ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 283 (2005) 317–326
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Hypercentral units in alternative loop rings ☆

Edgar G. Goodaire [a,*], Yuanlin Li [b], Michael M. Parmenter [a]

[a] *Memorial University of Newfoundland, St. John's, Newfoundland, Canada A1C 5S7*
[b] *Brock University, St. Catherine's, Ontario, Canada L2S 3A1*

Received 19 April 2004

Available online 16 September 2004

Communicated by Georgia Benkart

Abstract

Let L be an RA loop, that is, a loop whose loop rings are alternative, but not associative, rings (in any characteristic). We find necessary and sufficient conditions under which the hypercentral units in the integral loop ring $\mathbb{Z}L$ are central.

1. Introduction

Let L be a Moufang loop, that is, a loop satisfying any of the following three equivalent identities:

$$(xy \cdot z)y = x(y \cdot zy) \quad \text{right Moufang,}$$
$$(xy \cdot x)z = x(y \cdot xz) \quad \text{left Moufang,}$$
$$(xy)(zx) = x(yz \cdot x) \quad \text{middle Moufang.}$$

☆ This research was supported by Discovery Grants from the Natural Sciences and Engineering Research Council of Canada.
* Corresponding author.
E-mail addresses: edgar@math.mun.ca (E.G. Goodaire), yli@spartan.ac.brocku.ca (Y. Li), michael1@math.mun.ca (M.M. Parmenter).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2004.08.012

Perhaps the most important property of Moufang loops is their *diassociativity*: the subloop of a Moufang loop generated by any two elements is a group [8, §IV.2]. In particular, the Moufang identity is often used (unambiguously) in the form $(xy \cdot z)y = x(yzy)$. More generally, Moufang proved that if three elements of a Moufang loop associate in any order, then they generate a group [8, §IV.2].

For $x, y, z \in L$, the *commutator* (x, y) of x and y and the *associator* (x, y, z) of x, y, and z are defined, respectively, by

$$xy = (yx)(x, y) \quad \text{and} \quad xy \cdot z = (x \cdot yz)(x, y, z).$$

Using diassociativity, notice that $(x, y) = x^{-1}y^{-1}xy$, just as with groups, and $(x, y, z) = [xy \cdot z][z^{-1}y^{-1} \cdot x^{-1}]$. The *commutator–associator* subloop of L is the subloop L' generated by all commutators and associators.

The *centre*, $\mathcal{Z}(L)$, of L is the set of all elements of L which commute with all other elements and associate with all pairs of elements of L:

$$\mathcal{Z}(L) = \{a \in L \mid (a, x) = (a, x, y) = (x, a, y) = (x, y, a) = 1 \text{ for all } x, y \in L\}.$$

Just as in group theory, a Moufang loop L has an *upper central series*

$$\{1\} = \mathcal{Z}_0(L) \subseteq \mathcal{Z}_1(L) \subseteq \mathcal{Z}_2(L) \subseteq \cdots,$$

where $\mathcal{Z}_{i+1}(L)/\mathcal{Z}_i(L) = \mathcal{Z}(L/\mathcal{Z}_i(L))$. (Note that $\mathcal{Z}_1(L) = \mathcal{Z}(L)$, the centre of L.) When there is no chance of ambiguity, we write $\mathcal{Z}_i$ rather than $\mathcal{Z}_i(L)$. The *hypercentre* of L is the subloop $\widetilde{\mathcal{Z}}(L) = \bigcup_{i \geqslant 0} \mathcal{Z}_i(L)$.

For $x, y, a \in L$, there are bijections $R(x)$, $L(x)$, $T(x)$ and $R(x, y)$ defined by

$$aR(x) = ax, \qquad aL(x) = xa, \qquad T(x) = R(x)L(x)^{-1},$$
$$R(x, y) = R(x)R(y)R(xy)^{-1}.$$

A subloop H of L is *normal* if and only if $HT(x) \subseteq H$ and $HR(x, y) \subseteq H$ for all $x, y \in L$. For instance, the commutator–associator subloop of a loop is always normal [1, Proposition II.1.8].

Throughout, $\mathcal{U}(\mathsf{Z}L)$ denotes the loop of units (that is, the invertible elements) in $\mathsf{Z}L$, the integral loop ring of L, and we often write $\mathcal{U}$ for $\mathcal{U}(\mathsf{Z}L)$. We denote by $\mathcal{N}_{\mathcal{U}}(L)$ the *normalizer* of L in $\mathcal{U}$, this being the largest subloop of $\mathcal{U}$ in which L is normal.

An *alternative ring* is one in which $x(xy) = x^2y$ and $(yx)x = yx^2$ are identities. Alternative rings are so-named because in these rings, the (*ring*) *associator* $[a, b, c] := (ab)c - a(bc)$ is an alternating function of its arguments. (We use square brackets for ring associators to avoid confusion with loop associators.)

