PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 4, April 1996

# FINITE SUBLOOPS OF UNITS IN AN ALTERNATIVE LOOP RING

EDGAR G. GOODAIRE AND CÉSAR POLCINO MILIES

(Communicated by Lance W. Small)

Abstract. An RA loop is a loop whose loop rings, in characteristic different from 2, are alternative but not associative. In this paper, we show that every finite subloop $H$ of normalized units in the integral loop ring of an RA loop $L$ is isomorphic to a subloop of $L$. Moreover, we show that there exist units $\gamma_i$ in the rational loop algebra $\mathbf{Q}L$ such that $\gamma_k^{-1}(\dots(\gamma_2^{-1}(\gamma_1^{-1}H\gamma_1)\gamma_2)\dots)\gamma_k \subseteq L$. Thus, a conjecture of Zassenhaus which is open for group rings holds for alternative loop rings (which are not associative).

## 1. Introduction

Let $\mathbf{Z}G$ denote the group ring of a finite group $G$ over the integers. In this ring, elements of the form $\pm g$, $g \in G$, are torsion units, but there are usually many others as well. For instance, if $g \in G$ and $\gamma$ is a unit in the rational group algebra $\mathbf{Q}G$ such that $\alpha = \gamma^{-1}g\gamma \in \mathbf{Z}G$, then certainly $\pm\alpha$ are torsion units in $\mathbf{Z}G$. In the mid 1960's, H. J. Zassenhaus suggested that all torsion units in $\mathbf{Z}G$ arise in precisely this way. Furthermore, he surmised that any finite subgroup of normalized units in $\mathbf{Z}G$ (a unit is *normalized* if the sum of its coefficients is 1) was isomorphic to a subgroup of $G$, the isomorphism being conjugation by a unit in $\mathbf{Q}G$. These conjectures have been established for various kinds of groups, although they remain open in general.

In an earlier work, the authors established a variation of one of the conjectures of Zassenhaus for alternative loop rings which are not associative [6].

**Theorem 1.1.** *Let $r$ be a normalized torsion unit in the integral alternative loop ring $\mathbf{Z}L$ of a finite loop $L$ which is not a group. Then there exist units $\gamma_1, \gamma_2 \in \mathbf{Q}L$ and $\ell \in L$ such that $\gamma_2^{-1}(\gamma_1^{-1}r\gamma_1)\gamma_2 = \ell$.*

Were this theorem to hold without the caveat of nonassociativity, it would, of course, reduce immediately to the first of the conjectures of Zassenhaus described above. In this paper, we prove a theorem about nonassociative alternative loop rings which, if true for group rings, would imply the second of the Zassenhaus conjectures previously mentioned. Our aim is to prove

Received by the editors March 23, 1994.

1991 *Mathematics Subject Classification.* Primary 17D05; Secondary 16S34, 20N05.

This research was conducted while the first author was a guest of and partially supported by the Instituto de Matemática e Estatística, Universidade de São Paulo, to whom he is most grateful. The research was also supported by FAPESP and CNPq. of Brasil (Proc. No. 93/4440-0 and 501253/91-2, respectively) and the Natural Sciences and Engineering Research Council of Canada, Grant No. 0GP0009087.

**Theorem 1.2.** *If $H$ is a finite subloop of normalized units in a nonassociative alternative loop ring $\mathbf{Z}L$, then $H$ is isomorphic to a subloop of $L$. Moreover, there exist units $\gamma_1, \gamma_2, \ldots, \gamma_k$ of $\mathbf{Q}L$ such that $\gamma_k^{-1}(\ldots(\gamma_2^{-1}(\gamma_1^{-1}H\gamma_1)\gamma_2)\ldots)\gamma_k \subseteq L$.*

**Corollary 1.3.** *If $H$ is a subloop of normalized units in $\mathbf{Z}L$ such that $|H| = |L|$, then $H$ is isomorphic to $L$; in fact, we have $L = \gamma_k^{-1}(\ldots(\gamma_2^{-1}(\gamma_1^{-1}H\gamma_1)\gamma_2)\ldots)\gamma_k$ for units $\gamma_1, \ldots, \gamma_k \in \mathbf{Q}L$.*

## 2. RA Loops and their loop rings

An *RA loop* is a loop $L$ whose loop ring $RL$ over any ring of characteristic different from 2 is an alternative ring. The following theorem is the basis behind the theory of alternative loop rings [3].

