

Units in right alternative loop rings

By EDGAR G. GOODAIRE (St. John's)

Abstract. We find conditions under which a right alternative loop ring has a Bol loop of units.

1. Background

A *groupoid* is a set L together with a (closed) binary operation $(a, b) \mapsto a \cdot b$ (often denoted by juxtaposition). If both translation maps

$$R(a) : x \mapsto xa \quad \text{right multiplication}$$

and

$$L(a) : x \mapsto ax \quad \text{left multiplication}$$

are bijections of L for all $a \in L$, then the pair $(L, \cdot)$ is a *quasigroup*. A quasigroup with two-sided identity element is a *loop*.

If a, b, c are elements of a quasigroup $(L, \cdot)$, the *commutator* (a, b) of a and b , and the *associator* (a, b, c) of a, b and c are the elements of L uniquely defined by the equations

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

A loop is (*right*) *Bol* if it satisfies the (*right*) *Bol identity*,

$$(1.1) \quad (xy \cdot z)y = x(yz \cdot y),$$

Mathematics Subject Classification: 17D15, 20N05, 16S34.

Key words and phrases: loop, right alternative, unit.

Research supported in part by the Natural Sciences and Engineering Research Council of Canada, Grant No. OGP0009087.

and *Moufang* if it satisfies the right Bol identity and also the *left Bol identity*:

$$x(y \cdot xz) = (x \cdot yx)z.$$

A right Bol loop L is *power associative* (that is, the subloop generated by a single element is associative) and, more generally, *right power alternative*:

$$(xy^m)y^n = xy^{m+n}$$

for any $x, y \in L$ and any integers m and n [Rob66]. With $H = \langle y \rangle$, the subloop generated by y , right power alternativity implies $x(hH) = xH$ for any $x \in L$ and $h \in H$. Thus L is the disjoint union of left cosets of H and it follows, as in group theory, that if L is finite, the order of H divides the order of L [Bru46, §V.1]. Thus the order of any element of L divides $|L|$ [Bur78].

If $(R, +, \cdot)$ is a (not necessarily associative) ring, and $x, y, z \in R$, we denote the (*ring*) *commutator* of x and y by $[x, y]$ and the (*ring*) *associator* of x, y and z by $[x, y, z]$. Thus,

$$[x, y] = xy - yx \quad \text{and} \quad [x, y, z] = (xy)z - x(yz).$$

A ring is *right alternative* if it satisfies the *right alternative law*: $(xy)y = xy^2$. Right alternative rings with no nonzero elements of additive order 2 also satisfy the right Bol identity. (See [ZSSS82, §16.1], but note that the identity called *right Moufang* in that work is, in fact, the right Bol identity.) Rings which satisfy just the right alternative law need not even be power associative [Kun98], [Goo00], so we always assume that right alternative rings are *strongly right alternative*, that is, they also satisfy the right Bol identity. As with loops, the right Bol identity in a ring with 1 implies power associativity and right power alternativity (for nonnegative exponents), Robinson's inductive argument in [Rob66] working verbatim.

If R is any commutative associative ring with 1 and L is a loop (with identity, also denoted 1), one constructs the *loop ring* RL just as the familiar group ring is formed. The elements of RL are formal (finite) sums

$$\sum_{\ell \in L} \alpha_\ell \ell, \quad \alpha_\ell \in R,$$

with the understanding that

$$\sum_{\ell \in L} \alpha_\ell \ell = \sum_{\ell \in L} \beta_\ell \ell \text{ if and only if } \alpha_\ell = \beta_\ell \text{ for all } \ell \in L.$$

Addition and multiplication are defined in the obvious ways:

$$\begin{aligned} \sum_{\ell \in L} \alpha_\ell \ell + \sum_{\ell \in L} \beta_\ell \ell &= \sum_{\ell \in L} (\alpha_\ell + \beta_\ell) \ell \\ \left(\sum_{\ell \in L} \alpha_\ell \ell \right) \left(\sum_{k \in L} \beta_k k \right) &= \sum_{\ell, k \in L} (\alpha_\ell \beta_k) \ell k. \end{aligned}$$

Of importance in this paper is the fact that in any loop ring, the *augmentation map* $\epsilon : RL \rightarrow R$, which is defined by $\epsilon(\sum \alpha_\ell \ell) = \sum \alpha_\ell$, is a ring homomorphism. The ring element $\epsilon(\alpha)$ is called the *augmentation* of α .

