

# ON SOME CENTRE-LIKE SUBSETS OF RINGS

By

HOWARD E. BELL\*

Department of Mathematics, Brock University, St Catharines, Ontario,  
Canada, L2S3A1

and

ABRAHAM A. KLEIN

Sackler Faculty of Exact Sciences, School of Mathematical Sciences,  
Tel Aviv University, Tel Aviv 69978, Israel

[Received 27 May 2003. Read 18 October 2004. Published 11 March 2005.]

## ABSTRACT

For arbitrary rings  $R$ , let  $F_r(R) = \{a \in R \mid |\{a, b\}^2| \leq 3 \text{ for all } b \in R\}$ , and let  $F_r^*(R) = \{a \in R \mid \text{for each } b \in R, \text{ either } [a, b] = 0 \text{ or } a^2 = b^2\}$ . We study the properties of these sets for large classes of rings, and we provide sufficient conditions for these sets to coincide with the centre. Several examples are given.

## 1. Introduction

In [1] and [2] we proved commutativity of rings  $R$  with 1 such that for each  $a, b \in R$ ,  $|\{a, b\}^2| = |\{a^2, ab, ba, b^2\}| \leq 3$ . Localising the setwise commutativity condition in this theorem, we obtain certain centre-like subsets that frequently coincide with the centre. We study various properties of these subsets and establish some sufficient conditions for them to be equal to the centre.

Throughout the paper,  $R$  will denote a ring with centre  $Z = Z(R)$ ; and  $N$  will denote the set of nilpotent elements of  $R$ . As usual, the symbol  $[x, y]$  will denote the commutator  $xy - yx$ ; and for each subset  $S$  of  $R$ ,  $C(S)$  will be the centraliser of  $S$  in  $R$ , and  $A_\ell(S)$  and  $A(S)$  will be the left and two-sided annihilators of  $S$ , respectively.

## 2. Freiman centres

Our work in this section, which extends ring-theoretic results in [1] and [2], has roots in a group-theoretic paper of Freiman [3].

We define the Freiman centre  $F_r(R)$  and the restricted Freiman centre  $F_r^*(R)$  by

$$F_r(R) = \{a \in R \mid |\{a, b\}^2| \leq 3 \text{ for all } b \in R\}$$

---

\*Corresponding author; e-mail: h.bell@brocku.ca

and by

$$F_r^*(R) = \{a \in R \mid \text{for each } b \in R, \text{ either } [a, b] = 0 \text{ or } a^2 = b^2\}.$$

Clearly  $Z(R) \subseteq F_r^*(R) \subseteq F_r(R)$  for all rings  $R$ . As we would expect, there exist rings  $R$  for which  $F_r^*(R) \neq F_r(R)$ .

**Theorem 2.1.**

- (a) For any ring  $R$ , either  $F_r^*(R) = Z$  or  $R$  is nil of index  $\leq 4$ .
- (b) If  $R$  is any ring with 1,  $F_r^*(R) = Z$ .
- (c) If  $R$  is any 2-torsion-free ring, either  $F_r^*(R) = Z$ , or  $R$  is a non-commutative nil ring of index 2 and  $F_r^*(R) = R$ .

PROOF.

- (a) Assume that  $F_r^*(R) \neq Z$ , and let  $a \in F_r^*(R) \setminus Z$ . If  $b \in R \setminus C(a)$  and  $c \in C(a)$ , then  $[a, b] = [a, b + c] \neq 0$  and hence  $a^2 = b^2 = (b + c)^2$ . It follows that

$$bc + cb + c^2 = 0 \text{ for all } c \in C(a) \text{ and } b \notin C(a); \quad (2.1)$$

and replacing  $b$  by  $b + c$ , we get  $2c^2 = 0$ . Multiplying (2.1) by  $c$  on both sides, we obtain  $bc^2 = c^2b$  for all  $c \in C(a)$  and  $b \notin C(a)$ ; therefore, if  $c \in C(a)$ ,  $c^2$  centralises the complement of the proper subgroup  $C(a)$ , hence is central. Now replacing  $c$  by  $c^2$  in (2.1), we get  $c^4 = -c^2b - bc^2 = -2c^2b = 0$  for all  $c \in C(a)$ . In particular,  $a^4 = 0$ ; and since  $b^2 = a^2$  for all  $b \notin C(a)$ , we have  $b^4 = 0$  for all  $b \notin C(a)$ . Thus,  $x^4 = 0$  for all  $x \in R$ .

