Quasigroups and Related Systems **15** (2007), 1 − 18

Advances in loop rings and their loops

Edgar G. Goodaire

Dedicated to the Memory of D. A. Robinson

Abstract

We describe some of the advances in the theory of loops whose loop rings satisfy "interesting" identities that have taken place in the past ten years.

1. Introduction

Let L be a loop and R a commutative associative ring with 1. The loop ring RL is constructed in precisely the same way the group ring would be constructed if L were associative. Of special significance is the fact that each $\alpha \in RL$ can be represented uniquely in the form $\alpha = \sum_{\ell \in L} \alpha_\ell \ell$, with the $\alpha_\ell \in R$ almost all 0.

While historically, loop rings made an occasional appearance in the literature, notably with a semisimplicity result of Bruck [2] (a nonassociative version of the theorem of Maschke for group rings), and a proof by Paige that in most characteristics, a commutative power associative loop algebra is a group algebra [31], nonassociative loop rings[1] appear to have been little more than a curiosity until the 1980s when the author found a class of nonassociative Moufang loops whose loop rings satisfy the alternative laws.

In 1998, at the fifteenth Brazilian "Escola de Álgebra" held that summer in Canela, I gave a talk on the history of loop rings, such as the subject was at that time [13]. "Loops '07" presents a natural forum for an update, which is the subject of this paper. Much of the work described here is joint with Orin Chein or César Polcino Milies.

2000 Mathematics Subject Classification: Primary: 20N05; Secondary: 17D05

Keywords: Loop, Moufang, Bol, Jordan, loop ring

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

2. Alternative loop rings

Alternative rings are those satisfying

the right alternative law $(yx)x = yx^2$

and

the left alternative law $x(xy) = x^2y$

and can be thought of as the ring-theoretic analogues of Moufang loops. For instance, the subring of an alternative ring generated by any two elements is associative (this property is called *diassociativity*). Moreover, alternative rings satisfy the familiar

right Moufang identity $(xy \cdot z)y = x(y \cdot zy)$

and

left Moufang identity $(xy \cdot x)z = x(y \cdot xz)$.

Thus, if RL is an alternative ring, then L is a Moufang loop. The converse is certainly not true, in general. It is not hard to see that the repeated variable in a Moufang identity makes it unlikely to linearize to the ring RL. On the other hand, some Moufang loops do have alternative loop rings. Those that have alternative loop rings in any characteristic are called *RA loops*. Such loops are well understood.

Let G be any nonabelian group with an involution $g \mapsto g^*$ satisfying $gg^* \in \mathcal{Z}(G)$, the centre of G, for all $g \in G$. Let u be an indeterminate and let L be the set $G \cup Gu$. Extend the multiplication from G to L via the rules

$$g(hu) = (hg)u$$
$$(gu)h = (gh^*)u$$
$$(gu)(hu) = g_0h^*g$$

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

If L is RA, then L has form $M(G, *, g_0)$. Moreover,

- G has a unique nonidentity commutator, always denoted s, which is a unique nonidentity commutator and associator in L,

- both G and L have what is known as

  the LC property: $ab = ba$ if and only if a or b or ab is central

  and

- the involution on G takes the form

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{Z}(G) \\ sg & \text{otherwise.} \end{cases} \tag{1}$$

These properties were first found by Orin Chein and the author [7] and are fully described in a monograph written with Eric Jespers and César Polcino Milies [15].

With a hint at what was to come in other varieties, it soon became clear that by restricting the coefficient ring to characteristic 2, many more loops have alternative loop rings. Calling such loops *RA2*, those with the structure $M(G, *, g_0)$ have been classified [13, 11], although there are indeed RA2 loops not of this form. The smallest is the one Chein denotes $M_{32}(B, 5)$.

Suggestion 1. (Reasonable) Find more classes of RA2 loops.

Suggestion 2. (Optimistic) Classify RA2 loops.

3. Strongly right alternative loop rings

A *right alternative* ring is a ring which satisfies the right alternative law. In characteristic different from 2, it is not hard to show that a right alternative ring satisfies

the right Bol identity $(xy \cdot z)y = x(yz \cdot y)$.

