

SPLITTING AUTOMORPHISMS AND MOUFANG LOOPS

GÁBOR P. NAGY

Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary
e-mail: nagyg@math.u-szeged.hu
URL: <http://www.math.u-szeged.hu/~nagyg/>

and MAURIZIO VALSECCHI

Mathematisches Institut, Universität Erlangen-Nürnberg, Bismarckstr. 1 $\frac{1}{2}$, D-91054 Erlangen, Germany
e-mail: maurizio@mi.uni-erlangen.de

(Received 21 March, 2003; accepted 10 December, 2003)

Abstract. It is known that the concept of Moufang loops, Moufang 3-nets and groups with triality are strongly related. Due to S. Doro, a group with a splitting automorphism of order 3 can lead to a group with triality. This construction naturally appears in the classification of simple Moufang loops. In this paper, we consider groups with triality related to groups with splitting automorphism. We give a classification of Moufang loops corresponding to this construction.

2000 *Mathematics Subject Classification.* 20N05, 20F19.

1. Basic concepts. Let L be a set endowed by a binary operation $x \cdot y = xy$ and let us define the *left* and *right translations* $\lambda_x(y) = xy$, $\rho_x(y) = yx$.

DEFINITION 1.1. We say that (L, \cdot) is a *loop* if on the one hand $\lambda_x, \rho_x : L \rightarrow L$ are invertible maps and on the other hand, $1x = x1 = x$ holds for a distinguished element $1 \in L$. The loop L is a *Moufang loop* if the identity $((xy)z)y = x(y(zy))$ holds.

The Moufang property can be equivalently expressed by both identities $x(y(xz)) = ((xy)x)z$ and $(xy)(zx) = x((yz)x)$.

DEFINITION 1.2. For a Moufang loop L , we define the multiplication group $\text{Mlt}(L)$ of L as the permutation group generated by the left and right translations $\lambda_x, \rho_x, x \in L$.

To a loop (L, \cdot) , one can associate a incidence geometric structure called *3-net*.

DEFINITION 1.3. A 3-net consists of a point set \mathcal{P} and a line set \mathcal{L} which is partitioned in three classes $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$ such that the following hold.

- (i) Two lines from the same class have no points in common and lines from different classes have precisely one point in common.
- (ii) Every point is incident with precisely one line from each class.

If L is a loop then the choice $\mathcal{P} = L \times L$, $\mathcal{L}_1 = \{(c, y) \mid y \in L\} \mid c \in L$, $\mathcal{L}_2 = \{(x, c) \mid x \in L\} \mid c \in L$, $\mathcal{L}_3 = \{(x, y) \mid x, y \in L, xy = c\} \mid c \in L$ defines a 3-net.

The first author was supported by the FKFP grant 0063/2001 of the Hungarian Ministry for Education and the OTKA grants nos. F042959 and T043758.

The second author was supported by Istituto Nazionale di Alta Matematica – Rome.

Conversely, given a 3-net $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ and the origin $O \in \mathcal{P}$, we can introduce a multiplication on the 1-line ℓ through O that turns ℓ into a loop, called the *coordinate loop* of \mathcal{N} . For introductory reference on loops and 3-nets see [2], [9].

Let $\ell \in \mathcal{L}_i$ be a line of a 3-net and let $\mathcal{L}_j, \mathcal{L}_k$ be the other two line classes. We denote by σ_ℓ the permutation of \mathcal{P} which interchanges the line classes $\mathcal{L}_j, \mathcal{L}_k$ and leaves the points of ℓ fixed. These properties determine σ_ℓ uniquely and imply $\varphi\sigma_\ell\varphi^{-1} = \sigma_{\varphi(\ell)}$ for any collineation φ of the 3-net. A theorem of G. Bol says that σ_ℓ is a collineation of the 3-net for every line ℓ if and only if the coordinate loop is Moufang. We call such 3-nets *Moufang nets*.

