Resenhas IME-USP 1995, Vol. 2, No. 1, 47 - 82.

Ring Alternative Loops and their Loop Rings[1]

Edgar G. Goodaire[2] and César Polcino Milies[3]

Abstract: In 1983, a few examples of Moufang loops whose loop rings are alternative, but not associative, were discovered. Since that time, there has been a great deal of work devoted to the study of such loops and to their loop rings. This paper is a survey of some of the more important results in this still relatively young area.

Key words: Alternative Ring, Moufang loop. Loop of Units, Torsion Units, Trivial Units, Isomorphism Problem.

AMS classification: Primary 17D05; Secondary 20N05, 16S34.

Contents

1. Loops whose Loop Rings are Alternative

1.1. **Historical Background.** The formula $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2$ which shows that the product of two sums of two squares is again the

[1]Primary 17D05; Secondary 20N05, 16S34

[2]The research was supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. 0GP0009087.

[3]The research was supported by CNPq. of Brasil, Proc. 501253/91-2.

sum of two squares is very familiar and most elegantly established with reference to the field of complex numbers.

The first noncommutative "field" was discovered in the early 1840's by Sir William Rowan Hamilton. More properly called a "division algebra" and denoted H in Hamilton's honour, this algebra is the 4-dimensional vector space over R (the reals) with basis $\{1, \mathsf{i}, \mathsf{j}, \mathsf{k}\}$. Thus a quaternion is a formal sum

$$q = a + b\mathsf{i} + c\mathsf{j} + d\mathsf{k}.$$

Two such elements are added "coordinatewise"

$$(a_1 + b_1\mathsf{i} + c_1\mathsf{j} + d_1\mathsf{k}) + (a_2 + b_2\mathsf{i} + c_2\mathsf{j} + d_2\mathsf{k}) =$$

$$(a_1 + a_2) + (b_1 + b_2)\mathsf{i} + (c_1 + c_2)\mathsf{j} + (d_1 + d_2)\mathsf{k}$$

and multiplied using the distributive laws and the following table which shows how to multiply the basis elements:

	1	i	j	k
1	1	i	j	k
i	i	−1	k	−j
j	j	−k	−1	i
k	k	j	−i	−1

Like the complex numbers, there is in the quaternions a notion of norm—for $q = a+b\mathsf{i}+c\mathsf{j}+d\mathsf{k} \in \mathsf{H}$, we set $|q| = a^2+b^2+c^2+d^2$—and, as with the complex numbers, norm is multiplicative: $|q_1q_2| = |q_1||q_2|$. This gives rise to a formula which shows that the product of two sums of four squares is another sum of four squares. This particular formula plays an important role in number theory; for example, it shows that to prove that every natural number is the sum of four squares, it is sufficient to establish the result just for primes.

For what integers n is it possible to write the product of two sums of n squares of variables as the sum of n squares of terms each of which is quadratic in the given variables? The answer, which was given by A. Hurwitz in 1898 is $n = 1, 2, 4, 8$. We refer the reader to a beautiful article on the history and solution of the n-squares problem by Charles Curtis [Cur63]. That there exist n-squares formulas for $n = 1, 2, 4, 8$ follows from the existence of the real numbers, complex numbers, quaternions and a certain nonassociative algebra called the *Cayley numbers*. That these are the only integers for which formulas exist is a consequence of the fact that the reals, complexes, quaternions and Cayley numbers are the only *alternative* division algebras over the real numbers. Most of the algebras in this paper will be alternative, a term we will define in Section 1.2.

Alternative rings arose out of the work of Ruth Moufang in the 1930's [Mou33]. Given a projective plane, one can label the points and the lines with elements from a set R and then define the addition and multiplication of elements of R in terms of incidence relations in the plane. (See [Hal59, Chapter 20] for an introduction to

projective planes and their coordinatization.) One can then relate various geometrical properties of the plane to algebraic properties of the "ring", $(R, +, \cdot)$. Two of the nicest theorems in this regard concern planes in which certain theorems due to Desargues and Pappus hold. A plane is desarguesian (pappian) if and only if it can be coordinatized by a planar alternative division ring (field). Since a field is a particular kind of alternative division ring (one which is commutative), one sees that a pappian plane is always desarguesian. Since a finite alternative division ring must be a field, a finite desarguesian plane is necessarily pappian. Much of Moufang's attention was directed at the multiplicative structure of an alternative division ring. Just as the non-zero elements of a field form a group under multiplication, so the non-zero elements of an alternative division ring form a *Moufang loop* under multiplication. All the loops in this paper will be Moufang, a term which will be defined in Section 1.3.

Group rings were implicitly introduced in a paper by Arthur Cayley in 1854 [Cay54]. Given Hamilton's definition of quaternions several years earlier, it was natural to consider more general algebraic expressions

$$a_1e_1 + a_2e_2 + \cdots + a_ne_n$$

where the a_i belong to some field F (originally the real or complex numbers) and the $\{e_1, \ldots, e_n\}$ is the basis for a vector space over the field. Multiplication of two elements with the above form could naturally be defined in terms of multiplication of basis elements (and distributivity). As a specific example, Cayley considered the case where the e_i were the six elements of the symmetric group S_3 and, thereby, gave the first instance of the now-familiar group algebra CS_3. The importance of group algebras became clear in the early 1900's after the work of T. Molien, G. Frobenius, I. Schur, H. Maschke, and later R. Brauer and E. Noether, on group representation theory. Since then, group algebras have taken on a life of their own. The appearance of two large books on the subject [Seh78, Pas77] at almost the same time, with very little subject matter in common and neither considering issues related to group representations, made it clear how the subject had grown by the mid 1970's.

The idea of relaxing the requirement of associativity and considering general loop rings or algebras is due to R. H. Bruck who introduced the idea of a *quasigroup algebra* in [Bru44]. There, Bruck proved that over a nonmodular field, the loop algebra of a finite loop was the direct sum of simple algebras (the analogue of the well-known theorem of Maschke for group algebras). Two years later, Bruck determined the centre of a loop algebra [Bru46]. The subject of loop algebras seems then to have laid dormant until 1955. In that year, Lowell Paige proved that in characteristic different from 2, in a commutative loop algebra, the very weak identity, $x^2x^2 = x^3x$, implies full associativity [Pai55]. In other words, there are no "interesting" nonassociative commutative loop algebras which are not already group algebras. This result strongly suggested that it was fruitless to expect that a loop algebra could satisfy any important identity without, in fact, being a group algebra. Nevertheless, in 1983, E. G. Goodaire showed that there

do exist alternative loop algebras (which are not group algebras) [Goo83]. It is this paper which gave birth to the subject we are surveying here.

1.2. **Alternative Rings.** A (not necessarily associative) ring is a triple $(R, +, \cdot)$ where $(R, +)$ is an abelian group, $(a, b) \mapsto a \cdot b$ is a binary operation on R, and both distributive laws hold: $a(b+c) = ab+ac$, $(a+b)c = ac+bc$, for all $a, b, c \in R$. If, in addition, $(R, +)$ is a module over a commutative, associative ring Φ such that $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for all $\alpha \in \Phi$ and all $a, b \in R$, then $(R, +, \cdot)$ is said to be a *(nonassociative) algebra.*

If a, b, c are three elements of a ring, the *commutator* $[a, b]$ and the *associator* $[a, b, c]$ are defined like this:

$$[a, b] = ab - ba \qquad \text{(ring) commutator}$$
$$[a, b, c] = (ab)c - a(bc). \qquad \text{(ring) associator}$$

Both these are linear functions of each of their arguments. The *nucleus* $\mathcal{N}(R)$ and centre $\mathcal{Z}(R)$ are the subrings of R defined by

$$\mathcal{N}(R) = \{a \in R \mid [a, x, y] = [x, a, y] = [x, y, a] = 0 \text{ for all } x, y \in R\}$$

$$\mathcal{Z}(R) = \{a \in \mathcal{N}(R) \mid [a, x] = 0 \text{ for all } x \in R\}.$$

A ring R is *alternative* if $[x, x, y] = [x, y, y] = 0$ for all $x, y \in R$. From these two identities, it can be shown easily that the associator is an alternating function of its arguments (whence the name "alternative"). So also is the *Kleinfeld function*

$$f(w, x, y, z) = [wx, y, z] - x[w, y, z] - [x, y, z]w.$$

(See [Kle63] for a proof.) It follows that in any alternative ring, the following are identities.

$$[x^2, y, z] = x[x, y, z] + [x, y, z]x$$
$$[xy, x, z] = [y, x, z]x$$
$$[yx, x, z] = x[y, x, z]$$
$$((xy)x)z = x(y(xz)) \qquad \text{left Moufang identity}$$
$$((xy)z)y = x(y(zy)) \qquad \text{right Moufang identity}$$
$$(xy)(zx) = (x(yz))x \qquad \text{middle Moufang identity}$$

As indicated, the last three identities are known as the left, right and middle *Moufang* identities respectively because they were first studied by R. Moufang.

In nonassociative products, we frequently use dots instead of parentheses to indicate order of multiplication, juxtaposition taking precedence over dot. So, for example, we might write $(x \cdot yz)x$ instead of $(x(yz))x$.

One of the most useful properties of alternative rings is the fact that if three elements associate, then the subring which they generate is associative [BK51]. For example, since the associator is an alternating function, x, x and y associate for any x, y in an alternative ring. Thus alternative rings are *diassociative* in the sense

that the subring generated by any two elements is always associative. This result is due to E. Artin and its proof appears, for example, in R. D. Schafer's classic text [Sch66, Theorem 3.1, p. 29].

The most important example of an alternative ring (which is not associative) is the ring of Cayley numbers whose underlying set is

$$\mathcal{C} = \mathsf{H} + \mathsf{H}\ell = \{a + b\ell \mid a, b \in \mathsf{H}\}$$

where H denotes the real quaternion algebra and ℓ is an indeterminate. In $\mathcal{C}$, one adds in the obvious way and multiplies in a way which mimics multiplication in the complex numbers:

$$(a + b\ell) + (c + d\ell) = (a + c) + (b + d)\ell$$
$$(a + b\ell)(c + d\ell) = (ac - \bar{d}b) + (da + b\bar{c})\ell,$$

where $a, b, c, d \in \mathsf{H}$ and $\bar{x}$ denotes the conjugate of the quaternion x. The Cayley numbers form an 8-dimensional algebra over R with basis

$$\{1, i, j, k\} \cup \{\ell, i\ell, j\ell, k\ell\} \tag{1.2.1}$$

where $\{1, i, j, k\}$ is the usual basis for H.

More general than the Cayley numbers is a *Cayley-Dickson* algebra, which we now describe. Let B be an associative algebra with an involution $b \mapsto \bar{b}$ (an antiautomorphism of period 2) such that $b + \bar{b}$ and $b\bar{b}$ are scalars for all $b \in B$. Let ℓ be an indeterminate and α be a scalar, and let A be the vector space direct sum $B \oplus B\ell$. Define addition and multiplication by

$$(a + b\ell) + (c + d\ell) = (a + c) + (b + d)\ell$$

$$(a + b\ell)(c + d\ell) = (ac + \alpha\bar{d}b) + (da + b\bar{c})\ell.$$

Then A is an alternative algebra known as a Cayley-Dickson algebra. Any Cayley-Dickson algebra is simple. It is a division algebra if and only if, for all nonzero $a \in A$, we have $a\bar{a} \neq 0$. Thus, if a Cayley-Dickson algebra over a field F is not a division algebra, then it has zero divisors and, interestingly, in this case it is unique (up to isomorphism) [Sch66, Sections 4 and 5]. That Cayley-Dickson algebra over F which is not a division algebra is called the *split* Cayley algebra.

With $F = \mathsf{R}$ and $\alpha = -1$, the Cayley numbers are an instance of a Cayley-Dickson division algebra. The unique split Cayley algebra over R has several presentations, one as the *vector-matrix algebra* of M. Zorn. The elements of Zorn's algebra are matrices of the form

$$\begin{bmatrix} a & x \\ y & b \end{bmatrix}$$

where $a, b \in \mathsf{R}$ and x, y are elements of R^3 which we think of as vectors. Such matrices are added entrywise, but multiplied according to the following modification of the usual rule:

$$\begin{bmatrix} a_1 & \mathsf{x}_1 \\ \mathsf{y}_1 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & \mathsf{x}_2 \\ \mathsf{y}_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + \mathsf{x}_1 \cdot \mathsf{y}_2 & a_1\mathsf{x}_2 + b_2\mathsf{x}_1 - \mathsf{y}_1 \times \mathsf{y}_2 \\ a_2\mathsf{y}_1 + b_1\mathsf{y}_2 + \mathsf{x}_1 \times \mathsf{x}_2 & b_1b_2 + \mathsf{y}_1 \cdot \mathsf{x}_2 \end{bmatrix}$$

where $\cdot$ and $\times$ denote the dot and cross products respectively in R^3.

1.3. **Moufang Loops.** A *loop* is a set L together with a (closed) binary operation $(a, b) \mapsto ab$ for which there is a two-sided identity element 1 and such that the right and left translation maps

$$R_x : a \mapsto ax \qquad \text{and} \qquad L_x : a \mapsto xa \tag{1.3.1}$$

are bijections for all $x \in L$. This requirement implies that, for any $a, b \in L$, the equations $ax = b$ and $ya = b$ have unique solutions x, y. (The multiplication table of a finite loop is a Latin square.)

