Publ. Math. Debrecen
72/1-2 (2008), 173–187

Jordan loops and loop rings

By EDGAR G. GOODAIRE (St. John's) and REBECCA G. KEEPING (St. John's)

Abstract. Jordan loop rings can exist only in characteristics not relatively prime to 6. In this paper, we show they exist in characteristic 2, give a number of examples of loops with Jordan loop rings and initiate a study of Jordan loops, a class of loops which has hitherto been largely ignored, perhaps for good reason.

1. Jordan loop rings

A *quasigroup* is a set L together with a binary operation $(a, b) \mapsto ab$ which has the property that given any two of three elements a, b, c in L, the third is uniquely determined by the equation $ab = c$. A *loop* is a quasigroup with identity. Given any loop L and any commutative, associative ring R with 1, one forms the loop ring RL precisely as in the case that L is a group.

Loop rings satisfying interesting identities other than associativity are hard to find. Over twenty years ago, it was shown that a certain restricted class of Moufang loops have loop rings that are not associative, but *alternative*, in the sense that they satisfy the identities

$$x(xy) = x^2y \qquad \text{the left alternative law}$$

and

$$(yx)x = yx^2 \qquad \text{the right alternative law}$$

2000 *Mathematics Subject Classification:* Primary: 20N05; Secondary: 17C50, 17D99, 13M99.
Key words and phrases: Jordan loop, loop ring.
Research supported by a Discovery Grant and an Undergraduate Student Research Award from the Natural Sciences and Engineering Research Council of Canada.

[Goo83]. Some time later, the existence of loop rings satisfying just one of the alternative laws was established [GR95]. Such rings exist only in characteristic 2 [CG88], [Kun98].

A *power associative* loop or ring is one in which every element generates an associative subloop (or subring). A loop (or ring) is *Jordan* if it is commutative and satisfies

$$(x^2y)x = x^2(yx) \qquad \text{the Jordan identity.}$$

In characteristic prime to 6, any commutative power associative loop ring is associative [Pai55], [Osb84]. Since a Jordan ring of characteristic different from 2 is power associative [Sch66, §IV.1], Jordan loop rings of characteristic prime to 6 are associative. One purpose of this paper is to begin filling the implicit gap in these observations by showing that nonassociative[1] Jordan loop rings do exist if the characteristic of the coefficient ring is 2. We then provide a brief introduction to the theory of Jordan loops, a topic to which little attention has apparently been paid hitherto.

In the proof of our main theorem, Theorem 1.1 that follows, it is convenient to use the term *support* for the set of loop elements which actually appear in the canonical representation of a loop ring element, that is, with nonzero coefficients: For $\alpha = \sum_{\ell \in L} \alpha_\ell \ell$, $\text{supp}(\alpha) = \{\ell \mid \alpha_\ell \neq 0\}$.

Theorem 1.1. *Let R be a commutative, associative ring with 1 and of characteristic 2 and let L be a loop. The loop ring RL is nonassociative Jordan if and only if L is a nonassociative Jordan loop and either*

(1) *R is a Boolean ring, that is, $r^2 = r$ for all $r \in R$, and, given any elements $x, y, z \in L$, either*

J1: $x^2y \cdot z = x^2 \cdot yz$ *and* $x \cdot yz^2 = xy \cdot z^2$, *or*

J2: $x^2y \cdot z = xy \cdot z^2$ *and* $x \cdot yz^2 = x^2 \cdot yz$, *or*

J3: $x^2y \cdot z = x \cdot yz^2$ *and* $x^2 \cdot yz = xy \cdot z^2$

or else

(2) J1 *holds for all $x, y, z \in L$.*

Proof. Suppose the loop ring RL is Jordan, but not associative. As a subset of RL, the loop L is certainly Jordan and, were it associative, RL would also be associative, which is not the case. So L is not associative. Next, replacing x by $x + z$ in the Jordan identity, we obtain

$$(x^2y + z^2y)(x + z) = (x^2 + z^2)(yx + yz)$$

[1] In this paper, "nonassociative" means "not associative."

(in characteristic 2). Expanding and cancelling two pairs of terms that are equal because RL is Jordan, we obtain

$$x^2y \cdot z + z^2y \cdot x = x^2 \cdot yz + z^2 \cdot yx. \tag{1}$$

Thinking of x, y, z as loop elements, each side of this equation is the sum of loop elements and these are linearly independent over R. If $x^2y \cdot z$ is not in the support of the left side, then the two terms on the left are equal, the two terms on the right are equal, and we have J3. (Remember that L is commutative.) On the other hand, if $x^2y \cdot z$ is in the support of the left side, then it is in the support of the right as well, so we have either J1 or J2.