It has long been known that a finite dimensional simple right alternative algebra with 1 is alternative [1]. This fact, together with Bruck's version of Maschke's theorem referenced earlier, allowed Chein and the author to conclude that in characteristic different from 2, when the loop is finite, a right alternative loop algebra must be alternative [8]. Later, Kenneth Kunen removed the restriction on finiteness and placed whatever theory might develop for right alternative loop rings squarely within the context of characteristic 2 [27], a rather idiosyncratic characteristic since it is the only characteristic in which the right Bol identity is not a consequence of the right alternative law. In fact, Kunen has even found a right alternative loop ring which does not satisfy the right Bol identity. Since such rings are bizarre (and probably to be avoided), we say that a loop ring RL is *strongly right alternative* and the loop L is *SRAR* (for *strongly right alternative ring*) if RL satisfies the right Bol identity, but not the left, $(x \cdot yx)z = x(y \cdot xz)$. [A ring satisfying both Bol identities is alternative.]

We emphasize that strongly right alternative loop rings that are not alternative can exist only in characteristic 2. In the 1990s, D. A. Robinson and the author showed that RL is strongly right alternative if and only if L is a (right) Bol loop (that is, a loop satisfying the right Bol identity,[2]) and, for every $x, y, z, w \in L$, at least one of the following conditions holds:

$$\begin{aligned} D(x,y,z,w)\colon &\ [(xy)z]w = x[(yz)w] \text{ and } [(xw)z]y = x[(wz)y] \\ E(x,y,z,w)\colon &\ [(xy)z]w = x[(wz)y] \text{ and } [(xw)z]y = x[(yz)w] \qquad (2) \\ F(x,y,z,w)\colon &\ [(xy)z]w = [(xw)z]y \text{ and } x[(yz)w] = x[(wz)y]. \end{aligned}$$

It was observed that any Bol loop with a unique nonidentity commutator/associator is SRAR [24, 25] and, for a long time, such loops provided the only examples of SRAR loops. Indeed, there are families of Bol loops such as those Chein and the author have denoted $L(B, m, n, r, s, t, z, w)$ which are SRAR only if the subloop L' generated by all commutators and associatiors has order 2 [10].

Research with Orin Chein, currently still at the preprint stage, has shown that the conjecture that $|L'| = 2$ characterizes SRAR loops is false. Some of this work we now describe.

Let L be a Bol loop with an index 2 left nucleus N. Fix $u \in L\backslash N$. Then L is the union $N \cup Nu$ and multiplication in L can be defined entirely in terms of multiplication in N and two bijections $\theta\colon N \to N$ and $\phi\colon N \to N$, these being defined by

$$un = (n\theta)u \quad \text{ and } \quad n\phi = u(nu).$$

Specifically, for $n_1, n_2 \in N$, we have

$$\begin{aligned} n_1(n_2u) &= (n_1n_2)u, \\ (n_1u)n_2 &= n_1(un_2) = [n_1(n_2\theta)]u \qquad (3) \end{aligned}$$

[2] In this paper, all Bol loops are assumed to satisfy the right Bol identity.

and

$$(n_1u)(n_2u) = n_1[u(n_2u)] = n_1(n_2\phi).$$

Furthermore, if L is not Moufang, then in either of the cases $\theta = I$, the identity map on N, or $\phi = R(u^2)$, right multiplication by $u^2 \in N$, L is SRAR [6]. Using this fact, one can exhibit families of examples of SRAR loops many of which have more than a single nonidentity commutator/associator. We present two such families.

Let N be an elementary abelian 2-group of order at least 8, let $\theta = I$ and let ϕ be any nonidentity bijection on N such that $\phi^2 = I$ and ϕ is not a right multiplication map. Let $L = N \cup Nu$, u an indeterminate, and extend the binary operation on N to L by means of the equations (3). Then L is an SRAR loop with left nucleus N and, in many cases, $|L'| > 2$.

Alternatively, let N be an abelian group of exponent 4, let u^2 be any element of order 2 in N, let $\phi = R(u^2)$, let $n\theta = n^{-1}$ for $n \in N$ and construct a loop L as before. Again, L is SRAR and often $|L'| > 2$. In passing, we mention that this family of loops is one discussed by P. Vojtěchovský in [36], specifically the class labelled $G(\theta_{xy}, \theta_{xy}, \theta_{x^{-1}y}, \theta_{xy})$. (The reader should, however, be aware of the fact that Vojtěchovský's loops are left Bol.)

