Journal of Algebra 321 (2009) 1813–1825

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Sylow's theorem for Moufang loops

Alexander N. Grishkov[a,∗,1], Andrei V. Zavarnitsine[b,∗∗,2]

[a] Departamento de Matemática, Universidade de São Paulo, Caixa Postal 66281, São Paulo-SP 05311-970, Brazil
[b] Sobolev Institute of Mathematics, pr. Koptyuga 4, Novosibirsk 630090, Russia

ARTICLE INFO

Article history:
Received 15 May 2006
Available online 29 January 2009
Communicated by Efim Zelmanov

Keywords:
Moufang loop
Sylow's theorem
Group with triality

ABSTRACT

For finite Moufang loops, we prove an analog of the first Sylow theorem giving a criterion for the existence of a p-Sylow subloop. We also find the maximal order of p-subloops in the Moufang loops that do not possess p-Sylow subloops.

1. Introduction

After a positive solution to the Lagrange problem for finite Moufang loops was given [8], proving an analog of Sylow's theorems has become an important problem in the theory of finite Moufang loops [7]. We should mention right away that an obvious obstruction to the precise analog of the first Sylow theorem about the existence of a p-Sylow subloop has been known for a long time: if $\mathrm{M}(q)$ is the finite simple Paige loop over a finite field $\boldsymbol{F}_q$ then the orders of elements of $\mathrm{M}(q)$ divide $q(q^2-1)$, whereas the order of $\mathrm{M}(q)$ is $\frac{1}{d}q^3(q^4-1)$, where $d=\gcd(2,q-1)$. Hence, for a prime p dividing $\frac{1}{d}(q^2+1)$, a p-Sylow subloop of $\mathrm{M}(q)$ does not exist; consequently, nor does it exist in any finite Moufang loop having a composition factor isomorphic to $\mathrm{M}(q)$.

The main result of the present paper asserts that this obstruction to the existence of a p-Sylow subloop is in fact the only one. Namely, if a composition series of a Moufang loop M contains no simple factors $\mathrm{M}(q)$ such that $p \mid \frac{1}{d}(q^2+1)$, then M has a p-Sylow subloop. In this case, we call p a *Sylow prime* for M. In particular, every prime is Sylow for all solvable finite Moufang loops, i.e.,

[∗] Principal corresponding author.
[∗∗] Corresponding author.
E-mail addresses: grishkov@ime.usp.br (A.N. Grishkov), zav@math.nsc.ru (A.V. Zavarnitsine).

[1] Supported by FAPESP and CNPq, Brazil.
[2] Supported by FAPESP, Brazil; RFBR (grant No. 05-01-00797) and SB RAS (grant No. 29 for junior scientists and Integration Project 2006.1.2), Russia.

0021-8693/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2008.08.035

a p-Sylow subloop exists in this case for every p. We note that this result for Moufang loops of odd order (in fact, a stronger result about the existence of Hall π-subloops) was proved in [5].

Many major results about finite Moufang loops were proved based on the correspondence between Moufang loops and groups with triality [4]. This paper is not an exception. Clearly, the existence of a p-Sylow subloop is related to the existence of an S-invariant subgroup in a corresponding group G with triality S. Unfortunately, even when the above obstruction to the existence of a p-Sylow subloop in M is absent (which is always the case, for example, when $p = 2$ or 3), one cannot guarantee existence in G of an S-invariant p-Sylow subgroup. We therefore prove only that G possesses a sufficiently large S-invariant p-subgroup whose corresponding p-subloop in M is p-Sylow.

A Moufang loop M may still have nontrivial p-subloops even when p is not a Sylow prime for M. The order of such a p-subloop is obviously bounded by the product of the orders of p-Sylow subloops of the composition factor of M for which p is Sylow. In the last section, we show that this bound is actually achieved for all finite Moufang loops M. We call such p-subloops of maximal order *quasi-p-Sylow*. In this way, Sylow's theorem can be reformulated as follows:

Theorem A. *Every finite Moufang loop has a quasi-p-Sylow subloop for all primes p.*

The proof of this result uses the following important structural theorem (see Theorem 3 in Section 5) for Moufang loops:

Theorem B. *Every finite Moufang loop M contains a uniquely determined normal series*

$$1 \leqslant \mathrm{Gr}(M) \leqslant M_0 \leqslant M$$

such that M/M_0 is an elementary abelian 2*-group, $M_0/\operatorname{Gr}(M)$ is the direct product of simple Paige loops* $\mathrm{M}(q)$ (*where q may vary*)*, the composition factors of* $\mathrm{Gr}(M)$ *are groups, and* $\mathrm{Gr}(M/\mathrm{Gr}(M)) = 1$.

Another interesting auxiliary fact that we obtain is that a nonassociative minimal normal subloop of a finite Moufang loop must necessarily be simple, see Theorem 3(i). This extends the well-known group-theoretic assertion that a minimal normal subgroup of a finite group is the direct product of isomorphic simple groups.

It is natural to conjecture that analogs of other two Sylow theorems, namely the embedding of p-subloops of M into a quasi-p-Sylow subloop and the conjugacy of quasi-p-Sylow subloops by (inner) automorphisms of M, are true for finite Moufang loops as well. As far as determining the number of quasi-p-Sylow subloops, at present we do not have a formulation of the corresponding conjecture for lack of sufficient experimental data.

2. Preliminaries

All loops we consider are finite. If x, y are elements of a group G then $x^y = y^{-1}xy$, $x^{-y} = (x^{-1})^y$, $[x, y] = x^{-1}x^y$. $Z(G)$ is the center of G. If $\varphi \in \mathrm{Aut}(G)$ then x^φ is the image of x under φ. If n is an integer and p is a prime then the notation $p^k \parallel n$ for $k \geqslant 0$ means that $p^k \mid n$ and $p^{k+1} \nmid n$. For natural numbers m, n, we write (m, n) for $\gcd(m, n)$.

A loop M is called a *Moufang loop* if $xy \cdot zx = (x \cdot yz)x$ for all $x, y, z \in M$. For $x, y, z \in M$ define the *commutator* $[\![x, y]\!]$ by $xy = yx \cdot [\![x, y]\!]$. The *nucleus* $\mathrm{Nuc}(M)$ of a Moufang loop M is the set $\{a \in M \mid a \cdot xy = ax \cdot y \ \forall x, y \in M\}$. For basic properties of Moufang loops, see [1].

To arbitrary elements x, y of a Moufang loop M, there are associated bijections L_x, R_x, T_x, $L_{x,y}$, $R_{x,y}$ of M defined as follows:

$$yL_x = xy, \qquad yR_x = yx \quad \text{for all } y \in M;$$
$$T_x = L_x^{-1}R_x, \qquad L_{x,y} = L_xL_yL_{yx}^{-1}, \qquad R_{x,y} = R_xR_yR_{xy}^{-1}. \tag{1}$$

The *multiplication group* $\mathrm{Mlt}(M)$ of M is the group of permutations of M generated by L_x and R_x for all $x \in M$, and the *inner mapping group* $\mathfrak{I}(M)$ is the subgroup of $\mathrm{Mlt}(M)$ generated by T_x and $R_{x,y}$ for all x, y in M.

A *pseudoautomorphism* of a Moufang loop M is a bijection $A : M \to M$ with the property that there exists an element $a \in M$ such that

$$xA(yA \cdot a) = (x \cdot y)A \cdot a \quad \text{for all } x, y \in M.$$

Such an element a is called a *right companion* of A. Denote by $\mathrm{PsAut}(M)$ the group formed by all pairs (A, a), where A is a pseudoautomorphism of M with right companion a, with respect to the operation $(A,a)(B,b) = (AB, aB \cdot b)$. Denote by $\mathrm{PsInn}(M)$ the subgroup of $\mathrm{PsAut}(M)$ generated by the elements (T_x, x^{-3}) and $(R_{x,y}, [\![x, y]\!])$ for all x, y in M (such elements are in $\mathrm{PsAut}(M)$ by [1, Lemma VII.2.2]).

