Canad. Math. Bull. Vol. **52** (2), 2009 pp. 245–256

Involutions of RA Loops

Edgar G. Goodaire and César Polcino Milies

Abstract. Let L be an RA loop, that is, a loop whose loop ring over any coefficient ring R is an alternative, but not associative, ring. Let $\ell \mapsto \ell^\theta$ denote an involution on L and extend it linearly to the loop ring RL. An element $\alpha \in RL$ is *symmetric* if $\alpha^\theta = \alpha$ and *skew-symmetric* if $\alpha^\theta = -\alpha$. In this paper, we show that there exists an involution making the symmetric elements of RL commute if and only if the characteristic of R is 2 or θ is the canonical involution on L, and an involution making the skew-symmetric elements of RL commute if and only if the characteristic of R is 2 or 4.

1 Introduction

This is a contribution to the volume of recent papers that consider involutions of group rings and, specifically, the sets of elements that are symmetric [Cri, CM06, Lee03, Lee99, GSV98] or skew-symmetric [CM, JM05, GM03] relative to an involution. The twist here is that we focus attention on RA loops and their loop rings.

An RA or "ring alternative" loop is a loop for which the loop ring RL is alternative (but not associative) for any associative, commutative coefficient ring R with 1. If L is an RA loop, then L is Moufang and it has a unique nonidentity commutator/associator that we always denote s. Thus, if $a, b \in L$, then either $ba = ab$ or $ba = (ab)s$ and, if $a, b, c \in L$, either $ab \cdot c = a \cdot bc$ or $ab \cdot c = (a \cdot bc)s$. It is easy to see that $s \in \mathcal{Z}(L)$, the centre of L, and that s has order 2. For $\ell \in L$, define

$$\ell^* = \begin{cases} \ell & \text{if } \ell \in \mathcal{Z}(L) \\ s\ell & \text{otherwise.} \end{cases}$$

Then $\ell \mapsto \ell^*$ is an involution on L (that is, an antiautomorphism of order 2) that extends to the loop ring RL by linearity. We refer to $*$ as the *canonical involution* of L. *Diassociativity* is a fundamental property of Moufang loops and alternative rings; that is, the subloop (or subring) generated by any pair of elements is associative. More generally, if three elements of a Moufang loop (or alternative ring) associate, they generate a group (or an associative ring). One useful and important property of an RA loop is called *LC* for "lack of commutativity": if $a, b \in L$ and $ab = ba$, then at least one of a, b, ab is central; in particular squares in L are always central. The standard reference for the theory of RA loops and their alternative rings is [GJM96]. In this paper, we try also to quote the original literature wherever possible. For example, the LC property was established in [CG86], but one can also consult [GJM96, §4.2].

Received by the editors September 6, 2006; revised February 6, 2007.
This research was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada, by FAPESP, Proc. 2005/60411-8 and CNPq., Proc. 300243/79-0(RN) of Brasil.
AMS subject classification: Primary: 20N05; secondary: 17D05.

Any involution of an RA loop L extends by linearity to an involution of the loop ring RL. Throughout this paper, it is convenient to use the same label θ for such a map. Call $\alpha \in RL$ *symmetric* if $\alpha^\theta = \alpha$ and *skew-symmetric* if $\alpha^\theta = -\alpha$. Denote by L^+ and $(RL)^+$ the symmetric elements in L and RL, respectively, and by L^- and $(RL)^-$ the skew-symmetric elements of L and RL, respectively. Since s is the only nonidentity commutator in L, it is easy to see that this element must be symmetric.

The product of symmetric elements is symmetric if and only if, given $\alpha, \beta \in RL$ with $\alpha^\theta = \alpha$ and $\beta^\theta = \beta$, we have $(\alpha\beta)^\theta = \alpha\beta$. This occurs if and only if $\beta^\theta\alpha^\theta = \alpha\beta$, that is, if and only if $\beta\alpha = \alpha\beta$. Thus the symmetric elements of RL form a commutative set if and only if $(RL)^+$ is a subring. It is well known that the "bracket" operation $[a, b] = ab - ba$ turns an associative algebra into a Lie algebra. On an alternative algebra, the bracket induces the structure of a *Malcev* algebra, that is, an anticommutative algebra that satisfies the identity

$$(xy)(xz) = (xy \cdot z)x + (yz \cdot x)x + (zx \cdot x)y$$

[Sag61]. It follows that if RL is an alternative algebra, then RL^- is Malcev with respect to the bracket operation and, when $(RL)^-$ is commutative, this new product is clearly trivial. These two observations explain some of the interest in the commutativity of $(RL)^+$ and $(RL)^-$.

2 Skew-Symmetric Elements

Throughout this paper, θ denotes an involution of an RA loop L and (by linear extension) also on the alternative ring RL. In characteristic 2, elements that are skew or symmetric relative to θ coincide. Since we will investigate the commutativity of symmetric elements in characteristic 2 in the next section, we assume here that $\operatorname{char} R \neq 2$.

In what follows, we shall find it convenient to refer to the *support* of a loop ring element $\alpha = \sum_{\alpha_\ell \in R} \alpha_\ell \ell$, this being the set of those elements of L which actually appear in the sum: $\operatorname{supp}(\alpha) = \{\ell \in L \mid \alpha_\ell \neq 0\}$.