The concepts of commutator and associator have definitions in loops which are entirely analogous to their definitions for rings. Given a, b, c in a loop L, the *commutator* (a, b) and *associator* (a, b, c) are defined (uniquely) by

$$\begin{aligned} ab &= ba(a, b) && \text{(loop) commutator} \\ (ab)c &= [a(bc)](a, b, c) && \text{(loop) associator} \end{aligned}$$

The *commutator subloop* is the subloop generated by the set of all commutators and the *associator subloop* is the subloop generated by all associators. The *nucleus* and *centre* of L are the subloops $\mathcal{N}(R)$ and $\mathcal{Z}(R)$, respectively, defined by

$$\begin{aligned} \mathcal{N}(R) &= \{x \in L \mid (a, b, x) = (a, x, b) = (x, a, b) = 1, \text{ for all } a, b \in L\} \\ \mathcal{Z}(L) &= \{x \in \mathcal{N}(L) \mid (a, x) = 1 \text{ for all } a \in L\}. \end{aligned}$$

A loop L is *Moufang* if it satisfies any of the three Moufang identities encountered earlier:

$$\begin{aligned} ((xy)x)z &= x(y(xz)) && \text{left Moufang identity} \\ ((xy)z)y &= x(y(zy)) && \text{right Moufang identity} \\ (xy)(zx) &= (x(yz))x && \text{middle Moufang identity} \end{aligned}$$

Moufang showed that any of these identities implies the other two (in a loop). For proofs, we refer the reader to [Pfl90, Chapter IV]. Just as with alternative rings, if three elements of a Moufang loop associate in some order, then they associate in all orders; moreover, the subloop which they generate is a group. In particular, Moufang loops are *diassociative*: the subloop generated by any pair of elements is always associative.

Just as the quaternion group of order 8 is related to the quaternion algebra, so the *Cayley loop* is related to the Cayley numbers. The Cayley loop is that Moufang

loop (of order 16) whose elements are the eight elements which form the basis for the Cayley numbers (1.2.1) together with their negatives.

In a very real sense, the Cayley loop plays the role in the theory of Moufang loops that the quaternions play in group theory. For example, any Moufang loop which is not a group and in which all subloops are normal (such a loop is called *Hamiltonian*) is the direct product of the Cayley loop, an abelian group of exponent 2 and an abelian group all of whose elements have odd order [Nor52].

Since the Moufang identities are satisfied in an alternative ring, any subset of an alternative ring which is closed under multiplicative inverses and ring multiplication is a Moufang loop. Thus, the full set of all invertible elements of an alternative ring R is a Moufang loop; it's called the (Moufang) *loop of units* or *unit loop* of the ring and is denoted $\mathcal{U}(R)$.

We now give a construction of a whole family of Moufang loops, due to Orin Chein [Che74]. Let G be a nonabelian group and u be an indeterminate. Let L be the disjoint union $L = G \dot{\cup} Gu$ and define multiplication in L by

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^{-1})u \\ (gu)(hu) &= h^{-1}g \end{aligned}$$

for $g, h \in G$. Then L is a Moufang loop which is not a group; it is denoted $M(G, 2)$. The case $G = S_3$, the symmetric group on three letters, gives rise to $M(S_3, 2)$, a Moufang loop of order 12 and the smallest Moufang loop which is not a group.

Generalizing this construction, suppose G is again a nonabelian group, g_0 is a central element in G, and $g \mapsto g^*$ is an involution of G such that gg^* is in the centre of G for every $g \in G$. Let $L = G \dot{\cup} Gu$ and define multiplication on G by

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= g_0 h^* g \end{aligned} \tag{1.3.2}$$

for $g, h \in G$, where $u^2 = g_0$ is central in G and $g_0^* = g_0$. Then L is a Moufang loop denoted $M(G, *, g_0)$. When $*$ is the inverse map on G and $g_0 = 1$, the loop $M(G, *, 1)$ is just $M(G, 2)$. With $G = Q$, the quaternion group of order 8, g_0 the nonidentity element in the centre of Q and $*$ again the inverse map, it can be shown that $M(Q, *, g_0)$ is the Cayley loop.

1.4. **Alternative Loop Rings.** Let L be a loop and let R be a commutative associative ring with 1. The *loop ring* of L with coefficients in R is the free R-module RL with basis L and multiplication given by extending, via the distributive laws, the multiplication in L. Thus the elements of RL are formal sums, $\sum_{g \in L} \alpha_g g$,

where the $\alpha_g \in R$ are almost all 0 and unique in the sense that

$$\sum \alpha_g g = \sum \beta_g g \quad \text{implies} \quad \alpha_g = \beta_g \text{ for all } g \in L.$$

Addition and multiplication are given by

$$\sum \alpha_g g + \sum \beta_g g = \sum (\alpha_g + \beta_g) g$$

$$\left(\sum \alpha_g g\right)\left(\sum \beta_g g\right) = \sum \Big(\sum_{hk=g} \alpha_h \beta_k\Big) g.$$

By an *alternative loop ring*, we mean a loop ring which happens also to be alternative. As a subloop of the loop of units of an alternative loop ring RL, the loop L which defines RL must of course be Moufang, as noted earlier. That such (nonassociative) loops actually exist was first shown by E. G. Goodaire [Goo83].

1.4.1 Theorem. *Suppose R is a commutative and associative ring with unity and with no elements of additive order 2. Suppose L is a Moufang loop of the form $L = M(G, *, g_0)$. Then RL is an alternative ring if and only if $g + g^*$ is in the centre of RL for each $g \in G$, and this occurs if and only if, for each $g \in G$, either g is central or else $h^{-1}gh \in \{g, g^*\}$ for all $h \in G$.*

We assume throughout this paper that all rings are without elements of additive order 2. Consider the implications of Theorem 1.4.1 in the case that $g^* = g^{-1}$. According to the theorem, RL is alternative if and only if $g + g^{-1}$ is in the centre of RG for all $g \in G$. It is well-known that the centre of RG is spanned by the finite class sums of G, a class sum being the sum of all the elements in a conjugacy class (see, for example, [Pas77, Chapter 4]). Thus, $g + g^{-1}$ is central if and only if, for all $h \in G$, $h^{-1}gh \in \{g, g^{-1}\}$. This forces all subgroups of G to be normal, so that G is Hamiltonian and hence the direct product $Q \times E \times A$, where Q is the quaternion group of order 8, E is an abelian group of exponent 2 and A is an abelian group all of whose elements have odd order [Hal59]. In our situation, A is necessarily trivial as can be seen by considering the possibility that an element $(q, 1, a) \in Q \times E \times A$ has a conjugate equal to its inverse. Since, for $G = Q \times E$, every conjugate of $g \in G$ is g or g^{-1}, we obtain the following theorem which establishes, unequivocally, the existence of (nonassociative) alternative loop rings.

1.4.2 Theorem. *Let R be a ring without elements of additive order 2, G a nonabelian group, g_0 a central element in G and $L = M(G, -1, g_0)$. Then the loop ring RL is alternative if and only if $G = Q \times E$ is the direct product of the quaternion group of order 8 and an abelian group of exponent 2.*

For example, the loop rings of the Cayley loop are alternative since the Cayley loop is $M(Q, -1, g_0)$, where g_0 is the nonidentity element of $Z(Q)$. Similarly, $M(Q, 2) = M(Q, -1, 1)$ also has alternative loop rings.

It is more difficult to determine, for a general involution on a group G, the conditions under which $g + g^*$ is central for all g.

1.4.3 Theorem (Chein and Goodaire [CG86]). *Let R be a ring without elements of additive order 2 and let G be a nonabelian group. Then RL is alternative for some $L = M(G, *, g_0)$ if and only if G has a unique commutator $s \neq 1$ and property*

$$LC: \quad gh = hg \text{ for } g, h \in G \text{ if and only if } g, h \text{ or } gh \text{ is central.}$$

In any group (or diassociative loop), elements x and y will commute if any of x, y, xy is central. If this is the only situation in which elements commute, it is unlikely that a randomly chosen pair of elements will commute; there is a certain lack of commutativity within the group. For this reason, we refer to the above property in a group (or loop) as the *LC property*, "LC" for lack of commutativity.

Groups with LC can be rather tightly characterized. Suppose G is a nonabelian group with LC. Then squares are central so that $G/\mathcal{Z}(G)$ is a 2-group and a vector space over the field of two elements. It follows $G/\mathcal{Z}(G)$ has a basis of precisely two elements; i.e., that G is an extension of its centre by $C_2 \times C_2$. Conversely, it is easy to see that such a group must have LC.

1.4.4 Proposition. *A nonabelian group has the lack of commutativity property if and only if $G/\mathcal{Z}(G) \cong C_2 \times C_2$.*

Groups G in which $G/\mathcal{Z}(G) \cong C_p \times C_p$ for a prime p were studied by G. Leal and C. Polcino Milies in [LM93]. With $p = 2$, one of their results gives the following.

1.4.5 Theorem. [LM93, Lemma 1.1] *G has property LC if and only if G can be written in the form $G = D \times A$, where A is abelian and D is an indecomposable 2-group generated by its centre and two elements x and y which satisfy*

i) $\mathcal{Z}(D) = C_{2^{m_1}} \times C_{2^{m_2}} \times C_{2^{m_3}}$, *where $C_{2^{m_i}}$ is cyclic of order 2^{m_i} for $i = 1, 2, 3$, $m_1 \geq 1$ and $m_2, m_3 \geq 0$;*
ii) $(x, y) \in C_{2^{m_1}}$;
iii) $x^2 \in C_{2^{m_1}} \times C_{2^{m_2}}$ *and* $y_2 \in C_{2^{m_1}} \times C_{2^{m_2}} \times C_{2^{m_3}}$.

An *indecomposable* group is one that is not a direct product except in the trivial way (one of the groups is the one element group). Those finite indecomposable groups for which $D/\mathcal{Z}(D) \cong C_2 \times C_2$ have been completely classified by Jespers, Leal and Polcino Milies who obtained the following theorem.

1.4.6 Theorem. [JLM] *Let G be a finite group. Then $G/\mathcal{Z}(G) \cong C_2 \times C_2$ if and only if G can be written in the form $G = D \times A$, where A is abelian and $D = \langle \mathcal{Z}(D), x, y \rangle$ is of one of the following five types of indecomposable 2-groups:*

Type	$\mathcal{Z}(D)$	D
D_1	$\langle t_1 \rangle$	$\langle x, y, t_1 \mid (x,y) = t_1^{2^{m_1}-1}, x^2 = y^2 = t_1^{2^{m_1}} \rangle$
D_2	$\langle t_1 \rangle$	$\langle x, y, t_1 \mid (x,y) = t_1^{2^{m_1}-1}, x^2 = y^2 = t_1,$ $t^{2^{m_1}} = 1 \rangle$
D_3	$\langle t_1 \rangle \times \langle t_2 \rangle$	$\langle x, y, t_1, t_2 \mid (x,y) = t_1^{2^{m_1}-1}, x^2 = t_1^{2^{m_1}} =$ $t_2^{2^{m_2}} = 1, y^2 = t_2 \rangle$
D_4	$\langle t_1 \rangle \times \langle t_2 \rangle$	$\langle x, y, t_1, t_2 \mid (x,y) = t_1^{2^{m_1}-1}, x^2 = t_1, y^2 = t_2,$ $t_1^{2^{m_1}} = t_2^{2^{m_2}} = 1 \rangle$
D_5	$\langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle$	$\langle x, y, t_1, t_2, t_3 \mid (x,y) = t_1^{2^{m_1}-1}, x^2 = t_2,$ $y^2 = t_3, t_1^{2^{m_1}} = t_2^{2^{m_2}} = t_3^{2^{m_3}} = 1 \rangle$

1.5. **RA Loops.** An *RA (ring alternative)* loop is a loop whose loop ring RL over some ring R (without elements of additive order 2) is alternative, but not associative. These loops can be described in various ways, the most basic of which is this.

1.5.1 Theorem. [Goo83] *A nonassociative L is an RA loop if and only if*

(i) *if three elements $g, h, k \in L$ associate in some order, then they associate in all orders;*

(ii) *if three elements $g, h, k \in L$ do not associate, then $gh \cdot k = g \cdot kh = h \cdot gk$.*

Using this theorem, it is not hard to show

1.5.2 Corollary. *The direct product $L \times K$ of loops is an RA loop if and only if precisely one of L and K is an RA loop while the other is an abelian group.*

In loop theory, a subloop H of a loop L is *normal* if $Hx = xH$, $Hx \cdot y = H \cdot xy$, $xH \cdot y = x \cdot Hy$ and $x \cdot yH = xy \cdot H$ for all x and y in L. The following corollary is therefore of interest. We supply a proof, in part to illustrate the use of the theorem.

1.5.3 Corollary. *A subloop H of an RA loop L is normal if and only if $xH = Hx$ for all $x \in G$.*

Proof. We show that, for RA loops, the conditions

$$Hx \cdot y = H \cdot xy, \quad xH \cdot y = x \cdot Hy \quad \text{and} \quad x \cdot yH = xy \cdot H \text{ for all } x, y$$

follow from $Hx = xH$ for all x. Assuming $Hx = xH$ for all x, to prove $Hx \cdot y = H \cdot xy$, for instance, let $x, y \in L$ and $h \in H$. Then either $hx \cdot y = h \cdot xy$ or

$hx \cdot y = x \cdot hy = xy \cdot h = h' \cdot xy$ for some $h' \in H$ (since $H \cdot xy = xy \cdot H$), so $Hx \cdot y \subseteq H \cdot xy$. The other inclusion follows by reversing the argument. In a similar way, one shows that $xH \cdot y = x \cdot Hy$ and $x \cdot yH = xy \cdot H$ for all x, y. □

The next theorem summarizes some of the most fundamental characteristics of an RA loop.

1.5.4 Theorem. *An RA loop L has the following properties:*

(i) *for each $x \in L$, $x^2 \in \mathcal{N}(L)$;*
(ii) $\mathcal{N}(L) = \mathcal{Z}(L)$;
(iii) $(g, h) = 1$ *for $g, h \in L$ if and only if $(g, h, k) = 1$ for all $k \in L$;*
(iv) $(g, h, k) \neq 1$ *implies $(g, h, k) = (g, h) = (g, k) = (h, k)$ is a central element of order 2;*
(v) *the associator and commutator subloops of L are equal, of order 2 and contained in the centre of L. (This subloop is denoted L'.)*

Suppose x, y and z are elements of an RA loop L. Since L is Moufang, if these elements do not associate in one particular order, they cannot associate in any order. In this case, by part (iii) of the theorem, $(x, y) \neq 1$, $(x, z) \neq 1$ and $(y, z) \neq 1$. By part (iv), there exists a central element s of order 2 such that $L' = \langle s \rangle$, so

$$(x, y, z) \neq 1 \quad \text{implies} \quad (x, y, z) = (x, y) = (x, z) = (y, z) = s.$$

This condition may be used to characterize RA loops.

