Canad. Math. Bull. Vol. **56** (2), 2013 pp. 344–353
http://dx.doi.org/10.4153/CMB-2011-178-2

Involutions and Anticommutativity in Group Rings

Edgar G. Goodaire and César Polcino Milies

Abstract. Let $g \mapsto g^*$ denote an involution on a group G. For any (commutative, associative) ring R (with 1), $*$ extends linearly to an involution of the group ring RG. An element $\alpha \in RG$ is *symmetric* if $\alpha^* = \alpha$ and *skew-symmetric* if $\alpha^* = -\alpha$. The skew-symmetric elements are closed under the Lie bracket, $[\alpha, \beta] = \alpha\beta - \beta\alpha$. In this paper, we investigate when this set is also closed under the ring product in RG. The symmetric elements are closed under the Jordan product, $\alpha \circ \beta = \alpha\beta + \beta\alpha$. Here, we determine when this product is trivial. These two problems are analogues of problems about the skew-symmetric and symmetric elements in group rings that have received a lot of attention.

1 Introduction

In this paper, as usual, RG denotes the group ring of a group G over a commutative associative ring R with 1 and *involution* means an antiautomorphism of order 2. An involution $g \mapsto g^*$ on G extends to RG in an obvious way: for $\alpha = \sum \alpha_g g \in RG$, $\alpha^* = \sum \alpha_g g^*$. Throughout this paper, all involutions on RG will be of this type.

An element $\alpha \in RG$ is *symmetric* if $\alpha^* = \alpha$ and *skew-symmetric* (sometimes we abbreviate to *skew*) if $\alpha^* = -\alpha$. By $(RG)^+$ and G^+, we mean the sets of symmetric elements of RG and G, respectively, whereas, we use the notation $(RG)^-$ and G^- for the respective sets of skew-symmetric elements.

In recent years there has been increasing interest in problems regarding the properties of RG as a ring with involution. See, for example, [6,8–10,12,13,19–21] and the rather fundamental paper [7]. The monograph [18] highlights many recent results in this growing field. Notice that the product of symmetric elements in RG is symmetric if and only if, given $\alpha, \beta \in RG$ with $\alpha^* = \alpha$ and $\beta^* = \beta$, we have $(\alpha\beta)^* = \alpha\beta$. This occurs if and only if $\beta^*\alpha^* = \alpha\beta$, that is, if and only if $\beta\alpha = \alpha\beta$. Thus the symmetric elements of RG form a subring of RG if and only if they commute. This question has been studied by several authors [2, 11, 17].

Notice too that the set $(RG)^-$ is closed under the Lie bracket $[\alpha, \beta] = \alpha\beta - \beta\alpha$, and this Lie bracket is trivial if and only if for $\alpha, \beta \in (RG)^-$, $\alpha\beta - \beta\alpha = 0$, that is, if and only if the skew-symmetric elements commute. This problem has also received much attention [3–6, 16].

In this paper we consider two problems related to these. First we address the question of when the skew-symmetric elements of RG form a subring, that is, when

Received by the editors November 18, 2010.
Published electronically September 15, 2011.
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.
This research was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada, by FAPESP, Proc. 2004/15319-3 and 2008/57553-3, and by CNPq., Proc. 300243/79-0(RN) of Brasil.
AMS subject classification: **16W10**, 16S34.

does $\alpha, \beta \in (RG)^-$ imply that $\alpha\beta$ is also in $(RG)^-$? Clearly the answer is if and only if $(\alpha\beta)^* = -\alpha\beta$, that is, if and only if $\beta^*\alpha^* = (-\beta)(-\alpha) = -\alpha\beta$. So $(RG)^-$ is a subring if and only if the skew-symmetric elements anticommute.

The set $(RG)^+$ is closed under the Jordan product, $\alpha \circ \beta = \alpha\beta + \beta\alpha$. Clearly this product is trivial if and only if the symmetric elements anticommute. This is a second situation we study, and resolve, in this paper.

In what follows, we shall find it convenient to refer to the "support" of elements in a group ring. The *support* of $\alpha = \sum_{\alpha_g \in R} \alpha_g g$, denoted $\operatorname{supp}(\alpha)$, is the set of group elements which actually appear in the representation of α, that is, with nonzero coefficients: $\operatorname{supp}(\alpha) = \{g \in G \mid \alpha_g \neq 0\}$.

2 When is $(RG)^-$ a Subring?

Let $g \mapsto g^*$ be any involution of a group G and extend linearly to an involution of RG. In this section, we classify the groups G for which the set $(RG)^-$ of elements that are skew-symmetric relative to $*$ is a subring of RG. As we know, this problem is equivalent to determining when the skew-symmetric elements of RG anticommute.