For a group G , we use the common notation x^α instead of $\alpha(x)$ for $x \in G$ and $\alpha \in \text{Aut}(G)$. Moreover, we put $x^y = y^{-1}xy$, $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$ and $[x, \alpha] = x^{-1}x^\alpha$.

DEFINITION 1.4. Let G be a group and $S = \langle \sigma, \rho \mid \sigma^2 = \rho^3 = (\sigma\rho)^2 = 1 \rangle \leq \text{Aut}(G)$. We say that the pair (G, S) is a *group with triality* if the following identity holds for all $x \in G$.

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

REMARK 1.5. An equivalent formulation of this concept is the following. Let Γ be a group with normal subgroup G . Take three involutions $\sigma_i \in \Gamma \setminus G$ and put $\mathcal{C}_i = \sigma_i^G = \{g^{-1}\sigma_i g \mid g \in G\}$, $i = 1, 2, 3$. Assume $\Gamma/G \cong S_3$ and $(\tau_i\tau_j)^3 = 1$ for all $\tau_i \in \mathcal{C}_i, \tau_j \in \mathcal{C}_j, i \neq j$. Then, $(G, \langle \tau_i, \tau_j \rangle)$ is a group with triality. (Cf. [4, Lemma 3.2].)

Let \mathcal{N} be a Moufang net. Let us define the following collineation groups of \mathcal{N} : $\Gamma = \langle \sigma_\ell \mid \ell \in \mathcal{L} \rangle$, $G = \{\gamma \in \Gamma \mid \gamma(\mathcal{L}_i) = \mathcal{L}_i, i = 1, 2, 3\}$. Then, $G \triangleleft \Gamma$ and $\Gamma/G \cong S_3$. Let P be a point of \mathcal{N} and ℓ_1, ℓ_2, ℓ_3 be the three lines through P . Then $\sigma_{\ell_1}\sigma_{\ell_2}\sigma_{\ell_1} = \sigma_{\ell_2}\sigma_{\ell_1}\sigma_{\ell_2} = \sigma_{\ell_3}$, hence $(\sigma_{\ell_1}\sigma_{\ell_2})^3 = 1$. By Remark 1.5, this implies that for $S_P = \langle \sigma_{\ell_1}, \sigma_{\ell_2} \rangle = \langle \sigma_{\ell_1}, \sigma_{\ell_2}, \sigma_{\ell_3} \rangle \cong S_3$, (G, S_P) is a group with triality.

Conversely, any group with triality determines a Moufang net if one puts $\mathcal{L}_i = \mathcal{C}_i$, and the points are defined as subgroups $\langle \tau_i, \tau_j \rangle \cong S_3, \tau_i \in \mathcal{C}_i, \tau_j \in \mathcal{C}_j, i \neq j$. The incidence is the reverse containment. This construction appeared in [4]. The original observation on the relation between Moufang loops and groups with triality was made in [3].

The relation between Moufang loops, Moufang nets and groups with triality is in force for surjective homomorphisms as well. This means the equivalence of a surjective homomorphism of the coordinate loop, a surjective direction preserving collineation of a Moufang net and an S -homomorphism of the group with triality. In particular, there is a 1-1 relation between simple Moufang loops, simple 3-nets and S -simple groups with triality. (Cf. [4, Proposition 4.2].)

2. Some groups with triality. The following examples of groups with triality are of big importance. The constructions come basically from Doro [3].

EXAMPLE 2.1. **Type I.** Let A be a group, $G = A^3$, and define the automorphisms $\sigma : (a_1, a_2, a_3) \mapsto (a_2, a_1, a_3)$ and $\rho : (a_1, a_2, a_3) \mapsto (a_2, a_3, a_1)$ of G . Then G is a group with triality with respect to $S = \langle \sigma, \rho \rangle$.

EXAMPLE 2.2. **Type II.** Let A be a group with $\varphi \in \text{Aut}(G)$ satisfying $x x^\varphi x^{\varphi^2} = 1$ for all $x \in A$. Put $G = A \times A, \sigma : (a_1, a_2) \mapsto (a_2, a_1)$ and $\rho : (a_1, a_2) \mapsto (a_1^\varphi, a_2^{\varphi^{-1}})$. Then G is a group with triality with respect to $S = \langle \sigma, \rho \rangle$.