We conclude this section with some suggestions for further investigations. It may be important to note that this is certainly not the first time that loops with large nuclei have appeared in the literature. Indeed, some years ago, D. A. Robinson and the author showed that any loop with an index 2 nucleus is *conjugacy closed* and hence a *G-loop*, that is, isomorphic to all its loop isotopes [23]. This is certainly not the case for a Bol loop with left nucleus of index 2. Still, such loops may have other elements of interest.

Suggestion 3. What can be said about a Bol loop with index 2 left nucleus?

Suggestion 4. While it is probably unrealistic to try to characterize SRAR loops at this time, it would be useful to find more families of SRAR loops.

4. Jordan loops

Much of the work described in this section is joint with a student, Rebecca Keeping.

The theorem of Lowell Paige cited earlier, asserting that in most characteristics a commutative power associative loop ring is associative, may explain why the possible existence of Jordan loop rings has been overlooked. A ring is *Jordan* if it is commutative and satisfies

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

Paige's work (with a small correction by Marshall Osborn [30]) shows that a Jordan loop ring is associative in characteristic prime to 6, so nonassociative Jordan loop rings can exist only in characteristics divisible by 2 or by 3. As we shall see, they certainly exist in characteristic 2.

Theorem 1. [16] *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 commutative loop satisfying the Jordan identity 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*

   $$\begin{aligned} &J1: (x^2y)z = x^2(yz) \ \textit{ and } \ x(yz^2) = (xy)z^2, \ \textit{ or} \\ &J2: (x^2y)z = (xy)z^2 \ \textit{ and } \ x(yz^2) = x^2(yz), \ \textit{ or} \\ &J3: (x^2y)z = x(yz^2) \ \textit{ and } \ x^2(yz) = (xy)z^2 \end{aligned}$$

   or else

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

Each of the properties RA, RA2 and SRAR is equivalent to conditions just on the loop. Those which characterize SRAR loops were given in (2), for instance. Theorem 1 highlights the first instance of a situation where the possibility of a loop ring satisfying an "interesting" identity may depend also on the coefficient ring. (No examples of this phenomenon are known as yet.)

Question 5. *Does there exist a nonassociative loop whose loop ring is Jordan over one coefficient ring of characteristic 2 but not over some other ring of characteristic 2?*

Until this question has been answered, we use the term $RJ2$ to describe a loop which has a nonassociative Jordan loop ring over **some** coefficient ring of characteristic 2.

There are other instances in the literature where the existence of an identity in an algebra may depend on the field of coefficients. L. Kokoris, for example, has shown that a Jordan algebra over a field of characteristic 2 is power associative provided that field contains at least four elements [26]. It follows from this that any loop which is $RJ2$ because it satisfies J1 identically must be power associative. We do not know if this must always be the case.

Question 6. Is an $RJ2$ loop power associative?

One can also ask an apparently stronger question.

Question 7. Is a Jordan loop ring power associative?

The second question might follow from the first, of course.

Question 8. *Is the loop ring of a power associative $RJ2$ loop power associative?*

Call a loop *Jordan* if it is commutative and satisfies the Jordan identity. Clearly any $RJ2$ loop is Jordan though the converse is certainly false. Jordan loops exist in abundance as we demonstrate with an observation and some constructions. Any commutative loop of exponent 2 is Jordan and even $RJ2$ because it clearly satisfies J1 identically. Here is a way to construct some such loops.

Let n be an odd positive integer, let $A = \{1, 2, 3, \ldots, n\}$, and define $f\colon A \times A \to \{0, 1, 2, \ldots, n-1\}$ 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, $f(i,\cdot)\colon A \to \{0, 1, 2, \ldots, n-1\}$ is a bijection and for each fixed j, $f(\cdot,j)\colon A \to \{0, 1, 2, \ldots, n-1\}$ 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 their natural order in row one and in column one. The unique nonassociative commutative loop of order 6 arises from this construction with $n = 5$ and is defined by Table 1. For reasons noted, the loop ring of this loop is Jordan in characteristic 2.

	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

Table 1: The unique (nonassociative) Jordan loop of order 6.

The literature contains many examples of nonassociative loops constructed by "doubling" groups [35, 36, 4, 5],[15, §II.5]. Suggested by the notation $M(G,2)$ which Orin Chein introduced for a certain family of Moufang loops, we label $J(G,\alpha)$ a Jordan loop constructed by the following theorem.