Now suppose that given three elements $x, y, z \in L$, we have either J1 or J2 or J3, but that J1 does not hold identically in L. In the first instance, suppose there exist elements $x = \ell_1$, $y = k$, $z = \ell_2$ in L which satisfy J2, but not J1. Thus

$$\ell_1^2k \cdot \ell_2 = \ell_1k \cdot \ell_2^2 \quad \text{and} \quad \ell_1 \cdot k\ell_2^2 = \ell_1^2 \cdot k\ell_2, \tag{2}$$

but

$$\ell_1^2k \cdot \ell_2 \neq \ell_1^2 \cdot k\ell_2 \quad \text{or} \quad \ell_1 \cdot k\ell_2^2 \neq \ell_1k \cdot \ell_2^2. \tag{3}$$

[Note that these two inequalities are equivalent, because of (2).] We claim that R is Boolean. If not, there exists $r \in R$ with $r^2 \neq r$. Let $\alpha = \ell_1 + r\ell_2$ and $\beta = k$ and compare

$$A = (\alpha^2\beta)\alpha = [(\ell_1^2 + r^2\ell_2^2)k](\ell_1 + r\ell_2)$$

with

$$B = \alpha^2(\beta\alpha) = (\ell_1^2 + r^2\ell_2^2)[k(\ell_1 + r\ell_2)]$$

which are equal elements of RL because RL satisfies the Jordan identity. Expanding, subtracting, and using the Jordan identity in L to cancel two pairs of elements, we have

$$A - B = A + B = \left[r\ell_1^2k \cdot \ell_2 + r^2\ell_2^2k \cdot \ell_1\right] + \left[r\ell_1^2 \cdot k\ell_2 + r^2\ell_2^2 \cdot k\ell_1\right].$$

Using equations (2), this is $(r^2 + r)(\ell_1^2k \cdot \ell_2 + \ell_1^2 \cdot k\ell_2)$ which, in view of (3), is a linear combination of two different loop elements with nonzero coefficients and hence nonzero in the Jordan loop ring RL, a contradiction.

With a similar argument, we derive a contradiction from the assumption that there exist elements $x, y, z \in L$ which satisfy J3, but not J1, and obtain necessity of the conditions given in the theorem.

Conversely, suppose L is a Jordan loop that is not associative and either J1 holds for all $x, y, z \in L$ or else R is Boolean and, for any $x, y, z \in L$, at least one

of J1, J2, J3 holds. Clearly the loop ring RL is not associative, so it remains simply to establish the Jordan identity, namely, that $(\alpha^2\beta)\alpha = \alpha^2(\beta\alpha)$ for any $\alpha, \beta \in RL$.

Write $\alpha = \sum_{\ell\in L} \alpha_\ell \ell$ and $\beta = \sum_{k\in L} \beta_k k$. Because $\operatorname{char} R = 2$, $\alpha^2 = \sum \alpha_\ell^2 \ell^2$ so that $(\alpha^2\beta)\alpha$ is the sum of terms of the form $[(\alpha_1^2\ell_1^2)(\beta_k k)](\alpha_2\ell_2) = \alpha_1^2\alpha_2\beta_k\ell_1^2 k\cdot\ell_2$ while $\alpha^2(\beta\alpha)$ is the sum of terms of the form $\alpha_1^2\alpha_2\beta_k\ell_1^2 \cdot k\ell_2$. We wish to show that $(\alpha^2\beta)\alpha = \alpha^2(\beta\alpha)$. After using the Jordan identity to cancel the terms where $\ell_1 = \ell_2$, we note that for each term $\alpha_1^2\alpha_2\beta_k\ell_1^2 k\cdot\ell_2$ in $(\alpha^2\beta)\alpha$ with $\ell_1 \neq \ell_2$, there is a corresponding term $\alpha_2^2\alpha_1\beta_k\ell_2^2 k\cdot\ell_1$, so that $(\alpha^2\beta)\alpha$ is the sum of pairs of terms of the form $A = \alpha_1^2\alpha_2\beta_k\ell_1^2 k\cdot\ell_2 + \alpha_1\alpha_2^2\beta_k\ell_1 \cdot k\ell_2^2$. Similarly, $\alpha^2(\beta\alpha)$ is the sum of pairs of terms of the form $B = \alpha_1^2\alpha_2\beta_k\ell_1^2 \cdot k\ell_2 + \alpha_1\alpha_2^2\beta_k\ell_1 k\cdot\ell_2^2$. We claim that $A = B$ or, equivalently (in characteristic 2), that

$$\alpha_1^2\alpha_2\beta_k(\ell_1^2 k\cdot\ell_2 + \ell_1^2\cdot k\ell_2) + \alpha_1\alpha_2^2\beta_k(\ell_1\cdot k\ell_2^2 + \ell_1 k\cdot\ell_2^2) = 0.$$

