On finite right central loops

V. S. RAMAMURTHI (Jacksonville, Fl.) and A. R. T. SOLARIN (Ile-Ife)

Abstract. Loops which satisfy the identity $(zy \cdot x)x = z(yx \cdot x)$ are investigated.

Introduction. A set L is called a quasigroup if there is a binary operation $(.)$ defined in L and if the equation $a \cdot b = c$ is uniquely solvable for the third element when any two elements are given. A loop is a quasigroup which has a two-sided identity element. Loops whose elements satisfy the identity $(ab)(ca) = (a(bc))a$ arose in the geometric considerations of MOUFANG (5) and are known as Moufang loops. Im similar considerations, BOL (1) encountered the identity $((ab)c)b = a((bc)b)$. ROBINSON (7) called such loops (right) Bol loops and initiated an algebraic study of such loops. Recently BURN (3) and NIEDERREITER and ROBINSON (6) have carried out deeper investigations into the existence and classification of Bol loops of small orders. It may be noted that the identities mentioned above have the following form: both sides of the identity contain the same three letters taken in the same order but one of them occurs twice on each side. Such identities are said to be of Bol—Moufang type. A study of all possible such identities was undertaken by FENYVES (4) who called a loop satisfying the identity $((zy)x)x = z((yx)x)$ (resp. $x(x(yz) = (x(xy))z$, $((zx)x)y = z(x(xy))$) as a right central loop (resp. left central, central).

Among other things Fenyves established the following in his paper: (i) The right central identity is neither implied by nor implies the Bol identity (ii) Any right central loop has the right inverse property, is right alternative and the square of any element in sucha loop lies in the right nucleus of the loop. (iii) For any two elements x, y in a right central loop, the equation $xy^m \cdot y^n = xy^{m+n}$ holds for all integers m, n. This paper continues Fenyves's investigations. Several characterizations of right central loops are given. It is shown that the order of any element of a right central loop of finite order is a divisor of the order of the loop. It follows from this that any finite right central loop of odd order is associative. In contrast, existence of non-associative right central loops of every even order is established by a construction. Constructions for loops which are both Bol and right central and for loops which are Bol but not right central are also given. The methods of this paper follow those of ROBINSON (7) and BURN (3). For general information on the topic of loops and other binary systems, see BRUCK (2).

Terminology. All loops considered in this paper will be of finite order. The symbol e will denote the identity element. A loop L has the right inverse property if $(yx)z = y(xz)$ whenever $xz = e$; L is right alternative if $(yx)x = y(xx)$ for all y, x in L. The right nucleus of L is the subset $\{x: (yz)x = y(zx)$ for all y, z in $L\}$. The (right regular) representation of L is the set of right multiplications $\{R(u); u$ in $L\}$ where $R(u)(x) = xu$ for each x in L. This set will be denoted by $R(L)$. Given any loop

a ring defining multiplication by

$$(b_1, (\lambda_1, \varrho_1))(b_2, (\lambda_2, \varrho_2)) = (b_1 b_2 + \lambda_1 b_2 + b_1 \varrho_2, (\lambda_1 \circ \lambda_2, \varrho_1 \circ \varrho_2)).$$

The result then follows from the remarks above. We have given this example explicitly, although the result is due to RÉDEI, to compare it with the corresponding result for one-sided ideals, given in Theorem 3.

We recall the definition of the centroid of a ring B. Let E be the endomorphism ring of the additive group of B. For each $b \in B$ the mappings λ_b, ϱ_b defined above belong to E. The centroid of B is the set of all $\alpha \in E$ which commute with all these mappings λ_b, ϱ_b, $b \in B$. This is equivalent to α being a homomorphism of the bimodule ${}_B B_B$. In turn this is equivalent to the statement that α will pair with itself to form a double homothetism (α, α). The above extension then becomes the usual extension of a ring by an element of its centroid.

