Publ. Math. Debrecen
88/3-4 (2016), 261–267
DOI: 10.5486/PMD.2016.7147

On the structure of automorphic Moufang loops

By ALEXANDER GRISHKOV (São Paulo), MARINA RASSKAZOVA (Omsk)
and LIUDMILA SABININA (Cuernavaca)

Abstract. It is known that any automorphic Moufang loop M is an epimorphic image of a subdirect product of a group and a commutative Moufang loop. We show that this epimorphism can be chosen minimal for a suitable partial order. We give an example showing that in general this minimal epimorphism is not uniquely determined and study properties of the kernels of these minimal epimorphisms.

1. Preliminaries and definitions

A *Moufang loop* is a universal algebra $\langle Q; \cdot, ()^{-1}, 1\rangle$ such that the identities

$$(x \cdot y) \cdot (z \cdot x) = (x \cdot (y \cdot z)) \cdot x,$$

$$1 \cdot x = x \cdot 1 = x, \ \ (y \cdot x) \cdot (x)^{-1} = (x)^{-1} \cdot (x \cdot y) = y$$

hold. In the following we often write xy instead of $x \cdot y$.

Furthermore, in this note we often say just *loop* instead of the term *Moufang loop*.

The bijection $L_a : Q \to Q$, $L_a x = ax$ is called a *left multiplication*, analogously the bijection $R_a : Q \to Q$, $R_a y = ya$ is called a *right multiplication*

Mathematics Subject Classification: 20N05.
Key words and phrases: Moufang loops, automorphic Moufang loops.
The authors thank to Peter Plaumann, Yuri Volkov, A. L. Shmelkin and I. P. Shestakov for useful discussions. The first author thanks to FAPESP, CNPQ and Russian grant RFFI 13-01-00577a. The second author thanks CNPq(Brazil), process 456698/2014-0. The third author thanks for support to 2011-2013 UCMEXUS and CONACYT collaborative grant CN-11-567, 2012-2013 FAPESP grant processo 2012/11068-2 and 2012-2013 CONACYT grant for sabbatical year at the Institute of Mathematics and Statistics of the University of Sao Paulo, Brazil.

for all $a \in Q$. The mappings L_a and R_a for all $a \in Q$ generate Mlt(Q), the *multiplication group* of Q.

The group Inn(Q), the *inner mapping group* of Q, is the stabilizer of the neutral element 1, that is

$$\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mlt(Q)} \mid \phi(1) = 1\}.$$

A loop Q is called *automorphic* if Inn(Q) is a subgroup of the group of all automorphisms of Q. As usual one defines a *normal subloop* as the kernel of a loop homomorphism. A subloop of a given loop Q is normal if and only if it is invariant under the group Inn(Q). In any automorphic loop all characteristic subloops are normal.

Moufang loops are diassociative, that is the subloop generated by two elements is a group. In a Moufang loop Q we define the *commutator subloop* $[Q, Q]$ as the normal closure of the subloop generated by all elements of the form $x^{-1}y^{-1}xy = [x, y]$, where $x, y \in Q$ and the *associator subloop* (Q, Q, Q) as the normal closure of the subloop generated by all elements of the form $(x(yz))^{-1}((xy)z) = (x, y, z)$ for all $x, y, z \in Q$.

We will call $\Delta(Q) = [Q, Q] \cap (Q, Q, Q)$ the *radical-defect* or the *radical* of the loop Q.

For a Moufang loop Q the subloop

$$N(Q) = \{x \in Q : (x, a, b) = (a, x, b) = (a, b, x) = 1, \text{ for all}\, a, b \in Q\},$$

is called the *nucleus* of Q.

The subloop $C(Q) = \{z \in N(Q) \mid xz = zx \text{ for all}\, x \in Q\}$ is called the *center* of the loop Q. In any Moufang loop the nucleus and the center are normal subloops. In an automorphic Moufang loop Q the radical-defect $\Delta(Q)$ is an elementary abelian 3-subgroup of the center ([GPS]).

