Pacific Journal of Mathematics

ZERO SQUARE RINGS

RICHARD PETER STANLEY

Vol. 30, No. 3 November 1969

PACIFIC JOURNAL OF MATHEMATICS
Vol. 30, No. 3, 1969

ZERO SQUARE RINGS

RICHARD P. STANLEY

A ring R for which $x^2 = 0$ for all $x \in R$ is called a *zero-square ring*. Zero-square rings are easily seen to be locally nilpotent. This leads to two problems: (1) constructing finitely generated zero-square rings with large index of nilpotence, and (2) investigating the structure of finitely generated zero-square rings with given index of nilpotence. For the first problem we construct a class of zero-square rings, called *free* zero-square rings, whose index of nilpotence can be arbitrarily large. We show that every zero-square ring whose generators have (additive) orders dividing the orders of the generators of some free zero-square ring is a homomorphic image of the free ring. For the second problem, we assume $R^n \neq 0$ and obtain conditions on the additive group R_+ of R (and thus also on the order of R). When $n = 2$, we completely characterize R_+. When $n > 3$ we obtain the smallest possible number of generators of R_+, and the smallest number of generators of order 2 in a minimal set of generators. We also determine the possible orders of R.

Trivially every null ring (that is, $R^2 = 0$) is a zero-square ring. From every nonnull commutative ring S we can make $S \times S \times S$ into a nonnull zero square ring R by defining addition componentwise and multiplication by

$$(x_1, y_1, z_1) \times (x_2, y_2, z_2) = (0, 0, x_1y_2 - x_2y_1) .$$

In this example we always have $R^3 = 0$. If S is a field, then R is an algebra over S. Zero-square algebras over a field have been investigated in [1].

2. Preliminaries. Every zero-square ring is anti-commutative, for $0 = (x + y)^2 = x^2 + xy + yx + y^2 = xy + yx$. From anti-commutativity we get $2R^3 = 0$, for $yzx = y(-xz) = -(yx)z = xyz$ and $(yz)x = -x(yz)$, so $2xyz = 0$ for all $x, y, z \in R$. It follows that a zero-square ring R is commutative if and only if $2R^2 = 0$.

If R is a zero-square ring with n generators, then any product of $n + 1$ generators must contain two factors the same. By applying anti-commutativity we get a square factor in the product; hence $R^{n+1} = 0$. In particular, every zero-square ring is locally nilpotent.

If G is a finitely generated abelian group, then by the fundamental theorem on abelian groups we have

$$(1) \qquad G = C_{a_1} \oplus \cdots \oplus C_{a_n},\ a_i \mid a_{i+1} \text{ for } 1 \leqq i \leqq k - 1\ ,$$
$$a_{k+1} = \cdots = a_n = \infty\ ,$$

where C_{a_i} is a cyclic group of order a_i. If $X = \{x_1, \cdots, x_n\}$ generates G and if there is some decomposition (1) for which x_i generates C_{a_i}, $1 \leqq i \leqq n$, then we call X a *standard set of (group) generators* for G. Now let R be any finitely generated ring with a minimal set of ring generators $X' = \{x_1, \cdots, x_n\}$. Let $\langle X' \rangle$ denote the additive group generated by X' (whose elements are considered now as group, not ring, generators), and let X be a standard set of generators for $\langle X' \rangle$. Then X generates R as a ring since it generates $\langle X' \rangle$ as a group. Such a set X will be called a *standard set of ring generators* for R, and it follows that every finitely generated ring has a standard set of ring generators.

3. Free zero-square rings. For every positive integer n and every n-tuple $(a_1, \cdots, a_n)$, where $a_i \mid a_{i+1}$ for $i = 1, \cdots, k-1$, and $a_{k+1} = \cdots = a_n = \infty$, we define the *free* zero-square ring $R_F(a_1, \cdots, a_n)$ and derive its basic properties. Free zero-square ring are constructed from combinations of indeterminates called special monomials.

DEFINITION 3.1. Let $a_1, \cdots, a_n$ be integers $\geqq 2$ or ∞, such that for some $k \leqq n$, $a_i \mid a_{i+1}$ for $i = 1, \cdots, k-1$, while $a_{k+1} = \cdots = a_n = \infty$; and let $x_1, \cdots, x_n$ be indeterminates. We say that $x_{i_1} x_{i_2} \cdots x_{i_q}$ is a *special monomial* if $1 \leqq i_1 < i_2 < \cdots < i_q \leqq n$, and if a_{i_1} is even or ∞ whenever $q > 2$.