It is well-known that $A \lhd B$, $B \lhd C$, $A^2 = A$ implies $A \lhd C$. One has $CA = CA^2 \subset CBA \subset BA \subset A$ and a corresponding result for AC. In a private communication PUCZYLOWSKI asked me whether the class of rings R such that $A \cong R$, $A \lhd B$, $B \lhd C$ implies $A \lhd C$ contains any rings R with $R^2 \neq R$. Eventually I found an example which was an extension of $R \oplus (R/R^2)$ by Z, with multiplication defined in an ad hoc manner, which showed that no other such rings exist. When he saw my example Puczylowski was able to construct a better example, noting that the mapping λ from $R \oplus (R/R^2)$ to itself given by $\lambda(a, r + R^2) = (0, a + R^2)$ is an element of the centroid. Using the extension C by this element one sees that if $A = \{(a, 0) | a \in R\}$ and $R^2 \neq R$ then $A \cong R$ and $\lambda A \notin A$. Thus if $B = R \oplus (R/R^2)$ then $A \lhd B$, $B \lhd C$ but A is not an ideal of C. In fact, in this case, it is possible to pair λ with 0 so that $(\lambda, 0)$, $(0, \lambda)$ and (λ, λ) are each double homothetisms. Since $\lambda^2 = 0$ using $(\lambda, 0)$ the ring of double homothetisms consists of all mappings $(n\lambda, 0)$ $n \in Z$. This gives rise to the specific example C on the abelian group $Z \oplus R \oplus (R/R^2)$ with multiplification defined by

$$(n_1, a_1, r_1 + R^2)(n_2, a_2, r_2 + R^2) = (0, a_1 a_2, n_1 a_2 + R^2).$$

In this case $A = \{(0, a, 0 + R^2) | a \in R\}$ is an ideal of $B = \{(0, a, r + R^2) | a, r \in R\}$ and $B \lhd C$, while A is not a left ideal of C. If instead one uses $(0, \lambda)$, A is not a right ideal of C.

For left ideals one can consider the problem $A \lhd_l B$, $B \lhd_l C$ or the intermediate cases $A \lhd B$, $B \lhd_l C$ and $A \lhd_l B$, $B \lhd C$, asking in each case whether one has $A \lhd_l C$. An examination of the above proof and examples shows that in each case the same result holds as for ideals. We may summarize these results as follows.

Theorem 1. *Let R be a rng. Then the following conditions are equivalent: —*

(i) $R^2 = R$,
(ii) $A \lhd B$, $B \lhd C$, $A \cong R$ *implies* $A \lhd C$,
(iii) $A \lhd B$, $B \lhd_l C$, $A \cong R$ *implies* $A \lhd_l C$,
(iv) $A \lhd_l B$, $B \lhd C$, $A \cong R$ *implies* $A \lhd_l C$,
(v) $A \lhd_l B$, $B \lhd_l C$, $A \cong R$ *implies* $A \lhd_l C$.

where A, B, C may vary over all rings satisfying the conditions stated. There are corresponding equivalent conditions for right ideals.

It is well-known that if A is a semi-prime ideal of B and B is an ideal of C then A is an ideal of C. Thus if S is a semi-prime ring, $A \lhd B$, $B \lhd C$ and $B/A \cong S$ then $A \lhd C$. At a conference in Eger, Hungary in 1982 the question was raised as to whether there are any other rings S with this property. It follows from our next theorem that there are such rings.

Theorem 2. *Let S be a ring. Then the following conditions are equivalent:*
(i) *The middle annihilator of S is zero.*
(ii) *$A \lhd B$, $B \lhd C$, $B/A \cong S$ implies $A \lhd C$, where A, B, C may vary over all rings satisfying the stated conditions.*

Proof. Let the ring S have zero middle annihilator. Let A, B, C be rings such that $A \lhd B$, $B \lhd C$ and $B/A \cong S$. Let A^* be the ideal of C generated by A. Then $A^* = (1, C)A(1, C)$ and, as in Andrunakievic' Lemma, we have $BA^*B = B(1, C) \cdot A(1, C)B \subset BAB \subset A$. It follows that A^*/A is contained in the middle annihilator of B/A. Hence $A^* = A$ and A is an ideal of C.

