LOOP RINGS OF I.P. LOOPS

Luiz G. X. de Barros*
Instituto de Matemática e Estatística
Universidade de São Paulo
Caixa Postal 20.570 (Ag. Iguatemi) - 01452-090
São Paulo - SP - Brasil

Received January 5, 1994

ABSTRACT

Given an associative and commutative ring R with unity and two loops L and M with inverse property, we investigate conditions under which the loop ring RL is isomorphic to RM. In particular, we prove that GF(2), the field with two elements, determines the five Moufang loops of order 24. Also we give a description of the decomposition as a direct sum of simple algebras of the loop algebra of the smallest Moufang loop over a field with characteristic different from 2 and 3.

^{*}This work was supported by FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo - Brasil (Proc. 92/1907-1)

e-mail: lgxb@ime.usp.br

AMS Mathematics Subject Classification 17D05 20N05 68R99 68U30

1 Introduction

A loop is a set L together with a binary operation $(g,h) \longrightarrow g.h$ for which there is a two-sided identity and with the property that the left and right multiplication maps determined by any element of L are one-one and onto.

Over an associative and commutative ring R with identity, one can construct the *loop ring* RL in the same way we construct a group ring.

A loop L is said to be a *loop with inverse property*, or a I.P. loop if for all $x, y \in L$ the following identities hold:

$$x^{-1}.(xy) = y$$

 $(xy).y^{-1} = x$.

The isomorphism problem for loop rings is a version for loops of a classical question set by R.M. Thrall in 1947 for group rings, which here we may roughly state as follows: given a ring R and two loops L and M when will the ring isomorphism $RL \cong RM$ imply the loop isomorphism $L \cong M$? In an affirmative answer we are used to saying that the ring R determines the loop L.

Some answers are given in recent years for certain classes of loops (see, [11], [12], [1], [2], [3], [4]). In this paper we prove some results for loop rings of I.P. loops.

2 Background and Notation

The (loop) commutator of two elements x and y of a loop L is the element in L, denoted by (x,y), such that xy = (yx).(x,y). The subloop generated by all commutators of a loop L is called its commutator subloop and we will denote it by L'.

The (loop) 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)).(x, y, z). The subloop generated by all associators of a loop L is called its associator subloop and we will denote it by A(L).

We observe that if L is a I.P. loop then for all x, y and z in L, we have that

$$(x,y) = (yx)^{-1}.(xy)$$

 $(x,y,z) = ((xy)z)^{-1}.(x(yz)).$

A subloop N of a loop L is said to be a normal subloop of L if for all x and y in L we have that x(yN) = (xy)N

$$(Nx)y = N(xy)$$
$$xN = Nx.$$

If N is a normal subloop of a loop L we can define the quocient loop $\frac{L}{N}$. If R is an associative and commutative ring with identity and N is a normal subloop of a loop L, the natural epimorphism $L \to \frac{L}{N}$ extends to a ring epimorphism $RL \to R\left[\frac{L}{N}\right]$ whose kernel, denoted $\Delta_R(L:N)$, is the ideal of RL generated by elements of the form $1-n, n \in N$. In the special case L=N, the homomorphism above described maps $\sum \alpha_g g \in RL$ to $\sum \alpha_g \in R$. This map called the augmentation map, has a kernel written $\Delta_R(L)$ rather than $\Delta_R(L:L)$, which is known as the augmentation ideal of RL.

From these definitions it follows that for a normal subloop N of L,

$$\Delta_R(L:N) = RL.\Delta_R(N) \quad \text{ and } \quad R\left[\frac{L}{N}\right] \cong \frac{RL}{\Delta_R(L:N)} \quad .$$

In [6], R.H. Bruck showed that for any loop L, the subloop B(L) generated by all associators and all commutators of L is a normal subloop. We will call B(L), the associator-commutator subloop of L.

Then for I.P. loops we can state the following proposition which generalizes a result by D. Coleman [9] for group rings.

