+(q)$. We denote the image in $PGO(\mathbb{O})$ of an element $g \in GO(\mathbb{O})$ by $\check{g}$.

A *reflection* r_v in a non-singular vector $v \in \mathbb{O}$ is the linear transformation of $\mathbb{O}$ given by

$$xr_v = x - \frac{(x,v)}{Q(v)}v \quad \text{for all} \quad x \in \mathbb{O}. \tag{4.14}$$

Lemma 10 *Let $v, w \in \mathbb{O}$ be non-singular. Then we have*

(i) r_v is an involution in $GO(\mathbb{O})$ 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 $g \in GO(\mathbb{O})$,

(iv) $g \in GO(\mathbb{O})$ centralizes r_v if and only if $\langle v \rangle g = \langle v \rangle$.

Proof. Immediate consequence of the definition. ▲

Using (8.vi-vii), we can rewrite

$$xr_v = x - \frac{(x\overline{v})v + (v\overline{x})v}{Q(v)} = -\frac{1}{Q(v)}v\overline{x}v. \tag{4.15}$$

This expression is fundamental in that it relates the action of $GO(\mathbb{O})$ (which is generated by reflections) with the multiplication in $\mathbb{O}$. In particular, the conjugation in $\mathbb{O}$ is $-r_1$. The projective action of generators of $PGO(\mathbb{O})$ on $PG(\mathbb{O})$ is then written as

$$\langle x \rangle \check{r}_v = \langle v\overline{x}v \rangle \quad \text{for all} \quad x \in \mathbb{O}. \tag{4.16}$$

We also introduce, for every $\langle v \rangle \in PG(\mathbb{O})$, the projective analogs $U_{\langle v \rangle}$, $L_{\langle v \rangle}$, $R_{\langle v \rangle}$ of the operators (4.1) as follows:

$$\langle x \rangle U_{\langle v \rangle} = \langle vxv \rangle, \qquad \langle x \rangle L_{\langle v \rangle} = \langle vx \rangle, \qquad \langle x \rangle R_{\langle v \rangle} = \langle xv \rangle \qquad \text{for all} \quad \langle x \rangle \in PG(\mathbb{O}).$$

Note that

$$U_{\langle v\rangle} \in PGO(\mathbb{O}) \iff \langle v\rangle \in PGL(\mathbb{O}),$$
$$L_{\langle v\rangle}, R_{\langle v\rangle} \in PGO(\mathbb{O}) \iff \langle v\rangle \in PSL(\mathbb{O}).$$

In fact, whenever $\langle v\rangle \in PGL(\mathbb{O})$, we have $U_{\langle v\rangle} = \check{r}_1\check{r}_v$ by (4.16), which implies $U_{\langle v\rangle} \in PSO(\mathbb{O})$. Therefore, $U_{\langle v\rangle} \in P\Omega(\mathbb{O})$ iff $\langle v\rangle \in PSL(\mathbb{O})$ and we will show later (see 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 $x, y \in \mathbb{O}$ be singular elements. Then*

(i) $x\mathbb{O}$ and $\mathbb{O}x$ are t.s. 4-subspaces of $\mathbb{O}$,

(ii) every t.s. 4-subspace has form $x\mathbb{O}$ or $\mathbb{O}x$ for some x,

(iii) $\langle x\rangle = \langle y\rangle \iff x\mathbb{O} = y\mathbb{O} \iff \mathbb{O}x = \mathbb{O}y$,

(iv) $a \in x\mathbb{O} \iff \overline{x}a = 0$, and $a \in \mathbb{O}x \iff a\overline{x} = 0$,

(v) $(x,y) \neq 0 \iff \dim(x\mathbb{O} \cap y\mathbb{O}) = 0$,

(vi) $(x,y) = 0$ and $\langle x\rangle \neq \langle y\rangle$ if and only if $\dim(x\mathbb{O} \cap y\mathbb{O}) = 2$, in which case $x\mathbb{O} \cap y\mathbb{O} = x(\overline{y}\mathbb{O}) = y(\overline{x}\mathbb{O})$,

(vii) $xy = 0 \iff \dim(x\mathbb{O} \cap \mathbb{O}y) = 3$,

(viii) $xy \neq 0 \iff \dim(x\mathbb{O} \cap \mathbb{O}y) = 1$,

Proof. These properties are well known. For proofs, see, e.g., §2 in [10]. ▲

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

5 Automorphisms of the Cayley algebra

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

Let $A \in \{\mathbb{F}, \mathbb{P}\}$ be a commutative subalgebra of $\mathbb{O}$ defined by (4.10). By lemma 9 and (4.11), $\mathbb{O}$ is a 4-dimensional left and right A-module with basis $\mathfrak{w} = \{w_1, \ldots, w_4\}$. Every left A-(semi)linear transformation f of $A^\perp$ is also right A-(semi)linear, since by (9.i)

$$(va)f = (\bar{a}v)f = (\bar{a}\tau)(vf) = (vf)(a\tau) \tag{5.1}$$

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

$$\lambda = \begin{cases} e_2 + f_2 + sf_1, & \text{if } A = \mathbb{F}, \\ te_1 + t^{-1}f_1, & \text{if } A = \mathbb{P}, \end{cases} \tag{5.2}$$

Where $s, t \in \boldsymbol{F}$ are such that the polynomial $x^2 - sx + 1$ is irreducible over $\boldsymbol{F}$ and t generates $\boldsymbol{F}^*$. Then λ has order $q+1$ and $q-1$ in the respective cases $A = \mathbb{F}$ and $A = \mathbb{P}$. Note that $\lambda - \bar{\lambda}$ is invertible in A unless $A = \mathbb{P}$ and $q = 2, 3$. We will assume that $q \geqslant 4$ in this case. For arbitrary $x, y \in \mathbb{O}$ define

$$k_A(x,y) = \frac{\lambda(x,y) - (x, \lambda y)}{\lambda - \bar{\lambda}}. \tag{5.3}$$

Lemma 12 *We have*

(i) k_A is an A-sesquilinear form on $\mathbb{O}$,

(ii) $k_A(x,x) = Q(x)$,

(iii) $\mathfrak{w}$ is a k_A-orthonormal A-basis of $\mathbb{O}$.

(iv) k_A is non-degenerate.

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

$$\begin{aligned} \lambda k_A(x,y)(\lambda - \bar{\lambda}) &= \lambda^2(x,y) - \lambda(x, \lambda y), \\ k_A(\lambda x, y)(\lambda - \bar{\lambda}) &= \lambda(\lambda x, y) - (\lambda x, \lambda y) = \lambda(x, \bar{\lambda} y) - \lambda\bar{\lambda}(x,y). \end{aligned}$$

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,

$$\begin{aligned} k_A(y,x)(\lambda - \bar{\lambda}) &= \lambda(y,x) - (y, \lambda x) = \lambda(x,y) - (\lambda x, y), \\ \overline{k_A(x,y)}(\bar{\lambda} - \lambda) &= \bar{\lambda}(x,y) - (x, \lambda y) = \bar{\lambda}(x,y) - (\bar{\lambda} x, y). \end{aligned}$$

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

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

$$k_A(x,x)(\lambda-\overline{\lambda}) = \lambda(x,x)-(x,\lambda x) = 2\lambda Q(x)-(\mathbf{1},(\lambda x)\overline{x}) = 2\lambda Q(x)-Q(x)(\mathbf{1},\lambda) = Q(x)(\lambda-\overline{\lambda}).$$

(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 $1 \leqslant i \leqslant 4$ by (ii). Thus, $\mathfrak{w}$ is r_A-orthonormal.

(iv) This follows from (iii). ▲

Although λ appears in the definition (5.3), the form k_A depends only on A. Indeed, if $A = \langle \mathbf{1}, \lambda_0 \rangle_F$ for some $\lambda_0 = a\lambda + b \in A$ with $a, b \in F$, $a \neq 0$, then substitution λ_0 for λ 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. However, we will not be using this.

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

$$t_A(u,v,w) = k_A(u, vw). \tag{5.4}$$

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 $t_A(u,v,v) = k_A(u,-\overline{v}v) = -Q(v)k_A(u,\mathbf{1}) = 0$. It remains to show that $t_A(u,v,w) = t_A(v,w,u)$. By (9.vi), we obtain

$$k_A(u,vw)(\lambda-\overline{\lambda}) = \lambda(u,vw)-(u,\lambda(vw)) = \lambda(\overline{v}u,w)-(\overline{\lambda}u,vw) = -\lambda(vu,w)+(\overline{\lambda}u,\overline{v}w),$$
$$k_A(v,wu)(\lambda-\overline{\lambda}) = \lambda(v,wu)-(v,\lambda(wu)) = \lambda(v\overline{u},w)-(v,w(u\lambda)) = -\lambda(vu,w)-(\overline{w}v,u\lambda).$$

Subtracting the right-hand sides gives

$$(\overline{\lambda}u,\overline{v}w)+(\overline{w}v,u\lambda) = (u\lambda,\overline{v}w)+(u\lambda,\overline{w}v) = (u\lambda,\overline{v}w+\overline{w}v) = (\overline{v},\overline{w})(u\lambda,\mathbf{1}) = 0,$$

since $u\lambda \in A^\perp$. Thus, $t_A(u,v,w) = t_A(v,w,u)$. ▲

If V is an A-submodule of $\mathbf{O}$ 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 $\mathbf{O}$ that preserves the form k_A and leaves V invariant also leaves invariant $V^\perp$.