A (necessarily Moufang) loop L is an *RA loop* if, over any commutative associative coefficient ring R, the loop ring RL is an alternative, but not associative, ring. That there exist such loops came to light in 1983 [3]. By now, RA loops have been completely classified and many properties of the associated alternative loop rings explored. The best source of information on these subjects is [1] to which we make frequent reference here. We record now some properties of RA loops of special interest in this paper.

An RA loop L has the *LC property*: elements $g, h \in L$ commute if and only if one of g, h, gh is central [1, §IV.2]. In particular, this implies that the square of any element of an RA loop is central. In an RA loop L, the set of *torsion* elements (those of finite order) is a subloop of L [1, Lemma VIII.4.1] called the *torsion subloop* of L. If L is RA, then any loop ring RL of L is an alternative ring and so the unit loop of RL is Moufang [1, §II.5.3].

In an RA loop L, there is a unique nonidentity commutator (always denoted s) which is also the only nonidentity associator. This element has order 2 and is central in L (and hence central in $\mathcal{U}$) [4, Lemma 3.2]. It follows that $L/\mathcal{Z}(L)$ is an Abelian group, so $L = \mathcal{Z}_2(L)$, the *second centre* of L. It is rare for the entire unit loop $\mathcal{U}(\mathbb{Z}L)$ to equal its second centre. When this occurs $\mathcal{U}(\mathbb{Z}L)$ is nilpotent and hence itself an RA loop [1, Corollary XII.2.14]. On the other hand, as we show in this paper, the second centre of $\mathcal{U}(\mathbb{Z}L)$ equals the centre "most of the time." Specifically, we establish the following theorem.

Theorem 1.1. *Let L be an RA loop and let $\mathcal{U}$ be the loop of units of $\mathbb{Z}L$. Then $\widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U})$. Moreover, with T the torsion subloop of L, $\widetilde{\mathcal{Z}}(\mathcal{U}) \neq \mathcal{Z}(\mathcal{U})$ if and only if*

(i) *T is a Hamiltonian Moufang 2-loop and $\ell^{-1}t\ell = t^{\pm 1}$ for any $t \in T$ and any $\ell \in L$, or*
(ii) *T is an Abelian group and every subgroup of T is normal in L.*

The result for torsion RA loops (every element has finite order), was found by Goodaire and Li in 2001 [2].

Theorem 1.2. *If L is a torsion RA loop but not a Hamiltonian 2-loop, then $\mathcal{Z}_2(\mathcal{U}) = \mathcal{Z}(\mathcal{U})$.*

We also refer the reader to [5] where some of the results of this paper are established for group rings.

2. Preliminaries

For the rest of this paper, L denotes an RA loop and $\mathcal{U}$ is the loop of units of the integral loop ring $\mathbb{Z}L$. We begin with a short but very useful lemma.

Lemma 2.1. *Suppose $u, v \in \mathcal{U}$ and $(u, v) \in L$. Then $(u, v) \in L'$.*

Proof. Let $\alpha \mapsto \bar{\alpha}$ denote the extension to $\mathbb{Z}L$ of the natural map $L \to L/L'$. In the Abelian group ring $\mathbb{Z}[L/L']$, the commutator $(\bar{u}, \bar{v}) = \bar{1}$. Thus $\overline{(u, v)} = (\bar{u}, \bar{v}) = \bar{1}$, so $(u, v) \in L'$. $\square$

While the next theorem was stated in [2] for *torsion* loops, the proof given does not use the torsion property.

Theorem 2.2 (The normalizer conjecture). *Let L be an arbitrary RA loop. Then $\mathcal{N}_{\mathcal{U}}(L) = L \cdot \mathcal{Z}(\mathcal{U})$.*

If $\alpha = \sum \alpha_\ell \ell$ is an element of a loop ring, the scalar $\sum \alpha_\ell$ is called the *augmentation* of α and denoted $\varepsilon(\alpha)$. The map $\varepsilon : RL \to R$ is a ring homomorphism and so, if u is a unit of $\mathbf{Z}L$, its augmentation is ± 1. When trying to establish properties of units, it is often convenient to assume that the augmentation of a given unit u is 1 since if $\varepsilon(u) = -1$, the result for $-u$ (which has augmentation $+1$) usually gives the result for u immediately. This is clearly the case when trying to prove that units of $\mathbf{Z}L$ are *trivial*, that is, elements of $\pm L$.