1.5.5 Theorem. [Goo83] *A nonassociative loop L is an RA loop if and only if it contains a central element s of order 2 such that for all $x, y, z \in L$,*

(i) *if x, y, z associate in some order, then they associate in all orders;*
(ii) *if $(x, y, z) \neq 1$, then $(x, y, z) = (x, y) = (x, z) = (y, z) = s$.*

Proof. The paragraph preceding the statement of the theorem gives the proof in one direction. Conversely, suppose L is a nonassociative loop with central element s of order 2 such that (i) and (ii) hold for all $x, y, z \in L$. In order to show that L is an RA loop, it is enough, by Theorem 1.5.1, to show that if $(x, y, z) \neq 1$, then $xy \cdot z = y \cdot xz = x \cdot zy$. But

$$xy \cdot z = (x \cdot yz)(x, y, z) = (x \cdot yz)e = (x \cdot zy)s^2 = x \cdot zy$$

the third equality holding since $(y, z) = s$ is central. Also,

$$xy \cdot z = (yx \cdot z)s = (y \cdot xz)s^2 = y \cdot xz$$

completing the proof. □

Of the many remarkable properties of RA loops, perhaps none is more satisfying (and useful) than the fact that an RA loop has property LC. This property makes possible the following very simple characterization of RA loops.

1.5.6 Theorem (Chein and Goodaire [CG86]). *A Moufang loop is an RA loop if and only if it has property LC and a unique nonidentity commutator, and it is not associative.*

One important consequence of this theorem is this.

1.5.7 Corollary. *An RA loop L is an extension of its centre by $C_2 \times C_2 \times C_2$, where C_2 denotes the cyclic group of order 2.*

We are now in a position to describe quite explicitly the structure of an RA loop. Let L be an RA loop with unique nonidentity commutator s and centre $\mathcal{Z}$. Suppose a and b are any two elements of L which do not commute. Then there is some $u \in L$ for which a, b, u do not associate. Each subgroup $\mathcal{Z}a$, $\mathcal{Z}b$, $\mathcal{Z}u$ of $L/\mathcal{Z}$ is cyclic of order 2 (for any x, $x^2 \in \mathcal{N}(L) = \mathcal{Z}(L)$, by Theorem 1.5.4), and the product $\langle \mathcal{Z}a \rangle \times \langle \mathcal{Z}b \rangle \times \langle \mathcal{Z}u \rangle$ is direct, because of the LC property. By Corollary 1.5.7, this direct product is $L/\mathcal{Z}$. Letting G be the subloop of L generated by a, b and $\mathcal{Z}$, we note that G is a group by diassociativity and the definition of centre. Thus u is not in G and L is the disjoint union $G \dot{\cup} Gu$.

Now, for $g \in G$, define $g^* = ugu^{-1}$. Thus $g^* = g$ or sg. In fact, we can say much more. It turns out that $g \mapsto g^*$ is an involution on G such that

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{Z} \\ sg & \text{if } g \notin \mathcal{Z} \end{cases} \tag{1.5.8}$$

and that elements $L = G \cup Gu$ multiply according to the rules (1.3.2) given in Section 1.3. Thus the construction of the loop $M(G, *, g_0)$ given earlier turns out to describe exactly how RA loops arise.

1.5.9 Theorem. *If L is an RA loop, then L is a loop of the form $M(G, *, g_0)$, where G is any group generated by the centre of L and two noncommuting elements of L. If G is such a group, then $\mathcal{Z}(G) = \mathcal{Z}(L)$, G has LC and a unique nonidentity commutator s, and the involution $*$ is given by* (1.5.8). *Conversely, for any nonabelian group G with LC and a unique nonidentity commutator s, the loop $M(G, *, g_0)$ is an RA loop for any $g_0 \in \mathcal{Z}(G)$, where $*$ is given by* (1.5.8).

Just as with groups, we call a loop L *indecomposable* if it is not the direct product of two proper subloops. Moreover, we will say that ring alternative loops L_1 and L_2 are *equivalent* if $L_1 \cong L \times A_1$ and $L_2 \cong L \times A_2$ where A_1 and A_2 are abelian groups, possibly of order 1, and L is an indecomposable RA loop.

1.5.10 Theorem. *Any periodic RA loop is equivalent to an RA loop which is a 2-loop.*

Proof. Suppose that x is an element of odd order $2n + 1$ in the RA loop L. Then $x^{-1} = (x^2)^n \in \mathcal{Z}(L)$ and so $x \in \mathcal{Z}(L)$. Thus the set A of elements of odd order is central, from which it is readily apparent that A is a normal (abelian) subgroup of L. Next, consider the set L_1 consisting of those elements of L whose order is a power of 2. If x and y are any two elements in L, then for $s \geq 2$, $(xy)^{2^s} = x^{2^s} y^{2^s}$

from whence it follows that L_1 is a subloop of L. Since L is periodic, $L = L_1 A$. Clearly $L_1 \cap A = \{1\}$ and A is normal. Also L_1 is normal because for any $x = y_1 a \in L$, $y_1 \in L_1$ and $a \in A$, we have $x^{-1} L_1 x = a^{-1} y_1^{-1} L_1 y_1 a = y_1^{-1} L_1 y_1 \subseteq L_1$ since a is central and L_1 is a subloop. Hence $L \cong L_1 \times A$ [Bru58, Lemma 5.1, p. 73]. Finally, since L is not associative, neither is L_1, so L_1 is an RA 2-loop equivalent to L. □

Because of this theorem, the search for inequivalent finite RA loops can be limited to loops of order 2^n, $n \geq 4$ (any Moufang loop of order less than 12 is a group) and, in fact, we can construct RA loops of all these orders, no two equivalent, as follows. Let $N = 2^n$ with $n \geq 1$ and let G be the group generated by two elements a and b with $a^{2N} = b^2 = 1$, $ba = a^{N+1} b$. Then $\mathcal{Z}(G) = \langle a^2 \rangle$ is cyclic, $G' = \langle a^N \rangle$ is central of order 2, and $G/\mathcal{Z}(G) \cong C_2 \times C_2$. Necessarily, G has property LC and so all the loops of the form $M(G, *, g_0)$, $*$ given by (1.5.8), are RA loops of order $8|\mathcal{Z}(G)| = 8N = 2^{n+3}$. Furthermore, they are indecomposable because their centres are. Now it is not difficult to show that the group G described here is generated by any pair of elements which do not commute. This observation, as well as basic properties of RA loops (most importantly, the one expressed in Theorem 1.5.4(iii)), lead quickly to a most significant feature of the loops we have constructed ¿from G: all their proper subloops are associative. The argument, briefly, is as follows: if x_1, x_2 and x_3 are any elements of an RA loop $M(G, *, g_0)$ and they all belong to G, then obviously the subloop $\langle x_1, x_2, x_3 \rangle$ generated by the x_i is associative. If x_1 and x_2 are in G, x_3 is in Gu and x_1 and x_2 do not commute, then they generate G and so quite clearly $\langle x_1, x_2, x_3 \rangle = L$. The possibility that just x_1 is in G while both x_2 and x_3 lie in Gu reduces immediately to the case of two generators in G since $\langle x_1, x_2, x_3 \rangle = \langle x_1, x_2 x_3, x_3 \rangle$; so does the final case, all x_i in Gu, since $\langle x_1, x_2, x_3 \rangle = \langle x_1 x_2, x_2 x_3, x_3 \rangle$.

There are ten RA loops of order less than 64, which we wish to enumerate, but first, it is convenient to record here the following very useful result.

1.5.11 Proposition. *If G is a nonabelian group such that $M(G, *, g_0)$ is an RA loop, and if A is any abelian group, then $M(G \times A, *, (g_0, 1))$ is an RA loop isomorphic to $M(G, 2, g_0) \times A$.*

In the enumeration of the RA loops of order less than 64 which follows, we name the loop using the nomenclature of O. Chein [Che78] and also write each loop in the form $M(G, *, g_0)$ where, in each case, $*$ is the involution given by (1.5.8) and s is the unique nonidentity commutator in G. (Note that $*$ coincides with the map $g \mapsto g^{-1}$ in the quaternion group Q and in $Q \times E$ for any elementary abelian

2-group E.

$$Q = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b \rangle$$

$$D_4 = \langle a, b \mid a^4 = b^2 = 1, ba = a^{-1}b \rangle$$

$$16\Gamma_2 c_2 = \langle a, b \mid a^4 = b^4 = 1, (a, b) = a^2 \rangle$$

$$16\Gamma_2 b = \langle a, b, c \mid a^4 = 1, (a, c) = (b, c) = 1, a^2 = b^2 = c^2 = (a, b) \rangle$$

$$16\Gamma_2 d = \langle a, b \mid a^8 = b^2 = 1, (a, b) = a^4 \rangle$$

There are two (necessarily indecomposable) RA loops of order 16:

1. $M_{16}(Q) = M(Q, -1, s)$, the Cayley loop, and
2. $M_{16}(Q, 2) = M(Q, -1, 1) = M(D_4, *, s)$.

There are six RA loops of order 32, two of which are direct products of the loops of order 16 with the cyclic group of order 2,

3. $M_{32}(C, 9) = M_{16}(Q) \times C_2 = M(Q, -1, s) \times C_2 = M(Q \times C_2, -1, (s, 1))$ and
4. $M_{32}(Q \times C_2, 2) = M_{32}(Q \times C_2, -1, (1, 1)) = M(Q, -1, 1) \times C_2 = M_{16}(Q, 2) \times C_2$

and four of which are indecomposable loops:

5. $M_{32}(E_i, 16) = M(16\Gamma_2 b, *, a_2)$,
6. $M_{32}(5, 5, 5, 2, 2, 4) = M(16\Gamma_2 d, *, a^2)$,
7. $M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_1, 16\Gamma_2 c_1) = M(16\Gamma_2 c_2, *, a^2 b^2)$, and
8. $M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_2^\sharp, 16\Gamma_2 c_2^\sharp) = M(16\Gamma_2 c_2, *, a^2)$.

Finally, there are two RA loops of order 48, these being the direct products of $M_{16}(Q)$ and $M_{16}(Q, 2)$ with the cyclic group of order 3.

9. $M_{48}(7, 7, 7, 2, 2, 6) = M_{16}(Q) \times C_3 = M(Q \times C_3, *, s)$ and
10. $M_{48}(7, 7, 7, 2, 4, 6) = M_{16}(Q, 2) \times C_3 = M(D_4 \times C_3, *, s)$.

E. Jespers, G. Leal and C. Polcino Milies have classified all finite RA loops.

1.5.12 Theorem. [JLM] *Let $L = M(G, *, g_0)$ be a finite indecomposable RA loop. Then G is either one of the five groups specified in Theorem 1.4.6 or the direct product $D_5 \times \langle w \rangle$ of D_5 and a cyclic group $\langle w \rangle$ and L is one of the following seven types of loops:*

Type	G	x^2	y^2	g_0
L_1	D_1	1	1	1
L_2	D_2	t_1	t_1	t_1
L_3	D_3	1	t_2	1
L_4	D_4	t_1	t_2	t_1
L_5	D_5	t_2	t_3	1
L_6	D_5	t_2	t_3	t_1
L_7	$D_5 \times \langle w \rangle$	t_2	t_3	w

1.6. **The Nucleus and Centre of an Alternative Loop Ring.** We conclude this chapter by recording some rather basic information about the structure of an alternative loop ring.

Let R be an associative ring with 1 of characteristic different from 2. If L is a loop such that RL is an alternative ring, then, by Theorem 1.5.9, $L = M(G, *, g_0)$ for some nonabelian group G with LC and some central $g_0 \in G$. Furthermore $G' = \{1, s\}$ and the map $*: G \to G$ defined 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. This involution extends to an involution on L (change G to L in the definition) and then to ring involutions first on the group ring RG and then on the loop ring RL by setting

$$(\sum_{g \in G} \alpha_g g)^* = \sum_{g \in G} \alpha_g g^* \qquad \text{and} \qquad (\sum_{\ell \in \ell} \alpha_\ell \ell)^* = \sum_{\ell \in L} \alpha_\ell \ell^*.$$

Since $L = G \cup Gu$, any element in RL can be written in the form $x + yu$, where x and y are elements of the group ring RG. When elements of RL are expressed in this way, the involution on RL takes the form

$$(x + yu)^* = x^* + syu$$

since gu noncentral means $(gu)^* = sgu$.

Now the conjugacy class of an element $g \in G$ is $\{g\}$ or $\{g, sg\}$ according as g is central or not and since the finite class sums span the centre of RG (as we noted in Section 1.4), it follows that both $g + g^*$ and $g + sg$ are in $\mathcal{Z}(RG)$ for any $g \in G$; hence

$$\alpha + \alpha^* \text{ and } (1 + s)\alpha \in \mathcal{Z}(RG) \quad \text{for any } \alpha \in RG.$$

Furthermore, it can be readily verified that

$$\alpha \in \mathcal{Z}(RG) \text{ if and only if } \alpha^* = \alpha$$

and

$$\alpha \in RG \text{ and } s\alpha = \alpha \text{ implies } \alpha \in \mathcal{Z}(RG).$$

Writing elements of RL as elements of $RG + RGu$, multiplication in RL becomes reminiscent of multiplication in a Cayley-Dickson algebra:

$$(x + yu)(z + wu) = (xz + g_0 w^* y) + (wx + yz^*)u, \qquad \text{where } x, y, z, w \in RG.$$

It is straightforward now to determine the nucleus and centre of RL.

