THE RADICAL OF A MODULAR ALTERNATIVE LOOP ALGEBRA

EDGAR G. GOODAIRE

(Communicated by Lance W. Small)

ABSTRACT. If G is a group of order 2^n and F is a field of characteristic 2, it is well known that the augmentation ideal of the group algebra FG is nilpotent. In this paper, we extend this result to alternative loop algebras.

1. INTRODUCTION

A *loop* is a binary system $(L, \cdot)$ with an identity element 1 in which, given any two of three elements a, b, c in L, the third is uniquely determined by the equation $a \cdot b = c$. This paper is concerned with *Moufang* loops; that is, loops in which any one of the following three (equivalent) identities is valid.

$$
\begin{aligned}
x(y \cdot xz) &= (xy \cdot x)z & \text{the left Moufang identity,} \\
(xy \cdot z)y &= x(y \cdot zy) & \text{the right Moufang identity,} \\
xy \cdot zx &= (x \cdot yz)x & \text{the middle Moufang identity.}
\end{aligned}
$$

Over any commutative and associative ring R with identity (which we also denote by 1), one can form the *loop ring* RL in precisely the same manner that the group ring is constructed, but, in sharp contrast with the associative law, the Moufang identities do not usually lift to the loop ring. When they do, the left Moufang identity (with $y = 1$) implies the left alternative law— $x(xz) = x^2z$—and the right Moufang identity implies the right alternative law— $(xy)y = xy^2$—and the loop ring is, by definition, an *alternative ring*.

Moufang loops whose loop rings are alternative, but not associative, have been objects of study for the past dozen years. Over coefficient rings of characteristic different from 2 (where they are called *RA loops*) they have been completely classified [4]. Since the elements of odd order split from an RA loop as a direct factor, those RA loops of primary interest are 2-loops. As might be expected, over fields of characteristic different from 2, loop algebras of RA 2-loops are semi-simple. This is a general result of Bruck's for arbitrary loop algebras [1], but it also follows from work of Parmenter and the author [8] where

the semi-simplicity of an alternative loop ring, with respect to a variety of radi-
cals, was linked to the semi-simplicity of the group ring of a certain associative
subloop of the loop.

In this paper, we investigate the case where the field has characteristic 2 and
extend to alternative loop algebras a well-known result of Jennings [9] for group
algebras by proving that the augmentation ideal of the alternative loop algebra
of a loop of order 2^n in characteristic 2 is a nilpotent ideal (of dimension $2^n -
1$). This, of course, means that virtually all the familiar radicals of alternative
algebras coincide with the augmentation ideal. In characteristic 2, the class of
Moufang loops whose loop rings are alternative is much broader than the class
of RA loops [5] and, while this broader class is not yet completely understood, it
is pleasing that we are able to prove enough about these RA2 *loops*, as they have
been termed, that we can start to get information about their loop algebras. To
cite one difference between the classes of RA and RA2 loops, and a difference
which experience with group algebras suggests will be a major stumbling block
to proving theorems about RA2 loop algebras, we mention the fact that, whereas
RA loops are (centrally) nilpotent of class 2, RA2 loops need not be nilpotent (of
any class). For example, the smallest Moufang loop— $M(S_3, 2)$—is RA2, but
not nilpotent. It does, however, contain an abelian associative normal subloop
with a quotient which is an abelian group. This proves to be typical of RA2
loops, as we show in Section 3, and is the key to what we want to establish about
RA2 loop algebras in this paper.

2. Background and notation

If a, b, c are elements of an alternative ring, we denote the (*ring*) *commuta-
tor* of a and b by $[a, b]$ and the (*ring*) *associator* of a, b and c by $[a, b, c]$.
Thus

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

Each of these functions is skew-symmetric. The *Kleinfeld* function is defined
by

$$(2.1) \qquad f(x, y, z, w) = [xy, z, w] - y[x, z, w] - [y, z, w]x.$$

It too is skew-symmetric. (Our general reference for the theory of alternative
rings is [12].) An alternative ring R has a *nucleus*

$$\mathcal{N}(R) = \{x \in R \mid [x, a, b] = [a, x, b] = [a, b, x] = 0, \text{ for all } a, b \in R\}$$
$$= \{x \in R \mid [x, a, b] = 0 \text{ for all } a, b \in R\}$$