By [13], the only finite simple nonassociative Moufang loops are the Paige loops $\mathrm{M}(q)$ which exist for every finite field $\boldsymbol{F}_q$. The order of $\mathrm{M}(q)$ is $\frac{1}{d}q^3(q^4-1)$, where $d = (2, q-1)$, and is the product of two coprime numbers $q^3(q^2-1)$ and $\frac{1}{d}(q^2+1)$.

Let M be a Moufang loop and let p be a prime. M is a *p-loop* if the order of every element of M is a power of p (for Moufang loops, this is equivalent to the condition that $|M|$ be a power of p). A *p-Sylow subloop* of M is a subloop of order p^k, where $p^k \parallel |M|$, $k \geqslant 0$. We denote by $\mathrm{Syl}_p(M)$ the set of all p-Sylow subloops of M. The fact that $\mathrm{Syl}_p(M)$ can be empty for p dividing $|M|$ was observed long ago. For example, the simple Paige loop $\mathrm{M}(2)$ of order 120 does not have elements of order 5. The classification [9] of maximal subloops of $\mathrm{M}(q)$ implies the following assertion:

Lemma 1. *If $p \nmid \frac{1}{d}(q^2+1)$ then $\mathrm{Syl}_p(\mathrm{M}(q)) \neq \emptyset$. If $p \mid \frac{1}{d}(q^2+1)$ then $\mathrm{M}(q)$ does not have elements of order p; in particular, $\mathrm{Syl}_p(\mathrm{M}(q)) = \emptyset$ in this case.*

Proof. First, suppose that q is a power of p. Consider a maximal subloop of $\mathrm{M}(q)$ of shape $q^2 \colon \mathrm{PSL}_2(q)$ (i.e. a split extension of a normal elementary abelian subgroup order q^2 by the simple group $\mathrm{PSL}_2(q)$). This subloop obviously contains a subloop of order q^3 which is therefore p-Sylow in $\mathrm{M}(q)$.

If $p \mid q^2-1$ then consider a maximal subloop of type $M(\mathrm{PSL}_2(q), 2)$ (i.e. a loop with a normal subgroup $\mathrm{PSL}_2(q)$ of index 2 constructed by the Chein duplication process [2, Theorem 1]). Then, obviously, $\mathrm{Syl}_p(\mathrm{PSL}_2(q)) \subseteq \mathrm{Syl}_p(\mathrm{M}(q))$ whenever p is odd, and $M(S, 2) \in \mathrm{Syl}_2(\mathrm{M}(q))$ for every $S \in \mathrm{Syl}_2(\mathrm{PSL}_2(q))$.

If $p \mid \frac{1}{d}(q^2+1)$ then it can be easily seen by induction that every maximal subloop of $\mathrm{M}(q)$ either has order coprime with p, or contains no elements of order p. □

Note that we will give another proof (see Corollary 2 below) of the existence of a p-Sylow subloop in $\mathrm{M}(q)$ which does not use the classification [9]. However, the explicit structure of the Sylow subloops of $\mathrm{M}(q)$ is best seen from the proof of Lemma 1 above.

Lemma 1 also shows that there is an obstruction to the existence of a p-Sylow subloop in an arbitrary finite Moufang loop M having a composition factor $\mathrm{M}(q)$ with $\frac{1}{d}(q^2+1)$ divisible by p.

Definition. Let M be a Moufang loop. A prime p is called a *Sylow prime for M* if, for every composition factor of M that is isomorphic to $\mathrm{M}(q)$ for some q, we have $p \nmid \frac{q^2+1}{(2,q-1)}$.

Obviously, p is a Sylow prime for M if and only if it is such for all composition factors of M. We can now state the main theorem.

Theorem 1 *(Sylow's theorem). Let M be a finite Moufang loop and let p be a prime. Then M contains a p-Sylow subloop if and only if p is a Sylow prime for M.*

Before proving this theorem, we will require some facts about groups with triality which are introduced in the next section. As an important corollary to Sylow's theorem, we obtain the following assertion:

Corollary 1.

(i) *Every Moufang loop has a* 2*-Sylow and a* 3*-Sylow subloop.*
(ii) *If all composition factors of a Moufang loop M are groups then M has a p-Sylow subloop for all primes p.*

Proof. (i) The primes 2 and 3 are Sylow for every loop, since $\frac{q^2+1}{(2,q-1)}$ is coprime with 6 for all prime powers q.

(ii) If M is as stated then all primes are Sylow for M by definition. □

3. Groups with triality

A group G possessing automorphisms ρ and σ that satisfy $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ is called a *group with triality $\langle\rho, \sigma\rangle$* if

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

for every x in G, where $[x,\sigma] = x^{-1}x^{\sigma}$. We henceforth denote $S = \langle\sigma, \rho\rangle$. Obviously, S is a homomorphic image of the symmetric group S_3 of degree 3. (Strictly speaking, we have fixed a homomorphism $\gamma : S_3 \to \mathrm{Aut}(G)$ and then identified the generators ρ and σ of S_3 with their images under γ to simplify the notation. We thus implicitly consider G as a *group with operators* S_3 in the sense of [12, §15].) It should be noted that the identity (2) does not depend on a particular choice of the generators ρ and σ [4].

Let G be a group with triality S. Put $M = \{[x,\sigma] \mid x \in G\}$ and $H = C_G(\sigma)$. Then M endowed with the multiplication

$$m \,.\, n = m^{-\rho} n m^{-\rho^2} \quad \text{for all } m, n \in M, \tag{3}$$

becomes a Moufang loop $(M, .)$ of order $|G : H|$. We denote this loop by $\mathcal{M}(G)$. Every Moufang loop can be obtained in this way from a suitable group with triality. Moreover, for every subloop $M_0 \leqslant \mathcal{M}(G)$, there exists an S-invariant subgroup G_0 of G (in brief, *S-subgroup*) such that $M_0 = \mathcal{M}(G_0)$. Any element of $\mathcal{M}(G)$ has the same order whether viewed as a group or loop element. For more details on this, see [8,10]. We observe that

$$m^{\sigma} = m^{-1} \in M \quad \text{for all } m \in M. \tag{4}$$

A homomorphism $\varphi : G_1 \to G_2$ of groups G_1 and G_2 with triality S is called an *S-homomorphism* if $\alpha\varphi = \varphi\alpha$ for all $\alpha \in S$. (Again, strictly speaking, we have fixed homomorphisms $\gamma_i : S_3 \to \mathrm{Aut}(G_i)$, $i = 1, 2$, and then required $(\alpha\gamma_1)\varphi = \varphi(\alpha\gamma_2)$ for all $\alpha \in S_3$ thus making φ an *operator homomorphism* from G_1 to G_2. This is clearly a morphism in the category of groups with triality.) Denote by $Z_S(G)$ the *S-center* of G, which is by definition the maximal normal S-subgroup of G on which S acts trivially.

Lemma 2. *Let G be a group with triality S and let $M = \mathcal{M}(G)$. Then*

(i) $[[G,S],S] = [G,S]$,
(ii) $Z_S(G/Z_S(G)) = 1$ *and* $Z_S(G) = C_G([G,S]S)$,
(iii) $[G,S]$ *is generated by* $M \cup M^{\rho}$,
(iv) *the elements* m, m^{ρ}, m^{ρ^2} *of G pairwise commute for all* $m \in M$,
(v) $m^{-\rho}nm^{-\rho^2} = n^{-\rho^2}mn^{-\rho}$ *for all* $m, n \in M$.

Proof. See [10, Lemmas 1 and 2]. □

Lemma 3. *Let G be a group with triality $S = \langle \sigma, \rho \rangle$ and let $M = \mathcal{M}(G)$. Then the semidirect product $G_0 = G \rtimes \langle \rho \rangle$ is a group with triality S if and only if M has exponent* 3.

