ALTERNATIVE LOOP RINGS

Kenneth Kunen *
University of Wisconsin, Madison, WI 53706, U.S.A.
email: kunen@math.wisc.edu

December 24, 1996

DRAFT

Abstract

The right alternative law implies the left alternative law in loop rings of characteristic other than 2. We also exhibit a loop which fails to be a right Bol loop, even though its characteristic 2 loop rings are right alternative.

1 Introduction

Throughout this paper, $(L, \cdot)$ *always* denotes a loop, with identity element e, and $(R, +, \cdot)$ *always* denotes an associative commutative ring, with identity element $1 \neq 0$. Then, RL denotes the *loop ring* constructed from R and L. Elements of RL are represented by finite formal sums of the form $\sum_{i<n} a_i x_i$, where the x_i are elements of L and the a_i are elements of R. The sum and product operations on RL are defined in the obvious way. Then, $1e$ is the identity element of RL. See the survey by Goodaire and Milies [2] for more details, background information, and references to the earlier literature.

Note that L is embedded into RL via the map $x \mapsto 1x$; we usually write the element $1x$ simply as x. It is now trivial to verify:

Remark 1.1 *RL is associative iff L is associative.*

*Author supported by NSF Grant CCR-9503445.

However, the situation for weakened versions of the associative law is more complicated. In this paper, we focus on the *right alternative law* ($(xy)y = x(yy)$) and the *left alternative law* ($(yy)x = y(yx)$). The right alternative law in RL implies much more than just the right alternative law in L, since, as we shall prove in Section 2,

Theorem 1.2 *Suppose that RL satisfies the right alternative law and R satisfies $1 + 1 \neq 0$. Then RL (and hence also L) satisfies the left alternative law.*

Once both laws are known to hold in RL, one may refer to the extensive literature in non-associative algebra, both on general *alternative rings* (that is, rings in which *both* alternative laws hold), as well as alternative loop rings in particular. Every alternative ring (regardless of its characteristic) satisfies the Moufang identities. In particular, if RL is alternative, then L is a Moufang loop. See §1.2 of [2] for further discussion. However, Theorem 1.2 is not true for rings in general, since Михеев [7] describes an example of a non-associative ring satisfying $1 + 1 \neq 0$ plus the right alternative law, but not the left alternative law.

In the case that L is finite, Theorem 1.2 was proved by Chein and Goodaire [1]. Their proof relied on structure theorems of Bruck and Albert which are false for infinite L. Goodaire and Robinson [3][4] showed that the assumption in the theorem that R satisfies $1 + 1 \neq 0$ cannot be dropped. By [3][4], there are examples of finite L such that for rings of characteristic 2, RL is right alternative, but even L itself fails to be left alternative. The loops they construct also satisfy the right Bol identity, and they ask whether this identity must hold in L whenever RL is right alternative. The answer is "no", as we show by an example in Section 3.

Actually, in the study of alternative laws in loop rings RL, only L is relevant, by the following result from [1]:

Proposition 1.3 *For any L:*

RL satisfies the right alternative law for some R of characteristic $= 2$ iff RL satisfies the right alternative law for all R of characteristic $= 2$.

RL satisfies the right alternative law for some R of characteristic $\neq 2$ iff RL satisfies the right alternative law for all R of characteristic $\neq 2$.

This follows immediately from the fact that one can express the right alternativity of RL by a boolean combination of equations in L; there is one boolean combination for the characteristic = 2 case and another for the characteristic $\neq 2$ case; see [1] and Lemma 2.2 below. However, one cannot replace this boolean combination by any set of single equations; see Section 4 for further discussion of this point.

The proof of Theorem 1.2 was discovered with the aid of the automated reasoning tool OTTER [6], programmed by W. W. McCune. Then, following the standard method [5], the proof was simplified and rephrased in ordinary mathematical format. The example in Section 3 was constructed by experimenting with the program SEM [8], programmed by J. Zhang and H. Zhang.

2 Proof of Theorem 1.2

We begin by eliminating the rings from the theory of loop rings. Lemma 2.1 almost does that, since it expresses right alternativity in RL just in terms of elements of the form $1x$ (which, recall, we are writing as x). The material through Lemma 2.2 is from Chein and Goodaire [1].