Thus the special monomials consist of

$$\begin{aligned} &x_i\,, && 1 \leqq i \leqq n \\ &x_i x_j\,, && 1 \leqq i < j \leqq n \\ &x_{i_1} x_{i_2} \cdots x_{i_q}\,, && q \geqq 3 \text{ and } a_{i_1} \text{ even or } \infty\,. \end{aligned}$$

Now let $y_1, y_2, \cdots, y_r$ denote the r distinct special monomials (in some order) corresponding to $a_1, a_2, \cdots, a_n$. If $y_j = x_{i_1} x_{i_2} \cdots x_{i_q}$ is a special monomial, we define

$$b_j = b(y_j) = \begin{cases} a_{i_1}, & \text{if } q = 1 \text{ or } 2 \\ 2, & \text{if } q \geqq 3\,. \end{cases}$$

Let $R_F(a_1, \cdots, a_n)$ denote the set of formal sums

$$R_F(a_1, \cdots, a_n) = \left\{ \sum_{i=1}^{r} c_i y_i \,\middle|\, 0 \leqq c_j < b_j \text{ if } b_j \neq \infty\,, \right.$$
$$\left. -\infty < c_j < \infty \text{ if } b_j = \infty \right\}.$$

We define addition and multiplication on R_F as follows:

Addition. Define

$$\sum_{i=1}^{r} c_i y_i + \sum_{i=1}^{r} d_i y_i = \sum_{i=1}^{r} e_i y_i ,$$

where $e_i \equiv c_i + d_i \pmod{b_i}$, $0 \leqq e_i < b_i$ if $b_i \neq \infty$, $e_i = c_i + d_i$ if $b_i = \infty$. We are adding the i^{th} components mod b_i.

Multiplication. We first define multiplication of special monomials. If y_i and y_j have a factor x_s in common, define $y_j y_i = y_i y_j = 0$. In particular, $x_s^2 = 0$. If $y_i = x_s, y_j = x_t$ with $s < t$, define $(ay_i)(by_j) = \overline{ab}\, x_s x_t$; where if $b_i \neq \infty$, then $\overline{ab}$ is defined by $\overline{ab} \equiv ab \pmod{b_i}$, $0 \leqq \overline{ab} < b_i$, while if $b_i = \infty$, then $\overline{ab} = ab$. If we think of a and b as representatives of the congruence classes mod b_i and b_j, then since $b_i \mid b_j$ the product ab always represents the same element mod b_i regardless of the choice of a and b. Similarly define $(by_j)(ay_i) = \overline{-ab}(x_s x_t)$. If y_i and y_j do not have a factor x_s in common, and if at least one of y_i, y_j contains at least two distinct factors x_s and x_t, then define $(ay_i)(by_j) = cy_l$, where y_l is obtained by rearranging the factors x_h of y_i and y_j in ascending subscript order and defining

$$c = \begin{cases} 0, \text{ if } a_q \text{ is odd} \\ 0, \text{ if } a_q \text{ is even or } \infty \text{ and } ab \text{ is even} \\ 1, \text{ if } a_q \text{ is even or } \infty \text{ and } ab \text{ is odd} , \end{cases}$$

where a_q is the order of the indeterminate x_q with least subscript appearing in y_l.

We now define in general

$$\Big(\sum_i c_i y_i\Big)\Big(\sum_j d_j y_j\Big) = \sum_{i,j} (c_i y_i)(d_j y_j) ,$$

where this sum is to be rearranged according to the previously defined rules of special monomial multiplication and of addition.

We call this set $R_F(a_1, \cdots, a_n)$, together with the operations of addition and multiplication just defined, the *free zero square ring* $R_F(a_1, \cdots, a_n)$.

THEOREM 3.2. *$R_F(a_1, \cdots, a_n)$ is a zero-square ring.*

Proof. All the desired properties follow from the definitions except associativity of multiplication and the zero-square property.

It follows from the definition of multiplication that we need only to verify associativity for monomials $c_h y_h$, where c_h is a constant between 0 and $b_h - 1$ for $b_h \neq \infty$, while $-\infty < c_h < \infty$ for $b_h = \infty$, and y_h is a special monomial. But if either of y_h, y_i, y_j contain an indeterminate x_s of odd order, then $(c_h y_h)(c_i y_i)(c_j y_j) = 0$ upon any association, while if all orders are even or ∞, then

$$(c_h y_h)(c_i y_i)(c_j y_j) = \begin{cases} 0, \text{ if two of } y_h, y_i, y_j \text{ contain} \\ \quad \text{a common factor } x_e \\ 0, \text{ if any of } c_h, c_i, c_j \text{ is even} \\ \quad y_h y_i y_j, \text{ otherwise} \end{cases}$$

upon any association.

It remains only to show $(\sum c_i y_i)^2 = 0$. Now

$$(\sum c_i y_i)^2 = \sum_{i<j} c_i c_j (y_i y_j + y_j y_i) + \sum c_i^2 y_i^2 \,.$$

The latter sum is 0 by definition of special monomial multiplication. If $y_i y_j$ is the product of more than two indeterminates, then

$$c_i c_j (y_i y_j + y_j y_i) = 2 c_i c_j y_i y_j = 0 \,,$$

since either $y_i y_j = 0$ or $2 c_i c_j$ is taken mod 2. This completes the proof.