Lemma 2.3. *Let L be a group or an RA loop and let u be a central unit in $\mathbf{Z}L$. If u^n is trivial for some natural number n, then u is trivial too.*

Proof. It is sufficient to establish the result for u of augmentation 1. Let $\alpha \mapsto \alpha^\sharp$ be the extension to $\mathbf{Z}L$ of the map $\ell \mapsto \ell^{-1}$ in L; that is, for $\alpha = \sum \alpha_i \ell_i$, $\alpha^\sharp = \sum \alpha_i \ell_i^{-1}$. Easily $\alpha \mapsto \alpha^\sharp$ is an antiautomorphism of $\mathbf{Z}L$, so, letting $\ell = u^n \in L$, we have $(u^\sharp)^n = (u^n)^\sharp = \ell^{-1}$. Since u and $u^\sharp$ commute (and because $\mathcal{U}$ is a Moufang and hence diassociative loop), $(uu^\sharp)^n = 1$. As a central unit in $\mathbf{Z}L$ of finite order, $uu^\sharp$ is trivial [1, Corollary VIII.1.7]. Since $\varepsilon(u^\sharp) = \varepsilon(u) = 1$, the augmentation of $uu^\sharp$ is 1, so $uu^\sharp = \ell_1$ for some $\ell_1 \in L$. Since the coefficient of 1 in $uu^\sharp$ is not zero (it is the sum of squares of integers), it must be that $\ell_1 = 1$ from which it follows readily that u is trivial. □

Corollary 2.4. *Let L be an RA loop and let $\mathcal{U}$ be the loop of units of $\mathbf{Z}L$. Let $u, v \in \mathcal{U}$ and $z = (u, v)$. If $z \in \mathcal{Z}(\mathcal{U})$ and z^n is trivial for some natural number n, then $z \in L'$.*

Proof. We have $z^n = \pm\ell$ for some $\ell \in L$. By Lemma 2.3, z is trivial. Since z is a commutator, $\varepsilon(z) = 1$, so $z \in L$. By Lemma 2.1, $z \in L'$. □

Theorem 2.5. *Let L be an RA loop and let $\mathcal{U}$ be the unit loop of $\mathbf{Z}L$. Then $\widetilde{\mathcal{Z}}(\mathcal{U}) \subseteq \mathcal{N}_{\mathcal{U}}(L)$.*

Proof. Writing $\mathcal{Z}_n$ for $\mathcal{Z}_n(\mathcal{U})$, we prove by induction on $n \geqslant 1$ that $\mathcal{Z}_n \subseteq \mathcal{N}_{\mathcal{U}}(L)$. For $n = 1$, $\mathcal{Z}_1 = \mathcal{Z}(\mathcal{U}) \subseteq \mathcal{N}_{\mathcal{U}}(L)$ by Theorem 2.2. Suppose the result is true for $k \geqslant 1$. Take $z_{k+1} \in \mathcal{Z}_{k+1}$ and $\ell \in L$. Then $(\ell, z_{k+1}) = z_k \in \mathcal{Z}_k \subseteq \mathcal{N}_{\mathcal{U}}(L)$ (and note that as a commutator, z_k has augmentation 1). By Theorem 2.2, we can write $z_k = z\ell_1$, $z \in \mathcal{Z}(\mathcal{U})$, $\ell_1 \in L$. Thus $z_{k+1}^{-1}\ell z_{k+1} = z\ell\ell_1$. Since ℓ^2 is central, $\ell^2 = z_{k+1}^{-1}\ell^2 z_{k+1} = z^2(\ell\ell_1)^2$, so z^2 is trivial. By Lemma 2.3, z is trivial, so z_k is trivial, hence in L (because this element has augmentation 1), and

$$\ell z_k = z_{k+1}^{-1}\ell z_{k+1} = \ell T(z_{k+1}) \in L. \tag{2.1}$$

It remains to show that $\ell R(z_{k+1}, w_{k+1}) \in L$ for any $z_{k+1}, w_{k+1} \in \mathcal{Z}_{k+1}$. To show this, we will use frequently that

$$(\ell, z_{k+1}) \in L' \quad \text{for any } \ell \in L \text{ and any } z_{k+1} \in \mathcal{Z}_{k+1}, \tag{2.2}$$

which follows from $(\ell, z_{k+1}) = z_k \in L$ and Lemma 2.1.