Proof. For every $g \in G$, we have $(g\rho)^{-1}(g\rho)^{\sigma} = \rho^2 g^{-1} g^{\sigma} \rho^2$ and $(g\rho^2)^{-1}(g\rho^2)^{\sigma} = \rho g^{-1} g^{\sigma} \rho$. Put $m = g^{-1} g^{\sigma}$. Then

$$(\rho m \rho)(\rho m \rho)^{\rho}(\rho m \rho)^{\rho^2} = m^{\rho^2} m^{\rho} m = 1,$$
$$\big(\rho^2 m \rho^2\big)\big(\rho^2 m \rho^2\big)^{\rho}\big(\rho^2 m \rho^2\big)^{\rho^2} = \big(m^{\rho}\big)^3.$$

Hence, G_0 is a group with triality iff $m^3 = 1$ for all $m \in \mathcal{M}(G)$. □

Note that if $\mathcal{M}(G)$ has exponent 3 then $G \rtimes S$ is also a group with triality S (where S acts by inner automorphisms). However, in this case $\mathcal{M}(GS) = \mathcal{M}(G\langle\rho\rangle)$.

Given a Moufang loop M, there exists a universal group with triality $\mathcal{D}(M)$ introduced by Doro [4] which satisfies $\mathcal{M}(\mathcal{D}(M)) \cong M$, $[\mathcal{D}(M), S] = \mathcal{D}(M)$, and, if G is any group with triality such that $\mathcal{M}(G) \cong M$ and $G = [G, S]$, then there is an S-epimorphism $\tau : \mathcal{D}(M) \to G$. Denote $\mathcal{E}(M) \cong \mathcal{D}(M)/Z_S(\mathcal{D}(M))$. Then $\mathcal{M}(\mathcal{E}(M)) \cong M$.

A nontrivial group G with triality is said to be *S-simple* if it has no proper S-homomorphic images or, equivalently, contains no proper normal S-subgroups.

Lemma 4. *Every finite S-simple group is S-isomorphic to one of the following S-simple groups*:

(i) *A finite simple group G with trivial S-action. In this case, $\mathcal{M}(G)$ is the trivial loop*;
(ii) $G = \langle a \mid a^3 = 1\rangle \cong \mathbb{Z}_3$, $a^{\rho} = a$, $a^{\sigma} = a^{-1}$. *In this case,* $\mathcal{M}(G) \cong \mathbb{Z}_3$;
(iii) $G = \langle a, b \mid a^p = b^p = [a,b] = 1\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$, $p \neq 3$ *is a prime,* $a^{\rho} = b$, $b^{\rho} = a^{-1}b^{-1}$, $a^{\sigma} = b$, $b^{\sigma} = a$. *In this case,* $\mathcal{M}(G) \cong \mathbb{Z}_p$;
(iv) $G = V_1 \times V_2 \times V_3$, $\alpha_i : V \to V_i$, $i = 1,2,3$, *are isomorphisms, V is a finite nonabelian simple group,* $(v_1, v_2, v_3)^{\sigma} = (v_2, v_1, v_3)$, $(v_1, v_2, v_3)^{\rho} = (v_3, v_1, v_2)$. *In this case,* $\mathcal{M}(G) \cong V$;
(v) $G \cong P\Omega_8^+(q)$, *S is the group of graph automorphisms of G. In this case,* $\mathcal{M}(G) \cong \mathrm{M}(q)$ *is the simple Paige loop.*

Proof. See [4,14]. □

Let F be a field. An FS-module V is called a *triality module* if V is a group with triality S. The representations $\varphi_i^{(\chi)}$ of S corresponding to the indecomposable FS-modules $V_i^{(\chi)}$ are shown in Table 1. They depend on whether the characteristic χ of F is 2, 3, or otherwise. We may assume F to be a prime field, since the decomposition field of S is prime in any characteristic [3]. If a module is a triality module, we put '✓' in the last column, and '–', otherwise.

Lemma 5. *Table* 1 *holds.*

Proof. The indecomposable FS-modules are well known and can be readily determined, for example, using [3, §§63, 64]. Namely, if $\chi \neq 2, 3$ then every indecomposable FS-module is irreducible by Maschke's theorem. If $\chi = 3$ then there are exactly 6 indecomposable FS-modules by [3, Theorem (64.6)] and the ones shown in Table 1 are easily seen to be indecomposable and pairwise nonisomorphic. If $\chi = 2$ then the indecomposable modules are the components of the regular and natural permutation FS-modules by [3, Theorem (63.8)].

The triality of a module V is equivalent to the condition that the element $(\sigma - 1)(1 + \rho + \rho^2)$ of FS annihilates V, which is directly verified in each case. □

Lemma 6. *Let G be an S-simple group with triality. Let p be a Sylow prime for $\mathcal{M}(G)$. Then G has a p-Sylow S-subgroup.*

Table 1
Indecomposable S_3-modules.

χ	V	$\dim V$	φ	$(12)\varphi$	$(123)\varphi$	Triality
$\neq 2, 3$	$V_1^{(0)}$	1	$\varphi_1^{(0)}$	1	1	✓
	$V_2^{(0)}$	1	$\varphi_2^{(0)}$	-1	1	–
	$V_3^{(0)}$	2	$\varphi_3^{(0)}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$	✓
2	$V_1^{(2)}$	1	$\varphi_1^{(2)}$	1	1	✓
	$V_2^{(2)}$	2	$\varphi_2^{(2)}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$	✓
	$V_3^{(2)}$	2	$\varphi_3^{(2)}$	$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	–
3	$V_1^{(3)}$	1	$\varphi_1^{(3)}$	1	1	✓
	$V_2^{(3)}$	1	$\varphi_2^{(3)}$	-1	1	✓
	$V_3^{(3)}$	2	$\varphi_3^{(3)}$	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	✓
	$V_4^{(3)}$	2	$\varphi_4^{(3)}$	$\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	✓
	$V_5^{(3)}$	3	$\varphi_5^{(3)}$	$\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1 & 1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}$	✓
	$V_6^{(3)}$	3	$\varphi_6^{(3)}$	$\begin{pmatrix}-1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix}$	$\begin{pmatrix}1 & -1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}$	–

Proof. We analyze the cases (i)–(v) of Lemma 4. If G is as in cases (i)–(iii), the claim readily follows. Let case (iv) hold. Then, for any $P \in \mathrm{Syl}_p(V)$, the group $P_1 \times P_2 \times P_3$ is the required p-Sylow S-subgroup of G, where $P_i = \alpha_i(P)$, $i = 1, 2, 3$. Suppose that $G \cong P\Omega_8^+(q)$ as in case (v) and S is the group of graph automorphisms of G. We will use the structure of some S-subgroups of G (for details, see [11]). We have $|G| = \frac{1}{d^2}q^{12}(q^6-1)(q^4-1)^2(q^2-1) = n_1n_2n_3$, where the integers

$$n_1 = \frac{3}{(3,q)}q^{12}\big(q^2-1\big)^4, \qquad n_2 = \frac{(3,q)(q^2+q+1)(q^2-q+1)}{3}, \qquad n_3 = \left(\frac{q^2+1}{d}\right)^2$$

are pairwise coprime. By hypothesis, $p \mid n_1n_2$. If $p \mid n_2$ then $\mathrm{Syl}_p(C_G(S)) \subseteq \mathrm{Syl}_p(G)$, since $C_G(S) \cong G_2(q)$ and n_2 divides $|G_2(q)| = q^6(q^6-1)(q^2-1)$. Hence, any subgroup in $\mathrm{Syl}_p(C_G(S))$ is the required one.

Therefore, we may assume that $p \mid n_1$. If $p \mid q$ then we consider an S-invariant parabolic subgroup R_{s2} of G (in the notation of [11]) of order $\frac{1}{d^2}q^{12}(q-1)^4(q+1)^3$. It has the following S-invariant structure $R_{s2} = q^9 \rtimes (\mathrm{SL}_2(q) \circ \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q))\,.\,(q-1)$ with S naturally permuting the three factors $\mathrm{SL}_2(q)$, where $\circ$ denotes the central product. The group $\mathrm{SL}_2(q) \circ \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q)$ has an obvious p-Sylow S-subgroup whose preimage in R_{s2} is the required subgroup.