(by skew-symmetry of the associator) and a *centre*

$$\mathcal{Z}(R) = \{x \in \mathcal{N}(R) \mid ax = xa \text{ for all } a \in R\}.$$

If a, b, c are elements of a loop, we denote the (*loop*) *commutator* of a and
b by (a, b) and the (*loop*) *associator* of a, b and c by (a, b, c). Thus

$$ab = (ba)(a, b) \qquad \text{and} \qquad ab \cdot c = (a \cdot bc)(a, b, c).$$

(It is often convenient to use dots instead of, or in addition to, parentheses to
denote the order of multiplication in a nonassociative product, with the conven-
tion that juxtaposition takes precedence over a dot.) A loop L has a nucleus,

$\mathcal{N}(L)$, and a centre, $\mathcal{Z}(L)$, defined in a way completely analogous to the manner in which they are defined in an alternative ring. The traditional reference for the theory of loops has been Bruck's classic text [2], but there is now available a more modern book by Pflugfelder [11] which contains the basic facts about loops and, in particular, about Moufang loops.

Moufang loops and alternative rings are *diassociative*: the subloop (or subring) generated by any pair of elements is associative. Even more, if three elements in a Moufang loop or an alternative ring associate in some order, then these three elements generate an associative substructure. (Thus, for example, the statement "three elements associate" is unambiguous.) We use these facts extensively and often implicitly.

This paper is concerned with RA2 loops which are, by definition, loops whose loop rings in characteristic 2 are alternative. They include the class of RA loops but, as we have mentioned, are far more numerous. (Of the 159 Moufang loops of order less than 64 which are not groups [3], just 10 are RA whereas 63 are RA2.) The most fundamental properties of RA2 loops are contained in the following restatement of Theorem 2.9 of [5].

Theorem 2.1. *An RA2 loop is a Moufang loop in which, given a triple g, h, k of elements which do not associate, precisely one of the following occurs:*

   I. *g, h and k commute pairwise and, if x, y, z are g, h, k in some order, $xy \cdot z = gh \cdot k$ and $x \cdot yz = g \cdot hk$;*

   II. *exactly one of g, h, k commutes with the other two and, if this element is g,*

$$hg \cdot k = gh \cdot k = g \cdot kh = k \cdot gh = k \cdot hg = hk \cdot g$$
$$\text{and } h \cdot gk = g \cdot hk = gk \cdot h = kg \cdot h = kh \cdot g = h \cdot kg;$$

   III. *exactly one of g, h, k commutes with neither of the other two and, if this element is g,*

$$gk \cdot h = k \cdot gh = kh \cdot g = hk \cdot g = gh \cdot k = h \cdot gk$$
$$\text{and } g \cdot kh = kg \cdot h = k \cdot hg = h \cdot kg = g \cdot hk = hg \cdot k;$$

   IV. *no pair of elements of the triple g, h, k commute and, if x, y, z are g, h, k in some order, $xy \cdot z = x \cdot zy = y \cdot xz$.*

We refer to a triple g, h, k of elements which do not associate as a triple of type I, II g, III g or IV, according as these elements satisfy I, II, III or IV, respectively, of the theorem.

If this theorem appears somewhat complicated, it should be noted that we can often manage with a more easily remembered consequence of it.

Corollary 2.2. *If g, h and k are three elements of an RA2 loop which do not associate, then either*

(2.2) $$gh \cdot k = hg \cdot k \quad \text{and} \quad g \cdot hk = h \cdot gk$$

or

(2.3) $$gh \cdot k = h \cdot gk \quad \text{and} \quad g \cdot hk = hg \cdot k$$

according as g and h do or do not commute, respectively.

3. RA2 LOOPS[1]

In this section, we establish a number of properties of RA2 loops, virtually all of which are generalizations of known results for RA loops.