- (b) is an obvious consequence of (a).
- (c) Letting  $a, b$  be as above, we already know that  $2c^2 = 0$  for all  $c \in C(a)$ ; hence  $c^2 = 0$  for all  $c \in C(a)$ . Since  $a \in C(a)$ , we have  $a^2 = 0 = b^2$  for all  $b \notin C(a)$ . Thus,  $x^2 = 0$  both for  $x \in C(a)$  and  $x \notin C(a)$ . ■

As we shall see later,  $F_r(R)$  is in general more complicated than  $F_r^*(R)$ ; however, we do have the following theorem:

**Theorem 2.2.** *If  $R$  is any 2-torsion-free ring with 1, then  $F_r(R) = Z$ .*

The proof of this theorem is elementary but lengthy, so we break it up into several lemmas. In the next four lemmas, it is assumed that  $R$  satisfies the hypotheses of the theorem.

**Lemma 2.3.** *If  $N$  is the set of nilpotent elements of  $R$  and  $u \in N \cap F_r(R)$ , then  $[u, N] = \{0\}$ .*

PROOF. Suppose  $u \in N \cap F_r(R)$  and  $v \in N$  with  $[u, v] \neq 0$ . Then  $[u, 1 + v] \neq 0$ , so we must have one of  $(1 + v)^2 = u^2$ ,  $(1 + v)^2 = (1 + v)u$ ,  $(1 + v)^2 = u(1 + v)$ ,  $u^2 = u(1 + v)$ ,  $u^2 = (1 + v)u$ . The first three cannot occur, because any one of those three cases implies an invertible nilpotent element. But either of the last two cases shows that  $u^k = 0$  implies  $u^{k-1} = 0$ , hence  $u = 0$ ; so neither of these can occur. ■

**Lemma 2.4.**  $N \cap F_r(R) \subseteq Z(R)$ .

PROOF. Suppose  $u \in (N \cap F_r(R)) \setminus Z(R)$  and let  $b \in R$  such that  $[u, b] \neq 0$ . Then we must have one of  $b^2 = u^2$ ,  $b^2 = ub$ ,  $b^2 = bu$ ,  $u^2 = bu$ ,  $u^2 = ub$ . Now  $b^2 \neq u^2$ , since  $b \notin N$  by Lemma 2.3. If  $b^2 = ub$ , then  $b^3 = ub^2 = u(ub) = u^2b$ , and by induction we get  $b \in N$ ; therefore we cannot have  $b^2 = ub$  or similarly  $b^2 = bu$ . Then we must have  $u^2 = bu$  or  $u^2 = ub$ . Now  $b$  may be replaced by  $b + 1$ , so one of the following occurs:

- (i)  $bu = u^2$  and  $(b + 1)u = u^2$ ;
- (ii)  $ub = u^2$  and  $u(b + 1) = u^2$ ;
- (iii)  $bu = u^2$  and  $u(b + 1) = u^2$ ;
- (iv)  $ub = u^2$  and  $(b + 1)u = u^2$ .

Either of (i) and (ii) implies  $u = 0$ , so suppose (iii) holds. Then right-multiplying each equality in (iii) by  $u$  gives  $bu^2 = u^3 = u(bu) + u^2 = u^3 + u^2$ ; therefore  $u^2 = 0 = bu$  and  $ub = -u$ . Now  $1 + 2b \notin N$ , since  $[u, b] \neq 0$ ; hence  $\{u, 1 + 2b\}^2 = \{0, -u, u, (1 + 2b)^2\}$  has 4 distinct elements, so (iii) cannot hold and similarly (iv) cannot hold. ■

**Lemma 2.5.** If  $a \in F_r(R) \setminus N$  and  $ab = 0$ , then  $ba = 0$ .

PROOF. Suppose  $a \in F_r(R) \setminus N$  and  $ab = 0 \neq ba$ . Then  $a(-b) = 0 \neq (-b)a$ ; and since we cannot have both  $b^2 = ba$  and  $b^2 = (-b)a$ , we may assume  $b^2 \neq ba$ .