**Theorem 2.1.** *A loop $L$ is RA if and only if*

(i) *$L = G \cup Gu$ is the disjoint union of a nonabelian group $G$ and a single coset $Gu$;*

(ii) *$G$ has a unique nonidentity commutator, $s$, which is necessarily central and of order 2;*

(iii) *the map $g \mapsto g^* = \begin{cases} g & \text{if } g \text{ is central} \\ sg & \text{otherwise} \end{cases}$ is an involution of $G$ (i.e., an antiautomorphism of order 2);*

(iv) *multiplication in $L$ is defined by $g(hu) = (hg)u$, $(gu)h = (gh^*)u$, $(gu)(hu) = g_0h^*g$, where $g_0 = u^2$ is a central element of $G$.*

The loop described in this theorem is denoted $M(G, *, u)$. It is a Moufang loop and therefore has the property that any two elements generate a group. More generally, if three elements associate in some order, they also generate a group. Thus, to say that three elements of a Moufang loop "associate" is unambiguous: if they associate in one particular order, they associate in all orders. The monograph by R. H. Bruck [2] has been the traditional reference for loop theory. For another introduction to the subject, we draw attention to the more recent book by H. Pflugfelder [11].

Let $g, h, k$ be elements of a loop. In this paper, we shall denote the *commutator* of $g$ and $h$ by $(g, h)$ and the *associator* of $g$, $h$ and $k$ by $(g, h, k)$. These are defined by the equations

$$\begin{aligned} gh &= (hg)(g,h) \\ \text{and} \quad (gh)k &= [g(hk)](g,h,k). \end{aligned}$$

As usual, $L'$ will be the subloop of $L$ generated by the commutators. The centre of a group or ring $X$ will be denoted $\mathcal{Z}(X)$. When $X$ is not associative, $\mathcal{Z}(X)$ is the set of elements which commute with all other elements of $X$ *and associate with all other pairs of elements* of $X$. RA loops have a number of special properties. Those of particular relevance in this paper are recorded in the next theorem. (See [3] and [4] for the details.)

**Theorem 2.2.** *Let $L$ be an RA loop. Then*

(i) *Given any three elements $x, y, u \in L$ which do not associate, the group $G$ generated by $x$, $y$ and the centre of $L$ defines $L$ in the sense that for this $G$ and the given $u$, we have $L = M(G, *, u)$.*

(ii) *If $L = M(G, *, u)$, then $\mathcal{Z}(L) = \mathcal{Z}(G)$.*

(iii) *For any $g \in L$, $g^2 \in \mathcal{Z}(L)$.*

(iv) *The unique nonidentity commutator, $s$, is also a unique nonidentity associator; thus, for every $g, h, k \in L$, both $(g, h)$ and $(g, h, k)$ are in $L' = \{1, s\}$.*

(v) *For $g, h \in L$, we have $(g, h) = 1$ if and only if $(g, h, k) = 1$ for all $k \in L$.*

(vi) *For $g, h \in L$, $(g, h) = 1$ if and only if $g \in \mathcal{Z}(L)$ or $h \in \mathcal{Z}(L)$ or $gh \in \mathcal{Z}(L)$. (This has been termed the "LC" property in other papers on alternative loop rings and RA loops.)*

We shall have reason to appeal to the following additional fact about RA loops.