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

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 $y, z \in \mathbb{O}$ the claim holds by A-(semi)linearity and by (5.1). ▲

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

The full group of automorphisms $Aut(\mathbb{O}(q))$ 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 the explicit form of this 8-dimensional representation of $G_2(q)$. Introduce some basic automorphisms of $\mathbb{O}$. For every $C \in SL_3(q)$, define

$$\delta_0(C) : \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} \longmapsto \begin{pmatrix} a & \mathbf{v}C \\ \mathbf{w}C^{-T} & b \end{pmatrix}, \tag{5.5}$$

and, for every $\mathbf{c} \in \boldsymbol{F}^3$, put

$$\delta_1(\mathbf{c}) : \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} \longmapsto \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} + \begin{pmatrix} \mathbf{v}\cdot\mathbf{c} & \mathbf{w}\times\mathbf{c} \\ (b-a)\mathbf{c} & -\mathbf{v}\cdot\mathbf{c} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ -(\mathbf{v}\cdot\mathbf{c})\mathbf{c} & 0 \end{pmatrix};$$

$$\delta_2(\mathbf{c}) : \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} \longmapsto \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} + \begin{pmatrix} -\mathbf{w}\cdot\mathbf{c} & (a-b)\mathbf{c} \\ -\mathbf{v}\times\mathbf{c} & \mathbf{w}\cdot\mathbf{c} \end{pmatrix} + \begin{pmatrix} 0 & -(\mathbf{w}\cdot\mathbf{c})\mathbf{c} \\ 0 & 0 \end{pmatrix}.$$

Then δ_0, δ_1, δ_2 are automorphisms of $\mathbb{O}$. Note that δ_1 and δ_2 are the exponents (in the sense of §3 in [24]) of the following derivations of $\mathbb{O}$:

$$d_1(\mathbf{c})\colon \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{v}\cdot\mathbf{c} & \mathbf{w}\times\mathbf{c} \\ (b-a)\mathbf{c} & -\mathbf{v}\cdot\mathbf{c} \end{pmatrix}; \quad d_2(\mathbf{c})\colon \begin{pmatrix} a & \mathbf{v} \\ \mathbf{w} & b \end{pmatrix} \mapsto \begin{pmatrix} -\mathbf{w}\cdot\mathbf{c} & (a-b)\mathbf{c} \\ -\mathbf{v}\times\mathbf{c} & \mathbf{w}\cdot\mathbf{c} \end{pmatrix}.$$

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:

$$\begin{gathered} X_{\omega_1}(t)=\delta_1(t\mathbf{i}), \qquad X_{\omega_2}(t)=\delta_1(t\mathbf{j}), \qquad X_{\omega_3}(t)=\delta_1(t\mathbf{k}); \\ X_{-\omega_1}(t)=\delta_2(t\mathbf{i}), \qquad X_{-\omega_2}(t)=\delta_2(t\mathbf{j}), \qquad X_{-\omega_3}(t)=\delta_2(t\mathbf{k}); \\ X_{\omega_i-\omega_j}(t)=\delta_0(E+tE_{i,j}), \quad 1\leqslant i,j\leqslant 3,\ i\neq j; \end{gathered} \tag{5.6}$$

where $t \in F^*$, E is the identity 3×3-matrix, and $E_{i,j}$ are the 3×3 matrix units. These root subgroups generate $D = Aut(\mathbb{O})$. 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 Φ is

$$\Pi = \left\{ \begin{matrix} \omega_1{=}\alpha+\beta, & \omega_2{=}\alpha, & -\omega_3{=}2\alpha+\beta, \\ \omega_1-\omega_3{=}3\alpha+2\beta, & \omega_1-\omega_2{=}\beta, & \omega_2-\omega_3{=}3\alpha+\beta \end{matrix} \right\}. \tag{5.7}$$

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

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

(For all these notions, see [17]. See also pp. 142–143 in [14].)

The group $D = Aut(\mathbb{O})$ lies in $\Omega(\mathbb{O})$ and induces automorphisms of all loops (4.13) associated with $\mathbb{O}$. We identify D with its image $\check{D}$ in $P\Omega(\mathbb{O})$. 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

$$\begin{gathered} \langle x\rangle f\sigma = \langle xf\rangle\sigma = \langle\overline{xf}\rangle = \langle\overline{x}f\rangle = \langle\overline{x}\rangle f = \langle x\rangle\sigma f, \\ \langle x\rangle f\rho = \langle xf\rangle\rho = \langle\overline{xf}\mathbb{O}\rangle = \langle\overline{x}\mathbb{O}\rangle f = \langle x\rangle\rho f. \end{gathered}$$

The two actions of D on $PSL(\mathbb{O})$ and $M(P\Omega(\mathbb{O}))$ are respected by the isomorphism (6.5), since, for every $m = [g, \sigma] \in M(P\Omega(\mathbb{O}))$, 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 in general D does not contain all automorphisms of $PSL(\mathbb{O})$. As follows from [20], the full group $Aut(M(q))$ is the extension of $G_2(q)$ by its field automorphisms.

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.

Table 4. Some maximal subgroups of $G_2(q)$

Type	Order	Comments
P_α	$q^6(q-1)^2(q+1)$	parabolic, short root
P_β	$q^6(q-1)^2(q+1)$	parabolic, long root
$(SL_2(q) \circ SL_2(q)).d$	$q^2(q^2-1)^2$	$q \neq 2$
$2^3{\cdot}PSL_3(2)$	$8 \cdot 168$	$q = p$ odd
$G_2(q_0)$	$q_0^6(q_0^6-1)(q_0^2-1)$	$q = q_0^k$, 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

6 The geometry of triality

Let $\mathfrak{P}$ be the *polar geometry* associated with Q. It is the geometry that 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 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 $Aut(\mathfrak{P})$ is just the extension of $P\Omega(\mathbb{O})$ by its field and diagonal automorphisms (see, e.g., [8], 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 it also admits transformations that preserve the incidence but permute the three types of points. These can be defined in the following way. Let ρ be the transformation of $\mathfrak{P}$ that acts on the points by the rule

$$\langle x\rangle \xmapsto{\rho} \bar{x}\mathbb{O} \xmapsto{\rho} \mathbb{O}\bar{x} \xmapsto{\rho} \langle x\rangle, \tag{6.1}$$

i.e., ρ bijectively maps

$$\{0\text{-points}\} \xmapsto{\rho} \{l\text{-points}\} \xmapsto{\rho} \{r\text{-points}\} \xmapsto{\rho} \{0\text{-points}\}.$$

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 $\sigma = \check{r}_1 \in PGO(\mathbb{O})$, i.e. the action of σ on all objects is induced by conjugation:

$$\langle x\rangle \xmapsto{\sigma} \langle\bar{x}\rangle, \qquad x\mathbb{O} \xmapsto{\sigma} \mathbb{O}\bar{x}, \qquad \mathbb{O}x \xmapsto{\sigma} \bar{x}\mathbb{O}, \qquad \langle x,y\rangle \xmapsto{\sigma} \langle\bar{x},\bar{y}\rangle. \tag{6.2}$$

For details, see [10, 11]. Clearly, ρ and σ normalize $Aut(\mathfrak{P})$ and, in particular, its characteristic subgroup $P\Omega(\mathbb{O})$. We henceforth denote $S = \langle\rho,\sigma\rangle$, where ρ and σ 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

$$\begin{aligned} \langle x\rangle[g,\sigma] &= \langle x\rangle\check{r}_v\check{r}_1 = \langle\overline{v}x\overline{v}\rangle, \\ (x\mathbb{O})[g,\sigma] &= (v(\mathbb{O}\overline{x})v)\check{r}_1 = (\mathbb{O}(\overline{x}v))\check{r}_1 = (\overline{v}x)\mathbb{O}, \\ (\mathbb{O}x)[g,\sigma] &= (v(\overline{x}\mathbb{O})v)\check{r}_1 = ((v\overline{x})\mathbb{O})\check{r}_1 = \mathbb{O}(x\overline{v}), \end{aligned} \tag{6.3}$$

where we have used (4.16), (7.i), and the fact that v is non-singular. Then we have

$$\begin{aligned} \langle x\rangle[g,\sigma]^\rho &= \langle x\rangle\rho^{-1}[g,\sigma]\rho = (\mathbb{O}\overline{x})[g,\sigma]\rho = (\mathbb{O}(\overline{x}\,\overline{v}))\rho = \langle vx\rangle, \\ \langle x\rangle[g,\sigma]^{\rho^2} &= \langle x\rangle\rho[g,\sigma]\rho^{-1} = (\overline{x}\mathbb{O})[g,\sigma]\rho^{-1} = ((\overline{v}\,\overline{x})\mathbb{O})\rho^{-1} = \langle xv\rangle. \end{aligned} \tag{6.4}$$