Suppose $\alpha = \sum \alpha_g g$ is skew-symmetric. Then

$$\sum \alpha_g g^* = \alpha^* = -\alpha = -\sum \alpha_g g$$

and, for an element $k \in \operatorname{supp}(\alpha)$, there are two possibilities. If $k^* = k$, then the coefficient of k in $-\sum \alpha_g g$ is $-\alpha_k$, whereas the coefficient of k in α^* is α_k, so $2\alpha_k = 0$. If $k^* \neq k$, then there exists $g \in \operatorname{supp}(\alpha)$ such that $-\alpha_k k = \alpha_g g^*$. Thus $g^* = k$ (and $g = k^*$), so that $k \neq g$, and $\alpha_k = -\alpha_g$. So $\alpha_k k + \alpha_g g = -\alpha_g g^* + \alpha_g g = \alpha_g(g - g^*)$. It follows that $(RG)^-$ is spanned by the set $\mathcal{R} \cup \mathcal{S}$, where

$$\mathcal{R} = \{\alpha g \mid g \in G^+,\ 2\alpha = 0\} \quad \text{and} \quad \mathcal{S} = \{g - g^* \mid g \in G\}. \tag{2.1}$$

Obviously, the skew-symmetric elements of RG anticommute if and only if the elements of $\mathcal{R} \cup \mathcal{S}$ anticommute.

We begin with a lemma.

Lemma 2.1 *Let $g \mapsto g^*$ denote an involution of a group G and let $*$ also denote the linear extension to RG. If the elements of RG that are skew-symmetric relative to $*$ anticommute, then one of the following holds:*

(i) *the characteristic of R is 2,*
(ii) *the characteristic of R is 4 and $gg^* = g^*g$ and $(g^*)^2 = g^2$ for all $g \in G$,*
(iii) *G is abelian and $*$ is the identity on G.*

Proof Suppose $\operatorname{char} R \neq 2$. For any $g \in G$, $g - g^*$ and $g^* - g$ anticommute if and only if $(g - g^*)(g^* - g) = -(g^* - g)(g - g^*)$, that is, if and only if

$$gg^* + g^*g + g^*g + gg^* = g^2 + (g^*)^2 + g^2 + (g^*)^2,$$

which reads

$$2gg^* + 2g^*g = 2g^2 + 2(g^*)^2. \tag{2.2}$$

https://doi.org/10.4153/CMB-2011-178-2 Published online by Cambridge University Press

Suppose $*$ is not the identity map and let $g \in G$ with $g^* \neq g$. Then gg^* is not in the support of the right side of this equation, so it is not in the support of the left side. This implies $gg^* = g^*g$ and $4gg^* = 0$, so char $R = 4$ and $g^2 = (g^*)^2$ too. Now let g be any element of G. Equation (2.2) implies that $gg^* = g^*g$ or $gg^* = g^2$ (so $g = g^*$) or $gg^* = (g^*)^2$ (so $g = g^*$). In all cases, $gg^* = g^*g$, the left side of (2.2) is 0 and $g^2 = (g^*)^2$ as well.

Finally, we note that the identity map on a group G is an involution only if G is abelian, giving case (iii) and the desired result. ■

In characteristic 2, skew elements are symmetric and anticommutativity is commutativity, so the groups in which the skew-symmetric elements anticommute are known [17, Theorem 3.3].

If $4 \neq 0$, G is abelian, and $*$ is the identity, then $g - g^* = 0$ for any $g \in G$, so, with reference to the definitions in (2.1), the elements of $\mathcal{S}$ most certainly anticommute with each other and also with elements of $\mathcal{R}$. Elements of $\mathcal{R}$ anticommute because if $2\alpha = 0$, $(\alpha g)(\beta h) + (\beta h)(\alpha g) = 2\alpha\beta gh = 0$.

These remarks and Lemma 2.1 classify the groups G for which $(RG)^-$ is a subring except in the case of characteristic 4. This case is more difficult and settled with the next theorem.

Theorem 2.2 *Let G be a group with an involution $*$ and let R be a coefficient ring of characteristic 4. Then the set $(RG)^-$ of elements that are skew-symmetric with respect to $*$ forms a subring of RG if and only if either*

(i) *G is an abelian group and there exists $s \in G$ with $s^2 = 1$ and $g^* = g$ or sg for all $g \in G$ (this includes the possibility that $*$ is the identity on G) or*

(ii) *G is a nonabelian group with a unique nonidentity commutator, s, for every $g \in G$, $g^* = g$ or sg, and either symmetric group elements commute or whenever $\alpha, \beta \in R$ satisfy $2\alpha = 2\beta = 0$, then $\alpha\beta = 0$.*