Now  $\{a, -a + b\}^2 = \{a^2, -a^2, -a^2 + ba, a^2 - ba + b^2\}$  has repetitions. But any of  $a^2 = -a^2$ ,  $a^2 = -a^2 + ba$ ,  $-a^2 = a^2 - ba + b^2$  and  $-a^2 + ba = a^2 - ba + b^2$  implies that  $a \in N$ ;  $-a^2 = -a^2 + ba$  implies  $ba = 0$ ; and  $a^2 = a^2 - ba + b^2$  implies  $b^2 = ba$ . Thus  $ba = 0$  as required. ■

**Lemma 2.6.** If  $a \in F_r(R) \setminus Z(R)$  and  $b \in R$  is such that  $[a, b] \neq 0$ , then  $a^2 = b^2$ .

PROOF. Suppose that this is not the case. Let  $a \in F_r(R) \setminus Z(R)$ ,  $[a, b] \neq 0$  and  $a^2 \neq b^2$ . Now  $\{a, b\}^2 = \{a^2, ab, ba, b^2\}$ . But  $a^2 = ab \Rightarrow a(a - b) = 0$ , hence  $(a - b)a = 0$  by Lemma 2.5 and therefore  $ab = ba$ . Similarly,  $a^2 \neq ba$ . Therefore, we have  $b^2 = ab$  or  $b^2 = ba$ . Since  $b$  may be replaced by  $-b$ , we also have  $b^2 = -ab$  or  $b^2 = -ba$ ; and since  $R$  is 2-torsion-free,  $ab = -ba$ .

Assume  $b^2 = ab$ . We cannot have both  $a^2 = (1 + b)^2$  and  $a^2 = (1 - b)^2$ , for this implies  $4b = 0$ ; hence we may assume  $a^2 \neq (1 + b)^2$ . Since  $\{a, 1 + b\}^2 = \{a^2, a + ab, a + ba, (1 + b)^2\}$  has repetition, we must have one of  $a^2 = a + ab$ ,  $a^2 = a + ba$ ,  $a + ab = (1 + b)^2$ ,  $a + ba = (1 + b)^2$ . But  $a^2 = a + ab \Rightarrow a(a - 1 - b) = 0 \Rightarrow (a - 1 - b)a = 0 \Rightarrow ab = ba$ ; and similarly,  $a^2 = a + ba \Rightarrow ab = ba$ . Also, since  $b^2 = ab = -ba$ , either  $a + ab = (1 + b)^2$  or  $a + ba = (1 + b)^2$  implies  $[a, b] = 0$ . Likewise, we cannot have  $b^2 = ba$ . ■

**Proof of Theorem 2.2.** We have shown that  $F_r(R) \subseteq F_r^*(R)$ . Therefore  $F_r(R) = Z$  by Theorem 2.1(b). ■

### 3. Some examples

**Example 3.1.** Let  $R_0 = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \mid x, y \in GF(2) \right\}$ . Then  $R_0 = \{0, a, b, a + b\}$ , where  $a = e_{11}$  and  $b = e_{12}$ . Now  $a$  and  $a + b$  are left identity elements and  $b \in A_r(R_0)$ ; hence  $F_r(R_0) = R_0 \neq F_r^*(R_0) = Z(R_0) = \{0\}$ .

**Example 3.2.** Letting  $R_0, a, b$  be as above, let  $R_1 = R_0 \oplus GF(2)$ ; and let  $z$  be the nonzero element of  $GF(2)$ . It is easily verified that  $F_r(R_1) = \{0, z, b, a + z, a + b + z\} \neq F_r^*(R_1) = \{0, z\} = Z(R_1)$ . This example shows that in general,  $F_r(R)$  need not be a subring of  $R$ .

**Example 3.3.** Let  $R_2 = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \mid x, y \in GF(3) \right\}$ . Then  $R_2$  is 2-torsion-free and  $F_r(R_2) = \left\{ \begin{bmatrix} 0 & y \\ 0 & 0 \end{bmatrix} \mid y \in GF(3) \right\} \neq Z(R_2)$ . This example shows that in Theorem 2.2 the hypothesis that  $R$  has 1 cannot be deleted.