2. Right alternative loop rings

A right alternative ring is *alternative* if it also satisfies the *left alternative law*: $x(xy) = x^2y$. Right alternative rings which are not alternative are, in some sense, hard to find. Albert showed that a finite dimensional right alternative algebra over a field of characteristic 0 which has no nonzero nil ideals is alternative [Alb49]. Mikheev obtained the same conclusion for right alternative rings without nilpotent elements or elements of additive order 2 [Mik69] and, more recently, Kunen proved that a right alternative loop ring of characteristic different from two is necessarily alternative [Kun98]. Thus, if there exists a right (but not left) alternative loop algebra over a field, the characteristic must be two. Such loop algebras do in fact exist.

Theorem 2.1 [GR95], [GR96]. *If B is a (right) Bol loop with a unique nonidentity commutator which is also a unique nonidentity associator and, if R is a ring of characteristic two, then RB is strongly right alternative.*

3. Units

A *unit* in a ring with unity is an element with a two-sided inverse. We write u^{-1} for the inverse of the unit u . For any ring R , let $\mathcal{U}(R)$

denote the set of all units in R . If R is an associative ring, then $\mathcal{U}(R)$ is a group. More generally, if R is an alternative ring, $\mathcal{U}(R)$ is a Moufang loop [GJM96, §II.5.3], but it appears difficult to prove (in general) that the units of a right alternative ring are even closed under multiplication. In this connection, the following lemma is of interest and later importance.

Lemma 3.1. *If a ring R satisfies the right Bol identity and $\mathcal{U}(R)$ is closed under multiplication, then $\mathcal{U}(R)$ is a (Bol) loop.*

PROOF. We must show that the left and right translation maps are bijective. Thus, let a and b be units. The equation $b = xL(a) = ax$ has solution $x = b(ab)^{-1} \cdot b$ since, using the Bol identity,

$$a(b(ab)^{-1} \cdot b) = [(ab)(ab)^{-1}]b = b.$$

Thus $L(a)$ is surjective and, interestingly, this fact shows that $R(a)$ is also surjective. To solve $b = xR(a) = xa$ for x , first solve $yL(a) = ay = a^{-1}$ for y , and then note that $x = (ba)y$ is a solution to $xR(a) = b$ since $(ba \cdot y)a = b(ay \cdot a) = b(a^{-1}a) = b$.

Now define $a^{-2} = a^{-1}a^{-1}$ and note that $a^{-1} = aa^{-1} \cdot a^{-1} = aa^{-2}$ by the right alternative law. Thus, for any $x \in R$, we have $(xa \cdot a^{-2})a = x(aa^{-2} \cdot a) = x$, so $xa = ya$ implies $x = y$; that is, $R(a)$ is one-to-one. As with the case of surjectivity, this fact implies that $L(a)$ is also one-to-one, for suppose $ax = ay$. Then

$$xa = (a^{-1}a \cdot x)a = a^{-1}(ax \cdot a) = a^{-1}(ay \cdot a) = (a^{-1}a \cdot y)a = ya,$$

so $x = y$. □

Now let B be a (finite) Bol loop with a unique nonidentity commutator which is also a unique nonidentity associator. For simplicity, we refer to such an element as a unique nonidentity “commutator/associator” and consistently use s to denote such an element. It is not hard to show that s is central and of order 2 [GR95, Lemma 3.2]. Let R be a commutative, associative ring with 1 and form the loop ring RB . If g and h are in B and we think of these as elements of the loop ring, then, if $gh \neq hg$,

$$gh - hg = gh - sgh = (1 - s)gh.$$

Similarly, if g , h and k are in B and $(gh)k \neq g(hk)$, then

$$(gh)k - g(hk) = (gh)k - s(gh)k = (1 - s)(gh)k.$$

In characteristic two, these statements imply

$$(3.1) \quad gh + hg = [g, h] \in (1 + s)RB$$

and

$$(3.2) \quad (gh)k + g(hk) = [g, h, k] \in (1 + s)RB,$$

properties which also hold if $gh = hg$ and $(gh)k = g(hk)$.