Lemma 2.1 *RL is right alternative iff L is right alternative and RL satisfies $x(yz) + x(zy) = (xy)z + (xz)y$ for all $x, y, z \in L$.*

Proof. If RL is right alternative, then L is trivially also right alternative, but also RL must satisfy $u(vv) = (uv)v$ for any $u, v \in RL$. If we let $u = x$ and $v = y + z$, and apply the right alternative law in L, we immediately get the equation $x(yz) + x(zy) = (xy)z + (xz)y$. Conversely, assuming this equation and the right alternativity of L, it is easy to verify $u(vv) = (uv)v$ simply by replacing u by $\sum_{i<m} a_i x_i$, and v by $\sum_{j<n} b_j y_j$, and expanding the product. □

Now, if p, q, r, s are arbitrary elements of L, the equation $p + q = r + s$ cannot hold in RL unless either $p = r$ and $q = s$, or $p = s$ and $q = r$, *except* in the case that R has characteristic 2, in which case there is also the possibility that $p = q$ and $r = s$. Applying this observation to the result of Lemma 2.1, the alternative law in RL reduces to a boolean combination of equations in L as follows:

Definition 2.1 *In any loop, define the properties* $A(x,y,z)$, $B(x,y,z)$, *and* $C(x,y,z)$ *by:*
$A(x,y,z)$ *iff* $x(yz) = (xy)z$ *and* $x(zy) = (xz)y$
$B(x,y,z)$ *iff* $x(yz) = (xz)y$ *and* $x(zy) = (xy)z$
$C(x,y,z)$ *iff* $x(yz) = x(zy)$ *and* $(xy)z = (xz)y$

Lemma 2.2 *For any* R *and* L*:*

If $1+1 \neq 0$ *in* R, *then* RL *is right alternative iff for all* x,y,z *in* L, *either* $A(x,y,z)$ *or* $B(x,y,z)$ *holds.*

If $1+1 = 0$ *in* R, *then* RL *is right alternative iff* L *is right alternative and for all* x,y,z *in* L, *either* $A(x,y,z)$ *or* $B(x,y,z)$ *or* $C(x,y,z)$ *holds.*

Proposition 1.3 is immediate from Lemma 2.2. Note that both $A(x,y,y)$ and $B(x,y,y)$ reduce to $x(yy) = (xy)y$, so that we do not have to postulate the right alternativity of L in the characteristic $\neq 2$ case. In deriving results in the characteristic $\neq 2$ case, it is often easier to distribute the OR over the AND in Lemma 2.2 and rephrase it as:

Lemma 2.3 *For any* R *of characteristic other than 2 and any* L, RL *is right alternative iff for all* x,y,z *in* L, *we have both:*
1. $x(yz) = (xy)z$ *or* $x(yz) = (xz)y$
2. $x(yz) = (xy)z$ *or* $x(zy) = (xy)z$

Proof. Write $A(x,y,z)$ as $P_1(x,y,z) \wedge P_2(x,y,z)$, and $B(x,y,z)$ as $Q_1(x,y,z) \wedge Q_2(x,y,z)$. Then, by the previous lemma, RL is right alternative iff for $i = 1,2$ and $j = 1,2$, we have $P_i(x,y,z) \vee Q_j(x,y,z)$ for each $x,y,z \in L$. But, by renaming the variables, these four statements reduce to just (1) and (2). □

We turn now to the proof of Theorem 1.2. Using hindsight, we know that the theorem will imply that L is Moufang, and hence satisfies the *inverse property*. That is, *define* $i(x)$ by $x \cdot i(x) = e$; equivalently, $i(x) = x \backslash e$. Just by the loop properties, i is a bijection from L onto L. But, in Moufang loops, we would also have $i(x) \cdot x = e$ and $i(x \cdot y) = i(y) \cdot i(x)$. This last equation implies that i is an isomorphism from $(L, \cdot)$ onto the "opposite" loop, $(L, \circ)$, defined by $x \circ y = y \cdot x$. Since the right alternativity of RL is equivalent to the left alternativity of its opposite, we are done if we can prove $i(x \cdot y) = i(y) \cdot i(x)$. So, we proceed with a few lemmas about $i(x)$.

Lemma 2.4 *If RL is right alternative and R has characteristic other than 2, then* $i(x) \cdot x = e$ *for all* $x \in L$.

Proof. Fix a, and let $b = i(a)$, so that $ab = e$, and assume $ba \neq e$. Then fix c such that $ca = e$; so, $b \neq c$. We shall derive a contradiction by using (1) and (2) of Lemma 2.3.