1.6.1 Proposition. [GP87] *Let $\mathcal{N}(RL)$ and $\mathcal{Z}(RL)$ denote, respectively, the nucleus and centre of the alternative loop ring RL. Then*

$$\begin{aligned} \mathcal{N}(RL) = \mathcal{Z}(RL) &= \{x + yu \mid x, y \in \mathcal{Z}(RG),\ sy = y\} \\ &= \{x + yu \mid x \in \mathcal{Z}(RG) \text{ and } sy = y\}. \end{aligned}$$

1.6.2 Corollary. *$\mathcal{Z}(RL)$ is spanned by the centre of L and the elements of RL of the form $\ell + s\ell$, $\ell \in L$.*

1.6.3 Corollary. *$r \in \mathcal{Z}(RL)$ if and only if $r^* = r$. In particular, for any $r \in RL$, $r + r^*$ and rr^* are central elements of RL.*

2. The Isomorphism Problem

2.1. **Background.** A classical question in group rings is the so-called *isomorphism problem*, whose analogue in the case of alternative loop rings can be stated as follows: *given a ring R, when does the loop ring RL determine L; i.e., if L_1 is another loop, when does the isomorphism $RL \cong RL_1$ imply that $L \cong L_1$?*

In the case of group rings, it is very well known that the most significant context in which to study this question is that of integral group rings, the main reason being that this is the strongest hypothesis possible: if two groups G and H are such that $\mathbb{Z}G \cong \mathbb{Z}H$ then it is rather easy to see that also $RG \cong RH$ for every ring with unity R. Moreover, it is also true that if G and H are finite, this hypothesis implies that G and H have the same table of characters.

The first result in that context was due to G. Higman [Hig40] who proved that if G is a finite abelian group and H is another group such that $\mathbb{Z}G \cong \mathbb{Z}H$ then $G \cong H$. Next came a result of A. Whitcomb [Whi68] proving that also finite metabelian groups are determined by their integral group rings. An interesting result of R. Sandling [San74] shows that finite groups G which can be obtained as the group of units of a ring (such as the linear groups $GL(n, F)$, F a finite field) are also among the solutions of the integral group ring problem and, since it is known that finite permutation groups are determined by their character tables, it follows that S_n is also determined by its integral group ring. The next progress in this direction was due to K. W. Roggenkamp and L. Scott [RS87] who proved that this problem has a positive answer for finite nilpotent groups.

The isomorphism problem over fields was first considered by S. Perlis and G. L. Walker [PW50], who proved that if G is finite abelian and $\mathbb{Q}G \cong \mathbb{Q}H$ for another group H, then $G \cong H$. A similar result was obtained by W. Deskins

[Des56], who proved that if G is a finite abelian p-group, F a field of characteristic $p > 0$ and H another group such that $FG \cong FH$, then $G \cong H$. In this direction, however, there soon came a very striking counterexample due to E. Dade [Dad71] who exhibited two metacyclic groups G, H, which are not isomorphic, but are such that $FG \cong FH$ for all fields F.

Finally, we should mention that it has been a long standing conjecture in the area that if G and H are p-groups and F_p is the field with p elements, then $F_pG \cong F_pH$ implies $G \cong H$ (see, for example [ZM75]). Recently, R. Sandling [San89] has shown that this is the case when G is a central-elementary-by-abelian p-group.

For a detailed account of results regarding this problem, as well as for its history, the reader is referred to the survey of R. Sandling [San85].

2.2. **Loop Rings over the Integers.** Now let us return to the study of RA loops. The first result in this direction is due to E. G. Goodaire and C. Polcino Milies [GM88] who proved that the answer is always affirmative, in the case of integral loop rings of finite RA loops.

2.2.1 Theorem. *Let L_1 and L be finite RA loops such that $\mathbb{Z}L_1 \cong \mathbb{Z}L$. Then $L_1 \cong L$.*

The proof somehow follows the lines of the one given by Whitcomb for group rings, though the actual arguments are quite different and rely heavily on properties that are peculiar to RA loops. First we extend some familiar concepts from the theory of group rings to loop rings and introduce some notation.

If N is a normal subloop of a loop L and R is a commutative and associative ring with unity, there is a natural homomorphism $\omega: RL \to R[L/N]$ whose kernel, which is denoted $\Delta(L, N)$, is the ideal of RL spanned by the elements $n-1$, $n \in N$. In the case that L is an RA loop, $\Delta(L, N)$ is the set of all finite sums of elements of the form $(x + yu)(n-1) = x(n-1) + y(n-1)^*u$, $x, y \in RG$. Therefore, for $\alpha, \beta \in RG$,

$$\alpha + \beta u \in \Delta(L, N) \text{ if and only if } \alpha, \beta \in \Delta(G, N).$$

In the special case that $N = \{1\}$, we write $\Delta(L)$ instead of $\Delta(L, L)$ and call this the *augmentation ideal* of L. Note that $\Delta(L)$ is just the kernel of the map (called the *augmentation map*)

$$\epsilon: L \to L \text{ defined by } \epsilon(\sum \alpha_g g) = \sum \alpha_g.$$

The *augmentation* of an element $\alpha = \sum \alpha_g g \in RL$ is just $\epsilon(\alpha)$. An isomorphism $\theta: RL_1 \to RL$ is called *normalized* if it preserves augmentations; equivalently, if $\varepsilon \circ \theta(g) = 1$ for all $g \in L$. We now specialize to the case that R is the ring $\mathbb{Z}$ of rational integers.

If $\phi: \mathbb{Z}L_1 \to \mathbb{Z}L$ is an isomorphism, then $\varepsilon \circ \phi(g) \in \mathbb{Z}$ is invertible and so $\varepsilon \circ \phi(g) = \pm 1$ for every $g \in L$. It is easy to see that $\theta: \mathbb{Z}L_1 \to \mathbb{Z}L$ defined by $\theta(g) = (\varepsilon \circ \phi(g))^{-1}\phi(g)$, $g \in L_1$, is normalized. For this reason, when considering

the isomorphism theorem, there is no loss of generality in making the assumption that isomorphisms are normalized.

The key step in the proof of the theorem is the following. Let $\theta: \mathbb{Z}L_1 \to \mathbb{Z}L$ be a normalized isomorphism; then, for every element $g \in L_1$ we have that $\theta(g)$ is a torsion unit of augmentation 1 in $\mathbb{Z}L$ and its image, $\overline{\theta(g)} \in \mathbb{Z}[L/L']$, is also torsion, of augmentation 1. Since L/L' is an abelian group, it follows from a well-known result of G. Higman and also of S. D. Berman (see [Seh93, Corollary I.1.6]) that $\overline{\theta(g)}$ is trivial; i.e., that $\overline{\theta(g)} \in L/L'$. Recalling that $L = G \cup Gu$, we have that either $\overline{\theta(g)} = \overline{h}$ or $\overline{\theta(g)} = \overline{h}\overline{u}$ for some $h \in G$.

A lemma due to A. Whitcomb states that if N is a normal subgroup of a group G, and if $x \in \mathbb{Z}G$ and $g \in G$ are such that $x \equiv g \pmod{\Delta(G, N)}$, then there exists an element $g_1 \in G$ such that $x \equiv g_1 \pmod{\Delta(G)\Delta(N)}$. Also, it is known that $G \cap (1 + \Delta(G)\Delta(N)) = 1$. (See, for example, [Kar79] for proofs of these results.)

Taking $N = G'$, in the present case we see that $x \equiv g_1 \pmod{\Delta(G)\Delta(G')}$, for a unique $g_1 \in G$. The case $\overline{\theta(g)} = \overline{h}\overline{u}$ is similar. Hence, we have two possibilities for $\theta(g) = x + yu$:

$$\text{(i)} \qquad x \equiv g_1 \pmod{\Delta(G)\Delta(G')} \quad \text{and} \quad y \equiv 0 \pmod{\Delta(G : G')}$$

$$\text{(ii)} \qquad x \equiv 0 \pmod{\Delta(G, G')} \quad \text{and} \quad y \equiv g_1 \pmod{\Delta(G)\Delta(G')}$$

Then it is possible to prove that the map $\rho: L_1 \to L$ given by:

$$\rho(g) = \begin{cases} g_0 & \text{in case (i)} \\ g_0 u & \text{in case (ii)} \end{cases}$$

is the desired isomorphism.

There is another question naturally related to the isomorphism problem over the integers which we discuss first in the context of groups; that of fully describing all the automorphisms of the integral group ring $\mathbb{Z}G$. Notice that any automorphism $\sigma: g \mapsto g^\sigma$ of G, can be extended linearly to an automorphism $\overline{\sigma}: \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^\sigma$ of $\mathbb{Z}G$. Also, if $\gamma \in \mathbb{Q}G$ is an invertible element in the rational group algebra such that $\gamma^{-1} g \gamma \in \mathbb{Z}G$ for all $g \in G$, then the map $\phi_\gamma: \mathbb{Z}G \to \mathbb{Z}G$ given by $\phi_\gamma(g) = \gamma^{-1} g \gamma$ is again an automorphism of $\mathbb{Z}G$. It has been conjectured that all automorphisms of $\mathbb{Z}G$ are compositions of automorphisms of these two types; more precisely, we have the following

2.2.2 Conjecture (Aut). Let θ be a normalized automorphism of $\mathbb{Z}G$. Then there exists a unit $\gamma \in \mathbb{Q}G$ and an automorphism σ of G such that $\theta(g) = \gamma^{-1} g^\sigma \gamma$ for all $g \in G$; i.e., such that $\theta = \phi_\gamma \circ \overline{\sigma}$.

It has been shown by S. K. Sehgal that this is the case if G is a finite nilpotent class two group [Seh69]. G. Peterson confirmed the conjecture for finite symmetric groups S_n [Pet76] and also extended these results to some classes of metacyclic

groups [Pet77]. The conjecture has also been verified by A. Giambruno, S. K. Sehgal and A. Valenti [GSV91] for $A \wr S_n$, where A denotes a finite abelian group and $\wr$ the wreath product and for $P \wr S_n$ where P denotes a finite p-group by A. Giambruno and S. K. Sehgal [GS92] in the case where p is odd and by M. M. Parmenter and S. K. Sehgal when $p = 2$. The problem remains open, for the class of alternating groups A_n, for instance, though a result of A. Giambruno [Gia] shows that it holds if $n < 8$, a fact consistent with the case of $n = 5$ which had been settled earlier by I. S. Luthar and I. B. S. Passi [LP89].

The conjecture is true in the case of RA loops, but some care should be taken. We recall the definition of *inner automorphism* in the alternative case. Given an alternative algebra A and an element $x \in A$, we define the translation maps $R_x\colon A \to A$ and $L_x : A \to A$ just as in (1.3.1). An *inner automorphism* of A is any automorphism in the group generated by the set $\{R_a, L_a \mid a \text{ is a unit in } A\}$. It can be shown that if A is associative, then this concept of inner automorphism coincides with the usual one. With this definition in mind, we can state:

2.2.3 Theorem. *Let L be a torsion RA loop and θ a normalized automorphism of $\mathbb{Z}L$. Then there exists an inner automorphism ϕ of the rational loop algebra $\mathbb{Q}L$ and an automorphism σ of L such that $\theta = \phi \circ \overline{\sigma}$.*

2.3. **Loop Algebras over Fields.** It is natural now to turn to loop algebras over a field as the context within which to investigate isomorphism questions. In this regard, a first step was achieved by G. Leal and C. Polcino Milies [LM93] who found a natural decomposition of the rational loop algebra of an RA loop L. Writing $L = M(G, *, g_0)$ as before, and letting s denote the unique nonidentity commutator of L, we can state the following.

2.3.1 Lemma. *Let L be a finite RA loop. Then:*

$$\mathbb{Q}L = \mathbb{Q}L\left(\frac{1+s}{2}\right) \oplus \mathbb{Q}L\left(\frac{1-s}{2}\right).$$

where $\mathbb{Q}L(\frac{1+s}{2}) \cong \mathbb{Q}[L/L']$ and $\mathbb{Q}L(\frac{1-s}{2}) \cong \Delta(L, L')$. Moreover, the centre of $\Delta(L, L')$ is $\mathcal{Z}(\Delta(L, L')) = \mathbb{Q}[\mathcal{Z}(G)]\,(\frac{1-s}{2})$.

With this result, one can obtain necessary and sufficient conditions for the existence of an isomorphism of rational loop algebras, with one restrictive hypothesis on the loop.

2.3.2 Theorem. *Let L be an RA loop and G a group, such that $L = M(G, *, g_0)$. Furthermore, assume that there exists an element $\alpha \in \mathcal{Z}(L)$ such that $\alpha^2 = s$. Let M be another loop. Then $\mathbb{Q}L \cong \mathbb{Q}M$ if and only if $L/L' \cong M/M'$ and $\mathcal{Z}(\mathbb{Q}L) \cong \mathcal{Z}(\mathbb{Q}M)$.*

The techniques involved in the proof of the above theorem also allow us to prove that $\mathcal{Z}(\mathbb{Q}L) \cong \mathbb{Q}[L/L'] \oplus \mathcal{Z}(\Delta(G, G'))$ and, as a consequence, it is easy to show that if $L = M(G, *, g_0)$ is an RA loop that contains an element $\alpha \in \mathcal{Z}(L)$ such that

$\alpha^2 = s$, then the loop algebra $\mathbb{Q}L$ is determined by L/L' and the group algebra of the group G.

The next advance was given L. G. X. de Barros [dB93a] who called the RA loops considered in the theorem above loops *of type* **I** and defined loops *of type* **II** as those RA loops which do not contain an element $\alpha \in \mathcal{Z}(L)$ such that $\alpha^2 = s$. By Theorem 1.4.5, writing $L = M(G, ^*, g_0)$ and setting $G = D \times A$ with A an abelian group and D an indecomposable 2-group, we have that L is an RA loop of type **II** if and only if $\mathcal{Z}(D)$ is of the form $\mathcal{Z}(D) = C_2 \times C_{2^{m_2}} \times C_{2^{m_3}}$, where the first cyclic direct factor is $C_2 = \{1, s\}$.