THEOREM 3.3. *If $a_n \neq \infty$ and i is the least integer for which a_i is even (except that if a_n is odd, put $i = n$), then $R_F(a_1, \cdots, a_n)$ has order*

$$a_1^n a_2^{n-1} \cdots a_n^1 2^{2^{n-i+1}-1} 2^{-(n-i+1)(n-i+2)/2} \,.$$

Proof. In general there are $\binom{n-j}{k-1}$ distinct special monomials with k factors such that j is the least subscript appearing among the factors. Such a monomial has order a_j if $k \leqq 2$, while if $k > 2$ the monomial has order 2 when a_j is even and vanishes when a_j is odd. Thus the order of R_F is given by

$$\begin{aligned} &(a_1 a_2 \cdots a_n)(a_1^{n-1} a_2^{n-2} \cdots a_{n-1})\left[2^{\binom{n-i}{2} + \binom{n-i-1}{2} + \cdots + \binom{2}{2}}\right]. \\ &\qquad \cdot\left[2^{\binom{n-i}{3} + \binom{n-i-1}{3} + \cdots \binom{3}{3}}\right] \cdots \left[2^{\binom{n-i}{n-i}}\right] \\ &= a_1^n a_2^{n-1} \cdots a_n^1 2^{2^{n-i-1}-1} 2^{-(n-i+1)(n-i+2)/2} \,, \end{aligned}$$

as asserted.

The next theorem elucidates the "free" nature of R_F.

THEOREM 3.4. *If R is a zero-square ring with a standard set of ring generators $x_1', \cdots, x_n'$ of orders $a_1', \cdots, a_n'$, and if $R_F(a_1, \cdots, a_n)$ is a free zero-square ring with $a_i' \mid a_i$ for $1 \leqq i \leqq n$ (with the convention that every integer and ∞ are divisors of ∞), then R is a homomorphic image of $R_F(a_1, \cdots, a_n)$.*

Proof. Let $x_1, \cdots, x_n$ be the indeterminates (generators) of R_F. Let $y_1, \cdots, y_r$ be the special monomials of R_F and $y'_1, \cdots, y'_r$ the corresponding monomials of R, so that if $y_i = x_{i_1} \cdots x_{i_g}$, then $y'_i = x'_{i_1} \cdots x'_{i_g}$. (Of course for some i we may have $y'_i = 0$.) We then claim that the mapping $\varphi: \sum c_i y_i \to \sum c_i y'_i$ is the desired homomorphism.

Since $a'_i \mid a_i$, the ring of integers mod a'_i is a homomorphic image of the ring of integers mod a_i. It follows from its definition that φ preserves sums and products. It remains only to verify that φ is onto R, i.e., that every element of R occurs among $\sum c_i y'_i$, $0 \leqq c_i < b_i$ if $b_i \neq \infty$, $-\infty < c_i < \infty$ if $b_i = \infty$. This, however, is an immediate consequence of the fact that R is anti-commutative and satisfies $R^{n+1} = 0$ and $2R^3 = 0$, and that the order of an anti-commutative product cannot exceed the g.c.d. of the orders of its factors. This completes the proof.

In general, a subring (or ideal) of $R_F(a_1, \cdots, a_n)$ need not be free. For instance, if $n > 2$ and each a_i is even, then $R_F^{[(n/2)+1]}$ is a null ideal with more than one generator.

If $R_F = R_F(a_1, \cdots, a_n)$ is a free zero-square ring such that i is the least integer for which a_i is even or ∞, and if $n - i \geqq 1$, then it is easily verified that R_F has index of nilpotence $n - i + 2$. Thus free zero-square rings provide examples of zero-square rings with arbitrarily large index of nilpotence.

4. Nonnull finite zero-square rings.

In this section we characterize the additive groups of nonnull finite zero-square rings and as a corollary characterize the orders of such rings. For this purpose we introduce a function $f(G)$ of a finitely generated abelian group G.

DEFINITION 4.1. If G is a finitely generated abelian group, define $f(G) = \max\{n: R \text{ is a zero-square ring}, R^n \neq 0, G \text{ is isomorphic to the additive group } R_+ \text{ of } R\}$.

It follows from the local nilpotence of zero-square rings that $f(G)$ is finite. In this section and the next we assume G is finite to avoid looking at a large number of cases. The results can easily be extended to arbitrary finitely generated G.

THEOREM 4.2. *Let G be a finite abelian group. Then $f(G) \geqq 2$ if and only if either of the following hold*:

(i) *The dimension of G is greater than two*; *or*

(ii) *$G = C_{a_1} \oplus C_{a_2}$, where $a_1 \mid a_2$ and either $(a_2/a_1, a_1) \neq 1$ or a_1 is divisible by a square > 1.* (This condition on a_1 and a_2 is equivalent to $a_1 \mid a_2$ and the existence of an integer b, $0 < b < a_2$, such that $a_2 \mid b(a_1, b)$.)

Proof. We first prove sufficiency of (i) and of (ii). Assume that $G = C_{a_1} \oplus C_{a_2} \oplus \cdots \oplus C_{a_n}$, with $a_i \mid a_{i+1}$ and $n \geqq 3$. Let Z be the null ring with additive group $C_{a_4} \oplus C_{a_5} \oplus \cdots \oplus C_{a_n}$. Let x_1, x_2 be generators for the free ring $R_F(a_2, a_3)$, and let J be the ideal of R_F generated by $a_1x_1x_2$. Then it is easily seen that the ring $(R_F/J) \oplus Z$ is a nonnull zero-square ring with additive group isomorphic to G. This proves the sufficiency of (i).

