The Isomorphism Problem for Loop Rings

Luiz G. X. de Barros

Abstract: We present some positive answers to the question: 'For which rings $R$ and loops $L$ and $M$ the ring isomorphism $RL \cong RM$ implies the loop isomorphism $L \cong M$?'

Key words: loop, loop ring, nonassociative algebra.

1 Loops

In this section we introduce some fundamental concepts about loops. The basic references are the books by R.H. Bruck [6] and H.O. Pflugfelder [18].

A loop is a set $L$ together with a binary operation $\cdot$ such that
i) There exists an element $1 \in L$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in L$.
ii) For all element $a \in L$, the maps $R_a$ and $L_a$ defined by $R_a(x) = x \cdot a$ and $L_a(x) = a \cdot x$ for all $x \in L$ are bijections.

As a consequence, it follows that in a loop $L$
(a) The equations $a \cdot X = b$ and $X \cdot a = b$ have unique solutions.
(b) Every element $a \in L$ has a unique left inverse $a^\lambda$ and a unique right inverse $a^\rho$ defined as the solutions of the equations $X \cdot a = 1$ and $a \cdot X = 1$ respectively.

Loops of order 2, 3 or 4 are groups, and, up to isomorphism, there are 6 loops of order 5; 109 loops of order 6 and 23,750 loops of order 7.

A diassociative loop is a loop in which, for all elements $x$ and $y$, the subloop $\langle x, y \rangle$ generated by $x$ and $y$ is a group. In a diassociative loop it holds that $a^\lambda = a^\rho = a^{-1}$ for all $a$.

The commutator of two elements $x$ and $y$ of a loop $L$ is the element in $L$, denoted by $(x, y)$, such that $xy = (yx) \cdot (x, y)$; and, the commutator subloop $L'$ is the subloop generated by all commutators of $L$.

The associator of three elements $x$, $y$ and $z$ of a loop $L$ is the element in $L$, denoted by $(x, y, z)$, such that $(xy)z = x(yz) \cdot (x, y, z)$; and, the associator subloop $A(L)$ is the subloop generated by all associators of $L$.

The nucleus $N(L)$ of a loop $L$ is the subset $\{x \in L \mid (x, a, b) = (a, x, b) = (a, b, x) = 1, \forall a, b \in L\}$. If we denote by $C(L)$ the subset $\{x \in L \mid (x, y) = 1, \forall a, b \in L\}$.

---

1Research partially supported by CNPq (Proc. 300411/94).
1, ∀y ∈ L}, then the centre of L is the set \( Z(L) = C(L) \cap N(L) \).

A Moufang loop is a loop in which, for all \( x, y \) and \( z \), the following Moufang identities hold:

\[
\begin{align*}
(xy)(zx) &= (x(yz))x \\
((zx)y)x &= z(x(yx)) \\
((xy)x)z &= x(y(xz))
\end{align*}
\]

In 1974 Orin Chein [7] gave a method to construct nonassociative Moufang loops from nonabelian groups:

**Theorem 1.1** Let \( G \) be a nonabelian group with an involution \( g \mapsto g^* \) such that \( gg^* \) is in the center of \( G \) for all \( g \in G \) and let \( g_0 \in G \) be a central element such that \( g_0 = g_0^* \). Let \( u \) be an indeterminate, set \( L = G \cup Gu \) and define

\[
\begin{align*}
g(hu) &= (hg)u \\
(gh)u &= (gh^*)u \\
(gu)(hu) &= g_0h^*g
\end{align*}
\]

for all \( g, h \in G \). Then \( L \) is a Moufang loop which is not a group.

We write \( L = L(G, \ast, g_0) \) to indicate that \( L \) is constructed in this way from \( G \). It's easy to see that \( L \) is not associative. To see this it is enough to take two elements \( g \) and \( h \) in \( G \) such that \( g \cdot h \neq h \cdot g \). Then:

\[
(u \cdot h^*) \cdot g^* = (h \cdot u) \cdot g = hg \cdot u \quad \text{and} \quad u \cdot (h^* \cdot g^*) = u \cdot (gh)^* = gh \cdot u .
\]

The smallest nonassociative Moufang loop is \( L(S_3, (\cdot)^{-1}, 1) \) of order 12, where \( S_3 \) denotes the symmetric group of order 6.

Given an associative and commutative ring \( R \) with unity and a loop \( L \), we can mimic the construction of a group ring to form the loop ring \( RL \).

A ring \( A \) is said to be alternative if for all \( x \) and \( y \) in \( A \) the following equalities hold:

\[ x \cdot xy = x^2 \cdot y \quad \text{and} \quad xy \cdot y = x \cdot y^2 .\]

The study of alternative loop rings begun in 1983 with Edgar G. Goodaire who published the article [14] about those loop rings. In 1986 himself and Orin Chein [9] defined R.A. loops as the loops whose loop algebra over some ring with characteristic different from 2 is alternative but not associative and gave a complete description of those loops. There they proved the following

**Theorem 1.2** Let \( L \) be an R.A. loop. Then, there exists a nonabelian group \( G \subseteq L \) and an element \( u \in L \) such that \( L = G \cup G \cdot u, G' = L' = \{1, s\} \subseteq Z(G) = Z(L) \).
and \( L = L(G, *, g_o) \) with the involution \( * : G \to G \) given by

\[
g^* = \begin{cases} 
g & \text{if } g \in Z(G) \\
g^{-1} & \text{if } g \notin Z(G) \
\end{cases}
\]

and \( u^2 = g_o \) is an element in \( Z(L) \).