PROPOSITION 2.3. *Let L be a Moufang loop giving rise to group with triality G .*

- (i) *If G is of type I, then $L \cong A$. In particular, L is associative.*
- (ii) *If G is of type II, then $L \cong (A, \circ)$, where the operation $x \circ y$ is defined on A by*

$$x \circ y = x^{-\varphi^2}yx^{-\varphi} = y^{-\varphi}xy^{-\varphi^2}.$$

Proof. Part (i) is shown in [3, Proposition 1]. (The proof does not use finiteness.) Applying (1) for $x^{-\varphi^2}y$, we obtain $x^{-\varphi^2}yx^{-\varphi} = y^{-\varphi}xy^{-\varphi^2}$. Hence, part (ii) makes sense. Put

$$\sigma_{1,a} = (a, a^{-1})\sigma, \quad \sigma_{2,a} = (a^\varphi, a^{-\varphi^{-1}})\rho\sigma, \quad \sigma_{3,a} = (a^{-\varphi^{-1}}, a^\varphi)\sigma\rho,$$

and

$$\mathcal{C}_i = \{\sigma_{i,a} \mid a \in A\} \subseteq \Gamma = G \rtimes S.$$

Then, $\mathcal{C}_1 = \sigma^G$, $\mathcal{C}_2 = (\sigma\rho)^G$ and $\mathcal{C}_3 = (\rho\sigma)^G$. Moreover, we have $\sigma_{3,a} = \sigma_2\sigma_{1,a}\sigma_2 = \sigma_1\sigma_{2,a}\sigma_1$, which means that $\sigma_{1,a}, \sigma_{2,1}, \sigma_{3,a}$ and $\sigma_{1,1}, \sigma_{2,a}, \sigma_{3,a}$ to reflections of concurrent line triples. In particular, the underlying set of L can be identified by A .

On the other hand, the lines through the point (x, y) correspond to the reflection $\sigma_{1,x}, \sigma_{2,y}$ and $\sigma_{3,xy}$, respectively, hence $\sigma_{3,xy} = \sigma_{1,x}\sigma_{2,y}\sigma_{1,x}$. In our case, this implies

$$\begin{aligned} \sigma_{3,xy} &= (x, x^{-1})\sigma(y^\varphi, y^{-\varphi^{-1}})\rho\sigma(x, x^{-1})\sigma \\ &= (x, x^{-1})(y^{-\varphi^{-1}}, y^\varphi)\rho^{-1}(x, x^{-1})\sigma \\ &= (x, x^{-1})(y^{-\varphi^{-1}}, y^\varphi)(x^\varphi, x^{-\varphi^{-1}})\rho^{-1}\sigma \\ &= (xy^{-\varphi^{-1}}x^\varphi, x^{-1}y^\varphi x^{-\varphi^{-1}})\sigma\rho \\ &= ((x \circ y)^{-\varphi^{-1}}, (x \circ y)^\varphi)\sigma\rho. \end{aligned}$$

Hence, we have indeed $x \circ y = x^{-\varphi^2}yx^{-\varphi}$.

The nucleus $N(L)$ of a loop L consists of the elements $n \in L$ for which $n(xy) = (nx)y$, $(xn)y = x(ny)$, $(xy)n = x(yn)$ hold for all $x, y \in L$. For a Moufang loop L , we have $N(L) = \{n \in L \mid n(xy) = (nx)y\}$, see [9, IV.1.5 Corollary]. The center of a loop L is $Z(L) = \{x \in N(L) \mid \forall y : xy = yx\}$. The second center $Z_2(G)$ of the group G consists of the elements $z \in G$, for which $[[z, x], y] = 1$ for all $x, y \in G$.