If R is not Boolean, but J1 holds identically, then the two elements within each pair of parentheses are equal, so the terms in the parentheses are 0, whereas, if R is Boolean, the coefficients $\alpha_1^2\alpha_2\beta_k$ and $\alpha_1\alpha_2^2\beta_k$ are equal and each of the conditions J1 or J2 or J3 with $x = \ell_1$, $y = k$, $z = \ell_2$ implies that

$$\ell_1^2 k\cdot\ell_2 + \ell_1^2\cdot k\ell_2 + \ell_1 k\cdot\ell_2^2 + \ell_1\cdot k\ell_2^2 = 0.$$

The proof is complete. □

Loops which have alternative loop rings over coefficient rings of any characteristic or in characteristic 2 are known as RA and RA2 loops, respectively. Correspondingly, we make the following definition.

Definition 1.2. A nonassociative loop is *RJ2* if it has a (commutative) Jordan loop ring over some coefficient ring of characteristic 2.

Obviously any commutative loop of exponent 2 satisfies the Jordan identity. Furthermore, since J1 will hold identically, our Theorem 1.1 shows that such a loop is RJ2. Any loop of order not exceeding 4 is a group, so a nonassociative commutative loop of exponent 2 must have order at least five. In fact, it has order at least six.

Lemma 1.3. *In a commutative loop of finite odd order, every element is a square. In particular, a commutative loop of exponent* 2 *has even order.*

Proof. Let a be any element of a commutative loop L of odd order n and consider the loop table. If a appears k times above the diagonal, it appears k times below the diagonal, giving an even number of off-diagonal appearances. Since n is odd, a also appears on the diagonal. □

By hand, by machine or by referring to Fisher and YATES [FY34], one can find representatives of the eight isomorphism classes of commutative loops of order 6. There is one (and only one) nonassociative Jordan loop of this order, with this table:

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	5	3	6	4
3	3	5	1	6	4	2
4	4	3	6	1	2	5
5	5	6	4	2	1	3
6	6	4	2	5	3	1

(4)

It has exponent 2, so it is also RJ2 and, since the only commutative loops of order less than 6 are groups, it is also the smallest nonassociative Jordan loop and the smallest RJ2 loop. We mention also that this loop is simple: there are just two conjugacy classes, $\{1\}$ and $\{2,3,4,5,6\}$.

2. Two constructions

In this section, we present two different constructions of Jordan loops, loops of the first type having Jordan loop rings over any coefficient ring of characteristic 2.

Some loops of exponent 2. For every even order exceeding 5, there exists a nonassociative commutative loop which satisfies the Jordan identity because it has exponent 2. We describe a construction of such loops here.

Let n be an odd positive integer, let $A = \{1,2,3,\ldots,n\}$, and define $f : A \times A \to \{0,1,2,\ldots,n-1\}$ by the rule

$$f(i,j) = \frac{1}{2}(n+1)(j-1) - \frac{1}{2}(n-1)(i-1) \pmod{n}.$$

It is easily checked that for each fixed i, $f(i,\cdot) : A \to \{0,1,2,\ldots,n-1\}$ is a bijection and for each fixed j, $f(\cdot,j) : A \to \{0,1,2,\ldots,n-1\}$ is a bijection. One can also verify that $f(i,j) = f(j,i)$ for all i, j and $f(i,i) = i-1 \pmod{n}$ for each i. As a consequence, the $n \times n$ array whose (i,j) entry is $f(i,j)+2$ is a symmetric Latin square on the integers $\{2,3,4,\ldots,n+1\}$ with (i,i) entry $i-1$. Now form the $(n+1)\times(n+1)$ table that has this square in the lower right corner with all diagonal entries changed to 1, and which has the integers $1,2,3,\ldots,n+1$ in order in row one and in column one. This table defines a commutative loop of exponent 2 and order $n+1$. The loop defined by (4) is an example of this construction with $n = 5$.