**Corollary 2.3.** *If $L_0$ is a subloop of an RA loop which is not commutative, then $\mathcal{Z}(L_0) \subseteq \mathcal{Z}(L)$.*

*Proof.* Let $a \in \mathcal{Z}(L_0)$. Let $x, y$ be elements of $L_0$ which do not commute; thus none of $x$, $y$, $xy$ is central. Since $ax = xa$, one of $a, x, ax$ is central, and this must be $a$ or $ax$. If $a$ is central, there is nothing to prove, so assume $ax$ is central. Similarly, assume $ay$ and $a(xy)$ are central. In this case,

$$a(xy) = a[(a^{-1} \cdot ax)(a^{-1} \cdot ay)] = a^{-1}(ax)(ay)$$

using centrality of $ax$ and $ay$. Thus $a^{-1}$ and hence $a$ are central. So in every case, $a \in \mathcal{Z}(L)$ as asserted. □

Let $R$ be any commutative and associative ring with 1 and of characteristic different from 2. Since the elements of $L = M(G, *, u)$ are those of $G \cup Gu$, it is easy to see that any $\alpha = \sum \alpha_\ell \ell$ in the loop ring $RL$ can be expressed in the form $\alpha = x + yu$, where $x$ and $y$ are in the group ring $RG$. Using this representation, multiplication in $RL$ takes the form

$$(x + yu)(z + wu) = (xz + g_0 w^* y) + (wx + yw^*)u \tag{2.1}$$

where $x, y, z, w \in RG$. The involution on $G$ extends first to $L$ by setting $(gu)^* = s(gu)$ and then to $RL$ by

$$\left(\sum \alpha_\ell \ell\right)^* = \sum \alpha_\ell \ell^* \quad \text{or, equivalently,} \quad (x + yu)^* = x^* + syu.$$

The centre of an alternative loop ring $RL$ is $\mathcal{Z}(RL) = \{\alpha \in RL \mid \alpha^* = \alpha\}$ [8], thus $\alpha\alpha^*$ is central for all $\alpha \in RL$, and $g^* = g$ for $g \in L$ if and only if $g \in \mathcal{Z}(L)$. The group or loop of units (invertible elements) in a ring $S$ is denoted $\mathcal{U}(S)$ while $T\mathcal{U}(S)$ is the group or loop of *torsion units* in $S$ (those units which have finite order). By $\mathcal{U}_1(RL)$ and $T\mathcal{U}_1(RL)$ we mean the *normalized* units and *normalized torsion* units, respectively, of the loop ring $RL$. These are the units whose *augmentation* is 1, where, for $\alpha = \sum \alpha_\ell \ell$, the augmentation of $\alpha$ is $\epsilon(\alpha) = \sum \alpha_\ell$. The augmention map $\epsilon$ is a ring homomorphism. Also, the elements of $L$ have augmentation 1. Thus, if we hope to prove a relation such as

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

for units $\gamma_i$ and a subloop $H$, then it is clear that we will have to restrict our attention to subloops $H$ of normalized units.

The following proposition and its proof involve straightforward translations from an analogous proposition and its proof for group rings. Since the proof is short, we include it here.

**Proposition 2.4.** *Any finite set of normalized units in $\mathbf{Z}L$ which forms a loop is linearly independent over $\mathbf{Z}$.*

*Proof.* If $\sum_{i=1}^{n} a_i\gamma_i = 0$, with $a_i \in \mathbf{Z}$ and $\gamma_i \in T\mathcal{U}_1(\mathbf{Z}L)$, then we can write

$$a_1 1 = -\sum_{i=2}^{n} a_i(\gamma_1^{-1}\gamma_i). \tag{2.2}$$

Each $\gamma_1^{-1}\gamma_i$ is a torsion unit and different from the identity element, hence, when it is expressed as a linear combination of loop elements, the coefficient of the identity is 0 [6, Proposition 2.1]. So, comparing coefficients of 1 on each side of (2.2), we obtain $a_1 = 0$. Similarly, all $a_i = 0$. □

A *composition algebra* is an algebra $A$ with 1 over a field $F$ on which there is a multiplicative nondegenerate quadratic form $q\colon A \to F$. By *multiplicative*, we mean that $q(xy) = q(x)q(y)$ for all $x, y \in A$. If $U$ is any subspace of $A$, the subspace $U^\perp$ is defined by

$$U^\perp = \{a \in A \mid f(a,u) = 0 \text{ for all } u \in U\}$$

where $f(x,y) = q(x+y) - q(x) - q(y)$ is the symmetric bilinear form associated with $q$. Nondegeneracy of the quadratic form $q$ means $A^\perp = 0$. Nondegeneracy on a subspace $U$ means $U \cap U^\perp = 0$.