Lemma 3.2. *Let F be a field of characteristic two and let B be a finite Bol loop of 2-power order with a unique nonidentity commutator/associator. If $\alpha \in FB$ has augmentation 0, then $\alpha^N = 0$ for some $N > 0$. Hence $1 + \alpha$ is a unit.*

PROOF. Write $\alpha = \sum \alpha_\ell \ell \in FB$. Using (3.1),

$$\alpha^2 = \sum \alpha_\ell^2 \ell^2 + (1 + s)\beta$$

for some $\beta \in FB$, and so, for any $n > 0$,

$$\alpha^{2^n} = \sum \alpha_\ell^{2^n} \ell^{2^n} + (1 + s)\beta$$

for some $\beta \in FB$. If $|B| = 2^n$, then $\ell^{2^n} = 1$ for all $\ell \in B$, so $\alpha^{2^n} = \gamma 1 + (1 + s)\beta$ for some $\beta \in FB$ and $\gamma \in F$. Since $(1 + s)^2 = 1 + 2s + s^2 = 0$, it follows that the square of α^{2^n} is in $F1$, so $\alpha^N \in F1$ for some N . Now $\epsilon(\alpha^N) = \epsilon(\alpha)^N = 0$ implies $\alpha^N = 0$.

The final statement of the lemma holds because $1 + \alpha + \alpha^2 + \cdots + \alpha^{N-1}$ is a two-sided inverse of α . $\square$

Corollary 3.3. *With F and B as in Lemma 3.2, the set of units of FB is $\mathcal{U}(FB) = \{\mu \in FB \mid \epsilon(\mu) \neq 0\}$. In particular, $\mathcal{U}(FB)$ is closed under multiplication.*

PROOF. Since the augmentation map ϵ is a ring homomorphism, the set $\{\mu \in FB \mid \epsilon(\mu) \neq 0\}$ is certainly closed under multiplication. To see that this is the set of units, note first that the equation $\mu\nu = 1$ implies $\epsilon(\mu)\epsilon(\nu) = 1$ so, if μ is a unit, $\epsilon(\mu) \neq 0$. Conversely, if $\mu \in FB$ and $\epsilon(\mu) = \alpha \neq 0$, $\alpha \in F$, then $\epsilon(\alpha^{-1}\mu) = 1$, $\epsilon(1 + \alpha^{-1}\mu) = 0$, so $1 + (1 + \alpha^{-1}\mu) = \alpha^{-1}\mu$ is a unit by Lemma 3.2. Thus μ is a unit. $\square$

The main result of this paper follows quickly.

Corollary 3.4. *If F is a field of characteristic two and B is a finite Bol loop of 2-power order with unique nonidentity commutator/associator, then the set $\mathcal{U}(FB)$ of units in FB is a Bol loop.*

PROOF. By Corollary 3.3, $\mathcal{U}(FB)$ is closed under multiplication. By Theorem 2.1, $\mathcal{U}(FB)$ satisfies the right Bol identity, so the result follows from Lemma 3.1. $\square$

4. Indecomposability

In this section, we justify our special interest in Bol loops of 2-power order in much of Section 3.

Call a loop *indecomposable* if it is not a nontrivial direct product. It is known that any finite indecomposable group or Moufang loop with a unique nonidentity commutator/associator is a *2-loop*, that is, it consists entirely of elements whose order is a power of 2 [GJM96, §V.1], and hence must have order 2^n for some n [GW68]. As we show here, an indecomposable Bol loop with a unique nonidentity commutator/associator is also a 2-loop. While we do not know if this implies that the Bol loop must have 2-power order, Bol loops of 2-power order do consist entirely of elements of order a power of 2 (since the order of an element in a finite Bol loop divides the order of the loop).

We require some identities satisfied by right alternative rings. Recall that $[x, y, z] = (xy)z - x(yz)$ denotes the associator of elements x, y, z in a ring. Thus, the right alternative identity $(xy)y = xy^2$ can be written $[x, y, y] = 0$. Let R be a ring of characteristic two which satisfies this identity. Replacing y by $y + z$ in $[x, y, y] = 0$ gives

$$[x, y, y] + [x, y, z] + [x, z, y] + [x, z, z] = 0.$$

Since $[x, y, y] = [x, z, z] = 0$, we obtain $[x, y, z] + [x, z, y] = 0$ and hence

$$[x, y, z] = [x, z, y]$$

(in characteristic two). Suppose R is strongly right alternative in that it also satisfies the Bol identity (1.1). Then

$$(x \cdot yz)y - x(yz \cdot y) = (x \cdot yz)y - (xy \cdot z)y = -[x, y, z]y = [x, z, y]y,$$

which says that R satisfies the identity

$$[x, yz, y] = [x, z, y]y.$$

Any ring satisfies the *Teichmüller* identity

$$(4.1) \quad [x, y, zw] - [x, yz, w] + [xy, z, w] = x[y, z, w] + [x, y, z]w$$

which can be verified directly. Setting $w = y$ gives

$$[x, y, zy] - [x, yz, y] + [xy, z, y] = x[y, z, y] + [x, y, z]y$$

so that (in characteristic two),

$$(4.2) \quad x[y, y, z] = x[y, z, y] = [x, y, zy] + [x, yz, y] + [xy, z, y] + [x, y, z]y.$$