The equivalency of the two conditions in (ii) can be verified straightforwardly. To prove the sufficiency of (ii), assume that $G = C_{a_1} \oplus C_{a_2}$ where a_1 and a_2 satisfy the conditions of (ii). In view of Theorem 3.4 we need to prove that if $R_F(a_1, a_2)$ is generated by x_1, x_2, then the ideal J generated by $x_1x_2 - bx_2$ does not contain x_1x_2, where b is defined in (ii). Assume to the contrary that $x_1x_2 \in J$. Then for some $y \in R_F$ and some integer c,

$$x_1x_2 = c(x_1x_2 - bx_2) + y(x_1x_2 - bx_2) .$$

Since $y(x_1x_2 - bx_2)$ contains no term in x_2, we must have $cbx_2 = 0$. This means $a_2 \mid bc$. The remaining way an x_1x_2 term can appear is for $y = dx_1$. Thus we get

$$x_1x_2 = (c - bd)x_1x_2 .$$

We therefore have $(a_1, c - bd) = 1$, since the order of x_1x_2 in $R_F(a_1, a_2)$ is a_1. This implies $(a_1b, bc - b^2d) = b$. We have just proved $a_2 \mid bc$, and from $a_2 \mid b(a_1, b)$ we get $a_2 \mid a_1b$ and $a_2 \mid b^2$. Thus $a_2 \mid (a_1b, bc - b^2d)$, or $a_2 \mid b$, contradicting $0 < b < a_2$. This proves the sufficiency of (ii).

If G has one generator, then R is clearly null. Hence to prove necessity, we need to show that if R is generated by x_1, x_2 of orders a_1, a_2 with $a_1 | a_2$ and $R^2 \neq 0$, then a_1 and a_2 satisfy the conditions in (ii). Let

$$x_1x_2 = b_1x_1 + b_2x_2$$

in R. Without loss of generality it may be assumed that $0 \leqq b_1 < a_1$, $0 \leqq b_2 < a_2$.

Assume first that $b_2 = 0$. Then $x_1x_2 = b_1x_1$, so $0 = x_1x_2^2 = b_1x_1x_2 = b_1^2x_1$; hence $a_1 \mid b_1^2$. If a_1 is divisible by a square > 1, we have satisfied one of the conditions. Otherwise $b_1 = 0$ since $b_1 < a_1$. In this case R is null, a contradiction.

Now consider the remaining case $x_1x_2 = b_1x_1 + b_2x_2$, $b_2 \neq 0$. Let c be the order of x_1x_2. Then from $0 = cx_1x_2 = cb_1x_1 + cb_2x_2$, we get $0 = cb_1x_1 = cb_2x_2$, so $a_2 \mid cb_2$. Moreover, $0 = x_1^2x_2 = b_2x_1x_2$ gives $c \mid b_2$. Thus $a_2 \mid b_2^2$. But $a_1x_1x_2 = a_1b_2x_2$ gives $a_2 \mid a_1b_2$. Then from $a_2 \mid b_2^2$ and $a_2 \mid a_1b_2$ we deduce $a_2 \mid b_2(a_1, b_2)$. Since $b_2 \neq 0$, we can take $b = b_2$. This completes the proof.

COROLLARY 4.3. *There exists a nonnull finite zero-square ring of order r if and only if r is divisible by a cube.*

COROLLARY 4.4. *The smallest nonnull zero-square ring has order* 8.

A simple direct proof of Corollary 4.4 is given in [2], (see also Th. 5.7.) It can be shown that there are exactly two nonisomorphic nonnull zero-square rings of order 8. One of these is $R_F(2, 2)$.

5. Additive group structure of finite zero-square rings. In this section we extend Theorem 4.2 by considering conditions on G which make $f(G) \geqq n$ for $n > 2$. Theorem 5.5 gives some necessary conditions, while Theorem 5.6 provides a converse.

R will denote a finite zero-square ring and R_+ its additive group, while G denotes a finite abelian group and G_2 its Sylow 2-subgroup. Let $x_1, x_2, \cdots, x_n$ be a fixed standard set of ring generators of R. Let x denote the element $x_1x_2 \cdots x_n$ and $\overline{x_i}$ the element $x_1x_2 \cdots x_{i-1}x_{i+1} \cdots x_n$. More generally, if $y = x_{i_1}x_{i_2} \cdots x_{i_m}$, $i_1 < i_2 < \cdots < i_m$, then $\bar{y}$ denotes the element $x_{j_1}x_{j_2} \cdots x_{j_{n-m}}$, $j_1 < j_2 < \cdots < j_{n-m}$, such that the i's and j's include all the integers $1, 2, \cdots, n$. When $n > 2$ note that $y\bar{y} = x$. If $x \neq 0$, we call m the *length* of y, denoted by $|y|$. Note $|y| + |\bar{y}| = n$. If $z \in R$, then $c(z)$ denotes the additive order of z.

