Commentationes Mathematicae Universitatis Carolinae

Giordano Gallina

On a class of Moufang loops

Commentationes Mathematicae Universitatis Carolinae, Vol. 23 (1982), No. 2, 319--324

Persistent URL: http://dml.cz/dmlcz/106154

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
23,2 (1982)

ON A CLASS OF MOUFANG LOOPS

Giordano GALLINA

Abstract: Multiplication groups of Moufang loops derived from antiassociative rings are studied.

Key words: Moufang loop, multiplication group.

Classification: 20N05

In [1], a class of Moufang loops is constructed. In the present note, several properties of these loops are investigated. A special attention is paid to the corresponding multiplication groups.

1. Preliminaries. Throughout this paper, let R be a ring (possibly non-associative) such that $x^2 = 0 = x \cdot xy$ for all $x, y \in R$.

1.1. Lemma. (i) $xy = -yx$ and $x \cdot yz = -xy \cdot z$ for all $x, y, z \in R$.

(ii) $xy \cdot uv = x(y \cdot uv) = x(yu \cdot v) = -xy \cdot uv = (xy \cdot u)v =$ $= (x \cdot yu)v$ for all $x, y, u, v \in R$.

Proof. (i) We have $(x + y)^2 = 0$, and hence $xy = -yx$. Moreover, $(x + y)((x + y)z) = 0$, $x \cdot yz = -y \cdot xz$. From this, $x \cdot yz = -x \cdot zy = z \cdot xy = -xy \cdot z$.

(ii) This is an easy consequence of (i).

Put $R^2 = \{xy; x,y \in R\}$, $R^3 = \{x \cdot yz; x,y,z \in R\}$ and $R^4 = \{xy \cdot uv; x,y,u,v \in R\}$. Then $R^4 \subseteq R^3 \subseteq R^2$ and, according to 1.1, $R^3 = \{xy \cdot z; x,y,z \in R\}$, $R^4 = \{x(y \cdot uv)\} = \{x(yu \cdot v)\} = \{(xy \cdot u)v\} = \{(x \cdot yu)v\}$ and $2R^4 = 0$. Further, let $I = \{a \in R; 2a \cdot xy = 0$ for all $x,y \in R\}$ and $K = \{a \in R; 2ax = 0$ for every $x \in R\}$. Then both I and K are ideals of R, $K \subseteq I$, $R^3 \subseteq K$ and $R^2 \subseteq I$.

Now, we shall define a new binary operation $\circ$ on R by $x \circ y = x + y + xy$ for all $x,y \in R$.

1.2. Proposition. $R(\circ)$ is a Moufang loop, the nucleus $N(R(\circ))$ of $R(\circ)$ is equal to I and the centre $C(R(\circ))$ of $R(\circ)$ is equal to K.

Proof. All the assertions can be checked easily.

1.3. Lemma. $x^{-1} = -x$, $x \circ (y \circ z) = x + y + z + xy + xz + yz + x \cdot yz$ and $(x \circ y) \circ z = x + y + z + xy + xz + yz + xy \cdot z$ for all $x,y,z \in R$.

Proof. Obvious.

1.4. Proposition. $R(\circ)/C(R(\circ))$ is a group. In particular, $R(\circ)$ is associatrally nilpotent of class at most 2.

Proof. Let $x,y,z \in R$ and $a = x \circ (y \circ z)$, $b = (x \circ y) \circ z$. By 1.1 and 1.3, $a \circ b^{-1} = 3x \cdot yz \in R^3 \subseteq K = C(R(\circ))$. Consequently, $R(\circ)/C(R(\circ))$ is a group.

1.5. Proposition. $R(\circ)/N(R(\circ))$ is an abelian group.

Proof. By 1.4, the factorloop is a group. On the other hand, $(x \circ y) \circ (y \circ x)^{-1} = 2xy \in I = N(R(\circ))$ for all $x,y \in R$.

1.6. Proposition. The second centre $C_2(R(\circ))$ of $R(\circ)$ is equal to the set of all $a \in R$ such that $4a \cdot xy = 0$ for all $x,y \in R$. In particular, $N(R(\circ)) \subseteq C_2(R(\circ))$ and $R(\circ)$ is centrally nilpotent of class at most 3.

Proof. $a \in C_2(R(\circ))$ iff $(a \circ x) \circ (x \circ a)^{-1} \in C(R(\circ))$ for every $x \in R$ and the rest is clear (use 1.4 and 1.5).

