*Matemática Contemporânea, Vol. 16, 93–109*
http://doi.org/10.21711/231766361999/rmc166


# A BRIEF HISTORY OF LOOP RINGS

**Edgar G. Goodaire***

**Abstract**

Given a loop $L$ and a commutative associative ring $R$ with 1, one forms the loop ring $RL$ just as one would form a group ring if $L$ were a group. The theory of group rings has a long and rich history. In this paper, we sketch the history of loop rings which are not associative from early results of R. H. Bruck and L. J. Paige through the more recent discovery of alternative and right alternative rings and the work of O. Chein, D. A. Robinson and the author.

## 1. Origins

**Definition 1.1.** *A loop is an algebraic structure* $(L, \cdot)$ *with a two-sided identity element such that*

$$R(x) \colon a \mapsto a \cdot x \qquad \textit{right translation}$$
$$L(x) \colon a \mapsto x \cdot a \qquad \textit{left translation}$$

*are permutations of* $L$*, equivalently, such that the equations* $a \cdot x = b$ *and* $y \cdot a = b$ *have unique solutions* $x$ *and* $y$ *for any* $a, b \in L$.

Thus a group is just an associative loop. Two sources of information about loops in general are [Bru58] and [Pfl90]. We shall have reason to refer to the *commutator* of two elements $a$ and $b$ in a loop $L$ and to the *associator* of three elements $a, b, c$, these being the elements $(a, b)$ and $(a, b, c)$ defined, respectively, by

$$ab = ba(a, b) \quad \text{and} \quad (ab)c = [a(bc)](a, b, c).$$

*This paper is an expanded form of a talk given at the XVth Escola de Álgebra, Canela, Brazil, July 27, 1998

1991 *Mathematics Subject Classification*: Primary 17D05; Secondary 20N05, 16U80

Given a commutative and associative ring $R$ with 1, we form the *loop ring* $RL$ just as we would form the group ring if $L$ were a group. Thus $RL$ is the free $R$-module with the elements of $L$ as basis and, for $\alpha = \sum_{g\in L}\alpha_g g$ and $\beta = \sum_{g\in L}\beta_g g$ in $RL$, $\alpha+\beta$ and $\alpha\beta$ are defined by

$$\begin{aligned}\alpha+\beta &= \sum_{g\in L}(\alpha_g+\beta_g)g,\\ \alpha\beta &= \sum_{g\in L}\Big(\sum_{hk=g}\alpha_h\beta_k\Big)g.\end{aligned}$$

The history of group rings (the case that $L$ is a group) is well-documented. In particular, we draw the reader's attention to the accounts of C. Polcino Milies [Mil81] and R. Sandling [San81, San85]. To my knowledge, the concept of a nonassociative loop ring first made its appearance in a paper by R. H. Bruck in 1944 [Bru44].

**Theorem 1.2** (Bruck; 1944). *If $L$ is any finite loop and $F$ is a field of characteristic 0 or of positive characteristic relatively prime to the order of the multiplication group of $L$, then $FL$ is the direct sum of simple algebras.*

(The multiplication group $\mathrm{Mult}(L)$ of a loop $L$ is the subgroup of the symmetric group on $L$ generated by the translation maps.)

This version of the theorem of H. Maschke about group algebras [Pas77] is remarkable in its generality, although it raises an interesting question. Recall that Maschke's Theorem asserts that a group algebra $FG$ is semisimple if $G$ is finite and the field $F$ has characteristic 0 or $p>0$ relatively prime to $|G|$ (not to $|\mathrm{Mult}(G)|$).

**Question 1.3.** If $L$ is a finite loop and $F$ a field of positive characteristic relatively prime to $|L|$, is $FL$ the direct sum of simple algebras?

For any group $G$, a *class sum* is the sum of the elements in a finite conjugacy class. Such sums are known to span the centre of $RG$, for any coefficient ring $R$ [Pas77] . The notion of conjugacy has an extension to loops [GjM96] and

R. H. Bruck revealed that the group ring result about the centre has a natural extension [Bru46].

**Theorem 1.4** (Bruck; 1946). *The centre of a loop algebra is spanned by conjugacy class sums.*

Now it is "clear" that a loop $RL$ is associative (commutative) if and only if $L$ is associative (commutative). The argument in the case of associativity proceeds as follows.