Therefore,

$$\langle x\rangle[g,\sigma][g,\sigma]^\rho[g,\sigma]^{\rho^2} = \langle\overline{v}x\overline{v}\rangle[g,\sigma]^\rho[g,\sigma]^{\rho^2} = \langle v(\overline{v}x\overline{v})\rangle[g,\sigma]^{\rho^2} = \langle v(\overline{v}x\overline{v})v\rangle = \langle x\rangle$$

for every 0-point $\langle x\rangle$ by (8.vii). Remark 15 now implies $[g,\sigma][g,\sigma]^\rho[g,\sigma]^{\rho^2} = 1$ for all $g \in P\Omega(\mathbb{O})$. ▲

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

$$\theta : M(P\Omega(\mathbb{O})) \to PSL(\mathbb{O}) \tag{6.5}$$

as follows: given an $m = [g,\sigma] \in M(P\Omega(\mathbb{O}))$, put $m\theta = \langle\mathbf{1}\rangle g$. Then $m\theta \in PSL(\mathbb{O})$, since $\langle\mathbf{1}\rangle g$ is a +1-subspace. Note that

$$[g_1,\sigma] = [g_2,\sigma] \iff g_1g_2^{-1} \in C_{P\Omega(\mathbb{O})}(\sigma) \iff \langle\mathbf{1}\rangle g_1 = \langle\mathbf{1}\rangle g_2$$

by (10.iv). This implies that θ is well-defined and injective. It is also surjective, since $P\Omega(\mathbb{O})$ is transitive on +1-subspaces (see [9], Lemma 2.10.5). Therefore, for every $m \in M(P\Omega(\mathbb{O}))$, we have

$$m\theta = \langle v\rangle \iff \langle x\rangle m = \langle\overline{v}x\overline{v}\rangle \quad \text{for all 0-points} \quad \langle x\rangle \in \mathfrak{P} \tag{6.6}$$

by the first equality in (6.3).

Lemma 17 *The mapping θ is an isomorphism of loops $M(P\Omega(\mathbb{O}))$ and $PSL(\mathbb{O})$.*

Proof. Take $m, n \in M(P\Omega(\mathbb{O}))$ and write $m = [g, \sigma]$, $n = [h, \sigma]$ for suitable $g, h \in P\Omega(\mathbb{O})$. Let $\langle 1\rangle g = \langle v\rangle$ and $\langle 1\rangle h = \langle w\rangle$. Note that $m^{-1} = [g^\sigma, \sigma]$ and

$$\langle 1\rangle g^\sigma = \langle 1\rangle \sigma g \sigma = \langle 1\rangle g\sigma = \langle v\rangle \sigma = \langle \overline{v}\rangle.$$

Therefore, using (6.3), (6.4), and (7.iv), we have

$$\langle x\rangle(m.n) = \langle x\rangle m^{-\rho} n m^{-\rho^2} = \langle (\overline{w}(\overline{v}x)\overline{w})\overline{v}\rangle = \langle (\overline{vw})x(\overline{vw})\rangle$$

for every 0-point $\langle x\rangle \in \mathfrak{P}$. By (6.6), we have $(m.n)\theta = \langle vw\rangle = (m\theta)(n\theta)$. ▲

As a consequence, we have the following description:

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

We can also write the action of ρ on $M(P\Omega(\mathbb{O}))$ in terms of the operators $U_{\langle v\rangle}$, $L_{\langle v\rangle}$, $R_{\langle v\rangle}$. Using (6.6),(6.4), and Remark 15 we have

$$\begin{aligned} M(P\Omega(\mathbb{O})) &= \{U_{\langle v\rangle} \mid \langle v\rangle \in PSL(\mathbb{O})\}, \\ M(P\Omega(\mathbb{O}))^\rho &= \{L_{\langle v\rangle} \mid \langle v\rangle \in PSL(\mathbb{O})\}, \\ M(P\Omega(\mathbb{O}))^{\rho^2} &= \{R_{\langle v\rangle} \mid \langle v\rangle \in PSL(\mathbb{O})\}, \end{aligned} \tag{6.7}$$

and

$$U_{\langle \overline{v}\rangle} \overset{\rho}{\longmapsto} L_{\langle v\rangle} \overset{\rho}{\longmapsto} R_{\langle v\rangle} \overset{\rho}{\longmapsto} U_{\langle \overline{v}\rangle}. \tag{6.8}$$

7 The maximal subloops of $M(q)$

First, we introduce some subloops of the simple loop $PSL(\mathbb{O}) \cong M(q)$.

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

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

It can be verified using (4.4) that they form a subloop of $SL(\mathbb{O})$ whose order is $q^3(q^2-1)$. Its image P in $PSL(\mathbb{O})$ will be called a *parabolic* subloop of $PSL(\mathbb{O})$. We will later show that it is a maximal subloop. Note that $|P| = \frac{1}{d}q^3(q^2-1)$ 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 $r_1 = r_2 = 0$. Even though the composition factors of P are groups, it is non-associative.

2. $(PSL_2(q), 2)$, $q \neq 3$. Recall the process of duplication of a group introduced by Chein in Theorem 1 of [12]. Let H be a group. The set of $2|H|$ symbols $\{h, \widetilde{h} \mid h \in H\}$ with a new multiplication ' $\cdot$ ' defined by

$$g \cdot h = gh, \quad g \cdot \widetilde{h} = \widetilde{hg}, \quad \widetilde{g} \cdot h = \widetilde{gh^{-1}}, \quad \widetilde{g} \cdot \widetilde{h} = h^{-1}g \tag{7.2}$$

for all $g, h \in H$ becomes a Moufang loop. We denote it by $(H, 2)$. Clearly, H is embedded as a normal subgroup of $(H, 2)$ of index 2. Fixing an arbitrary $u \in (H,2)\backslash H$, every element of $(H, 2)$ is uniquely written as h or $h \cdot u$ for suitable $h \in H$. Then, suppressing the ' $\cdot$ ', (7.2) can be rewritten as

$$g(hu) = (hg)u, \quad (gu)h = (gh^{-1})u, \quad (gu)(hu) = hg^{-1}. \tag{7.3}$$

It can be seen that $(H, 2)$ is non-associative iff H is non-abelian.

Now consider the Zorn matrices of the two types

$$\begin{pmatrix} a_1 & (a_2, 0, 0) \\ (a_3, 0, 0) & a_4 \end{pmatrix}, \; a_1a_4 - a_2a_3 = 1; \quad \begin{pmatrix} 0 & (0, r_1, r_3) \\ (0, r_2, r_4) & 0 \end{pmatrix}, \; r_1r_2 + r_3r_4 = -1. \tag{7.4}$$

They form a subloop of $SO(\mathbb{O})$ 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 $(PSL_2(q), 2)$ of order $\frac{2}{d}q(q^2-1)$.

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. The field subloop $PSL(\mathbb{O}(q_0))$ of $PSL(\mathbb{O})$ is of index 2 in a larger subloop. Namely, consider the mapping $\varphi : GL(\mathbb{O}(q_0)) \to PSL(\mathbb{O}(q))$ defined by $x \overset{\varphi}{\mapsto} \langle x\rangle_{F_q}$. It is well defined as every element in $F_{q_0}^*$ is a square in F_q^*. It is easy to see that φ 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. 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 $\{\mathbf{1} = \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_7\}$ that multiply as in Table 3. The quadratic form defined by (4.9) turns $O(\mathbb{R})$ into a Eucledian 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 [16] that $O(\mathbb{R})$ contains a certain set Φ of 240 elements of norm 1, called the units of integral Cayley numbers, which is multiplicatively closed, contains $\mathbf{1}$, and such that $\overline{\Phi} = \Phi$. In other words, Φ is a loop. This set can be defined in terms of an f_Q-orthonormal basis $\{l_1, \ldots, l_8\}$ of $O(\mathbb{R})$, where

$$\begin{array}{llll} l_1 = \frac{1}{2}(\varepsilon_0 + \varepsilon_3), & l_3 = \frac{1}{2}(\varepsilon_2 + \varepsilon_5), & l_5 = \frac{1}{2}(\varepsilon_1 + \varepsilon_7), & l_7 = \frac{1}{2}(\varepsilon_6 + \varepsilon_4), \\ l_2 = \frac{1}{2}(\varepsilon_0 - \varepsilon_3), & l_4 = \frac{1}{2}(\varepsilon_2 - \varepsilon_5), & l_6 = \frac{1}{2}(\varepsilon_1 - \varepsilon_7), & l_8 = \frac{1}{2}(\varepsilon_6 - \varepsilon_4), \end{array} \tag{7.5}$$

as follows:

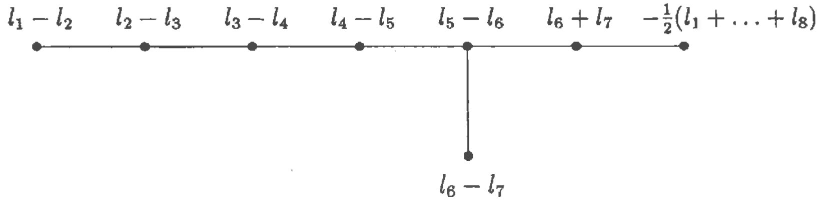
$$\Phi = \left\{ \begin{array}{l} \pm l_s \pm l_t; \;\; 1 \leqslant s, t \leqslant 8, \;\; s \neq t, \\ \frac{1}{2}(i_1 l_1 + i_2 l_2 \ldots + i_8 l_8); \;\; i_s = \pm 1, \;\; i_1 i_2 \ldots i_8 = 1 \end{array} \right\}. \tag{7.6}$$

We have changed here the sign of one of Coxeter's l_i's (see §10 in [16]) so that the product $i_1 i_2 \ldots i_8$ 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. Π is a basis of $O(\mathbb{R})$,

2. The coefficients every $u \in \Phi$ in Π are either all non-negative or all non-positive.

The standard fundamental system Π of Φ 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., [17]).