LEMMA 5.1. *Every symmetric matrix of odd order over $GF(2)$ with 0's on the main diagonal is singular.*

The proof is a straightforward application of the definition of the determinant and will be omitted.

LEMMA 5.2. *If a matrix E has the form*

$$E = \begin{pmatrix} E_1 & & & 0 \\ & E_2 & & \\ & & \ddots & \\ * & & & E_t \end{pmatrix},$$

where the E_k are square matrices and some E_j is singular, then E is singular.

Proof. This is a special case of the well-known result $\det E = (\det E_1) \cdots (\det E_t)$.

The next theorem reduces the problem of evaluating $f(G)$ to the case where G is a 2-group.

THEOREM 5.3. *If G is a finite abelian group and $f(G) \geqq 3$, then $f(G) = f(G_2)$.*

Proof. Let R be a finite zero-square ring with $R^n \neq 0, n \geqq 3$. By anti-commutativity the elements R' of R whose additive order is a power of two form a subring. If $z_i \in R, 1 \leqq i \leqq n$, such that $z_1 z_2 \cdots z_n \neq 0$, where $c(z_i) = a_i 2^{b_i}$, a_i odd, then $a_i z_i \in R'$ and

$$(a_1 z_1)(a_2 z_2) \cdots (a_n z_n) \neq 0$$

since $2 z_1 z_2 \cdots z_n = 0$. Hence $(R')^n \neq 0$, so $f(G_2) \geqq f(G)$.

Conversely, assume $R^n \neq 0$ and R_+ is a 2-group. If G is a finite abelian group with $G_2 \cong R_+$, write $G = G_2 \oplus H$, and let S be the null ring with $S_+ \cong H$. Then $(R \oplus S)_+ \cong G$ and $(R \oplus S)^n \neq 0$, so that $f(G_2) \leqq f(G)$. Thus $f(G) = f(G_2)$ and the theorem is proved.

We can now assume in what follows that the additive group R_+ of R is a 2-group.

LEMMA 5.4. *Let R be a finite zero-square ring (with R_+ a 2-group) with $n \geqq 3$ elements $x_1, \cdots, x_n$ satisfying $x = x_1 \cdots x_n \neq 0$.*

(i) *There exists a standard set of group generators for R_+ containing every special monomial y_j in the x_i of length $3 \leqq |y_j| \leqq n-2$.*

(ii) *The group generated by those y_j satisfying $1 \leqq |y_j| \leqq n-2$ is generated irredundantly by them (though not necessarily standardly).*

(iii) *If we assume $x_1, \cdots, x_n$ is a standard set of ring generators for the ring R' they generate, then there exists a standard set of group generators for R'_+ containing every special monomial y_j in the x_i satisfying $|y_j| = 1$ or $3 \leqq |y_j| \leqq n-2$.*

Proof. (i) If G is a finite abelian p-group and $t_1, \cdots, t_s \in G$, then $t_1, \cdots, t_s$ extend to a standard set of group generators for G if and only if the following two condition are satisfied:

(1) For any integers $a_1, \cdots, a_s$,

$$\sum_{i=1}^{s} a_i t_i = pz \Rightarrow p \sum_{i=1}^{s} b_i t_i = pz ,$$

for some integers $b_1, \cdots, b_s$.

(2) For any integers $a_1, \cdots, a_s$,

$$\sum_{i=1}^{s} a_i t_i = 0 \Rightarrow a_i t_i = 0, \text{ all } i .$$

To prove (1) in our case, assume

$$\sum_{3 \leqq |y_i| \leqq n-2} a_i y_i = 2z \; . \tag{3}$$

Since $2y_i = 0$ when $|y_i| \geqq 3$, we can take $a_i = 0$ or 1. Let y_j be a special monomial of minimal length satisfying $a_j = 1$. Then from (3) we get

$$x = \overline{y_j} \sum_{3 \leqq |y_i| \leqq n-2} a_i y_i = 2(\overline{y_j} z) = 0 \; ,$$

since $\overline{y_j} z \in R^3$ when $|y_j| \leqq n-2$. This contradicts $x \neq 0$ and proves (1).

To prove (2), assume

$$\sum_{3 \leqq |y_i| \leqq n-2} a_i y_i = 0 \; , \tag{4}$$

where at least one $a_i y_i \neq 0$. As in (1), let y_j be of minimal length such that $a_j y_j \neq 0$. Multiplying (4) by $\overline{y_j}$ gives the contradiction $x = 0$, and completes the proof of (i).

(ii) We need to prove that

$$\sum_{1 \leqq |y_i| \leqq n-2} a_i y_i = 0 \Rightarrow a_i = 2b_i \text{ all } i \; . \tag{5}$$

Letting y_j be of minimal length such that $a_i \neq 2b_i$ for any integer b_i, an argument similar to those used in (i) leads to a contradiction.