2. Radical-defectless coverings of automorphic Moufang loops

The automorphic Moufang loops form a variety. In [Bruck, Lemma 2.2, page 113] the fundamental properties of automorphic Moufang loops were determined. Commutative Moufang loops are examples of automorphic Moufang loops [Bruck], Groups are examples of automorphic Moufang loops, too. In [GPS] the finitely generated free automorphic Moufang loops were constructed and it was shown that their radical-defect is trivial. It is easy to see that it is true without assuming finite rank.

Lemma 2.1. *A free automorphic Moufang loop has a trivial radical-defect.*

Proof. Let F be a free automorphic Moufang loop. Then

$$i:\ F \hookrightarrow F/(F,F,F) \times F/[F,F],$$

is an inclusion. Here $F/(F,F,F)$ is a free group and $F/[F,F]$ is a free commutative loop. (See [GPS] for details.) □

We can show the following theorem.

Theorem 2.2. (i) *A Moufang loop with a trivial radical-defect is automorphic. In particular $M/\Delta(M)$ is automorphic for every Moufang loop M.*

(ii) *If M is a free Moufang loop, then $M/\Delta(M)$ is a free automorphic Moufang loop.*

Proof. (i) If A, B are normal subloops of a loop L, then the kernel of the homomorphism

$$\rho : (L \to L/A \times L/B), x \mapsto (xA, xB)$$

is $A \cap B$. Putting $A = [L,L]$ and $B = (L,L,L)$ gives us the proof of (i) of the theorem. To prove (ii) see [GPS]. □

Here for every automorphic Moufang loop A we will construct a minimal radical-defectless covering in the following sense.

Let us fix an automorphic Moufang loop A and denote by $\mathcal{P}(A)$ the category of all pairs (α, X) where X is an automorphic Moufang loop such that $\Delta(X) = 1$ and α is an epimorphisms $\alpha : X \to A$.

We will call a pair $(\phi_1, A_1) \in \mathcal{P}(A)$ *minimal* if for any $(\phi_2, A_2) \in \mathcal{P}(A)$ and any epimorphism $\psi : A_1 \twoheadrightarrow A_2$, such that $\phi_1 = \phi_2 \circ \psi$, the epimorphism *psi* is an isomorphism.

Let F be a free automorphic Moufang loop and $\phi : F \to A$ be an epimorphism. Denote $K = \ker\phi$ and define $\mathcal{S}(A) = \{I \triangleleft F \mid I \subseteq K,\ \ \Delta(F/I) = 1\}$. One has $\mathcal{S}(A) \neq \emptyset$ since $\{1\} \in \mathcal{S}(A)$. Indeed $\Delta(F) = 1$ by the Lemma 2.1. Let us consider $\mathcal{S}(A)$ as a partially ordered set with the order:

$$I_1 \leq I_2 \text{ if and only if } I_1 \subseteq I_2.$$

For our purpose we use Zorn's lemma in the following form:

In a partially ordered set $(\mathcal{S}, \leq)$ there exists a maximal element if every well *ordered subset of $\mathcal{S}$ has an upper bound in $\mathcal{S}$.* (see [Halmos, p. 68]).

In order to prove the existence of maximal element in $\mathcal{S}(A)$, it is sufficient to show that the upper bound $I = \cup I_i \in \mathcal{S}(A)$ where $I_i \in \mathcal{S}(A),\ I_i \leq I_{i+1}$ for all i.