Any composition algebra is equipped with an involution $x \mapsto \overline{x}$ such that $q(x) = x\overline{x}$. Also, when char $F \neq 2$, by the theorem of Hurwitz, the only possible dimensions of a composition algebra are 1, 2, 4 and 8. Those of dimension 8 are not associative and are called *Cayley-Dickson algebras* [10, p. 425]

**Proposition 2.5.** *Let $A$ be a Cayley-Dickson algebra over a field $F$ with quadratic form $q$ and suppose that $B$ is a noncommutative associative subalgebra such that $\overline{B} \subseteq B$. Then, for any $\ell \in B^\perp$ such that $q(\ell) = -c \neq 0$, $A$ is the vector space direct sum $A = B \oplus B\ell$ and multiplication in $A$ is given by $(x + y\ell)(z + w\ell) = (xz + c\overline{w}y) + (wx + y\overline{z})\ell$, where $x, y, z, w \in B$. If $A = B_1 \oplus B_1\ell_1 = B_2 \oplus B_2\ell_2$ for subalgebras $B_1$ and $B_2$ of $A$ and if $q(\ell_1) = q(\ell_2)$, then any isomorphism $\sigma\colon B_1 \to B_2$ which commutes with the involution on $A$ (i.e., $\sigma(\overline{b}) = \overline{\sigma(b)}$ for all $b \in B_1$), extends to an inner automorphism of $A$.*

*Proof.* The first part of this proposition is contained in [10, Lemma 3, p. 424]. For the last part, if $A = B_1 \oplus B_1\ell_1 = B_2 \oplus B_2\ell_2$, if $q(\ell_1) = q(\ell_2)$ and if $\sigma\colon B_1 \to B_2$ is an isomorphism, it is immediate that $\sigma(x + y\ell_1) = \sigma(x) + \sigma(y)\ell_2$ extends $\sigma$ to an automorphism of $A$. The result now follows since any automorphism of a composition algebra is inner [9]. □

**Proposition 2.6.** *Let $F$ be a field of characteristic different from 2. Suppose $B$ is a simple subalgebra with 1 of an alternative loop algebra $FL$ such that $B^* \subseteq B$ and whose centre is contained in the centre of $FL$. Then the map $n\colon B \to \mathcal{Z}(B)$ defined by $n(b) = bb^*$ is a multiplicative nondegenerate quadratic form on $B$. Thus, $B$ is a composition algebra.*

*Proof.* For any $\alpha \in \mathcal{Z}(B)$ and $b \in B$, we have $n(\alpha b) = (\alpha b)(b^*\alpha^*) = \alpha^2 n(b)$ since $bb^* \in \mathcal{Z}(FL)$ and $\alpha \in \mathcal{Z}(FL)$ implies $\alpha^* = \alpha$. Since $n(x+y) - n(x) - n(y) = xy^* + yx^*$, the form associated with $n$ is bilinear; thus $n$ is quadratic. That $n$ is multiplicative follows from centrality of $bb^*$ for any $b \in FL$. To prove nondegeneracy, we follow standard arguments. Replacing $x$ by $x + z$ in the identity $n(xy) = n(x)n(y)$ gives

$$n(xy) + n(zy) + f(xy, zy) = [n(x) + n(z) + f(x,z)]n(y),$$

where $f$ is the bilinear form associated with $n$, and so $f(xy, zy) = f(x, z)n(y)$. Then replacing $y$ by $y + w$ gives

$$f(xw, zy) + f(xy, zw) = f(x, z)f(y, w).$$

With $w \in B \cap B^{\perp}$, $x = 1$ and $y, z \in B$, we get $f(y, zw) = 0$. So $B \cap B^{\perp}$ is a left ideal of $B$. Similarly it is a right ideal. Since $B \cap B^{\perp} \neq B$ $(1 \in B \setminus B^{\perp})$, it follows that $B \cap B^{\perp} = 0$, so $n$ is nondegenerate on $B$. □

Suppose $L$ is a finite loop and $F$ is a field of characteristic relatively prime to the order of $L$. Even in this most general situation, the loop algebra $FL$ is known to be the direct sum of simple algebras [1, Theorem 7A]; certainly then, the loop algebra of an RA loop is the direct sum of simple subalgebras.