Proposition 2.1 Let R be an associative and commutative ring with identity. Let L and M be I.P. loops with associator-commutator subloops B(L) and B(M) respectively. Then $RL \cong RM$ implies that $R\left[\frac{L}{B(L)}\right] \cong R\left[\frac{M}{B(M)}\right]$.

Proof: Consider the natural epimorphism $L \to \frac{L}{B(L)}$ and its ring extension $RL \to R\left[\frac{L}{B(L)}\right]$ whose kernel is $\Delta_R(L:B(L)) = RL.\Delta_R(B(L))$.

For all α, β, γ in RL, let [RL, RL] denote the left ideal of RL generated by the elements of the form $\alpha\beta - \beta\alpha$, and [RL, RL, RL] denote the left ideal of RL generated by the elements of the form $\alpha(\beta\gamma) - (\alpha\beta)\gamma$.

We claim that $\Delta_R(L:B(L)) = [RL,RL] + [RL,RL,RL].$

In fact, [RL, RL] is generated over RL by elements of the form xy - yx with x, y in L and, since $xy - yx = xy - xy \cdot (y, x) = xy \cdot (1 - (y, x))$, it follows that $[RL, RL] \subset \Delta_R(L:B(L))$. In the same way, [RL, RL, RL] is generated over RL by elements of the form x(yz) - (xy)z with x, y and z in L and, since

 $x(yz) - (xy)z = x(yz) - (x(yz)).(x,y,z) = (x(yz)).(1 - (x,y,z)), \text{ it follows that } [RL,RL,RL] \subset \Delta_R(L:B(L)).$ Hence $[RL,RL] + [RL,RL,RL] \subset \Delta_R(L:B(L)).$

On the other hand, the equality 1 - gh = (1 - g) + g.(1 - h) for all g, h in L shows that $\Delta_R(L:B(L))$ is generated over RL by elements of the form 1 - (x, y) or 1 - (x, y, z) with x, y and z in L.

Since $1 - (x, y) = 1 - (yx)^{-1}.(xy) = (yx)^{-1}.(yx - xy)$ and, since $1 - (x, y, z) = 1 - ((xy)z)^{-1}.(x(yz)) = ((xy)z)^{-1}.[x(yz) - (xy)z]$, it's easy to see that $\Delta_R(L:B(L)) \subset [RL,RL] + [RL,RL,RL]$.

Now given an isomorphism $\varphi:RL\to RM$, we have that $\varphi(\Delta_R(L:B(L)))=\varphi([RL,RL]+[RL,RL,RL])=$

 $[RM,RM]+[RL,RL,RL]=\Delta_R(M:B(M))$. Consequently, φ induces an isomorphism between the corresponding factor rings and finally we have that

$$R\left[\frac{L}{B(L)}\right] \cong \frac{RL}{\Delta_R(L:B(L))} \cong \frac{RM}{\Delta_R(M:B(M))} \cong R\left[\frac{M}{B(M)}\right] \quad .$$

Observing that $\frac{L}{B(L)}$ is an abelian group we can state the following

Corollary 2.2 Let \mathbf{Q} be the rational field. Let L and M be I.P. loops with associator-commutator subloops B(L) and B(M) respectively. Then $\mathbf{Q}L \cong \mathbf{Q}M$ implies that $\frac{L}{B(L)} \cong \frac{M}{B(M)}$.

Proof: From proposition 2.1 we have $\mathbf{Q}\left[\frac{L}{B(L)}\right] \cong \mathbf{Q}\left[\frac{M}{B(M)}\right]$. The result follows by a classical result by S.Perlis and G.L.Walker [13].

Corollary 2.3 Let F be a prime field with characteristic p. Let L and M be I.P. loops with associator-commutator subloops B(L) and B(M), respectively, such that $\frac{L}{B(L)}$ is a p-group. Then $FL \cong FM$ implies that $\frac{L}{B(L)} \cong \frac{M}{B(M)}$.

Proof: From proposition 2.1 we have $F\left[\frac{L}{B(L)}\right] \cong F\left[\frac{M}{B(M)}\right]$. The result follows by a classical result by W.E.Deskins [10, Theorem 8].

