Matemática Contemporânea, Vol. 6, 137–145
http://doi.org/10.21711/231766361994/rmc610

INDECOMPOSABLE R.A. LOOPS AND RELATED TOPICS

César Polcino Milies

1. Introduction

Let R be a commutative (and associative) ring with unity and let L be a loop. The *loop ring* of L over R was introduced in 1944 by R.H.Bruck as a means to obtain an important family of examples of non-associative algebras.

They are defined in precisely the same way as the more familiar concep of *group ring* is; namely, RL is the free R- module with basis L in which multiplication is introduced by extending that of L via the distributive laws.

Alternative loop algebras are the non-associative structures which are closest to group rings. They were first considered by E. G. Goodaire [4] in the case where R has no 2-torsion. He actually showed that the fact that RL is alternative depends only on the structure of L (but not on R). Thus, a loop L is called a *ring alternative loop*, or simply, an *R.A. loop* if its loop ring over any ring R, on the above conditions, is alternative.

In a subsequent paper, the inner structure of R.A. Loops was studied by O. Chein and E. G. Goodaire [3], who showed that R.A. loops are almost groups (they have a normal subgroup of index 2) and almost commutative (the commutator subloop is of order 2). Actually, they can be described as a particular instance of a well-known general construction of Moufang Loops (O. Chein [1], [2])

It is easy to see that any R.A. Loop can be written as the direct product of an indecomposable R.A. Loop and an abelian group. In what follows, we classify all indecomposable R.A. Loops, up to isomorphisms, and we describe the structure of their rational loop algebras.

The study of the structure of R.A. Loops, has focused attention on a particular type of groups; namely, those groups G whose quotient by their center $\mathcal{Z}(G)$ is isomorphic to the direct product of two cyclic groups of order two. The natural generalization of these groups for an arbitrary prime p, i.e., those groups G such that $G/\mathcal{Z}(G) \cong C_p \times C_p$ was studied by G. Leal and C. Polcino Milies in [12]. Using this fact, it was possible to obtain new results regarding the units of integral group rings of p-groups, a study started by J. Ritter and S. K. Sehgal in [13]. We quote these in our last section.

The proof of these results can be found in [9], [10] and [11] and will be published elsewhere.

2. Classifying Indecomposable R. A. Loops

We start by recalling the construction of R.A. Loops due to Chein and Goodaire.

Theorem 2.1. *Let L be an R.A. loop. Then, there exists a group $G \subset L$ and an element $u \in L$ such that $L = G \cup Gu$, $G' = L' = \{1, s\} \subseteq \mathcal{Z}(G) = \mathcal{Z}(L)$ and $L/\mathcal{Z}(L) = C_2 \times C_2 \times C_2$ where C_2 denotes a cyclic group of order 2 (and consequently, $G/\mathcal{Z}(G) = C_2 \times C_2$).*

Furthermore, the map $^* : L \to L$ given by

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

is an involution of L which extends linearly to RL. Setting $u^2 = g_0$, we have that $g_0 \in \mathcal{Z}(G)$ and multiplication in L is given by:

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= g_0 h^* g \end{aligned}$$

A loop constructed in such a way is denoted as $L(G, *, g_0)$. Conversely, given a group G and a map $^* : G \to G$ as above, the loop $L = L(G, *, g_0)$ is an R.A. loop.

As mentioned above, groups G such that $G/\mathcal{Z}(G) \cong C_p \times C_p$, p a rational prime, were studied in [12]. We quote these result below, though in the present case we shall need only to consider $p = 2$.