Now let (ii) be satisfied. Let K be the left annihilator of S. Let

$$B = \begin{bmatrix} S & K \\ 0 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & K \\ 0 & 0 \end{bmatrix}.$$

Then $A \lhd B$, $B/A \cong S$. By condition (ii) and Rédei's results, A is invariant under every double homothetism of B. Consider $\varrho: B \to B$ defined by

$$\varrho \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix}$$

for all $x \in S$, $y \in K$. A routine check shows that $(0, \varrho)$ is a double homothetism of B. Since A is invariant under $(0, \varrho)$ we have $A\varrho \subset A$ and so $K = 0$. There is a dual argument showing that S has zero right annihilator. Then $SaS = 0$ implies $Sa = 0$, which implies $a = 0$. Therefore S has zero middle annihilator.

Since we need the quotient ring B/A there is only one corresponding problem here for left ideals; for which rings S does $A \lhd B$, $B \lhd_l C$, $B/A \cong S$ imply $A \lhd_l C$?. This time the answer is not the same as for ideals. There is no result for left ideals corresponding to Andrunakievic' Lemma and the following example shows that the answer is the zero ring only.

Let S be a non-zero ring. Let

$$A = \begin{bmatrix} 0 & 0 \\ (1, S) & 0 \end{bmatrix} \quad B = \begin{bmatrix} S & 0 \\ (1, S) & 0 \end{bmatrix} \quad C = \begin{bmatrix} S & S \\ (1, S) & S \end{bmatrix}.$$

Then $A \lhd B$, $B \lhd_l C$, $B/A \cong S$ and A is not a left ideal of C.

There is a similar example, using rows instead of columns, for right ideals.

Having considered this question for fixed rings A and for fixed rings B/A it is natural to consider it for fixed rings C/B. Again, however, a routine example shows that the answer is the zero ring.

Let T be a non-zero ring.

$$\text{Let} \quad C = \begin{bmatrix} T & (1, T) \\ 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & (1, T) \\ 0 & 0 \end{bmatrix} \quad A = \begin{bmatrix} 0 & Z \\ 0 & 0 \end{bmatrix}$$

where, in this case, by Z we mean the set of elements $\{(n, 0)|n\in Z\}$. Then $A\lhd B$, $B\lhd C$, $C/B\cong T$ and A is not a left ideal of C. This example also shows that the answer is also only the zero ring in the corresponding problem for left ideals. A dual example, using columns instead of rows, gives the same result for right ideals.

Recalling Rédei's result that an ideal A of a ring B is characteristic if and only if A is invariant under all double homothetisms of B we now consider the corresponding results for one-sided ideals. $E(B_B)$ and $E({}_BB)$ denote the rings of endomorphisms of the right B-module B_B and of the left B-module ${}_BB$.

Theorem 3. *Let A be a left ideal of the ring B. Then the following conditions are equivalent:*

(i) $\lambda\in E(B_B)$ *implies* $\lambda A\subset A$,

(ii) $B\lhd_l C$ *implies* $A\lhd_l C$,

where C varies over all rings satisfying this condition. There is a corresponding result for right ideals using $E({}_BB)$.

Proof. Assume that (i) holds and let B be a left ideal of C. Let $c\in C$. Define λ_c by $\lambda_c(x)=cx$ for all $x\in B$. Then $\lambda_c\in E(B_B)$. Hence $cA=\lambda_c A\subset A$. It follows that A is a left ideal of C.