A loop L is said to be a *Moufang loop* if for all x, y, z in L one of the following equivalent *Moufang identities* holds:

$$(xy)(zx) = (x(yz))x$$

$$((zx)y)x = z(x(yx))$$

$$((xy)x)z = x(y(xz))$$

According to [14, Theorem IV.1.4], Moufang loops are P.I. loops, and Lagrange's theorem holds for them [7].

In [8], O. Chein and E.G. Goodaire defined RA2 loops as being loops whose loop ring over any field of characteristic 2 is an alternative nonassociative ring. There they proved that RA2 loops are Moufang loops. They also proved (Corollary 2.12, p.667) that for any RA2 loop L, $A(L) \subset L'$. Then, in this case B(L) = L'.

As a particular case of corollary 2.2, we can state the following

Corollary 2.4 Let \mathbf{Q} be the rational field and L and M be RA2 loops such that $\mathbf{Q}L \cong \mathbf{Q}M$. Then $\frac{L}{L'} \cong \frac{M}{M'}$.

And as a particular case of corollary 2.3, we can state the following

Corollary 2.5 Let F be a prime field with characteristic p. Let L and M be RA2 loops such that $\frac{L}{L'}$ is a p-group. Then $FL \cong FM$ implies $\frac{L}{L'} \cong \frac{M}{M'}$.

In [7], O. Chein classified all nonassociative Moufang loops whose order is smaller than 32. There are 5 nonassociative Moufang loops of order 24, which we have displayed in table 1, using the notation for loops and groups as in [7].

| L | B(L) | $\frac{L}{B(L)}$ | RA2 loop? |
|----------------------------------------|-------|-----------------------------|---------------|
| $L_1 = M_{24}(D_6, 2)$ | C_3 | $C_2 \times C_2 \times C_2$ | $y\epsilon s$ |
| $L_2 = M_{24}(G_{12}, C_2 \times C_4)$ | C_3 | $C_2 \times C_4$ | $y\epsilon s$ |
| $L_3 = M_{24}(A_4, 2)$ | A_4 | C_2 | no |
| $L_4 = M_{24}(G_{12}, 2)$ | C_6 | $C_2 \times C_2$ | no |
| $L_5 = M_{24}(G_{12}, Q)$ | C_6 | $C_2 \times C_2$ | no |

Table 1

In the presence of corollary 2.3, table 1 shows us that to study the isomorphism problem for those 5 loops over the field F = GF(2), the field with 2 elements, we just need to study it for the two last loops of the

table. Using a computer program, we count the non-null elements in the respective loop algebra whose square is null. In FL_4 we have found 67,583 such elements and in FL_5 we have found 22,527 such elements. Then we can establish the following

Corollary 2.6 The field GF(2) determines all nonassociative Moufang loops of order 24.

3 The Semisimple Case

When the characteristic of a field F does not divide the order of a loop L, R.H.Bruck in [5, Th.7A, p.160] shows that the loop algebra FL is semisimple. In this section we will consider this case.

We begin with a result which holds for loop rings in general and it is similar to one by D.Coleman for group rings in [9].

Proposition 3.1 Let N be a finite normal subloop of a loop L and R be an associative and commutative ring with identity such that |N| is invertible in R. Then

$$RL \cong R\left[\frac{L}{N}\right] \bigoplus \Delta_R(L:N)$$

Proof: Since |N| is invertible in R, we can define the loop ring element $\widehat{N} = \frac{1}{|N|} \cdot \sum_{n \in N} n$. It is easy to prove that \widehat{N} is a central idempotent element

in RL, and we have that $RL = RL.\hat{N} \bigoplus RL.(1 - \hat{N})$.

Firstly we observe that $RL.(1-\hat{N}) \subset \Delta_R(L:N)$. Since $\Delta_R(L:N) = RL.\Delta_R(N)$ and $\Delta_R(N)$ is generated by elements of the form $1-n, n \in N$, the equalities $1-n=(1-n).(1-\hat{N})$ for all $n \in N$ imply that the reverse inclusion holds. So we have that $RL.(1-\hat{N}) = \Delta_R(L:N)$.