If $p \nmid q$ and $p \neq 3$ then consider an S-subgroup I_{+4} of order $\frac{4}{d^2}q^4(q^2-1)^4$. It has the structure $(\mathrm{SL}_2(q) \circ \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q))\,.\,d \rtimes K$, where $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K \rtimes S \cong S_4$ naturally permutes the four factors $\mathrm{SL}_2(q)$. It is easy to see that this group contains a p-Sylow S-subgroup.

Finally, if $p \nmid q$ and $p = 3$ then let $q \equiv \varepsilon(3)$, $\varepsilon = \pm 1$. The required 3-Sylow subgroup is inside an S-subgroup $I_{\varepsilon 2}$ of order $\frac{192}{d^2}(q-\varepsilon)^4$. To see this, consider an $\varepsilon 2$-decomposition of the Cayley algebra $\mathbb{O}(q) = V_1 \oplus \dots \oplus V_4$ which is also a $\mathbb{Z}_2 \times \mathbb{Z}_2$-grading with $\mathbf{1} \in V_1$, see [9, Section 4]. Let R be the centralizer of this decomposition in $\Omega_8^+(q)$ extended by the 4-group $\langle (12)(34), (13)(24)\rangle$ of permutations of the subspaces $\{V_i\}$, $i = 1, \dots, 4$. This group has the following structure $R = (\mathbb{Z}_{\frac{1}{d}(q-1)})^4\,.\,d^3\,.\,2^3\,.\,2^2$. In particular, the 3-Sylow subgroup of R is characteristic. Take the group $T = \langle (23), (34)\rangle \cong S_3$ of permutations of $\{V_i\}$, $i = 2, 3, 4$, which acts identically on V_1 and induces automorphisms of $\mathbb{O}(q)$. Then the group $I_{\varepsilon 2} = \overline{R} \rtimes \overline{T}$ is the image in $P\Omega_8^+(q)$ of $R \rtimes T \subseteq \Omega_8^+(q)$. It is S-invariant with S centralizing $\overline{T}$ (because T is a group of automorphisms of $\mathbb{O}(q)$). It is now clear that the 3-Sylow subgroup $O_3(\overline{R}) \rtimes \langle \overline{(2,3,4)} \rangle$ of $I_{\varepsilon 2}$ is S-invariant. □

Lemma 7. *Let G be a group with triality $S = \langle \rho, \sigma \rangle$ and let $\mathcal{M}(G) = \{[g,\sigma] \mid g \in G\} = (M, .)$ be the corresponding Moufang loop. Then, for every subloop $P \leqslant \mathcal{M}(G)$, the group $Q = \langle P \cup P^{\rho} \rangle$ is an S-subgroup of G such that $\mathcal{M}(Q) = P$ and $[Q, S] = Q$.*

Proof. By [8, Theorem 1], Q is an S-subgroup and $\mathcal{M}(Q) = P$. By Lemma 2, $[Q, S]$ is the S-subgroup of G generated by P. Hence, we have $Q \subseteq [Q, S]$. □

Lemma 8. *Let M be a finite Moufang p-loop. Then*

(i) $\mathrm{PsInn}(M)$ *is a p-group;*
(ii) *Any group with triality G such that $\mathcal{M}(G) \cong M$ and $[G, S] = G$ is a p-group.*

Proof. (i) The kernel of the natural epimorphism $\lambda : \mathrm{PsInn}(M) \to \mathcal{I}(M)$ which acts by $\lambda : (A, a) \mapsto A$ is a subgroup of $\mathrm{Nuc}(M)$ hence is a p-group. The group $\mathcal{I}(M)$ is a subgroup of $\mathrm{Mlt}(M)$ which is a p-group by [1, Lemma VI.2.2] and [5, Theorem 4].

(ii) Let G be as stated. Then G is finite, since it is a quotient of the finite group $\mathcal{D}(M)$, see [4, Corollary 3]. We have $G/Z_S(G) \cong \mathcal{E}(M)$ and $|\mathcal{E}(M)| = |\mathrm{PsInn}(M)| \cdot |M|$ (see [10]) is a power of p by (i). Hence, it remains to prove that $K = Z_S(G)$ is a p-group. Let $P \in \mathrm{Syl}_p(G)$. We have $G = O_{p'}(K) \times P$, since K is a central subgroup of G. The condition $[G, S] = G$ now implies $O_{p'}(K) = 1$. □

In the following lemma, for an integer n and a prime p, we denote by n_p the maximal power of p dividing n.

Lemma 9. *Let G be a group with triality $S = \langle \rho, \sigma \rangle$, let $M = \mathcal{M}(G)$, and let p be a prime.*

(i) *If $N \leqslant G$ is an S-subgroup containing a p-Sylow subgroup of G then $|\mathcal{M}(N)|_p = |M|_p$.*
(ii) *If $P \in \mathrm{Syl}_p(G)$ is S-invariant then $\mathcal{M}(P) \in \mathrm{Syl}_p(M)$.*

Proof. (i) Let $H = C_G(\sigma)$. We have $|\mathcal{M}(N)| = |N|/|N \cap H|$, and $|M| = |G|/|H|$. By Lagrange's theorem [8], $|M|/|\mathcal{M}(N)| = |G|/|NH|$ is an integer. However, $|G|_p = |N|_p$ divides $|N|$ which, in turn, divides $|NH|$. Hence $|M : \mathcal{M}(N)|$ is coprime with p.

(ii) Since $\mathcal{M}(P)$ is a p-loop and $|M : \mathcal{M}(P)|$ is coprime with p by (i), it follows that $\mathcal{M}(P) \in \mathrm{Syl}_p(M)$. □

As a consequence, we have an alternative proof independent of the classification [9] of the following assertion (cf. Lemma 1 above):

Corollary 2. *If p is a Sylow prime for* $\mathrm{M}(q)$ *then* $\mathrm{Syl}_p(\mathrm{M}(q)) \neq \emptyset$.

Proof. We have $\mathrm{M}(q) = \mathcal{M}(G)$, where $G = P\Omega_8^+(q)$ is S-simple. By Lemma 6, G contains a p-Sylow S-subgroup. The claim follows by Lemma 9(ii). □

Lemma 10. *Let $G = VP$ be a group with triality S such that P is a p-group, $V \trianglelefteq G$, $p \nmid |V|$. Suppose that $\mathcal{M}(\overline{P})$ is generated by at most* 2 *elements, where $\overline{P} = G/P$ satisfies $[\overline{P}, S] = \overline{P}$. Then G has a p-Sylow S-subgroup.*

Proof. Denote $M = \mathcal{M}(G)$. Let $\{m_i\}_{i \in I}$ generate M modulo $W = \mathcal{M}(V)$. By hypothesis, we may assume $|I| \leqslant 2$. In particular, $N = \langle \{m_i\}_{i \in I} \rangle$ is a group (since Moufang loops are diassociative) and $M = WN$. Hence, any $R \in \mathrm{Syl}_p(N)$ is in $\mathrm{Syl}_p(M)$. By Lemma 7, $Q = \langle R \cup R^{\rho} \rangle$ is an S-subgroup of G such that

$\mathcal{M}(Q) = R$ and $[Q, S] = Q$. Hence $QV/V = \overline{P}$ in view of $[\overline{P}, S] = \overline{P}$. By Lemma 8, Q is the required p-Sylow S-subgroup. □

4. Proof of the theorem

We are going to prove the following extended form of Theorem 1:

Theorem 2. *Let M be a finite Moufang loop and let p be a prime. Let G be a group with triality such that $\mathcal{M}(G) = M$. Then the following conditions are equivalent*:

(i) *M has a p-Sylow subloop,*
(ii) *p is a Sylow prime for M,*
(iii) *G has an S-invariant p-subgroup Q such that $\mathcal{M}(Q) \in \mathrm{Syl}_p(M)$.*

Proof. Let $k \geqslant 0$ be such that $p^k \parallel |M|$.