Now assume that (ii) holds. Let $E=E(B_B)$. Let C consist of all pairs (b, λ), $b\in B$, $\lambda\in E$, where addition is defined in C pointwise and multiplication by

$$(b_1, \lambda_1)(b_2, \lambda_2) = (b_1b_2+\lambda_1 b_2, b_1\lambda_2+\lambda_1\circ\lambda_2),$$

where $(b_1\lambda_2)x=b_1(\lambda_2 x)$ for all $x\in B$. A routine verification shows that C is a ring and that the mapping $b\to(b, 0)$ embeds B as a left ideal of C. By condition (ii) the set $\{(a, 0)|a\in A\}$ is a left ideal of C. Then $(0, \lambda)(a, 0)=(\lambda a, 0)$ belongs to this set and so $\lambda A\subset A$ for all $\lambda\in E$.

We may consider instead the situation where $A\lhd_l B$ but B is an ideal of C. Using Redei's methods we see that A is a left ideal of C, for all such C, if and only if $\lambda A\subset A$ for all double homothetisms (λ, ϱ) of B. Since a given mapping $\lambda\in E(B_B)$ need not pair with any $\varrho\in E({}_BB)$ to form a double homothetism this condition is weaker than condition (i) of Theorem 3. The following example shows that the corresponding sets of left ideals in a ring B may be different.

Let F be a field. Let

$$A=\begin{bmatrix}0 & 0\\ F & 0\end{bmatrix}\quad B=\begin{bmatrix}F & 0\\ F & 0\end{bmatrix}\quad C_1=\begin{bmatrix}F & F\\ F & F\end{bmatrix}.$$

Then A is a (left) ideal of B, B is a left ideal of C_1 and A is not a left ideal of C_1. However A is the Jacobson radical of B and, by the Anderson—Divinsky—Sulinski theorem [1], if B is an ideal of C_2 then A is an ideal, and so a left ideal, of C_2. Thus A is invariant under every double homothetism of B, but not under every mapping $\lambda\in E(B_B)$. So, for example, if λ is determined by premultiplication by $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$ then λ will not pair with any $\varrho\in E({}_BB)$ to form a double homothetism.

As is well-known every ideal A in a ring B with 1 is characteristic. Similarly every left ideal A in a ring B with left identity element e satisfies the conditions of Theorem 3. For if $\lambda\in E(B_B)$ and $\lambda(e)=b$ then $\lambda(x)=\lambda(ex)=\lambda(e)x=bx$ for all $x\in B$ and the result follows.

We consider now rings C such that $A \lhd B$, $B \lhd C$ implies $A \lhd C$ and the corresponding cases for one-sided ideals. It is clear that these are the rings such that every (left, right) accessible subring is a (left, right) ideal. The description of these rings which follows is given in terms of elements and so it will not be as straightforward to test a given ring to see if it satisfies these conditions as to test for the conditions in Theorems 1 and 2.

Theorem 4. *Every accessible subring of a ring C is an ideal of C if and only if $(c)=(c)^2+Zc$ for all $c \in C$.*

PROOF. Let every accessible subring of C be an ideal of C and let $c \in C$. Then $(c)^2+Zc \lhd (c) \lhd C$. It follows that $(c)^2+Zc \lhd C$. Since $c \in Zc$ it follows that $(c)^2+Zc=(c)$.

Now let $(c)^2+Zc=(c)$ for every $c \in C$. Let $A \lhd B$, $B \lhd C$. We need to show that $A \lhd C$. Let $D=(1, C)A(1, C)$ be the ideal of C generated by A. Then $D \subset B$, $D^3 \subset A$, $A \lhd D$. Let $c \in A+D^2$. Then $Cc \subset (c)=(c)^2+Zc$. Now $(c) \in D$ and so $(c)^2 \subset D^2$. Therefore $Cc=(c)^2+Zc \subset A+D^2$. By a similar argument $cC \subset A+D^2$. Therefore $A+D^2$ is an ideal of C. Since $A \subset A+D^2 \subset D$ it follows that $A+D^2=D$. Then $D^2=(A+D^2)^2 \subset A+D^3=A$. Hence $A=A+D^2=D$ and $A \lhd C$.