LEMMA 2.4. *Let A be a group and let $\varphi \in \text{Aut}(A)$ satisfy $xx^\varphi x^{\varphi^2} = 1$ for all $x \in A$. Define the loop (A, \circ) by $x \circ y = x^{-\varphi^2}yx^{-\varphi}$. Then, $N(A) = Z_2(A)$ and $Z(A, \circ) = \{x \in Z_2(A) \mid x^{-1}x^\varphi \in Z(A)\}$.*

Proof. We have

$$\begin{aligned} x \circ (y \circ z) &= x^{-\varphi^2}y^{-\varphi^2}zy^{-\varphi}x^{-\varphi}, \\ (x \circ y) \circ z &= xy^{-\varphi^2}x^\varphi zx^{\varphi^2}y^{-\varphi}x. \end{aligned}$$

Therefore, $x \circ (y \circ z) = (x \circ y) \circ z$ holds for all $y, z \in A$ if and only if $z = azb$, where $a = y^{\varphi^2}x^{\varphi^2}xy^{-\varphi^2}x^\varphi$ and $b = x^{\varphi^2}y^{-\varphi}xx^\varphi y^\varphi$. However, on the one hand, we have

$$\begin{aligned} ab &= y^{\varphi^2}x^{\varphi^2}xy^{-\varphi^2}x^\varphi x^{\varphi^2}y^{-\varphi}xx^\varphi y^\varphi \\ &= y^{\varphi^2}x^{-\varphi}y^{-\varphi^2}x^{-1}y^{-\varphi}x^{-\varphi^2}y^\varphi \\ &\stackrel{(*)}{=} y^{\varphi^2}x^{-\varphi}x^\varphi yx^{\varphi^2}x^{-\varphi^2}y^\varphi \\ &= y^{\varphi^2}yy^\varphi = 1, \end{aligned}$$

where in step (*), we used $y \circ x^{-1} = y^{-\varphi^2} x^{-1} y^{-\varphi} = x^\varphi y x^{\varphi^2} x^{-\varphi^2}$. Thus, $ab = 1$ and $x \circ (y \circ z) = (x \circ y) \circ z$ holds if and only if for all $y \in A$, $a = y^{\varphi^2} x^{\varphi^2} x y^{-\varphi^2} x^\varphi = [y^{-\varphi^2}, x^\varphi]$ commutes with all $z \in A$. This precisely means that $[y^{-\varphi^2}, x^\varphi] \in Z(A)$ for all $y \in A$, that is, $x^\varphi \in Z_2(A)$. This shows $N(A) = Z_2(A)$.

Let us now suppose $x \circ y = y \circ x$ for all $y \in A$. This is equivalent with $x^{-\varphi^2} y x^{-\varphi} = x^{-\varphi} y x^{-\varphi^2}$, that is, $y = x^{\varphi^2} x^{-\varphi} y x^{-\varphi^2} x^\varphi$. Since x and x^φ commute, this is equivalent with the fact that $x^{-\varphi} x^{\varphi^2}$ commutes with every $y \in A$. With other words, $x \circ y = y \circ x$ holds for all $y \in A$ if and only if $x^{-1} x^\varphi \in Z(A)$. This finishes the proof.

At the end of this section, we consider S -simple groups with triality in details. The results of the next paragraph are due to S. Doro [3].

Since G must be characteristically simple and $S \cong S_3$, we have $G = A^k$, where $k \in \{1, 2, 3, 6\}$. The case $k = 6$ contradicts to the triality property immediately. If $k = 3$, then G must be of type I and the 3-net turns out to be coordinatized by the simple group A . Conversely, if the coordinate loop of the 3-net is the noncommutative simple group A , then the associated group with triality is of type I. Let us suppose $k = 2$. Doro shows that in this case, G is of type II. He rules out this possibility only for the finite case, using heavy theory of groups and Moufang loops. In the rest of this paper, we classify all Moufang loops of type II. In particular, we show that they can be simple only by being a group of prime order.

3. Splitting automorphisms. DEFINITION 3.1. If G is any group, we say that an automorphism φ of G is a *splitting automorphism* of order n if $x^{\varphi^n} = 1$ and

$$x x^\varphi x^{\varphi^2} \cdots x^{\varphi^{n-1}} = 1 \tag{2}$$

for every $x \in G$.