Proof Suppose first that $(RG)^-$ is a subring of RG and let g and h be elements of G. Then $g - g^*$ and $h - h^*$ anticommute, that is, $(g - g^*)(h - h^*) = -(h - h^*)(g - g^*)$, so

$$gh + g^*h^* + hg + h^*g^* = h^*g + hg^* + gh^* + g^*h. \tag{2.3}$$

We first suppose that G is abelian. In this case, (2.3) reads

$$2gh + 2g^*h^* = 2gh^* + 2g^*h. \tag{2.4}$$

If $*$ is the identity map on G, there is nothing to do, so assume this is not the case and let $g, h \in G$ with $g^* \neq g$ and $h^* \neq h$. Then gh is not in the support of the right side of (2.4), so the only possibility is $gh = g^*h^*$ and $gh^* = g^*h$. The second equation gives $g^{-1}g^* = h^*h^{-1}$. Fixing g with $g^* \neq g$, we see that for any $h \in G$ with $h^* \neq h$, the element $h^*h^{-1} = g^{-1}g^*$ is independent of h; call it s, so that $h^* = sh$. If h is moved by $*$, so is h^*, in which case $(h^*)^* = sh^* = s^2h$, so $s^2 = 1$. Thus G is as specified in statement (i) of the theorem.

Now assume that G is not abelian. Since the elements of $\mathcal{R}$ anticommute, for any $\alpha, \beta \in R$ with $2\alpha = 2\beta = 0$ and any symmetric elements $g, h \in G$, the elements αg

https://doi.org/10.4153/CMB-2011-178-2 Published online by Cambridge University Press

and βh anticommute, so $\alpha\beta(gh + hg) = 0$. This says that either $gh = hg$ or $\alpha\beta = 0$. Thus the ring R has the property specified in statement (ii) of the theorem.

Next, select $g, h \in G$ with $gh \neq hg$, hence also $g^*h^* \neq h^*g^*$. Assume that $g^* \neq g$ and $h^* \neq h$. Then it is not hard to see that gh is in the support of the left-hand side of (2.3), so gh is in the support of the right side. There are two possibilities: $gh = h^*g$ or $gh = hg^*$.

In the first case, $gh = h^*g$, we have $h^*g^* = g^*h$ as well and (2.3) becomes $g^*h^* + hg = hg^* + gh^*$, giving $hg = gh^*$. In the second case, $gh = hg^*$, we have also $h^*g^* = gh^*$ and (2.3) reduces to $g^*h^* + hg = h^*g + g^*h$, implying $hg = g^*h$. In the second case, it is relevant that we also have $g^* = h^{-1}gh$. We intend to show that this happens in the first case as well.

So assume $gh = h^*g$. We note that g and gh do not commute and that $(gh)^* \neq gh$ because the alternative, $(gh)^* = gh$, gives $h^*g^* = gh = h^*g$, so $g = g^*$, which is a contradiction. So we may apply to the pair g, gh our observations about g and h, where there were two possibilities. Given the first of these, and applying $hg = gh^*$ to the pair g, gh, we have $(gh)g = g(gh)^*$, so $hg = h^*g^*$. But $hg = gh^*$, so $gh^* = h^*g^*$ and $g^* = (h^*)^{-1}gh^*$. Applying the involution, we get $g = hg^*h^{-1}$, so $g^* = h^{-1}gh$. Given the second possibility, and applying $gh = hg^*$ to the pair g, gh we get $g(gh) = (gh)g^*$, so $gh = hg^*$ and again $g^* = h^{-1}gh$.

To this point, we have shown that if $gh \neq hg$, $g^* \neq g$, and $h^* \neq h$, then $g^* = h^{-1}gh$.

Suppose $gh \neq hg$, $g^* \neq g$ but $h^* = h$. If $(gh)^* = gh$, then $h^*g^* = gh$, so $hg^* = gh$ and $g^* = h^{-1}gh$. If $(gh)^* \neq gh$, we can again apply some of what we have learned about the pair g, h to the pair g, gh, specifically, $g^* = (gh)^{-1}g(gh) = h^{-1}gh$.

In summary, we have shown that for any $g \in G$, either $g = g^*$ or else $h^{-1}gh \in \{g, g^*\}$ for all $h \in G$.

Proceeding as in [14], we now focus attention on $T = \{g \in G \mid g^* \neq g\}$, the complement in G of the set of elements that are symmetric with respect to *, and upon the subgroup $A = \langle T\rangle$ which T generates. Note that $T \neq \varnothing$ because G is not abelian.

Fix $t \in T$. If $g \notin A$, then $tg \notin T$, so $tg = (tg)^* = g^*t^* = gt^*$ and $t^* = g^{-1}tg$. (Similarly, replacing t by t^*, we have $g^{-1}t^*g = t$.) If also $h \notin A$, then gh must belong to A because

$$(gh)^{-1}t(gh) = h^{-1}g^{-1}tgh = h^{-1}t^*h = t.$$

We have proven that $g \notin A$ and $h \notin A$ implies $gh \in A$, so the index of A in G is at most 2.