Suppose $\alpha = \sum \alpha_\ell \ell$ is a skew-symmetric element in the loop ring RL. Then

$$\sum \alpha_\ell \ell^\theta = \alpha^\theta = -\alpha = -\sum \alpha_\ell \ell.$$

Assume k is in the support of α. There are two possibilities. If $k^\theta = k$, then the coefficient of k in $-\sum \alpha_\ell \ell$ is $-\alpha_k$, whereas the coefficient of k in α^θ is α_k, so $2\alpha_k = 0$. If $k^\theta \neq k$, then there exists $\ell \in \operatorname{supp}(\alpha)$ such that $-\alpha_k k = \alpha_\ell \ell^\theta$. Thus $\ell^\theta = k$ (and $\ell = k^\theta$), so that $k \neq \ell$, and $\alpha_k = -\alpha_\ell$. So $\alpha_k k + \alpha_\ell \ell = -\alpha_\ell \ell^\theta + \alpha_\ell \ell = \alpha_\ell(\ell - \ell^\theta)$. It follows that $(RL)^-$ is spanned by the set $\mathcal{R} \cup \mathcal{S}$, where

$$\mathcal{R} = \{\alpha\ell \mid \ell \in L^+,\ 2\alpha = 0\} \quad \text{and} \quad \mathcal{S} = \{\ell - \ell^\theta \mid \ell \in L\}.$$

Proposition 2.1 *Let L be an RA loop and let θ denote an involution θ of L with the property that the set $(RL)^-$ of skew-symmetric elements commutes. For noncommuting elements $k, \ell \in L$, consider the conditions*

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

(a) $k^\theta = k$ *or* $\ell^\theta = \ell$ *or* $(k\ell)^\theta = k\ell$,
(b) $k\ell = \ell k^\theta = \ell^\theta k$ *or* $k\ell = \ell k^\theta = k^\theta \ell^\theta$ *or* $k\ell = \ell^\theta k = k^\theta \ell^\theta$.

If the coefficient ring R has characteristic different from 2, 3 *and* 4, *then condition* (a) *holds. If* char $R = 3$, *then* (a) *or* (b) *holds.*

Proof If $(RL)^-$ is commutative, so is $\mathcal{S}$, so

$$(k - k^\theta)(\ell - \ell^\theta) = (\ell - \ell^\theta)(k - k^\theta) \tag{2.1}$$

for any $k, \ell \in L$, that is,

$$k\ell + \ell k^\theta + \ell^\theta k + k^\theta \ell^\theta = \ell k + k\ell^\theta + k^\theta \ell + \ell^\theta k^\theta. \tag{2.2}$$

Suppose $k\ell \neq \ell k$. In characteristic different from 2, 3, 4, $k\ell$ is in the support of the left side, so it is in the support of the right. Thus $k\ell \in \{k\ell^\theta, k^\theta \ell, \ell^\theta k^\theta\}$, meaning that $k^\theta = k$ or $\ell^\theta = \ell$ or $k\ell = \ell^\theta k^\theta = (k\ell)^\theta$. If char $R = 3$, then, in addition, it is possible that $k\ell$ is not in the support of the left side. This occurs in exactly the three situations described by condition (b). ■

Lemma 2.2 *Let R be a coefficient ring of characteristic different from* 2 *and suppose* θ *is an involution of an RA loop L such that* $(RL)^-$ *is commutative. If* $a \in L$ *has the property that* $a^\theta = sa$, *then, for any* $b \in L$, *either* $b^\theta = b$ *or* $ab = ba$. *Thus,* $ab = ba$ *for every* $b \notin L^+$.

Proof Suppose $b \in L$ and $ab \neq ba$. The elements $a - a^\theta = (1 - s)a$ and $b - b^\theta$ commute, so

$$(1 - s)(ab - ab^\theta) = (1 - s)(ba - b^\theta a).$$

If a and b^θ commute, this becomes $(1-s)ab = (1-s)ba = (1-s)(sab) = -(1-s)ab$, which cannot happen. Thus $b^\theta a = sab^\theta$ and

$$(1 - s)(ab - ab^\theta) = (1 - s)(sab - sab^\theta) = -(1 - s)(ab - ab^\theta),$$

so $(1 - s)(ab - ab^\theta) = 0$. This says $ab + sab^\theta = sab + ab^\theta$. Since $ab \neq sab$, we have $ab = ab^\theta$ and hence $b^\theta = b$. ■

A fact about RA loops that is crucial in the proof of the proposition and theorem that follow is that an RA loop L cannot contain a commutative subloop of index 2. This is so because if B is a commutative subloop and $x \in L$, then $\langle B, x\rangle$ is a group [GM96], [GJM96, Corollary IV.2.4].

Proposition 2.3 *In characteristic different from* 2, *commutativity of* $(RL)^-$ *implies that* L^+ *is an abelian group.*

Proof Suppose there exist $x, y \in L^+$ with $xy \notin L^+$. Then $xy \neq (xy)^\theta = y^\theta x^\theta = yx$, so $yx = sxy$. Let $a = xy$. Then $a^\theta = sa$ and a is not central (x and y do not commute), so $C(a) = \{b \in L \mid ab = ba\}$ is proper and a subloop [GJM96, Corollary IV.1.15]. Let $b, c \in C(a)$. The LC property and $ab = ba$ imply that a is central or b is central or ab is central. Since a is not central, either b is central, or $ab = z$ for some $z \in \mathcal{Z}(L)$ giving that $b = a^{-2}za$ is a central multiple of a. Similarly, c is central or a central multiple of a. In all cases, we have $bc = cb$, so $C(a)$ is commutative. Suppose $w \notin C(a)$ and $t \notin C(a)$. By Lemma 2.2, $w = w^\theta$ and $t = t^\theta$, and a third appeal to Lemma 2.2 gives either $wt \in C(a)$ or $(wt)^\theta = wt$. Suppose $wt \notin C(a)$. Then $wt = t^\theta w^\theta = tw$, so t is central or w is central or wt is central. None of these possibilities actually occurs, however, because none of w, t, wt commute with a. Thus $wt = c \in C(a)$ and $t = w^{-2}cw \in C(a)w$. It follows that $C(a)$ has index 2. As noted prior to the statement of the proposition, this cannot occur in an RA loop because $C(a)$ is commutative. Thus L^+ is closed under multiplication, hence commutative and hence a group. (In an RA loop, if two elements commute, they associate with every third element [Goo83], [GJM96, Theorem IV.1.8].) ■

Theorem 2.4 *Let R be a coefficient ring of characteristic different from* 2 *and* 4*, and let θ be an involution of an RA loop L. Then $(RL)^-$ is not commutative.*

Proof We obtain the result by contradiction, assuming initially that $(RL)^-$ is indeed a commutative set.