Theorem 5. *Every left accessible subring of a ring C is a left ideal of C if and only if $(c)_l=(c^2)_l+Zc$ for all $c \in C$. There is a corresponding result for right ideals.*

PROOF. Let every left accessible subring of a ring C be a left ideal of C and let $c \in C$. Then $(c^2)_l+Zc \lhd_l (c)_l \lhd_l C$. Therefore $(c^2)_l+Zc \lhd_l C$. Since $c \in Zc$ it follows that $(c^2)_l+Zc=(c)_l$.

Now let $(c)_l=(c^2)_l+Zc$ for all $c \in C$. Let $A \lhd_l B$, $B \lhd_l C$. Let $a \in A$, $c \in C$. Then $ca \in (a)_l=(a^2)_l+Za$. Therefore there exist $d \in C$, m, $n \in Z$ such that $ca=da^2+ +ma^2+na$. From $da \in B$ it follows that $da^2 \in A$. Therefore $ca \in A$ and A is a left ideal of C. It follows that every left accessible subring of C is a left ideal of C.

We note that Theorem 4 involves the square of the ideal generated by c, while Theorem 5 involves the left ideal generated by the square of c. One of our previous examples shows that these differences are essential. As before let F be a field and let

$$A=\begin{bmatrix}0 & 0\\ F & 0\end{bmatrix} \quad B=\begin{bmatrix}F & 0\\ F & 0\end{bmatrix} \quad C=\begin{bmatrix}F & F\\ F & F\end{bmatrix}$$

C is a simple ring with 1. Hence every accessible subring of C is an ideal of C. If $a=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}$, then $a^2=0$ and $(a^2)+Za \neq (a)=C$. $A \lhd_l B$, $B \lhd_l C$ but A is not a left ideal of C. For any left ideal D of C we have $D^2=D$ and so $(c)_l=(c)_l^2=(c)_l^2+Zc$. So neither in Theorem 4 nor in Theorem 5 can one condition be replaced by the other.

Finally we consider some open questions. Given rings R, S, T we have considered $A \lhd B$, $B \lhd C$ where $A \cong R$, $B/A \cong S$, $C/B \cong T$. In Theorems 1 and 2 and a remark after Theorem 2 we have found conditions for this situation to imply $A \lhd C$, firstly for fixed R and all S, T, then for fixed S and all R, T, and then for fixed T and all R, S. It seems natural to ask the same questions for fixed pairs of rings from R, S, T and then for three fixed rings. Satisfactory answers to these questions have not been given so far. We make some observations now on one of them. For given

rings R, S when does $A \lhd B$, $B \lhd C$, $A \cong R$, $B/A \cong S$ imply $A \lhd C$? By Redei's results this is equivalent to the statement that R should be characteristic in every extension by S of R. Given the above situation and an element $c \in C$, left and right multiplication by c will induce mappings λ and ϱ from R/R^2 to S. $A \lhd B$ induces an S-bimodule structure on R/R^2. It is easy to see that λ is a homomorphism of right S-modules whose image is in the right annihilator of S and similar results hold for ϱ, replacing right by left. Other elementary properties may be deduced but these on their own are not necessary and sufficient for the above problem to be solved.

Consider the following examples. Let F be the field of two elements and let

$$S = \begin{bmatrix} F & F \\ 0 & 0 \end{bmatrix}.$$

First let R_1 be the trivial ring, i.e. $R_1^2 = 0$, on the additive cyclic group of order 2. Then taking

$$A_1 = \begin{bmatrix} 0 & 0 & F \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad B_1 = \begin{bmatrix} F & F & F \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad C_2 = \begin{bmatrix} F & F & F \\ 0 & 0 & 0 \\ 0 & F & 0 \end{bmatrix}$$