If T is a commutative set, then A is abelian and the index is precisely 2 (because G is not abelian). Write $G = A \cup Ac$, $c \notin A$. Suppose $a_1, a_2 \in A$ with $a_1^* \neq a_1$ and $a_2^* \neq a_2$. Anticommutativity of $a_1 - a_1^*$ and $a_2 - a_2^*$ gives

$$2(a_1a_2 + a_1^*a_2^*) = 2(a_1a_2^* + a_1^*a_2).$$

Now a_1a_2 is not in the support of the right side here, so each side must be 0, in particular $a_1a_2^* = a_1^*a_2$, implying $a_1^{-1}a_1^* = a_2^*a_2^{-1}$. Call this element s. We have shown that if $a \in A$ and $a^* \neq a$, then $a^{-1}a^* = s$, equivalently, $a^* = sa$. Note that

https://doi.org/10.4153/CMB-2011-178-2 Published online by Cambridge University Press

$s \in A$ because T is closed under $*$, so $A = \langle T \rangle$ is too. Now if a is moved by $*$, so also is a^*. It follows that $(a^*)^* = sa^* = s(sa)$, giving $s^2 = 1$. This also shows that $s^* = s$ because the contrary implies $s^* = ss = 1$, which is not true. The last relevant property of s is its commutativity with c. To see this, we use the fact that $sc \notin A$ (because $s \in A$, $c \notin A$), so that $sc \notin T$, and this says that $sc = (sc)^* = c^*s^* = cs$.

Let $a \in A$ be any element with $a^* \neq a$. If $ac \neq ca$, previous arguments show that $a^* = c^{-1}ac$. But $a^* = sa$ so $c^{-1}ac = sa$ and $s = (c, a^{-1})$, the commutator of c and a^{-1}. This holds for any a moved by $*$. Replacing a by a^{-1}, we have $s = (c, a)$ for any a with $a^* \neq a$. Since $s^2 = 1$, we have also $s = (a, c)$. So $(a, c) = 1$ or s for any $a \in A$. Also, since $c^2 \in A$,

$$(ac, c) = c^{-1}a^{-1}c^{-1}ac^2 = c^{-1}a^{-1}c^{-1}c^2a = (c, a) = 1 \text{ or } s. \tag{2.5}$$

If $a_1, a_2 \in A$, we have

$$\begin{aligned}(a_1, a_2c) &= a_1^{-1}(a_2c)^{-1}a_1a_2c = a_1^{-1}c^{-1}a_2^{-1}a_1a_2c \\ &= a_1^{-1}c^{-1}a_1cc^{-1}a_1^{-1}a_2^{-1}a_1a_2c = (a_1, c) = 1 \text{ or } s.\end{aligned} \tag{2.6}$$

We now use the well-known commutator formulas

$$(xy, z) = (x, z)^y(y, z) \text{ and } (x, yz) = (x, z)(x, y)^z \tag{2.7}$$

to show that s is actually a unique (nonidentity) commutator in G. The only remaining pair of elements to consider has the form a_1c, a_2c with $a_1, a_2 \in A$, and for these we have $(a_1c, a_2c) = (a_1, a_2c)^c(c, a_2c) = 1$ or s by (2.5) and (2.6). All this shows that when T is a commutative set, the group G and ring R are described by statement (ii) of the theorem.

Suppose now that T is not commutative, and choose $t_1, t_2 \in T$ with $t_1t_2 \neq t_2t_1$. Since $t_1t_2t_1^{-1} \neq t_2$, we must have $t_1t_2t_1^{-1} = t_2{}^*$, that is, $t_1t_2 = t_2{}^*t_1$. We have $t_1t_2 = t_2t_1{}^*$ as well, because $t_2^{-1}t_1t_2 = t_1{}^*$, so $t_2{}^*t_1 = t_2t_1{}^*$. This gives $t_2^{-1}t_2{}^* = t_1{}^*t_1^{-1} = t_1^{-1}t_1{}^*$, since t_1 and $t_1{}^*$ commute (by Lemma 2.1). Note also that $t_1^{-1}t_1{}^* = t_1^{-1}t_2^{-1}t_1t_2$ and similarly $t_2^{-1}t_2{}^* = t_2^{-1}t_1^{-1}t_2t_1$. Thus, if $t_1, t_2 \in T$ and $t_1t_2 \neq t_2t_1$, then $(t_2, t_1) = t_2^{-1}t_2{}^* = t_1^{-1}t_1{}^* = (t_1, t_2)$.