Suppose first that char $R = 3$ and that there exist noncommuting elements $k, \ell \in L$ satisfying condition (b) of Proposition 2.1. The first set of equations, $k\ell = \ell k^\theta = \ell^\theta k$, imply $k^\theta = \ell^{-1}k\ell = sk$ and, similarly, that $\ell^\theta = s\ell$. The second set of equations, $k\ell = \ell k^\theta = k^\theta \ell^\theta$, imply $k^\theta = sk$ and $s\ell k = k\ell = (\ell k)^\theta$, and the third set of equations, $k\ell = \ell^\theta k = k^\theta \ell^\theta$, imply $\ell^\theta = s\ell$ and $(\ell k)^\theta = s\ell k$. Thus each alternative of (b) gives two noncommuting elements a and b with $a^\theta = sa$ and $b^\theta \neq b$, a situation in conflict with Lemma 2.2. We conclude that for every $k, \ell \in L$ with $k\ell \neq \ell k$, we have condition (a) of Proposition 2.1.

As in the proof of Proposition 2.3, we show that L contains a commutative subloop of index 2, which can never be the case for L an RA loop. The subloop A generated by $\mathcal{Z}(L)$ and L^+ is commutative by Proposition 2.3. Suppose $k, \ell \notin A$. If $k\ell = \ell k$, then $k\ell \in \mathcal{Z}(L) \subseteq A$ because L has LC and neither k nor ℓ is in $\mathcal{Z}(L)$. If $k\ell \neq \ell k$, then $k\ell \in L^+ \subseteq A$ because $k^\theta \neq k$ and $\ell^\theta \neq \ell$, and we know that condition (a) of Proposition 2.1 is the case. So, whether or not k and ℓ commute, $k\ell = a \in A$, so $\ell = k(k^{-2}a) \in kA$. Thus A has index 2. ■

2.1 Characteristic 4

When considering the commutativity of elements that are skew relative to some involution of an RA loop L, and in view of Theorem 2.4, it is clear that characteristic 4 is special because, in this case, the canonical involution on L makes $(RL)^-$ commutative. To see why, notice that $L^+ = \{\ell \in L \mid \ell^* = \ell\} = \mathcal{Z}(L)$, so the elements of $\mathcal{R} = \{\alpha\ell \mid \ell \in L^+,\ 2\alpha = 0\}$ are central. Also, if $k, \ell \in L$ and either of these elements is central, then $k^* = k$ or $\ell^* = \ell$ and (2.1) holds whereas, if neither k nor ℓ is central, then $k^* = sk$ and $\ell^* = s\ell$, the left side of (2.1) is $(1-s)^2 k\ell$ and the right side is $(1-s)^2\ell k$. The two sides are clearly equal if $k\ell = \ell k$; otherwise, $\ell k = sk\ell$, the right side is $-(1-s)^2 k\ell = (1-s)^2 k\ell$ since $2(1-s)^2 = 4 - 4s = 0$ and again the two sides are equal. In all situations, (2.1) holds, and the set $\mathcal{S} = \{\ell - \ell^\theta \mid \ell \in L\}$ is commutative, so $\mathcal{R} \cup \mathcal{S}$ and hence $(RL)^-$ are commutative as well.

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

Other involutions force commutativity of $(RL)^-$ as well in characteristic 4. See Example 2.10.

We proceed now towards a theorem giving necessary and sufficient conditions for $(RL)^-$ to be commutative in characteristic 4 (Theorem 2.8). Thus our underlying assumption is that R is a coefficient ring of characteristic 4 and that θ is an involution of an RA loop L for which $(RL)^-$ is commutative.

Suppose that for any $k \in L$, it is the case that $k^\theta \neq sk$. The first two lines of the proof of Proposition 2.3 show that L^+ is closed under multiplication and hence an abelian group. Moreover, for any $k, \ell \in L$ with $k\ell \neq \ell k$, $k\ell$ is in the support of the left hand side of equation (2.2) because the possibilities $k\ell = \ell k^\theta$, $k\ell = \ell^\theta k$, $k\ell = k^\theta \ell^\theta$ imply, respectively, $k^\theta = sk$, $\ell^\theta = s\ell$, $(\ell k)^\theta = s(\ell k)$. So for any $k, \ell \in L$ with $k\ell \neq \ell k$, we have $k\ell \in \{k\ell^\theta, k^\theta \ell, \ell^\theta k^\theta\}$, so $\ell^\theta = \ell$ or $k^\theta = k$ or $(k\ell)^\theta = k\ell$, these possibilities comprising condition (a) of Proposition 2.1. The last paragraph of the proof of Theorem 2.4 carries over verbatim to the present situation giving a commutative subloop of L of index 2, which cannot be the case.

The next lemma is now clear.

Lemma 2.5 *The loop L contains an element k with $k^\theta = sk$.*

Now take $k \in L$ with $k^\theta = sk$ and suppose $k\ell \neq \ell k$ for some $\ell \in L$. Commutativity of $k - k^\theta = k - sk$ and $\ell - \ell^\theta$ implies

$$(1 - s)(k\ell - k\ell^\theta) = (1 - s)(\ell k - \ell^\theta k). \tag{2.3}$$

If $k\ell^\theta = \ell^\theta k$, we are left with $(1 - s)k\ell = (1 - s)\ell k = -(1 - s)k\ell$, so $2(1 - s) = 0$, a contradiction. Thus $k\ell^\theta \neq \ell^\theta k$. This little argument establishes the next lemma.

Lemma 2.6 *If $k \in L$ satisfies $k^\theta = sk$, then $k\ell = \ell k$ for $\ell \in L$ if and only if $k\ell^\theta = \ell^\theta k$.*

Lemma 2.7 *For any $\ell \in L$, we have $\ell^\theta \in \{\ell, s\ell\}$.*

Proof By Lemma 2.5, the set $K = \{k \in L \mid k^\theta = sk\}$ is nonempty. We claim it is not central. Supposing otherwise, the first two lines of the proof of Proposition 2.3 show that L^+ is an abelian group. Then the argument establishing Lemma 2.5 shows that condition (a) of Proposition 2.1 holds for any k, ℓ with $k\ell \neq \ell k$ and the last paragraph of the proof of Theorem 2.4 produces a commutative subloop of index two in L, an impossibility. Thus we may fix a noncentral element $k \in K$.