Theorem 3.1. *Let L be an RA2 loop and let g and h be elements of L such that $(g, h, L) = 1$ (that is, $(g, h, k) = 1$ for all $k \in L$). Then*

(a) $(g, h)^2 = 1$,

(b) $g^2 h = h g^2$ (and $g h^2 = h^2 g$), and

(c) *the commutator (g, h) commutes with g (and with h).*

Proof. Thinking of L as embedded in an alternative ring RL of characteristic 2, we see that $(g, h, L) = 1 \implies [g, h, RL] = 0$. Then, following Kleinfeld [10, p. 133] (the argument is also presented in [7, Theorem 3(iii)]), we obtain $n = gh + hg \in \mathcal{N}(RL)$ and then, noting that we also have $(g, hg, L) = 1$, that $[g, hg] = ng$ is also in $\mathcal{N}(RL)$. (Here, we begin to use freely the fact that we are working in characteristic 2.) It follows that $[ng, x, y] = 0$ for all $x, y \in RL$, and so, from (2.1),

$$(3.1) \qquad 0 = g[n, x, y] + [g, x, y]n + f(n, g, x, y) = [g, x, y]n$$

since $n \in \mathcal{N}(L)$ and $f(n, g, x, y) = f(g, x, n, y)$ is the sum of three terms each of which involves an associator containing n.

Assume for the moment that $g \in \mathcal{N}(L)$. Then $g^2 \in \mathcal{Z}(L)$ and $(g, h)^2 = 1$ by [5, Corollaries 3.5 and 3.6], so (a) and (b) of the theorem hold. As for (c), this holds if $\mathcal{N}(L)$ is not commutative by [5, Theorem 3.2], so we now consider the implications of a commutative nucleus. In this case, and if, furthermore, $\mathcal{N}(L) = \mathcal{Z}(L)$, then statement (c) holds since we would then have $g \in \mathcal{Z}(L)$. Finally, if $\mathcal{N}(L) \neq \mathcal{Z}(L)$ (but still assuming the nucleus is commutative), then L is an *extra* loop [6] in which squares, and hence commutators, are in the nucleus (because $(a, b) = a^{-1}b^{-1}ab = a^{-2}(ab^{-1})^2b^2$). So g and (g, h), being in the nucleus, must commute. The theorem is therefore true if $g \in \mathcal{N}(L)$.

It remains to consider the case that $g \notin \mathcal{N}(L)$. In this case, choose a and b in L with $(g, a, b) \neq 1$. Write $ga \cdot b = (g \cdot ab)k$ for $k = (g, a, b) \in L$ and note that $[g, a, b] = ga \cdot b + g \cdot ab = (g \cdot ab)(k + 1)$. Then, from (3.1), $[g, a, b]n = 0$, so $(g \cdot ab)(k + 1)n = 0$ and, because $g \cdot ab$ is invertible, $(1 + k)n = 0$. Recalling that $n = gh + hg$, we obtain $gh + hg + k \cdot gh + k \cdot hg = 0$. Now $gh \neq k \cdot gh$ since $k \neq 1$, so, by linear independence of loop elements in the loop ring, either $gh = hg$, in which case the theorem is true trivially, or $gh = k \cdot hg$ and $hg = k \cdot gh$. In this last case, we have $gh = k(k \cdot gh)$, implying that $k^2 = 1$. Moreover, $k = (g^{-1}, h^{-1})$ and so

$$(3.2) \qquad\qquad k = (g, a, b) = (g^{-1}, h^{-1}).$$

Now, since $(g, h, L) = 1$, we have also $(g, gh, L) = 1$. Repeating the foregoing argument for g and gh and noting that the theorem holds if g and gh commute, we may assume that $(g, a, b) = (g^{-1}, (gh)^{-1})$, so that $(g^{-1}, h^{-1}) = (g^{-1}, (gh)^{-1})$. This immediately gives that g and (g^{-1}, h^{-1})

---

[1]Some of the results in this section are based upon unpublished work with Orin Chein and are used here with his permission and the author's gratitude.