If $n+1$ is not a power of 2, no loop realized by this construction can be associative. To show that no such loop is ever associative in general apparently acquires a small calculation. Specifically, we show that $2(2\cdot 3) \neq 2^2 \cdot 3 = 3$. We have

$$2 \cdot 3 = f(1,2) = [\tfrac{1}{2}(n+1) \pmod n] + 2.$$

Since this is not 2,

$$2(2\cdot 3) = f(1, f(1,2)-1) + 2 = \left[\left(\tfrac{1}{2}(n+1)\right)^2 \pmod n\right] + 2.$$

If $2(2\cdot 3) = 3$, then $[\frac{1}{2}(n+1)^2] \pmod n = 1$, so $4 \equiv (n+1)^2 \equiv 1 \pmod n$, a contradiction.

$J(G,\alpha)$ loops. The literature contains many examples of nonassociative loops constructed by "doubling" groups [Voj03], [Voj04], [GJM96, §II.5]. Suggested by the notation $M(G,2)$, which Orin Chein introduced for a family of Moufang loops [Che74], we label $J(G,\alpha)$ a Jordan loop constructed by the following theorem.

Theorem 2.1. *Let G be an abelian group, let u be some element not in G and let $L = G \cup Gu$. Extend the multiplication in G to L by setting*

$$g(hu) = (hu)g = (gh)u$$

and

$$(gu)(hu) = \alpha(g,h)$$

for some symmetric map $\alpha : G\times G \to G$, that is, a map satisfying $\alpha(g,h) = \alpha(h,g)$ for all $g,h \in G$.

i. *The structure $(L,\cdot)$ is a loop if and only if for each $g \in G$, the function $\alpha_g : G \to G$ defined by $\alpha_g(x) = \alpha(g,x)$ is a bijection.*

ii. *The Jordan identity is satisfied in $(L,\cdot)$ if and only if $\alpha(\alpha(g,g)h,g) = \alpha(g,g)\alpha(g,h)$ for all $g,h \in G$.*

iii. *Associativity holds in $(L,\cdot)$ if and only if there exists $a \in G$ such that $\alpha(g,h) = agh$ for all $g,h \in G$.*

Before beginning the proof, we note that for finite G the existence of a map α as described is equivalent to the existence of a symmetric Latin square of order $|G|$, where $\alpha(g,h)$ is the (g,h) entry of the square.

Proof. i. Suppose L is a loop and fix $g \in G$. For any $h \in G$, the equation $(gu)(xu) = h$, which is $\alpha_g(x) = h$, has a unique solution, so α_g is a bijection. Conversely, given that α_g is a bijection for all g, we must prove that given any two

of $a, b, c \in L$, the third element is uniquely determined by the equation $ab = c$. Given a and b, this is clear from the definition of L.

Assume we are given a and c. Table 1, in which g and h are always assumed to be elements of G, shows an element b satisfying $ab = c$ given the four possibilities for $a, c \in G \cup Gu$.

a	c	b
g	h	$g^{-1}h$
g	hu	$(g^{-1}h)u$
gu	h	$\alpha_g^{-1}(h)$
gu	hu	$g^{-1}h$

Table 1. g and h are elements of G.

In each case, uniqueness of b is not hard to establish. In the third line, for example, given $g, h \in G$, the solution b to $(gu)b = h$ must be an element xu, $x \in G$, because of the way multiplication in L is defined. Since $(gu)(xu) = \alpha(g, x) = \alpha_g(x)$ and α_g is invertible, $x = \alpha_g^{-1}(h)$ is unique.

Finally, given b and c, the existence and uniqueness of a solution a to $ab = c$ can be established with an argument similar to the one just given.

ii. The loop is Jordan if and only if $(x^2y)x = x^2(yx)$ for each x and y in G or Gu. Table 2, where again g and h are assumed to be elements of G, establishes this part.

x	y	$(x^2y)x$	$x^2(yx)$
g	h	$(g^2h)g = g^3h$	$g^2(hg) = g^3h$
g	hu	$[(g^2h)u]g = (g^3h)u$	$g^2[(gh)u] = (g^3h)u$
gu	h	$[\alpha(g,g)h]gu = [\alpha(g,g)gh]u$	$[\alpha(g,g)][(gh)u] = [\alpha(g,g)gh]u$
gu	hu	$[\alpha(g,g)(hu)]gu = [\alpha(g,g)h]u \cdot gu$ $= \alpha(\alpha(g,g)h, g)$	$\alpha(g,g)\alpha(h,g)$

Table 2. g and h are elements of G.