Let $[x, y, z] = (xy)z - x(yz)$ denote the *(ring) associator* of $x$, $y$, and $z$. If $\alpha = \sum \alpha_g g$, $\beta = \sum \beta_g g$ and $\gamma = \sum \gamma_g g$ are elements of $RL$,

$$[\alpha, \beta, \gamma] = \sum_{g,h,k \in L} \alpha_g \beta_h \gamma_k [g, h, k],$$

so $[\alpha, \beta, \gamma] = 0$ for all $\alpha, \beta, \gamma \in RL$ if and only if $[g, h, k] = 0$ for all $g, h, k \in L$.

The associative and commutative identities are very special, however. In general, an identity in $L$ does not lift to $RL$ and an identity on $RL$ imposes much more than simply the same identity on $L$. Lowell Paige gave a striking example of this phenomenon in 1955 [Pai55].

**Theorem 1.5** (Paige; 1955). *If $R$ is a ring of characteristic relatively prime to 30 and $L$ is a loop such that $RL$ is commutative and power associative, then $L$ is a group.*

Marshall Osborn was the first to notice that there were some minor difficulties with Paige's proof, which assumes characteristic different from only 2 [Osb84]. We refer the reader to [GJM96] for a proof of the theorem as stated.

## 2. The right Moufang identity

**Definition 2.1.** *The right Moufang identity is $((xy)z)y = x(y(zy))$. A Moufang loop is a loop which satisfies this identity.*

As the name suggests, the Moufang identity is named for Ruth Moufang who discovered it in some geometrical investigations in the first half of this century [Mou33]. There is an excellent account of this work in Marshall Hall's text [Hal59, Chapter 20]. Any group is a Moufang loop, but here is a family of Moufang loops which are not associative, discovered by Orin Chein [Che74].

**Example 2.2.** Let $G$ be a nonabelian group and let $u$ be an indeterminate. Let $L = G \cup Gu$ and extend the multiplication in $G$ to $L$ by means of the rules

$$\begin{array}{rcl} g(hu) &=& (hg)u, \\ (gu)h &=& (gh^{-1})u, \\ (gu)(hu) &=& h^{-1}g. \end{array}$$

We denote this loop $M(G)$ and observe, in passing, that the smallest Moufang loop (which is not a group) is $M(S_3)$, of order 12 [CP71].

If $L$ is Moufang, it is highly unlikely that $RL$ also satisfies the Moufang identity. The problem is the repeated variable in the Moufang identity.

Suppose $A$ is a ring satisfying $((xy)z)y = x(y(zy))$. Then, replacing $y$ by $y + w$,[1] we see that $A$ must also satisfy

$$\{[x(y+w)]z\}(y+w) = x\{[y+w][z(y+w)]\},$$

which is

$$\begin{aligned} ((xy)z)y + ((xy)z)w + ((xw)z)y \;\; + \;\; ((xw)z)w &= x(y(zy)) + x(y(zw)) \\ &+ x(w(zy)) + x(w(zw)). \end{aligned}$$

After cancelling two pairs of equal terms, we get

$$((xy)z)w + ((xw)z)y = x(y(zw)) + (x(w(zy)). \tag{2.1}$$

If $A = RL$ is a loop ring and $x, y, z, w$ are in $L$, then recalling that the elements of $L$ are linearly independent over $R$ and noting that each side of (2.1) is the sum of loop elements, we see that the element $((xy)z)w$ must equal (at least) one of the other three elements in this equation, and there is no reason for this to be the case.

[1] in nonassociative algebra, this process is known as *linearization*

Suppose $A$ is any ring with 1 satisfying the Moufang identity $((xy)z)y = x(y(zy))$. Setting $z = 1$ gives $(xy)y = xy^2$ or, equivalently, $[x, y, y] = 0$. This is known as the *right alternative identity.* Setting $x = 1$ in the Moufang identity gives $(yz)y = y(zy)$. Thus $A$ satisfies the *flexible identity* $[y, z, y] = 0$.

Linearizing $[x, y, x] = 0$ gives $[x, y, z] + [z, y, x] = 0$, and then setting $z = y$ gives $[x, y, y] + [y, y, x] = 0$. Since $[x, y, y] = 0$, so also $[y, y, x] = 0$. Thus $A$ also satisfies the *left alternative identity.* As a ring satisfying both alternative identities, $A$ is an *alternative ring*, the name deriving from the fact that in an alternative ring, the associator $[x, y, z]$ is an alternating function of its arguments.