**Corollary 2.7.** *Any simple component of the loop algebra of an RA loop $L$ over a field of characteristic relatively prime to $|L|$ is a composition algebra with respect to the quadratic form $n(\alpha) = \alpha\alpha^*$.*

*Proof.* If $A$ is such a simple component, then both $A$ and $A^*$ are ideals of $FL$, so $A \cap A^*$ is an ideal of $A$ which is not zero (it contains $1_A$, the identity of $A$). So $A^* = A$ and the result follows from the proposition. □

**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 $\pi$ 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 of $A$, and a Cayley-Dickson algebra if and only if $\pi(s) = -1_A$.*

*Proof.* In what follows, it is important to remember that $\operatorname{char} F$ relatively prime to $|L|$ implies, in particular, that $\operatorname{char} F \neq 2$ since $|L|$ is divisible by 2. (Actually, $L$ is the direct product of a 2-loop and an abelian group (which could be trivial) [3].) Let $A$ be a simple component of $FL$. Since $s$ is central of order 2 in $FL$, $\pi(s) = \pm 1_A$ in $A$. Now $A$ is spanned over $F$ by the elements $\pi(g)$, $g \in L$. Since $(g, h) \in \{1, s\}$ for any $g, h \in L$, it follows that $A$ is commutative and hence a field if $\pi(s) = +1_A$. On the other hand, suppose $\pi(s) = -1_A$ and let $g, h \in L$ be elements which do not commute. Then $gh = hgs$, so $\pi(g)\pi(h) = -\pi(h)\pi(g) \neq \pi(h)\pi(g)$, so $A$ is not commutative, hence not a field. So $\pi(s) = 1_A$ if and only if $A$ is a field. Noting that $A$ is a composition algebra by Corollary 2.7, and remembering that a nonassociative composition algebra is a Cayley-Dickson algebra, we can complete the proof by showing that if $A$ is not commutative, then it is not associative. Let $g$ and $h$ be elements in $L$ whose images in $A$ do not commute. Then there exists $k \in L$ such that $g, h, k$ do not associate (Theorem 2.2); thus $(gh)k = g(hk)s$. But then in $A$, $\pi(g)\pi(h) \cdot \pi(k) = -\pi(g) \cdot \pi(h)\pi(k) \neq \pi(g) \cdot \pi(h)\pi(k)$. So $A$ is not associative. □

The latter part of this proof identifies what is perhaps a surprising fact.

**Corollary 2.9.** *Let $F$ be a field of characteristic relatively prime to the order of a finite RA loop $L$. If the images of elements $g, h \in L$ commute in any simple component of $FL$ which is not a field, then $g$ and $h$ commute. If the images of three elements $g, h, k \in L$ associate in any simple component of $FL$ which is not a field, then $g, h, k$ associate.*

## 3. THE MAIN RESULTS

**Theorem 3.1.** *If $L$ is a finite RA loop and $H$ is a finite subloop of $T\mathcal{U}_1(\mathbf{Z}L)$, then there is a one-to-one homomorphism $\rho_H\colon H \to L$ such that*

(i) *$\rho_H(\alpha) = \alpha$ for all $\alpha \in H \cap L$;*
(ii) *if $\alpha \in H$, then there exist units $\gamma_1, \gamma_2 \in \mathbf{Q}L$ 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.* Most of this theorem is in fact contained in previous papers by the authors; the opening statement and part (i) in [5] and part (ii) in [6]. In an alternative algebra, the subalgebra generated by any pair of elements is associative; thus, as with associative algebras, $(\gamma^{-1}\alpha\gamma)^n = \alpha^n$. Now part (iii) follows immediately since squares of elements in an RA loop are central. □

**Corollary 3.2.** *Let $L$ be a finite RA loop with $L' = \{1, s\}$ and let $H$ be a finite subloop of $T\mathcal{U}_1(\mathbf{Z}L)$. 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 $\mathcal{Z}(H) \subseteq \mathcal{Z}(L)$.*