Let $\ell \in L$ and let $z_{k+1}, w_{k+1} \in \mathcal{Z}_{k+1}$. We have

$$\begin{aligned}
\ell z_{k+1} \cdot w_{k+1} &= \big[(z_{k+1}\ell)(\ell, z_{k+1})\big] w_{k+1} \\
&= s_1 z_{k+1}\ell \cdot w_{k+1} \quad s_1 \in L' \text{ by (2.2)} \\
&= s_1\big[(z_{k+1}\ell \cdot w_{k+1})\ell\big]\ell^{-1} \quad \text{diassociativity implies } ab \cdot b^{-1} = a \\
&\qquad \text{in a Moufang loop} \\
&= s_1\big[z_{k+1}(\ell w_{k+1}\ell)\big]\ell^{-1} \quad \text{using the right Moufang identity} \\
&= s_1 s_2\big[z_{k+1}(w_{k+1}\ell^2)\big]\ell^{-1} \quad \text{since } s_2 = (\ell, w_{k+1}) \in L' \text{ is central} \\
&= s_1 s_2 z_{k+1} w_{k+1} \cdot \ell \quad \text{since } \ell^2 \text{ is central} \\
&= s_1 s_2 s_3 \ell \cdot z_{k+1} w_{k+1} \quad s_3 = (z_{k+1}w_{k+1}, \ell), \text{ using (2.2) a final time.}
\end{aligned}$$

Thus $\ell R(z_{k+1}, w_{k+1}) = [(\ell z_{k+1})w_{k+1}](z_{k+1}w_{k+1})^{-1} = s_1 s_2 s_3 \ell \in L$, as desired. This completes the induction step and the proof. □

Corollary 2.6. *Torsion hypercentral units are trivial.*

Proof. Let $\tilde{z} \in \widetilde{\mathcal{Z}}(\mathcal{U})$ and suppose $(\tilde{z})^n = 1$ for some positive integer n. By Theorems 2.2 and 2.5, we can write $\tilde{z} = z\ell$, $z \in \mathcal{Z}(\mathcal{U})$, $\ell \in L$, and $z^n \ell^n = 1$. This gives $z^n \in L$, so $z \in \pm L$ by Lemma 2.3. Thus $\tilde{z} \in \pm L$, as claimed. □

Corollary 2.7. $\widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U})$.

Proof. It suffices to prove that $\mathcal{Z}_3 \subseteq \mathcal{Z}_2$, so take $z_3 \in \mathcal{Z}_3$ and $u \in \mathcal{U}$. In view of Theorems 2.2 and 2.5, we can write $z_3 = z\ell$, $z \in \mathcal{Z}(\mathcal{U})$, $\ell \in L$, so $(z_3, u) = (\ell, u) = z_2 \in \mathcal{Z}_2$. By (2.1), $(z_2, \ell) \in L$, so Lemma 2.1 gives $z_2\ell = \ell z_2 c$, with $c \in L'$ (hence $c^2 = 1$). Since ℓ^2 is central and $u^{-1}\ell u = \ell z_2$, $\ell^2 = u^{-1}\ell^2 u = \ell z_2 \ell z_2 = c\ell^2 z_2^2$, so $z_2^2 = c$ is trivial. Corollary 2.4 says $z_2 \in L' \subseteq \mathcal{Z}(L)$, so $z_3 \in \mathcal{Z}_2$. □

Corollary 2.8. *If $z_2 \in \widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U})$, then z_2^2 is central.*

Proof. Take any $\ell \in L$. By Theorem 2.5, $z_2^{-1}\ell^{-1}z_2 \in L$, so (z_2, ℓ) is in L, hence in L'. Write $z_2^{-1}\ell^{-1}z_2 = c\ell^{-1}$, $c \in L'$. Then $z_2^{-2}\ell^{-1}z_2^2 = c(z_2^{-1}\ell^{-1}z_2) = c^2\ell^{-1} = \ell^{-1}$. Thus z_2^2 commutes with ℓ^{-1} and hence with ℓ. Since any element that commutes elementwise with L is in the centre of $\mathrm{Z}L$, the proof is complete. □

Lemma 2.9. *If $u \in \widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U})$ and $v = 1 + n$, $n^2 = 0$, then $(u, v) = 1$.*

Proof. Since $u \in \mathcal{Z}_2(\mathcal{U})$, we have $(u^{-1}, v^{-1}) \in \mathcal{Z}(\mathcal{U})$, so $uvu^{-1} = cv$ for some $c \in \mathcal{Z}(\mathcal{U})$. By Corollary 2.8, u^2 is central, so $u^2vu^{-2} = v$, but also, $u^2vu^{-2} = u(cv)u^{-1} = c^2v$. Thus $c^2 = 1$, $uv^2u^{-1} = (uvu^{-1})^2 = c^2v^2 = v^2$, and $uv^2 = v^2u$. Since $v^2 = 1 + 2n$, it follows that u and n commute, so v and u commute. □

Lemma 2.10. *Let L be an RA loop with torsion subloop T. Let $\mathcal{U}=\mathcal{U}(\mathbb{Z}L)$ be the loop of units in $\mathbb{Z}L$. If $t\in T$ and $u\in\widetilde{\widetilde{\mathcal{Z}}}(\mathcal{U})=\mathcal{Z}_2(\mathcal{U})$, then $u^{-1}tu=t^{\pm1}$. In the case $u^{-1}tu=t^{-1}$, the order of t divides* 4.