Theorem 2. [16] *Let G be an abelian group, let u be an indeterminate, let $L = G \cup Gu$ and let $\alpha\colon G \times G \to G$ be any symmetric map, that is, a map satisfying $\alpha(g,h) = \alpha(h,g)$ for all $g,h \in G$. Extend the multiplication in G to L by setting*

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

and

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

for $g,h \in G$. The pair $(L,\cdot)$ is a loop if and only if for each $g \in G$, the function $\alpha_g\colon G \to G$ defined by $\alpha_g(x) = \alpha(g,x)$ is a bijection and, when this is the case,

1. *Jordan if and only if $\alpha(\alpha(g,g)h,g) = \alpha(g,g)\alpha(g,h)$ for all $g,h \in G$, and*
2. *associative if and only if there exists $a \in G$ such that $\alpha(g,h) = agh$ for all $g,h \in G$.*

Remark 3. *Notice that maps α which define loops correspond to $|G| \times |G|$ Latin squares with $\alpha(g,h)$ in position (g,h).*

As an example of how this theorem can be used, start with $G = \mathsf{Z}_n$, the group of integers under addition $\pmod n$. We require a symmetric map $\alpha\colon \mathsf{Z}_n \times \mathsf{Z}_n \to \mathsf{Z}_n$ with the property that

$$\alpha(i,\alpha(i,i)+j) = \alpha(i,i) + \alpha(i,j)$$

for all $i, j \in G$. Equivalently, writing $\alpha_i(\cdot) = \alpha(i, \cdot)$ and setting $\lambda_i = \alpha_i(i)$, for each $i \in \{0, 1, 2, \ldots, n\}$, we need a bijection α_i of $\{0, 1, 2, \ldots, n-1\}$ (which becomes row i of a Latin square) satisfying

$$\alpha_i(\lambda_i + j) = \lambda_i + \alpha_i(j) \tag{4}$$

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

One obvious solution to (4) can be obtained by setting $\lambda_i = 0$ for all i, in which case any (symmetric) Latin square with 0s on the diagonal defines a suitable α. The table

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \tag{5}$$

shows a smallest such square and yields the loop $J(\mathsf{Z}_4, \alpha)$ described by Table 2. While this loop is not of exponent 2, it is $RJ2$ by virtue of Theorem 4 that follows.

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

Theorem 4. *Let $L = J(G, \alpha)$ be a loop constructed as in Theorem 2. 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 $g, h, k \in G$. If $\alpha(g, h)g^{-1}h^{-1}$ is not constant, then L is $RJ2$.

Is there a future for Jordan loops? They have little structure. We have noted that they need not be power associative. They don't 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, $y(xy)^{-1} = x^{-1}$. Also, even in a finite power associative Jordan loop where there is a well-defined notion of "order of an element," the order of an element need not divide the order of the loop nor must conjugate elements have the same order.

As to existence, we recall that any commutative loop of order less than 6 is associative and we have shown how to construct nonassociative Jordan loops of every even order $n \geqslant 6$. There are two Jordan loops of order 7 (neither of which is $RJ2$) so, by taking direct products, we have a nonassociative Jordan loop of order $7k$ for any positive integer k. A referee has reported a construction that produces Jordan loops of order $2^n - 1$ and perhaps of some other odd orders as well. All this work addresses a natural question.

Question 9. *For what positive integers n does there exist a nonassociative Jordan loop of order n?*

5. The unit loop of an alternative loop ring

Just as with associative rings, the set of invertible elements or *units* of an alternative ring is closed under multiplication and hence forms a (Moufang) loop. The loops of units in alternative loop rings present a class of Moufang loops which have been and continue to be studied from a number of points of view.

5.1 Properties shared by L and $\mathcal{U}$(RL). An RA loop L is a subloop of the unit loop $\mathcal{U}(RL)$ and so one can ask what these loops might have in common. Here, the coefficient ring R is critical since, for example, over the integers, if L is finite and $\mathcal{U}(\mathsf{Z}L)$ contains nontrivial units ($\mathcal{U}(\mathsf{Z}L) \neq \pm L$), then it contains a free group [15, §VIII.5], so it is rare that $\mathcal{U}(\mathsf{Z}L)$ is nilpotent or solvable or torsion over its centre, these being known properties of L. These properties do prove interesting, however, for infinite loops and over fields. It turns out that the *torsion subloop* of L, this being the set of all elements of finite order in L (which is a subloop of an RA loop), often plays an important role. Here is a typical result.