**Example 3.4.** Let  $R_3$  be the ring of upper-triangular  $2 \times 2$  matrices over  $GF(2)$ . Then  $F_r(R_3) = \{0, 1, e_{12}, 1 + e_{12}\}$ , which is a subring of  $R_3$ . This example shows that even if  $R$  has 1 and  $F_r(R)$  is a subring,  $F_r(R)$  need not equal  $Z(R)$ . It also shows that in Theorem 2.2 the hypothesis that  $R$  is 2-torsion-free cannot be deleted.

**Example 3.5.** Let  $R_4$  be the algebra over  $GF(2)$  with basis  $x_1, x_2, x_3$  and multiplication defined by  $x_1^2 = x_2^2 = x_1x_2 = x_3$  and  $x_2x_1 = 0 = x_3x_i = x_ix_3$  for all  $i = 1, 2, 3$ . Then  $R_4$  is a nilpotent ring of index 3 and  $F_r^*(R_4) = R_4$ . This example shows that for  $R$  with 2-torsion, there are more possibilities for  $F_r^*(R)$  than those outlined in Theorem 2.1(c).

### 4. Further results on $F_r^*(R)$

In this section we consider rings  $R$  with  $2R = \{0\}$ , in which case (2.1) becomes

$$c^2 = bc - cb \text{ for all } c \in C(a) \text{ and } b \notin C(a), \quad (4.1)$$

where  $a \in F_r^*(R) \setminus Z$ .

**Lemma 4.1.** *Let  $F_r^*(R) \neq Z$ , and  $a \in F_r^*(R) \setminus Z$ . Then*

- (a) *For any  $c \in C(a) \setminus Z$ ,  $C(c) = C(a)$ ;*
- (b) *For any  $b \notin C(a)$ ,  $C(a) \cap C(b) = Z$ ;*
- (c)  $Z = \{z \in R \mid z^2 = 0\}$ .

**PROOF.**

- (a) Note that if  $x, y \in C(a)$ , then  $x^2 = bx - xb, y^2 = by - yb$  and  $(x + y)^2 = b(x + y) - (x + y)b$ ; hence  $xy + yx = 0 = xy - yx$ . Thus  $C(a)$  is commuta-

tive, and consequently  $C(c) \supseteq C(a)$  for all  $c \in C(a) \setminus Z$ . If there exists  $b' \in C(c) \setminus C(a)$ , then (4.1) gives  $c^2 = 0$ ; and it follows immediately from (4.1) that  $bc = cb$  for all  $b \notin C(a)$ . But then  $c$  centralises the complement of the proper additive subgroup  $C(a)$ , hence  $c \in Z$ , contrary to our hypothesis that  $c \in C(a) \setminus Z$ . Therefore,  $C(c) \subseteq C(a)$ . For any  $c \in C(a) \setminus Z$ ,  $C(c) = C(a)$ ; For any  $b \notin C(a)$ ,  $C(a) \cap C(b) = Z$ ;  $Z = \{z \in R \mid z^2 = 0\}$ .

- (b) Obviously  $C(a) \cap C(b) \supseteq Z$ . Conversely, if  $c \notin Z$ , either  $c \notin C(a)$  or  $c \in C(a) \setminus Z$ ; and in the latter case, since  $C(c) = C(a)$ , we have  $c \notin C(b)$ . Thus, if  $c \notin Z$ ,  $c \notin C(a) \cap C(b)$ —i.e.  $C(a) \cap C(b) \subseteq Z$ .
- (c) It is immediate from (4.1) that  $z^2 = 0$  for all  $z \in Z$ . Now consider  $c \notin Z$ . If  $c \in C(a)$ , then  $C(c) = C(a)$ ; hence for  $b \notin C(a)$ ,  $bc \neq cb$  and (4.1) gives  $c^2 \neq 0$ . In particular,  $a^2 \neq 0$ , and if  $c \notin C(a)$ ,  $a^2 = c^2 \neq 0$ . Thus,  $c \notin Z$  implies  $c^2 \neq 0$ . ■

**Theorem 4.2.** *Let  $R$  be a ring with  $2R = \{0\}$ , such that  $F_r^*(R) \neq Z$ . Then one of the following holds:*

- (i)  $F_r^*(R) = R$ .
- (ii)  $F_r^*(R)$  is commutative and is equal to  $Z(R) + \mathbb{Z}_2 a$  for any  $a \in F_r^*(R) \setminus Z(R)$ .

