Quasigroups and Related Systems **14** (2006), 1 – 9

Loop algebras of loops whose derived subloop is central

Luiz G. X. de Barros

Abstract

The *isomorphism problem* for loops, that is, to know under which conditions the loop algebra isomorphism implies the loop isomorphism, is studied in the semisimple case for loops whose derived subloop is central. This is done by studying the structure of the semisimple loop algebra and by proving that it can be decomposed as a direct sum of an associative and commutative subalgebra with a nonassociative and non-commutative subalgebra.

1. Nomenclature and Introduction

A *loop* is a set L with a binary operation $\cdot$ which admits an identity element 1 and that the equations $X \cdot a = b$ and $a \cdot X = b$ have unique solutions for all a and b in L.

The unique solution of the equation $a \cdot b = (b \cdot a) \cdot X$ in L is called the *commutator* of the elements a and b, while the unique solution of the equation $(a \cdot b) \cdot c = (a \cdot (b \cdot c)) \cdot X$ is called the *associator* of the elements a,b and c. For a loop L, the subloop L' generated by all commutators and all associators is called the *derived subloop* of L. The quotient loop L/L' is an abelian group and L' is the smallest subloop of L with such property.

The *centre* of a loop L is the set $\mathcal{Z}(L)$ of the elements in L which commute with any element in L and which associate with any two others elements in L in any order of association.

2000 Mathematics Subject Classification: Primary 17A99; Secondary 20N05
Keywords: loop, loop algebra

In a loop, the solution of the equation $X \cdot a = 1$ is called the *left inverse* of the element a and it is denoted by a^λ, while the solution of the equation $a \cdot X = 1$ is called the *right inverse* of a and it is denoted by a^ρ.

Given an associative and commutative ring R and a loop L, the *loop ring* RL is the free R-module with basis L and multiplication defined distributively from the multiplication of L. For a field K, the *loop algebra* KL is defined in the same way.

For a normal subloop N of a loop L , the epimorphism $L \longrightarrow L/N$ extends to the algebra epimorphism $KL \longrightarrow K[L/N]$ whose kernel, denoted by $\Delta(L,N)$, is the ideal of KL generated by the set $\{n-1 \mid n \in N\}$.

We shall denote by $[KL, KL]$ the left ideal of KL generated by all elements of the form $\alpha\beta - \beta\alpha$ with $\alpha, \beta \in KL$, and by $[KL, KL, KL]$ the left ideal of KL generated by all elements of the form $\alpha\beta \cdot \gamma - \alpha \cdot \beta\gamma$ with $\alpha, \beta, \gamma \in KL$.

The *isomorphism problem* for group rings, posed by Graham Higman in his 1940 thesis, asks if a group is *determined* by its group ring, that is, given a ring R and groups G and H, does the ring isomorphism $RG \cong RH$ imply the group isomorphism $G \cong H$?

G. Higman himself proved that the integral group ring of a finite abelian group determines the group. Later, A. Whitcomb extended this result to integral group ring of finite metabelian groups.

The isomorphism problem over fields was first considered in 1950 by S. Perlis and G.L. Walker who proved that if G is a finite abelian group then G is determined its rational group algebra $\mathbf{Q}G$. Solutions for many classes of group, many kinds of rings and fields are found during this time.

On the '80s, the problem was reposed for loops and expressive results for RA-loops were obtained. For details, Chapter XI of the book *"Alternative Loop Rings"*, Elsevier, (1996), by E.G. Goodaire, E. Jespers and C. Polcino Milies, is recommended.

During the '90s, the author has worked in extending these results to other classes of loops. In this work, some advances on the loops whose derived subloop is central are shown. The semisimple case, that is, when the characteristic of the field does not divide the order of the loop, is completely solved. This is made studying the structure of the loop algebra and proving that it can be decomposed as a direct sum of an associative and commutative subalgebra with a non-associative and non-commutative subalgebra.

2. Loop algebras of loops whose derived subloop is central

Here we focus our attention on the class $\mathcal{L}$ of the finite loops whose derived subloop is central. These loops appear very often in the theory of loops. Code loops [6], RA-loops [5], loops with a unique non-trivial commutator-associator element [8] are examples of such loops.