Suppose $\ell \in L$ and $k\ell \neq \ell k$. Applying θ to $k\ell = s\ell k$ gives $\ell^\theta k^\theta = sk^\theta \ell^\theta = k\ell^\theta$, so $\ell^\theta k = sk\ell^\theta$ and (2.3) becomes

$$(1 - s)(k\ell - k\ell^\theta) = -(1 - s)(k\ell - k\ell^\theta),$$

giving $2(1 - s)(k\ell - k\ell^\theta) = 0$. This is $2k\ell + 2sk\ell^\theta = 2sk\ell + 2k\ell^\theta$. If $\ell \neq \ell^\theta$, then $k\ell$ is not in the support of the right side, so $k\ell = sk\ell^\theta$ implying $\ell^\theta = s\ell$.

Suppose $\ell \in L$ and $k\ell = \ell k$. Fix an element a with $ak \neq ka$ (so that $a^\theta = a$ or $a^\theta = sa$ by what we have already shown). In an RA loop, two commuting elements associate with every third, so parentheses are not needed when we record the fact that $(a\ell)k \neq k(a\ell)$ [GJM96, Theorem IV.1.8]. Using again what we have already learned about elements that do not commute with k, we have $\ell^\theta a^\theta = (a\ell)^\theta \in \{a\ell, sa\ell\}$, so $\ell^\theta \in \{\ell, s\ell\}$ too. ■

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

We have reached our main theorem about the commutativity of skew-symmetric elements in characteristic 4.

Theorem 2.8 *Suppose θ is an involution of an RA loop L and R is a coefficient ring of characteristic 4. Then the set $(RL)^-$ of skew-symmetric elements of RL is commutative if and only if elements of RL of the form $\alpha\ell$ with $\ell \in L^+$ and $2\alpha = 0$ commute and $k^\theta \in \{k, sk\}$ for each $k \in L$.*

Proof Recall that $(RL)^-$ is spanned by $\mathcal{R} \cup \mathcal{S}$, where

$$\mathcal{R} = \{\alpha\ell \mid \ell \in L^+,\ 2\alpha = 0\} \quad \text{and} \quad \mathcal{S} = \{\ell - \ell^\theta \mid \ell \in L\},$$

so that $(RL)^-$ is commutative if and only if $\mathcal{R}$ is commutative, $\mathcal{S}$ is commutative, and each element of $\mathcal{R}$ commutes with each element of $\mathcal{S}$. If $(RL)^-$ is commutative, then $k^\theta \in \{k, sk\}$ for any k by Lemma 2.7, so we have the theorem in one direction.

Conversely, assume that $\mathcal{R}$ is commutative and that $k^\theta \in \{k, sk\}$ for any $k \in L$. First we claim that $k - k^\theta$ and $\ell - \ell^\theta$ commute for any $k, \ell \in L$. This is clear if $k^\theta = k$ or $\ell^\theta = \ell$, so assume the contrary. Thus $k^\theta = sk$, $\ell^\theta = s\ell$ and $(k - k^\theta)(\ell - \ell^\theta) = (1 - s)^2 k\ell$ while

$$(\ell - \ell^\theta)(k - k^\theta) = (1 - s)^2 \ell k = \begin{cases} (1 - s)^2 k\ell & \text{if } k\ell = \ell k \\ -(1 - s)^2 k\ell & \text{if } k\ell = s\ell k. \end{cases}$$

Since $s^2 = 1$ and we work in characteristic 4, we have $(1 - s)^2 = 2 - 2s = -(2 - 2s) = -(1 - s)^2$. It follows that $\mathcal{S}$ is commutative. By assumption, $\mathcal{R}$ is commutative, so it remains to prove that each element of $\mathcal{R}$ commutes with each element of $\mathcal{S}$. So let $\alpha\ell \in \mathcal{R}$, $k - k^\theta = (1 - s)k \in \mathcal{S}$ and compare the elements

$$\alpha\ell(k - k^\theta) = \alpha(1 - s)\ell k \quad \text{and} \quad \alpha(k - k^\theta)\ell = \alpha(1 - s)k\ell.$$

These are certainly equal if $k\ell = \ell k$ whereas, if $\ell k = sk\ell$, the elements in question are $\alpha(1 - s)sk\ell = \alpha(s - 1)k\ell = -\alpha(1 - s)k\ell$ and $\alpha(1 - s)k\ell$. Again these are equal because $\alpha = -\alpha$. This completes the theorem. ∎

Remarks 2.9. (1) With reference to Theorem 2.8, suppose $\ell_1, \ell_2 \in L^+$ do not commute. Then $\ell_1\ell_2 - \ell_2\ell_1 = (1 - s)\ell_1\ell_2$. If $\alpha\ell_1, \beta\ell_2 \in \mathcal{R}$, then $0 = \alpha\beta(\ell_1\ell_2 - \ell_2\ell_1) = \alpha\beta(1 - s)\ell_1\ell_2$ and it follows that $\alpha\beta = 0$. So the condition that $\mathcal{R}$ be commutative is equivalent to the condition

- either L^+ is commutative or $\alpha, \beta \in R$ with $2\alpha = 2\beta = 0$ implies $\alpha\beta = 0$.

From this we see, for example, that $\mathcal{R}$ is commutative when the coefficient ring $R = Z_4$ is the ring of integers modulo 4 or, more generally, any ring that is free as a module over Z_4.

(2) We have observed that, in characteristic 4, the standard involution forces the skew-symmetric elements to commute. It is interesting to note that the converse is nearly satisfied in the sense that when the skew-symmetric elements commute, for each pair of elements $k, \ell \in L$ which do not commute and for which $k^\theta = sk$ and $\ell^\theta = s\ell$, the map θ is the restriction of the canonical involution to the group $\langle k, \ell\rangle$ generated by k and ℓ.