Now we observe that

$$RL.\hat{N} \cong \frac{RL}{RL.(1-\hat{N})} = \frac{RL}{\Delta_R(L:N)} \cong R\left[\frac{L}{N}\right]$$
.

Proposition 3.2 Let L be an I.P. loop and B(L) be its associator-commutator subloop. Let R be an associative and commutative ring with identity ring such that |B(L)| is invertible in R. Suppose I and J are two-sided ideals of RL with $RL = I \bigoplus J$. Then I is associative and commutative if and only if $J \supset \Delta_R(L:B(L))$.

Proof: If $I \cong \frac{RL}{J}$ is associative and commutative, then we have that i) For all x and y in L, $xy - yx = xy - xy \cdot (y, x) = xy \cdot (1 - (y, x)) \in J$, which implies that $(xy)^{-1} \cdot [xy \cdot (1 - (y, x))] = 1 - (y, x) \in J$.

ii) For all x, y and z in L, $x(yz) - (xy)z = x(yz) - (x(yz)).(x, y, z) = (x(yz)).(1-(x,y,z)) \in J$, which implies that $(x(yz))^{-1}.[(x(yz)).(1-(x,y,z))] = 1-(x,y,z) \in J$.

From i) and ii) we conclude that $\Delta_R(L:B(L)) \subset J$.

On the other hand, if $J \supset \Delta_R(L:B(L))$, from

R
$$\left[\frac{L}{B(L)}\right] \cong \frac{RL}{\Delta_R(L:B(L))} = \frac{I \bigoplus J}{\Delta_R(L:B(L))} \cong I \bigoplus \frac{J}{\Delta_R(L:B(L))}$$
, we can conclude that I is associative and commutative.

As a direct consequence of the proposition 3.2, we have the following results:

Theorem 3.3 Let L and M be I.P. loops with associator-commutator subloops B(L) and B(M) respectively. Let R be an associative and commutative ring with identity such that |B(L)| and |B(M)| are invertible in R. Then $RL \cong RM$ if and only if $R\left[\frac{L}{B(L)}\right] \cong R\left[\frac{M}{B(M)}\right]$ and $\Delta_R(L:B(L)) \cong \Delta_R(M:B(M))$.

Corollary 3.4 Let L and M be RA2 loops with commutator subloops L' and M' respectively. Let F be a field such that $char(F) \nmid |L|$. Then $FL \cong FM$ if and only if $F\left[\frac{L}{L'}\right] \cong F\left[\frac{M}{M'}\right]$ and $\Delta_F(L:L') \cong \Delta_F(M:M')$.

Corollary 3.5 Let L and M be RA2 loops with commutator subloops L' and M' respectively. Let \mathbf{Q} be the rational field. Then $\mathbf{Q}L \cong \mathbf{Q}M$ if and only if $\frac{L}{L'} \cong \frac{M}{M'}$ and $\Delta_{\mathbf{Q}}(L:L') \cong \Delta_{\mathbf{Q}}(M:M')$.

4 The Structure of Semisimple Loop Algebras of RA2 Loops

For RA2 loops, proposition 3.2 becomes

Proposition 4.1 Let L be an RA2 loop and L' be its commutator subloop. Let R be an associative and commutative ring with identity ring such that |L'| is invertible in R. Suppose I and J are two-sided ideals of RL with $RL = I \bigoplus J$. Then I is associative and commutative if and only if $J \supset$ $\Delta_R(L:L')$.

Then we can establish the following

Theorem 4.2 Let L be an RA2 loop with commutator subloop L'. Let F be a field such that the characteristic of F does not divide the order of L. Then the semisimple loop algebra FL decomposes as a direct sum of simplecomponents which are extensions of F by a primitive root of unity or simple algebras that are not commutative nor associative.