Some of the results in this section are extensions of those obtained for RA-loops in [1] by the author and in [3] by C. Polcino Milies and the author.

This first lemma is fundamental for the sequence and extends to loop algebras of loops in $\mathcal{L}$ a very known result of group algebras.

Lemma 2.1. *Let K be a field and L be a loop in $\mathcal{L}$ with derived subloop L'. Then*

$$[KL, KL] + [KL, KL, KL] = \Delta(L, L').$$

Proof. First, we observe that $[KL, KL]$ is generated by elements of the form $lm - ml$ with $l, m \in L$. Since $lm = ml \cdot (l, m)$ we have that

$$lm - ml = ml \cdot (l, m) - ml = ml \cdot ((l, m) - 1) \in \Delta(L, L') \ .$$

Also, $[KL, KL, KL]$ is generated by elements of the form $lm.n - l.mn$ with $l, m, n \in L$. Since, $lm.n = (l.mn) \cdot (l, m, n)$ we have that

$$lm.n - l.mn = (l.mn) \cdot (l, m, n) - l.mn = (l.mn) \cdot ((l, m, n) - 1) \in \Delta(L, L') \ .$$

Thus $[KL, KL] + [KL, KL, KL] \subset \Delta(L, L')$.

On the other hand, since $lm = ml \cdot (l, m)$ and (l, m) is central, we have that $(l, m) = (ml)^\lambda \cdot lm$ and $(l, m)^{-1} = (lm)^\lambda \cdot ml$.

Then

$$\begin{aligned} 1 - (l, m) = 1 - (ml)^\lambda \cdot lm &= (ml)^\lambda \cdot ml - (ml)^\lambda \cdot lm \\ &= (ml)^\lambda \cdot (ml - lm) \in [KL, KL] \end{aligned}$$

and

$$\begin{aligned} 1 - (l, m)^{-1} = 1 - (lm)^\lambda \cdot ml &= (lm)^\lambda \cdot lm - (lm)^\lambda \cdot ml \\ &= (lm)^\lambda \cdot (lm - ml) \in [KL, KL]. \end{aligned}$$

Also, since $lm.n = (l.mn) \cdot (l, m, n)$ and (l, m, n) is central, we have that $(l, m, n) = (l.mn)^\lambda \cdot (lm.n)$ and $(l, m, n)^{-1} = (lm.n)^\lambda \cdot (l.mn)$.

Then

$$\begin{aligned}1-(l,m,n) &= 1-(l.mn)^{\lambda}\cdot(lm.n) = (l.mn)^{\lambda}\cdot(l.mn)-(l.mn)^{\lambda}\cdot(lm.n)\\ &= (l.mn)^{\lambda}\cdot(l.mn-lm.n)\in[KL,KL,KL]\end{aligned}$$

and

$$\begin{aligned}1-(l,m,n)^{-1}1-(lm.n)^{\lambda}\cdot(l.mn) &= (lm.n)^{\lambda}\cdot(lm.n)-lm.n)^{\lambda}\cdot(l.mn)\\ &= (lm.n)^{\lambda}\cdot(lm.n-l.mn)\in[KL,KL,KL].\end{aligned}$$

An element $x\in L'$ is a product of commutators, associators and their inverses. The identity $1-cd=(1-c)+(1-d)-(1-c)\cdot(1-d)$ shows that $1-x$ can be separated in terms of the form $\alpha\cdot(1-c)$ where $\alpha\in KL$ and c is a commutator (or its inverse) or an associator (or its inverse). Each one of these terms of the form $\alpha\cdot(1-c)$ belongs to $[KL,KL]$ or $[KL,KL,KL]$. Thus $\Delta(L,L')\subset[KL,KL]+[KL,KL,KL]$. □

For a future use we recall a classical result about group algebras of finite abelian groups due to S. Perlis and G.L. Walker [10],

Theorem 2.2. (Theorem X.2.1, [7]) *Let G be a finite abelian group of order n and K be field whose characteristic does not divide n. Then*

$$KG\cong\oplus_{d|n}a_dK(\xi_d)\ ,$$

where $a_d=n_d/[K(\xi_d):K]$, n_d denotes the number of elements of order d in G and ξ_d denotes a primitive dth root of unity over K.