(7.7)

Let W be the Weyl group of Φ, 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 $2.P\Omega_8^+(2).2$ (see §4 of chap.VI in [18]). Let $W_0 = W' \cong 2.P\Omega_8^+(2)$. Note that

$$W_0 = \langle r_u r_1 \mid u \in \Pi \rangle = \langle U_{\bar{u}} \mid u \in \Pi \rangle. \tag{7.8}$$

Lemma 19 *W_0 acts transitively on Φ.*

Proof. Take $u \in \Phi$. First of all, every u is W-conjugate to a fundamental root in Π (see Proposition 2.1.8 in [17]). 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 $wr_b \in W_0$. 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, $ar_b r_a = b$. Since $r_a r_b \in W_0$ and (7.7) is connected, all fundamental roots are W_0-conjugate and the claim follows. ▲

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

Proof. Let $g \in GO(O(\mathbf{R}))$ leave Φ fixed. It is easy to see that Πg is also a fundamental system of Φ. However, all fundamental systems are W-conjugate by Theorem 2.2.4 in [17], 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 Π, i.e., $g = w^{-1} \in W$. Clearly, $L_u, R_u \in N_{GO(O(\mathbf{R}))}(\Phi)$ for all $u \in \Phi$ and the claim follows. ▲

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 (4.15) 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 Φ is multiplicatively closed and $-\overline{\Phi} = \Phi$. These remarks show that Φ 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 Φ and W with their respective images in $SL(\mathbb{O})$ and $GO(\mathbb{O})$. Denote by $\check{\Phi}$ the image of Φ in $PSL(\mathbb{O})$. Clearly, it is a subloop there of order 120. It is now easy to determine its isomorphism type. Note that $\check{W}_0 \cong P\Omega_8^+(2)$ is an S-subgroup of $P\Omega(\mathbb{O})$. Indeed, $\check{W}_0$ is σ-invariant since $\sigma = \check{r}_1 \in \check{W}$. It is also ρ-invariant by (7.8), (6.8), and Lemma 20. Finally, the Moufang loop $M(\check{W}_0) \cong M(2)$ is isomorphic by Corollary 18 to $\langle 1 \rangle^{\check{W}_0} \leqslant PSL(\mathbb{O})$ which is exactly $\check{\Phi}$ by Lemma 19. In other words, we have demonstrated an explicit embedding of a simple loop $M(2)$ of order 120 into $PSL(\mathbb{O}(p)) \cong M(p)$ for every odd prime p.

It is our purpose 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.

Lemma 21 *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 $\mathbf{v}, \mathbf{w} \in F^3$, we can find a matrix $C \in SL_3(q)$ such that both $\mathbf{v}C$ and $\mathbf{w}C^{-T}$ are in $\langle \mathbf{i} \rangle$, where $\mathbf{i} = (1,0,0)$. 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 $PSL_2(q) \leqslant PSL(\mathbb{O})$. 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 [15]). ▲

Lemma 22 *The subloops of $PSL(\mathbb{O}(q))$ of 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 $M = (PSL_2(q), 2)$ 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 parabolic or $(PSL_2(q), 2)$ such that 120 divides $|N|$. The embedding $M < N$ is impossible, since the composition factors of N are groups and M is simple and non-associative.

c) $q = q_0^2$, $M = (PSL_2(q), 2)$ 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 21, a contradiction.

d) $q = p = 5$, $N = M(2)$, and $M = (PSL_2(5), 2)$. 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. ▲

We note that when $q = 3$, the subloop $(PSL_2(3), 2) \leqslant M(3)$ is isomorphic to a parabolic subloop of $M(2) \leqslant M(3)$ and thus is not maximal (see [13]).

We will need several auxiliary facts. Given a +4-decomposition $\mathbb{O} = V_0 \oplus V_1$, define

$$\mathcal{L}(V_0 \oplus V_1) = \{l \in \mathfrak{P} | \; l \subseteq V_0 \cup V_1\} \tag{7.9}$$

Given an ϵ2-decomposition $\mathbb{O} = V_1 \oplus V_2 \oplus V_3 \oplus V_4$, where $\epsilon = \pm 1$, define

$$\mathcal{L}(V_1 \oplus \ldots \oplus V_4) = \{l \in \mathfrak{P} | \; l \subseteq V_i \oplus V_j \text{ for } 1 \leqslant i < j \leqslant 4\}. \tag{7.10}$$

Let $\boldsymbol{d}$ be a +4- or ϵ2-decomposition of $\mathbb{O}$. Then $\boldsymbol{d}$ is called *S-invariant* if the set of lines $\mathcal{L}(\boldsymbol{d})$ is S-invariant.

Lemma 23 *We have*

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

(ii) If an ϵ2-decomposition $\mathbb{O} = V_1 \oplus \ldots \oplus V_4$ 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 $\overline{x} = y_0 + y_1$, where $y_j \in V_j$. Then $x\overline{x} = xy_0 + xy_1 \in V_0$. Thus $xy_{i+1} = 0$. In particular, if x is invertible then $y_{i+1} = 0$ and $\overline{x} = y_i \in V_i$. Note that V_i contains a basis consisting of invertible elements. By linearity, we have $\overline{V_i} = V_i$ for $i \in \mathbb{Z}_2$. Hence, $\mathcal{L}(V_0 \oplus V_1)$ is σ-invariant.

Let $l = \langle x, y \rangle \subseteq V_i$. First, suppose $x\overline{y} \neq 0$. By Lemma 11, if $l \subseteq \mathbb{O}\overline{z}$ for some singular z then $\langle z \rangle \subseteq l^\rho$. Moreover, $xz = yz = 0$; hence, $(x, \overline{z}) = (y, \overline{z}) = 0$ and $\overline{z} \subseteq l^\perp = l \oplus V_{i+1}$.

Write $z = a\overline{x} + b\overline{y} + \overline{w}$, where $a, b \in F$, $w \in V_{i+1}$. Then

$$xz = bx\overline{y} + x\overline{w} = 0, \quad yz = ay\overline{x} + y\overline{w} = 0.$$

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

Now, suppose $x\overline{y} = 0$. By Lemma 11, $x \in \mathbb{O}y$ and $y \in \mathbb{O}x$. Hence, $l = \mathbb{O}x \cap \mathbb{O}y$. It follows that $l^\rho = \langle \overline{x}, \overline{y} \rangle = l\sigma \subseteq (V_i)\sigma = V_i$ by the first part.

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

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 is the subgroup of $Aut(M(q))$ 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 "✓" ("—") 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 $M(q)$ 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 $G = P\Omega(\mathbb{O})$.

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 $\mathbb{O}$, where $p_0 \leqslant p_l \cap p_r$, 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 $\mathfrak{P}$. It is exactly the normalizer of a triple (p_0, p_l, p_r) of pairwise incident 0-, r-, and l-points of $\mathfrak{P}$. For brevity, call such a triple *a triangle*. Clearly, if a triangle is S-invariant then so is

Table 5. Subloops of $M(q)$ associated with S-maximal subgroups of $P\Omega_8^+(q)$