Now fix noncommuting elements $t_1, t_2 \in T$, let $s = (t_1, t_2)$, and note that $s^2 = 1$. Let t be any element of T. If t fails to commute with t_1, say, then, as above, we can deduce $t^{-1}t^* = t_1^{-1}t_1{}^*$, giving $t^{-1}t^* = s$. Thus, if $t^{-1}t^* \neq s$, then t must commute with both t_1 and t_2. Let t be such an element. If $(tt_1)^* \neq tt_1$, then $t_2^{-1}(tt_1)t_2 = tt_1$ or $(tt_1)^*$ (and note that the second element $(tt_1)^* = t_1^*t^* = t^*t_1^*$). But $t_2^{-1}(tt_1)t_2 = (t_2^{-1}tt_2)(t_2^{-1}t_1t_2) = tt_1{}^*$, while $tt_1{}^* \neq tt_1$ and $tt_1{}^* \neq t^*t_1{}^*$. So $(tt_1)^* = tt_1$. Therefore $t_1{}^*t^* = tt_1 = t_1t$ and so $t^*t^{-1} = (t_1{}^*)^{-1}t_1 = s^{-1} = s$. This shows that $s = (t_1, t_2)$ is independent of the elements t_1 and t_2 in T, that is, for any $t \in T$, $t^{-1}t^* = s$. This gives part of the desired statement (ii) of the theorem, namely, that if $g^* \neq g$, then $g^* = sg$ (because such g is in T).

https://doi.org/10.4153/CMB-2011-178-2 Published online by Cambridge University Press

We know that s is the commutator of any two (non-commuting) elements of T. Also, if $t \in T$ and $g \in G$ is arbitrary with $gt \neq tg$, then $t^{-1}g^{-1}tg = t^{-1}t^* = s$. Finally, if $g \notin T$, $h \notin T$, and $gh \neq hg$, then $gh \in T$, for otherwise $(gh)^* = gh$, so $h^*g^* = gh$ and hence $hg = gh$. So we have $gh \in T$ and $g \in G$ and $(gh)g \neq g(gh)$. We have already considered this possibility and found $(gh, g) = s$. Since $(gh, g) = (h, g)$, we get $(h, g) = s$, so $(g, h) = s^{-1} = s$. All this establishes that s is a unique (non-identity) commutator in G and again G and R are described by statement (ii).

To complete the proof, we show that the conditions given in each statement of the theorem guarantee that the skew-symmetric elements of RG anticommute. For this, it is sufficient to show that the elements of $\mathcal{R} \cup \mathcal{S}$ anticommute, where $\mathcal{R}$ and $\mathcal{S}$ are defined in (2.1).

Suppose $(G, *)$ is a pair described by statement (i). Thus G is an abelian group, $s \in G$ satisfies $s^2 = 1$, and for any $g \in G$, either $g^* = g$ or $g^* = sg$. If $\alpha g, \beta h \in \mathcal{R}$, then $(\alpha g)(\beta h) + (\beta h)(\alpha g) = 2\alpha\beta gh = 0$, so αg and βh anticommute. If $\alpha g \in \mathcal{R}$ and $h - h^* \in \mathcal{S}$, then $\alpha g(h - h^*) + (h - h^*)(\alpha g) = 2\alpha g(h - h^*) = 0$, so elements of $\mathcal{R}$ anticommute with elements of $\mathcal{S}$. To show that two elements of $\mathcal{S}$ anticommute, let $g - g^*, h - h^* \in \mathcal{S}$. Clearly we may assume $g^* \neq g$ and $h^* \neq h$, and then $(g-g^*)(h-h^*) = (1-s)^2 gh = 2(1-s)gh$ while $-(h-h^*)(g-g^*) = -2(1-s)gh = 2(1-s)gh$ in characteristic 4.

Suppose $(G, *)$ and R are as described by statement (ii) of the theorem. Let $\alpha g, \beta h \in \mathcal{R}$. We wish to show that $\alpha\beta(gh+hg) = 0$. If symmetric elements commute, this is clear because $2\alpha = 0$. Otherwise, the hypothesis on the ring says $\alpha\beta = 0$ and again we have the desired anticommutativity of elements of R.

To show that $\alpha g \in \mathcal{R}$ and $h - h^* \in \mathcal{S}$ anticommute, we may assume $h^* \neq h$ so that $h^* = sh$. We want to show that $\alpha(1-s)gh = -\alpha(1-s)hg$. If $gh = hg$, this holds because $2\alpha(1-s)gh = 0$ while, if $gh \neq hg$, we have $hg = sgh$ and $\alpha(1-s)hg = \alpha(1-s)sgh = -\alpha(1-s)gh$.

Finally, we must show that $g - g^*$ and $h - h^*$ anticommute for any $g, h \in G$. For this, we may assume that $g^* = sg$ and $h^* = sh$. We have $(g - g^*)(h - h^*) = (1-s)^2 gh = 2(1-s)gh$ (using centrality of s) while $-(h-h^*)(g-g^*) = -2(1-s)hg$. If $gh = hg$, then $2(1-s)gh = -2(1-s)hg$ in characteristic 4. On the other hand, if $gh \neq hg$, then $hg = sgh$ and $-2(1-s)hg = -2(1-s)sgh = +2(1-s)gh$, again the desired anticommutativity. This completes the proof. ∎