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

To see why, assume that $(RL)^-$ is commutative. By Theorem 2.8, $k^\theta \in \{k, sk\}$ and so $(k^2)^\theta = k^2$ for any $k \in L$. Let $k, \ell \in L$ with $k\ell \neq \ell k$, $k^\theta = sk$ and $\ell^\theta = s\ell$, and let $G = \langle k, \ell \rangle$. Since squares in L are central and since L has just one nonidentity (central) commutator/associator, any $g \in G$ can be written $g = zk$ or $g = z\ell$ or $g = zk\ell$ with $z \in \mathcal{Z}(G)$. Also, easily, $\mathcal{Z}(G) = \langle s, k^2, \ell^2 \rangle$. Thus θ is the identity on $\mathcal{Z}(G)$ and, since $\ell^\theta = \ell^*$, $k^\theta = k^*$ and $(k\ell)^\theta = \ell^\theta k^\theta = (s\ell)(sk) = \ell k = sk\ell = (k\ell)^*$, we have $\theta(w) = sw$ for $w \notin \mathcal{Z}(G)$. Thus θ is canonical on G.

Example 2.10. We offer an example of an involution of an RA loop different from the canonical involution, with $(RL)^-$ commutative and L^+ not commutative. Let $x, y, u \in L$ be elements which do not associate and let $G = \langle \mathcal{Z}(L), x, y \rangle$ be the subloop generated by x, y, and the centre of L. It is known that G is a group of index 2 in L and so $L = G \cup Gu$ [CG86, §3], [GJM96, Corollary IV.2.3]. The reader may check that the map $\theta\colon L \to L$ defined by $g^\theta = g^*$ and $(gu)^\theta = gu$ for $g \in G$ is an involution with $k^\theta \in \{k, sk\}$ for all $k \in L$. With $R = \mathbb{Z}_4$, the set $\mathcal{R}$ is commutative by the first of Remarks 2.9, so $(RL)^-$ is commutative by Theorem 2.8.

3 Symmetric Elements

In this section, we consider involutions that force the symmetric elements to commute. As with our considerations of skew-symmetric elements, characteristic is important. We have two theorems, according as the characteristic is or is not 2.

Theorem 3.1 *Let θ be an involution of an RA loop L. Assume R is a commutative associative ring with* 1 *and characteristic different from* 2*. Then the following are equivalent assertions.*

(1) *$(RL)^+$ is closed under multiplication.*
(2) *The elements of $(RL)^+$ commute.*
(3) *$(RL)^+ = \mathcal{Z}(RL)$, the centre of RL.*
(4) *$\theta = *$ is canonical.*

Proof This theorem and its proof are suggested by [JM06].

We noted the equivalence of (1) and (2) at the end of the introduction. That (3) implies (2) is trivial while (4) implies (3) is a known property of $*$ [GP87, Corollary 2.2], [GJM96, Corollary III.4.3] so, to complete the proof, it suffices to show that (2) implies (4).

So assume that the elements of $(RL)^+$ commute. Then the elements of

$$\mathcal{S} = L^+ \cup \{\ell + \ell^\theta \mid \ell \in L, \ell^\theta \neq \ell\}$$

commute because $\mathcal{S}$ spans $(RL)^+$. We claim that $L^+ \subseteq \mathcal{Z}(L)$. For this, take $\ell_0 \in L^+$ and $\ell \in L$. If $\ell \in L^+$, then $\ell_0\ell = \ell\ell_0$ because the elements of $\mathcal{S}$ commute. If $\ell \notin L^+$, then $\ell_0(\ell + \ell^\theta) = (\ell + \ell^\theta)\ell_0$ gives $\ell_0\ell \in \{\ell\ell_0, \ell^\theta\ell_0\}$. In the case $\ell_0\ell = \ell^\theta\ell_0$, we have $\ell_0\ell = \ell^\theta\ell_0 = \ell^\theta\ell_0^\theta = (\ell_0\ell)^\theta$ giving $\ell_0\ell \in L^+$. Since $\mathcal{S}$ is a commutative set, it follows that ℓ_0 commutes with $\ell_0\ell$, so ℓ_0 commutes with ℓ. In any case, ℓ_0 and ℓ commute, so $L^+ \subseteq \mathcal{Z}(L)$ as claimed.

Now let $k, \ell \in L$ with $k\ell \neq \ell k$. Thus neither k nor ℓ is central, so $k \notin L^+$, $\ell \notin L^+$ and $k + k^\theta$, $\ell + \ell^\theta$ must commute. We obtain

$$k\ell + k\ell^\theta + k^\theta\ell + k^\theta\ell^\theta = \ell k + \ell k^\theta + \ell^\theta k + \ell^\theta k^\theta \tag{3.1}$$

and claim that $k\ell$ is in the support of the left hand side. To see why, note that $k\ell \neq k\ell^\theta$ because ℓ is not central (hence not in L^+) and, similarly, $k\ell \neq k^\theta\ell$. So $k\ell$ is in the support of the left side with a coefficient of 1 or $2 \neq 0$, so $k\ell$ is in the support of the right side too. Thus $k\ell \in \{\ell k^\theta, \ell^\theta k, \ell^\theta k^\theta\}$.

If $k\ell = \ell^\theta k^\theta$, then $k\ell = (k\ell)^\theta$, so $k\ell \in L^+ \subseteq \mathcal{Z}(L)$, giving $k\ell = \ell k$ which is not true. So either $k\ell = \ell k^\theta$ or $k\ell = \ell^\theta k$.

Assume that $k\ell = \ell k^\theta$. Applying to $k\ell$ and ℓ what we have learned about non-commuting elements, we have $(k\ell)\ell = \ell(k\ell)^\theta$ or $(k\ell)\ell = \ell^\theta(k\ell)$. In the first case, $(k\ell)\ell = \ell(k\ell)^\theta = \ell\ell^\theta k^\theta$. (No parentheses are needed in the product $\ell\ell^\theta k^\theta$ because $\ell\ell^\theta \in L^+ \subseteq \mathcal{Z}(L)$ implies that ℓ and ℓ^θ commute and hence associate with every third element.) Moreover, $k\ell\ell = k^\theta\ell^\theta\ell$, so $k\ell = k^\theta\ell^\theta$. In the second case, $(k\ell)\ell = \ell^\theta(k\ell) = \ell^\theta\ell k^\theta$, so $\ell^2 k = k\ell^2 = \ell\ell^\theta k^\theta$ and $\ell k = \ell^\theta k^\theta$. Thus $k^\theta\ell^\theta = (\ell k)^\theta = k\ell$. In both cases, $k\ell = k^\theta\ell^\theta$. Thus $\ell k^\theta = k^\theta\ell^\theta = s\ell^\theta k^\theta$ giving $\ell^\theta = s\ell$. In passing, note too that the assumption of this paragraph gives $k^\theta = \ell^{-1}k\ell = sk$.