PROOF. Suppose now that  $F_r^*(R)$  is not commutative, and let  $a, b \in F_r^*(R)$  such that  $ab \neq ba$ . Then  $a^2 = b^2$ . If  $x$  and  $y$  are any noncommuting elements of  $R$ , then by Lemma 4.1(b), each of  $x, y$  fails to commute with at least one of  $a$  and  $b$ , and therefore  $x^2 = y^2 = a^2 = b^2$ . Thus  $F_r^*(R) = R$ .

To complete the proof, we show that (ii) holds if  $F_r^*(R)$  is commutative but not central. Let  $a \in F_r^*(R) \setminus Z$ . For  $z \in Z$ , Lemma 4.1(c) yields  $(z + a)^2 = z^2 + a^2 = a^2$ ; and since  $C(z + a) = C(a)$ ,  $z + a \in F_r^*(R)$ . Thus  $Z + \mathbb{Z}_2 a \subseteq F_r^*(R)$ . To obtain the reverse inclusion, we show that if  $a, c \in F_r^*(R) \setminus Z$ , then  $a + c \in Z$ . For such  $a, c$ , we have  $C(a) = C(c)$  by Lemma 4.1(a), so that for all  $b \notin C(a)$ ,  $b^2 = a^2 = c^2$ . Also, by (4.1) we have  $bc - cb = c^2 = a^2 = ba - ab$ , from which it follows that  $a + c \in C(b)$  and hence that  $a + c \in C(a) \cap C(b) = Z$ .

It is not obvious that (ii) can actually occur. By Theorem 2.1(a) and Lemma 4.1(c), we see that if  $R$  satisfies (ii), then  $x^2 \in Z$  for all  $x \in R$ . Therefore we must have  $a \in F_r^*(R) \setminus Z$ ,  $b \notin C(a)$  and  $z \in Z$ , such that  $a^2 = b^2 = z$ . Since  $F_r^*(R)$  is commutative,  $b \notin F_r^*(R)$ ; hence there exists  $c \in R$  such that  $b^2 \neq c^2$  and  $[b, c] \neq 0$ . Thus  $c^2 \neq a^2$ ; hence  $c \in C(a)$  and there exists  $w \in Z \setminus \{z\}$  such that  $c^2 = w$ . These observations lead us to an example.

**Example 4.3.** Let  $R$  be the 5-dimensional algebra over  $K = \mathbb{Z}_2$  with basis  $\{z, w, a, b, c\}$  and multiplication defined as follows:

	$z$	$w$	$a$	$b$	$c$
$z$	$0$	$0$	$0$	$0$	$0$
$w$	$0$	$0$	$0$	$0$	$0$
$a$	$0$	$0$	$z$	$z$	$0$
$b$	$0$	$0$	$0$	$z$	$w$
$c$	$0$	$0$	$0$	$0$	$w$

It is easy to see that  $Z(R) = Kz + Kw = A(R)$  and  $C(a) = C(c) = Kz + Kw + Ka + Kc$ ; and it follows that  $(C(a), +)$  has index 2 in  $(R, +)$  and  $R \setminus C(a) = b + C(a)$ .