First, we have $c(ab) = c \neq b = (ca)b$. Applying (1), we get $c(ab) = (cb)a$, so

$$(cb)a = c \qquad (\alpha)$$

Applying (2), we get $c(ba) = (ca)b$, so

$$c(ba) = b \qquad (\beta)$$

Applying (α) and the right alternative law,

$$(cb)a^2 = e \qquad (\gamma)$$

Applying (1), we have either $c(ba^2) = (cb)a^2$ or $c(ba^2) = (ca^2)b$. But by (γ), right alternativity, and the definitions of b and c, both equations simplify to

$$c(ba^2) = e \qquad (\delta)$$

Applying (1) again, either $c((ba)a) = (c(ba))a$ or $c((ba)a) = (ca)(ba)$. But by right alternativity, (δ), (β), and the definition of c, both equations simplify to $ba = e$, a contradiction. □

So, we have $i(x) \cdot x = x \cdot i(x) = e$, which immediately implies $i(i(x)) = x$.

Lemma 2.5 *If RL is right alternative and R has characteristic other than 2, then* $(y \cdot i(x)) \cdot x = y$ *for all* $x, y \in L$.

Proof. Apply (2) of Lemma 2.3 to get either $y \cdot (i(x) \cdot x) = (y \cdot i(x)) \cdot x$ or $y \cdot (x \cdot i(x)) = (y \cdot i(x)) \cdot x$, either of which implies $(y \cdot i(x)) \cdot x = y$. □

Lemma 2.6 *If RL is right alternative and R has characteristic other than 2, then* $x \cdot (i(x) \cdot y) = y$ *for all* $x, y \in L$.

Proof. Fix any $a, b \in L$, and let $\hat{a} = i(a)$, so $a\hat{a} = \hat{a}a = e$. We assume $\hat{a}(ab) \neq b$, and derive a contradiction.

Apply (2) of Lemma 2.3 to get either $\hat{a}(ab) = (\hat{a}a)b$ or $\hat{a}(ba) = (\hat{a}a)b$, which implies $\hat{a}(ba) = b$ (since $\hat{a}(ab) \neq b$).

Applying (2) again, either $a\,(\hat{a}\,(ba)) = (a\,\hat{a})\,(ba)$ or $a\,((ba)\,\hat{a}) = (a\,\hat{a})\,(ba)$. Using $\hat{a}(ba) = b$ and Lemma 2.5, both these equations reduce to $ba = ab$, so that we have $\hat{a}(ab) = b$, a contradiction. □

Proof of Theorem 1.2. For any $x, y \in L$, we have, by applying Lemmas 2.6, 2.5, 2.5 in that order, $i(xy) \cdot [(xy) \cdot i(y)] = i(y)$, and then $i(xy) \cdot x = i(y)$, and then $i(x \cdot y) = i(y) \cdot i(x)$, which, as remarked above, is sufficient to prove the theorem. □

3 Bol Loops

As pointed out in the Introduction, Goodaire and Robinson [3][4] showed that Theorem 1.2 can fail if R has characteristic 2. Their examples all satisfied the right Bol identity, $((xy)\,z)\,y = x\,((yz)\,y)$, and they ask whether this is necessary. That may seem plausible, since if RL is both left and right alternative, then, regardless of the characteristic, L satisfies the Moufang identities, which imply the right and left Bol identities. However, it turns out that right alternativity alone of RL does not even imply the special case of the right Bol identity when $x = y = z$ – namely, $x^3\,x = x\,x^3$. Note that right alternativity does imply that $x^2\,x = x\,x^2$, so the notation x^3 is unambiguous. Note also that left alternativity of L then fails in our example, since otherwise $x^3\,x = (x^2\,x)\,x = x^2\,x^2 = x\,(x\,x^2) = x\,x^3$.

Theorem 3.1 *For each $n \geq 3$, there is a loop L of size $2n$ such that RL is right alternative whenever R has characteristic 2, but L does not satisfy $x^3\,x = x\,x^3$.*

Proof. As a set, let L be $\{j : 0 \leq j < 2n\}$. On this set, $+$ will always denote addition modulo $2n$. Let φ be a permutation of the set of odd elements, $\{2i + 1 : 0 \leq i < n\}$. Given φ, we define the operation $\circ$ on L by letting $x \circ y$ be $x + y$ unless x, y are *both* odd, in which case we let $x \circ y = x + \varphi(y)$. We shall show that for some choices of φ, $(L, \circ)$ satisfies the theorem.

First, using the fact that φ is a permutation, it is easy to see that $(L, \circ)$ is a loop, with identity element 0.

Next, note that L is right alternative, since for odd y, we have $x \circ (y \circ y) = x + y + \varphi(y) = (x \circ y) \circ y$, while for even y, we have $x \circ (y \circ y) = x + y + y = (x \circ y) \circ y$.

Whenever x is odd, $x^3 x = 2x + 2\varphi(x)$, while $x x^3 = x + \varphi(2x + \varphi(x))$. We can make these differ for $x = 1$ by letting $\varphi(1) = 1$ and $\varphi(3) \neq 3$.