Lemma 2.2. *([12], Lemma 1.1) Let G be a group such that $G/\mathcal{Z}(G) \cong C_p \times C_p$. Then $G' =< s > \subseteq \mathcal{Z}(G)$ is cyclic of order p.* □

Theorem 2.3. *([12], Theorem 1.2) Let G be a group. Then $G/\mathcal{Z}(G) \cong C_p \times C_p$ if and only if G can be written in the form $G = D \times A$ where A is abelian and D is an indecomposable p-group such that $D =< x, y, \mathcal{Z}(D) >$ where $\mathcal{Z}(D) = C_{p^{m_1}} \times C_{p^{m_2}} \times C_{p^{m_3}}$ with $C_{p^{m_i}}$ cyclic of order p^{m_i}, $i = 1, 2, 3; m_1 \geq 1$; $m_2, m_3 \geq 0$ and $s = Ox, y \neq\in C_{p^{m_1}}$, $x^p \in C_{p^{m_1}} \times C_{p^{m_2}}$, $y^p \in C_{p^{m_1}} \times C_{p^{m_2}} \times C_{p^{m_3}}$.*

In what follows, we shall denote by t_i a generator of the cyclic group C_i, $1 \leq i \leq 3$.

Now, we turn our attention to indecomposable R.A. loops.

Theorem 2.4. *([9] , Theorem 2.2) Let $L = L(G, *, g_0)$ be an indecomposable R.A. loop. Then $G = D \times C$ where D is an indecomposable 2-group and C is a cyclic group of order 2^n, $n \geq 0$. Also if $n > 0$ then $g_0 = dc$ with $d \in \mathcal{Z}(D), c \in C, c \neq 1$.*

We shall always use w to denote a generator of the cyclic group C.

With the notation above, all possible types of indecomposable R.A. loops are given by the following table (see [9]) :

Indecomposable R.A. Loops

	$\mathcal{Z}(D)$	x^2	y^2	G	$u^2 = g_0$
$\mathbf{L_1}$	$< t_1 >$	1	1	D_1	1
$\mathbf{L_2}$	$< t_1 >$	t_1	t_1	D_2	t_1
$\mathbf{L_3}$	$< t_1 > \times < t_2 >$	1	t_2	D_3	1
$\mathbf{L_4}$	$< t_1 > \times < t_2 >$	t_1	t_2	D_4	t_1
$\mathbf{L_5}$	$< t_1 > \times < t_2 > \times < t_3 >$	t_2	t_3	D_5	1
$\mathbf{L_6}$	$< t_1 > \times < t_2 > \times < t_3 >$	t_2	t_3	D_5	t_1
$\mathbf{L_7}$	$< t_1 > \times < t_2 > \times < t_3 >$	t_2	t_3	$D_5 \times < w >$	w

3. Description of Rational Loop Algebras

Our main result regarding loop algebras of indecomposable R. A. Loops is the following.

Theorem 3.1. *Let L be an indecomposable R.A. loop. Then*

$$\mathbf{Q}L = \mathbf{Q}L(\frac{1+s}{2}) \oplus \mathbf{Q}L(\frac{1-s}{2})$$

and

1. $\mathbf{Q}L(\frac{1+s}{2}) \cong \mathbf{Q}(L/L') \cong \oplus_{2d\,|\,|L|}\, a_d \mathbf{Q}(\xi_d)$, *with a_d equal to the number of cyclic factors of L/L' of order d, and ξ_d a primitive dEth-root of unity.*

2. $\mathbf{Q}L(\frac{1-s}{2}) = \Delta(L : L')$ *is a sum of a_L simple alternative algebras with a_L equal to the number of subgroups H in $\mathcal{Z}(L)$ such that $\mathcal{Z}(L)/H$ is cyclic and $s \notin H$.*

3. $\mathcal{Z}(\Delta(L : L')) \cong \bigoplus \mathbf{Q}(\xi_H)$, *where the direct sum runs over all subgroups H as in (2) and ξ_H is a primitive $|\mathcal{Z}(L)/H|^{th}$-root of unity.*

Furthermore:

if $L = L_i$, $i = 1, 3$ or 5, then all simple components of $\Delta(L : L')$ are split Cayley-Dickson algebras.

if $L = L_i$, $i = 2, 4, 6$ or 7, then all simple components, but one, are split Cayley-Dickson algebras. The non-split component, in each case, is determined *by a primitive central idempotent of the form* $e = \widehat{H}(\frac{1-s}{2})$. *We list below the corresponding subgroup in each case.*