Any associative ring is alternative. An example which is not associative is the real division algebra of Cayley numbers, $\mathcal{C}$, which are defined as follows.

Let $\mathsf{H}$ denote the real quaternion algebra and let $\ell$ be an indeterminate. Then $\mathcal{C} = \mathsf{H} + \mathsf{H}\ell$ with multiplication defined by

$$(a + b\ell)(c + d\ell) = (ac - \overline{d}b) + (da + b\overline{c})\ell,$$

$a, b, c, d \in \mathsf{H}$. (Here, $q \mapsto \overline{q}$ denotes the standard conjugation in $\mathsf{H}$.) We would be remiss at this point in continuing without drawing the reader's attention to the beautiful exposition on the Cayley numbers by Erwin Kleinfeld [Kle63].

We have now seen that if the Moufang identity on $L$ extends to a loop ring $RL$, then $RL$ must be an alternative ring. We have already seen that this is unlikely. The first theorem making this statement precise appeared in an article by the author in 1983 [Goo83].

**Theorem 2.3** (Goodaire; 1983). *If $R$ is a ring of characteristic different from 2, then $RL$ is alternative if and only if*

*i. if $x, y, z \in L$ associate in some order, they associate in all orders, and*

*ii. if $x, y, z \in L$ do not associate, then $(xy)z = x(zy) = y(xz)$.*

Subsequent collaboration with Orin Chein yielded more satisfying information about *RA loops* (as those loops which are described by Theorem 2.3 but are not groups soon came to be known) [CG86].

**Theorem 2.4** (Chein, Goodaire; 1986). *Let $R$ be a commutative and associative ring with 1 and of characteristic different from 2 and let $L$ be a loop. Then the loop ring $RL$ is alternative but not associative (that is, $L$ is $RA$) if and only if $|L'| = 2$ and $L$ has the property that $gh = hg$ for $g, h \in L$ if and only if $g$, $h$ or $gh$ is central.*

(Here $L'$ denotes the subloop of a loop $L$ generated by all commutators and associators.)

The paper [CG86] implicitly contained more information about the structure of an RA loop, and this was made explicit in the introduction to a paper with M. M. Parmenter [GP87].

**Theorem 2.5** (Chein, Goodaire). *An RA loop $L$ has the following structure:*

- *$L = G \cup Gu$ where $G$ is a nonabelian group and $u \notin G$;*
- *$G$ has an involution $g \mapsto g^*$ (that is, an antiautomorphism of period 2) such that $gg^*$ is in the centre of $G$ for each $g \in G$;*
- *multiplication in $L$ is given by the rules*

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= g_0 h^* g \end{aligned}$$

*for $g, h \in G$, where $u^2 = g_0$ is central in $G$ and $g_0^* = g_0$.*

*Conversely, if $G$ is a nonabelian group with $|G'| = 2$ and the property that $g, h \in G$ commute if and only if $g$, $h$ or $gh$ is central, then $G$ has an involution $*$ with $gg^*$ central for all $g \in G$ and the loop constructed as above has an alternative loop ring.*

The loop described by this theorem is labelled $M(G, *, g_0)$. Note how strikingly similar these loops are to those described in Example 2.2. In fact, $M(G)$ is just the special case $(M, -1, 1)$, where "$-1$" refers to the involution $g \mapsto g^{-1}$.

There is an interesting side issue raised by Theorems 2.3, 2.4 and 2.5. We have noted that the loop ring of a given Moufang loop is unlikely to be alternative. We can still ask, however, whether a given Moufang loop is a subloop of the loop of units of some alternative ring. The answer to this question is trivial for groups, but apparently not otherwise. Very little attention seems to have been given to this problem. There is a mildly negative result implicit in [GM89]. If $\alpha$ is a unit of augmentation one in an integral alternative loop ring $\mathsf{Z}L$, there are units $\gamma_1, \gamma_2$ in the rational loop algebra $\mathsf{Q}L$ such that $\gamma_2^{-1}(\gamma_1^{-1}\alpha\gamma_1)\gamma_2$ is in $L$. (Thus, a variation of a conjecture of H. Zassenhaus for group rings holds for alternative loop rings which are not associative [RS83].) Since elements of odd order in an RA loop are central, the following theorem is immediate.