Theorem 5. [20] *Let L be an RA loop with torsion subloop T and let K be a field of characteristic* 0. *Assume $\mathcal{U} = \mathcal{U}(KL)$ contains an element of infinite order. Then the following statements are equivalent:*

1. *$\mathcal{U}$ is torsion over its centre;*
2. *T is central;*
3. *$u^2 \in \mathcal{Z}(\mathcal{U})$ for all $u \in \mathcal{U}$;*
4. *$\mathcal{U}$ is torsion of bounded exponent over its centre.*

5.2 Involutions of RA Loops. An RA loop L has a canonical involution $\ell \mapsto \ell^*$, defined by lifting the involution in (1), whose fixed point set is precisely $\mathcal{Z}(L)$, the centre of L. Any involution of L extends linearly to an involution of the loop ring and, when canonical, the fixed point set of this extended involution is $\mathcal{Z}(RL)$, the centre of RL. Interestingly, this is the only involution of an RA loop with this property.

Theorem 6. *[22] Let θ be an involution of an RA loop and let $(RL)^+ = \{\alpha \in RL \mid \alpha^\theta = \alpha\}$ denote the fixed points of RL. Assuming* $\operatorname{char} R \neq 2$, *the following statements are equivalent:*

1. *$(RL)^+$ is closed under multiplication;*
2. *the elements of $(RL)^+$ commute;*
3. *$(RL)^+ = \mathcal{Z}(RL)$;*
4. *$\theta = *$ is the canonical involution on L.*

Incidentally, Polcino Milies and the author have also considered the possibility that the set $(RL)^- = \{\alpha \in RL \mid \alpha^\theta = -\alpha\}$ of skew-symmetric elements of an involution θ commute. This happens only in characteristic 2 or 4 and in characteristic 2, often with severe restrictions on L [22].

Theorem 7. [21] *Let L be a finite RA* 2*-loop, F a field of characteristic* 2 *and θ the involution of RL which is the linear extension of $\ell \mapsto \ell^{-1}$ for $\ell \in L$. If $(RL)^-$ is a commutative set, then $L = L_0 \times A$ is the direct product of an abelian group A and a loop L_0 which is either the Cayley loop or the loop $M(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_2^\sharp, 16\Gamma_2 c_2^\sharp)$ (in the notation of Chein* [5]*).*

5.3 The units of a right alternative loop ring. The units of a strongly right alternative loop ring form a loop in the presence of a certain condition on the *augmentation ideal*, this being the kernel $\Delta(L)$ of the *augmentation map* $\epsilon\colon RL \to R$ which is defined by $\epsilon(\sum \alpha_\ell \ell) = \sum \alpha_\ell$. Thus

$$\Delta(L) = \{\textstyle\sum \alpha_\ell \ell \in L \mid \sum \alpha_\ell = 0\}.$$

If $\delta \in \Delta(L)$ is *nil*, that is, $\delta^n = 0$ for some $n \geqslant 1$, then it is easily checked that $1+\delta$ is a unit with inverse $1+\delta+\delta^2+\cdots+\delta^{n-1}$. (We now necessarily assume characteristic 2.) Conversely, if $u \in RL$ is a unit, then $uv = 1$ for some v yields $\epsilon(u) = 1$, because ϵ is a homomorphism, so $\delta = 1+u \in \Delta(L)$ and $u = 1+\delta$. These observations show that if $\Delta(L)$ is nil, then

$$\mathcal{U}(RL) = \{u \in RL \mid \epsilon(u) = 1\},$$

a set which is clearly closed under multiplication and hence a Bol loop.

If L is a finite 2-group or RA2 2-loop and F is a field of characteristic 2, then the augmentation ideal of FL is actually *nilpotent*: there exists a fixed n so that any product of n elements is always 0 [28, 12]. Gábor Nagy has shown the same thing for Bol 2-loops with a unique nonidentity commutator/associator [29] but the unrestricted case appears to be open.

Question 10. *If L is any SRAR 2-loop, is $\Delta(L)$ nilpotent?*

A positive answer would imply that the unit loop of RL is Bol for any SRAR loop L, a fact currently known just for SRAR loops with a unique nonidentity commutator/associator [14].