iii. Table 3 shows that the loop is associative if and only if

$$\alpha(gh, k) = g\alpha(h, k) \tag{5}$$

$$\alpha(gh, k) = \alpha(g, hk) \tag{6}$$

$$\alpha(g, hk) = \alpha(g, h)k \tag{7}$$

and

$$\alpha(g,h)k = g\alpha(h,k) \tag{8}$$

for all $g, h, k \in G$.

x	y	z	$(xy)z$	$x(yz)$
g	h	k	$(gh)k$	$g(hk)$
g	h	ku	$(gh)(ku) = (ghk)u$	$g[(hk)u] = (ghk)u$
g	hu	k	$[(gh)u]k = (ghk)u$	$g[(hk)u] = (ghk)u$
g	hu	ku	$[(gh)u](ku) = \alpha(gh,k)$	$g\alpha(h,k)$
gu	h	k	$[(gh)u]k = (ghk)u$	$(gu)(hk) = (ghk)u$
gu	h	ku	$[(gh)u](ku) = \alpha(gh,k)$	$gu[(hk)u] = \alpha(g,hk)$
gu	hu	k	$\alpha(g,h)k$	$(gu)[(hk)u] = \alpha(g,hk)$
gu	hu	ku	$[\alpha(g,h)](ku) = [\alpha(g,h)k]u$	$(gu)[\alpha(h,k)] = [g\alpha(h,k)]u$

Table 3. g, h and k are elements of G.

Suppose L is associative. Setting first $h = 1$ and then $k = 1$ in (5) gives $\alpha(g,k) = g\alpha(1,k)$ and $\alpha(g,1) = g\alpha(1,1)$, so $\alpha(g,k) = g\alpha(1,k) = g\alpha(k,1) = gk\alpha(1,1)$ for all g and k. This is the condition of statement iii with $a = \alpha(1,1)$. Conversely, if there exists $a \in G$ with $\alpha(g,h) = agh$ for all $g, h \in G$, then equations (5), (6), (7) and (8) all hold for any $g, h, k \in G$ and L is associative. We have verified statement iii. □

Let $G = \mathsf{Z}_n$, the group of integers under addition (mod n). To produce a Jordan loop of the type $J(G,\alpha)$, we require a symmetric map $\alpha : \mathsf{Z}_n \times \mathsf{Z}_n \to \mathsf{Z}_n$ which satisfies condition ii of Theorem 2.1 or, equivalently, n maps α_i, $i = 0, 1, \ldots, n-1$ satisfying

$$\alpha_i(\alpha_i(i) + j) = \alpha_i(i) + \alpha_i(j) \tag{9}$$

for all i, j. To avoid associativity, we must also ensure that $\alpha_i(j) - i - j$ is not constant.

We find it convenient to set $\lambda_i = \alpha_i(i)$ so that (9) becomes

$$\alpha_i(\lambda_i + j) = \lambda_i + \alpha_i(j) \tag{10}$$

and then to look for symmetric Latin squares on the elements $0, 1, 2, \ldots, n-1$, row i consisting of the elements $\alpha_i(0), \alpha_i(1), \ldots, \alpha_i(n-1)$.

Example 2.2. One obvious solution to (10) can be obtained by setting $\lambda_i = 0$ for all i, in which case any (symmetric) Latin square with 0s on the diagonal "works." The array

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \tag{11}$$

is one such Latin square and this produces the loop $J(\mathsf{Z}_4, \alpha)$ described by Table 4. Note that the Latin square (11) is in the lower right corner and Z_4 is in the upper left. The other corners are defined as in Theorem 2.1: specifically, $g(hu) = (hu)g = (gh)u$. Here $4 = u$, $5 = 1 + u$, $6 = 2 + u$, $7 = 3 + u$ so that, for example, we have $3 + 6 = 3 + (2 + u) = (3 + 2) + u = 1 + u = 5$. Also, $\alpha(0, 0) = 0$ (the $(0, 0)$-entry of the table in (11)) while $\alpha(1, 1) = 0$, so $\alpha(i, j) - i - j$ is not constant. Part iii of Theorem 2.1 now says that this loop of order 8 is not associative.

0	1	2	3	4	5	6	7
1	2	3	0	5	6	7	4
2	3	0	1	6	7	4	5
3	0	1	2	7	4	5	6
4	5	6	7	0	1	2	3
5	6	7	4	1	0	3	2
6	7	4	5	2	3	0	1
7	4	5	6	3	2	1	0

Table 4. The loop $J(\mathsf{Z}_4, \alpha)$ has a Jordan loop ring.