**Theorem 2.6** (Goodaire, Polcino Milies). *The integral alternative loop ring* $\mathsf{Z}L$ *of a finite loop L (which is not associative) does not contain noncentral elements of finite odd order.*

Thus, for example, $M(S_3)$ is not contained in any integral alternative loop ring. It is, however, contained in *Zorn's Vector Matrix Algebra* $\mathfrak{Z}(\mathsf{Q})$ over the rationals and this suggests an investigation of the subloops of $\mathfrak{Z}(\mathsf{Q})$ reminiscent of Behnam Banieqbal's classification of the finite subgroups of $M_2(\mathsf{Q})$ [Ban88].

Zorn's vector matrix algebra, $\mathfrak{Z}(\mathsf{R})$, over a ring $R$ is the set of matrices of the form

$$\begin{bmatrix} a & \mathsf{x} \\ \mathsf{y} & b \end{bmatrix}$$

where $a, b \in R$ and $\mathsf{x}, \mathsf{y} \in R^3$. One adds such matrices entry by entry in the obvious way, but multiplies according to the following variation of the usual rule:

$$\begin{bmatrix} a_1 & \mathsf{x}_1 \\ \mathsf{y}_1 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & \mathsf{x}_2 \\ \mathsf{y}_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + \mathsf{x}_1 \cdot \mathsf{y}_2 & a_1\mathsf{x}_2 + b_2\mathsf{x}_1 - \mathsf{y}_1 \times \mathsf{y}_2 \\ a_2\mathsf{y}_1 + b_1\mathsf{y}_2 + \mathsf{x}_1 \times \mathsf{x}_2 & b_1b_2 + \mathsf{y}_1 \cdot \mathsf{x}_2 \end{bmatrix}$$

where $\mathsf{x}\cdot\mathsf{y}$ and $\mathsf{x}\times\mathsf{y}$ denote, respectively, the dot and cross products of $\mathsf{x}, \mathsf{y} \in R^3$. Under these operations, $\mathfrak{Z}(\mathsf{R})$ is an alternative ring and one which often occurs as the simple component in a rational alternative loop algebra [GJM96, Section VII.2].

## 3. RA2 Loops

Another way to determine which Moufang loops are subloops of the unit loop of an alternative ring is to consider loop rings in characteristic 2. In fact, in characteristic 2 "many" Moufang loops have alternative loop rings. For instance, of the 158 Moufang loops of order less than 64 (which are not groups) [Che78], just 10 are RA while 64 are *RA2*, in the sense that they have alternative loop rings which are not associative in characteristic 2. Unfortunately, there is as yet no characterization of RA2 loops in the spirit of Theorems 2.4 or 2.5. The analogue of Theorem 2.3 is this [CG90b].

**Theorem 3.1** (Chein, Goodaire). *Assume $R$ has characteristic 2. Then $RL$ is right alternative if and only if $L$ is right alternative and, for every three elements $x, y, z \in L$, one of the following three conditions holds:*

$$\begin{array}{lrclcrcl} A(x,y,z): & (xy)z & = & x(yz) & \text{and} & (xz)y & = & x(zy) \\ B(x,y,z): & (xy)z & = & x(zy) & \text{and} & x(yz) & = & (xz)y \\ C(x,y,z): & (xy)z & = & (xz)y & \text{and} & x(yz) & = & x(zy). \end{array}$$

*Also, $RL$ is left alternative if and only if $L$ is left alternative and, for every three elements $x, y, z \in L$, one of the $D(x,y,z)$, $E(x,y,z)$, $F(x,y,z)$ holds:*

$$\begin{array}{lrclcrcl} D(x,y,z): & (xy)z & = & x(yz) & \text{and} & (yx)z & = & y(xz) \\ E(x,y,z): & (xy)z & = & y(xz) & \text{and} & x(yz) & = & (yx)z \\ F(x,y,z): & (xy)z & = & (yx)z & \text{and} & x(yz) & = & y(xz). \end{array}$$

For Moufang loops, there is a substantial improvement. If a Moufang loop has a right alternative loop ring, then this ring is necessarily alternative [CG88] and so a Moufang loop $L$ has an alternative loop ring (in characteristic 2) if and only if for every three elements $x, y, z \in L$ which do not associate, either $B(x,y,z)$ or $C(x,y,z)$.