1.7. Proposition. $R(\circ)$ is a group iff $2R^3 = 0$.

Proof. Apply 1.2.

For every $a \in R$, define three permutations L_a, R_a and V_a of R by $L_a(x) = a \circ x$, $R_a(x) = x \circ a$ and $V_a = R_a^{-1}L_a$. Further, put $S_{a,b} = L_b^{-1} L_a^{-1} L_{a\circ b}^{-1}$ and $T_{a,b} = R_a^{-1} R_b^{-1} R_{a\circ b}$ for $a,b \in R$. Clearly, all these permutations belong to the multiplication group $M(R(\circ))$ of the loop $R(\circ)$.

1.8. Proposition. For all $a,b \in R$, the permutations $S_{a,b}$ and $T_{a,b}$ are automorphisms of $R(\circ)$.

Proof. We have $S_{a,b}(x) = x - 2a\cdot bx$ for every $x \in R$ and it is easy to verify that $S_{a,b}$ is an automorphism of $R(\circ)$. Similarly for $T_{a,b}$.

1.9. Proposition. Let $a \in R$. Then V_a is an automorphism of $R(\circ)$ iff $6a\cdot xy = 0$ for all $x,y \in R$.

Proof. We have $V_a(x) = x + 2ax$ and the rest is clear.

1.10. Proposition. The loop $R(\circ)$ is an A-loop if $6R^3 = 0$.

Proof. An A-loop is a loop such that every of its inner permutations is an automorphism. Now, the statement is clear from 1.8, 1.9 and from the well known fact that the inner mapping group is generated by the permutations $S_{a,b}$, $T_{a,b}$ and V_a.

2. The multiplication group $M(R(\circ))$. Let $n \geq 1$ be an integer, $I_n = \{1,2,\dots,n\}$ and let f be a mapping of I_n into the set $T = \{L_a, R_a; a \in R\}$. We have $f(i) \in \{L_{a_i}, R_{a_i}\}$ and put

$A = \{i \in I_n; f(i) = L_{a_i}\}$ and $B = I_n \setminus A$.

Further, let us designate $p(f) = f(n)f(n-1) \dots$ $\dots f(2)f(1) \in M(R(\circ))$, $g_1(f) = \sum_{i \in I_m} a_i$, $g_2(f) =$ $= \sum_{i \in A} \sum_{\substack{j \in I_m \\ j<i}} a_i a_j - \sum_{i \in B} \sum_{\substack{j \in I_m \\ j<i}} a_i a_j$, $g_3(f) =$

$$= \sum_{i \in A} \sum_{\substack{j \in A \\ j<i}} \sum_{\substack{k \in I_m \\ k<j}} a_i(a_j a_k) - \sum_{i \in A} \sum_{\substack{j \in B \\ j<i}} \sum_{\substack{k \in I_m \\ k<j}} a_i(a_j a_k) +$$
$$+ \sum_{i \in B} \sum_{\substack{j \in B \\ j<i}} \sum_{\substack{k \in I_m \\ k<j}} a_i(a_j a_k) - \sum_{i \in B} \sum_{\substack{j \in A \\ j<i}} \sum_{\substack{k \in I_m \\ k<j}} a_i(a_j a_k)$$ and

$g_m(f) = \sum_{i_1 > \dots > i_m} a_{i_1} \dots a_{i_m}$ for every $m \geq 4$.

2.1. Lemma. $p(f)(x) = (h(f) + \sum_{i=3}^{m} g_i(f))x + \sum_{i=1}^{m} g_i(f) +$ $= x$ for every $x \in R$, where $h(f) = \sum_{i \in A} a_i - \sum_{i \in B} a_i -$

$$- \sum_{i \in A} \sum_{\substack{j \in A \\ j<i}} a_i a_j + \sum_{i \in A} \sum_{\substack{j \in B \\ j<i}} a_i a_j - \sum_{i \in B} \sum_{\substack{j \in B \\ j<i}} a_i a_j +$$
$$+ \sum_{i \in B} \sum_{\substack{j \in A \\ j<i}} a_i a_j.$$

Proof. Some tedious calculations and induction on n.

Now, let $m \geq 1$. Define a mapping $f^{(m)}$ of I_{mn} into T by $f^{(m)}(1) = f(1)$, $f^{(m)}(2) = f(2), \dots, f^{(m)}(n) = f(n), \dots,$ $f^{(m)}(n(m-1)+1) = f(1)$, $f^{(m)}(n(m-1)+2) = f(2), \dots,$ $f^{(m)}(nm) = f(n)$.