(i) ⇒ (ii). Suppose that M possesses a p-Sylow subloop P. We prove by induction on the length of a composition series of M that p is a Sylow prime for M. If M is simple, this follows from Lemma 1. Let N be a proper normal subloop of M. It suffices to show that p is a Sylow prime for both N and $\overline{M} = M/N$. Note that $P \cap N$ is a p-subloop of N and $\overline{P} = \langle P, N\rangle/N$ is a p-subloop of $\overline{M}$ by

$$\frac{\langle P, N\rangle}{N} \cong \frac{P}{P \cap N}, \tag{5}$$

see [1, Theorem IV.1.5]. By Lagrange's theorem [8], $|P|$ divides $|\langle P, N\rangle|$ which in turn divides $|M|$. Hence (5) also implies that the integers

$$\frac{|N|}{|P \cap N|} = \frac{|\langle P, N\rangle|}{|P|}, \qquad \frac{|\overline{M}|}{|\overline{P}|} = \frac{|M|}{|\langle P, N\rangle|}$$

are coprime with p. It follows that $P \cap N \in \mathrm{Syl}_p(N)$ and $\overline{P} \in \mathrm{Syl}_p(\overline{M})$. By induction, p is a Sylow prime for both N and $\overline{M}$.

(ii) ⇒ (iii). We now suppose that p is a Sylow prime for $M = \mathcal{M}(G)$. Proceed by induction on $|M|$.

If $Z_S(G) \neq 1$ then consider $G_0 = G/Z_S(G)$. This group satisfies $Z_S(G_0) = 1$ and $\mathcal{M}(G_0) = M$. If we show that P_0 is an S-invariant p-subgroup of G_0 such that $\mathcal{M}(P_0) \in \mathrm{Syl}_p(M)$ then the preimage P of P_0 in G also satisfies $\mathcal{M}(P) \in \mathrm{Syl}_p(M)$. If P is not a p-group then we take $[P, S]$ which is a p-group by Lemma 8(ii) and $\mathcal{M}([P, S]) = \mathcal{M}(P)$.

Hence, we may assume that $Z_S(G) = 1$. Clearly, we may also assume that $[G, S] = G$. Take a minimal normal S-subgroup V of G. Then V is characteristically simple see [6, Chapter 2, Theorem 1.5]. Two cases are possible:

(1) $p \mid |V|$. Then we may assume that V is nonabelian (otherwise V is a p-group and we apply induction for G/V, which is possible, since p is a Sylow prime for $\mathcal{M}(G/V)$ and $|\mathcal{M}(G/V)| < |M|$). We have $V = V_1 \times \cdots \times V_s$ is the product of isomorphic nonabelian simple groups V_i's. Since p is Sylow for $\mathcal{M}(V)$ and V is a direct product of S-simple groups, it follows by Lemma 6 that V has a p-Sylow S-subgroup W.

By assumption $W \neq 1$. We have $G = VN$, where $N = N_G(W)$ is S-invariant. Observe that N contains a p-Sylow subgroup of G. Moreover $N < G$, since $W \ntrianglelefteq V$; and $\mathcal{M}(N) < M$, since $[G, S] = G$. Also note that p is Sylow for $\mathcal{M}(N)$, since $W \trianglelefteqslant N \cap V \trianglelefteqslant N$ is an S-invariant series for N and W is a p-group, $(N \cap V)/W$ is a p'-group, and $N/(N \cap V) \cong G/V$. By induction, there exists a p-subgroup P in N such that $\mathcal{M}(P) \in \mathrm{Syl}_p(\mathcal{M}(N))$. By Lemma 9(i), $\mathcal{M}(P) \in \mathrm{Syl}_p(M)$.

(2) $p \nmid |V|$. By induction, we may assume that $\overline{P} = G/V$ is a p-group. It is sufficient to show that G has a nontrivial S-invariant p-subgroup P_0 such that $\overline{P_0} = P_0V/V$ is normal in $\overline{P}$. Indeed, if such a subgroup exists then the condition $Z_S(G) = 1$ implies that either $\mathcal{M}(P_0) \neq 1$ or $P_0 \ntrianglelefteq G$. In both

cases we can use induction for N/P_0, where $N = N_G(P_0)$. This is because $|\mathcal{M}(N/P_0)| < |M|$ and p is Sylow for $\mathcal{M}(N/P_0)$, since N/P_0 is an extension of the p'-group $C_V(P_0)$ by the p-group $\overline{P}/\overline{P_0}$. By induction, N/P_0 contains an S-invariant p-subgroup $\overline{P_1}$ such that $\mathcal{M}(\overline{P_1}) \in \mathrm{Syl}_p(\mathcal{M}(N/P_0))$. Then the full preimage P_1 of $\overline{P_1}$ in N is the required S-subgroup, since $\mathcal{M}(P_1) \in \mathrm{Syl}_p(\mathcal{M}(N)) \subseteq \mathrm{Syl}_p(M)$.

Let $\overline{Z} = Z(\overline{P})$ and suppose that $\mathcal{M}(\overline{Z}) \neq 1$. The existence of P_0 in this case is easy. Take $z \in \mathcal{M}(G)$ such that $1 \neq \bar{z} \in \mathcal{M}(\overline{Z})$, where $\bar{z} = Vz$. The group $G_0 = \langle V, z, z^\rho \rangle$ satisfies the conditions of Lemma 10. We take P_0 to be a p-Sylow S-subgroup of G_0. Then $\overline{P_0} \trianglelefteq \overline{P}$ as a central subgroup of $\overline{P}$.

Suppose that $\mathcal{M}(\overline{Z}) = 1$. Then $\mathcal{M}(\overline{Z_1}) \neq 1$, where $\overline{Z_1}/\overline{Z} = Z(\overline{P}/\overline{Z})$, since otherwise we would have $\overline{Z}_1 \leqslant Z_S(\overline{P}) \leqslant \overline{Z}$ (the latter inclusion follows from $[\overline{P}, S] = \overline{P}$ and Lemma 2(ii)). Take $a \in \mathcal{M}(G)$ such that $1 \neq \bar{a} \in \mathcal{M}(\overline{Z_1})$ and set $A = \langle a, a^\rho \rangle$. Then A is an S-subgroup of G not contained in Z, where Z is the full preimage of $\overline{Z}$ in G.

The elementary abelian group $\overline{P}/\Phi(\overline{P})$ is the direct product $U_1 \times \cdots \times U_t$ of indecomposable triality $\boldsymbol{F}_p S$-modules U_i's. The condition $[\overline{P}, S] = \overline{P}$ implies that the U_i's are at most 2-dimensional and, depending on p, are isomorphic to one of the modules $V_3^{(0)}$, $V_2^{(2)}$, $V_2^{(3)}$, $V_4^{(3)}$ from Table 1. Moreover, we have $\mathcal{M}(U_i) = \langle u_i \rangle$ is cyclic of order p and $U_i = \langle u_i, u_i^\rho \rangle$ (observe that $u_i^\rho = u_i$ if $U_i \cong V_2^{(3)}$). Let w_i be corresponding preimages of u_i in $\mathcal{M}(G)$. Then G is generated modulo V by the S-subgroups $W_i = \langle w_i, w_i^\rho \rangle$. Since $Z_1 \geqslant A \nleqslant Z$, where Z_1 is the full preimage of $\overline{Z_1}$ in G, it follows that there exists i_0 such that $W = [A, W_{i_0}] \nleqslant V$. On the other hand, $W \leqslant Z$, since $A \leqslant Z_1$. Denote $G_0 = \langle V, A, W_{i_0} \rangle$ and $\overline{G_0} = G_0/V$. Then the S-subgroup G_0 satisfies the conditions of Lemma 10, since the images of a and w_{i_0} in $\overline{G_0}$ generate $\mathcal{M}(\overline{G_0})$ as a loop and $\overline{G_0}$ as an S-group (whence the condition $[\overline{G_0}, S] = \overline{G_0}$). Let P_1 be a p-Sylow S-subgroup of G_0. Put $P_0 = P_1 \cap Z$. It remains to observe that $P_0 \neq 1$, since $P_0 \cap WV = P_1 \cap WV \neq 1$ in view of $W \nleqslant V$.