While there is no "nice" characterization of RA2 loops, much is known about their structure. An RA2 loop, for instance, contains a normal subloop which is an abelian group with quotient an elementary abelian 2-group. This was key to proving that the augmentation ideal of certain alternative loop rings in characteristic 2 is nilpotent [Goo95].

It is easy to produce families of RA2 loops:

- any Moufang loop with a unique commutator/associator [CG90c];
- more generally, any Moufang loop with precisely two squares [CG90a];
- certain loops of the form $M(G,*,g_0)$.

In fact, there is a very satisfying characterization of RA2 loops of the form $M(G,*,g_0)$ which we proceed to describe. Suppose then that $L = M(G,*,g_0)$ is RA2. The first thing to notice is that elements of the loop ring $RL$ can be written in the form $x + yu$, where $x$ and $y$ are in the group ring $RG$. Then, after extending the involution from $G$ to $RG$ in the obvious way, multiplication in $RL$ strongly resembles multiplication in the Cayley numbers:

$$(x + yu)(z + wu) = (xz + g_0 w^* y) + (wx + yz^*)u.$$

It involves only a straightforward calculation to show that $RL$ is alternative if and only if $g + g^*$ is central for all $g \in G$; that is, if and only if

$$g + g^* = h^{-1}(g + g^*)h = h^{-1}gh + h^{-1}g^*h.$$

for every $h \in G$.

In characteristic 2, this leads to an entirely group-theoretical question. What nonabelian groups $G$ have the property that they possess an involution such that for every $g \in G$, either $g^* = g$ or else $h^{-1}gh \in \{g, g^*\}$ for every $h \in G$?

First notice that in such a group $G$, $g$ and $g^*$ commute for every $g \in G$. This is certainly true if $g = g^*$. On the other hand, if $g \neq g^*$, then $g^{-1}g^*g \in \{g^*, (g^*)^*\} = \{g, g^*\}$ and $g^{-1}g^*g = g$ cannot be the case since $g \neq g^*$. Thus $g^{-1}g^*g = g^*$.

Now look at the complement of the set of fixed points of the involution, that is, the set

$$T = \{g \in G \mid g^* \neq g\}.$$

Let $A = \langle T \rangle$ be the subgroup of $G$ generated by $T$. Fix $t \in T$ and let $x$ be an element not in $A$. Then $tx \notin T$, so $tx = (tx)^* = x^* t^* = xt^*$ and $t^* = x^{-1}tx$. Similarly, $x^{-1}t^*x = t$. It follows that if $y$ is another element not in $A$, then $xy$ must belong to $A$ because

$$(xy)^{-1}t(xy) = y^{-1}x^{-1}txy = y^{-1}t^*y = t.$$

Thus $A$ has index at most 2 in $G$ and so, if $T$ is a commutative set, then $A$ has index two (because $A$ is abelian and $G$ is not).

Suppose now that $T$ is not commutative. Fix $s, t \in T$ with $st \neq ts$. Then $sts^{-1} \neq t$, so $sts^{-1} = t^*$, that is, $st = t^*s$. Similarly, since $t^{-1}st \neq s$, we have $st = ts^*$. So $t^*s = ts^*$, $t^{-1}t^* = s^*s^{-1} = s^{-1}s^*$ ($s$ and $s^*$ commute). Hence

$$(s,t) = s^{-1}t^{-1}st = s^{-1}s^* = t^{-1}t^* = t^{-1}s^{-1}ts = (t,s), \tag{3.1}$$

$(a,b)$ denoting the group commutator $a^{-1}b^{-1}ab$.

Let $f = (s,t)$ and note that $f^{-1} = f$. Let $x$ be any element of $T$. If $x$ fails to commute with $s$, say, as before we can deduce that $x^{-1}x^* = s^{-1}s^*$ giving $x^{-1}x^* = f$. Thus, if $x^{-1}x^* \neq f$, then $x$ must commute with both $s$ and $t$. Suppose $(sx)^* \neq sx$. Then

$$t^{-1}(sx)t = sx \text{ or } (sx)^*(= x^*s^* = s^*x^*)$$

while

$$t^{-1}(sx)t = (t^{-1}st)(t^{-1}xt) = s^*x$$

contradicting the fact that $s^*x \notin \{sx, s^*x^*\}$. Thus $(sx)^* = sx$, which implies $x^*s^* = sx = xs$ and

$$x^{-1}x^* = s(s^*)^{-1} = (s^*)^{-1}s = f^{-1} = f.$$

All this shows that $f = x^{-1}x^*$ is independent of $x \in T$. We claim that $f$ is the only nonidentity commutator in $G$.