De Barros's approach is as follows. First, he shows that the isomorphism problem for rational loop algebras of RA loops of type **II** can be reduced to the study of 2-loops of this type, by proving the following.

2.3.3 Proposition. *Let $L = L_1 \times H$ and $M = M_1 \times K$ be RA loops where L_1 and M_1 are RA 2-loops and H and K are abelian groups of odd order. Then $\mathbb{Q}L \cong \mathbb{Q}M$ if and only if $H \cong K$ and $\mathbb{Q}L_1 \cong \mathbb{Q}M_1$.*

Next, if L and M are RA 2-loops, we can write $L = L_1 \times H$, $M = M_1 \times K$, where L_1 and M_1 are indecomposable RA loops and H and K are 2-groups. Then, one has the following.

2.3.4 Lemma. *Let L and M be RA 2-loops of type* **II** *such that $\mathbb{Q}L \cong \mathbb{Q}M$. With L_1, M_1, H and K as above, if $H \cong K$, then $L_1 \cong M_1$.*

Finally, the main result in this context is as follows.

2.3.5 Theorem. *Let L and M be RA loops of type* **II**. *Then $\mathbb{Q}L \cong \mathbb{Q}M$ if and only if $L \cong M$.*

Similar results, for semisimple alternative loop algebras were also obtained by L. G. X. de Barros in [dB93b]. First, he obtained the following descriptions of such algebras.

2.3.6 Theorem. *Let $L = M(G, *, g_0)$ be an RA loop and let K be a field such that* $\operatorname{char} K \nmid |L|$. *Writing $\widehat{G'} = \frac{1+s}{2}$, we have:*

(i) $KG = K[G/G'] \oplus \Delta(G, G')$, *and* $KL = K[L/L'] \oplus \Delta(L, L')$;
(ii) $K[G/G'] \cong KG \cdot \widehat{G'}$ *and* $\Delta(G, G') \cong KG \cdot (1 - \widehat{G'})$;
(iii) $K[L/L'] \cong KL \cdot \widehat{G'}$ *and* $\Delta(L, L') \cong KL \cdot (1 - \widehat{G'})$.

2.3.7 Theorem. *Let L and M be RA loops. Let K be a field such that* $\operatorname{char} K \nmid |L|$. *Then $KL \cong KM$ if and only if $K[L/L'] \cong K[M/M']$ and $\Delta(L, L') \cong \Delta(M, M')$.*

2.3.8 Theorem. *Let $L = M(G, *, g_0)$ be an RA loop and let K be a field such that* $\operatorname{char} K \nmid |L|$. *Then*

(i) $\mathcal{Z}(\Delta(G, G')) \cong \mathcal{Z}(\Delta(L, L')) \cong K[\mathcal{Z}(L)] \cdot (1 - \widehat{G'}) \cong \bigoplus_{i=1}^{m} K_i$, *where each field K_i is an extension of K by a primitive n^{th} root of unity;*
(ii) $\Delta(G, G') \cong \bigoplus_{i=1}^{m} \mathcal{B}_i$, *where each $\mathcal{B}_i$ is an algebra of generalized quaternions over the field K_i;*

(iii) $\Delta(L, L') \cong \bigoplus_{i=1}^{m} \mathcal{A}_i$, *where each* $\mathcal{A}_i$ *is a Cayley-Dickson algebra over the field* K_i.

He then studies in the nonassociative setting a certain notion of field *equivalence* which we now describe.

Let $\mathcal{L}$ be a class of finite RA loops. Let F and K be fields of characteristic not 2. (This restriction will be placed on all fields considered here.). Call the fields F and K *equivalent on* $\mathcal{L}$ if for all $L, M \in \mathcal{L}$, it is the case that $FL \cong FM$ if and only if $KL \cong KM$.

In [ST76], E.Spiegel and A.Trojan studied this equivalence relation on the class of all finite 2-groups and for fields whose characteristic is not 2. The following definitions and results are due to them.

Let K be a field and let ξ_{2^n} denote a primitive 2^n-th root of unity. Define $\gamma_K(n) = [K(\xi_{2^{n+2}}) : K(\xi_{2^{n+1}})]$ and call $\{\gamma_K(n)\}_{n=1,2,\ldots}$ the 2-*sequence* of K. This sequence has one of the following forms:

$$1, 1, 1, \ldots$$
$$1, 1, 1, \ldots, 1, 2, 2, \ldots$$
$$2, 2, 2, \ldots$$

Define:

$$\mathrm{ind}_2(K) = \begin{cases} 1 & \text{if } \gamma_K(1) = 2 \\ n & \text{if } \gamma_K(n) = 2 \text{ and } \gamma_K(n-1) = 1 \text{ for } n \geq 2 \\ \infty & \text{if } \gamma_K(n) = 1 \text{ for } n = 1, 2, 3, \ldots \end{cases}$$

$$O(K) = \begin{cases} 1 & \text{if } X^2 + 1 = 0 \text{ is solvable in } K \\ 0 & \text{if } X^2 + 1 = 0 \text{ is not solvable in } K \end{cases}$$

$$t(K) = \begin{cases} 1 & \text{if } X^2 + Y^2 = -1 \text{ is solvable in } K \\ 0 & \text{if } X^2 + Y^2 = -1 \text{ is not solvable in } K \end{cases}$$

They call $\mathrm{ind}_2(K)$, $O(K)$ and $t(K)$ the 2-*invariants* of K and, for finite groups, obtained the following two results:

2.3.9 Proposition. [Spi75] *The fields* K *and* F *are equivalent on the class of all finite abelian 2-groups if and only if* $O(K) = O(F)$ *and* $\mathrm{ind}_2(K) = \mathrm{ind}_2(F)$.

2.3.10 Proposition. [ST76] *The fields* K *and* F *are equivalent on the class of all finite 2-groups if and only if* $t(K) = t(F)$, $O(K) = O(F)$ *and* $\mathrm{ind}_2(K) = \mathrm{ind}_2(F)$.

To study the equivalence problem in the case of RA loops, it is necessary to introduce another invariant for a field K, defined in [dB93b] as:

$$c(K) = \begin{cases} 1 & \text{if } X^2 + Y^2 + Z^2 + W^2 = -1 \text{ is solvable in } K \\ 0 & \text{if } X^2 + Y^2 + Z^2 + W^2 = -1 \text{ is not solvable in } K \end{cases}$$

With this notation, it is possible to solve the equivalence problem on the class of RA 2-loops.

2.3.11 Theorem. *Let F and K be fields (with characteristics different from 2). Let $\mathcal{L}$ be the class of all RA 2-loops. Then F is equivalent to K on $\mathcal{L}$ if and only if the following conditions hold:*

(a) $O(F) = O(K)$;
(b) $\text{ind}_2(F) = \text{ind}_2(K)$;
(c) $c(F) = c(K)$.

Finally, let us consider the modular case which was studied by L. G. X. de Barros and C. Polcino Milies in [dBM]. The following lemma is frequently used in the proofs of results relating to this case, though it actually holds for arbitrary fields. We include its proof, since it is quite simple.

2.3.12 Lemma. *Let L and L_1 be RA loops and let F be any field such that $FL \cong FL_1$. Then $F[L/L'] \cong F[L_1/L_1']$.*

Proof. We shall denote by $\pi: L \to L/L'$, the natural epimorphism and we consider its linear extension $\overline{\pi}: FL \to F[L/L']$. Set $\Delta(L, L') = \ker(\overline{\pi}) = FL(1-s)$.

Denote by $[FL, FL]$ the left ideal of FL generated by all the elements of the form $\alpha\beta - \beta\alpha$ with $\alpha, \beta \in FL$. We claim that $[FL, FL] = \Delta(L, L')$. In fact, given two elements $\ell, m \in L$, if they do not commute, we have $\ell m - m\ell = \ell m(1-s)$ so, in any case, $\ell m - m\ell \in FL(1-s)$ and we see that $[FL, FL] \subseteq FL(1-s)$. On the other hand, if we choose any two elements $\ell, m \in L$ which do not commute, we have $1 - s = 1 - (\ell, m) = m^{-1}\ell^{-1}(\ell m - m\ell) \in [FL, FL]$ and thus the opposite inclusion also follows.

Now, given an isomorphism $\phi: FL \to FL_1$ we have $\phi(\Delta(L, L')) = \phi([FL, FL]) = [FL_1, FL_1] = \Delta(L_1, L_1')$; consequently ϕ induces an isomorphism $\overline{\phi}$ of the corresponding factor rings and we have

$$F[L/L'] \cong \frac{FL}{\Delta(L, L')} \overset{\overline{\phi}}{\cong} \frac{FL_1}{\Delta(L_1, L_1')} \cong F[L_1/L_1']. \quad \square$$

2.3.13 Theorem. *Let L_1, L_2 be finite RA loops and F a field whose characteristic does not*

divide the order of either of these loops. Write $L_i = M_i \times A_i$, where M_i is an RA 2-loop and A_i an abelian group of odd order, $i = 1, 2$. Then, $FL_1 \cong FL_2$ if and only if $FM_1 \cong FM_2$ and $FA_1 \cong FA_2$.

Let F denote a field of characteristic p. The cases where p is odd will certainly be different—and simpler—than the case $p = 2$ since, given an RA loop L, we can write $L = L_0 \times A$ where L_0 is an indecomposable RA loop (and hence, by Theorem 1.5.10, a 2-loop) and A is an abelian group. If p is odd and divides $|L|$, then p is only involved in A while if $p = 2$ then it is certainly involved in L_0.

So we start working over fields of characteristic $p \neq 2$. In this case it is possible to give a complete answer to the isomorphism problem. Using the structure theorem for finite abelian groups we can always write L as $L = M \times A_p \times A_{p'}$ where

M is a 2-loop (obtained as the direct product of the indecomposable RA loop L_0 and the 2-primary component of A), A_p is an abelian p-group and $A_{p'}$ an abelian group whose order is odd and not divisible by p. Then, we can state the following.

2.3.14 Theorem. *Let F be a field of characteristic $p \neq 2$ and let $L_1 = M_1 \times A_p \times A_{p'}$ and $L_2 = M_2 \times B_p \times B_{p'}$ be two RA loops written as above. Then, if $FL_1 \cong FL_2$, we have*

$$\begin{aligned} FM_1 &\cong FM_2 \\ FA_{p'} &\cong FB_{p'} \\ A_p &\cong B_p. \end{aligned}$$

Notice that Theorem 2.3.14 actually permits a full study of the isomorphism problem in the present case since the isomorphism of semisimple loop algebras was studied in [dB93b] and the isomorphism of semisimple abelian group algebras was discussed by E. Spiegel in [Spi75].

The case where $\operatorname{char} F = 2$ needs a description of the loop of units of the loop ring, which is used to construct a reduction.

2.3.15 Proposition. *Assume that $L = M \times A$, where M is an RA 2-loop and A is an abelian group of odd order. Then $1 + \Delta(L, M)$ is a normal subloop of $\mathcal{U}(FL)$ with an exponent which is a power of 2, and we have*

$$\mathcal{U}(FL) = (1 + \Delta(L, M)) \times \mathcal{U}(FA).$$

Now one can give a splitting of the isomorphism under consideration.

2.3.16 Theorem. *Let L_1 and L_2 be RA loops and F a field with $\operatorname{char} F = 2$ such that $FL_1 \cong FL_2$. Write $L_i = M_i \times A_i$, where M_i is a 2-loop and A_i is an abelian group of odd order, $i = 1, 2$. Then $FM_1 \cong FM_2$ and $FA_1 \cong FA_2$.*

Proof. First we recall from Proposition 2.3.12 that $FL_1 \cong FL_2$ implies that $F[L_1/L_1'] \cong F[L_2/L_2']$; i.e. $F[M_1/M_1' \times A_1] \cong F[M_2/M_2' \times A_2]$. Once again, this is an isomorphism of abelian group algebras and thus, in particular, $FA_1 \cong FA_2$ [Des56, Theorem 3].

Now let $t \geq 1$ be an integer such that $\gamma^{2^t} = 1$ for all $\gamma \in 1 + \Delta(L_2, M_2)$. Then it is easily seen that, for all $\alpha \in \mathcal{U}(FL_2)$, we have $\alpha^{2^t} \in \mathcal{U}(FA_2)$. Letting $\theta\colon A_1 \to A_1$ be the mapping given by $\theta(a) = a^{2^t}$, it follows that θ is one-to-one (since $|A_1|$ is odd) and hence also onto. Thus, given $a \in A_1$, there exists $b \in A_1$ such that $b^{2^t} = a$. If we denote by $\phi\colon FL_1 \to FL_2$ the given isomorphism, then, since we are assuming that ϕ is normalized, we have

$$\phi(a) = \phi(b^{2^t}) = \phi(b)^{2^t} \in \mathcal{U}(FA_2).$$

Thus

$$\phi(a - 1) = \phi(b)^{2^t} - 1 \in \Delta(L_2, A_2).$$

This shows that $\phi(\Delta(L_1, A_1)) = \Delta(L_2, A_2)$; hence ϕ induces an isomorphism $\overline{\phi}$ on the corresponding quotients. We obtain

$$FM_1 \cong \frac{FL_1}{\Delta(L_1, A_1)} \overset{\overline{\phi}}{\cong} \frac{FL_2}{\Delta(L_2, A_2)} \cong FM_2. \quad \square$$

Once again, the isomorphism $FA_1 \cong FA_2$ obtained above has been studied by E. Spiegel in [Spi75], so it remains only to consider isomorphisms of modular loop algebras of RA 2-loops. At least in the case of algebras over the field of two elements, this problem has been settled.

