

Aleš Drápal

A-loops close to code loops are groups

Commentationes Mathematicae Universitatis Carolinae, Vol. 41 (2000), No. 2, 245--249

Persistent URL: <http://dml.cz/dmlcz/119160>

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 2000

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

A-loops close to code loops are groups

ALEŠ DRÁPAL

Abstract. Let Q be a diassociative A-loop which is centrally nilpotent of class 2 and which is not a group. Then the factor over the centre cannot be an elementary abelian 2-group.

Keywords: A-loop, central nilpotency, Osborn problem

Classification: 20N05

This modest note concerns diassociative A-loops that are centrally nilpotent of class 2. Its basic result can be expressed in the following way:

Proposition 1. *Suppose that Q is a diassociative A-loop with a central subloop N . If Q/N is a group of exponent 2, then Q is a group.*

The result is an offshoot of my interest in code loops and I hope that it will help to stimulate further research in the indicated direction.

It can be also understood in the context of the *Osborn problem*: Decide if every (finite) diassociative A-loop is a Moufang loop.

Osborn [6] solved this problem affirmatively for commutative, diassociative A-loops, and some progress in the general case has been recently reported by J.D. Phillips [7].

A subloop N of a loop Q is *central*, if all its elements associate and commute with all elements of Q . Suppose that $Q/N \simeq V$ and that N and V are fixed. The group N is abelian by definition, and we shall assume that V is an abelian group as well (though some of our initial observations can be easily generalized to the case of non-abelian groups). The loop Q is obviously isomorphic to one of the loops $Q(\vartheta)$, where $\vartheta : V \times V \rightarrow N$ is a mapping with $\vartheta(u, 0) = \vartheta(0, u) = 0$ for all $u \in V$, and where the binary operation of $Q(\vartheta)$ is defined by

$$(a, u) \cdot (b, v) = (a + b + \vartheta(u, v), u + v),$$

for all $a, b \in N$ and $u, v \in V$.

A loop Q is said to be a *code loop* ([5], [4], [1]), if $|N| = 2$ and V is an elementary abelian 2-group. Statements about code loops are often proved by computations in $Q(\vartheta)$, and this approach will be used also here. (It is clear that one could

Research partially supported by Grant Agency of the Czech Republic, grant number 201/99/0263, and by an institutional grant of the Czech Republic, code CEZ:J13/98:113200007.

construct a proof which would not resort to ϑ -techniques. However, it is not clear if such proofs would be more transparent or more readable. Description of extensions by means of factor systems ϑ is for loops and quasigroups very natural and has been used many times, starting from [2].)

For a loop Q and $\alpha \in Q$ denote by L_α the left translation $\beta \mapsto \alpha\beta$, $\beta \in Q$, and by R_α the right translation $\beta \mapsto \beta\alpha$, $\beta \in Q$. Call Q a *left* (or *right*, or *middle*) *A-loop*, if $L_{\alpha\beta}^{-1}L_\alpha L_\beta$ (or $R_{\beta\alpha}^{-1}R_\alpha R_\beta$, or $R_\alpha^{-1}L_\alpha$) is an automorphism for all $\alpha, \beta \in Q$, respectively. A loop Q is an *A-loop* if it is simultaneously a left A-loop, a right A-loop and a middle A-loop. The primary source for A-loops is [3].

Fix now $\vartheta : V \times V \rightarrow N$, $\vartheta(u, 0) = \vartheta(0, u) = 0$ for all $u \in V$, and for all $u, v, w \in V$ put

$$C(u, v) = \vartheta(u, v) - \vartheta(v, u), \quad \text{and}$$

$$A(u, v, w) = -\vartheta(u, v) + \vartheta(u, v + w) - \vartheta(u + v, w) + \vartheta(v, w).$$

Suppose that $Q = Q(\vartheta)$, $\alpha = (a, u)$ and $\beta = (b, v)$. Then $L_\alpha L_\beta$ sends (c, x) to $(a + b + c + \vartheta(u, v + x) + \vartheta(v, x), u + v + x)$, and $L_{\alpha\beta}$ sends (c, x) to $(a + b + c + \vartheta(u, v) + \vartheta(u + v, x), u + v + x)$. Hence $L_\alpha L_\beta$ equals $L_{\alpha\beta}$ if and only if $A(u, v, x) = 0$ for all $x \in V$, and we see that $Q(\vartheta)$ is a group if and only if $A(u, v, w) = 0$ for all $u, v, w \in V$.

It is now also clear that $L_{\alpha\beta}^{-1}L_\alpha L_\beta(c, x)$ equals $(A(u, v, x) + c, x)$ for all $(c, x) \in Q$. Put $\varphi = L_{\alpha\beta}^{-1}L_\alpha L_\beta$ and consider $\gamma = (c, x) \in Q$ and $\delta = (d, y) \in Q$. Then $\varphi(\gamma)\varphi(\delta)$ equals $(A(u, v, x) + A(u, v, y) + c + d + \vartheta(x, y), x + y)$, while $\varphi(\gamma\delta)$ is equal to $(A(u, v, x + y) + c + d + \vartheta(x, y), x + y)$. Comparison of the both results yields claim (i) of the following lemma. Claims (ii) and (iii) can be obtained in a similar way.