For this, let $x, y \in G$ with $xy \neq yx$. If $x \in T$, then, as above, $x^{-1}y^{-1}xy = x^{-1}x^* = f$. If $x \notin T$ and $y \in T$, then

$$x^{-1}y^{-1}xy = (y^{-1}x^{-1}yx)^{-1} = (y^{-1}y^*)^{-1} = f^{-1} = f,$$

while if $y \notin T$, then $xy \in T$; otherwise, $(xy)^* = xy$, so $yx = y^*x^* = (xy)^* = xy$, contradicting the fact that $x$ and $y$ do not commute. So $xy \in T$ and $(xy)x \neq x(xy)$. We have already considered this possibility and found $(xy, x) = f$. Since $(xy, x) = (y, x)$, we get $(y, x) = f$, so $(x, y) = f^{-1} = f$.

**Theorem 3.2.** *Let $L = M(G, *, g_0)$ be an RA2 loop. Then either $G$ has an abelian subgroup of index 2 or $|G'| = 2$.*

Conversely, given any group with an abelian subgroup of index 2 or $|G'| = 2$, there exists an involution $*$ on $G$ such that $M(G, *, g_0)$ is RA2. We refer the reader to [Goo91] for more details.

## 4. The right Bol identity

**Definition 4.1.** *The* right Bol identity *is $((xy)z)y = x((yz)y)$. A (right) Bol loop is a loop which satisfies this identity.*

Note the subtle distinction between the right Bol and the right Moufang identity which, recall, is $((xy)z)y = x(y(zy))$. The Moufang identity implies flexibility—$(yz)y = y(zy)$—which the Bol identity does not.

Many loop identities arose or have been studied in a geometrical setting. The Bol identity was first investigated by Gerrit Bol [Bol37] who showed that it corresponds to a certain configuration in 3-webs [Pfl90, Section II.3]. Michael Kallaher and Ted Ostrom studied quasifields whose multiplicative loop satisfies the right Bol identity [KO71].

Any Moufang loop is a Bol loop. The smallest order of a Bol loop (which is not Moufang) is eight. There are six such loops [Bur78], one of which is $\mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2$ with multiplication defined by

$$(i, j, k)(p, q, r) = (i + p, j + q, k + r + jp(q + 1)).$$

The multiplication table for this loop

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 2 | 1 | 6 | 7 | 8 | 3 | 4 | 5 |
| 3 | 3 | 6 | 1 | 8 | 4 | 2 | 5 | 7 |
| 4 | 4 | 7 | 5 | 1 | 3 | 8 | 2 | 6 |
| 5 | 5 | 8 | 4 | 6 | 1 | 7 | 3 | 2 |
| 6 | 6 | 3 | 2 | 5 | 7 | 1 | 8 | 4 |
| 7 | 7 | 4 | 8 | 2 | 6 | 5 | 1 | 3 |
| 8 | 8 | 5 | 7 | 3 | 2 | 4 | 6 | 1 |

shows clearly that loops of exponent two need not be commutative! As defined here, this loop was discovered by D. A. Robinson whose pioneering work [Rob66] is still the standard reference for Bol loops.

Here is a class of Bol loops which are not Moufang.

**Example 4.2.** Let $S$ be any associative ring which contains an element $k$ of additive order 2. Assume there exist $b, c \in S$ such that $k(bcb + b^2c) \neq 0$. Let $L = S \times S$ and define multiplication by

$$(a, \alpha)(b, \beta) = (a + b, \alpha + \beta + kab^2).$$

Then $L$ is (right) Bol, but not Moufang.

The right Bol identity implies the right alternative identity: putting $z = 1$ in $((xy)z)y = x((yz)y)$ gives $(xy)y = xy^2$. Are there loop rings which are right alternative but not alternative? Interestingly, we are immediately restricted to characteristic 2 because of a recent result of Kenneth Kunen [Kun98].