2.3.17 Theorem. *Let F be the field with two elements and let L_1, L_2 be RA 2-loops such that $FL_1 \cong FL_2$. Then $L_1 \cong L_2$.*

3. Trivial Units

The determination of the group of units in a group ring is a subject of continuing interest to many people. In any integral group ring $\mathbb{Z}G$, the elements of $\pm G$, which are so obviously invertible, are called *trivial* units. Several of the early results about units in group rings give conditions under which certain types of units are trivial. For example, when G is abelian, it is known that all the units of finite order in $\mathbb{Z}G$ are trivial. In 1940, Graham Higman [Hig40] found necessary and sufficient conditions for all the units in an integral group ring of a torsion group to be trivial and later, S. D. Berman [Ber55] proved a similar theorem for finite groups for the units of finite order. In 1965, J. A. Cohn and D. Livingstone [CL65] proved that all the central units of finite order in an integral group ring are trivial. In 1978, M. M. Parmenter and C. Polcino Milies showed that for a finite group G, the condition that $\mathbb{Z}G$ have only trivial torsion units is equivalent to several others, the most fundamental being that the torsion units of $\mathbb{Z}G$ should form a subgroup of the full unit group [PM78]. This theorem was later extended by Polcino Milies to arbitrary groups [Mil81]. Our goal in this section is to show how to generalize all these results to ring alternative loops. What we present here is based heavily on two papers [GP86, GMa].

3.1. Units of Finite Order.

An element of finite order in a loop is often termed a *torsion* element.

3.1.1 Proposition. [GM89] *Let $r = \sum_{\ell \in L} \alpha_\ell \ell$ be a torsion unit in the integral loop ring of an RA loop L. If $\alpha_1 \neq 0$, then $r = \alpha_1 = \pm 1$.*

Proof. For a given element $x = \sum \alpha_\ell \ell \in \mathbb{Z}(L)$, the right translation map $R_x : \mathbb{Z}L \to \mathbb{Z}L$ is linear and satisfies $R_{x^m} = R_x^m$ by Artin's Theorem (Section 1.2). The matrix for R_x is similar over $\mathbb{C}$ to a diagonal matrix $A = \mathrm{diag}(\xi_1, \ldots, \xi_n)$, where the ξ_i are mth roots of unity for some m. Thus the trace of R_x is, on the one hand $\sum_{i=1}^n \xi_i$, while, on the other, it is $\sum \alpha_\ell \,\mathrm{tr}(R_\ell) = n\alpha_1$. Thus all the ξ_i are equal (in fact, equal to α_1) and $\alpha_\ell = 0$ if $\ell \neq 1$. $\square$

3.1.2 Corollary. *If $r = \sum \alpha_\ell \ell \in L$ is a torsion unit in $\mathbb{Z}L$ and $\alpha_\ell \neq 0$ for some $\ell \in \mathcal{Z} = \mathcal{Z}(L)$, then $r = \pm\ell$.*

Proof. The element $\ell^{-1}r$ is a torsion unit with nonzero coefficient of 1. □

Suppose now that $L = M(G, *, g_0)$ is an RA loop for some nonabelian group G with central element g_0, where $*: G \to G$, defined by (1.5.8), is an involution. If $x + yu$, $x, y \in \mathbb{Z}G$, is a unit in the alternative ring $\mathbb{Z}L$, then for some $z + wu \in \mathbb{Z}L$,

$$(x + yu)(z + wu) = (z + wu)(x + uy) = 1.$$

Therefore, $xz + g_0 w^* y = zw + g_0 y^* w = 1$ and $wx + yz^* = yz + wx^* = 0$. So $x^* - yu$ is invertible too, since

$$\begin{aligned}(x^* - yu)(z^* - wu) &= (x^* z^* + g_0 w^* y) + (-wx^* - yz)u \\ &= (zx + g_0 y^* w)^* = 1\end{aligned}$$

and, similarly, $(z^* - wu)(x^* - yu) = 1$. It follows that the product $(x + yu)(x^* - yu) = xx^* - g_0 yy^*$ is also invertible. On the other hand, if x and y in $\mathbb{Z}L$ are such that $xx^* - g_0 yy^*$ is invertible (with inverse a, say), then $x + yu$ is invertible, with inverse $ax^* - ayu$. Furthermore, the map $\theta: \mathbb{Z}L \to \mathbb{Z}L$ defined by $(x + yu)\theta = x^* - yu$ is easily seen to be an involution on $\mathbb{Z}L$. Since $r \in \mathbb{Z}L$ and $r\theta$ commute, if r has finite order, so does $r(r\theta) = xx^* - g_0 yy^*$. It is now clear that

3.1.3 Proposition. *An element $x + yu$ is a unit in $\mathbb{Z}L$ if and only if $xx^* - g_0 yy^*$ is a central unit in $\mathbb{Z}G$. If $x + yu$ has finite order, so does $xx^* - g_0 yy^*$.*

Let $\ell \mapsto \overline{\ell}$ denote the natural homomorphism $L \to L/L'$, where $L' = \{1, s\}$ denotes the commutator (and associator) subloop of L. This map extends to a ring homomorphism $\mathbb{Z}L \to \mathbb{Z}[L/L']$ (we use $\overline{r}$ to denote the image of r) with kernel the ideal $\Delta(L, L')$ of $\mathbb{Z}L$ generated by $1 - s$. Thus, if $r = x + yu \in \mathbb{Z}L$ and $\overline{r} = \overline{0}$, then $(1 + s)r = 0$, so $(1 + s)x = (1 + s)y = 0$; i.e., $x, y \in (1 - s)\mathbb{Z}G$. Suppose that $\overline{r}$ is a trivial unit in the group ring $\mathbb{Z}[L/L']$; i.e., $\overline{r} = \pm\overline{g}$ or $\pm\overline{gu}$ for some $g \in G$. In the first case, $(\overline{x} \mp \overline{g}) + \overline{yu} = \overline{0}$ implies that both $x \mp g$ and y are in $(1 - s)\mathbb{Z}G$, while, in the second case, both x and $y \mp g$ are in $(1 - s)\mathbb{Z}G$. All this shows

3.1.4 Proposition. *Let $L = M(G, *, g_0)$ be an RA loop. Suppose $r = x + yu$, $x, y \in \mathbb{Z}G$, is a unit in $\mathbb{Z}L$ such that $\overline{r}$ is a trivial unit in the group ring $\mathbb{Z}[L/L']$. Then either*

$$x = \pm g + (1 - s)x_1, \quad y = (1 - s)y_1 \tag{1}$$

for certain elements x_1 and y_1 in the group ring $\mathbb{Z}G$ or

$$x = (1 - s)x_1, \quad y = \pm g + (1 - s)y_1 \tag{2}$$

for some $x_1, y_1 \in \mathbb{Z}G$.

3.1.5 Corollary. *Suppose r is a central unit in an alternative loop ring $\mathbb{Z}L$ such that $\overline{r}$ is trivial. Then r is in the group ring $\mathbb{Z}G$.*

If r is a central unit of finite order in an alternative loop ring, then $\overline{r}$ is a unit of finite order in an abelian group ring, so it's trivial. The corollary says that r is in the group ring. Therefore r is trivial because central units of finite order in a group ring are trivial. This establishes the result more generally for alternative loop rings.

3.1.6 Theorem. [GP86] *Central units of finite order in an alternative loop ring are trivial.*

Now the Cayley loop is an RA loop, hence so also is the direct product of the Cayley loop with an abelian group, by Corollary 1.5.2. D. A. Norton has shown that a Moufang loop is of this type if and only if all its subloops are normal [Nor52]. Such a loop is called *Hamiltonian.* Since all the units in the integral group ring of the quaternion group Q are trivial or, more generally, in the integral group ring of $Q \times E$ for any elementary abelian 2-group E [Hig40], the following theorem is not surprising.

3.1.7 Theorem. [GP86] *The units in the integral loop ring of a Hamiltonian Moufang 2-loop are trivial.*

We conclude this section by quoting the extensions to alternative loop rings of the well-known theorems of G. Higman and S. D. Berman for group rings. Proofs of both can be found in [GP86]. (A torsion (or periodic) loop is a loop all of whose elements have finite order.)

3.1.8 Theorem. *Suppose L is a torsion loop. Then $\mathbb{Z}L$ is an alternative ring in which all units are trivial if and only if L is an abelian group of exponent 2, 3, 4 or 6, or a Hamiltonian Moufang 2-loop.*

3.1.9 Theorem. *Let L be a finite loop. Then $\mathbb{Z}L$ is an alternative loop ring in which all torsion units are trivial if and only if L is an abelian group or a Hamiltonian Moufang 2-loop.*

3.2. **Central units.** In this section, we give necessary and sufficient conditions for all the central units in an alternative (but not associative) loop ring to be trivial. This is one instance where work in alternative loop rings motivated group ring research because at the time the main theorem, Theorem 3.2.2, of this section appeared, the analogous result for group rings was not known. The issue, however, has since been settled [RS90].

We begin with a lemma.

3.2.1 Lemma. *If all central units in the integral group ring $\mathbb{Z}G$ of a finite group G are trivial, then all the units in the abelian group ring $\mathbb{Z}[G/G']$ are trivial.*

Proof. As an ideal of the semisimple group algebra $\mathbb{Q}G$, the ideal $\Delta(G, G')$ is a direct summand of $\mathbb{Q}G$, thus $\mathbb{Q}(G) \cong \Delta(G, G') \oplus A$ for some ideal A. Since $A \cong \mathbb{Q}G/\Delta(G, G') \cong \mathbb{Q}[G/G']$, we have

$$\mathbb{Q}G \cong \mathbb{Q}[G/G'] \oplus \Delta(G, G').$$

Let f be a (central) idempotent of $\mathbb{Q}G$ such that $\mathbb{Q}Gf \cong \mathbb{Q}[G/G']$ (and so $\mathbb{Q}G(1-f) \cong \Delta(G,G')$). Then $\mathbb{Q}G = \mathbb{Q}Gf \oplus \mathbb{Q}G(1-f)$ and so

$$\mathbb{Z}G \subseteq R = \mathbb{Z}Gf \oplus \mathbb{Z}G(1-f) \subseteq \mathbb{Q}Gf \oplus \mathbb{Q}G(1-f) = \mathbb{Q}G.$$

This shows that, as a Z-module, R has rank $|G| = \operatorname{rank} \mathbb{Z}G$, so, by an argument of Sehgal [Seh78, pp. 49–50], the unit group of $\mathbb{Z}G$ is of finite index in the unit group of the ring R. Now let u be any unit in $\mathbb{Z}[G/G']$ and let $v \in \mathbb{Z}G$ be any preimage of u under the map $\mathbb{Q}G \to \mathbb{Q}[G/G']$. Then $vf \oplus (1-f)$ is a unit in R, so $v^t f \oplus (1-f)$ is a unit in $\mathbb{Z}G$ for some t and it's central because u is central in R ($\mathbb{Z}[G/G']$ is abelian). By hypothesis, $v^t f \oplus (1-f)$ is trivial. In particular, it has finite order, so $vf \oplus (1-f)$ is a central unit of finite order in $\mathbb{Z}G$. By the result of Cohn and Livingstone, this element is trivial, so u is trivial and the lemma is established. □

3.2.2 Theorem. *Suppose L is a torsion Moufang loop and $\mathbb{Z}L$ is an alternative loop ring which is not associative. Let A denote the centre of L. Then the central units in $B\mathbb{Z}L$ are trivial if and only if all units in $\mathbb{Z}A$ and $\mathbb{Z}[L/L']$ are trivial; i.e., if and only if both A and L/L' are abelian groups of exponents 2, 4 or 6.*

Proof. Suppose $\mathbb{Z}A$ and $\mathbb{Z}[L/L']$ have only trivial units. If r is any central unit in $\mathbb{Z}L$, then it follows by Corollary 3.1.5 that r is in the group ring $\mathbb{Z}G$. Write $r = r_1 + r_2$, where $r_1 \in \mathbb{Z}A$ and $r_2 \in \sum_{g \notin A} \alpha_g g$. Since r is central, $r = r^*$, hence $r_2 = sr_2$. On the other hand, since $\overline{r}$ is a trivial unit in $\mathbb{Z}[G/G']$, for some $g \in G$ we have $r \pm g \in (1-s)\mathbb{Z}G$ and hence $s(r \pm g) = -(r \pm g)$. Remembering that $sr_2 = r_2$, we obtain $(1+s)r_1 + 2r_2 \pm (1+s)g = 0$; whence $r_2 = 0$. Therefore $r \in \mathbb{Z}A$ and, by assumption, all units in this ring are trivial.

Conversely, if all the central units in $\mathbb{Z}L$ are trivial, then all units in $\mathbb{Z}A$ are trivial and so A has exponent 2, 3, 4 or 6. (but not 3 since $s \in A$ has order 2). By the Lemma, $\mathbb{Z}[G/G']$ has only trivial units, so G/G' has exponent 2, 3, 4 or 6 and, since $\ell^2 \in G$ for any $\ell \in L$ and $L' = G'$, L/L' has exponent 2, 3, 4, 6, 8 or 12. If we eliminate the possibilities of 8 and 12, then it will follow that the units of the abelian group ring $\mathbb{Z}[L/L']$ are trivial and the theorem will have been proven. Suppose then L/L' has exponent 8. Thus, for some $g \in L$, g^8, but no lower power, is in L'. Remember that $L' = \{1, s\}$. If $g^8 = s$, g^2 would be a central element of order 8 in a group of exponent 2, 4 or 6. This cannot be, so g has order 8 and can't be central; hence by Theorem 1.5.9, it's an element in some nonabelian group H contained within L with $\mathcal{Z}(H) = A$. Since $H' = L'$, the element $\overline{g} \in H/H'$ has order 8. But all the central units in $\mathbb{Z}H$ are trivial, so, by Lemma 3.2.1, all units in $\mathbb{Z}[H/H']$ are trivial. Thus H/H' has exponent 2, 3, 4 or 6, contradicting the fact that g has order 8. So L/L' cannot have exponent 8. Similarly, it cannot have exponent 12. □

As a corollary, it is not hard to establish the result which motivated the aforementioned theorem of J. Ritter and S. K. Sehgal [RS90].