Similarly, if we assume $k\ell = \ell^\theta k$, we can again show that both $k^\theta = sk$ and $\ell^\theta = s\ell$. All this shows that if $k \notin \mathcal{Z}(L)$, then $k^\theta = sk$.

Now let ℓ be a central element of L and let k be any element which is not central. Then $k\ell \notin \mathcal{Z}(L)$, so $\ell^\theta k^\theta = (k\ell)^\theta = s(k\ell)$. Since $k^\theta = sk$, we have $\ell^\theta = \ell$. Thus $\theta = *$ is canonical. ■

Now we turn our attention to the case of characteristic 2, where the next theorem tells the story.

Theorem 3.2 *Suppose R is a commutative, associative coefficient ring with* 1 *and of characteristic* 2*, and L is an RA loop. Then there exists an involution θ of L which makes the set $(RL)^+$ of symmetric elements in RL commutative if and only if there exists a map $\varphi\colon L \to \mathcal{Z}(L)$ satisfying*

(i) *if $\varphi(\ell) = 1$, then $\ell \in \mathcal{Z}(L)$,*

(ii) *$\varphi(\ell)^2 = 1$ for all $\ell \in L$,*

(iii) $\varphi(k\ell) = \begin{cases} \varphi(k)\varphi(\ell) & \text{if } k\ell = \ell k \\ s\varphi(k)\varphi(\ell) & \text{if } k\ell \neq \ell k, \end{cases}$

(iv) *if $k\ell \neq \ell k$, then $\varphi(k) = s$ or $\varphi(\ell) = s$ or $\varphi(k) = \varphi(\ell)$,*

and $\ell^\theta = \varphi(\ell)\ell$ for all $\ell \in L$.

Proof We remind the reader that any involution of an RA loop must fix s, the unique nonidentity commutator/associator. As in Theorem 3.1, $(RL)^+$ is commutative if and only if

$$\mathcal{S} = L^+ \cup \{\ell + \ell^\theta \mid \ell \in L, \ell^\theta \neq \ell\}$$

is a commutative set.

Suppose there exists a map $L \to \mathcal{Z}(L)$ with the indicated properties. It is straightforward to check that the map $\theta\colon L \to L$ defined by $\ell^\theta = \varphi(\ell)\ell$ is an involution. If

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

$\ell \in L^+$, then $\ell^\theta = \ell$ so $\varphi(\ell) = 1$ and ℓ is central so, to show that $(RL)^+$ is commutative, we have only to show that two elements of the form $k + k^\theta$, $k \notin L^+$, commute; that is, for $k, \ell \notin L^+$,

$$k\ell + k\ell^\theta + k^\theta \ell + k^\theta \ell^\theta = \ell k + \ell k^\theta + \ell^\theta k + \ell^\theta k^\theta.$$

This is

$$k\ell + \varphi(\ell)k\ell + \varphi(k)k\ell + \varphi(k)\varphi(\ell)k\ell = \ell k + \varphi(k)\ell k + \varphi(\ell)\ell k + \varphi(k)\varphi(\ell)\ell k. \tag{3.2}$$

This equation is obviously satisfied if k and ℓ commute. We use condition (iv) to show that it also holds if they do not. For example, if $k\ell \neq \ell k$ and $\varphi(k) = s$, using $\ell k = sk\ell$, equation (3.2) reads

$$k\ell + \varphi(\ell)k\ell + sk\ell + s\varphi(\ell)k\ell = sk\ell + k\ell + s\varphi(\ell)k\ell + \varphi(\ell)k\ell.$$

The situation is similar if $\varphi(\ell) = s$. Finally, if $k\ell \neq \ell k$ and $\varphi(k) = \varphi(\ell)$, then $\varphi(k)\varphi(\ell) = 1$ by condition (ii), and (3.2) reads

$$k\ell + \varphi(k)k\ell + \varphi(k)k\ell + k\ell = \ell k + \varphi(k)\ell k + \varphi(k)\ell k + \ell k.$$

In characteristic 2, each side is 0, so we have established sufficiency.

For necessity, we suppose that θ is an involution of L with the property that $(RL)^+$ and hence $\mathcal{S}$ are commutative sets. As in Theorem 3.1, $L^+ \subseteq \mathcal{Z}(L)$ because the argument used previously was characteristic independent. Thus $\ell\ell^\theta \in \mathcal{Z}(L)$ for any $\ell \in L$ and, since $\ell^{-1} = \ell^{-2}\ell$ with ℓ^{-2} central, $\ell^\theta = \varphi(\ell)\ell$ for some $\varphi(\ell) \in \mathcal{Z}(L)$. If $\varphi(\ell) = 1$, then $\ell \in L^+ \subseteq \mathcal{Z}(L)$ giving statement (i).

Towards the proof of statement (ii), note first that for any $k, \ell \in L$ that do not commute, we have

$$k\ell + k\ell^\theta + k^\theta \ell + k^\theta \ell^\theta = \ell k + \ell k^\theta + \ell^\theta k + \ell^\theta k^\theta,$$

just as in Theorem 3.1. This shows that if $\ell \in L$ is not central and $k \in L$ does not commute with ℓ, then

$$k\ell \in \{k^\theta \ell^\theta, \ell k^\theta, \ell^\theta k\}. \tag{3.3}$$

In what follows, we use implicitly that ℓ, ℓ^θ, and k associate for any $k, \ell \in L$ (because centrality of $\ell\ell^\theta$ implies that ℓ and ℓ^θ commute).