Suppose that $I \notin \mathcal{S}(A)$. This implies that $\Delta(F/I) \neq 1$ since $I \subseteq K$. There exists $\bar{1} \neq \bar{d} \in \bar{F} = F/I,\ \bar{d} \in [\bar{F}, \bar{F}],\ \bar{d} \in (\bar{F}, \bar{F}, \bar{F})$. Therefore there exist $x, y \in F$ $x, y \notin I$ and there exists $k \in [F, F],\ a \in (F, F, F)$ such that $x = ku_1,\ y = au_2$, where $u_1,\ u_2 \in I$ and $x = yu_3$, where $u_3 \in I$. Put $k = au_4,\ u_4 \in I$. Since $u_4 \in I$ there exists an index n such that $u_4 \in I_n$ and this implies that $k \in I_n$ since $\Delta(F/I_n) = 1$. This forms a contradiction.
We have $I \in \mathcal{S}(A)$ and therefore by Zorn's lemma there exists a maximal element $N \in \mathcal{S}(A)$.

Theorem 2.3. *There exists a minimal pair in $\mathcal{P}(A)$.*

Proof. By definition of $\mathcal{P}(A)$ it is enough to prove that the pair $(\phi_N, F/N)$ is a minimal object in the category $\mathcal{P}(A)$, where ϕ_N is induced by the map $\phi : F \to A$. Denote $F/N = B$. Suppose there exists $(\psi, C) \in \mathcal{P}(A)$ such that

$$B \overset{\mu}{\twoheadrightarrow} C \overset{\psi}{\twoheadrightarrow} A$$

where the maps μ, ψ are not isomorphisms. This implies the existence of $N_0 \in \mathcal{S}(A)$ such that $N \subsetneqq N_0$, where $F/N_0 \simeq C$. We get a contradiction. $\square$

Theorem 2.4. *Let (π, A_0) be a minimal object of $\mathcal{P}(A)$ for some automorphic Moufang loop A. Then*
(i) $\ker\, \pi \subseteq C(A_0)$,
(ii) $\ker\, \pi \cap (A_0, A_0, A_0)[A_0, A_0] \simeq \Delta(A)$.

Proof. (i) Let $I = [\ker\, \pi,\ A_0] \neq 1$. Then I is a normal subloop of A_0. Put $B = A_0/I$. We will show that $\Delta(B)$ is trivial. By Dedekind's modular law (see [Bruck, Lemma 2.2, p. 65]) one has

$$\big([A_0, A_0] \cap (A_0, A_0, A_0)\big)I = [A_0, A_0] \cap (A_0, A_0, A_0)I = I$$

since $I \subseteq [A_0, A_0]$.

Thus,

$$\Delta B = \Delta(A_0/I) = [A_0/I\, A_0/I] \cap (A_0/I,\ A_0/I,\ A_0/I)$$

$$= \big([A_0, A_0] \cap (A_0, A_0, A_0)\big) \cdot I/I = 1.$$

Because of $I \subset \ker\,\pi$ there exists $\eta : B \to A$, such that $\pi = \eta \circ \phi$ for the natural homomorphism $\phi :\ A_0 \to B$ with the kernel I. Hence

$$(\eta, B) \in \mathcal{P}(A) \quad \text{and} \quad (\pi,\ A_0) \geq (\eta, B),$$

but ϕ is not an isomorphism. This is a contradiction to the fact that $(\pi,\ A_0)$ is a minimal pair in $\mathcal{P}(A)$. Thus $[\ker\,\pi,\ A_0] = I = 1$.

By the analogous arguments the normal subloop $J = (\ker\,\pi,\ A_0,\ A_0)$ is trivial and $\ker\,\pi \subseteq N(A_0)$. Hence $\ker\,\pi \subseteq C(A_0)$. Thus the condition (i) of the Theorem 2.4 is proved.

To prove the condition (ii) define a map

$$\tau : \ker\,\pi \cap (A_0, A_0, A_0)[A_0, A_0] \to \Delta(A)$$

in the following way. Let $x \in \ker\,\pi$, and $x = ac^{-1}$, where $a \in (A_0, A_0, A_0)$, and $c \in [A_0, A_0]$. Then put $\tau(x) = \pi(a)$.