(iii) ⇒ (i). Obvious. □

We note that in general it is not true that if G is a group with triality and p is Sylow for $\mathcal{M}(G)$ then G contains a p-Sylow S-subgroup. For example, let $G = S$ on which S acts by inner automorphisms. Then 2 is a Sylow prime for $\mathcal{M}(G) \cong \mathbb{Z}_3$, but G does not have a 2-Sylow S-subgroup.

5. The group-type radical of Moufang loops

A finite Moufang loop M is said to be a loop of *group type* if all composition factors of M are groups. For example, all solvable Moufang loops are loops of group type. It is clear that the normal subloop of M generated by two normal subloops of group type is again a loop of group type. Hence we have

Proposition 1. *Every finite Moufang loop has a unique maximal normal subloop of group type.*

We denote this maximal normal subloop of group type by $\mathrm{Gr}(M)$. It is obvious that $\mathrm{Gr}(M/\mathrm{Gr}(M)) = 1$, hence we call $\mathrm{Gr}(M)$ the *group-type radical* of M.

For q odd, the simple Paige loop $\mathrm{M}(q)$ has a two-fold extension isomorphic to the loop $\mathrm{PGL}(\mathbb{O}(q))$, where $\mathbb{O}(q)$ is the Cayley algebra over $\boldsymbol{F}_q$, see [9, Section 4]. We denote this extension by $\mathrm{M}(q)\,.\,2$. Also, we define

$$\widehat{\mathrm{M}(q)} = \begin{cases} \mathrm{M}(q)\,.\,2, & \text{if } q \text{ is odd,} \\ \mathrm{M}(q), & \text{if } q \text{ is even.} \end{cases}$$

It can be seen that the group $\mathrm{InnDiag}(P\Omega_8^+(q))$ of inner-diagonal automorphisms of $P\Omega_8^+(q)$ is a group with triality S corresponding to $\widehat{\mathrm{M}(q)}$, where S is the group of graph automorphisms of $P\Omega_8^+(q)$. It is known that the factor group

$$\mathrm{InnDiag}\big(P\Omega_8^+(q)\big)/P\Omega_8^+(q)$$

is trivial for q even and isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ for q odd. Moreover, in the latter case, S acts nontrivially on $\mathbb{Z}_2 \times \mathbb{Z}_2$ so that $\mathcal{M}(\mathbb{Z}_2 \times \mathbb{Z}_2) = \mathbb{Z}_2$, whence $|\widehat{\mathrm{M}(q)}| = 2|\mathrm{M}(q)|$.

The following assertion is the main result of this section (cf. Theorem B in the introduction):

Theorem 3. *Let M be a finite Moufang loop and let N be a minimal normal subloop of M. Then we have*

(i) *N is the direct product of isomorphic simple loops. Furthermore, if N is nonassociative then it is simple.*
(ii) *Suppose, additionally, that M satisfies $\mathrm{Gr}(M) = 1$. Then by* (i) *every minimal normal subloop of M is a simple Paige loop $\mathrm{M}(q)$ for some q. Denote $\mathrm{Soc}(M) = \prod \mathrm{M}(q)$ and $\widehat{\mathrm{Soc}(M)} = \prod \widehat{\mathrm{M}(q)}$, where both products are taken over all minimal normal subloops of M. Then*

$$\mathrm{Soc}(M) \trianglelefteqslant M \trianglelefteqslant \widehat{\mathrm{Soc}(M)}.$$

In particular, $M/\mathrm{Soc}(M)$ is an elementary abelian 2-group.

Proof. Suppose that M and N are as stated.

(i) Let G be a group with triality $S = \langle \rho, \sigma \rangle$ such that $\mathcal{M}(G) = M = \{x^{-1}x^{\sigma} \mid x \in G\}$, $[G, S] = G$, and let Q_0 be a minimal normal S-subgroup of G corresponding to N. Since Q_0 is characteristically simple, we have $Q_0 = Q_1 \times \cdots \times Q_n$, where Q_i, $1 \leqslant i \leqslant n$, are isomorphic simple groups. Note that we also have the decomposition $Q_0 = R_1 \times \cdots \times R_k$, where R_j, $1 \leqslant j \leqslant k$, are S-simple groups if Q_0 is nonabelian or indecomposable S-modules if Q_0 is abelian; moreover, $N = \mathcal{M}(Q_0) = \mathcal{M}(R_1) \times \cdots \times \mathcal{M}(R_k)$. If $Q_1 \ncong P\Omega_8^+(q)$ for any q then Lemmas 5 and 4 imply that all $\mathcal{M}(R_j)$'s are either trivial or isomorphic simple groups. Hence, we may assume that $Q_1 \cong P\Omega_8^+(q)$, with $q = p^m$, p a prime. We denote $I = \{i \mid Q_i^S = Q_i\}$. If either $I = \emptyset$ or $[Q_i, S] = 1$ for all $i \in I$ then each R_j is either an S-group from Lemma 4(iv) with $V_t = P\Omega_8^+(q)$, $t = 1, 2, 3$, or is isomorphic to $P\Omega_8^+(q)$ with trivial S-action. Hence, in this case, N is the direct product of several $P\Omega_8^+(q)$'s and the claim holds. Consequently, we may assume that $1 \in I$ and $\mathcal{M}(Q_1) = \mathrm{M}(q) \neq 1$. We prove that $n = 1$ in this case. Assume the contrary. Denote $K = N_G(Q_1)$. Observe that K is S-invariant. We have $K \neq G$, since otherwise Q_1 would be a normal S-subgroup contrary to the choice of Q_0. Note that we cannot have the inclusion $M \subseteq K$, since G is S-generated by M (i.e., $G = \langle \bigcup_{\tau \in S} M^{\tau} \rangle$, which follows from $[G, S] = G$ by Lemma 2(iii)). Hence, there exists $x \in M \setminus K$ such that $x^l \in K$ for a prime l. Let $y = x^{\rho}$. Then we have

$$x^{\sigma} = x^{-1}, \qquad y^{\rho} = x^{-1}y^{-1}, \qquad y^{\sigma} = xy, \qquad [x, y] = 1 \tag{6}$$

in view of (4) and Lemma 2(iv). Denote $Q_{(i,j)} = Q_1^{x^i y^j}$, $i, j \in \mathbb{Z}/l\mathbb{Z}$, $Q = Q_{(0,0)} = Q_1$. Suppose that $x^a y^b \in K$, then by (6) we have $(x^a y^b)^{\sigma} = x^{b-a} y^b \in K$ and $(x^a y^b)^{\rho} = x^{-b} y^{a-b} \in K$. Hence $3a \equiv 3b \equiv 0 \pmod{l}$.

I. $l > 3$. Then $a \equiv b \equiv 0 \pmod{l}$ and all groups $Q_{(i,j)}$ are different. By (6) we obtain

$$Q_{(i,j)}^{\sigma} = Q_{(j-i,j)}, \qquad Q_{(i,j)}^{\rho} = Q_{(-j,i-j)}. \tag{7}$$

Since Q_0 is a group with triality, the orbits of S on the set $\{Q_1, \ldots, Q_n\}$ are all of size 1 or 3. Hence by (7) the set

$$\bigl\{(i, j), (j - i, j), (-j, i - j), (i, i - j), (-j, -i), (j - i, -i)\bigr\}$$

has 3 elements or less for all $i, j \in \mathbb{Z}/l\mathbb{Z}$. However, this is possible only in the case $l = 2$.

II. $l = 3$. Since $x^3, y^3 \in K$ we have by (6)

$$\big(Q^{xy^{-1}}\big)^{\rho} = Q^{xy^2} = \big(Q^{y^3}\big)^{xy^{-1}} = Q^{xy^{-1}},$$
$$\big(Q^{xy^{-1}}\big)^{\sigma} = Q^{x^{-2}y^{-1}} = \big(Q^{x^{-3}}\big)^{xy^{-1}} = Q^{xy^{-1}}.$$

Similarly, we can prove that the set $X = \{Q^x, Q^{x^2}, Q^y, Q^{y^2}, Q^{xy}, Q^{x^2y^2}\}$ is an S-orbit. Since $|X| > 1$ and Q is a simple group, we have $|X| = 3$. If $Q^x = Q^{y^2}$, an application of ρ gives $Q^y = Q^{xy}$, which implies $Q^x = Q$ in contradiction with the choose of x. The cases $Q^x = Q^{x^2}$ or $Q^x = Q^{xy}$ are treated similarly. In the other cases: $Q^x = Q^y$, $Q^x = Q^{x^2y^2}$ we have $|X| = 2$, a contradiction.