Case 1 Assume first that $k\ell = k^\theta \ell^\theta$. Then $\ell^\theta k^\theta = \ell k$, and (3.1) becomes

$$k\ell^\theta + k^\theta \ell = \ell k^\theta + \ell^\theta k. \tag{3.4}$$

Now k and ℓ^θ cannot commute, for otherwise, $k\ell^\theta \ell = \ell^\theta k\ell$, so $\ell^\theta \ell k = \ell^\theta k\ell$ implying $k\ell = \ell k$, which is not true. Thus (3.4) yields either $k\ell^\theta = k^\theta \ell$ and $\ell k^\theta = \ell^\theta k$ or $k\ell^\theta = \ell k^\theta = (k\ell^\theta)^\theta$. The latter implies $k\ell^\theta \in L^+ \subseteq \mathcal{Z}(L)$ giving that k and ℓ^θ commute, which is not true. So we must have $k\ell^\theta = k^\theta \ell$, which says $k^\theta = k\ell^\theta \ell^{-1}$, $k\ell = k^\theta \ell^\theta = (k\ell^\theta \ell^{-1})\ell^\theta$, $\ell = \ell^\theta \ell^{-1} \ell^\theta = (\ell^\theta)^2 \ell^{-1}$ and $(\ell^2)^\theta = (\ell^\theta)^2 = \ell^2$; that is, $\ell^2 \in L^+$.

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

Case 2 Assume that $k\ell = \ell k^\theta$. Then $k^\theta = \ell^{-1}k\ell = sk$, implying $(k^2)^\theta = (k^\theta)^2 = s^2k^2 = k^2$, that is, $k^2 \in L^+$. Now k and ℓ^θ do not commute; otherwise, $(k\ell^\theta)^\theta = (\ell^\theta k)^\theta$, hence $k\ell = \ell k^\theta = k^\theta \ell$, and $k \in L^+$ is central. Now apply (3.3) to the noncommuting elements $k\ell$ and ℓ, obtaining

$$(k\ell)\ell \in \{(k\ell)^\theta \ell^\theta, \ell(k\ell)^\theta, \ell^\theta(k\ell)\}.$$

There are three possibilities.

(i) If $(k\ell)\ell = (k\ell)^\theta\ell^\theta$, then $k\ell^2 = \ell^\theta k^\theta \ell^\theta = s\ell^\theta k\ell^\theta = k(\ell^\theta)^2 = k(\ell^2)^\theta$, so $\ell^2 \in L^+$.

(ii) If $(k\ell)\ell = \ell(k\ell)^\theta$, then $k\ell^2 = \ell\ell^\theta k^\theta = k^\theta\ell\ell^\theta = sk\ell\ell^\theta$ so $\ell^\theta = s\ell$ and $(\ell^2)^\theta = (\ell^\theta)^2 = s^2\ell^2 = \ell^2$. Again $\ell^2 \in L^+$.

(iii) If $(k\ell)\ell = \ell^\theta k\ell$, then $k\ell = \ell^\theta k$, so $\ell^\theta = k\ell k^{-1} = s\ell$ giving, again, $\ell^2 \in L^+$.

Case 3 Suppose $k\ell = \ell^\theta k$. Then $s\ell k = k\ell = \ell^\theta k$, so $\ell^\theta = s\ell$, giving $\ell^2 \in L^+$.

In all three cases, we have $\ell^2 \in L^+$, showing that squares of noncentral elements are fixed by θ. On the other hand, if $x \in \mathcal{Z}(L)$ and $\ell \notin \mathcal{Z}(L)$ is arbitrary, then $\ell x \notin \mathcal{Z}(L)$, so $[(\ell x)^2]^\theta = (\ell x)^2$, that is, $(\ell^2x^2)^\theta = \ell^2x^2 = (\ell^2)^\theta(x^2)^\theta$. Since $(\ell^2)^\theta = \ell^2$, we have $(x^2)^\theta = x^2$ too. Thus any square is fixed by θ.

Now remember that $\varphi(\ell)$ was defined by $\ell^\theta = \varphi(\ell)\ell$ and $\varphi(\ell)$ is central. Thus $\ell^2 \in L^+$ implies $\ell^2 = (\ell^\theta)^2 = \varphi(\ell)^2\ell^2$, so $\varphi(\ell)^2 = 1$, which is statement (ii).

Furthermore, if $k\ell = \ell k$, then $\varphi(k\ell)k\ell = (k\ell)^\theta = k^\theta\ell^\theta = \varphi(k)\varphi(\ell)k\ell$, so $\varphi(k\ell) = \varphi(k)\varphi(\ell)$. On the other hand, if $k\ell \neq \ell k$, then $k\ell = s\ell k$ gives $\varphi(k\ell)(k\ell) = (k\ell)^\theta = (s\ell k)^\theta = sk^\theta\ell^\theta = s\varphi(k)\varphi(\ell)k\ell$, hence $\varphi(k\ell) = s\varphi(k)\varphi(\ell)$. So we have statement (iii).

Finally, if k and ℓ do not commute, we have (3.3) and three possibilities. If $k\ell = k^\theta\ell^\theta$, then $\varphi(k)\varphi(\ell) = 1$, so $\varphi(k) = \varphi(\ell)$ because of (ii). If $k\ell = \ell k^\theta = \varphi(k)sk\ell$, then $\varphi(k) = s$, while, if $k\ell = \ell^\theta k = \varphi(\ell)sk\ell$, we have $\varphi(\ell) = s$. Thus statement (iv) holds and the proof is complete. ■

Examples 3.3. As noted in Section 2, an RA loop L is generated by its centre and three elements x, y, u which do not associate. Since squares are central, each element of L can be written in the form zw, where $z \in \mathcal{Z}(L)$ and $w \in W = \{x, y, u, xy, xu, yu, (xy)u\}$. Moreover, since $w_1^{-1}w_2 \notin \mathcal{Z}(L)$ for distinct $w_1, w_2 \in W$, the elements z and w in the representation zw are unique. Suppose $\varphi\colon L \to \mathcal{Z}(L)$ satisfies properties i–iv of Theorem 3.2 and $\mathcal{Z}(L)$ is cyclic of order a power of 2. (For example, L could be an indecomposable loop in classes $\mathcal{L}_1$ or $\mathcal{L}_2$—see [GJM96, Chapter V].) Then s is the unique element of order 2 in the centre so, if $\ell \notin \mathcal{Z}(L)$, $\varphi(\ell) = s$ because $\varphi(\ell)$ has order 2. It follows readily that $\varphi(a) = 1$ if $a \in \mathcal{Z}(L)$, so $\theta = *$ is the canonical involution on L.