The following theorem is important from the point of view of simple Moufang loops. The content seems to be folklore. On the one hand, it is mentioned without proof and any reference in E. I. Khukhro’s book [7, p. 223], and neither could the authors locate it stated explicitly elsewhere. On the other hand, as pointed out by the referee, the proof is contained in a relatively old paper [8] by B. H. Neumann, however, the result he formulates is much more specific.

THEOREM 3.2. *Let G be a group admitting a splitting automorphism of order 3. Then for every $x, y \in G$ it is $[x, y, y] = [[x, y], y] = 1$. In particular, G is nilpotent with nilpotency class less or equal to 3. Moreover, if G has no elements of order 3, then the nilpotency class is at most 2.*

Proof. (We replaced the additive notation by multiplicative one in Neumann’s proof.) The splitting property of the automorphism φ is equivalent to

$$x x^\varphi = (x^{-1})^{\varphi^2} \tag{3}$$

for all $x \in G$. We use (3) for several values of x . Let g, h be arbitrary in G . Then, by (3) with $x = h^{-1}g$ and $x = g$,

$$\begin{aligned} (h^{-1}g)(h^{-1}g)^\varphi &= ((h^{-1}g)^{-1})^{\varphi^2} \\ &= (g^{-1})^{\varphi^2} h^{\varphi^2} \\ &= g g^\varphi h^{\varphi^2}. \end{aligned}$$

Now, multiply on the left by g^{-1} and on the right by $((h^{-1}g)^\varphi)^{-1}h$:

$$g^{-1}[(h^{-1}g)(h^{-1}g)^\varphi]((h^{-1}g)^\varphi)^{-1}h = g^{-1}[gg^\varphi h^{\varphi^2}]((h^{-1}g)^\varphi)^{-1}h$$

$$g^{-1}h^{-1}gh = g^\varphi h^{\varphi^2} (g^\varphi)^{-1} h^\varphi h.$$

Next use (3) with $x = h$:

$$g^{-1}h^{-1}gh = g^\varphi h^{\varphi^2} (g^{-1})^\varphi (h^{-1})^{\varphi^2}$$

$$[g, h] = [(g^{-1})^\varphi, (h^{-1})^{\varphi^2}].$$

This last identity is used three times, giving

$$[g, h] = [(g^{-1})^\varphi, (h^{-1})^{\varphi^2}]$$

$$= [g^{\varphi^2}, h^\varphi]$$

$$= [(g^{-1})^{\varphi^3}, (h^{-1})^{\varphi^3}]$$

$$= [g^{-1}, h^{-1}];$$

that is, $(hg)^{-1}gh = (gh)(hg)^{-1}$. This says gh commutes with $(hg)^{-1}$ and so also with hg . Therefore $[hg, gh] = 1$. Now set $h = y^{-1}$ and $g = xy$ to find $[y^{-1}xy, x] = 1$ for any $x, y \in G$. Since this is equivalent to the identity $[x, [x, y]] = 1$, we obtain the statement on the nilpotency class of G from Levi's Theorem [5, Satz 6.5].

4. Moufang loops and splitting automorphisms of order 3. In this section, we make two applications of the above results. On the one hand, we classify those Moufang loops which correspond to groups with triality of type II. On the other hand, we show that the multiplication group of arbitrary proper simple Moufang loops is simple.

THEOREM 4.1. *Let L be a Moufang loop and let us assume that the associated group with triality G has type II. Then L is centrally nilpotent of class at most 3. If L has no element of order 3, then L is a group of nilpotency class at most 2.*

Proof. Since G is of type II, we can put $G = A^2$ and denote by φ the splitting automorphism of order 3 of A . By Theorem 3.2, A is nilpotent of class $c \leq 3$, hence so does G . $G/Z(G)$ is a group with triality of type II with respect to the automorphism induced by φ on $A/Z(G)$. Moreover, $G/Z(G)$ has class $c - 1$, thus, using induction, we obtain that L is nilpotent of class at most c .