	I	II	III	IV	V	VI	VII
	G_0	restrictions on q	isomorphism type of $M(G_0)$	$\lvert M(G_0)\rvert$	maximality in $M(q)$	$N_D(M(G_0))$	number of subloops
1.	P_2	—	non-maximal parabolic	$\frac{1}{d}q^3(q-1)$	—	P_β	$(q^6-1)/(q-1)$
2.	R_{s2}	—	maximal parabolic	$\frac{1}{d}q^3(q^2-1)$	✓	P_α	$(q^6-1)/(q-1)$
3.	N_1	—	$\mathbb{Z}_{\frac{1}{d}(q+1)}$	$\frac{1}{d}(q+1)$	—	$SU_3(q):2$	$\frac{1}{2}q^3(q^3-1)$
4.	N_2	$q \geqslant 4$	$\mathbb{Z}_{\frac{1}{d}(q-1)}$	$\frac{1}{d}(q-1)$	—	$SL_3(q):2$	$\frac{1}{2}q^3(q^3+1)$
5.	N_4^4	$q=p \geqslant 3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	8	—	$2^3 \cdot PSL_3(2)$	$\frac{1}{1344}q^6(q^6-1)(q^2-1)$
6.	I_{+2}	$q \geqslant 7$	$(\mathbb{D}_{\frac{2}{d}(q-1)}, 2)$	$\frac{4}{d}(q-1)$	—	$(q-1)^2.(S_3 \times 2)$	$\frac{1}{12}q^6(q^4+q^2+1)(q+1)^2$
7.	I_{-2}	$q \neq 3$	$(\mathbb{D}_{\frac{2}{d}(q+1)}, 2)$	$\frac{4}{d}(q+1)$	$q=2$	$(q+1)^2.(S_3 \times 2)$	$\frac{1}{12}q^6(q^4+q^2+1)(q-1)^2$
8.	I_{+4}	$q \geqslant 3$	$(PSL_2(q), 2)$	$\frac{2}{d}q(q^2-1)$	$q \geqslant 4$	$(SL_2(q) \circ SL_2(q)).d$	$q^4(q^4+q^2+1)$
9.	G_2^1	—	$\langle 1 \rangle$	1	—	D	1
10.	$P\Omega_8^+(q_0)$	$q=q_0^k, k$ prime, $(d,k)=1$	$M(q_0)$	$\frac{1}{d}q_0^3(q_0^4-1)$	✓	$G_2(q_0)$	$\lvert G_2(q_0^k):G_2(q_0)\rvert$
11.	$P\Omega_8^+(q_0).2^2$	$q=q_0^2$ odd	$PGL(\mathbb{O}(q_0))$	$q_0^3(q_0^4-1)$	✓	$G_2(q_0)$	$q_0^6(q_0^6+1)(q_0^2+1)$
12.	$P\Omega_8^+(2)$	$q=p \geqslant 3$	$M(2)$	120	✓	$G_2(2)$	$\frac{1}{12096}q^6(q^6-1)(q^2-1)$

the corresponding parabolic subgroup. By (11.iv), (6.1), and (6.2), it is easy to see that a triangle is S-invariant iff it has the form $(\langle x\rangle, x\mathbb{O}, \mathbb{O}x)$ for every non-zero $x \in \mathbb{O}$ satisfying $x^2 = 0$. Now put $x = e_4$. Then, by Table 2, we have $p_0 = \langle e_4\rangle$, $p_l = e_4\mathbb{O} = \langle e_1, e_4, f_2, f_3\rangle$, $p_r = \mathbb{O}e_4 = \langle e_4, f_1, f_2, f_3\rangle$. 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

$$(p_r \cap p_l)^\perp = \langle e_1, e_4, f_1, f_2, f_3\rangle. \tag{7.11}$$

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

$$\begin{pmatrix} a & (0,0,r_1) \\ (r_2,b,0) & a^{-1} \end{pmatrix}, \quad a, b, r_1, r_2 \in F, \quad a \neq 0. \tag{7.12}$$

This is obviously a subloop of (7.1). We 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 $\langle e_4\rangle$ 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_l, p_r). However, P_β is maximal in D by Table 4. Therefore, $P_\beta = G_0 \cap D$. Since

$$|G_0 : P_\beta| = \frac{\frac{1}{d^2}q^{12}(q-1)^4(q+1)}{q^6(q-1)^2(q+1)} = \frac{1}{d^2}q^6(q-1)^2 = |M(G_0)|^2,$$

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 $\langle x\rangle$ of $\mathfrak{P}$ with $x^2 = 0$ (the so-called *absolute points* of the geometry $\mathfrak{P}$) 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 $\mathbb{O}$, i.e. a line l of $\mathfrak{P}$. Thus S-invariant lines of $\mathfrak{P}$ correspond to S-invariant subgroups in $[G_0]$. Let $l = \langle x, y\rangle$. Since $l^\sigma = \langle \overline{x}, \overline{y}\rangle$ and $l^\rho = \overline{x}\mathbb{O} \cap \overline{y}\mathbb{O}$, 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 $M(G_0) \cong \langle \mathbf{1}\rangle^{G_0}$ is the image in $PSL(\mathbb{O})$ 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 $|G_0 : P_\alpha| = |M(G_0)|^2$; 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 $|D : G_0 \cap D| = (q^6-1)/(q-1)$. Also, there exists a one-to-one correspondence between the S-invariant lines (which are the *absolute lines* of $\mathfrak{P}$) and maximal parabolic subloops of $M(q)$.

3-4. G_0 is an N_1- or N_2-subgroup. In the latter case, assume $q \geq 4$. To treat these two cases uniformly, we slightly change the notation used in [5]. Let $\epsilon = \pm 1$. By definition, an ***$R_{\epsilon 2}$*-subgroup** of G is the normalizer $N_G(W)$ of an ϵ2-subspace W of $\mathbb{O}$. An ***F_{-2}*-subgroup** is the image in G of the normalizer of an irreducible subgroup of $\Omega(\mathbb{O})$ isomorphic to $SU_4(q)$. An ***F_{+2}*-subgroup** (called I_{s4}-subgroup in [5]) is the stabilizer of a decomposition of $\mathbb{O}$ into the direct sum of two t.s. 4-subspaces. If K is either an $R_{\epsilon 2}$ subgroup or an $F_{\epsilon 2}$-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 $N \leqslant G$ is an ***$N_{\epsilon 1}$*-subgroup** (called N_1-subgroup for $\epsilon = -1$ and N_2-subgroup for $\epsilon = +1$ in [5]) if $N = R \cap F$, with R an $R_{\epsilon 2}$ subgroup, F an $F_{\epsilon 2}$-subgroup, and $[\eta(R), \eta(F)] = 1$.

We explain a geometric interpretation of $F_{\epsilon 2}$- and $R_{\epsilon 2}$-subgroups of G. Let $A = \mathbb{F}$ if

$\epsilon = -1$ and $A = \mathbb{P}$ if $\epsilon = +1$. By (4.11), $\mathbb{O}$ is a left A-module of dimension 4 with A-basis $\mathfrak{w} = \{w_1, \ldots, w_4\}$. 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 $G_{\epsilon 1}$ of $GL(W_{\epsilon l})$ consisting of A-linear maps that preserve k_A is naturally embedded into $GO(\mathbb{O})$. We identify $G_{\epsilon 1}$ with its image in $GO(\mathbb{O})$. Observe that G_{-1} is the unitary group $GU(W_{-l}) \cong GU_4(F)$. Also, there is an obvious natural isomorphism between $GL(W_{+l}) = GL_4(\mathbb{P})$ and $GL_4(F) \times GL_4(F)$ under which G_{+1} is mapped onto the subgroup $\{(C, C^{-T}) \mid C \in GL_4(F)\} \cong GL_4(F)$. Shortly, $G_{\epsilon 1} \cong GL_4^{\epsilon}(F)$.

Since the involution in A is induced by $-r_{w_1}$, the element $\delta = -r_{w_1} r_{w_3} r_{w_2} r_{w_4} \in \Omega(\mathbb{O})$ normalizes $G_{\epsilon 1}$ and induces in it the contragredient automorphism $C \mapsto C^{-T}$ of order 2. Let

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

By (12.ii), the elements of $\mathcal{L}(W_l)$ are lines in $\mathfrak{P}$ and the normalizer $F_{\epsilon l} = N_G(\mathcal{L}(W_{\epsilon l}))$ is exactly an $F_{\epsilon 2}$-subgroup of G. Indeed, $G_{\epsilon 1}$ clearly normalizes $\mathcal{L}(W_{\epsilon l})$ and so does δ. However, the images in G of $G_{\epsilon 1} \cap \Omega(\mathbb{O})$ and δ generate an $F_{\epsilon 2}$-subgroup which coincides with $F_{\epsilon l}$. Note that $\eta(F_{\epsilon l})$ lies in the image in G of $\langle \mathrm{diag}_{\mathfrak{w}}(\lambda, \lambda, \lambda, \lambda) \rangle$, where λ 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 $\mathcal{L}(W_{\epsilon r})$ of form xA for all singular $x \in W_{\epsilon r}$, and see that the normalizer $F_{\epsilon r} = N_G(\mathcal{L}(W_{\epsilon r}))$ is an $F_{\epsilon 2}$-subgroup of G.