commute. It is not hard to show that this forces g and (g, h) to commute as well. Also, since k has order 2, so does (g, h). Hence

$$(g^2, h) = g^{-2}h^{-1}g^2h = g^{-1}(g^{-1}h^{-1}g)gh$$
$$= g^{-1}(g^{-1}h^{-1}g)hg(g, h)$$
$$= g^{-1}(g^{-1}h^{-1}gh)g(g, h)$$
$$= g^{-1}(g, h)g(g, h) = 1$$

and the theorem is complete. $\square$

Lemma 3.2. *Let g and h be elements of an RA2 loop L. Then*

$$gh = hg \implies (g^2, h, L) = (g, h^2, L) = 1.$$

Proof. Let $k \in L$. If $(g, h, k) = 1$, then g, h and k generate a group and, clearly, $(g^2, h, k) = (g, h^2, k) = 1$. So assume $(g, h, k) \neq 1$. Then g, h and gk cannot associate; else, they would generate a group containing g, h and k. So

$$hg^2 \cdot k = (ghg)k = g(h \cdot gk) \quad \text{(by the left Moufang identity)}$$
$$= h(g \cdot gk) \quad \text{(by (2.2))}$$
$$= h \cdot g^2k.$$

Thus h, g^2 and k associate and, by symmetry, so do g, h^2 and k. $\square$

Theorem 3.3. *For any $g, h \in L$, g^2 and h^2 commute.*

Proof. The result certainly holds if g and h commute or, by Theorem 3.1, if $(g, h, L) = 1$. So we assume that $gh \neq hg$ and that $(g, h, k) \neq 1$ for some $k \in L$. There are four cases to consider.

Case 1. If no two of g, h, k commute, then they are a triple of type IV. None of these elements can commute with a product of the other two; for example, if k were to commute with hg, then $hk \cdot g = k \cdot hg = hg \cdot k = h \cdot kg$, a contradiction. Also, the square of any of g, h, k associates with the other two. To see why, suppose g^2 did not associate with h and k. Then

$$hk \cdot g^2 = k \cdot hg^2 \quad \text{by (2.3)}$$
$$= k(hg \cdot g)$$
$$= (hg \cdot k)g \quad \text{by (2.3) and the fact that } hg \text{ and } k \text{ do not commute}$$
$$= (h \cdot kg)g \quad \text{since } h, k, g \text{ is a type IV triple}$$
$$= (kh \cdot g)g$$
$$= kh \cdot g^2$$

which implies that $hk = kh$, a contradiction. Now we observe that since hg, g, k do not associate and hg and g do not commute, $(hg \cdot g)k = g(hg \cdot k)$ by (2.3) and so

$$hg^2 \cdot k = (hg \cdot g)k = g(hg \cdot k) = g(g \cdot hk) = g^2 \cdot hk = g^2h \cdot k.$$

This gives $g^2h = hg^2$, so the squares of g and h commute as desired.

Case 2. If $gk \neq kg$ and $hk = kh$, then (because $gh \neq hg$) g, h, k is a triple of type III g. Noting that $(h^2, k, L) = 1$ (Lemma 3.2), that gh and k commute (see Theorem 2.1, III), and that $(gh \cdot k)h = g(h \cdot kh)$ by the right Moufang identity, we have

$$h^2 g \cdot k = h(h \cdot gk) = h(gk \cdot h) = (h \cdot gk)h$$
$$= (gh \cdot k)h = g(h \cdot kh) = g \cdot h^2 k = gh^2 \cdot k$$

and hence, again, $h^2 g = gh^2$ (and g^2 and h^2 commute).

Case 3. If $hk \neq kh$ and $gk = kg$, then g, h, k is a triple of type III h, so, as in Case 2, we obtain $g^2 h = hg^2$, from which it follows that g^2 and h^2 also commute.

Case 4. If $gk = kg$ and $hk = kh$, then g, h, k is a triple of type II k. In this case gh and k do not commute, so gh, h, k is a triple of type III gh. As in Case 2, it follows that h^2 commutes with gh and hence also with g and with g^2. $\square$

Theorem 3.4. *Let g and h be elements of an RA2 loop L. Then $(g^2, h^2, L) = 1$.*

Proof. Let $k \in L$ and suppose $(g, h, k) \neq 1$. If any two of g, h and k commute, the result follows by Lemma 3.2. For example, if $hk = kh$, then $(h^2, g, k) = 1$, so h^2, g and k would generate a group and h^2, g^2 and k would associate. So we assume no two of g, h and k commute. Thus they are a triple of type IV. Now consider

$$g(h \cdot gk) = (gh \cdot g)k \implies g(gh \cdot k) = (g \cdot hg)k \implies g(g \cdot kh) = hg \cdot gk$$

using (2.3) to rewrite $(g \cdot hg)k$. (Note that the triple g, hg, k does not associate and the pair g, hg does not commute.) Now $g(g \cdot kh) = g^2 \cdot kh$. As for $hg \cdot gk$, notice that h and gk do not commute. (We saw this in Theorem 3.3.) Thus no two elements in the triple h, g, gk commute; this triple is therefore of type IV and so $hg \cdot gk = g(h \cdot gk) = (g \cdot gk)h = g^2 k \cdot h$. We see thereby that g^2, k and h associate, and the result follows. $\square$