Using Lemma VI.1.2 of [7], we can prove

Lemma 2.3. *Let L be a loop in $\mathcal{L}$ and let K be any field whose characteristic does not divide $|L'|$, the order of L'. Define $\hat{L}'=\frac{1}{|L'|}\cdot\sum_{n\in L'}n$. Then*

i) $\hat{L}'$ *is a central idempotent in* KL*,*

ii) $KL\cdot\hat{L}'\cong K[L/L']$ *and* $KL\cdot(1-\hat{L}')\cong\Delta(L,L')$*,*

iii) $KL\cong KL\cdot\hat{L}'\oplus KL\cdot(1-\hat{L}')\cong K[L/L']\oplus\Delta(L,L')$.

The next result is valid for any field.

Proposition 2.4. *Let L_1 and L_2 be loops in $\mathcal{L}$ and K be any field. Suppose that $KL_1\cong KL_2$. Then $K[L_1/L_1']\cong K[L_2/L_2']$ and $\Delta(L_1,L_1')\cong\Delta(L_2,L_2')$.*

Proof. Let $KL_1 \longrightarrow K[L_1/L_1']$ be the natural epimorphism whose kernel is $\Delta(L_1, L_1')$.

Given an isomorphism $\Psi : KL_1 \longrightarrow KL_2$, we have

$$\Psi(\Delta(L_1, L_1')) = \Psi([KL_1, KL_1] + [KL, KL, KL]) =$$
$$= [KL_2, KL_2] + [KL_2, KL_2, KL_2] = \Delta(L_2, L_2').$$

This shows that Ψ also induces an isomorphism $\overline{\Psi}$ of the corresponding factor rings, so

$$K[L_1/L_1'] \cong KL_1/\Delta(L_1, L_1') \cong KL_2/\Delta(L_2, L_2') \cong K[L_2/L_2']. \qquad \square$$

As a consequence of both results, we obtain the next theorem which is an extension of Theorem 3.2 in [2] for RA-loops

Theorem 2.5. *Let L_1 and L_2 be loops in $\mathcal{L}$ and K be any field whose characteristic does not divide $|L_1'|$ and $|L_2'|$. Then $KL_1 \cong KL_2$ if and only if $K[L_1/L_1'] \cong K[L_2/L_2']$ and $\Delta(L_1, L_1') \cong \Delta(L_2, L_2')$.*

Using Theorem 2.2 we have

Corollary 2.6. *Let L_1 and L_2 be loops in $\mathcal{L}$ and let $\mathbf{Q}$ be the rational field. Then $\mathbf{Q}L_1 \cong \mathbf{Q}L_2$ if and only if $L_1/L_1' \cong L_2/L_2'$ and $\Delta(L_1, L_1') \cong \Delta(L_2, L_2')$.*

3. A subclass of $\mathcal{L}$

In this section we study the class $\mathcal{L}_1$ of the finite loops L such that $L/\mathcal{Z}(L) \cong C_2 \times C_2$. These loops appear as groups in the main papers about RA-loops as [5] and [9].

Proposition 3.1. *Let $L \in \mathcal{L}_1$. Then*
i) $L' \subset \mathcal{Z}(L)$, *that is,* $\mathcal{L}_1 \subset \mathcal{L}$,
ii) $L^2 \subset \mathcal{Z}(L)$,
iii) $L = < x, y, \mathcal{Z}(L) >$, *the subloop generated by x, y and $\mathcal{Z}(L)$, for all non-central elements $x, y \in L$ such that $x.\mathcal{Z}(L) \neq y.\mathcal{Z}(L)$.*

Proof.
i) It comes from the fact that $L/\mathcal{Z}(L)$ is an abelian group.
ii) It comes from the fact that the group $C_2 \times C_2$ has exponent 2.
iii) It comes from the fact that $L/\mathcal{Z}(L) \cong C_2 \times C_2$ can be generated by two non-central elements x and y such that $x.\mathcal{Z}(L) \neq y.\mathcal{Z}(L)$. $\square$