Note that A is an $\epsilon 2$-subspace of $\mathbb{O}$. Hence, the normalizer $R_\epsilon = N_G(A)$ is an $R_{\epsilon 2}$-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 $\langle \mathrm{diag}_{\mathfrak{w}}(\lambda, 1, 1, 1) \rangle$, which implies $[\eta(R_\epsilon), \eta(F_{\epsilon l})] = 1$. Define

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

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

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

for which it suffices to show that

$$\mathcal{L}(A^\perp) \xmapsto{\rho} \mathcal{L}(W_{\epsilon l}) \xmapsto{\rho} \mathcal{L}(W_{\epsilon r}) \xmapsto{\rho} \mathcal{L}(A^\perp). \qquad (7.13)$$

Let $l = Ax \in \mathcal{L}(W_{\epsilon l})$. Then $l = \langle x, \lambda x\rangle_F$. Since $(\lambda x)\overline{x} = x(\overline{\lambda x}) = 0$, (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 $l\rho = \langle \overline{x}, \overline{\lambda x}\rangle = \overline{x}A \in \mathcal{L}(W_{\epsilon r})$ and $l\rho^2 = x\mathbb{O} \cap (\lambda x)\mathbb{O} = x((\overline{\lambda x})\mathbb{O}) = (\lambda x)(\overline{x}\mathbb{O})$ by (11.vi). Note that a line of form $a(\overline{b}\mathbb{O})$ is orthogonal to $v \in \mathbb{O}$ if and only if $b(\overline{a}v) = 0$, since

$$(a(\overline{b}\mathbb{O}), v) = (\overline{b}\mathbb{O}, \overline{a}v) = (\mathbb{O}, b(\overline{a}v))$$

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

Denote $N_{\epsilon 1} = R_\epsilon \cap F_{\epsilon l} \cap F_{\epsilon r}$. The above remarks show that $N_{\epsilon 1}$ is ρ-invariant. Since $A\sigma = \overline{A} = A$, we have $R_\epsilon^\sigma = R_\epsilon$ and $F_{\epsilon l}^\sigma = R_\epsilon^{\rho\sigma} = R_\epsilon^{\sigma\rho^2} = R_\epsilon^{\rho^2} = F_{\epsilon r}$. Hence, $N_{\epsilon 1}$ is σ-invariant and S-invariant. Show that $N_{\epsilon 1} = R_\epsilon \cap F_{\epsilon l}$. This will imply that $N_{\epsilon 1}$ is an $N_{\epsilon 1}$-subgroup of G in the sense of the definition given above. By triality, it suffices to show that $F_{\epsilon l} \cap F_{\epsilon r} \subseteq R_\epsilon$. Every $g \in F_{\epsilon l} \cap F_{\epsilon r}$ normalizes $\mathcal{L}_0 = \mathcal{L}(W_{\epsilon l}) \cap \mathcal{L}(W_{\epsilon r})$. If we show that

$$\mathcal{L}_0 = \mathcal{L}(W_{\epsilon l}) \cap \mathcal{L}(A^\perp) \tag{7.14}$$

this will imply that $g \in N_G(\langle \mathcal{L}_0\rangle_F) = N_G(A^\perp) = R_\epsilon$ as is required. By triality, (7.14) is equivalent to $\mathcal{L}(W_{\epsilon l}) \cap \mathcal{L}(A^\perp) \subseteq \mathcal{L}(W_{\epsilon r})$. However, every line $l = Ax$ in $A^\perp$ has form $l = xA$ by (9.ii) and the claim follows.

Therefore, $N_{\epsilon 1}$ is an S-invariant $N_{\epsilon 1}$-subgroup of G and we may assume that $G_0 = N_{\epsilon 1}$. 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 $\check{r}_v$, where $\langle v\rangle_F \leqslant A$ is a $+1$-subspace, and that all such involutions are G_0-conjugate. By Corollary 18, $M(G_0) \cong \langle 1\rangle^{G_0}$ is the set of all such $+1$ subspaces. Clearly, λ, which has order $q - \epsilon$, generates the subgroup of all elements with norm 1 in A. Since λ has the first form in (7.4), the subloop $M(G_0) \cong \mathbb{Z}_{\frac{1}{2}(q-\epsilon)}$ lies in $(PSL_2(q), 2)$ and thus is not maximal.

We find $G_0 \cap D$. Consider the group $SL^\epsilon(A^\perp)$, which consists of 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 $\mathfrak{w}$. Then the elements of $SL^\epsilon(A^\perp)$, together with δ, 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 $t_A(w_2f, w_3f, w_4f) = det(a_{ij})\tau t_A(w_2, w_3, w_4)$, where τ 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 $SL^\epsilon(A^\perp)$, together with δ, are automorphisms of $\mathbb{O}$. Hence, their images in G lie in $G_0 \cap D$ and generate a subgroup isomorphic to $SL_3^\epsilon(q) : 2$. Since this group is maximal in D by Table 4, it must coincide with $G_0 \cap D$.

We now have

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

By Lemma 6, all subloops of $M(q)$ arising from S-invariant $N_{\epsilon 1}$-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 $\mathbf{b} = (\mathbf{1} = \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_7)$ be the basis of $\mathbb{O}$ 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 $\check{z}_1$, $\check{z}_2$, $\check{z}_3$, where

$$\begin{aligned} z_1 &= \mathrm{diag}_{\mathbf{b}}(-1,-1,-1,\ \ 1,-1,\ \ 1,\ \ 1,\ \ 1),\\ z_2 &= \mathrm{diag}_{\mathbf{b}}(-1,\ \ 1,-1,-1,\ \ 1,-1,\ \ 1,\ \ 1),\\ z_3 &= \mathrm{diag}_{\mathbf{b}}(-1,\ \ 1,\ \ 1,-1,-1,\ \ 1,-1,\ \ 1) \end{aligned}$$

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

Since $\check{z}_i = \check{r}_{\varepsilon_0}\check{r}_{\varepsilon_i}\check{r}_{\varepsilon_{i+1}}\check{r}_{\varepsilon_{i+3}}$, for $i = 1,2,3$, we have $(\check{z}_i)^\sigma = \check{r}_{\overline{\varepsilon}_0}\check{r}_{\overline{\varepsilon}_i}\check{r}_{\overline{\varepsilon}_{i+1}}\check{r}_{\overline{\varepsilon}_{i+3}} = \check{z}_i$ by (4.8). Hence σ centralizes P. For brevity, put $j = i+1$, $k = i+3$. Then, for every 0-point $\langle x\rangle$, (4.16) and (4.8) imply

$$\begin{aligned} \langle x\rangle\check{z}_i = \langle x\rangle\check{r}_1\check{r}_{\varepsilon_i}\check{r}_{\varepsilon_j}\check{r}_{\varepsilon_k} = \langle\overline{x}\rangle\check{r}_{\varepsilon_i}\check{r}_{\varepsilon_j}\check{r}_{\varepsilon_k} = \langle\varepsilon_i x\varepsilon_i\rangle\check{r}_{\varepsilon_j}\check{r}_{\varepsilon_k} = \\ \langle\varepsilon_j(\varepsilon_i\overline{x}\varepsilon_i)\varepsilon_j\rangle\check{r}_{\varepsilon_k} = \langle\varepsilon_k(\varepsilon_j(\varepsilon_i x\varepsilon_i)\varepsilon_j)\varepsilon_k\rangle. \end{aligned}$$

By (6.1) and (7.i), we also have

$$\begin{aligned} \langle x\rangle(\check{z}_i)^\rho = \langle x\rangle\rho^{-1}\check{z}_i\rho = (\mathbb{O}\overline{x})\check{r}_1\check{r}_{\varepsilon_i}\check{r}_{\varepsilon_j}\check{r}_{\varepsilon_k}\rho = (x\mathbb{O})\check{r}_{\varepsilon_i}\check{r}_{\varepsilon_j}\check{r}_{\varepsilon_k}\rho = \\ (\mathbb{O}(\overline{x}\varepsilon_i))\check{r}_{\varepsilon_j}\check{r}_{\varepsilon_k}\rho = ((\varepsilon_j(\varepsilon_i x))\mathbb{O})\check{r}_{\varepsilon_k}\rho = \big(\mathbb{O}(((\overline{x}\varepsilon_i)\varepsilon_j)\varepsilon_k)\big)\rho = \big\langle\varepsilon_k(\varepsilon_j(\varepsilon_i x))\big\rangle. \end{aligned}$$

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

$$\langle\varepsilon_k(\varepsilon_j(\varepsilon_i x\varepsilon_i)\varepsilon_j)\varepsilon_k\rangle = \langle\varepsilon_k\big((\varepsilon_j(\varepsilon_i x))(\varepsilon_i\varepsilon_j)\big)\varepsilon_k\rangle = \big\langle\big((\varepsilon_k(\varepsilon_j(\varepsilon_i x)))((\varepsilon_i\varepsilon_j)\varepsilon_k)\big)\big\rangle = \langle\varepsilon_k(\varepsilon_j(\varepsilon_i x))\rangle.$$

Therefore, $(\check{z}_i)^\rho = \check{z}_i$ by Remark 15; i.e., ρ 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 $\mathfrak{b}$. (see item 6 of the proof of Theorem 2 in [1]). By Corollary 18, the subloop $M(G_0) \cong \langle\mathbf{1}\rangle^{G_0}$ 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 $\{e_1, \ldots, f_4\}$ of $\mathbb{O}$, we see by (4.6) that ε_1, ε_2, ε_3 have form (7.4). Hence, $M(G_0)$ lies in the subloop $(PSL_2(2), 2)$ of $M(G)$ and thus is not maximal.