Example 2.3. With $G = \mathsf{Z}_6$ and $i, j \in \{0, 1, 2, 3, 4, 5\}$, define $\alpha(i, j)$ by the table

$$\begin{array}{cccccc} 5 & 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 4 & 5 & 3 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 3 & 1 & 2 & 0 \end{array}$$

This produces the loop $L = J(\mathsf{Z}_6, \alpha)$ defined by Table 5 and the reader may verify that (10) holds for all i, j. Thus L is Jordan, but not associative: $(5 \cdot 6)8 = 11 \cdot 8 = 3$, while $5(6 \cdot 8) = 5 \cdot 1 = 0$. In fact, it is not even power associative:

$7(7(7(7\cdot 7))))=3$, whereas $7^3\cdot 7^3=8\cdot 8=0$.

0	1	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	0	7	8	9	10	11	6
2	3	4	5	0	1	8	9	10	11	6	7
3	4	5	0	1	2	9	10	11	6	7	8
4	5	0	1	2	3	10	11	6	7	8	9
5	0	1	2	3	4	11	6	7	8	9	10
6	7	8	9	10	11	5	0	1	2	3	4
7	8	9	10	11	6	0	1	2	3	4	5
8	9	10	11	6	7	1	2	0	4	5	3
9	10	11	6	7	8	2	3	4	5	0	1
10	11	6	7	8	9	3	4	5	0	1	2
11	6	7	8	9	10	4	5	3	1	2	0

Table 5. The Jordan loop $J(\mathsf{Z}_6,\alpha)$ is not RJ2 and not power associative.

To avoid associativity with this construction when $G=\mathsf{Z}_n$, it is interesting to observe that not all λ_i can be relatively prime to n. Setting $j=0$ and then $j=\lambda_i$ repeatedly in (10) and with $a_i=\alpha_i(0)$, we have $\alpha_i(\lambda_i)=\lambda_i+a_i$, $\alpha_i(2\lambda_i)=\lambda_i+\alpha_i(\lambda_i)=2\lambda_i+a_i$ and, in general, $\alpha_i(r\lambda_i)=r\lambda_i+a_i$. If λ_i is relatively prime to n, any j is of the form $r\lambda_i$, so $\alpha_i(j)=j+a_i$ for each j. Now $\alpha_i(j)=\alpha_j(i)$ gives $j+a_i=i+a_j$ for all i,j. Setting $j=0$, we get $a_i=i+a_0$, so $\alpha_i(j)=j+a_i=i+j+a_0$ for all i,j, with a_0 constant. Thus L is associative.

We now identify some $J(G,\alpha)$ loops that are RJ2.

Theorem 2.4. *Let $L=J(G,\alpha)$ be a loop constructed as in Theorem 2.1. Suppose*

i. $\alpha(g^2h,k)=g^2\alpha(h,k)$ *and*

ii. $\alpha(\alpha(g,g)h,k)=\alpha(g,g)\alpha(h,k)$

for all $g,h,k\in G$. Then L is RJ2.

Proof. Notice that condition ii, with $k=g$ is precisely the condition that L be a Jordan loop—see Theorem 2.1. We conclude the proof by showing that the two conditions are equivalent to J1 holding for all $x,y,z\in L$ and then appeal to Theorem 1.1.

There are eight cases to consider, according as each of the loop elements x, y, z are in G or Gu. We leave it to the reader to verify that in five of the eight cases, J1 holds simply because G is abelian and associative. In one of the remaining

cases, we have $x = g$, $y = hu$, $z = ku$ with $g, h, k \in G$ and require the equality of $x^2y \cdot z = \alpha(g^2h, k)$ and $x^2 \cdot yz = g^2\alpha(h, k)$. In another case, we have $x = gu$, $y = hu$, $z = k$, $g, h, k \in G$ and need the equality of $xy \cdot z^2 = \alpha(g, h)k^2$ and $x \cdot yz^2 = \alpha(g, hk^2)$. In the last case, with $x = gu$, $y = hu$, $z = ku$, $g, h, k \in G$, the condition $x^2y \cdot z = x^2 \cdot yz$ is $\alpha(\alpha(g, g)h, k) = \alpha(g, g)\alpha(h, k)$. □

Remark 2.5. If one defines $\alpha(g, g) = 1$ for all g, then condition ii of Theorem 2.4 is true trivially so, to find an α which makes $J(G, \alpha)$ an RJ2 loop, one has only to make sure that α satisfies condition i. For example, with $G = \mathsf{Z}_4$, the array in (11) defines such an α, and this explains why $J(\mathsf{Z}_4, \alpha)$, the loop depicted in Table 4, has a Jordan loop ring. As shown in the proof of Theorem 2.4, this loop satisfies condition J1 identically, but not for the trivial reason that it has exponent 2.