Lemma 1. (i) $Q(\vartheta)$ is a left A-loop if $A(u, v, x + y) = A(u, v, x) + A(u, v, y)$ for all $x, y, u, v \in V$;

(ii) $Q(\vartheta)$ is a right A-loop if $A(x + y, v, u) = A(x, v, u) + A(y, v, u)$ for all $x, y, u, v \in V$;

(iii) $Q(\vartheta)$ is a middle A-loop if $C(u, x + y) = C(u, x) + C(u, y)$ for all $x, y, u \in V$.

The loop $Q(\vartheta)$ is a group, if $A(u, v, w) = 0$ for all $u, v, w \in V$. If $Q(\vartheta)$ is a left A-loop, then each pair $u, v \in V$ determines, by Lemma 1 (i), a group homomorphism $V \rightarrow N$. All such homomorphisms are trivial if and only if the loop $Q(\vartheta)$ is a group. Since finite groups of coprime order admit only trivial homomorphisms, Lemma 1 yields the following corollary:

Corollary 1. *Let Q be a finite centrally nilpotent loop of class 2 which is not a group, and let Z be its centre. If $|Z|$ and $|Q/Z|$ are coprime, then Q is neither a left A-loop, nor a right A-loop. Furthermore, if $|Z|$ and $|Q/Z|$ are coprime, then Q is a middle A-loop if and only if it is commutative.*

It will be useful to express the equation of Lemma 1 (i) just in terms of ϑ . We

obtain the equality:

$$\begin{aligned}
 (1) \quad & \vartheta(u, v) + \vartheta(u, v + x + y) - \vartheta(u + v, x + y) + \vartheta(v, x + y) \\
 & - \vartheta(u, v + x) + \vartheta(u + v, x) - \vartheta(v, x) \\
 & - \vartheta(u, v + y) + \vartheta(u + v, y) - \vartheta(v, y) = 0.
 \end{aligned}$$

Lemma 2. *Suppose that V is of exponent 2. Then $Q(\vartheta)$ is diassociative if and only if*

$$\begin{aligned}
 \vartheta(u, u + v) = \vartheta(u, u) - \vartheta(u, v), \quad \vartheta(u + v, u) = \vartheta(u, u) - \vartheta(v, u), \quad \text{and} \\
 2\vartheta(v, u) = 2\vartheta(u, v)
 \end{aligned}$$

are true for all $u, v \in U$.

PROOF: Consider $u, v \in V$. By our assumption, $2u = 2v = 0$, and hence the equations $A(u, u, v) = 0$ and $A(v, u, u) = 0$ are equivalent to equations $\vartheta(u, u) - \vartheta(u, u + v) - \vartheta(u, v) = 0$ and $-\vartheta(v, u) - \vartheta(v + u, u) + \vartheta(u, u) = 0$, respectively. If these equalities are true, then $A(u, v, u) = 0$ is equivalent to $2\vartheta(v, u) = 2\vartheta(u, v)$, as $A(u, v, u) = -\vartheta(u, v) + \vartheta(u, v + u) - \vartheta(u + v, u) + \vartheta(v, u) = (\vartheta(v, u) - \vartheta(u, v)) + (\vartheta(u, u) - \vartheta(u, v) - \vartheta(u, u) + \vartheta(v, u)) = 2\vartheta(v, u) - 2\vartheta(u, v)$.

It is now clear that the direct implication of the lemma holds. To prove the converse implication means to show that the ϑ -equalities imply $A(u, v, w) = 0$ whenever u, v and w belong to a subgroup of V with ≤ 4 elements. One clearly has $A(u, v, w) = 0$ if $0 \in \{u, v, w\}$. From the first part of the proof one gets the cases $u = v, v = w$ and $u = w$, and so the only remaining case is the case when $0, u, v$ and w are pairwise different. However, the assumed equalities yield $A(u, u + v, v) = -\vartheta(u, u + v) + \vartheta(u, u) - \vartheta(v, v) + \vartheta(u + v, v) = \vartheta(u, v) - \vartheta(u, v) = 0$. □

We are now ready to prove Proposition 1. Assume that V is of exponent 2 and that $Q(\vartheta)$ is a diassociative A-loop.