Corollary 3.5. *Let $A = \langle L^2 \rangle$ be the subloop of the RA2 loop L generated by the squares in L. Then $(A, A, L) = 1$.*

Proof. First we use induction to show that $(x, h^2, L) = 1$ for any $x = g_1^2 g_2^2 \cdots g_n^2$, $g_i \in L$, the case $n = 1$ being the theorem. For $x = x_1 g^2$, with x_1 the product of squares of elements in L, we have

$$[x, h^2, k] = [x_1 g^2, h^2, k]$$
$$= g^2 [x_1, h^2, k] + [g^2, h^2, k]x_1 + f(x_1, g^2, h^2, k) = 0$$

because $f(x_1, g^2, h^2, k) = f(x_1, k, g^2, h^2)$ and f vanishes whenever its last two arguments associate with all other elements. The final step, that $[x, y, k] = 0$ for any $x, y \in A$ and $k \in L$, follows with a similar inductive argument. $\square$

The main theorem of this section is now quite straightforward.

Theorem 3.6. *Let L be an RA2 loop. Then the subloop A generated by the squares of the elements in L is an associative commutative normal subloop of L.*

Proof. That A is associative follows immediately by Corollary 3.5; that it is commutative, by Theorem 3.3. To prove normality, we note that, while there are three things to check in the general setting of Moufang loops, in an RA2 loop we have only to verify that $k^{-1}ak \in A$ for every $k \in L$ and $a \in A$ (see [5, Corollary 2.11]). By diassociativity, $k^{-1}g^2k$ is a square and then, for $x = x_1g^2$ with x_1 and $k^{-1}x_1k \in A$,

$$k^{-1}xk = k^{-1}(x_1g^2)k = (k^{-1}x_1k)(k^{-1}g^2k) \in A$$

using the fact that k, x_1 and g^2 generate a group, by Corollary 3.5. □

With A as in the theorem, we see that L/A is an RA2 loop of exponent 2. So it is commutative and hence a group [5, Corollary 2.5].

Corollary 3.7. *In any RA2 loop, the commutators and associators lie in the subloop generated by the squares. If each of a and b is a commutator or an associator in an RA2 loop, then $(a, b) = (a, b, x) = 1$ for any $x \in L$.*

We conclude this section with a result of independent interest. It is convenient to include it here since it depends so heavily on the results just obtained. Our starting point is (3.2). At this stage of the proof of Theorem 3.1 we have shown that, if g and h are two elements which do not commute in an RA2 loop L and if $(g, h, L) = 1$, then, whenever an associator $(g, a, b) \neq 1$, it is the element $k = (g^{-1}, h^{-1})$. Note that this element is independent of a and b. Thus any associator in L of the form (g, a, b) takes on at most two values, 1 and k. It follows that $(g, a, k) = 1$ for all $a \in L$; otherwise, $ga \cdot k = (g \cdot ak)k$ quickly gives $k = 1$, a contradiction. Thus

$$(g, c, (g, a, b)) = 1$$

for all $a, b, c \in L$. We use this fact repeatedly in the next few lines. Let $a, b \in L$. Then

$$
\begin{aligned}
g^2a \cdot b &= (g \cdot ga)b \\
&= \{g(ga \cdot b)\}(g, ga, b) \\
&= \{g\{(g \cdot ab)(g, a, b)\}\}(g, ga, b) \\
&= \{\{g(g \cdot ab)\}(g, a, b)\}(g, ga, b) \\
&= (g^2ab)\{(g, a, b)(g, ga, b)\}.
\end{aligned}
$$

Now g, ga, and b associate if and only if g, a, and b do. Also, each of the associators (g, ga, b) and (g, a, b) assumes at most two values, 1 or k. It is therefore the case that these associators are equal and, because $k^2 = 1$, their product is 1. We have shown that g^2 is in the nucleus $\mathscr{N}(L)$ and, by symmetry, so is h^2. Replacing h by gh^{-1} in the foregoing (note that g and gh^{-1} do not commute and $(g, gh^{-1}, L) = 1$), we also have $(gh^{-1})^2 \in \mathscr{N}(L)$ and therefore $(g, h) \in \mathscr{N}(L)$ too, because $(g, h) = g^{-2}(gh^{-1})^2h^2$. In an RA loop, $(g, h, L) = 1$ if and only if $(g, h) = 1$ [7]. In an RA2 loop, we have the following weaker statement.