Observe that the power of the elements of A are equal in the group A and in the loop $L = (A, \circ)$. Therefore, the assumption that L has no element of order 3 is equivalent with the assumption that the group A has no such element. By Theorem 3.2, the nilpotency class c of A and G is at most 2 in this case. Lemma 2.4 implies $N(A, \circ) = Z_2(A) = A$, which means that L is a group.

REMARK 4.2. The last theorem is related to the following result of T. Hsu [6, Theorem 3.8]. Let L be a nilpotent Moufang loop of class 2 and assume that L does not contains elements of order 2 or 3. Then L is a group.

THEOREM 4.3. *Let L be a nonassociative simple Moufang loop. Then the multiplication group $\text{Mlt}(L)$ is a simple group.*

Proof. It is known that for a simple L , $G = \text{Mlt}(L)$ is a group with triality. See [3, Theorem 1]. Moreover, G must be S -simple. Since L is nonassociative, G is either simple or of type II. Assume G is of type II. Hence $G = A \times A$ for some simple group A . Furthermore, A has a splitting automorphism of order 3. By Theorem 3.2, A is nilpotent, so that A is an abelian group of prime order p . This gives a contradiction and so G is a simple group.

COROLLARY 4.4. *Let L be a simple Moufang loop with associated group with triality G . We have the following possibilities.*

- (i) *If L is a group of prime order $p \neq 3$, then $G = \mathbb{Z}_p^2$.*
- (ii) *If L is a group of prime order $p = 3$, then $G = \mathbb{Z}_3$.*
- (iii) *If L is a noncommutative simple group, then $G = A^3$.*
- (iv) *If L is a nonassociative simple Moufang loop, then $G = \text{Mlt}(L)$ is a simple group.*

Proof. The case of a nonassociative simple L follows from Theorem 4.3. Assume L is associative. If L is commutative, then it is finite, and we obtain (i) and (ii) by [3, Proposition 1]. If L is not commutative, then calculation gives $L \cong A$.

COROLLARY 4.5. *Let L be a locally finite nonassociative simple Moufang loop. Then the multiplication group $\text{Mlt}(L)$ is a locally finite simple group with triality.*

Proof. By Theorem 4.3, we only have to show that $\text{Mlt}(L)$ is locally finite. A finite number of elements of $\text{Mlt}(L)$ is the product of the left and right translations $\{\lambda_x, \rho_x \mid x \in S\}$ for some finite subset S of L . S generates a finite subloop K of L . Doro proved in [3, Corollary 3 of Theorem 2] that the associated group with triality of a finite Moufang loop is finite. This implies the finiteness of $\langle \lambda_x, \rho_x \mid x \in K \rangle$ and hence that $\text{Mlt}(L)$ is locally finite.

ACKNOWLEDGEMENT. The authors would like to thank the referee for many valuable suggestions concerning Section 3 and especially for calling their attention to Neumann's paper [8].

REFERENCES

1. R. Baer, Nets and groups, *Trans. Amer. Math. Soc.* **46** (1939), 110–141.
2. R. H. Bruck, *A survey of binary systems* (Springer-Verlag, 1958).
3. S. Doro, Simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **83** (1978), 377–392.
4. J. I. Hall and G. P. Nagy, On Moufang 3-nets and groups with triality, *Acta Sci. Math. (Szegeed)* **67**(3–4) (2001), 675–685.
5. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, 1967).
6. T. Hsu, Moufang loops of class 2 and cubic forms, *Math. Proc. Cambridge Philos. Soc.* **128** (2000), no. 2., 197–222.
7. E. I. Khukhro, *Nilpotent groups and their automorphisms* (W. de Gruyter, Berlin, 1993).
8. B. H. Neumann, Groups with automorphisms that leave only the neutral element fixed. *Arch. Math.* **7** (1956), 1–5.
9. H. O. Pflugfelder, *Quasigroups and loops* (Heldermann-Verlag, Berlin, 1990).