Proof. Let $u\in\mathcal{Z}_2$ and $v\in\mathcal{U}$. Then $(u,v)=c\in\mathcal{Z}(\mathcal{U})$. As in Lemma 2.9, $c^2=1$, and $c\in L'$ by Corollary 2.4. Let $t\in T$ have order n and set $\hat{t}=1+t+t^2+\cdots+t^{n-1}$. Notice that $t\hat{t}=\hat{t}t=\hat{t}$. Let v be the unit $v=1+(1-t)u\hat{t}$. By Lemma 2.9, $(u,v)=1$, so

$$u(1-t)u\hat{t}=(1-t)u\hat{t}u. \tag{2.3}$$

By Theorems 2.2 and 2.5, (u,t) is in L, so it's in $L'=\{1,s\}$.

Suppose $(u,t)\neq 1$. Then $tu=sut$, so (2.3) and the fact that $t\hat{t}=\hat{t}$ give $u^2\hat{t}-su^2\hat{t}=u\hat{t}u-su\hat{t}u$, hence

$$u\hat{t}u^{-1}-su\hat{t}u^{-1}=\hat{t}-s\hat{t}. \tag{2.4}$$

Now $u\in\mathcal{Z}_2\subseteq\widetilde{\widetilde{\mathcal{Z}}}$, so u is in the normalizer of L in $\mathcal{U}$ by Theorem 2.5. Writing $\hat{t}$ as a sum of powers of t, each side of (2.4) is a sum of loop elements. Now st is one term in $s\hat{t}$ so either $st=t^i$ for some i or $st=sut^iu^{-1}$ for some i. In the first case, s is a power of t, so $u^{-1}tu=st$ is a power of t. In the second case $t=ut^iu^{-1}$, so again $u^{-1}tu$ is a power of t. In either case, s is a power of t and $u^{-1}tu=t^i$ for some i, $1\leqslant i<n=\mathrm{o}(t)$, the order of t.

Suppose $u^{-1}tu=t^i\notin\{t,t^{-1}\}$. Thus $1<i<n-1$, i is relatively prime to n, and $u^{-1}tu=st=t^{n/2+1}$ since $s\in\langle t\rangle$ has order 2. The element

$$b=\left(1+t+\cdots+t^{i-1}\right)^{\phi(n)}+\frac{1-i^{\phi(n)}}{n}\hat{t}$$

is a unit known as a *Bass cyclic unit* (see [6]) and it has infinite order [6, Proposition 8.1.12]. Now

$$u^{-1}bu=\left(1+t^i+\cdots+t^{i(i-1)}\right)^{\phi(n)}+\frac{1-i^{\phi(n)}}{n}\hat{t}$$

and, more generally,

$$\left(u^r\right)^{-1}bu^r=\left(1+t^{i^r}+\cdots+t^{i^r(i-1)}\right)^{\phi(n)}+\frac{1-i^{\phi(n)}}{n}\hat{t}.$$

It follows that

$$bb^ub^{u^2}\cdots b^{u^{\phi(n)-1}}=\left(1+t+\cdots+t^{i^{\phi(n)}-1}\right)^{\phi(n)}+m\hat{t}$$

for some integer m. But $(1+t+\cdots+t^{i^{\phi(n)}-1})^{\phi(n)}=(1+k\hat{t})^{\phi(n)}$ for some integer k, so

$$bb^ub^{u^2}\cdots b^{u^{\phi(n)-1}}=1+m_1\hat{t}$$

for some integer m_1. (See [6, Theorem 11.1.8] for more details.) Since b has augmentation 1, $m_1 = 0$ and

$$bb^u \cdots b^{u^{\phi(n)-1}} = 1. \tag{2.5}$$

Since $(u, b) \in L'$, by Lemma 2.1, each factor b^{u^k} is either b or sb. So Eq. (2.5) implies that a power of b is 1 or s. This contradicts the fact that b has infinite order and shows that $u^{-1}tu$ is indeed either t or t^{-1}.

Finally, in the case $u^{-1}tu = t^{-1}$, we have $(u, t^{-1}) = u^{-1}tut^{-1} = t^{-2}$, so $t^{-4} = (u, t^{-1})^2 = 1$ and $\mathrm{o}(t) \mid 4$. □

Lemma 2.11. *Let L be an RA loop with torsion subloop T. Let $\mathcal{U} = \mathcal{U}(\mathbb{Z}L)$ denote the unit loop of L in $\mathbb{Z}L$. If $t \in T$ and $\langle t\rangle$ is not normal in L, then $(u, \ell) = 1$ for every $u \in \widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U})$ and every $\ell \in L$. In particular, $\widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U}) = \mathcal{Z}(\mathcal{U})$.*

Proof. Let $u \in \mathcal{Z}_2(\mathcal{U})$. We use the fact that $s \notin \langle t\rangle$, an easy consequence of $\langle t\rangle$ being not normal. (See also [1, Corollary IV.1.11].)