**Theorem 4.3.** *Suppose $RL$ satisfies the right alternative identity and $1+1 \neq 0$ in $R$. Then $RL$ satisfies the left alternative identity; hence $RL$ is an alternative ring.*

Unfortunately, this causes additional complications. In characteristic different from 2, a ring is right alternative if and only if it satisfies the right Bol identity. This is not true, however, in characteristic 2, however. Indeed, Kunen has an example of a loop ring which is right alternative but does not even satisfy $x^2x = xx^2$. So, if we want $RL$ to satisfy the right Bol identity, then we need a stronger version of Theorem 3.1. This was given by the author and D. A. Robinson who suggested the acronym *SRAR—strongly right alternative ring*—to describe a loop whose loop rings (in characteristic 2) satisfy the right Bol identity but are not alternative [GR95].

**Theorem 4.4** (Goodaire, Robinson; 1996). *A loop $L$ is SRAR if and only if, for every $x$, $y$, $z$ and $w$ in $L$, one of the following three conditions is satisfied:*

$$P(x,y,z,w) : ((xy)z)w = x((yz)w) \quad \text{and} \quad ((xw)z)y = x((wz)y)$$
$$Q(x,y,z,w) : ((xy)z)w = x((wz)y) \quad \text{and} \quad ((xw)z)y = x((yz)w)$$
$$R(x,y,z,w) : ((xy)z)w = ((xw)z)y \quad \text{and} \quad x((yz)w) = x((wz)y).$$

This theorem would appear to make the possibility of classification rather remote. It would be lovely if we had a positive answer to the next question, for then we could use the first part of Theorem 3.1 rather than the more complicated Theorem 4.4 in our search for SRAR loops and a potential classification.

**Question 4.5.** If $L$ is a Bol loop satisfying $A(x,y,z)$, $B(x,y,z)$ or $C(x,y,z)$ for each $x, y, z \in L$, does $RL$ satisfy the right Bol identity?

At the moment, only one class of SRAR loops has been identified [GR96].

**Theorem 4.6.** *Let $R$ be a commutative, associative ring with* 1 *and of characteristic* 2. *If $L$ is a Bol loop with $|L'| = 2$, then $RL$ satisfies the right Bol identity and it is not alternative.*

In particular, all six Bol loops of order eight have this property. Another example can be obtained by means of the construction in Example 4.2.

**Example 4.7.** Let

$$S = \begin{bmatrix} \mathsf{Z}_{2n} & \mathsf{Z}_{2n} \\ 0 & \mathsf{Z}_{2n} \end{bmatrix} \quad \text{and} \quad k = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}.$$

Then $S$ satisfies the conditions of Example 2.2 with

$$b = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad c = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

So the Bol loop $L$ described there is not Moufang. It is easy to check that $L' = \{(0,0),(0,k)\}$ and so $RL$ satisfies the right Bol identity.

## References


**[Ban88]** Banieqbal, B., *Classification of finite subgroups of* $2\times 2$ *matrices over a division algebra of characteristic* 0, J. Algebra 119 (1988), 449–512.

**[Bol37]** Bol, G., *Gewebe und Gruppen*, Math. Ann. 114 (1937), 414–431.

**[Bru44]** Bruck, R. H., *Some results in the theory of linear nonassociative algebras*, Trans. Amer. Math. Soc. 56 (1944), 141–199.

**[Bru46]** Bruck, R. H., *Contributions to the theory of loops*, Trans. Amer. Math. Soc. 60 (1946), 245–354.

**[Bru58]** Bruck, R. H., *A survey of binary systems*, Ergeb. Math. Grenzgeb., vol. 20, Springer-Verlag, 1958.

**[Bur78]** Burn, R. P., *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. 84 (1978), 377–385.

**[CG86]** Chein, O. and Goodaire, E. G., *Loops whose loop rings are alternative*, Comm. Algebra 14 (1986), no. 2, 293–310.

**[CG88]** Chein, O. and Goodaire, E. G., *Is a right alternative loop ring alternative?*, Algebras Groups Geom. 5 (1988), 297–304.

**[CG90a]** Chein, O. and Goodaire, E. G., *Code loops are $RA2$ loops*, J. Algebra 130 (1990), no. 2, 385–387.

**[CG90b]** Chein, O. and Goodaire, E. G., *Loops whose loop rings in characteristic* 2 *are alternative*, Comm. Algebra 18 (1990), no. 3, 659–688.

**[CG90c]** Chein, O. and Goodaire, E. G., *Moufang loops with a unique nonidentity commutator (associator, square)*, J. Algebra 130 (1990), no. 2, 369–384.