*Proof.* Let $\rho_H\colon H \to L$ be the homomorphism of the Theorem. For $\alpha, \beta \in H$, we have $\rho_H(\alpha, \beta) = (\rho_H(\alpha), \rho_H(\beta))$. Since $\rho_H$ is one-to-one, $(\alpha, \beta) \neq 1$ implies $\rho_H(\alpha, \beta) \neq 1$; hence $\rho_H(\alpha, \beta) = (\rho_H(\alpha), \rho_H(\beta)) = s$. Since $\rho_H(\alpha, \beta) = \gamma_2^{-1}(\gamma_1^{-1}(\alpha, \beta)\gamma_1)\gamma_2$ for units $\gamma_1, \gamma_2 \in \mathbf{Q}L$ and since $\rho_H(\alpha, \beta) = s$ is central, we have $(\alpha, \beta) = s$. A similar argument establishes the second statement of the corollary. Finally, suppose $H$ is not commutative and let $\alpha \in \mathcal{Z}(H)$. Then $\rho_H(\alpha)$ is central in the subloop of $L$ which is the image of $\rho_H$, hence central in $L$ by Corollary 2.3. The result now follows by part (ii) of the theorem. □

**Corollary 3.3.** *Let $H$ be a finite noncommutative subloop of $T\mathcal{U}_1(\mathbf{Z}L)$ and $\rho_H\colon H \to L$ the homomorphism described in the theorem. Then $H^* \subseteq H$ and $\rho_H$ commutes with $*$.*

*Proof.* Since $H$ is not commutative, $s \in H$ by the previous corollary. Now if $\alpha \in H$ is central, then it is trivial [7, Theorem 6], and $\alpha^* = \alpha \in H$. If $\alpha \in H$ is not central, then it has no central elements in its support [6, Corollary 2.2], so $\alpha^* = s\alpha \in H$. Thus $H^* \subseteq H$. Next, let $\alpha \in H$. If $\alpha$ is central in $\mathbf{Z}L$, then $\alpha$ is trivial, $\rho_H(\alpha) = \alpha$ (by part (i) of the theorem) and so $\rho_H(\alpha^*) = \rho_H(\alpha) = \alpha = \alpha^* = \rho_H(\alpha)^*$. If $\alpha$ is not central, $\alpha^* = s\alpha$. Also, by part (ii) of the theorem, we know that $\rho_H(\alpha)$ is not central. So again $\rho_H(\alpha^*) = \rho_H(s\alpha) = \rho_H(s)\rho_H(\alpha) = s\rho_H(\alpha) = \rho_H(\alpha)^*$. □

We now turn our attention to the proof of our main theorem.

*Proof of Theorem 1.2.* Let $H$ be a finite subloop of $T\mathcal{U}_1(\mathbf{Z}L)$ and let $\rho\colon H \to L$ be the homomorphism of Theorem 3.1. Set $L_0 = \rho(H)$.

We suppose first that $H$ is an abelian group. Then $L_0$ is also an abelian group and it's contained in $L$. If $L_0$ is not central, it contains a noncentral element $\ell_0$. If $x$ is any other element in $L_0$, since $\ell_0 x = x\ell_0$, either $x$ or $\ell_0 x$ is central by Theorem 2.2. In the latter case, $x = x^2(\ell_0 x)^{-1}\ell_0$ is a central multiple of $\ell_0$. It follows that $L_0$ is generated by a set $S$ of central elements and the single element $\ell_0$. Now $L_0 = \rho(H)$ and $S$ is fixed elementwise by $\rho$, by Theorem 3.1, so $H$ is generated by $S$ and the single element $\widehat{\ell_0} = \rho^{-1}(\ell_0)$. Moreover, there exist $\gamma_1, \gamma_2 \in \mathbf{Q}L$ 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.