Theorem 3.8. *Let L be an RA2 loop and $g, h \in L$. Then $(g, h, L) = 1 \implies (g, h) \in \mathscr{N}(L)$. If $(g, h, L) = 1$ and $(g, h) \neq 1$, then also $g^2, h^2 \in \mathscr{N}(L)$.*

4. Nilpotence of the augmentation ideal

A nonassociative ring S is said to be *nilpotent* if, for some natural number n, the product of any n elements in S, with any order of multiplication, is 0. Defining $S^1 = S$ and then, inductively, $S^{k+1} = S^k S$, S is *right nilpotent* if, for some natural number n, $S^n = 0$. In an alternative ring, right nilpotence implies nilpotence [12, p.119].

If R is a ring of characteristic 2, if L is an RA2 loop, and if N is a normal subloop of L, then the natural homomorphism $L \to L/N$ extends linearly to a ring homomorphism $RL \to R[L/N]$ whose kernel, denoted $\Delta(L, N)$, is the ideal of RL generated by elements of the form $1 + n$, $n \in N$. In the special case $L = N$, the homomorphism just described maps $\sum \alpha_g g \in RL$ to $\sum \alpha_g \in R$. This map, called the *aumentation map*, has a kernel, written $\Delta(L)$ rather than $\Delta(L, L)$, known as the *augmentation ideal* of RL. It follows directly from the definitions that, for a normal subloop N of L,

$$\Delta(L, N) = RL \Delta(N).$$

Assume now that $R = F$ is a field of characteristic 2 and that the order of L is 2^n for some $n > 0$. Since the elements of $\mathscr{S} = \{1 + g \mid g \in L\}$ are linearly independent over F and span $\Delta(L)$ (because $g(1 + h) = (1 + gh) + (1 + g)$), it is clear that $\Delta(L)$ has dimension $2^n - 1$.

As previously, we let A be the normal subloop of L generated by the squares of L and note that L/A is a group of exponent 2. By Jennings' result for modular group algebras, $\Delta(L/A)$ $(= \Delta(L)/\Delta(L, A))$ is nilpotent. For finite-dimensional alternative algebras, nilpotence is a radical property closed under extensions. Thus, to prove $\Delta(L)$ nilpotent, it suffices now to prove that $\Delta(L, A)$ is nilpotent.

Now $\Delta(L, A) = FL \Delta(A)$ is spanned over F by elements of the form $g(1 + a)$, $g \in L$, $a \in A$, and the identity $g(1 + a) = (1 + g)(1 + a) + (1 + a)$ shows that $\Delta(L, A) \subseteq \Delta(A) + \Delta(L)\Delta(A) = I + JI$ where we have set $I = \Delta(A)$ and $J = \Delta(L)$. Since I is nilpotent (by the result for group algebras), the nilpotency of $\Delta(L, A)$ is an obvious consequence of

$$(4.1) \qquad\qquad (I + JI)^n \subseteq I^n + I^n J \quad \text{for all } n \geq 1,$$

a fact we proceed to establish. In so doing, we shall use regularly that I and A are commutative, that $(A, A, L) = 1$, and hence that $[A, A, FL] = [I, I, FL] = 0$.

For any $g, h \in L$, we can write $gh = hg \cdot f_1$ or $hg = f_2 \cdot gh$ for commutators f_1, f_2 which are in A, by Corollary 3.7. Then $[g, h] = gh + hg = (hg)(1 + f_1) = (1 + f_2)(gh)$, with both $1 + f_1$ and $1 + f_2$ in $\Delta(A)$. Furthermore, since (loop) associators of elements of L are in A, we also have such equations as

$$[g, h, k] = (gh \cdot k)(1 + f_3) = (1 + f_4)(g \cdot hk)$$

with $1 + f_3, 1 + f_4 \in \Delta(A)$, whenever g, h and k are elements of L. We establish (4.1) with a sequence of lemmas.