Proof: From proposition 3.1 we have that $FL \cong F\left[\frac{L}{L'}\right] \bigoplus \Delta_F(L:L')$. Since $\frac{L}{L'}$ is an abelian group, then $F\left[\frac{L}{L'}\right] \cong \bigoplus_{i=1}^n F(\xi_i)$, where ξ_i is a i^{th} -mitive root of writer i.

primitive root of unity, i = 1, ..., n, by a classical result by S. Perlis and G.L. Walker [13] for commutative group algebras.

Since FL is semisimple, then $\Delta_F(L:L')$ is also semisimple, and we can write $\Delta_F(L:L') \cong \bigoplus_{i=1}^{t} A_i$, where A_i is a simple algebra for i=1,...,t.

From proposition 4.1, we have that A_i is neither commutative nor associative.

O. Chein has proved in [7, Th. 1, p.35] the following result about Moufang loops, which we will need in the sequence.

Theorem 4.3 If L is a nonassociative Moufang loop for which every minimal set of generators contains an element of order 2, then there exists a nonabelian group G, and an element u of order 2 in L. such that each element of L may be uniquely expressed in the form $g.u^{\circ}$, where $g \in G$, $\alpha = 0, 1$. and the product of two elements of L is given by

$$g_1.(g_2.u) = (g_2g_1).u$$

 $(g_1.u).g_2 = (g_1g_2^{-1}).u$
 $(g_1.u).(g_2.u) = g_2^{-1}g_1$

Conversely, given any nonabelian group G, the loop L constructed as indicated above is a nonassociative Moufang loop.

Using the symmetric group S_3 of order 6 we can construct, as in theorem 4.3, the loop $L = M_{12}(S_3, 2)$, the smallest Moufang loop according to [7], which is also the smallest RA2 loop.

Labeling $G = S_3 = \{1, g_2, g_3, g_4, g_5, g_6\}$ and calling $u = g_7, g_2.u = g_8, g_3.u = g_9, g_4.u = g_{10}, g_5.u = g_{11}$ and $g_6.u = g_{12}$, we have the following loop table for L:

From this table it is easy to see that for $L=M_{12}(S_3,2)$ it holds that $L'=\{1,g_2,g_3\}\cong C_3$, the cyclic group of order 3 and $\frac{L}{L'}\cong C_2\times C_2$, the Klein group.

Let F be a field and suppose that the characteristic of F is different from 2 and 3. Then the loop algebra FL is semisimple. We will show the decomposition of FL as a direct sum of simple algebras.

Applying proposition 3.1 for N = L' we have

$$FL \cong F\left[\frac{L}{L'}\right] \bigoplus \Delta_F(L:L') \cong F[C_2 \times C_2] \bigoplus \Delta_F(L:L') \cong$$
$$\cong F \bigoplus F \bigoplus F \bigoplus F \bigoplus \Delta_F(L:L') .$$

We are going to exhibit a F-basis for the algebra $\Delta_F(L:L')$.

Define
$$f_o = 1 - \widehat{L'} = 1 - \frac{1}{3}.(1 + g_2 + g_3) = \frac{1}{3}.(2 - g_2 - g_3)$$

$$f_1 = (g_2 - g_3).f_o = g_2 - g_3$$

$$f_2 = g_4.f_o = \frac{1}{3}.(2g_4 - g_5 - g_6)$$

$$f_3 = (g_2 - g_3).g_4.f_o = g_5 - g_6$$

$$f_4 = g_7.f_o = \frac{1}{3}.(2g_7 - g_8 - g_9)$$

$$f_5 = ((g_2 - g_3).g_7).f_o = g_8 - g_9$$

$$f_6 = g_{10}.f_o = \frac{1}{3}.(2g_{10} - g_{11} - g_{12})$$

$$f_7 = ((g_2 - g_3).g_{10}).f_o = g_{12} - g_{11}$$

It's easy to see that $\{f_o, f_1, ..., f_7\}$ is linearly independent and generates $\Delta_F(L:L')$ over F. Its multiplication table is