Remark 2.3 In the last twenty-five years, considerable attention has been paid to the fact that there exist loop rings that are not associative, but nearly so in the sense that subrings generated by two elements are associative. In characteristic different from 2, the loops that produce such "alternative" loop rings are constructed from groups G having a unique nonidentity commutator and a property called LC, which says that two elements of G commute if and only if one of the elements, or their product, is central. See Chapter IV of [15], and especially Theorem 3.1 of that chapter, for more details. In such G, one can show that the map $g \mapsto g^*$, with $g^* = g$ on the centre and sg otherwise, is an involution. Further, the elements of G that are symmetric with respect to this involution are central and so commute. It seems most curious that such groups therefore satisfy the conditions of statement (ii) of Theorem 2.2, so

https://doi.org/10.4153/CMB-2011-178-2 Published online by Cambridge University Press

that the skew-symmetric elements in the group ring RG form a subring.

3 Anticommutativity of $(RG)^+$

As the heading suggests, in this section we classify groups G with the property that the Jordan product $\alpha \circ \beta = \alpha\beta + \beta\alpha$ is trivial on the set $(RG)^+$ of elements that are symmetric with respect to an involution of RG that fixes the elements of R. As noted in the introduction, this problem is equivalent to finding conditions under which symmetric elements anticommute. Since 1 is always symmetric, this statement implies, in particular, that 1 anticommutes with 1, so that the characteristic of R is 2. Thus, as posed, our problem has been solved because in characteristic 2 the groups G for which the symmetric elements of RG commute (and hence anticommute) are known [17]. We therefore restrict our problem and ask when it is the case that symmetric elements of the form $g + g^*$ anticommute.

As in the preceding section, we begin with a lemma which shows that the characteristic of R is always critical.

Lemma 3.1 *Suppose $g \mapsto g^*$ is an involution of a group G with the property that elements of the form $g + g^*$, $g \in G$, anticommute in a group ring RG. Then one of the following holds:*

(i) $\operatorname{char} R = 2$,
(ii) $\operatorname{char} R = 4$ *and* $gg^* = g^*g$ *and* $g^2 = (g^*)^2$ *for all* $g \in G$,
(iii) $\operatorname{char} R = 8$, *$G$ is abelian, and* $g^* = g$ *for all* $g \in G$.

Proof With $g = 1$, $g^* = 1$, so $1 + 1$ and $1 + 1$ anticommute. Thus $4 = -4$, $8 = 0$ in R, and $\operatorname{char} R = 2$, 4, or 8. For any $g \in G$, we have $(g + g^*)^2 = -(g + g^*)^2$, so

$$2g^2 + 2gg^* + 2g^*g + 2(g^*)^2 = 0.$$

Suppose $\operatorname{char} R = 4$. Then for a given g either $g^2 = gg^*$ and $gg^* = (g^*)^2$ or $g^2 = g^*g$ and $gg^* = (g^*)^2$ or $g^2 = (g^*)^2$ and $gg^* = g^*g$. So either $g = g^*$ or else $g^2 = (g^*)^2$ and $gg^* = g^*g$. The latter condition holds in any case, so for all $g \in G$, $g^2 = (g^*)^2$ and $gg^* = g^*g$, giving the second statement of the lemma. Finally, if $\operatorname{char} R = 8$, then all the elements $g^2, gg^*, g^*g, (g^*)^2$ are equal for any $g \in G$, in particular, $g^2 = gg^*$, so $g^* = g$, showing that $*$ is the identity on G. Since $*$ is also an involution, G is abelian and the proof is complete. ■

As observed, the case of characteristic 2 has been settled. In characteristic 8, Lemma 3.1 says that G must be abelian with $g^* = g$ for all $g \in G$. This condition is sufficient as well because anticommutativity of $g + g^*$ and $h + h^*$ is the condition

$$gh + g^*h + gh^* + g^*h^* + hg + h^*g + hg^* + h^*g^* = 0, \tag{3.1}$$

which becomes $8gh = 0$ when G is abelian, $g^* = g$ and $h^* = h$. As in Section 2, then, the case requiring some analysis is characteristic 4.

Theorem 3.2 *Let G be a group with an involution $*$ and let R be a coefficient ring of characteristic 4. Then elements of the form $g + g^*$, $g \in G$, anticommute in RG if and only if either*

https://doi.org/10.4153/CMB-2011-178-2 Published online by Cambridge University Press

(1) *G is abelian and there exists $s \in G$ with $s^2 = 1$ and $g^* = g$ or sg for all $g \in G$ or*
(2) *G is a nonabelian group with a unique commutator $s \neq 1$ and $g^* = g$ or $g^* = sg$ for all $g \in G$.*

Proof This time we begin by showing that elements of the form $g + g^*$ anticommute when G is a group of either of the described types. To do this, we must establish the validity of (3.1) for each type of group.