Since S centralizes P, we have $P \leqslant D$ (see the remarks before Table 4). The group P can be characterized as the group of automorphisms of $\mathbb{O}$ that centralize the set of basis $+1$-subspaces $\{\langle\varepsilon\rangle \mid \varepsilon \in \mathfrak{b}\}$. Consider the group P_0 of automorphisms of $\mathbb{O}$ that *normalize* this set. Define two transformations α_1 and α_2 of $\mathbb{O}$ on the basis by

$$\varepsilon_i \overset{\alpha_1}{\mapsto} \varepsilon_{i\tau_1},\ i = 1, \ldots, 7, \quad \tau_1 = (1234567);$$
$$\varepsilon_i \overset{\alpha_2}{\mapsto} -\varepsilon_{i\tau_2},\ i = 1, \ldots, 6, \quad \varepsilon_7 \overset{\alpha_2}{\mapsto} \varepsilon_7, \quad \tau_2 = (12)(36).$$

A direct verification shows that α_1 and α_2 belong to P_0 and generate (modulo P) a group isomorphic to the non-split extension $2^3{\cdot}PSL_3(2)$ 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 [16]). Hence, we have $G_0 \cap D = N_D(P) = P_0$ and

$$|G_0 : G_0 \cap D| = (2^{12}\cdot 3\cdot 7)/(8\cdot 168) = 64 = |M(G_0)|^2.$$

Hence, by Lemma 6, all subloops of $M(q)$ arising from S-invariant N_4^4-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 $I_{\epsilon 2}$-subgroup, $\epsilon = \pm 1$. If $\epsilon = +1$ then assume that $q \geqslant 7$ and if $\epsilon = -1$ then assume that $q \neq 3$. An *$I_{\epsilon 2}$-subgroup* G_0 is the normalizer in G of an $\epsilon 2$-decomposition $\mathbb{O} = V_1 \oplus \ldots \oplus V_4$. Denote this decomposition by $\boldsymbol{d}$. Observe that G_0 also normalizes the set of lines $\mathcal{L}(\boldsymbol{d})$ (see 7.10). Conversely, suppose $g \in G$ normalizes $\mathcal{L}(\boldsymbol{d})$. Then g also normalizes the set of +4-subspaces that can be represented as $l_1 \oplus l_2$ for $l_1, l_2 \in \mathcal{L}(\boldsymbol{d})$. Clearly, these are the subspaces $V_i \oplus V_j$ for $1 \leqslant i < j \leqslant 4$. Since their nontrivial pairwise intersections are the components V_i, $i = 1, \ldots, 4$, it follows that g normalizes $\boldsymbol{d}$. In particular, if $\boldsymbol{d}$ is S-invariant then so is G_0.

Now let $\boldsymbol{d}$ be the first decomposition in (4.11) if $\epsilon = -1$ and the second one if $\epsilon = +1$. Since $\boldsymbol{d}$ is a $\mathbb{Z}_2 \times \mathbb{Z}_2$-grading, (23.ii) implies that $\boldsymbol{d}$ is S-invariant. Hence, we may assume that $G_0 = N_G(\boldsymbol{d})$. We showed (see items 7-8 of the proof of Theorem 2 in [1]) that the only triality involutions normalizing G_0 are those of form $\check{r}_v$ where $\langle v \rangle$ runs through all +1-subspaces in $\cup_{i=1}^{4} V_i$ 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 $V_i = Aw_i$, $i = 1, \ldots, 4$, where $A = \mathbb{F}$ or $\mathbb{P}$ according as $\epsilon = -1$ or $\epsilon = +1$, the elements of $M(G_0)$ have form $\langle \lambda^j w_i \rangle$, where λ 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 λ, w_2, and w_3 have form (7.4), we see that $M(G_0)$ is a subloop of $(PSL_2(q), 2)$ and thus is not maximal unless $\epsilon = -1$ and $q = 2$, in which case $M(G_0) = (PSL_2(q), 2)$. Also, it is easy to see that $M(G_0)$ is the duplication of the dihedral group $\mathbb{D}_{\frac{2}{d}(q-\epsilon)}$ generated by $\langle \lambda \rangle$ and $\langle w_2 \rangle$.

We find $G_0 \cap D = N_D(\boldsymbol{d})$. Let $g \in G_0 \cap D$. Since $\mathbf{1}g = \mathbf{1}$, we have $Ag = A$ and thus g is A-(semi)linear. Then g preserves the A-sesquilinear form (5.3) on $\mathbb{O}$ and the A-trilinear form (5.4) on $A^\perp$. Therefore, $det(g) = 1$ and $g \in SL^\epsilon(A^\perp) : 2 = SL_3^\epsilon(q) : 2$. However, the normalizer of the decomposition $A^\perp = Aw_2 \oplus Aw_3 \oplus Aw_4$ in $SL^\epsilon(A^\perp)$ has form $(q-\epsilon)^2.S_3$ (see Proposition 4.2.9 in [9]). Consequently, $N_D(\boldsymbol{d}) = (q-\epsilon)^2.(S_3 \times 2)$. 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 $I_{\epsilon 2}$-subgroups of G are D-conjugate. The number of such subloops is $|D : G_0 \cap D| = \frac{1}{12}q^6(q^4 + q^2 + 1)(q + \epsilon)^2$.

8. G_0 is an I_{+4}-subgroup. Let $q \geqslant 3$. An *I_{+4}-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 $l_1, l_2 \in \mathcal{L}(V_0 \oplus V_1)$, it follows that both $l_1 g$ and $l_2 g$ are either in V_0 or in V_1 (otherwise, $\langle l_1 g, l_2 g \rangle = V_i g$ 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 (23.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 $M(G_0) \cong (PSL_2(q), 2)$.

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

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

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 $AB \cong (SL_2(q) \circ SL_2(q)).d$. By Table 4 this subgroup is maximal in D provided $q \geqslant 3$. Hence, in this case, $G_0 \cap D = AB$ and $|G_0 : G_0 \cap D| = \frac{4}{d^2} q^4(q^2-1)^4 / q^2(q^2-1)^2 = \frac{4}{d^2} q^2(q^2-1)^2 = |M(G_0)|^2$. 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 $|D : G_0 \cap D| = q^4(q^4 + q^2 + 1)$.

9. G_0 is a G_2^1-subgroup. A *G_2^1-subgroup* is a subgroup G_0 of G isomorphic to $G_2(q)$ and such that $GN_{GS}(G_0) = GS$. 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 $M(G_0) = \langle 1 \rangle$ is the identity subloop of $M(q)$. The fact that $G_0 S$ 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 subloop arises in this case.

10-11. G_0 is a $P\Omega_8^+(q_0)$- or a $P\Omega_8^+(q_0).2^2$-subgroup. Suppose that $q = q_0^k$, with k prime. Let $H_0 \leqslant G$ and $\mathbb{O}_0 \leqslant \mathbb{O}$ 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 $\sigma = \check{r}_1$ 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 σ-invariant. Note that H_0 is generated by elements of the form $U_{\langle v \rangle}$, with $\langle v \rangle \in PSL(\mathbb{O}_0)$, and $U_{\langle w_1 \rangle} U_{\langle w_2 \rangle}$, with $\langle w_1 \rangle, \langle w_2 \rangle \in PGL(\mathbb{O}_0) \backslash PSL(\mathbb{O}_0)$. By (6.8), $U^{\rho}_{\langle v \rangle} = L_{\langle \overline{v} \rangle}$ and $(U_{\langle w_1 \rangle} U_{\langle w_2 \rangle})^{\rho} = L_{\langle \overline{w}_1 \rangle} L_{\langle \overline{w}_2 \rangle}$. Since $L_{\langle \overline{v} \rangle}, L_{\langle \overline{w}_1 \rangle} L_{\langle \overline{w}_2 \rangle} \in H_0$, it follows that H_0 is ρ-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 $G_0 = N_G(H_0) \cong \mathrm{InnDiag}(P\Omega_8^+(q_0))$, i.e. the group of inner-diagonal automorphisms of $P\Omega_8^+(q_0)$, see [5], Proposition 2.2.9. By Lemma 4 we see that all triality S_3-complements in $G_0 S$ are G_0-conjugate in view of the structure of $Aut(P\Omega_8^+(q_0))$. 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 $G_0 S / H_0 \cong S_4$ 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 $\check{b}$ and $\check{c}$, where

$$b = \mathrm{diag}(\mu, \mu, \mu, \mu, \mu^{-1}, \mu^{-1}, \mu^{-1}, \mu^{-1}),$$
$$c = \mathrm{diag}(\lambda^{-1}, 1, 1, 1, \lambda, 1, 1, 1)$$

written in the standard basis, with μ a non-square in F and $\lambda = \mu^2$. Note that λ is a non-square in F_{q_0}. By Corollary 18, $M(G_0) \cong (\langle 1 \rangle_F)^{G_0}$. Hence, $M(G_0)$ is isomorphic to the extension of $M(H_0) \cong PSL(\mathbb{O}_0)$ by $\langle 1 \rangle_F \check{b}$ and $\langle 1 \rangle_F \check{c}$. However,

$$\langle 1 \rangle_F \check{c} = \langle \lambda^{-1} e_1 + \lambda f_1 \rangle_F \in PSL(\mathbb{O}_0),$$
$$\langle 1 \rangle_F \check{b} = \langle \mu e_1 + \mu^{-1} f_1 \rangle_F = \langle \lambda e_1 + f_1 \rangle_F \in PGL(\mathbb{O}_0) \backslash PSL(\mathbb{O}_0).$$

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 $\check{W}_0$ 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 $G_0 = \check{W}_0$. 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 $M(2)$ of $M(q)$ 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 Corollary 1 in [1]). In view of D-conjugacy of all subloops $M(G_0)$ 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}-subgroup. By Lemma 22, the subloops $M(G_0)$ in all of the remaining cases are maximal (unless $q = 3$ and G_0 is an I_{+4}-subgroup) and thus column V of Table 5 holds. The other columns hold by the above discussion. ▲

References

[1] A. N. Grishkov, A. V. Zavarnitsine, Lagrange's theorem for Moufang loops, to appear in *Math. Proc. Camb. Phil. Soc.*

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

[3] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, A. I. Shirshov, Rings that are nearly associative, Pure and Applied Mathematics, 104. Academic Press, New York-London, 1982.