| | f_o | f_1 | f_2 | f_3 | f_4 | f_5 | f_6 | f_7 |
|-------|-------|---------------|--------|-----------|--------|-----------|------------|---------|
| | | | | | | f_5 | | |
| f_1 | | $-3f_{\circ}$ | | | | $-3f_4$ | | |
| f_2 | f_2 | $-f_3$ | f_o | $-f_1$ | f_6 | $-f_7$ | f_4 | $-f_5$ |
| f_3 | f_3 | $3f_2$ | f_1 | $3f_o$ | $-f_7$ | $-3f_{6}$ | $-f_5$ | $-3f_4$ |
| f_4 | f_4 | $-f_{5}$ | f_6 | $-f_7$ | f_o | $-f_1$ | f_2 | $-f_3$ |
| f_5 | f_5 | $3.f_{4}$ | $-f_7$ | $-3f_{6}$ | f_1 | $3f_o$ | $-f_3$ | $-3f_2$ |
| f_6 | f_6 | $-f_7$ | f_4 | $-f_5$ | f_2 | $-f_3$ | f_{ϕ} | $-f_1$ |
| f_7 | f_7 | $3.f_{6}$ | $-f_5$ | $-3f_{4}$ | $-f_3$ | $-3f_{2}$ | f_1 | $3f_o$ |

The inequality $f_2.f_1 = -f_3 \neq f_1.f_2 = f_3$ shows that $\Delta_F(L:L')$ is not commutative and the inequality $(f_2 + f_4).[(f_2 + f_4).f_5)] = 2f_3 + 2f_5 \neq [(f_2 + f_4).(f_2 + f_4)].f_5 = 2f_5 - 2f_3$ shows that $\Delta_F(L:L')$ is not associative. A direct calculation shows that $\Delta_F(L:L')$ is simple.

ACKNOWLEDGEMENTS

This work was done while the author was visiting the Department of Mathematics and Statistics of Memorial University of Newfoundland (MUN). He wishes to thank to Dr. Bruce Watson and Shannon O'Brien for helping in the computations on the loop algebras of the Moufang loops of order 24 over GF(2).

References

- [1] L.G.X. de Barros, Isomorphisms of Rational Loop Algebras, Comm. in Algebra, 21 (11), (1993), 3977-3993.
- [2] L.G.X. de Barros, On Semisimple Alternative Loop Algebras, Comm. in Algebra, 21 (11), (1993), 3995-4011.

- [3] L.G.X. de Barros and C. Polcino Milies, Modular Loop Algebras of R.A. Loops, J. Algebra, to appear.
- [4] L.G.X. de Barros and B. Watson, Modular Loop Algebras of RA2 Loops, preprint
- [5] R.H. Bruck, Some results in the theory of linear nonassociative algebras, Trans. Amer. Math. Soc. 56, (1944), 141-199.
- [6] R.H. Bruck, A Survey of Binary Systems, Ergeb. Math. Grenzgeb 30, Springer-Verlag, Berlin, 1958.
- [7] O.Chein, Moufang Loops of Small Order I, Trans. Amer. Math. Soc., 188, (1974), 31-51.
- [8] O. Chein and E. G. Goodaire, Loops whose Loop Rings in Characteristic 2 are Alternative, Comm. in Algebra, 18(3) (1990), 659-688.
- [9] D.Coleman, Finite Groups with Isomorphic Group Algebras, Trans. Amer. Math. Soc., 105, (1962), 1-8.
- [10] W.E Deskins, Finite abelian groups with isomorphic group algebras, **Duke Math. J., 23**, (1956), 35-40.
- [11] E.G. Goodaire and C. Polcino Milies, Isomorphisms of Integral Alternative Loop Rings, Rend. Circolo Mat. Palermo, 37, (1988), 126-135.
- [12] G. Leal and C. Polcino Milies, Isomorphic Group (and Loop) Algebras,J. Algebra, 155, 1, (1993), 195-210.
- [13] S. Perlis and G.L. Walker, Abelian Group Algebras of Finite Order, Trans. Amer. Math. Soc., 68, (1950), 420-426.
- [14] H.O. Pflugfelder, Quasigroups and Loops: Introduction, Heldermann Verlag, Berlin, 1990.