3.2.3 Corollary. *Let L be a finite RA loop. Then all central units in $\mathbb{Z}L$ are trivial if and only if, for all $x \in L$ and for all j with $(j, |L|) = 1$, the element x^j is conjugate to x or to x^{-1}.*

3.3. **Can the torsion units form a subloop?** In this section, we summarize some quite recent work by the authors [GMb]. As we have mentioned, the early literature on group rings contains several results giving conditions under which various sorts of torsion units are trivial and hence, obviously, form a subgroup of the full unit group. It was Parmenter and Polcino Milies who realized the significance of this latter property [PM78], which motivates this section.

We begin with two lemmas, the first of which is not generally true for groups, while the second is still an open question in the case of arbitrary groups.

3.3.1 Lemma. *Let T denote the set of torsion elements of an RA loop L. Then T is a normal subloop of L. If L is finitely generated, then T is finite.*

3.3.2 Lemma. *Suppose $L = M(G, *, u)$ is an RA loop. Then the idempotents of $\mathbb{Z}L$ are trivial; i.e., equal to 0 or 1.*

Then we show that a lemma of Sehgal's [Seh78, Lemma VI.3.22] holds also in the setting of RA loops.

3.3.3 Lemma. *Let L be a finitely generated RA loop and T its normal torsion subloop. Suppose that $\mathbb{Q}T \cong D_1 \oplus \cdots \oplus D_n$ is the direct sum of division rings and that every idempotent of $\mathbb{Q}T$ is central in $\mathbb{Q}L$. Then*

(i) *Every unit $\mu \in \mathbb{Z}L$ can be written in the form $\mu = \sum d_i \ell_i$, with $d_i \in D_i$, $\ell_i \in L$, and*
(ii) $\mathcal{U}(\mathbb{Z}L) = [\mathcal{U}(\mathbb{Z}T)]L$.

Finally we put these ideas together to generalize two theorems about group rings. The first, due to M. M. Parmenter and C. Polcino Milies [PM78], applies to finite groups. The second, by C. Polcino Milies [Mil81], extends the first to arbitrary groups. Our theorem makes no assumptions about finiteness.

3.3.4 Theorem. *Let L be an RA loop and T its torsion subloop. Then the torsion units in the integral loop ring of L form a subloop of $\mathcal{U}(\mathbb{Z}L)$ if and only if T is an abelian group or a Moufang Hamiltonian 2-loop and, for every $\ell \in L$ and $t \in T$, $\ell^{-1} t \ell \in \langle t \rangle$.*

The following corollary is the nonassociative analogue of a lemma of C. Polcino Milies [Mil81].

3.3.5 Corollary. *The torsion units of an alternative loop ring form a subloop if and only if they are trivial.*

It now becomes apparent that several properties of the loop of units in $\mathbb{Z}L$, known to be equivalent for groups which are finite [PM78], are always equivalent when L is an RA loop (finite or infinite).

As with groups, a loop L is said to be an *FC loop* if the set $[a] = \{x^{-1}ax \mid x \in L\}$ is finite. Any RA loop L is an FC loop (since any element $\ell \in L$ has at most two conjugates, ℓ and $s\ell$).

A loop L is *n-Engel* if for any $x, y \in L$, the extended commutator $(\ldots((x,y),y),\ldots,y)$ (with y repeated n times) is the identity. Since commutators of an RA loop are central, an RA loop is 2-Engel (and hence n-Engel for all $n \geq 2$).

3.3.6 Theorem. [GMb] *Let L be an RA loop with torsion subloop T. Then the following are equivalent:*

(i) *$\mathcal{U}(\mathbb{Z}L)$ is an RA loop.*
(ii) *$\mathcal{U}(\mathbb{Z}L)$ is FC.*
(iii) *$\mathcal{U}(\mathbb{Z}L)$ is nilpotent.*
(iv) *$\mathcal{U}(\mathbb{Z}L)$ is nilpotent of class 2.*
(v) *$[\mathcal{U}(\mathbb{Z}L)]'$ is a torsion loop.*
(vi) *$[\mathcal{U}(\mathbb{Z}L)]'$ is a group of order 2.*
(vii) *$\mathcal{U}(\mathbb{Z}L)$ is n-Engel for some $n \geq 2$.*
(viii) *$\mathcal{U}(\mathbb{Z}L)$ is 2-Engel.*
(ix) *T is an abelian group or a Moufang Hamiltonian 2-loop and, for any $t \in T$ and any $x \in L$, we have $x^{-1}tx = t^{\pm 1}$. Moreover, if T is abelian and $x \in L$ is an element that does not centralize T, then $x^{-1}tx = t^{-1}$ for all $t \in T$.*

4. Some Conjectures of H. J. Zassenhaus

4.1. **Group Rings.** Let us return for a moment to the isomorphism problem for group rings. Let $\mathbb{Z}G$ denote the group ring of a finite group G over the ring $\mathbb{Z}$ of rational integers, let G_1 denote another group and let $\theta\colon \mathbb{Z}G_1 \to \mathbb{Z}G$ be a normalized isomorphism. Then, for every element $g \in G_1$, we have that $\theta(g)$ is a torsion unit of augmentation 1 in $\mathbb{Z}G$.

According to the well-known theorems of G. Higman and S. D. Berman discussed in Section 3, if G is either abelian or a Hamiltonian 2-group, then all normalized units of finite order are trivial; i.e., they belong to G. Hence, in this particular case, θ gives, by restriction, an isomorphism $\theta\colon G_1 \to G$ and we obtain a positive answer to the isomorphism problem.

For any other group G, all we can say is that $\theta(G_1)$ is a subgroup of normalized units of the same order as G itself. On the other hand, J.A. Cohn and D. Livingstone [CL65] have shown that any finite subgroup of normalized units in $\mathbb{Z}G$ is a set of independent elements and thus its order is less than or equal to $|G|$. (Actually, it can be shown that its order must be a divisor of $|G|$.) Moreover, they have shown that if H is such a subgroup and $|H| = |G|$, then $\mathbb{Z}G = \mathbb{Z}H$. Thus, it is only natural to be curious about normalized torsion units and, in particular, about subgroups of normalized units which have order the order of G.

There is a rather obvious way of constructing normalized torsion units. If g is an element in G and γ is a unit in the rational group algebra $\mathbb{Q}G$ such that $u = \gamma^{-1}g\gamma \in \mathbb{Z}G$, then certainly α is a normalized torsion unit in $\mathbb{Z}G$. In the mid

1960's, H. J. Zassenhaus suggested that all such units of ZG arise in precisely this way. He made the following conjecture:

4.1.1 Conjecture (ZC1). Every normalized unit of finite order $u \in \mathcal{V}(ZG)$ is rationally conjugate to an element $g \in G$; i.e., there exists a unit $g \in \mathbb{Q}G$ such that $\gamma^{-1}u\gamma \in G$.

There are two stronger versions of this conjecture dealing with subgroups of normalized units, the first being clearly related to the isomorphism problem and the second one, a generalization of the first.

4.1.2 Conjecture (ZC2). Let H be a subgroup of normalized units in ZG such that $|H| = |G|$. Then H is rationally conjugate to G.

4.1.3 Conjecture (ZC3). Let H be any finite subgroup of normalized units in ZG. Then H is rationally conjugate to a subgroup of G.

Clearly, **ZC3** implies the other two conjectures and a positive answer to **ZC2** will imply a solution of the isomorphism problem. It is also easy to verify that **ZC2** implies the conjecture **Aut** which we discussed in Section 2 and that a positive answer to both **Aut** and the isomorphism problem would imply **ZC2** (see [Seh93, p. 207]).

These conjectures have been established for various kinds of groups, although they remain open in general. All of them have long been known to be true for nilpotent class 2 groups (see S. K. Sehgal [Seh69]). The most far reaching result in this direction is a theorem due to A. Weiss [Wei91] which shows that **ZC3** holds for group rings of finite nilpotent groups.

ZC1 was proved for metacyclic groups $G = \langle a \rangle \rtimes \langle x \rangle$ such that $\gcd(\mathrm{o}(a), \mathrm{o}(x)) = 1$ by C. Polcino Milies, J. Ritter and S. K. Sehgal[4] [MRS86] and A. Valenti has shown that **(ZC3)** holds for a group of the form $G = \langle a \rangle \rtimes X$, where $\gcd(\mathrm{o}(a), |X|) = 1$ and X is abelian (see also O. S. Juriaans [Jur]). The book by S. K. Sehgal [Seh93] contains an exposition of most of the known results on this subject.

An interesting fact is that K. W. Roggenkamp and L. Scott [RSpre] found a metabelian group of order $2^6 \cdot 3 \cdot 5 \cdot 7$ which is a counterexample to **ZC2** and, afterwords, L. Klinger [Kli91] found another counterexample with a group of the same order, but using different methods.

In another direction, it should be mentioned that **ZC1** was proved for S_4 by N. A. Fernandes [Fer87], for A_4 by I. S. Luthar and I. B. S. Passi [LP89], and for S_5 by I. S. Luthar and P. Trama [LT].

4.2. **Loop Rings.** Henceforth, we shall discuss the validity of the conjectures of H.J. Zassenhaus for loop rings of finite RA loops and show that, in this context, all of them do hold. We begin considering **ZC1**.

Let x be a normalized unit of finite order in ZL. As was mentioned in the proof sketched for Theorem 2.2.1, we can find an element $g \in G$ such that either:

[4]Here, $\mathrm{o}(a)$ and $\mathrm{o}(x)$ denote the orders of a and x, respectively.

(i) $x = g + \delta_1 + \delta_2 u$, $\delta_1 \in \Delta(G)\Delta(G')$ and $\delta_2 \in \Delta(G, G')$, or
(ii) $x = (g + \delta_1)u + \delta_2$, $\delta_1 \in \Delta(G)\Delta(G')$ and $\delta_2 \in \Delta(G, G')$.

Using Corollary 3.1.2, it can be shown that the square of every torsion unit in $\mathbb{Z}L$ actually belongs to the centre of L. In fact, we can obtain more information about these squares.

4.2.1 Proposition. *Let x be a normalized unit of finite order in $\mathbb{Z}L$. Then $r^2 = g^2$ or $r^2 = (gu)^2$ according as x is of the form (i) or (ii) respectively.*

Proof. Assume that x can be written in the form $x = g + \delta_1 + \delta_2 u$ as in (i). Then, it is easy to see that r^2 can be written as

$$r^2 = g^2 + \delta_1' + \delta_2' u, \qquad \delta_1' \in \Delta(G)\Delta(G'), \quad \delta_2' \in \Delta(G, G').$$

Corollary 3.1.2 shows that $r^2 \in \mathcal{Z} \subseteq G$, so we must have that $r^2 = g^2 + \delta_1'$ and $\delta_2' u = 0$. Thus

$$g^{-2} r^2 = 1 + \delta_2'' \in G \cap (1 + \Delta(G)\Delta(G')) = 1$$

and so $r^2 = g^2$. If x is as in (ii), the argument is similar. □

Actually, solving **ZC1** now amounts to showing that if x is a normalized torsion unit such that $r^2 = g^2$ or $r^2 = (gu)^2$ as above, then x is conjugate, in $\mathbb{Q}L$, to either g or gu respectively. To do so, it is first necessary to show that the problem can be reduced to the question of conjugacy in the complex loop algebra, as was noticed in the case of group rings by C. Polcino Milies and S. K. Sehgal [MS84]. Using the same techniques as in the associative case, it is possible to establish the following.

4.2.2 Lemma. *Let $k \subseteq K$ be infinite fields. Let L be a finite loop whose loop algebra over k is semisimple and alternative. If two elements $\alpha, \beta \in kL$ are conjugate in KL, then they are also conujugate in kL.*

Before stating the theorem which gives a positive answer to **ZC1**, we should remind the reader that in our present nonassociative context, the composition of two automorphisms of the form $x \mapsto r^{-1}xr$ need not be itself of this form (though it is still inner, in the sense defined in Section 2.2); hence, one should expect that the result will look somehow more complicated in this setting. As mentioned above, we do not prove that a torsion unit x is conjugate to an element $g \in L$, but rather that both x and g have a common conjugate in $\mathbb{Q}L$. We obtain the following.

4.2.3 Theorem. [GM89, Theorem 0.1] *Let u be a normalized torsion unit in the integral loop ring $\mathbb{Z}L$ of a finite RA loop L. Then, there exist units $\gamma_1, \gamma_2 \in \mathbb{Q}L$ and $\ell \in L$ such that $\gamma_2^{-1}(\gamma_1^{-1} u \gamma_1)\gamma_2 = \ell$.*

As noted, in the case of group rings the validity of both the isomorphism conjecture and **Aut** imply that **ZC2** also holds. Since the arguments in [Seh93, p. 207] can be easily applied in the alternative case, at this point we also obtain that **ZC2** holds. However, the result will also follow as an immediate corollary from the fact that an analogue of **ZC3** holds.

The first step in the proof of our main result is to determine the structure of semisimple alternative loop algebras. Remember (Lemma 2.3.1) that if L is a finite RA loop, then

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

where

$$\mathbb{Q}L(\frac{1+s}{2}) \cong \mathbb{Q}[L/L'] \text{ and } \mathbb{Q}L(\frac{1-s}{2}) \cong \Delta(L, L'),$$

and the centre of $\Delta(L, L')$ is

$$\mathcal{Z}(\Delta(L, L')) = \mathbb{Q}(\mathcal{Z}(G))\left(\frac{1-s}{2}\right).$$

Exactly the same results hold for the loop algebra KL if we assume that K is a field whose characteristic does not divide $|L|$.

Since L/L' is an abelian group, $K[L/L']$ is a direct sum of fields. It was shown in [LM93, proof of Lemma 2.3] that $\Delta(L, L')$ contains no commutative simple components. Since, for RA loops, L' is the associator as well as the commutator subloop (Theorem 1.5.4) similar arguments show that $\Delta(L, L')$ also contains only nonassociative components.

More precisely, we can state the following.

4.2.4 Theorem. [GMa, Theorem 2.8] *The loop algebra of a finite RA loop L over a field F of characteristic relatively prime to $|L|$ is the direct sum of fields and Cayley-Dickson algebras. If $L' = \{1, s\}$ and π denotes the projection of FL onto a simple component A of FL, then A is a field if and only if $\pi(s) = 1_A$, the identity element of A, and a Cayley-Dickson algebra if and only if $\pi(s) = -1_A$.*

This gives a good characterization of the loop algebra since Cayley-Dickson algebras are well understood (see Section 1.2).