Lemma 4.1. *With* $I = \Delta(A)$ *and* $J = \Delta(L)$, $JI^n \subseteq I^n + I^n J$ *for all* $n \geq 1$.

Proof. An element of JI is an F-linear combination of elements of the form $(1 + g)(1 + a)$, $g \in L$, $a \in A$. Now

$$
\begin{aligned}
(1 + g)(1 + a) &= (1 + a)(1 + g) + [g, a] \\
&= (1 + a)(1 + g) + (1 + f)ag \qquad \text{for some } 1 + f \in I \\
&= (1 + a)(1 + g) + (1 + f)a(1 + g) + (1 + f)a,
\end{aligned}
$$

which is in $IJ + I$ because $(1 + f)a \in I$ (I is an ideal of FA). Thus $JI \subseteq IJ + I$ and the lemma is true for $n = 1$. Assuming $JI^k \subseteq I^k + I^k J$, we have

$$
\begin{aligned}
JI^{k+1} = JI^k \cdot I &\subseteq (I^k + I^k J)I \\
&\subseteq I^{k+1} + I^k \cdot JI \\
&\subseteq I^{k+1} + I^k(IJ + I) \\
&\subseteq I^{k+1} + I^{k+1}J + I^{k+1},
\end{aligned}
$$

from which the lemma follows. $\square$

For our next proof, it will be important to note that $I \cdot I^n = I^n \cdot I$ ($= I^{n+1}$) for any $n \geq 1$ because elements of I commute.

Lemma 4.2. *With* $I = \Delta(A)$ *and* $J = \Delta(L)$, $[I^n, J, J] \subseteq I^n + I^n J$ *for all* $n \geq 1$.

Proof. Let $a \in A$ and $g, h \in L$. Then $[1 + a, 1 + g, 1 + h] = [a, g, h] = (1 + f)(a \cdot gh)$, for some $1 + f \in I$. Now $(1 + f)(a \cdot gh) = (1 + f)(1 + a \cdot gh) + (1 + f) \in IJ + I$, so the result holds for $n = 1$. Now assume $[I^k, J, J] \subseteq I^k + I^k J$ and let $a \in I^k$, $b \in I$, $x, y \in J$. Then

$$
[ab, x, y] = b[a, x, y] + [b, x, y]a
$$

because $f(a, b, x, y) = f(x, y, a, b)$ and $[FL, I, I] = 0$. Now

$$
b[a, x, y] \in I(I^k + I^k J) \subseteq I^{k+1} + I^{k+1}J
$$

and

$$
\begin{aligned}
[b, x, y]a &\in (I + IJ)I^k \\
&\subseteq I \cdot I^k + IJ \cdot I^k \\
&\subseteq I^{k+1} + I \cdot JI^k \\
&\subseteq I^{k+1} + I(I^k + I^k J) \qquad \text{by Lemma 4.1} \\
&\subseteq I^{k+1} + I^{k+1}J,
\end{aligned}
$$

completing the induction. $\square$

Lemma 4.3. *With* $I = \Delta(A)$ *and* $J = \Delta(L)$, *we have* $(I + JI)^n \subseteq I^n + I^n J$, *for any* $n \geq 1$.

Proof. When $n = 1$, the result follows immediately from Lemma 4.1. Assume inductively that $(I + JI)^k \subseteq I^k + I^k J$ for some $k \geq 1$. Then

$$
\begin{aligned}
(I + JI)^{k+1} &= (I + JI)^k(I + JI) \\
&\subseteq (I^k + I^k J)(I + IJ) \\
&\subseteq I^{k+1} + I^k \cdot IJ + I^k J \cdot I + I^k J \cdot IJ.
\end{aligned}
$$