Now suppose that $H$ is not an abelian group. We wish to show the existence of $\gamma_i \in \mathbf{Q}L$ such that

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

In fact, we shall show that there exist units $\gamma_i \in \mathbf{Q}L$ such that, for all $\alpha \in H$,

$$\gamma_k^{-1}(\dots(\gamma_2^{-1}(\gamma_1^{-1}\alpha\gamma_1)\gamma_2)\dots)\gamma_k = \rho(\alpha). \tag{3.1}$$

Expressing $\mathbf{Q}L$ as the sum of fields and Cayley-Dickson algebras, it is sufficient to show that in each simple component of $\mathbf{Q}L$, there exist units such that (3.1) is valid (in that component). Since the elements of $H$ and their corresponding images through $\rho$ have common conjugates in $\mathbf{Q}L$, it follows that they have equal images in the commutative components of $\mathbf{Q}L$, so we need only to consider the components which are Cayley-Dickson algebras. Let $A$ be such a simple component and $\pi\colon \mathbf{Q}L \to A$ the natural projection. There remain two cases to consider, according to whether or not $H$ is associative.

Suppose $H$ is a nonabelian group. Then $L_0 = \rho(H)$ is a nonabelian group contained in $L$. Let $x$ and $y$ be noncommuting elements of $L_0$ and let $u$ be an element of $L$ such that $(x, y, u) \neq 1$. Let $G$ be the group generated by $x$, $y$ and $\mathcal{Z}(L)$. Thus $L = M(G, *, u)$. Let $B$ be the subalgebra of $\mathbf{Q}L$ generated by $x$ and $y$. Since $xy \neq yx$, $\pi(x)\pi(y) \neq \pi(y)\pi(x)$ (Corollary 2.9), so $\pi(B)$ is an associative subalgebra of $A$ which is not commutative. Recalling that $A$ is a composition algebra with respect to the quadratic form $n\colon a \mapsto aa^*$, we claim that $\pi(u) \in \pi(B)^\perp$. For this, let $b \in B$ (hence $b \in \mathbf{Q}G$) and let $f$ be the bilinear form associated with $n$. Note that

$$f(x, y) = n(x + y) - n(x) - n(y) = xy^* + yx^*$$

for any $x, y \in \mathbf{Q}L$. Using the multiplication rule (2.1) and noting that $u^* = su$ because $u$ is not central, we have $f(b, u) = bu^* + ub^* = sbu + bu = (1 + s)bu$ which is 0 in $A$ because $\pi(s) = -1_A$. Also, $n(u) = uu^* = su^2$, so $n(\pi(u)) \neq 0$ ($\pi(u)$ is a unit). As well, $B^* \subseteq B$ because $x^* = sx$, $y^* = sy$ ($x, y$ being noncentral), so $\pi(B)^* \subseteq \pi(B)$. Hence, by Proposition 2.5, $A = \pi(B) \oplus \pi(B)\pi(u)$.

Next, let $\widehat{x}, \widehat{y}, \widehat{u}$ be preimages under $\rho$ of $x, y, u$ respectively and let $\widehat{B}$ be the subalgebra of $\mathbf{Q}L$ generated by $\widehat{x}$ and $\widehat{y}$. (We now find it convenient to use $\widehat{\ }$ instead of $\rho^{-1}$.) Then $\widehat{x}, \widehat{y}, \widehat{u} \in H$ and $\pi(\widehat{B})$ is an associative, but not commutative, subalgebra of $A$. Since the elements of $H$ are linearly independent over $\mathbf{Z}$, they are linearly independent over $\mathbf{Q}$, and we can identify the subalgebra $\langle H\rangle$ of $\mathbf{Q}L$ generated by $H$ with $\mathbf{Q}H$. In this way, we see that the isomorphism $\rho\colon H \to L_0$ extends to a ring isomorphism $\langle H\rangle \to \mathbf{Q}L_0$ which restricts to a ring isomorphism $\widehat{B} \to B$ and induces a ring isomorphism $\pi(\widehat{B}) \to \pi(B)$.