2.2. Lemma. For every $m \geq 1$ and every $i \in I_n$, $g_i(f^{(m)}) =$ $= mb_{i,m}$, where $b_{i,m}$ is a sum of products of the elements $a_1, \dots, a_n$.

Proof. The proof is purely of technical character, and hence omitted.

2.3. Lemma. For every $m \geq 1$, $h(f^{(m)}) = mh(f)$.

Proof. By induction on m. The assertion is obvious for

$m = 1$. Further, $h(f^{(m+1)}) = h(f) + h(f^{(m)}) -$
$- m \sum_{i \in A} \sum_{j \in A} a_i a_j + m \sum_{i \in A} \sum_{j \in B} a_i a_j - m \sum_{i \in B} \sum_{j \in B} a_i a_j +$
$+ m \sum_{i \in B} \sum_{j \in A} a_i a_j$.

However, $\sum_{i,j \in A} a_i a_j = \sum_{\substack{i,j \in A \\ j < i}} a_i a_j + \sum_{\substack{i,j \in A \\ j > i}} a_i a_j$,

while the last sum is equal to $- \sum_{\substack{i,j \in A \\ j < i}} a_i a_j$.

Consequently, $\sum_{i,j \in A} a_i a_j = 0$. Similarly for B and we can write $h(f^{(m+1)}) = h(f) + h(f^{(m)}) = h(f) + mh(f) = (m + 1)h(f)$.

2.4. Lemma. Let $m \geq 1$. Then $g_k(f^{(m)}) = mg_1(f)$ and $g_i(f^{(m)}) = mg_i(f)$ for every $i \geq 4$.

Proof. Easy.

2.5. Theorem. Suppose that the abelian group $R(+)$ contains no elements of infinite order. Then the order of $p(f)$ (in $M(R(\circ))$) is a divisor of the least common multiple of the orders of the elements $a_1, \dots, a_n$ (in $R(+)$).

Proof. We have $p(f)^m(x) = p(f^{(m)})(x) = (h(f^{(m)}) + \sum_{i=3}^{n} g_i(f^{(m)}))x + \sum_{i=1}^{n} g_i(f^{(m)}) + x$ for all $m \geq 1$ and $x \in R$ (take into account 2.1 and the fact that $g_i(f^{(m)}) = 0$ for each $i \geq n + 1$). By 2.2, 2.3 and 2.4, $p(f)^m(x) = max + mb + x$, where both the elements a and b are sums of products of the a_i. Therefore, if m is the least common multiple of the orders of the elements a_i, then $ma = mb = 0$ and $p(f)^m = id_R$. The result is now clear.

2.6. Lemma. For all $a \in R$ and $m \geq 1$, $L_a^m = L_{ma}$.

Proof. By induction on m.

2.7. Lemma. Let $a,b,c\in R$ and $m\geq 1$. Then $(L_aL_b)^m = L_c$ iff $2m(a\cdot bx) = 0$ for every $x\in R$. In that case, $(L_aL_b)^m = L_{m(a\circ b)}$.

Proof. We have $(L_aL_b)^m(x) = m(a + b - ab)x + m(a + b + ab)x + x = m(b\circ a)x + m(a\circ b) + x$. Since $b\circ a = a\circ b - 2ab$, $(L_aL_b)^m(x) = m(a\circ b)x + m(a\circ b) - 2m(ab)x$. Hence $(L_aL_b)^m = L_c$ iff $m(a\circ b)x + m(a\circ b) + x - 2m(ab)x = c + x + cx$ for every $x\in R$. In particular, $c = m(a\circ b)$.

2.8. Proposition. Suppose that $R(+)$ is a p-group. Then $M(R(\circ))$ is a p-group of the same exponent.

Proof. Apply 2.5 and 2.6.

References

[1] R.H. BRUCK: Some results in the theory of quasigroup, Trans. Amer. Math. Soc. 55(1944), 19-52.

[2] R.H. BRUCK: A survey of binary systems, Springer-Verlag, Berlin 1958.

[3] M. GARDASCHNIKOFF: Über einen Typus endlicher Gruppen ohne das Associativgesetz , Comm. Inst. Sci. Mat. Mec. Univ. Kharkoff 17(1940), 29-33.

[4] A.K. SUSKEVIC: On a generalization of the associative law, Trans. Amer. Soc. 32(1931), 204-214.

Istituto di Matematica Università degli Studi, Via Università 12, 43100 Parma, Italia

(Oblatum 17.12. 1981)