3. Jordan loops, Jordan loop rings: Is there a future?

Certainly the most-studied loop identities have always been those of "Bol–Moufang type" that were identified and classified by F. Fenyves, that is, identities such as $(xy \cdot z)y = x(yz \cdot y)$ where each side is a monomial of degree four in three variables with the same variable repeated on each side [Fen69]. Whether the Jordan identity has been overlooked because it is not of this type we cannot say. It is clear, though, that Jordan loops fail to satisfy most of the properties typically studied in loop theory. Table 5 describes a Jordan loop that is not power associative. The loop defined by Table 4 shows that Jordan loops do not satisfy the inverse property $(xy)y^{-1} = x$ (which is the same as the cross inverse property in a commutative loop) nor the weak inverse property $y(xy)^{-1} = x^{-1}$ (in each case, take $y = 3$ and $x = 2$). Even when a Jordan loop is power associative so that there is a well-defined notion of "order of an element," one should not expect the order of an element in a finite Jordan loop to divide the order of the loop, as shown by each loop in Table 6 where all nonidentity elements have order 3.

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	5	4	7	6
3	3	1	2	6	7	4	5
4	4	5	6	7	2	3	1
5	5	4	7	2	6	1	3
6	6	7	4	3	1	5	2
7	7	6	5	1	3	2	4

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	5	4	7	6
3	3	1	2	6	7	4	5
4	4	5	6	7	3	2	1
5	5	4	7	3	6	1	2
6	6	7	4	2	1	5	3
7	7	6	5	1	2	3	4

Table 6. The two Jordan loops of order 7

Table 7 describes a power associative Jordan loop of order 8. Let $x = y = 3$ and observe that the inner map $R(x, y) = R(x)R(y)R(xy)^{-1}$ sends 2 to 5, so these elements are conjugate. They do not have the same order, however, these being 2 and 4, respectively.

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

Table 7. A power associative Jordan loop

Historically, there has always been interest in the structure and properties of the units (that is, the invertible elements) of a group ring. In the case of alternative and right alternative loop rings, there has been the added bonus of finding more examples of Moufang and Bol loops, respectively [GJM96, §II.5.3], [Goo01], [Nag02]. Such investigations are of no relevance in the theory of Jordan loop rings because even the concept of "unit" in a Jordan loop ring makes no sense in general. For instance, for $i > 1$, renaming as ℓ_i element i in loop (4), consider the loop ring elements $\alpha = 1 + \ell_5 + \ell_6$ and $\beta = 1 + \ell_2 + \ell_3$. Then $\alpha^2 = \alpha\beta = 1$, so the "inverse" of α is not unique.

4. Open questions

We close with some questions we have considered with less than complete success.

Does there exist a nonassociative Jordan loop of every order greater than 8? We have seen that for every even integer $n \geq 6$, there exists a nonassociative commutative loop of exponent 2 and order n and, in Table 6, we exhibit tables for the two Jordan loops of order 7. By taking the direct product of either loop with a cyclic group of order k, we obtain a nonassociative Jordan loop of order $7k$. Our referee has reported that a computer search finds no nonassociative Jordan loops of order 9. On the other hand, he/she has found a construction for order

$2^n - 1$ that may be adapted to some other odd orders. We ourselves, however, are unable to find examples or constructions of Jordan loops of odd orders $n > 8$ (not of the form $7k$) and the question that heads this subsection is open.

Is a Jordan loop ring power associative? L. Kokoris has shown that if F is a field of characteristic 2 and containing at least four elements, then any Jordan algebra over F is power associative [Kok55]. While we do not know if a Jordan loop ring is power associative in general, we have the following suggestive fact about loops of the type $J(G, \alpha)$.

Theorem 4.1. *Let $L = J(G, \alpha)$ as in Theorem 2.1 and let R be any commutative, associative coefficient ring with 1 and of characteristic 2. If RL is Jordan, then L is power associative.*

Proof. We show that by itself, condition iii of Theorem 2.4

$$\alpha(\alpha(g, g)h, k) = \alpha(g, g)\alpha(h, k) \tag{12}$$

implies that x^n is well-defined for any $x \in L$ and any $n \geq 1$. This is clear for $x \in G$ so we take $x = gu$, $g \in G$, and proceed by mathematical induction. We show that for any $n \geq 1$

(1) any product of $2n$ gu's is $\alpha(g, g)^n$, and

(2) any product of $2n + 1$ gu's is $[\alpha(g, g)^n g]u$.