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

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

[6] R. H. Bruck, A survey of binary systems (Springer-Verlag, 1958).

[7] K. McCrimmon, Homotopes of alternative algebras, *Math. Ann.*, **191**, (1971), 253–262.

[8] Schellekens, G.J. On a hexagonic structure, I, *Indag. Math.*, **24**, (1962), 201–217.

[9] P. Kleidman, M. Liebeck, The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, 129. Cambridge etc.: Cambridge University Press. (1990).

[10] F. van der Blij, T.A. Springer, Octaves and triality, *Nieuw Arch. Wisk.* **8**, (3) 1960, 158–169.

[11] R. H. Dye, Some geometry of triality with applications to involutions of ceratain orthogonal groups, *Proc. London Math. Soc.* (3) **22**, 1971, 217–234.

[12] O. Chein, Moufang loops of small order, I, *Trans. Am. Math. Soc.* **188**, (1974), 31–51.

[13] A. N. Grishkov, M. L. Merlini Guiliani, A. V. Zavarnitsine, The maximal subloops of the simple Moufang loop of order 1080, to appear in *Acta Appl. Math.*

[14] N. Jacobson, Lie algebras, Intersci. Tracts in Pure and Appl. Math. 10. N.Y. and Lond.: Intersci. Publishers a Division of John Wiley and Sons. (1962).

[15] R. Brandl, W. Shi, The characterization of PSL$(2, q)$ by its element orders, *J. Algebra*, **163**, No.1, (1994), 109–114.

[16] H. S. M. Coxeter, Integral Cayley numbers, *Duke Math. J.*, **13**, (1946), 561-578.

[17] R. W. Carter, Simple groups of Lie type, Wiley Classics Library, New York: John Wiley & Sons, Inc.(1989).

[18] N. Bourbaki, Elements of mathematics. Lie groups and Lie algebras. Chapters 4–6, Berlin: Springer (2002).

[19] V. A. Vasil'ev, V. D. Mazurov, Minimal permutation representations of finite simple orthogonal groups. *Algebra and Logic*, **33**, N 6 (1994), 337-350; translation from *Algebra i Logika*, **33**, N 6 (1994), 603-627.

[20] G.P. Nagy, P. Vojtěchovský, Automorphism groups of simple Moufang loops over perfect fields, *Math. Proc. Camb. Phil. Soc.*, **135**, (2003), 193–197.

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

[22] B. N. Cooperstein, Maximal subgroups of $G_2(2^n)$, *J. Algebra*, **70**, (1981), 23–36.

[23] T. A. Springer, F. D. Veldkamp, Octonions, Jordan algebras and exceptional groups, Springer Monographs in Mathematics. Berlin: Springer. viii, (2000).

[24] R. Steinberg, Lectures on Chevalley groups, Notes prepared by John Faulkner and Robert Wilson. Yale University, New Haven, Conn., 1968.

TRABALHOS DO DEPARTAMENTO DE MATEMÁTICA

TÍTULOS PUBLICADOS

2003-01 COELHO, F.U. and LANZILOTTA, M.A. Weakly shod algebras. 28p.

2003-02 GREEN, E.L., MARCOS, E. and ZHANG, P. Koszul modules and modules with linear presentations. 26p.

2003-03 KOSZMIDER, P. Banach spaces of continuous functions with few operators. 31p.

2003-04 GORODSKI, C. Polar actions on compact symmetric spaces which admit a totally geodesic principal orbit. 11p.

2003-05 PEREIRA, A.L. Generic Hyperbolicity for the equilibria of the one-dimensional parabolic equation $u_t = (a(x)u_x)_x + f(u)$. 19p.

2003-06 COELHO, F.U. and PLATZECK, M.I. On the representation dimension of some classes of algebras. 16p.

2003-07 CHERNOUSOVA, Zh. T., DOKUCHAEV, M.A., KHIBINA, M.A., KIRICHENKO, V.V., MIROSHNICHENKO, S.G., ZHURAVLEV, V.N. Tiled orders over discrete valuation rings, finite Markov chains and partially ordered sets. II. 43p.

2003-08 ARAGONA, J., FERNANDEZ, R. and JURIAANS, S.O. A Discontinuous Colombeau Differential Calculus. 20p.

2003-09 OLIVEIRA, L.A.F., PEREIRA, A.L. and PEREIRA, M.C. Continuity of attractors for a reaction-diffusion problem with respect to variation of the domain. 22p.

2003-10 CHALOM, G., MARCOS, E., OLIVEIRA, P. Gröbner basis in algebras extended by loops. 10p.

2003-11 ASSEM, I., CASTONGUAY, D., MARCOS, E.N. and TREPODE, S. Quotients of incidence algebras and the Euler characteristic. 19p.

2003-12 KOSZMIDER, P. A space C(K) where all non-trivial complemented subspaces have big densities. 17p.

2003-13 ZAVARNITSINE, A.V. Weights of the irreducible $SL_3(q)$-modules in defining characteristic. 12p.

2003-14 MARCOS, E. N. and MARTÍNEZ-VILLA, R. The odd part of a N-Koszul algebra. 7p.

2003-15 FERREIRA, V.O., MURAKAMI, L.S.I. and PAQUES, A. A Hopf-Galois correspondence for free algebras. 12p.

2003-16 KOSZMIDER, P. On decompositions of Banach spaces of continuous functions on Mrówka's spaces. 10p.

2003-17 GREEN, E.L., MARCOS, E.N., MARTÍNEZ-VILLA, R. and ZHANG, P. D-Koszul Algebras. 26p.

2003-18 TAPIA, G. A. and BARBANTI, L. Um esquema de aproximação para equações de evolução. 20p.

2003-19 ASPERTI, A. C. and VILHENA, J. A. Björling problem for maximal surfaces in the Lorentz-Minkowski 4-dimensional space. 18p.

2003-20 GOODAIRE, E. G. and MILIES, C. P. Symmetric units in alternative loop rings. 9p.

2003-21 ALVARES, E. R. and COELHO, F. U. On translation quivers with weak sections. 10p.

2003-22 ALVARES, E.R. and COELHO, F.U. Embeddings of non-semiregular translation quivers in quivers of type $Z\Delta$. 23p.

2003-23 BALCERZAK, M., BARTOSZEWICZ, A. and KOSZMIDER, P. On Marczewski-Burstin representable algebras. 6p.

2003-24 DOKUCHAEV, M. and ZHUKAVETS, N. On finite degree partial representations of groups. 24p.

2003-25 GORODSKI, C. and PODESTÀ, F. Homogeneity rank of real representations of compact Lie groups. 13p.

2003-26 CASTONGUAY, D. Derived-tame blowing-up of tree algebras. 20p.

2003-27 GOODAIRE, E.G. and MILIES, C. P. When is a unit loop *f*-unitary? 18p.

2003-28 MARCOS, E.N., MARTÍNEZ-VILLA, R. and MARTINS, M.I.R. Hochschild Cohomology of skew group rings and invariants. 16p.

2003-29 CIBILS, C. and MARCOS, E.N. Skew category, Galois covering and smash product of a category over a ring. 21p.

2004-01 ASSEM, I., COELHO. F.U., LANZILOTTA, M., SMITH, D.and TREPODE, SONIA Algebras determined by their left and right parts. 34p.

2004-02 FUTORNY, V., MOLEV, A. and OVSIENKO, S. Harish-Chandra Modules for Yangians. 29p.

2004-03 COX, B. L. and FUTORNY, V. Intermediate Wakimoto modules for affine $sl(n+1, C)$. 35p.

2004-04 GRISHKOV, A. N. and ZAVARNITSINE, A. V. Maximal subloops of simple Moufang loops. 43p.

Nota: Os títulos publicados nos Relatórios Técnicos dos anos de 1980 a 2002 estão à disposição no Departamento de Matemática do IME-USP.
Cidade Universitária "Armando de Salles Oliveira"
Rua do Matão, 1010 - Cidade Universitária
Caixa Postal 66281 - CEP 05315-970