Consider (1) for the case $v + x + y = 0$, and note that the first row of (1) then yields $\vartheta(u, v) - \vartheta(u + v, v) + \vartheta(v, v)$, which is, by Lemma 2, equal to $2\vartheta(u, v) = 2\vartheta(u, x + y)$. Furthermore, $\vartheta(u, v + x) + \vartheta(u, v + y)$ equals $\vartheta(u, x) + \vartheta(u, y)$, and $\vartheta(v, x) + \vartheta(v, y) - \vartheta(u + v, x) - \vartheta(u + v, y)$ equals $\vartheta(x + y, x) + \vartheta(x + y, y) - \vartheta(x + y + u, x) - \vartheta(y + x + u, y) = \vartheta(x, x) - \vartheta(y, x) + \vartheta(y, y) - \vartheta(x, y) - \vartheta(x, x) + \vartheta(y + u, x) - \vartheta(y, y) + \vartheta(x + u, y) = -\vartheta(y, x) - \vartheta(x, y) + \vartheta(y + u, x) + \vartheta(x + u, y)$. Hence

$$\begin{aligned}
 (2) \quad & 2\vartheta(u, x + y) = \\
 & \vartheta(u, x) - \vartheta(y, x) + \vartheta(u, y) - \vartheta(x, y) + \vartheta(y + u, x) + \vartheta(x + u, y)
 \end{aligned}$$

holds for all $x, y, u \in V$.

By Lemma 1 (iii), $C(x, u + y)$ equals $C(x, u) + C(x, y)$, and hence $\vartheta(y + u, x) = \vartheta(x, u + y) + \vartheta(u, x) - \vartheta(x, u) + \vartheta(y, x) - \vartheta(x, y)$. Substitute now this expression of

$\vartheta(y + u, x)$ to (2). One gets $2\vartheta(u, x + y) = 2\vartheta(u, x) + \vartheta(u, y) - 2\vartheta(x, y) + \vartheta(x, u + y) + \vartheta(x + u, y) - \vartheta(x, u)$, and so we see that

$$(3) \quad \begin{aligned} 2(-\vartheta(u, x) + \vartheta(u, x + y) + \vartheta(x, y)) = \\ -\vartheta(x, u) + \vartheta(x, u + y) + \vartheta(x + u, y) + \vartheta(u, y) \end{aligned}$$

holds for all $u, x, y \in V$.

By adding $-2\vartheta(x + u, y)$ to the both sides of (3), we obtain

$$2A(u, x, y) = A(x, u, y) \quad \text{for all } x, y, u \in V.$$

However, $2A(u, x, y) = A(u, x, y) + A(u, x, y) = A(u, x, y + y) = A(u, x, 0) = 0$ by Lemma 1(i), and so we see that $A(x, u, y)$ is always zero, and that is what was needed to prove Proposition 1.

Note that our proof did not use the fact that Q is a right A-loop. In our last statement we give an explanation.

Proposition 2. *Let Q be a loop that is centrally nilpotent of class 2. If Q is simultaneously a left A-loop and a middle A-loop, then it is also a right A-loop.*

PROOF: One can obviously assume that Q equals $Q(\vartheta)$. When the equality $A(x + y, v, u) - A(x, v, u) - A(y, v, u) = 0$ is expressed in terms of ϑ , one gets

$$(4) \quad \begin{aligned} -\vartheta(v, u) - \vartheta(x + y + v, u) + \vartheta(x + y, u + v) - \vartheta(x + y, v) \\ + \vartheta(x + v, u) - \vartheta(x, u + v) + \vartheta(x, v) \\ + \vartheta(y + v, u) - \vartheta(y, u + v) + \vartheta(y, v) = 0. \end{aligned}$$

Summing up (1) and (4) one obtains

$$(5) \quad \begin{aligned} C(u, v) + C(u, v + x + y) - C(u + v, x + y) + C(v, x + y) \\ - C(u, v + x) + C(u + v, x) - C(v, x) \\ - C(u, v + y) + C(u + v, y) - C(v, y) = 0. \end{aligned}$$

Since $C(x, u + v) = C(x, u) + C(x, v)$ and $C(u + v, x) = C(u, x) + C(v, x)$ are true, by Lemma 1(iii), for all $x, u, v \in V$, we see that (5) is satisfied. Since (1) holds by Lemma 1(i), the equality (4) must be also true (for all $x, y, u, v \in V$), and hence Q is a right A-loop, by Lemma 1(ii). □

Acknowledgment. I thank J.D. Phillips for bringing Osborn’s problem to my attention and for communicating with me about this topic.

REFERENCES

- [1] Aschbacher M., *Sporadic Groups*, Cambridge Tracts in Mathematics **104**, Cambridge University Press, 1994.
- [2] Bruck R.H., *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.
- [3] Bruck R.H., Paige L.J., *Loops whose inner mappings are automorphisms*, Ann. of Math. **63** (1954), 308–323.
- [4] Chein O., Goodaire E.G., *Moufang loops with a unique non-identity commutator (associator, square)*, J. Algebra **130** (1990), 369–384.
- [5] Griess R.L., Jr., *Code loops*, J. Algebra **100** (1986), 224–234.
- [6] Osborn M.J., *A theorem on A-loops*, Proc. Amer. Math. Soc. **9** (1958), 347–349.
- [7] Phillips J.D., *On Moufang A-loops*, Comment. Math. Univ. Carolinae **41** (2000), 371–375.

DEPARTMENT OF ALGEBRA, FACULTY OF MATHEMATICS AND PHYSICS, CHARLES UNIVERSITY,
SOKOLOVSKÁ 83, 186 75 PRAGUE 8, CZECH REPUBLIC

(Received October 15, 1999)