Loop	H
L_2	$\{1\}$
L_4	$< t_1t_2 >$
L_6	$< t_1t_2 > \times < t_1t_3 >$
L_7	$< t_1t_2 > \times < t_1t_3 > \times < t_1w >$

We recall that the Cayley-Dickson matrix algebra over a field F is defined as

$$C(F) = \begin{bmatrix} F & F^3 \\ F^3 & F \end{bmatrix}$$

where F^3 denotes the set of 3-dimensional vectors over F, addition is defined componentswise and multiplication in $C(F)$ is given by:

$$\begin{bmatrix} a & V \\ W & b \end{bmatrix} \begin{bmatrix} a' & V' \\ W' & b' \end{bmatrix} = \begin{bmatrix} aa' + V \cdot W' & aV' + b'V - W \times W' \\ a'W + bW' + V \times V' & bb' + W \cdot V' \end{bmatrix}$$

(see [17, Theorem 2.4.7]).

In [9] concrete isomorphisms are given between the simple components of the rational loop algebras and the Cayley-Dickson algebra.

4. Group Rings of some p-groups

Let $\mathcal{U} = \mathcal{U}(\mathbf{Z}G)$ denote the group of units of the integral group ring of a finite group G, and set $\mathcal{V} = \mathcal{V}(\mathbf{Z}G) = \{u \in \mathcal{U} \mid \varepsilon(u) = 1\}$, where $\varepsilon : \mathbf{Z}G \to \mathbf{Z}$ denotes the augmentation map. Since it is difficult to describe explicitly the full group of units, it has been a recent trend to determine sets of generators for subgroups of finite index in $\mathcal{V}$ (see for example [14, 15]). In particular, this was done in [8] for 2-groups G such that $G/Z(G)$ is the Klein four-group, where $Z(G)$ denotes the center of G.

Here, we shall be interested on indecomposable p-groups G such that $G/Z(G) \cong C_p \times C_p$. We begin with those indecomposable p-groups which have cyclic center. We set $Z(G) =< t \mid t^{p^n} = 1 >$.

Lemma 4.1. *There exist $x, y \in G$ such that*

$$G \; = < x,\, y,\, t \mid x^p = t^r,\; y^p = t^s, yx = t^i xy >,$$

where $0 \leq r, s \leq p-1$, and $o(t^i) = p$. Moreover, either $r = s = 0$ or $r = 1,\; s = 0$.

We can give a full description of these groups:

Proposition 4.2. *Let G be a finite indecomposable group such that $G/Z(G) \cong C_p \times C_p$ and $Z(G)$ is cyclic. Then G is isomorphic to one of the following groups:*

$$\begin{aligned} G_1 &= \; < x,\, y,\, t \mid x^p = y^p = t^{p^n} = 1 >, \\ G_2 &= \; < x,\, y,\, t \mid x^p = t,\; y^p = t^{p^n} = 1 > \end{aligned}$$

where we are assuming that t is central and the commutator $[x, y] = t^{p^{n-1}}$. Also, G_1 and G_2 are non-isomorphic.

Now, we give a description of the structure of $\mathbf{Q}G$.

Proposition 4.3. *Let G be as above. Then*

$$\mathbf{Q}G \cong \bigoplus_{i=0}^{n+1} a_i \mathbf{Q}(\xi_i) \bigoplus M_p(\mathbf{Q}(\xi)),$$

where ξ_i is a primitive root of unity of order p_i, a_i is the number of cyclic factors of G/G' of order p^i, and ξ is a primitive root of unity of order p^n.

As a consequence of these results, it is possible to describe subgroups of units of finite index. To this end, we introduce some notation.

For a given p-by-p matrix $A = (a_{ij})$, $0 \leq i, j \leq p-1$, let A^D denote the matrix obtained from A by putting in the k-th row $(0 \leq k \leq p-1)$ of A^D, the k-th pseudodiagonal of A, i.e.

$$A^D = \begin{bmatrix} a_{0,0} & a_{1,1} & \cdots & a_{p-2,p-2} & a_{p-1,p-1} \\ a_{p-1,0} & a_{0,1} & \cdots & a_{p-3,p-2} & a_{p-2,p-1} \\ a_{p-2,0} & a_{p-1,1} & \cdots & a_{p-4,p-2} & a_{p-3,p-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{1,0} & a_{2,1} & \cdots & a_{p-1,p-2} & a_{0,p-1} \end{bmatrix}$$

Also, we set $\overline{G} = G/G'$.