we have $A_1 \lhd B$, $B_1 \lhd C_1$, $A_1 \cong R_1$, $B_1/A_1 \cong S$. However A_1 is not a right ideal of C_1 and if λ $(=0)$ is induced by left multiplication by c and ϱ is induced by right multiplication by c, where

$$c = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

we have a pair of mappings λ, ϱ not both zero, from $R_1/R_1^2 = R_1$ to S with all the given properties. Now take $R_2 = 2Z$. Then $R_2/R_2^2 \cong R_1$ and so the same mappings λ, ϱ exist as above. Now suppose $A \lhd B$, $B \lhd C$ with $2Z \cong A$ and $S \cong B/A$. Denoting these isomorphisms by α, β let $\alpha 2 = a$ and $\beta \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = b + A$. Now $2S = 0$ implies $2B \subset A$. If $2b = ma$ where m is odd then $a \in 2B$ and so $2B = A$. Then $B \lhd C$ implies $A = 2B \lhd C$. If $2b = ma$, where $m = 2n$, let $f = b - na$. Then $2f = 0$ and $\beta \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = f + A$. Now af, $fa \in A$ and from $2f = 0$ we have $2af = 2fa = 0$. Since $A \cong 2Z$ it follows that $af = fa = 0$. Let $c \in C$. Then $ac \in B$ and $fac = 0$. Since $f + A$ is a left identity element of B/A we have $ac - fac \in A$. Therefore $ac \in A$. $fc \in B$ implies $fac \in A$. Since $ca - fca \in A$ we have $ca \in A$. It follows that $A \lhd C$.

Thus we need conditions on R and S and not just the obvious conditions on R/R^2 and S to solve this problem. Here S has non-zero left annihilator, isomorphic to R/R^2, but S has zero annihilator. If there is a non-zero homomorphism, for given rings R, S, from R/R^2 to the annihilator of S then it is possible to construct an example. Let λ be such a mapping. Let B be the ring direct sum $R \oplus S$, with A the embedding of R in this ring, so that $B/A \cong S$. For each $(r, s) \in R \oplus S$ let $\bar{\lambda}(r, s) = (0, \lambda(r + R^2))$. Then it may be checked that $(\bar{\lambda}, \bar{\lambda})$ is a double homothetism of $R \oplus S$ under which A is not invariant. Thus there exists an extension C of B, with $B \lhd C$, but A not an ideal of C. However we have not managed to find necessary and sufficient conditions for a fixed pair of rings R, S to imply the desired result.

Acknowledgements. I am indebted to RICHARD WIEGANDT both for drawing my attention to the work of Rédei and for valuable consultations and correspondence concerning these results. I also thank the Carnegie Trust of the Universities of Scotland for financial support to allow these consultations to occur.

References

[1] T. ANDERSON, N. DIVINSKY and A. SULINSKI, Hereditary radicals in associative and alternative rings, *Canad. J. Math.* **17** (1965), 594—603.
[2] C. J. EVERETT, An extension theory for rings, *Amer. J. Math.* **64** (1942), 363—370.
[3] G. HOCHSCHILD, Co-homology and representation of associative algebras, *Duke Math. J.* **14** (1947), 921—948.
[4] S. MACLANE, Extension and obstruction for rings, *Illinois J. Math.* **2** (1958), 316—345.
[5] M. PETRICH, Ideal extensions of rings, *Acta Math. Hungar.* **45** (1985), 263—283.
[6] L. RÉDEI, Die verallgemeinerung der Schreierschen Erweiterungstheorie, *Acta Sci. Math. Szeged* **14** (1952), 252—273.
[7] L. RÉDEI, Die Holomorphentheorie für Gruppen und Ringen, *Acta Math. Acad. Sci. Hungar,* **5** (1954), 169—195.
[8] L. RÉDEI, *Algebra*, vol. 1, Oxford (1967).

DEPARTMENT OF MATHEMATICAL SCIENCES
THE UNIVERSITY
DUNDEE

(Received April 11, 1986)