Proposition 3.2. *Let $L =< x, y, \mathcal{Z}(L) >$ a loop in $\mathcal{L}_1$. Write $\mathcal{Z}(L) \cong E \times A$, where E is an abelian 2-group and A is an abelian group of odd order. Then there exist $x_0, y_0 \in L$, with $x_0^2, y_0^2 \in E$ such that $L =< x_0, y_0, \mathcal{Z}(L) >$.*

Proof. Write $x^2 = x_1.x_2$ and $y^2 = y_1.y_2$ with $x_1, y_1 \in E$ and $x_2, y_2 \in A$. Let $x_0 = x^{o(x_2)}$ and $y_0 = y^{o(y_2)}$. It is easy to see that x_0 and y_0 have the desired properties. □

Theorem 3.3. *Let L be a loop in $\mathcal{L}_1$. Then $L = M \times A$, where M is a 2-loop in $\mathcal{L}_1$ and A is an abelian group of odd order.*

Proof. Write $\mathcal{Z}(L) \cong E \times A$, where E is an abelian 2-group and A is an abelian group of odd order. By Proposition 3.2 there exist $x_0, y_0 \in L$, with $x_0^2, y_0^2 \in E$ such that $L =< x_0, y_0, \mathcal{Z}(L) >$. Define $M =< x_0, y_0, E >$. Then $\mathcal{Z}(M) = E$ and $M/\mathcal{Z}(M) \cong C_2 \times C_2$. Also $L = M \times A$. □

Corollary 3.4. *Let L be a loop in $\mathcal{L}_1$. Write $L = M \times A$, where M is a 2-loop in $\mathcal{L}_1$ and A is an abelian group of odd order. Then $L' = M'$.*

Proof. Given the elements $l = x_0^a.y_0^b.z_l$, $m = x_0^c.y_0^d.z_m$ and $n = x_0^e.y_0^f.z_n$ in L with $x_o, y_0 \in M$ and $z_l, z_m, z_n \in \mathcal{Z}(L)$, observe that

$$(l, m) = (x_0^a.y_0^b.z_l \ , \ x_0^c.y_0^d.z_m) = (x_0^a.y_0^b \ , \ x_0^c.y_0^d) \in M'$$

and

$$(l, m, n) = (x_0^a.y_0^b.z_l \ , \ x_0^c.y_0^d.z_m \ , \ x_0^c.y_0^d.z_n) = (x_0^a.y_0^b \ , \ x_0^c.y_0^d \ , \ x_0^c.y_0^d) \in M'$$

since z_l , z_m and z_n are central. □

We say that elements a and b of a loop L are *conjugate* if $b = \theta(a)$ for some $\theta \in Inn(L)$, the *inner mapping group* of L. Conjugacy defines an equivalence relation on L. In a loop ring, a (finite) *class sum* is the sum of all the elements in a finite conjugacy class of L.

The next theorem is a classical result due to R. H. Bruck and it appears in [7] as Theorem III.1.3

Theorem 3.5. *Let L be a loop and R be a commutative and associative ring. The (finite) class sums of the loop ring RL form a R-basis for the centre of RL .*

Now we focus our attention to the class $\mathcal{L}_2$ of the loops L in $\mathcal{L}_1$ with a unique nonidentity commutator-associator element.

As the Corollary III.1.5 in [7], we can prove

Corollary 3.6. *Let L be a loop in $\mathcal{L}_2$ with a unique nonidentity commutator-associator element s and let R be a commutative and associative ring. Then the centre of the loop ring RL is spanned by the centre of L and those elements of RL of the form $l + sl$, $l \in L$.*

Also, as the Corollary VI.1.3 in [7], we can prove

Lemma 3.7. *Let L be a loop in $\mathcal{L}_2$ with a unique nonidentity commutator-associator element s and let K be a field whose characteristic does not divide the order of L. Then $\mathcal{Z}(\Delta(L, L')) \cong K[\mathcal{Z}(L)](1 - \hat{L}')$, where $\hat{L}' = \frac{1+s}{2}$.*

The next theorem extends Theorem 2.5 of [4] from RA-loops to the class $\mathcal{L}_2$.