When $n = 1$ these statements are clearly true since any product of 2 gu's is $gu \cdot gu = \alpha(g, g)$ and any product of 3 gu's is $(gu)^2(gu) = \alpha(g, g) \cdot gu = \alpha(g, g)g \cdot u$. Now assume $n > 1$ and that statements (1) and (2) hold for all positive integers $k < n$. We verify the statements for n.

For the first statement, regardless of the order in which the $2n$ gu terms are multiplied, there will be a last multiplication, say of r gu terms and s gu terms, $r + s = 2n$. We have two cases.

Suppose $r = 2i$ and $s = 2j$ are both even. Since $i < n$ and $j < n$, the induction hypothesis shows that the product is

$$(gu)^{2i}(gu)^{2j} = \alpha(g, g)^i \alpha(g, g)^j = \alpha(g, g)^{i+j} = \alpha(g, g)^n,$$

as required.

If $r = 2i + 1$ and $s = 2j + 1$ are both odd, the induction hypothesis gives

$$(gu)^{2i+1}(gu)^{2j+1} = [\alpha(g, g)^i g \cdot u][\alpha(g, g)^j g \cdot u] = \alpha(\alpha(g, g)^i g, \alpha(g, g)^j g).$$

Repeated applications of (12) give

$$[\alpha(g, g)^i \alpha(g, g)^j]\alpha(g, g) = \alpha(g, g)^{i+j+1} = \alpha(g, g)^n,$$

as required.

Turning to statement (2), we again focus on the last multiplication in the product of $2n+1 = 2k+3$ gu's, which is the product of r factors each gu and s factors each gu. Since the sum of r and s is odd, this time there is only one case. Without loss of generality, let $r = 2i$ and $s = 2j+1$. Again $i < n$ and $j < n$, so the induction hypothesis gives

$$\begin{aligned}(gu)^{2i}(gu)^{2j+1} &= \alpha(g,g)^i[\alpha(g,g)^j g \cdot u] \\ &= \alpha(g,g)^{i+j} g \cdot u = \alpha(g,g)^{\frac{r+s-1}{2}} g \cdot u = \alpha(g,g)^n g \cdot u,\end{aligned}$$

as required. This completes the induction and the proof. □

Is the definition of RJ2 loop independent of coefficient ring? Our definition of "RJ2 loop" takes into account part (1) of Theorem 1.1 which suggests the possibility that a Jordan loop could have a Jordan loop ring over one coefficient ring (of characteristic 2) but not over some other. At present, we have no examples of such loops.

Acknowledgement. We thank the referee for unusually careful reading of our paper, obvious interest in our work and various suggestions for improvement.

References

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

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

[Fen69] Ferenc Fenyves, Extra loops II: On loops with identities of Bol-Moufang type, *Publ. Math. Debrecen* **16** (1969), 187–192.

[FY34] R. Fisher and F. Yates, The 6 × 6 Latin squares, *Math. Proc. Cambridge Philos. Soc.* **30** (1934), 492–507.

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

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

[Goo01] Edgar G. Goodaire, Units in right alternative loop rings, *Publ. Math. Debrecen* **59**, no. 3–4 (2001), 353–362.

[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.

[Kok55] Louis A. Kokoris, Power-associative rings of characteristic two, *Proc. Amer. Math. Soc.* **6**, no. 5 (1955), 705–710.

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

[Nag02] Gábor P. Nagy, On nilpotent loop rings and a problem of Goodaire, *Publ. Math. Debrecen* **61** (2002), 549–554.

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

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

[Sch66] R. D. Schafer, An Introduction to Nonassociative Algebras, *Academic Press, New York*, 1966.

[Voj03] Petr Vojtěchovský, On the uniqueness of loops $m(g, 2)$, *Comment. Math. Univ. Carolin.* **44**, no. 4 (2003), 629–635.

[Voj04] Petr Vojtěchovský, A class of Bol loops with a subgroup of index two, *Comment. Math. Univ. Carolin.* **45** (2004), 371–381.

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

E-mail: edgar@math.mun.ca

REBECCA G. KEEPING
MEMORIAL UNIVERSITY OF NEWFOUNDLAND
ST. JOHN'S, NEWFOUNDLAND
CANADA A1C 5S7

E-mail: rkeeping@math.mun.ca

(Received October 16, 2006; revised March 22, 2007)