If G is abelian, the left side of (3.1) becomes $2gh + 2g^*h + 2gh^* + 2g^*h^*$, which is clearly 0 if $g^* = g$ and $h^* = h$. If one of g, h is moved by the involution and the other is not, say $g^* = sg$ and $h^* = h$, then $2gh + 2g^*h + 2gh^* + 2g^*h^* = 2gh + 2sgh + 2gh + 2sgh = 4gh + 4sgh = 0$, and if $g^* = sg$ and $h^* = sh$, then $2gh + 2g^*h + 2gh^* + 2g^*h^* = 2gh + 2sgh + 2sgh + 2gh = 0$ again.

Suppose G is not abelian, that G has a unique nonidentity commutator s (easily seen to be central and to have order 2) and $g^* = g$ or sg for all $g \in G$. We consider three cases. If $g^* = g$ and $h^* = h$, then the left side of (3.1) is $gh + gh + gh + gh + hg + hg + hg + hg = 4gh + 4hg$ and this is 0 in characteristic 4. If one of g, h is moved by the involution and the other is not, say $g^* = sg$ and $h^* = h$, the left side of (3.1) is $gh + sgh + gh + sgh + hg + hg + shg + shg = 4gh + 4sgh$, and this is 0 if $gh = hg$ and $gh + sgh + gh + sgh + sgh + sgh + gh + gh = 4gh + 4sgh = 0$ otherwise. The final case, $g^* = sg$, $h^* = sh$, is similar.

Now assume that G is a group with involution and that elements of the form $g + g^*$ anticommute. We show that G is described by statement (i) or (ii) of the theorem.

First suppose that G is abelian. Then (3.1) becomes $2gh + 2g^*h + 2gh^* + 2g^*h^* = 0$. If $g^* \neq g$ and $h^* \neq h$, then (3.1) can hold only if $gh = g^*h^*$ and so $g^*h = gh^*$ too. This implies $h^{-1}h^* = g^{-1}g^*$ and so the element $s = g^{-1}g^*$ is independent of g with $g^* \neq g$. It follows that $g^* = g$ or sg for all $g \in G$. Note that $s^2 = 1$ because $g^2 = (g^*)^2$ by Lemma 3.1.

Now suppose that G is not abelian and that $g, h \in G$ do not commute. If $g^* \neq g$ and $h^* \neq h$, then the only way for g and h to satisfy (3.1) is for $gh = g^*h^*$; otherwise, $gh = hg^* = h^*g = h^*g^*$, which is not the case because $h^*g \neq h^*g^*$. So $gh = g^*h^*$ and $h^*g^* = hg$, and (3.1) becomes $2gh + 2hg + g^*h + gh^* + hg^* + h^*g = 0$. It follows that $gh = hg^* = h^*g$, so $g^* = h^{-1}gh$. Suppose $g^* \neq g$ and $h^* = h$. If $(gh)^* = gh$, then $gh = h^*g^* = hg^*$ and $g^* = h^{-1}gh$, while if $(gh)^* \neq gh$, we may apply to the noncommuting pair g, gh what we discovered about the pair g, h, specifically that $g^* = (gh)^{-1}g(gh)$. This says again that $g^* = h^{-1}gh$.

As in the proof of Theorem 2.2, we have learned that for any $g \in G$, either $g^* = g$ or else $h^{-1}gh \in \{g, g^*\}$ for all $h \in G$. As before, we let $T = \{g \in G \mid g^* \neq g\}$. If T is not commutative, we discover, exactly as before, that G has a unique commutator $s \neq 1$ and that for any $g \in G$, either $g^* = g$ or $g^* = sg$. On the other hand, if T is commutative, the subgroup A generated by T is abelian, $[G\colon A] = 2$, and the involution restricted to A maps into $A = \langle T \rangle$. We studied this situation in the previous paragraph, so we conclude here that there is an element $s \in A$ with $s^2 = 1$ and $a^* = a$ or sa for any $a \in A$. Now $g^* = g$ for any $g \notin A$ (since such $g \notin T$), so we have $g^* = g$ or $g^* = sg$ for each $g \in G$ and G is almost as described by statement (ii) of the theorem. Since G is not abelian, the map $*$ is not the identity, so $s \neq 1$. This implies $s^* = s$, because the contrary implies $s^* = ss = 1$. It remains only to prove that s is the only commutator different from 1 in G. Let c be any element not in A (so $c^* = c$). Then $G = A \cup Ac$ with s and c commuting, because $sc \notin A$ means $sc \notin T$, so $sc = (sc)^* = c^*s^* = cs$.