First let $\ell \in L$ and assume $\ell t\ell^{-1} \notin \langle t\rangle$. Consider the unit $v = 1 + (1 - t)\ell\hat{t}$. By Lemma 2.9, we know that $(u, v) = 1$, so $u[(1 - t)\ell\hat{t}\,] = [(1 - t)\ell\hat{t}\,]u$, which gives

$$u(\ell\hat{t})u^{-1} - u(t\ell\hat{t})u^{-1} = \ell\hat{t} - t\ell\hat{t}.$$

Since $\ell t\ell^{-1} \notin \langle t\rangle$, $\mathrm{supp}(\ell\hat{t}) \cap \mathrm{supp}(t\ell\hat{t}) = \emptyset$. It follows (using Theorem 2.5) that $u\ell u^{-1}$, which is an element of L and in the support of the left-hand side, must equal ℓt^i for some i. But $u\ell u^{-1} = \ell$ or $s\ell$ (Theorem 2.5 and Lemma 2.1) and the latter contradicts $s \notin \langle t\rangle$. So $u\ell u^{-1} = \ell$ as desired.

Next, let $\ell \in L$ and assume this time that $\ell t\ell^{-1} \in \langle t\rangle$. Since $s \notin \langle t\rangle$, we know that $\ell t\ell^{-1} = t$. If ℓ is central, there is nothing to prove, so we may assume that ℓ is not central. Since t is also not central, the LC property tells us that $\ell = zt$ for some $z \in \mathcal{Z}(L)$. If $(t, u) = t^{-1}u^{-1}tu = s$, then, by Lemma 2.10, $s = 1$ or $s = t^{-2}$, contradicting $s \notin \langle t\rangle$. Since $(t, u) \in L'$, we must have $(t, u) = 1$, so $(\ell, u) = 1$ and we are done. □

Remark 2.12. Units of the type $v = 1 + (1 - t)\ell\hat{t}$ which appeared in the last proof, $\ell \in L$, t a torsion element of L, are called *bicyclic*. We refer the reader to either [1] or [6, Example 8.1.4] for more information about this important type of unit.

3. Proof of Theorem 1.1

In this section, we complete the proof of Theorem 1.1, first reminding the reader that $\widetilde{\mathcal{Z}}(\mathcal{U}) = \mathcal{Z}_2(\mathcal{U})$ was established in Corollary 2.7.

Some explanations of terminology may be helpful. A Moufang loop which is not a group is *Hamiltonian* if every subloop is normal. Such loops were classified by Norton [7] as precisely those which are direct products $\mathcal{C} \times E \times A$ with $\mathcal{C}$ the *Cayley loop* (a Moufang loop similar to 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. (See also [1, §II.4].) A Moufang loop is a 2-*loop* if each element has order a power of 2. In particular then, a Hamiltonian Moufang loop necessarily has exponent 4.

Assume now that L is an RA loop and $\widetilde{\mathcal{Z}}(\mathcal{U}) \neq \mathcal{Z}(\mathcal{U})$. Using Theorems 2.2 and 2.5 and the fact that $\mathcal{Z}(\mathcal{U}) \subseteq \widetilde{\mathcal{Z}}(\mathcal{U})$, there must exist $\ell_0 \in L$, $\ell_0 \in \widetilde{\mathcal{Z}}(\mathcal{U}) \setminus \mathcal{Z}(\mathcal{U})$. By Lemma 2.11, every subloop of T is normal in L so, in particular, T is either an Abelian group or a Hamiltonian Moufang (possibly associative) loop [1, §II.4].

Suppose T is Hamiltonian. If T is not a 2-loop, there exists a noncentral element $x \in T$ of order $4p$, p an odd prime. Since $o(x) \nmid 4$, Lemma 2.10 says that $\ell_0 x = x\ell_0$. Now the LC property in L, and the fact that neither x nor ℓ_0 is central, gives $x = \ell_0 z$ for some $z \in \mathcal{Z}(L)$. Thus $x \in \widetilde{\mathcal{Z}}(\mathcal{U}) \setminus \mathcal{Z}(\mathcal{U})$, so $x \in \mathcal{Z}_2(\mathcal{U}(\mathsf{Z}T)) \setminus \mathcal{Z}(\mathcal{U}(\mathsf{Z}T))$. Since T is a torsion RA loop, this contradicts Theorem 1.2. Thus T is indeed a 2-loop and hence of exponent 4. Remembering that $\langle t\rangle$ is normal in L, it follows that $\ell^{-1}t\ell = t^{\pm 1}$ for every $t \in T$ and every $\ell \in L$ (since any conjugate of t must have the same order as t). This completes the proof in one direction.