Denoting by \( Q \) the quaternion group of order 8, the smallest R.A. loops are two loops of order 16, denoted, as in [7], by \( M_{16}(Q) = L(Q, *, s) \), the so called Cayley loop, and \( M_{16}(Q, 2) = L(Q, *, 1) \), where \( * \) is as in the above theorem and \( s \) is the nonidentity commutator in \( Q \).

Given an R.A. loop \( L \), since the Moufang identities hold in the alternative ring \( RL \), in particular, the elements of \( L \) also verify those identities and, thus, \( L \) must be a Moufang loop.

## 2 The Isomorphism Problem

The isomorphism problem for group rings asks for which rings \( R \) and groups \( G \) and \( H \) the isomorphism of group algebras \( RG \cong RH \) implies that the groups \( G \) and \( H \) are isomorphic. Or, more compactly, under what conditions is a group “determined” by its group ring?

Of course, this problem admits a version for loop rings. We will describe some results about the isomorphism problem for some types of loops over \( \mathbb{Z} \), the ring of integers, and \( \mathbb{Q} \), the rational field.

In 1988, Edgar G. Goodaire and César Polcino Milles [15] proved the following result:

**Theorem 2.1** Let \( L \) and \( M \) be R.A. loops such that \( ZL \cong ZM \). Then \( L \cong M \).

A subloop \( N \) of a loop \( L \) is said to be normal if for all \( x \) and \( y \) in \( L \) we have that \( x \cdot (yN) = (xy) \cdot N \), \( (Nx) \cdot y = N \cdot (xy) \) and \( xN = Nx \). If \( N \) is a normal subloop of a loop \( L \) we can define the quotient loop \( L/N \). The natural epimorphism \( L \to L/N \) extends to an algebra epimorphism \( RL \to R[L/N] \), and we will denote by \( \Delta(L : N) \) the kernel of this epimorphism.


**Theorem 2.2** Let \( L \) and \( M \) be R.A. loops. Then \( QL \cong QM \) if and only if \( L/L' \cong M/M' \) and \( \Delta(L : L') \cong \Delta(M : M') \).
In the same article they proved the following

**Theorem 2.3** Let \( L \) be an R.A. loop with \( L' = \{1, s\} \). Assume there exists an element \( \alpha \in Z(L) \) such that \( \alpha^2 = s \). Let \( M \) be another loop. Then \( QL \cong QM \) if and only if \( L/L' \cong M/M' \) and \( Z(QL) \cong Z(QM) \).

In 1993, Luiz G.X. de Barros [1] completed that result proving

**Theorem 2.4** Let \( L \) be an R.A. loop with \( L' = \{1, s\} \) and assume that there exists no element \( \alpha \in Z(L) \) such that \( \alpha^2 = s \). Let \( M \) be another loop. Then, \( QL \cong QM \) if and only if \( L \cong M \).

In 1990, Orin Chein and Edgar G. Goodaire [10] defined \((RA2)\) loops as being those loops whose loop algebra over a ring with characteristic 2 is alternative but not associative and proved that R.A. loops are also \((RA2)\) loops. Then, the modular case, that is, the case where the characteristic of the ring divides the order of the loop, could be studied.

**Theorem 2.5** (L.G.X. de Barros and C. Polcino Milles [4]) Let \( Z_2 \) denote the field with two elements. Let \( L \) and \( M \) be R.A. 2-loops such that \( Z_2L \cong Z_2M \). Then \( L \cong M \).

Code loops were introduced by R.L. Griess Jr. in [16] and classified by O. Chein and E.G. Goodaire in [11] and [12] who showed that nonassociative code loops are \((RA2)\) loops (and thus, Moufang loops) with a unique nonidentity commutator, a unique nonidentity associator and a unique nonidentity square, which coincide. This element is central of order 2.

**Theorem 2.6** (L.G.X. de Barros and C. Polcino Milles [5]) Let \( Z_2 \) denote the field with two elements. Let \( L \) and \( M \) be nonassociative code loops such that \( Z_2L \cong Z_2M \). Then \( L \cong M \).

A similar result holds over the ring of integers.

**Theorem 2.7** (L.G.X. de Barros and O.S. Juriaans [3]) Let \( L \) and \( M \) be nonassociative code loops such that \( ZL \cong ZM \). Then \( L \cong M \).

We recall that an algebra \( A \) is **flexible** if for all \( x, y \in A \) it holds that \( x \cdot (y \cdot x) = (x \cdot y) \cdot x \). In [2], Luiz G.X. de Barros and Orlando S. Juriaans defined \( R.F. \) loops as those loops whose loop algebra over a ring with characteristic different from 2 is flexible but not alternative. Using Chein's method (Theorem 1.1), a loop \( M = M(L, *, g_o) \) can be constructed from an R.A. loop \( L \), with \( * \) and \( g_o \) as in Theorem 1.2. This loop \( M \) is a non-Moufang diassociative R.F. loop.

**Theorem 2.8** (L.G.X. de Barros and O.S. Juriaans [2]) Let \( M \) and \( N \) be R.F. loops constructed from R.A. loops. Then \( ZM \cong ZN \) if and only if \( M \cong N \).

**Theorem 2.9** (L.G.X. de Barros and O.S. Juriaans [2]) Let \( M \) and \( N \) be R.F. loops constructed from R.A. loops. Then \( QM \cong QN \) if and only if \( M/M' \cong N/N' \) and \( \Delta(M : M') \equiv \Delta(N : N') \).
The Isomorphism Problem for Loop Rings

References


Luiz G. X. de Barros
Universidade de São Paulo
Instituto de Matemática e Estatística
Caixa Postal 66281 - São Paulo - SP
CEP 05389-970
lgxb@ime.usp.br
Brasil