(iii) We must show (1) and (2) hold, where the t_i's are the y_j's satisfying $|y_j| = 1$ or $3 \leqq |y_j| \leqq n-2$, and $p=2$. The proof of (1) is similar to the proof of (5). To prove (2), assume that

$$\sum_{i=1}^{n} a_i x_i + \sum_{3 \leqq |y_j| \leqq n-2} b_j y_j = 0 \; .$$

By (1), each $b_j y_j = 0$. It follows that each $a_i x_i = 0$ since $x, \cdots, x_n$ is a standard set of ring generators. This completes the proof of the lemma.

We can now give necessary conditions for $f(G) \geqq n \geqq 4$.

THEOREM 5.5. *Let G be a finite abelian 2-group.*

(i) *If $f(G) \geqq n \geqq 4$, then the dimension of G is at least* $2^n - 2[(n+2)/2]$, i.e., *every generating set of G has at least $2^n - 2[(n+2)/2]$ elements*. (Brackets denote the integer part.)

(ii) *If $f(G) \geqq n \geqq 4$, then at least $2^n - n(n+1)/2 - 2[(n+2)/2]$ generators in a standard set of generators for G have order* 2.

Proof. (i) Suppose R is a zero-square ring with $R^n \neq 0$ and $R_+ \cong G$, and that $x_1 x_2 \cdots x_n \neq 0$ in $R(n \geqq 4)$. Let R' be the subring of R generated by $x_1, x_2, \cdots, x_n$. Since $\dim R'_+ \leqq \dim R_+$, it suffices to show $\dim R'_+ \geqq 2^n - 2[(n+2)/2]$. By Lemma 5.4 (ii), $\dim R'_+$ is equal to at least the number of special monomials y_i in the indeterminates $x_1, \cdots, x_n$ satisfying $1 \leqq |y_i| \leqq n-2$. The number of such special monomials is $\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-2} = 2^n - n - 2$. Hence to complete the proof of (i) we need only to prove that when n is odd, we cannot have $\dim R'_+ = 2^n - n - 2$.

Assume that n is odd and R'_+ has $2^n - n - 2$ generators, $R'^n \neq 0$. By Lemma 5.4 there is a standard set of group generators for R'_+ containing (1) $x_1, \cdots, x_n$, (2) all special monomials y_j in the x_i satisfying $3 \leqq |y_j| \leqq n-2$, and (3) a standard set of generators $y'_1, \cdots, y'_m \left(m = \binom{n}{2}\right)$ for the group generated by all y_j of length 2. Since this accounts for $2^n - n - 2$ generators, these in fact generate all of R'_+. In particular the special monomials $\overline{x_1}, \cdots, \overline{x_n}$ of length $n-1$ can be written as

$$\overline{x}_j = \sum_{1 \leqq |y_i| \leqq n-2} b_{ij} y_i , \qquad j = 1, \cdots, n , \tag{6}$$

where b_{ij} is an integer. (This representation may not be unique since the y_i's of length 2 need not be standard generators.)

We show that b_{ij} is even. Let y_k be a term appearing on the right side of (6) whose coefficient b_{k_j} is odd, such that no y_i of smaller length has an odd coefficient. Then we get $0 = \overline{x}_j \overline{y}_k = b_{k_j} y_k \overline{y_k} = x$, a contradiction, so every b_{ij} is even. In particular, the terms $b_{ij} y_i$ with $|y_i| \geqq 3$ vanish since $2R'^3 = 0$. If we re-express $\overline{x_j}$ as a linear combination of the standard generators given above, then the terms $b_{ij} y_i$ with $|y_i| = 1$ remain the same. Since $2\overline{x_j} = 0$ when $n > 3$, we have $b_{ij} = 1/2\, c(y_i)$ or $b_{ij} = 0$ whenever $|y_i| = 1$. (This is where the argument fails for $n = 3$.) Hence we can rewrite (6) as

$$\overline{x}_j = 2z_j + \sum_{i=1}^{n} h_{ij} \left(\frac{1}{2}\, c(x_i)\right) x_i , \tag{7}$$

where

$$2z_j = \sum_{|y_i|=2} b_{ij} y_i ,$$

and where $h_{ij} = 0$ or 1.

We claim that the matrix $H = (h_{ij})$ over $GF(2)$ is nonsingular. If H were singular, then if we regard $1/2\, c(x_j) x_j$ as indeterminates over $GF(2)$, we can eliminate them from (7) and get a relation of the form

$$\sum_{i=1}^{n} r_i (\overline{x_i} + 2z_i) = 0 ,$$

where some $r_j = 1$. But then

$$x = x_j \sum_{i=1}^{n} r_i(\overline{x_i} + 2z_i) = x_j \cdot 0 = 0 ,$$

a contradiction. Hence H is nonsingular.

Therefore we can solve (7) for the n unknowns $1/2\, c(x_j)x_j$ over $GF(2)$ to get

$$\frac{1}{2} c(x_j)x_j = 2 \sum_{i=1}^{n} e_{ij}z_i + \sum_{i=1}^{n} e_{ij}\overline{x_i} , \qquad j = 1, \cdots, n , \tag{8}$$

where each $e_{ij} = 0$ or 1. If E denotes the matrix (e_{ij}) over $GF(2)$, then $E = H^{-1}$, so E is nonsingular.