Now we will show that this is a correct definition for τ. It is clear that $\pi(x) = \pi(a)\pi(c^{-1}) = 1$, hence $\tau(x) = \pi(a) = \pi(c)$.

$\pi(a) \in (A, A, A)$ since $a \in (A_0, A_0, A_0)$ and $\pi(c) \in [A, A]$ since $c \in [A_0, A_0]$. Hence $\tau(x) \in [A, A] \cap (A, A, A) = \Delta(A)$.

Suppose that

$$x = ac^{-1} = a_1c_1^{-1}, \text{where } a, a_1 \in (A_0, A_0, A_0), c, c_1 \in [A_0, A_0].$$

Since the commutator subloop of an automorphic Moufang loop is contained in the nucleus (see [Bruck, Lemma 2.2, p. 113]) , $c^{-1} = a^{-1} \cdot (a_1c_1^{-1}) = (a^{-1}a_1) \cdot\ c_1^{-1}$. Hence $a^{-1}a_1 = c^{-1}c_1 \in [A_0, A_0] \cap (A_0, A_0, A_0) = \Delta(A_0) = 1$. It follows that $a = a_1,\ c = c_1$ and thus τ is well defined.

We note that

$$(*)\ \ \ker\,\pi \cap [A_0, A_0] = 1$$

$$(**)\ \ \ker\,\pi \cap (A_0, A_0, A_0) = 1.$$

Indeed, if $I_c = \ker\,\pi \cap [A_0, A_0]$, then we have

$$\lambda : A_0 \to A_0/I_c \quad \text{and} \quad \pi_c : A_0/I_c \to A$$

such that

$$\pi_c \circ \lambda = \pi : A_0 \to A.$$

As above by Dedekind's modular law one has

$$\Delta(A_0/I_c) = [A_0/I_c,\ A_0/I_c] \cap (A_0/I_c,\ A_0/I_c,\ A_0/I_c)$$

$$= \big([A_0, A_0] \cap (A_0, A_0, A_0)\big) \cdot I_c/I_c = 1.$$

Since (π, A_0) is a minimal element of $\mathcal{P}(A)$, it follows that λ is an isomorphism. Hence $I_c = \ker \lambda = 1$.

Analogously one can prove that

$$\ker\, \pi \cap (A_0, A_0, A_0) = 1.$$

If $x \in \ker\, \tau$, then $x = ac^{-1}$ and $\pi(a) = \pi(c) = 1$. By $(*)$ and $(**)$ we get $a = c = 1$ and $x = 1$. Thus τ is monomorphism.

Let $y \in \Delta(A)$. Then there exist $a \in (A_0, A_0, A_0)$ and $c \in [A_0, A_0]$ such that $\pi(a) = \pi(c) = y$. In this case

$$x = ac^{-1} \in \ker\, \pi \cap [A_0, A_0](A_0, A_0, A_0)$$

and $\tau(x) = y$. Hence τ is an isomorphism. The theorem is proved. □

Conjecture 2.5. *For every automorphic Moufang loop A there exists a minimal pair $(\pi, A_0) \in \mathcal{P}(A)$ such that* $\ker\, \pi \subset [A_0, A_0](A_0, A_0, A_0)$.

The following example shows that, in general, there exists more than one minimal pair in $\mathcal{P}(A)$. In the variety of groups let us consider a group G such that

$$G = \left\langle a, b, c : [a, b] = c, [a, c] = [b, c] = b^3 = c^3 = 1, a^3 = c \right\rangle.$$

Then G is a 3-group of nilpotency class 2 and of order 3^3. In the variety of commutative Moufang loops let M be a commutative Moufang loop such that

$$M = \left\langle x, y, z, t : (x, y, z) = x^3 = t, y^3 = z^3 = t^3 = 1 \right\rangle.$$

Then M is a commutative Moufang loop of order 3^4. Put $I = \left\langle (a^3, t^2) \right\rangle \subset G \times M$. Then I is a normal subgroup of the loop $G \times M$.
$A = (G \times M)/I$ is an automorphic Moufang loop with radical-defect $\Delta(A) \simeq I$.