For the converse, first assume we are in case (i). Then [1, Corollary XII.2.14] tells us that $[\mathcal{U}(\mathsf{Z}L)]'$ has order 2, so $[\mathcal{U}(\mathsf{Z}L)]' = L' = \{1, s\}$ and, for any $u \in \mathcal{U} = \mathcal{U}(\mathsf{Z}L)$ and any $\ell \in L$, $\ell T(u) = u^{-1}\ell u = \ell$ or $s\ell$. Moreover, for any $u_1, u_2 \in \mathcal{U}$ and any $\ell \in L$,

$$\ell R(u_1, u_2) = (\ell u_1 \cdot u_2)(u_1u_2)^{-1} = \ell \text{ or } s\ell$$

because $\ell u_1 \cdot u_2 = \ell \cdot u_1u_2$ or $s\ell \cdot u_1u_2$. Clearly then L is normal in $\mathcal{U}$, so $\mathcal{U} = L \cdot \mathcal{Z}(\mathcal{U})$ by Theorem 2.2. Now choose $\ell_1 \in L \setminus \mathcal{Z}(L)$. Recalling that $L = \mathcal{Z}_2(L)$ (see Section 1), it follows that $\mathcal{U} = \mathcal{Z}_2(\mathcal{U})$ so $\ell_1 \in \mathcal{Z}_2(\mathcal{U}) \setminus \mathcal{Z}(\mathcal{U})$ and $\widetilde{\mathcal{Z}}(\mathcal{U}) \neq \mathcal{Z}(\mathcal{U})$.

Next, assume we are in case (ii). If T is central, then [1, Corollary XII.2.14] can be used again and we may complete the proof as in the preceding paragraph. So assume that T is not central and choose an element $t_0 \in T \setminus \mathcal{Z}(L)$. To complete the proof, it suffices to show that $t_0 \in \mathcal{Z}_2(\mathcal{U})$. For this, we must show that for any unit $u \in \mathcal{U}$, the commutator (t_0, u) is central and, for any units $u, v \in \mathcal{U}$, the three associators (u, v, t_0), (u, t_0, v), and (t_0, u, v) are central.

Let $A = T \cap \mathcal{Z}(L)$ and let $t \in T$. Since $tt_0 = t_0t$ (T is Abelian) and t_0 is not central, the LC property says that t is central (so $t \in A$) or $tt_0 = a \in A$ which implies $t = at_0^{-2}t_0 \in At_0$ since squares in L are central. It follows that $T = \langle t_0, A\rangle$ and (again using $t_0^2 \in A$) $T = \{at_0 \mid a \in A\}$. It follows that a unit in $\mathsf{Z}T$ has the form $u_0 + u_1t_0$, with $u_0, u_1 \in \mathsf{Z}A$ central. Since the conditions on T described in (ii) allow us to conclude that $\mathcal{U}(\mathsf{Z}L) = [\mathcal{U}(\mathsf{Z}T)]L$ [1, Proposition XII.1.3], every unit of $\mathsf{Z}L$ has the form $(u_0 + u_1t_0)\ell$, u_0, u_1 central and $\ell \in L$.

Let $u = (u_0 + u_1t_0)\ell$ be such a unit. Remembering that $\mathcal{U}$ is Moufang and hence diassociative, we have $ut_0 = u_0\ell t_0 + u_1t_0\ell t_0$ whereas $t_0u = u_0t_0\ell + u_1t_0^2\ell = ut_0(\ell, t_0)$. Thus

$$(u, t_0) = (\ell, t_0) \tag{3.1}$$

is in L' and so central as desired.

Now let $u = (u_0 + u_1t_0)\ell_1$ and $v = (v_0 + v_1t_0)\ell_2$, u_0, u_1, v_0, v_1 central, $\ell_1, \ell_2 \in L$, be units. We compute the associator (u, v, t_0).

To begin, we compute

$$uv\cdot t_0 = u_0v_0\ell_1\ell_2\cdot t_0 + u_0v_1(\ell_1\cdot t_0\ell_2)t_0 + u_1v_0(t_0\ell_1\cdot\ell_2)t_0 + u_1v_1(t_0\ell_1\cdot t_0\ell_2)t_0 \tag{3.2}$$

and

$$u\cdot vt_0 = u_0v_0\ell_1\cdot\ell_2t_0 + u_0v_1\ell_1(t_0\ell_2t_0) + u_1v_0(t_0\ell_1\cdot\ell_2t_0) + u_1v_1(t_0\ell_1)(t_0\ell_2t_0). \tag{3.3}$$