Take $t \in T$. Then $tc \notin A$, so $tc \notin T$. Therefore, $tc = (tc)^* = c^*t^* = cst = sct$, so $s = tct^{-1}c^{-1} = (t^{-1}, c^{-1})$. Applying the foregoing to t^{-1} and c^{-1}, we also have $s = (t, c)$. Since A is generated by T, the formula $(xy, c) = (x, c)^y(y, c)$ shows that $(a, c) = 1$ or $(a, c) = s$ for all $a \in A$. Now s is central in G because it commutes with c and with all elements of A. Hence we can show that $(a_1c, a_2c) = 1$ or s using the commutator formulas (2.7) as before. This completes our proof. ■

Remark 3.3 We conclude with a remark analogous to Remark 2.3. It is not hard to embed a group described by statement (ii) of Theorem 3.2 in a Moufang loop with the same description; the $M(G, *, 1)$ construction described in [15, §II.5] can be used, for example. With a coefficient ring of characteristic 2, such a loop is known to have a loop ring that is alternative (but not associative) [1]. Again we find the connection between group rings with involution satisfying the properties of this paper and alternative loop rings interesting and most curious.

References

[1] O. Chein and E. G. Goodaire, *Code loops are RA*2 *loops*. J. Algebra **130**(1990), no. 2, 385–387. http://dx.doi.org/10.1016/0021-8693(90)90088-6

[2] O. Broche Cristo, *Commutativity of symmetric elements in group rings*. J. Group Theory **9**(2006), no. 5, 673–683. http://dx.doi.org/10.1515/JGT.2006.043

[3] O. Broche Cristo, E. Jespers, C. Polcino Milies, and M. Ruiz Marín, *Antisymmetric elements in group rings. II*. J. Algebra Appl. **8**(2009), no. 1, 115–127. http://dx.doi.org/10.1142/S0219498809003254

[4] O. Broche Cristo and M. Ruiz Marín, *Lie identities in symmetric elements in group rings: A survey*. In: Groups, Rings and Group Rings. Lect Notes Pure Appl. Math. 248. Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 43–55.

[5] 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. http://dx.doi.org/10.1017/S0013091504000896

[6] A. Giambruno and C. Polcino Milies, *Unitary units and skew elements in group algebras*, Manuscripta Math. **111**(2003), no. 2, 195–209. http://dx.doi.org/10.1007/s00229-003-0365-5

[7] A. Giambruno and S. K. Sehgal, *Lie nilpotence of group rings*. Comm. Algebra **21**(1993), no. 11, 4253–4261. http://dx.doi.org/10.1080/00927879308824797

[8] A. Giambruno, C. Polcino Milies, and S. K. Sehgal, *Group algebras of torsion groups and Lie nilpotence*. J. Group Theory. **13**(2009), no. 2, 221–231. http://dx.doi.org/10.1515/JGT.2009.048

[9] ———, *Group identities on symmetric units*. J. Algebra **322**(2009), no. 8, 2801–2815. http://dx.doi.org/10.1016/j.jalgebra.2009.06.025

[10] ———, *Lie properties of symmetric elements in group rings*, J. Algebra **321**(2009), no. 3, 890–902. http://dx.doi.org/10.1016/j.jalgebra.2008.09.041

[11] A. Giambruno, S. K. Sehgal, and A. Valenti, *Symmetric units and group identities.* Manuscripta Math. **96**(1998), no. 4, 443–461. http://dx.doi.org/10.1007/s002290050076

[12] J. Z. Gonçalves and D. S. Passman, *Involutions and free pairs of bicyclic units in integral group rings.* J. Group Theory **13**(2010), no. 5, 721–742. http://dx.doi.org/10.1515/JGT.2010.019

[13] ———, *Unitary units in group algebras*. Israel J. Math. **125**(2001), 131–155. http://dx.doi.org/10.1007/BF02773378

[14] E. G. Goodaire, *Groups embeddable in alternative loop rings.* In: Contributions to General Algebra 7. Hölder-Pichler-Tempsky, Vienna, 1991, pp. 169–176.

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

[16] E. Jespers and M. Ruiz Marín, *Antisymmetric elements in group rings*. J. Algebra Appl. **4**(2005), no. 4, 341–353. http://dx.doi.org/10.1142/S0219498805001228

[17] ______, *On symmetric elements and symmetric units in group rings*. Comm. Algebra **34**(2006), no. 2, 727–736. http://dx.doi.org/10.1080/00927870500388018

[18] G. T. Lee, *Group identities on units and symmetric units of group rings*. Algebra and Applications 12. Springer-Verlag, London, 2010.

[19] G. T. Lee, S. K. Sehgal, and E. Spinelli, *Group algebras whose symmetric and skew elements are Lie solvable*. Forum Math. **21**(2009), no. 4, 661–671. http://dx.doi.org/10.1515/FORUM.2009.033

[20] ______, *Lie properties of symmetric elements in group rings. II.* J. Pure Appl. Algebra **213**(2009), no. 6, 1173–1178. http://dx.doi.org/10.1016/j.jpaa.2008.11.027

[21] S. K. Sehgal and A. Valenti, *Group algebras with symmetric units satisfying a group identity*. Manuscripta Math. **119**(2006), no. 2, 243–254. http://dx.doi.org/10.1007/s00229-005-0610-1

Memorial University of Newfoundland, St. John's, NF, A1C 5S7
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