Theorem 3.8. *Let L_1 and L_2 be loops in $\mathcal{L}_2$ and K be a field whose characteristic does not divide the order of either of these loops. For $1 = 1, 2$, write $L_i = M_i \times A_i$ where M_i is 2-loop in $\mathcal{L}_2$ and A_i is an abelian group of odd order. Then $KL_1 \cong KL_2$ if and only if $KM_1 \cong KM_2$ and $KA_1 \cong KA_2$.*

Proof. Suppose first that $KL_1 \cong KL_2$. By Proposition 2.4, we have $K[L_1/L_1'] \cong K[L_2/L_2']$; that is,

$$K[(M_1/M_1') \times A_1] \cong K[(M_2/M_2') \times A_2].$$

As these group algebras are commutative, using a result due to D. E. Cohen and which appears as Theorem X.2.5 in [7], we can conclude that

$$K[M_1/M_1'] \cong K[M_2/M_2'] \quad \textit{and} \quad KA_1 \cong KA_2.$$

In view of Theorem 2.5, in order to prove that $KM_1 \cong KM_2$ as well, it will suffice to show that $\Delta(M_1, M_1') \cong \Delta(M_2, M_2')$. By Theorem 2.5, $\Delta(L_1, L_1') \cong \Delta(L_2, L_2')$. Moreover, for $i = 1, 2$, denoting by $\hat{L}_i' = \frac{1}{|L_i'|} \cdot \sum_{n \in L_i'} n$ the central idempotent in KL_i,

$$\Delta(L_i, L_i') = KL_i(1 - \hat{L}_i') \cong (KM_i \otimes KA_i)(1 - \hat{L}_i') \cong \Delta(M_i, M_i') \otimes KA_i$$

since $\hat{L}_i' \in M_i$. Thus

$$\Delta(M_1, M_1') \otimes KA_1 \cong \Delta(L_1, L_1') \cong \Delta(L_2, L_2') \cong \Delta(M_2, M_2') \otimes KA_2.$$

Using Theorem 2.2, we have that $KA_1 \cong nK \oplus (\oplus_d m_d K(\xi_d)) \cong KA_2$, where ξ_d is a primitive root of unity of odd order d and d runs over the set of divisors of $|A_1|$ such that $K(\xi_d) \neq K$. For $i = 1, 2$,

$$\Delta(L_i, L_i') \cong n\Delta(M_i, M_i') \oplus (\oplus_d m_d(\Delta(M_i, M_i') \otimes K(\xi_d))).$$

By Lemma 3.7 , $\mathcal{Z}(\Delta(M_i, M_i')) = K[\mathcal{Z}(M_i)](1 - \hat{L}_i')$. Thus, using again Theorem 2.2, $\mathcal{Z}(\Delta(M_i, M_i')) \cong \oplus_j K(\xi_{a_j})$, where the ξ_{a_j} are primitive roots of unity of order 2^{a_j}. Consequently,

$$\mathcal{Z}(\Delta(M_i, M_i') \otimes K(\xi_d)) \cong \oplus_j K(\xi_{a_j}) \otimes K(\xi_d).$$

Since $(d, 2^{a_j}) = 1$, we have that

$$K(\xi_{a_j}) \otimes K(\xi_d) \cong K(\xi_{a_j})(\xi_d) = K(\xi_{a_j d}) ,$$

where $\xi_{a_j d}$ is a primitive root of unity of order $2^{a_j} d$. We claim that this field is never isomorphic to a field of the form $K(\xi_{a_i})$. In fact, assume that $K(\xi_{a_j d}) \cong K(\xi_{a_i})$. Then $K(\xi_d) \subset K(\xi_{a_i})$ and so

$$K(\xi_{a_i}) \otimes_K K(\xi_d) \cong K(\xi_{a_i d}) = K(\xi_{a_i})(\xi_d) = K(\xi_{a_i}).$$