The main tool for establishing our result will be, again, the homomorphism constructed in Section 2.2.

4.2.5 Theorem. *If L is a finite RA loop and H is a finite subloop of $TU_1(\mathbb{Z}L)$, then there is a one-to-one homomorphism $\rho_H : H \to L$ such that*

(i) *$\rho_H(\alpha) = \alpha$ for all $\alpha \in H \cap L$;*
(ii) *if $\alpha \in H$, there exist units $\gamma_1, \gamma_2 \in \mathbb{Q}L$ such that $\gamma_2^{-1}(\gamma_1^{-1}\alpha\gamma_1)\gamma_2 = \rho_H(\alpha)$; and,*
(iii) *if $\alpha \in H$, then $\alpha^2 = \rho_H(\alpha)^2 \in \mathcal{Z}L$.*

Proof. Part (i) follows from the construction of ρ and part (ii) is a consequence of Theorem 4.2.3. Recalling Artin's Theorem, that the subalgebra generated by any pair of elements in an alternative ring is associative, we see that $(\gamma^{-1}\alpha\gamma)^n = \alpha^n$ for any integer n. Now part (iii) follows because squares of elements in an RA loop are central. □

Remember that the unique nonidentity commutator, s, of an RA loop L is also a unique nonidentity associator (Theorem 1.5.4). Also, by Theorem 1.5.5, for $g, h \in L$, we have $(g, h) = 1$ if and only if $(g, h, k) = 1$ for all $k \in L$. One can use Theorem 4.2.5 to show that elements in any finite subloop of normalized units behave, in the respects just mentioned, like the elements of the RA loop itself.

4.2.6 Corollary. *Let L be a finite RA loop with $L' = \{1, s\}$ and let H be a finite subloop of $T\mathcal{U}_1(\mathbb{Z}L)$, the set of normalized units of finite order. If $\alpha, \beta \in H$ and $(\alpha, \beta) \neq 1$, then $(\alpha, \beta) = s$. If $\alpha, \beta, \gamma \in H$ and $(\alpha, \beta, \gamma) \neq 1$, then $(\alpha, \beta, \gamma) = s$. Also, if H is not commutative, then $\mathcal{Z}(H) \subseteq \mathcal{Z}(L)$.*

The next step consists in showing that finite subloops of normalized units have homomorphic images in L.

4.2.7 Corollary. *Let H be a finite noncommutative subloop of $T\mathcal{U}_1(\mathbb{Z}L)$ and let $\rho_H : H \to L$ be the homomorphism described in the theorem. Then $H^* \subseteq H$ and ρ_H commutes with $*$.*

Finally, one can describe this homomorphism in a precise way to obtain an analogue to **ZC3**.

4.2.8 Theorem. [GMb, Theorem 1.2] *If H is a finite subloop of normalized units in a (nonassociative) alternative loop ring $\mathbb{Z}L$, then H is isomorphic to a subloop of L. Moreover, there exist units $\gamma_1, \gamma_2, \ldots, \gamma_k$ of $\mathbb{Q}L$ such that*

$$\gamma_k^{-1}(\ldots(\gamma_2^{-1}(\gamma_1^{-1}H\gamma_1)\gamma_2)\ldots)\gamma_k \subseteq L.$$

Let H be a finite subloop of $T\mathcal{U}_1(\mathbb{Z}L)$ and let $\rho : H \to L$ be the homomorphism of Theorem 4.2.5. Set $L_0 = \rho(H)$.

The proof follows different lines depending on the structure of H. To give a hint of the ideas involved, let us discuss here the case where H is an abelian group. Then L_0 is also an abelian group and it is contained in L. If L_0 is not central, it contains a noncentral element ℓ_0. If x is any other element in L_0, since $\ell_0 x = x\ell_0$, either x or $\ell_0 x$ is central. In the latter case, $x = x^2(\ell_0 x)^{-1}\ell_0$ is a central multiple of ℓ_0. It follows that L_0 is generated by a set S of central elements and the single element ℓ_0. Now $L_0 = \rho(H)$ and S is fixed elementwise by ρ by Theorem 4.2.5, so H is generated by S and the single element $\widehat{\ell_0} = \rho^{-1}(\ell_0)$. Moreover, there exist $\gamma_1, \gamma_2 \in \mathbb{Q}L$ such that $\gamma_2^{-1}(\gamma_1^{-1}\widehat{\ell_0}\gamma_1)\gamma_2 = \ell_0$, hence also $\gamma_2^{-1}(\gamma_1^{-1}H\gamma_1)\gamma_2 = L_0$ which gives the result.

The cases where H is either a nonabelian group or a nonassociative loop require a more involved discussion.

References

[Ber55] S. D. Berman, *On the equation $x^m = 1$ in an integral group ring*, Ukrain. Mat. Zh. **7** (1955), 253–261.

[BK51] R. H. Bruck and E. Kleinfeld, *The structure of alternative division rings*, Proc. Amer. Math. Soc. **2** (1951), 878–890.

[Bru44] R. H. Bruck, *Some results in the theory of linear nonassociative algebras*, Trans. Amer. Math. Soc. **56** (1944), 141–199.

[Bru46] R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.

[Bru58] R. H. Bruck, *A survey of binary systems*, Ergeb. Math. Grenzgeb., vol. 20, Springer-Verlag, 1958.

[Cay54] A. Cayley, *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$, Philos. Mag. and Jour. of Science **7** (1854), 40–47.

[CG86] Orin Chein and Edgar G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra **14** (1986), no. 2, 293–310.

[Che74] Orin Chein, *Moufang loops of small order I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.

[Che78] Orin Chein, *Moufang loops of small order*, Mem. Amer. Math. Soc. **197** (1978), no. 13.

[CL65] J. A. Cohn and D. Livingstone, *On the structure of group algebras*, Canad. J. Math. **17** (1965), 583–593.

[Cur63] Charles W. Curtis, *The four and eight square problem and division algebras*, Studies in modern algebra (A. A. Albert, ed.), Studies in Mathematics, vol. 2, Math. Assoc. of America, 1963, pp. 100–125.

[Dad71] E. C. Dade, *Deux groups finis distincts ayant la même algebre de group sur tout corps*, Math. Z. **119** (1971), 345–348.

[dB93a] Luiz G. X. de Barros, *Isomorphisms of rational loop algebras*, Comm. Algebra **21** (1993), no. 11, 3977–3993.

[dB93b] Luiz G. X. de Barros, *On semisimple alternative loop algebras*, Comm. Algebra **21** (1993), no. 11, 3995–4011.

[dBM] L. G. X. de Barros and C. Polcino Milies, *Modular loop algebras of RA loops*, J. Algebra, to appear.

[Des56] W. E. Deskins, *Finite abelian groups with isomorphic group algebras*, Duke Math. J. **23** (1956), 35–40.

[Fer87] N. A. Fernandes, *Torsion units in the integral group ring of* S_4, Bol. Soc. Brasil. Mat. **18** (1987), 1–10.

[Gia] A. Giambruno, *Automorphisms of* ZA_n, preprint.

[Goo83] Edgar. G. Goodaire, *Alternative Loop Rings*, Publ. Math. Debrecen **30** (1983), 31–38.

[GMa] Edgar G. Goodaire and César Polcino Milies, *Finite subloops of units in an alternative loop rings*, preprint.

[GMb] Edgar G. Goodaire and César Polcino Milies, *On the loop of units of an alternative loop ring*, Nova J. of Alg. and Geom., to appear.

[GM88] Edgar G. Goodaire and César Polcino Milies, *Isomorphisms of integral alternative loop rings*, Rend. Circ. Mat. Palermo **XXXVII** (1988), 126–135.

[GM89] Edgar G. Goodaire and César Polcino Milies, *Torsion units in alternative loop rings*, Proc. Amer. Math. Soc. **107** (1989), 7–15.

[GP86] Edgar G. Goodaire and M. M. Parmenter, *Units in alternative loop rings*, Israel J. Math. **53** (1986), no. 2, 209–216.

[GP87] Edgar G. Goodaire and M. M. Parmenter, *Semi-simplicity of alternative loop rings*, Acta Math. Hungar. **50** (1987), no. 3–4, 241–247.

[GS92] A. Giambruno and S. K. Sehgal, *Automorphisms of the integral group ring of the wreath product of a p-group with* S_n, Rocky Mountain J. Math. **22** (1992), 1303–1316.

[GSV91] A. Giambruno, S. K. Sehgal, and A. Valenti, *Automorphisms of the integral group ring of some wreath products*, Comm. Algebra **19** (1991), 519–534.

[Hal59] M. Hall, Jr., *The theory of groups*, MacMillan, New York, 1959.

[Hig40] Graham Higman, *The units of group rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.

[JLM] Eric Jespers, Guilherme Leal, and C. Polcino Milies, *Indecomposable R.A. loops*, J. Algebra, to appear.

[Jur] O. S. Juriaans, *Torsion units in integral group rings*, Comm. Algebra, to appear.

[Kar79] G. Karpilovsky, *On the isomorphism problem for integral groups rings*, J. Algebra **59** (1979), 1–4.

[Kle63] E. Kleinfeld, *A characterization of the Cayley numbers*, Studies in modern algebra (A. A. Albert, ed.), Studies in Mathematics, vol. 2, Math. Assoc. of America, 1963, pp. 126–143.

[Kli91] L. Klinger, *Construction of a counterexample to a conjecture of Zassenhaus*, Comm. Algebra **19** (1991), 2303–2330.

[LM93] Guilherme Leal and C. Polcino Milies, *Isomorphic group (and loop) algebras*, J. Algebra **155** (1993), no. 1, 195–210.

[LP89] I. S. Luthar and I. B. S. Passi, *Zassenhaus conjecture for A_5*, Proc. Indian Acad. Sci. Math. Sci. **99** (1989), 1–5.

[LT] I. S. Luthar and P. Trams, *Zassenhaus conjecture for S_5*, preprint.

[Mil81] César Polcino Milies, *Group rings whose torsion units form a subgroup*, Proc. Amer. Math. Soc. **81** (1981), no. 2, 172–174.

[Mou33] R. Moufang, *Alternativkörper und der Satz vom vollständigen Vierseit (D_9)*, Abh. Math. Sem. Univ. Hamburg **9** (1933), 207–222.

[MRS86] C. Polcino Milies, J. Ritter, and S. K. Sehgal, *On a conjecture of Zassenhaus for torsion units in integral group rings II*, Proc. Amer. Math. Soc. **97** (1986), 210–216.

[MS84] C. Polcino Milies and S. K. Sehgal, *Torsion units in integral group rings of metacyclic groups*, J. Number Theory **19** (1984), 103–114.

[Nor52] D. A. Norton, *Hamiltonian loops*, Proc. Amer. Math. Soc. **3** (1952), 56–65.

[Pai55] Lowell J. Paige, *A theorem on commutative power associative loop algebras*, Proc. Amer. Math. Soc. **6** (1955), 279–280.

[Pas77] D. S. Passman, *The algebraic structure of group rings*, Wiley-Interscience, New York, 1977.

[Pet76] G. L. Peterson, *Automorphisms of the integral group ring of S_n*, Proc. Amer. Math. Soc. **17** (1976), no. 6, 986–994.

[Pet77] G. L. Peterson, *On the automorphism group of an integral group ring*, Illinois J. Math. **21** (1977), 836–844.

[Pfl90] H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Heldermann Verlag, Berlin, 1990.

[PM78] M. M. Parmenter and C. Polcino Milies, *Group rings whose units form a nilpotent or FC group*, Proc. Amer. Math. Soc. **68** (1978), no. 2, 247–248.

[PW50] S. Perlis and G. L. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420–426.

[RS90] J. Ritter and S. K. Sehgal, *Integral group rings with trivial central units*, Proc. Amer. Math. Soc. **108** (1990), no. 2, 327–329.

[RS87] K. W. Roggenkamp and L. L. Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. **126** (1987), 593–647.

[RSpre] K. W. Roggenkamp and L. L. Scott, *On a conjecture of Zassenhaus for finite group rings*, preprint.

[San74] R. Sandling, *Group rings of circle and unit groups*, Math. Z. **124** (1974), 195–202.

[San85] R. Sandling, *The isomorphism problem for group rings: a survey*, Lecture Notes in Math., vol. 1141, Springer, Berlin, 1985.

[San89] R. Sandling, *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52** (1989), 22–27.

[Sch66] R. D. Schafer, *An introduction to nonassociative algebras*, Academic Press, New York, 1966.

[Seh69] S. K. Sehgal, *On the isomorphism of integral group rings I*, Canad. J. Math. **21** (1969), 410–413.

[Seh78] S. K. Sehgal, *Topics in group rings*, Marcel Dekker, New York, 1978.

[Seh93] S. K. Sehgal, *Units in integral group rings*, Longman Scientific & Technical Press, Essex, 1993.

[Spi75] E. Spiegel, *On isomorphisms of abelian group algebras II*, Canad. J. Math. **27** (1975), 155–161.

[ST76] E. Spiegel and A. Trojan, *On semi-simple group algebras*, Pacific J. Math. **66** (1976), no. 2, 553–559.

[Wei91] A. Weiss, *Units in integral group rings*, J. Reine Angew. Math. **415** (1991), 175–187.

[Whi68] A. Whitcomb, *The group ring problem*, Ph.D. thesis, Chicago, 1968.

[ZM75] A. E. Zalesskii and A. V. Mikhalev, *Group rings*, J. Soviet Math. **4** (1975), 1–78.

Edgar G. Goodaire
Memorial University of Newfoundland
St. John's, Newfoundland A1C 5S7
e-mail: edgar@math.mun.ca
CANADA

César Polcino Milies
Universidade de São Paulo
Caixa Postal 66.281
05381-970 São Paulo
e-mail: polcino@ime.usp.br
BRASIL