5.4 Normal Complements. As we have noted, if L is a group, then $\mathcal{U}(RL)$ is a group and if L is RA, then $\mathcal{U}(RL)$ is a loop. It is often (perhaps always) the case that if L is SRAR, then $\mathcal{U}(RL)$ is loop. Whenever this happens, it is of interest to know how L sits within $\mathcal{U}(RL)$. It is rare that L is normal. A torsion RA loop L is normal in $\mathcal{U}(\mathsf{Z}L)$, for instance, only in the trivial case that $\mathcal{U}(\mathsf{Z}L) = \pm L$ [17] and, if finite, never normal in $\mathcal{U}(FL)$ when F is a field [19].

Question 11. *Can an infinite RA loop L ever be normal in $\mathcal{U}(FL)$, F a field?*

Assuming L is not normal, it is natural then to ask just what the normalizer of L in $\mathcal{U}(RL)$ might be. Certainly L normalizes itself, as does the centre of $\mathcal{U}(RL)$. The "normalizer conjecture," which asserts $\mathcal{N}_{\mathcal{U}}(L) = \mathcal{Z}[\mathcal{U}(RL)] \cdot L$, says that these are essentially the only normalizing sets. The conjecture is true for torsion RA loops in their integral loop rings [17].

Perhaps the most famous problem in the theory of loop rings has always been the *isomorphism problem*: When does $RL_1 \cong RL_2$ imply $L_1 \cong L_2$? Of special interest because of its connection to the isomorphism problem is the possibility that L might have a *normal complement* in $\mathcal{U} = \mathcal{U}(RL)$, a subloop N that is normal in $\mathcal{U}$ and satisfies $L \cap N = \{1\}$ and $\mathcal{U} = LN$. It is known, for example, that if L is a finite RA loop, then L has a normal complement in $\mathcal{U}(\mathsf{Z}L)$ which is also *torsion-free*: $u^n = 1$ with $n > 1$ implies $u = 1$. So the isomorphism problem has a positive solution over Z and the proof is not hard.

Theorem 8. [19, 18] *Let L and L_1 be finite RA loops and suppose that $\mathsf{Z}L_1 \cong \mathsf{Z}L$. Then $L_1 \cong L$.*

Proof. We observe that L and L_1 have the same order since each is the rank of the same free Z-module. Suppose $\varphi\colon \mathsf{Z}L_1 \to \mathsf{Z}L$ is the given isomorphism and let N be a torsion-free normal complement for L_1 in $\mathcal{U}(\mathsf{Z}L_1)$. Then $\varphi(N)$ is torsion-free in $\mathcal{U}(\mathsf{Z}L)$, so $L \cap \varphi(N) = \{1\}$ and $L\varphi(N)/\varphi(N) \cong L/(L \cap \varphi(N)) \cong L$.

Since $[\mathcal{U}(\mathsf{Z}L)\colon \varphi(N)] = |L_1| = |L| = [L\varphi(N)\colon \varphi(N)]$, we have $\mathcal{U}(\mathsf{Z}L) = L\varphi(N)$. Thus

$$L_1 \cong \mathcal{U}(\mathsf{Z}L_1)/N \cong \mathcal{U}(\mathsf{Z}L)/\varphi(N) \cong L\varphi(N)/\varphi(N) \cong L. \qquad \square$$

Another setting in which the isomorphism problem has been investigated for group rings is that where the group is a finite p-group and the coefficient ring is the field of p elements, the so-called *modular case.*

Suppose $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_d \rangle$ is an abelian p-group written as the direct product of cyclic groups generated by elements a_i of order $|a_i|$, $i = 1, \ldots, d$. For each d-tuple $\delta = (\delta_1, \delta_2, \ldots, \delta_d)$ of integers δ_i, $0 \leqslant \delta_i < |a_i|$ not all divisible by p, let $P(\delta) = (a_1 - 1)^{\delta_1}(a_2 - 1)^{\delta_2} \cdots (a_d - 1)^{\delta_d}$. Robert Sandling has shown that the elements $1 + P(\delta)$ generate the cyclic components of $\mathcal{U}(FG)$, F the field of p elements [33].

It is helpful to look at an example. Suppose $p = 2$ and $G = \langle a \rangle \times \langle b \rangle$ is the direct product of cyclic groups of orders 2 and 4, respectively. The elements $P(\delta)$ are

$$\begin{aligned} x_1 &= a+1 \\ x_2 &= (a+1)(b+1) \\ x_3 &= (a+1)(b+1)^2 \\ x_4 &= (a+1)(b+1)^3 \\ x_5 &= b+1 \\ x_6 &= (b+1)^3, \end{aligned}$$

so $\mathcal{U}(FG) = \prod\langle 1+x_i\rangle$. Notice that $1+x_1 = a$ and $1+x_5 = b$, so that G is actually a direct factor of the unit group.