Setting $z = y$ and $w = z$ in (4.1) and using $[x, y, y] = 0$ gives (in characteristic two)

$$[x, y, yz] + [x, y^2, z] + [xy, y, z] = x[y, y, z] + [x, y, y]z = x[y, y, z]$$

using the right alternative law at the last equality. Comparing with (4.2) gives

$$[x, y, zy] + [x, yz, y] + [xy, z, y] + [x, y, z]y = [x, y, yz] + [x, y^2, z] + [xy, y, z].$$

Since $[xy, z, y] = [xy, y, z]$ and $[x, yz, y] = [x, z, y]y = [x, y, z]y$, we obtain

$$(4.3) \quad [x, y, yz + zy] = [x, y^2, z].$$

In the proof of the theorem which follows, it is convenient to have available some standard loop theoretical terminology. A loop L has three subloops N_λ , N_μ and N_ρ called, respectively, the *left*, *middle* and the *right* nuclei. These are defined by

$$N_\lambda = N_\lambda(L) = \{a \in L \mid (ax)y = a(xy) \text{ for all } x, y \in L\},$$

$$N_\mu = N_\mu(L) = \{a \in L \mid (xa)y = x(ay) \text{ for all } x, y \in L\},$$

$$N_\rho = N_\rho(L) = \{a \in L \mid (xy)a = x(ya) \text{ for all } x, y \in L\}.$$

The *nucleus* of L is $N(L) = N_\lambda \cap N_\mu \cap N_\rho$ and the *centre* of L is

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

Theorem 4.1. *Let B be a finite Bol loop with a unique nonidentity commutator/associator. Then B is the direct product of an abelian group and a Bol 2-loop. In particular, if B is indecomposable and not associative, then B itself is a 2-loop.*

PROOF. Let R be a commutative associative coefficient ring of characteristic two. By Theorem 2.1, the loop ring RB is strongly right alternative. For any y and z in RB , the element $yz + zy$ is the sum of elements of the form $gh + hg$, $g, h \in B$, which is an element of $(1 + s)RB$ as noted in (3.1). Thus $yz + zy = (1 + s)w$ for some $w \in RB$, so $[x, y, yz + zy] = (1 + s)[x, y, w]$. The associator $[x, y, w]$ is the sum of elements of the form $(gh)k + g(hk)$, $g, h, k \in B$, which is also in $(1 + s)RB$ [see (3.2)], so $[x, y, w] = (1 + s)t$ for some $t \in RB$ and $[x, y, zy + yz] = (1 + s)^2 t = 0$. From (4.3), we conclude that $[x, y^2, z] = 0$ for all $x, y, z \in RB$. In particular, $[g, h^2, k] = 0$ for all $g, h, k \in B$; that is, $h^2 \in N_\mu(B)$ for all $h \in B$. In a right Bol loop, it is easy to see that the middle nucleus and right nucleus are identical. Thus $h^2 \in N_\rho(B)$ for all h . By Lemma 3.4 of [GR95], $h^2 \in N_\lambda$ and $gh^2 = h^2g$ for all $g \in L$. Thus squares in B are central.

Let T be the set of all elements in B whose order is a power of 2 and let S be the set of all elements of odd order in B . Since $x^{2n-1} = 1$ implies $x = x^{2n}$, the elements of S are central and hence form a normal subloop. Recall that there is just one commutator and one associator in B , that these are the same (the element we denote s), and that s is central and of order 2. Let $a, b \in T$ and consider

$$\begin{aligned}
 (ab)^2 &= (ab)(ab) \\
 &= a(b \cdot ab)(a, b, ab) \\
 &= a(ba \cdot b)(a, b, ab)(b, a, b) \\
 &= a(ab \cdot b)(a, b, ab)(b, a, b)(a, b) \\
 &= a(ab^2)(a, b, ab)(b, a, b)(a, b) && \text{by the right alternative law} \\
 &= a^2b^2(a, b, ab)(b, a, b)(a, b) && \text{since squares are central.}
 \end{aligned}$$