We will now reach a contradiction by showing that E is singular. We first show $e_{jj} = 0$. We have

$$0 = \frac{1}{2} c(x_j)x_j^2 = 2 \sum_{i=1}^{n} e_{ij}z_ix_j + \sum_{i=1}^{n} e_{ij}\overline{x_i}x_j = e_{jj}x .$$

Since $x \neq 0$, $e_{jj} = 0$.

Define $s_1, s_2, \cdots, s_t$ by

$$\begin{aligned} c(x_1) = c(x_2) = \cdots = c(x_{s_1}) \\ < c(x_{s_1+1}) = c(x_{s_1+2}) = \cdots = c(x_{s_2}) \\ < \cdots < c(x_{s_{t-1}+1}) = \cdots = c(x_{s_t}) , \end{aligned}$$

where $s_t = n$. Let E_k be the square submatrix of E defined by $E_k = (e_{ij})$, $s_{k-1} + 1 \leqq i, j \leqq s_k$, for $k = 1, 2, \cdots, t$. (Here s_0 is taken to be 0.) We show that each E_k is symmetric. Assume $e_{ij} = 1$ for some $s_{k-1} + 1 \leqq i, j \leqq s_k$. Then from (8) we get $1/2\, c(x_j)x_ix_j = x$, so $1/2\, c(x_j)x_ix_j \neq 0$. But $1/2\, c(x_j) = 1/2\, c(x_i)$, as $s_{k-1} + 1 \leqq i, j \leqq s_k$. Hence $1/2\, c(x_i)x_ix_j \neq 0$. From (8) we again get $0 \neq 1/2\, c(x_i)x_ix_j = e_{ji}x$, so $e_{ji} = 1$. This proves that E_k is symmetric. Moreover, E_k has 0's on the main diagonal since each $e_{jj} = 0$.

We now show that if for some k we have $i \leqq s_k, j > s_k$, then $e_{ij} = 0$. As in the previous paragraph we have

$$\frac{1}{2} c(x_j)x_ix_j = e_{ij}x . \tag{9}$$

Since $i \leqq s_k, j > s_k$ we have $c(x_i) < c(x_j)$. Therefore $1/2\, c(x_i)x_ix_j \neq 0$. But from (4), $1/2\, c(x_i)x_ix_j = e_{ji}x$, so $c(x_i)x_ix_j = 2e_{ji}x = 0$ (since $2x = 0$). But $c(x_i) < c(x_j)$ implies $c(x_i) \leqq 1/2\, c(x_j)$, so $1/2\, c(x_j)x_ix_j = 0$. Comparing with (9) shows $e_{ij} = 0$, as asserted.

This shows that E has the form given in Lemma 5.2. Since the sum of the orders of the E_j must be the order of E, some E_k has odd order. Then by Lemma 5.1 E_k is singular, so by Lemma 5.2 E is singular, a contradiction. This completes the proof of (i).

(ii) Using the notation of part (i), it follows from $2R'^3 = 0$ that every special monomial y_i satisfying $3 \leqq |y_i| \leqq n-2$ has order 2. There are $\binom{n}{3} + \binom{n}{4} + \cdots + \binom{n}{n-2} = 2^n - n(n+1)/2 - (n+2)$ such y_i, and by Lemma 5.4 they extend to a standard set of group generators for R_+. Moreover, we have just shown that when n is odd, there is at least one y_j with $|y_j| = n-1$ which cannot be expressed in the form $y_j = \sum_{1 \leqq |y_i| \leqq n-2} s_i y_i$. Exactly as in the proof of Lemma 5.4 it follows that the set of all y_i satisfying $3 \leqq |y_i| \leqq n-2$, along with y_j, extend to a standard set of group generators for R_+. Thus we have found $2^n - n(n+1)/2 - 2[(n+2)/2]$ generators of order 2, proving (ii) and completing the proof of the theorem.

The following theorem shows that the results of the previous theorem are best possible.

THEOREM 5.6. *Let $n \geqq 4$ be an integer.*

(i) *Given any integer $N \geqq 2^n - 2[(n+2)/2]$, there exists a finite abelian 2-group G of dimension N, such that $f(G) = n$.*

(ii) *Given any integer $M \geqq 2^n - n(n+1)/2 - 2[(n+2)/2]$, there exists a finite abelian 2-group G with precisely M generators of order 2 (in a standard set of generators), such that $f(G) = n$.*