For any  $x \in R \setminus C(a)$ , we have

$$x^2 = (b + \alpha z + \beta w + \gamma a + \delta c)^2 = (b + \gamma a + \delta c)^2 = b^2 + \gamma a^2 + \delta c^2 + \gamma ab + \delta bc \\ = z + \gamma z + \delta w + \gamma z + \delta w = z = a^2; \quad \text{hence } a \in F_r^*(R) \setminus Z.$$

Moreover,  $F_r^*(R) \cap (R \setminus C(a)) = \emptyset$ , for if  $d \in C(a) = C(c)$ , then  $(b + d)^2 = z$ ,  $[b + d, c] = [b, c] \neq 0$  and  $c^2 = w \neq z$ . Thus  $F_r^*(R) \subseteq C(a)$ , so that  $F_r^*(R)$  is commutative. It follows by Theorem 4.2 that  $R$  satisfies (ii). ■

*Remark.* If  $R$  is any ring of characteristic 2 with  $F_r^*(R) \neq Z$ , Lemma 4.1(c) shows that  $Z$  is an ideal of  $R$ . Thus, for all the cases treated in Theorem 2.1(c) and Theorem 4.2,  $F_r^*(R)$  is a subring of  $R$ . We conjecture that  $F_r^*(R)$  is a subring for all rings  $R$ . Using the Sonata program, Jürgen Ecker has verified this conjecture for rings with fewer than 32 elements.

### 5. The strong Freiman centre

We define the strong Freiman centre to be the set

$$\widehat{F}_r(R) = \{a \in R \mid |\{a, b\}^2| \leq 2 \text{ for all } b \in R\}$$

in any ring  $R$ ,  $0 \in \widehat{F}_r(R)$ ; and it is intuitively clear that  $\widehat{F}_r(R) = \{0\}$  for most rings. However,  $\widehat{F}_r(R)$  can be as large as  $R$ —for example, if  $R = GF(3)$  or if  $R$  is the ring of Example 3.5.

For rings with 1, we have complete information.

**Theorem 5.1.** *Let  $R$  be a ring with 1. Then one of the following holds:*

- (a)  $\widehat{F}_r(R) = \{0\}$ ;
- (b)  $R$  is a Boolean ring and  $\widehat{F}_r(R) = \{0, 1\}$ ;
- (c)  $R = GF(3)$  and  $\widehat{F}_r(R) = R$ .

**PROOF.** Assume  $\widehat{F}_r(R) \neq \{0\}$ . If  $e$  is any idempotent other than 0 or 1,  $\{e, 1 - e\}^2 = \{e, 1 - e, 0\}$  has three distinct elements, hence  $e \notin \widehat{F}_r(R)$ . Therefore, if  $a \in \widehat{F}_r(R) \setminus \{0\}$ , the fact that  $|\{a, 1\}^2| = |\{a^2, a, 1\}| \leq 2$  forces  $a^2 = 1$ . Since  $\{a, 2a\}^2$  is  $\{1, 2, 4\}$ , we must have  $2 = 0$  or  $3 = 0$ . If  $2 = 0$ , the condition  $|\{a, a + 1\}^2| = |\{1, 1 + a, 0\}| \leq 2$  yields  $a = 1$ ; if  $3 = 0$ , the condition  $|\{a, a + 1\}^2| = |\{1, 1 + a, 2(1 + a)\}| \leq 2$  yields  $a = 1$  or  $a = 2$ .

Consider the case  $2 = 0$ . For  $x \in R \setminus \{0, 1\}$ , the set  $\{1, x\}^2 = \{1, x, x^2\}$ , so  $x^2 = x$  or  $x^2 = 1$ ; hence  $N = \{0\}$ . In fact, the case  $x^2 = 1$  cannot occur, since this implies  $x + 1 \in N$  and hence  $x = 1$ . Therefore  $R$  is a Boolean ring.

Finally, suppose that  $3 = 0$ , and let  $b \in R \setminus \{0\}$ . For  $a = 1$  or  $2$ , the condition that  $\{a, b\}^2 = \{1, ab, b^2\}$  and  $\{a, 2b\}^2 = \{1, 2ab, b^2\}$  each have at most 2 elements implies that  $b^2 = 1$ ; hence  $\{a, a + ab\}^2 = \{1, 1 + b, 2 + 2b\}$ , and any repetition gives  $b = 1$  or  $b = 2$ . Thus,  $R = GF(3)$ . ■

For  $R$  without 1, we do not have a result like Theorem 5.1. However, the condition that  $\widehat{F}_r(R) \not\subseteq N$  has strong structural implications, as our final theorem shows.