Finally, to prove RL is right alternative, we apply Lemma 2.2 and show that at least one of $A(x, y, z)$, $B(x, y, z)$, $C(x, y, z)$ holds for $x, y, z \in L$. We consider the possible cases for x, y, z.

If at least two of x, y, z are even, then all possible associations and commutations of $x \circ y \circ z$ evaluate to $x + y + z$, so that $A(x, y, z)$, $B(x, y, z)$, $C(x, y, z)$ all hold.

If x, y, z are all odd, then $x \circ (y \circ z) = x + y + \varphi(z) = (x \circ z) \circ y$ and $x \circ (z \circ y) = x + z + \varphi(y) = (x \circ y) \circ z$, so that $B(x, y, z)$ holds.

If x is even and y, z are odd, then $x \circ (y \circ z) = x + y + \varphi(z) = (x \circ y) \circ z$ and $x \circ (z \circ y) = x + z + \varphi(y) = (x \circ z) \circ y$, so that $A(x, y, z)$ holds.

If y is even and x, z are odd, then $x \circ (y \circ z) = x + \varphi(y + z) = x \circ (z \circ y)$ and $(x \circ y) \circ z = x + y + \varphi(z) = (x \circ z) \circ y$, so that $C(x, y, z)$ holds. Likewise, $C(x, y, z)$ holds in the remaining case, where z is even and x, y are odd. □

4 Products

Lemma 2.2 expresses alternativity of RL in terms of boolean combinations of equations in L. Now, one might hope that these boolean combinations might be replaced by some set of single equations. However, all such hopes are refuted by the following observation:

Lemma 4.1 *Let L be any non-associative loop. Let $L_1 = L \times L$. Then RL_1 is neither left nor right alternative for any R.*

Proof. Assume that some RL_1 is right alternative. Since L is not associative, fix $a, b, c \in L$ such that $(ab)c \neq a(bc)$, so that $A(a, b, c)$ is false. Apply Lemma 2.2 to the elements $u = (a, x)$, $v = (b, y)$, $w = (c, z)$ in $L \times L$. Then $A(u, v, w)$ is false, so we know that for all $x, y, z \in L$, either $B(x, y, z)$ or $C(x, y, z)$ holds. Applying this with $x = e$ shows that L is commutative, which implies that $B(a, b, c)$ is also false. Now, applying Lemma 2.2 to u, v, w yields that $C(x, y, z)$ holds for all $x, y, z \in L$.

So, besides being commutative, L satisfies $(xy)z = (xz)y$ for all x, y, z. But then $(yx)z = (xy)z = (xz)y = y(xz)$ holds for all x, y, z, so L is associative, a contradiction. □

Corollary 4.2 *Let $\mathcal{K}$ be any class of loops closed under finite products. Assume that $\mathcal{K}$ contains some non-associative loop. Then $\mathcal{K}$ contains a loop L such that RL is neither left nor right alternative for any R.*

In particular, this corollary applies whenever $\mathcal{K}$ is any class defined by a set of equations.

References

[1] O. Chein and E. G. Goodaire, Is a Right Alternative Loop Ring Alternative?, *Algebras Groups Geom.* 5 (1988) 297 – 304.

[2] E. G. Goodaire and C. P. Milies, Ring Alternative Loops and their Loop Rings, *Resenhas* 2 (1995) 47 – 82.

[3] E. G. Goodaire and D. A. Robinson, A Class of Loops with Right Alternative Loop Rings, *Communications in Algebra* 22 (1994) 5623 – 5634.

[4] E. G. Goodaire and D. A. Robinson, A Construction of Loops Which Admit Right Alternative Loop Rings, *Results in Mathematics* 29 (1996) 56 – 62.

[5] J. Hart and K. Kunen, Single Axioms for Odd Exponent Groups, *J. Automated Reasoning* 14 (1995) 383 – 412. Available on WWW at: `http://www.math.wisc.edu/~kunen/`

[6] W. W. McCune, OTTER 3.0 Reference Manual and Guide, Technical Report ANL-94/6, Argonne National Laboratory, 1994. Available on WWW at: `http://www.mcs.anl.gov/`

[7] И. М. Михеев, Об Одном Тождестве в Правоальтернативных Кольцах, *Алгебра и Логика* 8 (1969) 357 – 366.

[8] J. Zhang and H. Zhang, SEM: a system for enumerating models, *Proc. 14th Int.. Joint Conf. on AI (IJCAI-95)*, Montréal, 1995, pp. 298 – 303. Available on WWW at: `http://www.cs.uiowa.edu/~hzhang/`