III. $l = 2$. Then the subgroup $Q \times Q^x \times Q^y \times Q^{xy}$ is S-invariant and

$$\big(Q^x\big)^{\sigma} = Q^x, \qquad \big(Q^y\big)^{\sigma} = Q^{xy}, \qquad \big(Q^x\big)^{\rho} = Q^y, \qquad \big(Q^y\big)^{\rho} = Q^{xy}, \qquad \big(Q^{xy}\big)^{\rho} = Q^x.$$

Let $a \in Q$. We apply the identity of triality (2) to $g = ax$. We have

$$r = g^{-1}g^{\sigma} = x^{-1}\big(a^{-1}a^{\sigma}\big)x^{-1} \quad \text{and}$$
$$\begin{aligned}1 = rr^{\rho}r^{\rho^2} &= x^{-1}\big(a^{-1}a^{\sigma}\big)x^{-1}x^{-\rho}\big(a^{-1}a^{\sigma}\big)^{\rho}x^{-\rho}x^{-\rho^2}\big(a^{-1}a^{\sigma}\big)^{\rho^2}x^{-\rho^2}\\ &= x^{-1}\big(a^{-1}a^{\sigma}\big)x^{-1}y^{-1}\big(a^{-1}a^{\sigma}\big)^{\rho}x\big(a^{-1}a^{\sigma}\big)^{\rho^2}xy = x^{-1}\big(a^{-1}a^{\sigma}\big)x^{-1}y^{-1}\big(a^{-1}a^{\sigma}\big)^{\rho}x^2y\big(\big(a^{-1}a^{\sigma}\big)^{\rho^2}\big)^{xy}\\ &= x^{-1}\big(a^{-1}a^{\sigma}\big)x\big(\big(a^{-1}a^{\sigma}\big)^{\rho}\big)^{x^2y}\big(\big(a^{-1}a^{\sigma}\big)^{\rho^2}\big)^{xy} = \big(a^{-1}a^{\sigma}\big)^{x}\big(\big(a^{-1}a^{\sigma}\big)^{\rho}\big)^{x^2y}\big(\big(a^{-1}a^{\sigma}\big)^{\rho^2}\big)^{xy}.\end{aligned}$$

Since $x^2 \in K$, the last expression is in $Q^x \times Q^y \times Q^{xy}$. Hence, $a^{-1}a^{\sigma} = 1$. By arbitrariness of a, we have $\mathcal{M}(Q) = \{a^{-1}a^{\sigma} \mid a \in Q\} = 1$, a contradiction. This proves item (i).

(ii) Suppose that $\mathrm{Gr}(M) = 1$. Let G be as above with the additional condition that $Z_S(G) = 1$. Let T be a minimal normal S-subgroup of G corresponding to $\mathrm{Soc}(M)$. By the above, $T = \prod_q P\Omega_8^+(q)$ with S acting on each factor of T by graph automorphisms. Observe that $C_G(T)$ is a normal S-subgroup of G. Denote $M_0 = \mathcal{M}(C_G(T)) \trianglelefteqslant M$. Since $C_G(T) \cap T = 1$, we have $M_0 \cap \mathrm{Soc}(M) = 1$, which implies $M_0 = 1$ and, therefore, $C_G(T) = 1$ in view of $Z_S(G) = 1$. It follows that $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$. We have

$$\mathrm{Aut}(T) = \prod_i \mathrm{Aut}\big(P\Omega_8^+(q_i)\big) \wr S_{n_i},$$

where each factor is the natural permutation wreath product with S_{n_i}. Since S acts on each $P\Omega_8^+(q_i)$ in the same way, this action commutes with the action of S_{n_i}. Moreover, S commutes with the field automorphisms of $P\Omega_8^+(q_i)$ (for details, see [11, p. 181], where the structure of $\mathrm{Aut}(P\Omega_8^+(q))$ is discussed). Thus, the condition $[G, S] = G$ forces G to be an S-subgroup of $\prod_j D_j \rtimes \Gamma_j \leqslant \mathrm{Aut}(T)$, where $D_j = \mathrm{InnDiag}(P\Omega_8^+(q_j))$ and Γ_j is the group of graph automorphisms of $P\Omega_8^+(q_i)$. Since the jth projection $G \to D_j \rtimes \Gamma_j$ commutes with the action of S, its image G_j must be a subgroup with triality in $D_j \rtimes \Gamma_j$. However $\mathcal{M}(G_j)$, containing $\mathrm{M}(q)$ as a subloop, does not have exponent 3. By Lemma 3, we must have $G_j \leqslant D_j$. Hence, G_j is either $P\Omega_8^+(q_j)$ or $\mathrm{InnDiag}(P\Omega_8^+(q_j))$, and $\mathcal{M}(G_j)$ is either $\mathrm{M}(q)$ or $\widehat{\mathrm{M}(q)}$, accordingly. □

Observe that part III of the proof of item (i) implies, in particular, the following useful fact:

Proposition 2. *Let the symmetric group S_4 act on the direct product of isomorphic groups $G = G_1 \times G_2 \times G_3 \times G_4$ in such a way that $(G_i)^{\tau} = G_{i^{\tau}}$ for all $i = 1, \ldots, 4$ and $\tau \in S$. Let $S_4 = S \ltimes N$, where $S = \langle \sigma =$*

$(12), \rho = (123)\rangle$ *and* $N = \langle(12)(34), (13)(24)\rangle$. *If the semidirect product* $N \ltimes G$ *is a group with triality* S *then* $G_4 \leqslant C_G(S)$.

The following lemma will be used in the next section:

Lemma 11. *Let* M *and* N *be Moufang loops.*

(i) *If* $\varphi : M \to N$ *is a homomorphism then* $\mathrm{Gr}(M)^{\varphi} \leqslant \mathrm{Gr}(M^{\varphi})$, *where the inclusion can be proper*;
(ii) *If* $\mathrm{Gr}(M) = 1$ *and* $N \trianglelefteqslant M$ *then* $\mathrm{Gr}(N) = 1$.

Proof. The inclusion in (i) readily follows from the definition. If we take $M = \widehat{\mathrm{M}(3)}$ and $N = \mathbb{Z}_2$ then N is a homomorphic image of M; however, $\mathrm{Gr}(M) = 1$ and $\mathrm{Gr}(N) = N$. To show (ii), define π_i to be the projection of $\widehat{\mathrm{Soc}(M)}$ to its ith direct factor isomorphic to $\widehat{\mathrm{M}(q)}$, see Theorem 3(ii). Then π_i maps N to a normal subloop of $\pi_i(M)$ which is either $\mathrm{M}(q)$ or $\widehat{\mathrm{M}(q)}$. In any case, $\mathrm{Gr}(N^{\pi_i}) = 1$. By (i), this implies $\mathrm{Gr}(N)^{\pi_i} = 1$ for all i and the claim follows. □

6. *p*-Subloops for non-Sylow primes *p*

The main theorem about the existence of p-Sylow subloops suggests the following natural question: How large can a p-subloop of a Moufang loop M be if p is not a Sylow prime for M? In this section, we show that it can be as large as possible. To give a more precise statement, we need another definition.