Consider an epimorphism $\alpha : G \times M \to A$. Since I is a normal cyclic subgroup of order 3, it is easy to see that $(\alpha, G \times M)$ is a minimal pair in $\mathcal{P}(A)$. Note that $G \times M$ is an automorphic Moufang loop of order 3^7 and that

$$\ker\, \alpha \subset [G \times M, G \times M](G \times M, G \times M, G \times M) = [G, G](M, M, M).$$

But $(\alpha, G \times M)$ is not the unique minimal pair of $\mathcal{P}(A)$ with this property. Indeed, consider the group

$$H = \left\langle u, v, w : [u, v] = w, [u, w] = [v, w] = u^3 = v^3 = w^3 = 1 \right\rangle,$$

and put $J = \left\langle (w, t^2) \right\rangle \subset H \times M$. Denote $\tilde{A} = (H \times M)/J$. Note that A and $\tilde{A}$ are isomorphic loops. Indeed, consider the surjective homomorphism

$$\lambda : G \times M \to (H \times M)/J$$

defined in the following way:

$$\lambda(1,m) = (1,m) \text{ for all } m \in M,$$
$$\lambda(a,1) = (u,x),\ \lambda(b,1) = (v,1),\ \lambda(c,1) = (w,1).$$

Since $\lambda(c,1) = (w,1)$, $\lambda(a^3,1) = (1,t)$ and $(a^3,1) = (c,1)$ it easy to see that $\lambda(a^3,t^2) = (w,t^2)$ and thus $\ker\lambda = I$.

Consider the epimorphism $\beta : H\times M \to A$. Therefore $(\beta, H\times M)$ is a minimal pair of $\mathcal{P}(A)$ of order 3^7, too.

Let us prove that $G\times M$ and $H\times M$ are not isomorphic. Denote by $\xi_n(Q) = |\{x \in Q | x^n = 1\}|$ the number of elements, whose order divides n in a loop Q. Then $\xi_3(G\times M) = 3^5$ and $\xi_3(H\times M) = 3^6$. Hence the loops $G\times M$ and $H\times M$ are not isomorphic. Here we used the fact that $\xi_n(G\times M) = \xi_n(G)\xi_n(M)$. The example of an automorphic Moufang loop of the order 3^6, which has a non-trivial radical-defect was also considered in [Gagola].

References

[Bruck] R. Bruck, A Survey of Binary Systems, *Springer-Verlag, New York, Heidelberg, Berlin*, 1966.

[Halmos] P. Halmos, Naive Set Theory, *Springer-Verlag, New York, Heidelberg, Berlin*, 1966.

[Gagola] S. M. Gagola, Nonsplitting F-quasigroups, *Comment. Math. Univ. Carolin.* **53** (2012), 375–381.

[GPS] A. Grishkov, P. Plaumann and L. Sabinina, Structure of free automorphic loops, *Proc. Amer. Math. Soc.* **140** (2012), 2209–2214.

ALEXANDER GRISHKOV
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
UNIVERSIDADE DE SÃO PAULO
RUA DE MATÃO 1010
SÃO PAULO, 05508-090
BRAZIL

E-mail: grishkov@ime.usp.br

LIUDMILA SABININA
UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE MORELOS
AV. UNIVERSIDAD 1001
CUERNAVACA, 62209
MÉXICO

E-mail: liudmila@uaem.mx

MARINA RASSKAZOVA
OMSK STATE INSTITUTE OF SERVICE
PEVTSOVA STREET 13
OMSK, 644099
RUSSIA

E-mail: marinarasskazova@yandex.ru

(Received August 23, 2014; revised October 16, 2015)