We claim that in any other situation, that is, where $\mathcal{Z}(L)$ contains an element $t \neq s$ of order 2, there are other maps φ satisfying the conditions of Theorem 3.2 and hence involutions θ other than the canonical one that force the symmetric elements to commute. Specifically, let $\varphi(a) = 1$ for $a \in \mathcal{Z}(L)$, choose $\varphi(x)$, $\varphi(y)$ and $\varphi(u)$ arbitrarily in $\{s, t\}$ (but not all s), extend φ to W by the rule $\varphi(w_1w_2) = s\varphi(w_1)\varphi(w_2)$, and then to L via the rule $\varphi(zw) = \varphi(w)$, for $z \in \mathcal{Z}(L)$, $w \in W$. One such φ is defined by the table

w	x	y	u	xy	xu	yu	$(xy)u$
$\varphi(w)$	s	t	s	t	s	t	t

.

https://doi.org/10.4153/CMB-2009-027-0 Published online by Cambridge University Press

It is straightforward to check that $\varphi(w_1 w_2) = s\varphi(w_1)\varphi(w_2)$ for any $w_1, w_2 \in W$, $w_1 \neq w_2$. For example, if $w_1 = xy$ and $w_2 = yu$, using the fact that xy, y, and u do not associate (otherwise, they would generate a group containing x, y, and u) we have $w_1 w_2 = (xy)(yu) = s(xy \cdot y)u = s(xy^2)u = (sy^2)xu$ with sy^2 central. So $\varphi(w_1 w_2) = \varphi(xu) = s$. On the other hand, $\varphi(w_1)\varphi(w_2) = ts$, so $\varphi(w_1 w_2) = s\varphi(w_1)\varphi(w_2)$. Now $z_1 w_1$ and $z_2 w_2$ commute if and only if $w_1 = 1$ or $w_2 = 1$ or $w_1 = w_2 \in W$, so φ indeed has the properties of Theorem 3.2 and the corresponding map θ is an involution of L, different from $*$, with the property that the symmetric elements of RL commute.

Theorem 3.4 *Let L be an RA loop and let R be an associative, commutative ring of coefficients with characteristic* 2*. The canonical involution $\ell \mapsto \ell^*$ has the property that the symmetric elements of RL commute. There exist other involutions with this property if and only if $\mathcal{Z}(L)$ contains more than one element of order* 2*.*

Proof We have just constructed a noncanonical involution with $(RL)^+$ commutative assuming $\mathcal{Z}(L)$ contains an element $t \neq s$ of order 2. Conversely, if s is the only element of order 2 in $\mathcal{Z}(L)$, then statement (ii) of Theorem 3.2 says $\varphi(\ell) \in \{1, s\}$ for any $\ell \in L$ and then statements (i) and (iv) say that $\varphi(\ell) = s$ for any $\ell \notin \mathcal{Z}(L)$. This implies that if $\ell \notin \mathcal{Z}(L)$, then $\varphi(\ell) = 1$: take $k \notin \mathcal{Z}(L)$; then $k\ell \notin \mathcal{Z}(L)$, so $s = \varphi(k\ell) = \varphi(k)\varphi(\ell) = s\varphi(\ell)$. So the involution θ defined by $\ell^\theta = \varphi(\ell)\ell$ is canonical. ■

Acknowledgements This paper was read carefully by a referee who was clearly interested in our work. We are grateful for the help and have tried to follow all suggestions in the report. The first author wishes to thank FAPESP of Brasil and the Instituto de Matemática e Estatística of the Universidade de São Paulo for their support and hospitality.

References

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

[CM] O. Broche Cristo and C. Polcino Milies, *Commutativity of skew symmetric elements in group rings.* Proc. Edinb. Math. Soc. **50**(2007), no. 1, 37–47.

[CM06] O. Broche Cristo and M. Ruiz Marín, *Lie identities in symmetric elements in group rings: a survey.* In: Groups, rings and group rings, Lecture Notes in Pure and Applied Mathematics 248, Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 43–55.

[Cri] O. Broche Cristo, *Commutativity of symmetric elements in group rings.* J. Group Theory, **9**(2006), no. 5, 673–683.

[GJM96] E. G. Goodaire, E. Jespers, and C. Polcino Milies, *Alternative loop rings.* North-Holland Mathematics Studies 184, North-Holland, Amsterdam, 1996.

[GM96] E. G. Goodaire and C. Polcino Milies, *Finite conjugacy in alternative loop algebras.* Comm. Algebra **24**(1996), no. 3, 881–889.

[GM03] A. Giambruno and C. Polcino Milies, *Unitary units and skew elements in group algebras.* Manuscripta Math. **111**(2003), no. 2, 195–209.

[Goo83] E. G. Goodaire, *Alternative loop rings.* Publ. Math. Debrecen **30**(1983), no. 1-2, 31–38.

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

[GSV98] A. Giambruno, S. K. Sehgal, and A. Valenti, *Symmetric units and group identities.* Manuscripta Math. **96**(1998), no. 4, 443–461.

[JM05] E. Jespers and M. Ruiz Marín, *Antisymmetric elements in group rings.* J. Algebra Appl. **4**(2005), no. 4, 341–353.

[JM06] ______, *On symmetric elements and symmetric units in group rings.* Comm. Algebra **34**(2006), no. 2, 727–736.
[Lee99] G. T. Lee, *Group rings whose symmetric elements are Lie nilpotent.* Proc. Amer. Math. Soc. **127**(1999), no. 11, 3153–3159.
[Lee03] ______, *Nilpotent symmetric units in group rings.* Comm. Algebra **31**(2003), no. 2, 581–608.
[Sag61] A. A. Sagle, *Malcev algebras.* Trans. Amer. Math. Soc. **101**(1961), 426–458.

Memorial University of Newfoundland, St. John's, Newfoundland A1C 5S7, Canada
e-mail: edgar@mun.ca

Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66.281, CEP 05314-970, São Paulo SP, Brasil
e-mail: polcino@ime.usp.br