**Theorem 5.2.** *Let  $R$  be any ring with  $\widehat{F}_r(R) \not\subseteq N$ . Then  $R = R_1 \oplus R_2$ , where  $R_1$  is either  $GF(3)$  or a Boolean ring with 1, and  $R_2$  is a nil ring of index at most 3.*

PROOF. Let  $a \in \widehat{F}_r(R) \setminus N$ . By considering the set  $\{a, 2a\}$ , we see that  $2a^2 = 0$  or  $3a^2 = 0$ . By considering the set  $\{a, a^2\}$ , we see that one of the following holds:

- (i)  $a^3 = a^2$ ;
- (ii)  $a^4 = a^3$ ;
- (iii)  $a^4 = a^2 \neq a^3$ .

In case (i),  $e = a^2$  is an idempotent with  $ea = ae = e$ ; and in case (ii)  $e = a^3$  is an idempotent with  $ea = ae = e$ . In case (iii), it is obvious that  $e = a^2$  is an idempotent; and considering the set  $\{a, a + a^2\}$  shows that  $3a^2 = 0$  and  $a^4 = -a^3$ , so that  $ae = -e$ .

We establish next that in every case,  $e \in Z$ . For each  $x \in R$ , the set  $\{a, ex - exe\}^2 = \{a^2, 0\}$ ; and since  $a(ex - exe) = \pm(ex - exe) \in N$ , we must have  $ex - exe = 0$ . Similarly,  $xe - exe = 0$ , hence  $e \in Z$  as required.

In fact,  $a \in Z$ , as we now show. For fixed  $x \in R$ , consider the set  $A = \{a, (1 - e)x\}$ , where 1 is purely formal and  $(1 - e)x = x - ex$ . Since  $((1 - e)x)^2$ ,  $a(1 - e)x$  and  $(1 - e)xa$  are all left-annihilated by  $a^3$  and therefore not equal to  $a^2$ , we have  $A^2 = \{a^2, ((1 - e)x)^2\}$  and  $a(1 - e)x = (1 - e)xa$ —i.e.  $ax - aex = xa - exa$ . But  $aex = \pm ex = \pm xe = xea = exa$ , hence  $ax = xa$ . Thus,  $a \in Z$ .

Since  $e \in Z$ , we have the direct-sum decomposition  $R = eR \oplus A(e)$ . Moreover, if  $e = ea$ ,  $|\{e, ex\}^2| = |e\{a, x\}^2| \leq 2$ ; and if  $e = -ea$ ,  $|\{e, -ex\}^2| = |e\{a, x\}^2| \leq 2$ . Thus,  $e \in \widehat{F}_r(eR)$ ; and by Theorem 5.1,  $eR$  is either a Boolean ring or  $GF(3)$ .

We complete the proof by showing that  $A(e)$  is nil of index at most 3. Since  $e$  is either  $a^2$  or  $a^3$ , it will suffice to show that  $A(a^3)$  has this property. Let  $x \in A(a^3)$ . Since  $a \in Z$ ,  $\{a, x\}^2 = \{a^2, ax, x^2\}$ ; and since  $a^2 = ax$  or  $a^2 = x^2$  implies  $a \in N$ , we have

$$x^2 = ax. \tag{5.1}$$

The same argument applied to  $\{a, x^2\}$  gives  $x^4 = ax^2$ ; and since (5.1) yields  $x^3 = ax^2$ , we have  $x^4 = x^3$  and hence  $x^6 = x^5 = x^4 = x^3$ . But it follows from (5.1) that  $x^6 = (ax)^3 = a^3x^3 = 0$ , so  $x^3 = 0$ . ■

## ACKNOWLEDGEMENT

Howard E. Bell was supported by the Natural Sciences and Engineering Research Council of Canada, Grant 3961.

## REFERENCES

- [1] H.E. Bell and A.A. Klein, On rings with redundancy in multiplication, *Archiv der Mathematik* **51** (1988), 500–504.
- [2] H.E. Bell, A near-commutativity property for rings, *Results in Mathematics* **42** (2002), 28–31.
- [3] G.A. Freiman, On two- and three-element subsets of groups, *Aequationes Mathematicae* **22** (1981), 140–52.