If ℓ_1, ℓ_2, t_0 associate, they generate a group (by Moufang's theorem) and $uv\cdot t_0 = u\cdot vt_0$. Thus we may assume that any associator of ℓ_1, ℓ_2, t_0 is s. In an RA loop, if two elements commute, they associate with any third element. It follows then that we may assume that the commutators (ℓ_1, t_0) and (ℓ_2, t_0) are each s as well, since if either is 1, then ℓ_1, ℓ_2, t_0 associate. We now examine the four terms on the right side of (3.2). We have

$$\begin{aligned}
\ell_1\ell_2\cdot t_0 &= s\ell_1\cdot\ell_2t_0,\\
(\ell_1\cdot t_0\ell_2)t_0 &= s(\ell_1t_0\cdot\ell_2)t_0\\
&= s\ell_1(t_0\cdot\ell_2t_0) \quad \text{by the right Moufang identity}\\
&= s\ell_1(t_0\ell_2t_0) \quad \text{by diassociativity,}\\
(t_0\ell_1\cdot\ell_2)t_0 &= s(t_0\cdot\ell_1\ell_2)t_0\\
&= st_0\ell_1\cdot\ell_2t_0 \quad \text{by middle Moufang and diassociativity,}
\end{aligned}$$

and

$$\begin{aligned}
(t_0\ell_1\cdot t_0\ell_2)t_0 &= s(t_0\ell_1\cdot\ell_2t_0)t_0\\
&= s\big[t_0(\ell_1\ell_2)t_0\big]t_0 \quad \text{by the middle Moufang identity}\\
&= t_0(\ell_1\cdot\ell_2t_0)t_0 \quad \text{using diassociativity to minimize parentheses}\\
&= st_0(\ell_1\cdot t_0\ell_2)t_0\\
&= s(t_0\ell_1)(t_0\ell_2t_0) \quad \text{by middle Moufang again.}
\end{aligned}$$

Comparing with (3.3) gives $uv\cdot t_0 = (u\cdot vt_0)s$, so $(u, v, t_0) = s$ is central.

Now the ring associator $[u, v, t_0] = uv\cdot t_0 - u\cdot vt_0 = u\cdot vt_0(s-1)$. Taking advantage of the alternating nature of associators in an alternative ring,

$$ut_0\cdot v - u\cdot t_0v = [u, t_0, v] = -[u, v, t_0] = u\cdot vt_0(1-s). \tag{3.4}$$

If v and t_0 were to commute, then ℓ_2 and t_0 would commute (as shown above—see (3.1)) and hence associate with every third element. It would follow that $(u, t_0, v) = 1$ is central.

Assume then that v and t_0 do not commute and, similarly, that u and t_0 do not commute. Thus $(u, t_0) = (\ell_1, t_0) = s$ by (3.1). Now (3.4) gives $ut_0 \cdot v - su \cdot vt_0 = u \cdot vt_0 - su \cdot vt_0$, so $ut_0 \cdot v = u \cdot vt_0 = su \cdot t_0 v$. Thus $(u, t_0, v) = s$ is central.

Finally (using $(u, t_0, v) = s$ and continuing to assume that $(u, t_0) = s$),

$$\begin{aligned} t_0 u \cdot v - t_0 \cdot uv = [t_0, u, v] = -[u, t_0, v] &= -ut_0 \cdot v + u \cdot t_0 v \\ &= -st_0 u \cdot v + u \cdot t_0 v = -st_0 u \cdot v + sut_0 \cdot v = -st_0 u \cdot v + t_0 u \cdot v, \end{aligned}$$

so $t_0 \cdot uv = st_0 u \cdot v$, giving $(t_0, u, v) = s^{-1} = s$. This completes the proof.

References

[1] E.G. Goodaire, E. Jespers, C. Polcino Milies, Alternative Loop Rings, North-Holland Math. Stud., vol. 184, Elsevier, Amsterdam, 1996.

[2] E.G. Goodaire, Y. Li, The normalizer conjecture in the alternative case, Algebra Colloq. 8 (4) (2001) 455–462.

[3] E.G. Goodaire, Alternative loop rings, Publ. Math. Debrecen 30 (1983) 31–38.

[4] E.G. Goodaire, D.A. Robinson, A class of loops with right alternative loop rings, Comm. Algebra 22 (14) (1995) 5623–5634.

[5] Y. Li, M.M. Parmenter, Some results on hypercentral units in integral group rings, Comm. Algebra 31 (7) (2003) 3207–3217.

[6] C. Polcino Milies, S.K. Sehgal, An Introduction to Group Rings, Algebras and Applications, Kluwer Academic, Dordrecht, 2002.

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

[8] H.O. Pflugfelder, Quasigroups and Loops: Introduction, Heldermann, Berlin, 1990.