However, as $K(\xi_d) \neq K$, the tensor product $K(\xi_{a_i}) \otimes_K K(\xi_d)$ has dimension at least two over the field $K(\xi_{a_i})$, a contradiction. Hence the centre of the algebra $\Delta(M_i, M_i')$ is a direct sum of fields which are all different from those appearing in the decomposition of the centre of $\Delta(M_i, M_i') \otimes K(\xi_d)$. Since

$$n\Delta(M_1, M_1') \oplus (\oplus_d m_d(\Delta(M_1, M_1') \otimes K(\xi_d))) \cong$$

$$\cong n\Delta(M_2, M_2') \oplus (\oplus_d m_d(\Delta(M_2, M_2') \otimes K(\xi_d)))$$

and because $\Delta(M_i, M_i')$ is a sum of algebras over fields of the form $K(\xi_{a_j})$ while $\mathcal{Z}(\Delta(M_i, M_i') \otimes K(\xi_d))$ contains no such direct summands, it follows that $n\Delta(M_1, M_1') \cong n\Delta(M_2, M_2')$. Hence $\Delta(M_1, M_1') \cong \Delta(M_2, M_2')$, as desired.

The converse is straightforward. □

Corollary 3.9. *Let L_1 and L_2 be loops in $\mathcal{L}_2$ and K be a field whose characteristic does not divide the order of either of these loops. For $1 = 1, 2$, write $L_i = M_i \times A_i$ where M_i is 2-loop in $\mathcal{L}_2$ and A_i is an abelian group of odd order. Then $KL_1 \cong KL_2$ if and only if $K[M_1/M_1'] \cong K[M_2/M_2']$, $\Delta(M_1, M_1') \cong \Delta(M_2, M_2')$ and $KA_1 \cong KA_2$.*

Corollary 3.10. *Let L_1 and L_2 be loops in $\mathcal{L}_2$ and $\mathbf{Q}$ be the field of rationals. For $1 = 1, 2$, write $L_i = M_i \times A_i$ where M_i is 2-loop in $\mathcal{L}_2$ and A_i is an abelian group of odd order. Then $\mathbf{Q}L_1 \cong \mathbf{Q}L_2$ if and only if $M_1/M_1' \cong M_2/M_2'$, $\Delta(M_1, M_1') \cong \Delta(M_2, M_2')$ and $A_1 \cong A_2$.*

References

[1] **L. G. X. de Barros**: *Isomorphisms of rational loop algebras*, Comm. Algebra **21** (1993), 3977 – 3993.

[2] **L. G. X. de Barros**: *On semisimple alternative loop algebras*, Comm. Algebra **21** (1993), 3995 – 4011.

[3] **L. G. X. de Barros, C. Polcino Milies**: *Loop algebras of code loops*, Comm. Algebra **23** (1995), 4781 – 4790.

[4] **L. G. X. de Barros, C. Polcino Milies**: *Modular loop algebras of RA loops*, J. Algebra **23** (1995), 1027 – 1040.

[5] **O. Chein, E. G. Goodaire**: *Loops whose loop rings are alternative*, Comm. Algebra **175** (1986), 293 – 310.

[6] **O. Chein, E. G. Goodaire**: *Moufang loops with a unique non-identity commutator (associator, square)*, J. Algebra **130** (1990), 369 – 384.

[7] **E. G. Goodaire, E. Jespers, C. Polcino Milies**, Alternative Loop Rings, North Holland Math. Series no. **184**, Elsevier, Amsterdam, 1996.

[8] **E. G. Goodaire, D. A. Robinson**: *A class of loops with right alternative loop rings*, Comm. Algebra **22** (1994), 5623 – 5634.

[9] **G. Leal, C. Polcino Milies**: *Isomorphic group (and loop) algebras*, J. Algebra **155** (1993), 195 – 210.

[10] **S. Perlis, G. L. Walker**: *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420 – 426.

Centro Universitário Senac
São Paulo, SP, CEP 04696-000
Brazil
e-mail: lbarros@sp.senac.br

Received June 27, 2005