Since $\widehat{x}$ is a noncentral torsion unit, it has no central elements in its support [6]. Thus $\widehat{x}^* = s\widehat{x}$ and, similarly, $\widehat{y}^* = s\widehat{y}$ and $\widehat{u}^* = s\widehat{u}$. We claim that $\pi(\widehat{u}) \in \pi(\widehat{B})^\perp$. For with $\widehat{b} \in \widehat{B}$, we have $f(\widehat{b}, \widehat{u}) = \widehat{b}\widehat{u}^* + \widehat{u}(\widehat{b})^* = s\widehat{b}\widehat{u} + \widehat{u}(\widehat{b^*})$ ($\rho$ commutes with $*$) $= s\widehat{b}\widehat{u} + \widehat{ub^*} = s\widehat{b}\widehat{u} + \widehat{bu} = (1+s)\widehat{b}\widehat{u}$, which is 0 in $A$. Also, we have $n(\widehat{u}) = \widehat{u}\widehat{u}^* = s\widehat{u}^2$ which is not 0 in $A$, and $\widehat{B}^* \subseteq \widehat{B}$ (since $\rho$ and $*$ commute), so $A = \pi(\widehat{B}) \oplus \pi(\widehat{B})\pi(\widehat{u})$.

Since $n(u) = su^2 = s\widehat{u}^2$ (Theorem 3.1) $= n(\widehat{u})$, we have, by Proposition 2.5, that $\rho\colon \pi(\widehat{B}) \to \pi(B)$ extends to an inner automorphism of $A$ which, by [9], is the product of *reflections*; that is, maps of the form $x \mapsto \gamma^{-1}x\gamma$.

Finally, we consider the case that $H$ is a nonassociative finite subloop of $T\mathcal{U}_1(\mathbf{Z}L)$. Since $H$ is not associative, neither is $L_0 = \rho(H)$. Let $x, y, u$ be three elements of

$L_0$ which do not associate and $\widehat{x}, \widehat{y}, \widehat{u}$ their preimages in $H$. By Corollary 2.9, $\pi(\widehat{x}), \pi(\widehat{y}), \pi(\widehat{u})$ do not associate, so they generate a nonassociative subalgebra of the Cayley-Dickson algebra. Since a Cayley-Dickson algebra has no proper subalgebras which are not associative, $\pi(H)$ generates $A$. Similarly, $\pi(L_0)$ generates $A$. The map $\rho\colon H \to L_0$ induces an isomorphism $\langle \pi(H) \rangle \to \langle \pi(L_0) \rangle$; that is, an automorphism of $A$, which is necessarily inner, the product of reflections. The result follows.

## References

1. R. H. Bruck, *Some results in the theory of linear nonassociative algebras*, Trans. Amer. Math. Soc. **56** (1944), 141–199. MR **6:**116b
2. ______, *A survey of binary systems*, Ergeb. Math. Grenzgeb., vol. 20, Springer-Verlag, 1958. MR **20:**76
3. Orin Chein and Edgar G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra **14** (1986), no. 2, 293–310. MR **87c:**20116
4. Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Debrecen **30** (1983), 31–38. MR **85k:**20200
5. Edgar G. Goodaire and César Polcino Milies, *Isomorphisms of integral alternative loop rings*, Rend. Circ. Mat. Palermo **XXXVII** (1988), 126–135. MR **90b:**20058
6. ______, *Torsion units in alternative loop rings*, Proc. Amer. Math. Soc. **107** (1989), 7–15. MR **89m:**20084
7. Edgar G. Goodaire and M. M. Parmenter, *Units in alternative loop rings*, Israel J. Math. **53** (1986), no. 2, 209–216. MR **87k:**17028
8. ______, *Semi-simplicity of alternative loop rings*, Acta Math. Hungar. **50** (1987), no. 3–4, 241–247. MR **89e:**20119
9. N. Jacobson, *Composition algebras and their automorphisms*, Rend. Circ. Mat. Palermo **VII** (1958), 55–80. MR **21:**66
10. Nathan Jacobson, *Basic algebra I*, W. H. Freeman and Company, San Francisco, 1974. MR **50:**9457
11. H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Heldermann Verlag, Berlin, 1990.

Department of Mathematics, Memorial University of Newfoundland, St. John's, Newfoundland, Canada A1C 5S7
*E-mail address*: edgar@math.mun.ca

Universidade de São Paulo, Caixa Postal 20570, 01452-990 São Paulo, Brasil
*E-mail address*: polcino@ime.usp.br