Each of the associators (a, b, ab) and (b, a, b) , and the commutator (a, b) , is either 1 or s . It follows that $(ab)^4 = a^4b^4$ so that ab also has order a power of 2. In fact, given the equation $ab = c$, it is easy to see that if any two of a, b, c have orders a power of 2, then the third element has order a

power of 2 also. Thus T is a subloop. To prove that T is normal, we must prove that for any $x, y \in B$,

$$xT = Tx, \quad (Tx)y = T(xy) \quad \text{and} \quad x(yT) = (xy)T.$$

Each of these properties follows immediately from the fact that B has a unique commutator/associator which is central of order 2. For example, for any $t \in T$, $(tx)y = t(xy)(t, x, y) = t'(xy)$ with $t' = t(t, x, y) \in T$. It remains only to observe that $B = TS$. For this, let $a \in B$ have order $2^k \ell$ with $2 \nmid \ell$. Write $u2^k + v\ell = 1$ for integers u and v and note that $a = a^{u2^k} a^{v\ell}$ with $(a^{u2^k})^\ell = 1$ (hence $a^{u2^k} \in S$) and $(a^{v\ell})^{2^k} = 1$ (hence $a^{v\ell} \in T$). $\square$

5. An open question

We conclude with an open question which this work has brought to light. For any loop L and field F , the set $\Delta(L) = \{\alpha \in FL \mid \epsilon(\alpha) = 0\}$ is always an ideal (because the augmentation map ϵ is a homomorphism). If FL is alternative (not necessarily associative), L is a 2-loop and F has characteristic two, it is known that $\Delta(L)$ is nilpotent [G0095]: $\Delta(L)^n = \{0\}$ for some n . Is this true if FL is merely (strongly) right alternative? Lemma 3.2 at least gives that $\Delta(L)$ is nil: $\alpha \in \Delta(L)$ implies $\alpha^n = 0$ for some n .

Acknowledgements. The author would like to thank the referee and other readers of this paper for their interest, encouragement and suggestions which have improved this manuscript considerably.

References

- [Alb49] A. A. ALBERT, On right alternative algebras, *Anal. Math.* **50** (1949), 318–328.
- [Bru46] R. H. BRUCK, Contributions to the theory of loops, *Trans. Amer. Math. Soc.* **60** (1946), 245–354.
- [Bur78] R. P. BURN, Finite Bol loops, *Math. Proc. Cambridge Philos. Soc.* **84** (1978), 377–385.
- [GJM96] E. G. GOODAIRE, E. JESPER and C. POLCINO MILIES, Alternative loop rings, vol. 184, *North-Holland Math. Studies, Elsevier, Amsterdam*, 1996.
- [Goo95] EDGAR G. GOODAIRE, The radical of a modular alternative loop algebra, *Proc. Amer. Math. Soc.* **123** no. 11 (1995), 3289–3299.

- [Goo00] EDGAR G. GOODAIRE, Nilpotent right alternative rings and Bol circle loops, *Comm. Algebra* **28** no. 5 (2000), 2445–2459.
- [GR95] EDGAR G. GOODAIRE and D. A. ROBINSON, A class of loops with right alternative loop rings, *Comm. Algebra* **22** no. 14 (1995), 5623–5634.
- [GR96] EDGAR G. GOODAIRE and D. A. ROBINSON, A construction of loops which admit right alternative loop rings, *Resultate Math.* **59** (1996), 56–62.
- [GW68] G. GLAUBERMAN and C. R. B. WRIGHT, Nilpotence of finite Moufang 2-loops, *J. Algebra* **8** (1968), 415–417.
- [Kun98] KENNETH KUNEN, Alternative loop rings, *Comm. Algebra* **26** (1998), 557–564.
- [Mik69] I. M. MIKHEEV, One identity in right alternative rings, *Algebra i Logika* **8** (1969), 357–366.
- [Rob66] D. A. ROBINSON, Bol loops, *Trans. Amer. Math. Soc.* **123** (1966), 341–354.
- [ZSSS82] K. A. ZHEVLAKOV, A. M. SLIN’KO, I. P. SHESTAKOV and A. I. SHIRSHOV, Rings that are nearly associative, *Academic Press, New York*, 1982, translated by Harry F. Smith.

EDGAR G. GOODAIRE
MEMORIAL UNIVERSITY OF NEWFOUNDLAND
ST. JOHN’S, NEWFOUNDLAND, A1C 5S7
CANADA

E-mail: edgar@math.mun.ca

(Received November 23, 2000; revised June 14, 2001)