**[Che74]** Chein, O., *Moufang loops of small order I*, Trans. Amer. Math. Soc. 188 (1974), 31–51.

**[Che78]** Chein, O., *Moufang loops of small order*, Mem. Amer. Math. Soc. 13 (1978), no. 197, 1–131.

**[CP71]** O. Chein and Pflugfelder, H . O., *The smallest Moufang loop*, Arch. Math. (Basel) 22 (1971), 573–576.

**[GJM96]** Goodaire, E. G., Jespers, E. and Polcino Milies, C., *Alternative loop rings*, North-Holland Math. Studies, vol. 184, Elsevier, Amsterdam, 1996.

**[GM89]** Goodaire, E. G. and Polcino Milies, C., *Torsion units in alternative loop rings*, Proc. Amer. Math. Soc. 107 (1989), 7–15.

**[Goo83]** Goodaire, E. G., *Alternative loop rings*, Publ. Math. Debrecen 30 (1983), 31–38.

**[Goo91]** Goodaire, E. G., *Groups embeddable in alternative loop rings*, Contributions to General Algebra 7 (1991), 169–176.

**[Goo95]** Goodaire, E. G., *The radical of a modular alternative loop algebra*, Proc. Amer. Math. Soc. 123 (1995), no. 11, 3289–3299.

**[GP87]** Goodaire, E. G. and Parmenter, M. M., *Semi-simplicity of alternative loop rings*, Acta Math. Hungar. 50 (1987), no. 3–4, 241–247.

**[GR95]** Goodaire, E. G. and Robinson, D. A., *A class of loops whose loop rings are strongly right alternative*, Comm. Algebra 22 (1995), no. 14, 5623–5634.

**[GR96]** Goodaire, E. G. and Robinson, D. A., *A construction of loops which admit right alternative loop rings*, Resultate Math. 59 (1996), 56–62.

**[Hal59]** Hall Jr., M., *The theory of groups*, MacMillan, New York, 1959.

**[Kle63]** Kleinfeld, E., *A characterization of the Cayley numbers*, Studies in modern algebra (A. A. Albert, ed.), Studies in Mathematics, vol. 2, Math. Assoc. of America, 1963, pp. 126–143.

**[KO71]** Kallaher, M. J. and Ostrom, T. G., *Fixed point free linear groups, rank three planes and Bol quasifields*, J. Algebra 18 (1971), 159–178.

**[Kun98]** Kunen, K., *Alternative loop rings*, Comm. Algebra 26 (1998), 557–564.

**[Mil81]** Polcino Milies, C., *Units of group rings—a short survey*, Groups–St. Andrew's 1981 (Cambridge–New York), London Math. Soc. Lecture Notes, vol. 71, Cambridge University Press, Cambridge–New York, 1981, pp. 281–297.

**[Mou33]** Moufang, R., *Alternativkörper und der Satz vom vollständigen Vierseit ($D_9$)*, Abh. Math. Sem. Univ. Hamburg 9 (1933), 207–222.

**[Osb84]** Osborn, J. M., *Lie-admissible noncommutative Jordan loop rings*, Algebras Groups Geom. 1 (1984), 453–489.

**[Pai55]** Paige, L. J., *A theorem on commutative power associative loop algebras*, Proc. Amer. Math. Soc. 6 (1955), 279–280.

**[Pas77]** Passman, D. S., *The algebraic structure of group rings*, Wiley-Interscience, New York, 1977.

**[Pfl90]** Pflugfelder, H. O., *Quasigroups and loops: Introduction*, Heldermann Verlag, Berlin, 1990.

**[Rob66]** Robinson, D. A., *Bol loops*, Trans. Amer. Math. Soc. 123 (1966), 341–354.

**[RS83]** Ritter, J. and Sehgal, S. K., *On a conjecture of Zassenhaus on torsion units in integral group rings*, Math. Ann. 264 (1983), 257–270.

**[San81]** Sandling, R., *Graham Higman's thesis "Units in group rings"*, Integral representations and applications (Oberwolfach, 1980) (Berlin–New York), Lecture Notes in Math., vol. 882, Springer, Berlin–New York, 1981, pp. 93–116.

**[San85]** Sandling, R., *The isomorphism problem for group rings: a survey*, Lecture Notes in Math., vol. 1141, Springer, Berlin, 1985.

Memorial University of Newfoundland
St. John's, Newfoundland
Canada A1C 5S7
*email*: edgar@math.mun.ca