Suppose that M is a finite Moufang loop and M_i, $1 \leqslant i \leqslant l$, are the composition factors of M. Let p be any prime. Take $P_i \in \mathrm{Syl}_p(M_i)$ if p is a Sylow prime for M_i and set $P_i = 1$, otherwise. Then a *quasi-p-Sylow* subloop of M is a subloop of order $\prod_{1 \leqslant i \leqslant l} |P_i|$. By Lemma 1, a quasi-$p$-Sylow subloop, if exists, must be a maximal p-subloop of M and its order must be the maximal order of all p-subloops of M. Denote by $\text{q-Syl}_p(M)$ the set of all quasi-p-Sylow subloops of M. Clearly, if p is a Sylow prime for M then $\text{q-Syl}_p(M) = \mathrm{Syl}_p(M)$. Our main result of this section is the following assertion (cf. Theorem A in the introduction):

Theorem 4. *Let* p *be a prime and* M *a finite Moufang loop. Then* M *contains a quasi-*p*-Sylow subloop.*

Proof. We may assume that p is non-Sylow for M, since otherwise the result follows from Theorem 2. This implies that $p > 3$. We proceed by induction on the composition length l of M. If $l = 1$ then the claim holds by definition. Assume that $l > 1$. Let N be a minimal normal subloop of M. By induction, there exists $\overline{P} \in \text{q-Syl}_p(\overline{M})$, where $\overline{M} = M/N$. Let P be the full preimage of $\overline{P}$ in M. If p is a Sylow prime for N then it is such for P as well. In this case, P contains a p-Sylow subloop by Theorem 2 which is obviously quasi-p-Sylow for M. Hence, we may assume that p is non-Sylow for N. But then N must be nonassociative and, by Theorem 3, N is simple. Note that a quasi-p-Sylow subloop of P, if exists, must have order $|\overline{P}|$. Let $R = \mathrm{Gr}(P)$. Since p is odd, it is easy to conclude by Theorem 2(ii) that $P/R \cong N$ and $|R| = |\overline{P}|$. Hence, $R \in \text{q-Syl}_p(P) \subseteq \text{q-Syl}_p(N)$. □

A corresponding fact about groups with triality can be stated as follows:

Corollary 3. *Let* p *be a prime and let* G *be a group with triality* S. *Then* G *possesses an* S*-invariant* p*-subgroup* P *such that* $\mathcal{M}(P) \in \text{q-Syl}_p(\mathcal{M}(G))$.

Proof. This assertion is a generalization of the implication (i) ⇒ (iii) of Theorem 2 and can be proved as follows. Denote $M = \mathcal{M}(G)$. We identify M with the subset $\{[x, \sigma] \mid x \in G\} \subseteq G$. Let $N \in \text{q-Syl}_p(M)$, which exists by Theorem 4. By Lemma 7, $P = \langle N \cup N^{\rho}\rangle$ is an S-subgroup of G such that $\mathcal{M}(P) = N$ and $[P, S] = P$. By Lemma 8(ii), P is the required p-subgroup. □

Let M be a Moufang loop and let p be a prime. Denote by $\mathrm{Gr}_p(M)$ the product of all normal subloops of M for which p is a Sylow prime. The properties of $\mathrm{Gr}_p(M)$ are as follows:

Proposition 3.

(i) $\mathrm{Gr}_p(M) \trianglelefteq M$ *and* p *is a Sylow prime for* $\mathrm{Gr}_p(M)$;
(ii) *The factor loop* $M/\mathrm{Gr}_p(M)$ *contains no elements of order* p;
(iii) *All* p*-subloops of* M *are contained in* $\mathrm{Gr}_p(M)$;
(iv) $\mathrm{Syl}_p(\mathrm{Gr}_p(M)) = \text{q-}\mathrm{Syl}_p(M)$;
(v) $\mathrm{Gr}(M) = \mathrm{Gr}(\mathrm{Gr}_p(M)) = \bigcap_p \mathrm{Gr}_p(M)$.

Proof. Item (i) follows directly from the definition. We may henceforth assume that p is non-Sylow for M, since otherwise $\mathrm{Gr}_p(M) = M$ and the claim trivially holds. In particular, we have $p > 3$. Observe that $\mathrm{Gr}(M) \leqslant \mathrm{Gr}_p(M)$. Hence, $M/\mathrm{Gr}_p(M) \cong \overline{M}/\mathrm{Gr}_p(\overline{M})$, where $\overline{M} = M/\mathrm{Gr}(M)$, and it is easy to conclude by Theorem 3 that $\mathrm{Soc}(M/\mathrm{Gr}_p(M))$ must be the product of $\mathrm{M}(q)$ for which p is non-Sylow. Hence, $M/\mathrm{Gr}_p(M)$ does not contain elements of order p by Lemma 1 and (ii) follows. If P is a p-subloop of M then $P\,\mathrm{Gr}_p(M)/\mathrm{Gr}_p(M)$ is a p-subloop of $M/\mathrm{Gr}_p(M)$ and hence must be trivial by (ii), which implies (iii). The inclusion $\mathrm{Syl}_p(\mathrm{Gr}_p(M)) \subseteq \text{q-}\mathrm{Syl}_p(M)$ holds by the definition of a quasi-p-Sylow subloop, since the composition factors of $M/\mathrm{Gr}_p(M)$ are $\mathrm{M}(q)$ for which p is non-Sylow and, possibly, cyclic groups of order 2, as we just explained in proving (ii). The reverse inclusion holds by (iii) and the fact that quasi-p-Sylow subloops are p-subloops of maximal order. Finally, we show that (v) holds. The inclusions $\mathrm{Gr}(M) \leqslant \mathrm{Gr}(\mathrm{Gr}_p(M))$ and $\mathrm{Gr}(M) \leqslant \bigcap_p \mathrm{Gr}_p(M)$ are obvious from $\mathrm{Gr}(M) \leqslant \mathrm{Gr}_p(M)$. Since $\mathrm{Gr}_p(M)/\mathrm{Gr}(M)$ is a normal subloop of $M/\mathrm{Gr}(M)$, its group-type radical must be trivial by Lemma 11. It follows easily that $\mathrm{Gr}(\mathrm{Gr}_p(M)) \leqslant \mathrm{Gr}(M)$. Now denote by R the image of $\bigcap_p \mathrm{Gr}_p(M)$ in $M/\mathrm{Gr}(M)$. Since R is a normal subloop, it follows by Lemma 11(ii) that every minimal normal subloop of R is $\mathrm{M}(q)$ for some q. However, for every $\mathrm{M}(q)$, there is a non-Sylow prime. Hence R has no nontrivial normal subloops and thus must be trivial. □

Proposition 3 shows that $\mathrm{Gr}_p(M)$ can be viewed as a p-analog of the group-type radical $\mathrm{Gr}(M)$. In particular, the study of embeddings of p-subloops into each other and determining the number of quasi-p-Sylow subloops of M can be reduced to the case where p is a Sylow prime for M.

References

[1] R.H. Bruck, A Survey of Binary Systems, Springer-Verlag, 1958.

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

[3] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Pure Appl. Math., vol. XI, Interscience Publishers, New York, 1962.

[4] S. Doro, Simple Moufang loops, Math. Proc. Cambridge Philos. Soc. 83 (1978) 377–392.

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

[6] D. Gorenstein, Finite Groups, Harper & Row Publishers, New York, 1968.

[7] A.N. Grishkov, A.V. Zavarnitsine, Sylow's theorem for Moufang loops I, preprint RT-MAT 2005-17, IME-USP, São Paulo, 2005, 14 p.

[8] A.N. Grishkov, A.V. Zavarnitsine, Lagrange's theorem for Moufang loops, Math. Proc. Cambridge Philos. Soc. 139 (1) (2005) 41–57.

[9] A.N. Grishkov, A.V. Zavarnitsine, Maximal subloops of finite simple Moufang loops, J. Algebra 302 (2) (2006) 646–677.

[10] A.N. Grishkov, A.V. Zavarnitsine, Groups with triality, J. Algebra Appl. 5 (4) (2006) 441–463.

[11] 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 (1) (1987) 173–242.

[12] A.G. Kurosh, The Theory of Groups, vol. 1, Chelsea Publishing Co., New York, 1960, 272 pp.

[13] M.W. Liebeck, The classification of finite simple Moufang loops, Math. Proc. Cambridge Philos. Soc. 102 (1987) 33–47.

[14] G.P. Nagy, P. Vojtěchovský, Octonions, simple Moufang loops and triality, Quasigroups Related Systems 10 (2003) 65–94.