Proposition 4.4.

1. *$\mathcal{U}(\mathbf{Z}G_1)$ has a subgroup of finite index isomorphic with the direct product*

$$\mathcal{U}(1+p\mathbf{Z}\overline{G}) \times \left\{1+(1-\omega)A \in \mathcal{U}(M_p(\mathbf{Z}[\xi])) \mid A^D V \in M_p(p\mathbf{Z}[\xi])\right\}$$

2. *$\mathcal{U}(\mathbf{Z}G_2)$ has a subgroup of finite index isomorphic with the direct product*

$$\mathcal{U}(1+p\mathbf{Z}\overline{G}) \times \left\{1+(1-\omega)A \in \mathcal{U}(M_p(\mathbf{Z}[\xi])) \mid (A')^D V \in M_p(p\mathbf{Z}[\xi])\right\}$$

We now give another subgroup of finite index which is somehow easier to describe; the non-commutative direct factor being the same for all groups G.

Corollary 4.5. *$\mathcal{U}(\mathbf{Z}G)$ has a subgroup of finite index isomorphic with the direct product*

$$\mathcal{U}(1+p\mathbf{Z}\overline{G}) \times \{1+p(1-\omega)A \mid 1+p(1-\omega)A \in \mathcal{U}(M_p(\mathbf{Z}[\xi]))\}$$

The descriptions in the general case follow naturally from the cases above; see [11]

References

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

[2] O. Chein, *Moufang loops of small order*, Memoirs Amer. Math. Soc. 197 (1978).

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

[4] E.G. Goodaire, *Alternative Loop Rings*, Publ. Math. Debrecen, 30 (1983), 31–38.

[5] E.G. Goodaire and M.M. Parmenter, *Units in Alternative Loop Rings*, Israel J. of Math., 53 (1986), 209–216.

[6] E.G. Goodaire and M.M. Parmenter, *Semi-Simplicity of Alternative Loop Rings*, Acta Math. Hung. 50 (1987), 241–247.

[7] M. Hall Jr and J.K. Senior, *The groups of order 2^n ($n \leq 6$)*, Mac Millan, New York, 1964.

[8] E. Jespers and G. Leal,*Describing units in integral group rings of some 2-groups*, Comm. Algebra 19(6) (1991), 1809–1827.

[9] E. Jespers, G. Leal, C. Polcino Milies, *Classifying Indecomposable R.A. Loops*, preprint.

[10] E. Jespers, G. Leal, C. Polcino Milies, *Loop Algebras of Indecomposable R.A. Loops*, Comm. in Algebra, to appear.

[11] E. Jespers and C. Polcino Milies, *Group Rings of some p-groups*, preprint.

[12] G. Leal and C. Polcino Milies, *Isomorphic Group (and Loop) Algebras*, J. of Algebra 155, 1 (1993), 195-210.

[13] J. Ritter and S. Sehgal,*Integral Group Rings of some p-Groups*, Canad. J. Math. 34 (1) (1982), 233–246.

[14] J. Ritter and S. Sehgal,*Generators of Subgroups of $\mathcal{U}(\mathbf{Z}G)$*, Contemporary Math. 93 (1989), 331–347.

[15] J. Ritter and S. Sehgal,*Construction of Units in Integral Group Rings of Finite Nilpotent Groups*, Trans. Amer. Math. Soc. , 324(2)(1991), 603–621.

[16] A.D. Thomas and G.V. Woods, *Group Tables*, Shiva Publishing Ltd., Devon, 1980.

[17] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov, A.I. Shirshov, *Rings that are nearly associative*, Academic Press, New York, 1982.

Departamento de Matemática e Estatística
Universidade de São Paulo
01452-990 - São Paulo - SP
Brazil