Now suppose G is a finite nonabelian p-group. Write

$$G/G' = \langle\bar{a}_1\rangle \times \langle\bar{a}_2\rangle \times \cdots \times \langle\bar{a}_d\rangle,$$

with $\bar{a} = G'a$ and this time, for each d-tuple $\delta = (\delta_1, \delta_2, \ldots, \delta_d)$ of integers δ_i, $0 \leqslant \delta_i < |\bar{a}_i|$ not all divisible by p, let

$$P(\delta) = (a_1-1)^{\delta_1}(a_2-1)^{\delta_2}\cdots(a_d-1)^{\delta_d}.$$

Let $J = \Delta(G)\Delta(G') + \Delta(G')\Delta(G)$ and let $w(G)$ be the ideal generated by $1+J$ and the set of all $1+P(\delta)$. Under certain conditions, which include the case $|G'| = 2$ of interest to us, Sandling proves that $w(G)$ is a normal complement to G in $\mathcal{U}(FG)$ [34] and then, with just a little more work, establishes a positive solution to the isomorphism problem. Here's an example.

Writing $D_4 = \langle a, b \mid a^4 = b^2 = 1, ba = a^{-1}b\rangle$ and $C_2 = \langle c\rangle$, let $G = D_4 \times C_2$. We have $G' = \{1, s\}$ with $s = a^2$ and $G/G' = \langle\bar{a}\rangle \times \langle\bar{b}\rangle \times \langle\bar{c}\rangle \cong C_2 \times C_2 \times C_2$, so the elements $P(\delta)$ here are precisely the elements

$$\begin{aligned} x_1 &= a+1 \\ x_2 &= (a+1)(b+1) \\ x_3 &= (a+1)(c+1) \\ x_4 &= b+1 \\ x_5 &= (b+1)(c+1) \\ x_6 &= c+1 \\ x_7 &= (a+1)(b+1)(c+1). \end{aligned}$$

Since $\Delta(G') = \{0, 1+s\}$, the ideal $J = \Delta(G)(1+s) = (1+s)X$, with $X = \{1, a, b, c, ab, ac, bc, abc\}$, and the subgroup $w(G)$ generated by $1+J$ and the $1+P(\delta)$ is a normal complement to G in $\mathcal{U}(FG)$. It is delightful that the normal complements described are so concrete.

While attempts have been made to adapt Sandling's arguments to the case of RA loops, these cannot meet with success, as we now show.

Let a, b, x be three elements which do not associate in an RA 2-loop L. The LC property says $(a,x) = (b,x) = (ab,x) = s$. (Noteworthy is the fact that such elements do not exist in the associative case.) With F the field of two elements, we compute

$$\begin{aligned} x^{-1}[(a+1)(b+1)]x &= x^{-1}(ab+a+b+1)x \\ &= sab+sa+sb+1 \\ &= 1+s[1+(a+1)(b+1)] \end{aligned}$$

and obtain

$$x^{-1}[1+(a+1)(b+1)]x = s[1+(a+1)(b+1)]. \tag{6}$$

Now think of a and b as amongst the generators of L/L' so that $1+(a+1)(b+1) = 1+P(\delta)$ for a certain δ. If $w(L)$ is normal, it contains the element (6), which is $s(1+P(\delta))$, so it contains s. We conclude that if $w(L)$ is normal, it is not a complement for L in $\mathcal{U}(FL)$.

This observation, of course, begs the question as to whether or not L might have some other normal complement. In this connection, we can report that Eric Moorhouse has verified computationally that none of the Moufang loops of order 16 (these are all RA2) has a normal complement in $\mathcal{U}(FL)$, F the field of two elements. Moreover, again via computation, it has been shown that three of the six nonMoufang Bol loops of order 8 (which are all SRAR) have normal complements in the units of FL (these are $B_8(\Pi_2)$, $B_8(\Pi_5)$,$B_8(\Pi_6)$ in the notation of R. P. Burn [3]), and three do not.