Proof. Clearly to prove both (i) and (ii) it suffices to construct a finite zero-square ring R with $R^n \neq 0\,(n \geqq 4)$, such that R_+ has precisely $N = 2^n - 2[(n+2)/2]$ standard group generators, with precisely $M = 2^n - n(n+1)/2 - 2[(n+2)/2]$, of these generators of order 2. Let $m = [n/2]$ and let $R_F(a_1 = 8, a_2 = 8, \cdots, a_n = 8)$ be a free ring with generators $x_1, \cdots, x_n$ (as defined in §3). If n is even let J be the ideal generated by $\{\bar{x}_1 - 4x_2, \bar{x}_2 - 4x_1, \bar{x}_3 - 4x_4, \bar{x}_4 - 4x_3, \cdots, \bar{x}_{n-1} - 4x_n, \bar{x}_n - 4x_{n-1}\}$, while if n is odd let J be generated by $\{\bar{x}_1 - 4x_2, \bar{x}_2 - 4x_1, \cdots, \bar{x}_{n-2} - 4x_{n-1}, \bar{x}_{n-1} - 4x_{n-2}\}$. Let $R = R_F/J$. Then R is generated by the images of all y_i satisfying $1 \leqq |y_i| \leqq n-2$ when n is even; with the additional generator $\bar{x}_n$ when n is odd. This gives a total of $2^n - 2[(n+2)/2]$ generators, as desired. Moreover, when n is even, a standard set of group generators for R_+ has $n+1$ elements of order 8, $2m^2 - m - 1$ elements of order 4, and exactly M elements of order 2. When n is odd, there are $n+1$ elements of order 8, $2m^2 + m - 1$ elements of order 4, and exactly M elements of order 2. Hence it remains to prove that the image of x in R_F/J is not 0, i.e., that $x \notin J$. We treat only the case when n is even; the case n odd is almost exactly the same.

Assume $x \in J$. Then

$$x = z_1(\bar{x}_1 - 4x_2) + z_2(\bar{x}_2 - 4x_1) + \cdots + z_n(\bar{x}_n - 4x_{n-1}) \\ + b_1(\bar{x}_1 - 4x_2) + b_2(\bar{x}_2 - 4x_1) + \cdots + b_n(\bar{x}_n - 4x_{n-1}) ,$$

where $z_i \in R_F$, $b_i = 0$ or 1. Hence we need at least one $z_j = x_j$, say $z_1 = x_1$. We then also get the term $-4x_1x_2$, which can only be cancelled by $z_2 = x_2$, giving another $-4x_1x_2$. But this also gives another x, and $x + x = 0$. Hence $x \notin J$, and the theorem is proved.

REMARK. The proofs of Theorems 5.5 and 5.6 are not valid for $n = 3$, basically because from $|y_i| = n - 1$ we cannot deduce $2y_i = 0$. If Theorem 5.5 (i) were false for $n = 3$, then there would be a 2-group G with three generators such that $f(G) = 3$. Although this seems highly unlikely, the question remains open. Clearly G cannot have less than three generators. Note that Theorem 5.5 (ii) is trivially satisfied for $n = 3$. Finally, Theorem 5.6 is easy to verify for $n = 3$ (though in part (ii) we of course must have $M \geqq 0$).

It is considerably simpler to get results on the *order* of zero-square rings satisfying $R^n \neq 0$.

THEOREM 5.7. *Assume $n > 2$. Then there exists a zero-square ring of order r satisfying $R^n \neq 0$ if and only if $2^{2^n-1} \mid r$.*

Proof. Assume $R^n \neq 0$. We know from the proof of Theorem 5.3 that there are elements $x_1, \cdots, x_n$ in the Sylow 2-subgroup R_2 of R_+ such that $x_1 \cdots x_n \neq 0$. Let $y_1, y_2, \cdots, y_{2^n-1}$ be the special monomials in the x_i. Claim that the 2^{2^n-1} elements of the form $\sum_{i=1}^{2^n-1} b_i y_i$, $b_i = 0$ or 1, are all distinct, otherwise we would have a relation of the form

$$\sum b_i y_i = 0 ,$$

with at least one $b_i = 1$. Let y_j be a special monomial of shortest length such that $b_j = 1$. Then multiplying (6) by $\bar{y}_j$ gives $x = 0$, a contradiction. Hence R_2 has order at least 2^{2^n-1}, so that $2^{2^n-1} \mid |R_2|$. Hence $2^{2^n-1} \mid r$.

Conversely, if $2^{2^n-1} \cdot s = r$, then we take R_+ to be $C_2^{2^n-1} \oplus C_s$. If we impose the free ring $R_F(2, 2, \cdots, 2)$ on $C_2^{2^n-1}$ and the null ring on C_s, then $R^n \neq 0$.

Finally we have the result of [3].

COROLLARY 5.8. *The smallest zero-square ring R satisfying $R^n \neq 0$, $n > 1$, has order 2^{2^n-1}.*

References

1. A. Abian and W. A. McWorter, *On the index of nilpotency of some nil algebras*, Boll. Un. Mat. Ital. (3) **18** (1963), 252-255.
2. L. Carlitz, *Solution to E 1665*, Amer. Math. Monthly **72** (1965), 80.
3. G. A. Heuer, *Two undergraduate projects*, Amer. Math. Monthly **72** (1965), 945.

Received September 9, 1968. This paper was written for the 1965 Bell prize at the California Institute of Technology, under the guidance of Professor Richard A. Dean.

CALIFORNIA INSTITUTE OF TECHNOLOGY
HARVARD UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. **36**, 1539-1546. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

Pacific Journal of Mathematics
Vol. 30, No. 3 November, 1969