Now $I^k \cdot IJ = I^{k+1}J$ (since $[I, I, FL] = 0$), and $I^k J \cdot I = I^k \cdot JI \subseteq$ $I^k(I + IJ) \subseteq I^{k+1} + I^{k+1}J$. Thus, it remains only to prove that $I^k J \cdot IJ \subseteq$ $I^{k+1} + I^{k+1}J$. Elements of $I^k J \cdot IJ$ are F-linear combinations of elements of the form $x(1 + g) \cdot (1 + a)(1 + h)$, where $x \in I^k$ and where $g, h \in L$ and $a \in A$, and such an element can be written as

$$(4.2) \qquad \{x(1 + g)(1 + a)\}(1 + h) + [x(1 + g), 1 + a, 1 + h].$$

The first of these terms is $\{x(1 + a)(1 + g) + x[1 + g, 1 + a]\} \cdot (1 + h)$

$$= \{x(1 + a)(1 + g) + x[g, a]\}(1 + h)$$
$$= \{x(1 + a)(1 + g) + x(1 + f)ag\}(1 + h) \qquad \text{for some } 1 + f \in I$$
$$= \{x(1 + a)(1 + g)\}(1 + h) + \{x(1 + f)(1 + ag) + x(1 + f)\}(1 + h).$$

The last of the three terms here, $x(1 + f)(1 + h)$, is certainly in $I^{k+1}J$, while the first two are of the form $uv \cdot w$, where $u \in I^{k+1}$ and $v, w \in J$. Writing $uv \cdot w = u \cdot vw + [u, v, w]$, we see at once that $uv \cdot w \in I^{k+1} + I^{k+1}J$, by the previous lemma.

The second term in (4.2) is

$$[x + xg, 1 + a, 1 + h] = [xg, a, h]$$
$$= g[x, a, h] + [g, a, h]x + f(x, g, a, h)$$
$$= [g, a, h]x$$

because $[I^k, I, FL] = 0$ and $f(x, g, a, h) = f(g, h, x, a) = 0$ since $f(g, h, x, a)$ is the sum of three terms involving associators in each of which the two elements x and a (of I) appear. As for $[g, a, h]x$, we write this as $[g, h, a]x$ and observe that this can be rewritten first as $(gh \cdot a)(1 + f)x$ for some $1 + f \in I$, and then as $(1 + gh \cdot a)(1 + f)x + (1 + f)x$, which is an element of $JI^{k+1} + I^{k+1} \subseteq I^{k+1} + I^{k+1}J$, by Lemma 4.1. □

Combining the results of this section with the known result for group algebras, we have the following theorem.

Theorem 4.4. *Let FL be the alternative loop algebra (associative or otherwise) of a loop L of order 2^n over a field of characteristic 2. Then, with respect to any radical property for which nilpotent algebras are radical and algebras with 1 are not, the radical of FL is its augmentation ideal $\Delta(L)$ and this is nilpotent of dimension $2^n - 1$.*

References

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

2. _____, *A survey of binary systems*, Ergeb. Math. Grenzgeb., vol. 20, Springer-Verlag, Berlin, 1958.

3. Orin Chein, *Moufang loops of small order*, Mem. Amer. Math. Soc. **197** (1978), no. 13.

4. Orin Chein and Edgar G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra **14** (1986), 293–310.

5. _____, *Loops whose loop rings in characteristic 2 are alternative*, Comm. Algebra **18** (1990), 659–688.

6. Orin Chein and D. A. Robinson, *An "extra" law for characterizing Moufang loops*, Proc. Amer. Math. Soc. **33** (1972), 29–32.

7. Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Debrecen **30** (1983), 31–38.

8. Edgar G. Goodaire and M. M. Parmenter, *Semi-simplicity of alternative loop rings*, Acta Math. Hungar. **50** (1987), 241–247.

9. S. A. Jennings, *The structure of the group ring of a p-group over a radical field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.

10. E. Kleinfeld, *A characterization of the Cayley numbers*, Studies in Modern Algebra (A. A. Albert, ed.), Studies in Math., vol. 2, Math. Assoc. Amer., Washington, DC, 1963, pp. 126–143.

11. H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Heldermann Verlag, Berlin, 1990.

12. K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov, *Rings that are nearly associative* (translated by Harry F. Smith), Academic Press, New York, 1982.

MEMORIAL UNIVERSITY OF NEWFOUNDLAND, ST. JOHN'S, NEWFOUNDLAND, CANADA A1C 5S7
E-mail address: `edgar@math.mun.ca`