Question 12. *If L is an RA (even an RA2) 2-loop, can L ever have a normal complement in $\mathcal{U}(FL)$, F the field of two elements?*

Suggestion 13. *Find conditions under which L has a normal complement in $\mathcal{U}(FL)$ in the case that L is an SRAR 2-loop, F the field of two elements, assuming the units of FL form a loop.*

Tribute

This paper has been written with a heavy heart within a month of the passing of a dear friend and research partner. I met Dan Robinson at Oberwolfach in the spring of 1976. During a sabbatical year at the Georgia Institute of Technology in 1979-80, Dan told me about loops and introduced me to some basic theory. It was during that year that my first paper on alternative loop rings was written. Daniel Robinson was a wonderful friend and mathematician whom I miss every day.

References

[1] **A. A. Albert**: *On right alternative algebras*, Anal. Math. **50** (1949), 318 – 328.

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

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

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

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

[6] **O. Chein and E. G. Goodaire**: *Bol loops with more than two commutators*, preprint.

[7] **O. Chein and E. G. Goodaire**: *Loops whose loop rings are alternative*, Comm. Algebra **14** (1986), 293 – 310.

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

[9] **O. Chein and E. G. Goodaire**: *Code loops are $RA2$ loops*, J. Algebra **130** (1990), 385 – –387.

[10] **O. Chein and E. G. Goodaire**: *When is an $L(B, m, n, r, s, t, z, w)$ loop SRAR?*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 245 – 255.

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

[12] **E. G. Goodaire**: *The radical of a modular alternative loop algebra*, Proc. Amer. Math. Soc. **123** (1995), 3289 – 3299.

[13] **E. G. Goodaire**: *A brief history of loop rings*, Mat. Contemp. **16** (1999), 93 – 109.

[14] **E. G. Goodaire**: *Units in right alternative loop rings*, Publ. Math. Debrecen **59** (2001), 353 – 362.

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

[16] **E. G. Goodaire and R. G. Keeping**: *Jordan loops and loop rings*, to appear, Publ. Mat. Debebrecen, post 2006.

[17] **E. G. Goodaire and Yuanlin Li**: *The normalizer conjecture in the alternative case*, Algebra Colloq. **8** (2001), 455 – 462.

[18] **E. G. Goodaire and C. P. Milies**: *Isomorphisms of integral alternative loop rings*, Rend. Circ. Mat. Palermo **37** (1988), 126 – 135.

[19] **E. G. Goodaire and C. P. Milies**: *Normal subloops in the integral loop ring of an RA loop*, Canad. Math. Bull. **44** (2001), 27 – 35.

[20] **E. G. Goodaire and C. P. Milies**: *Moufang unit loops torsion over their centres*, Quaestiones Math. **25** (2002), 1 – 12.

[21] **E. G. Goodaire and C. P. Milies**: *Symmetric units in alternative loop rings*, Algebra Colloq. **13** (2006), 361 – 370.

[22] **E. G. Goodaire and C. P. Milies**: *Involutions of RA loops*, to appear, Canad. Math. Bull., post 2006.

[23] **E. G. Goodaire and D. A. Robinson**: *A class of loops which are isomorphic to all loop isotopes*, Canad. J. Math. **34** (1982), 662 – 672.

[24] **E. G. Goodaire and D. A. Robinson**: *A class of loops with right alternative loop rings*, Comm. Algebra **22** (1995), 5623 – 5634.

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

[26] **L. A. Kokoris**: *Power-associative rings of characteristic two*, Proc. Amer. Math. Soc. **6** (1955), 705 – 710.

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

[28] **C. P. Milies and S. K. Sehgal**: *An introduction to group rings*, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.

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

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

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

[32] **D. A. Robinson**: *A Bol loop isomorphic to all loop isotopes*, Proc. Amer. Math. Soc. **19** (1968), 671 – 672.

[33] **R. Sandling**: *Units in the modular group algebra of a finite abelian p-group*, J. Pure Appl. Algebra **33** (1984), 337 – 346.

[34] **R. Sandling**: *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52** (1989), 22 – 27.

[35] **P. Vojtěchovský**: *On the uniqueness of loops* $M(G,2)$, Comment. Math. Univ. Carolin. **44** (2003), 629 – 635.

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

Received May 8, 2007

Department of Mathematics and Statistics
Memorial University
St. John's, Newfoundland
Canada A1C 5S7
E-mail: edgar@math.mun.ca