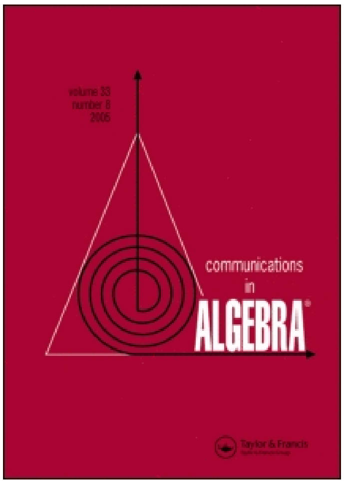
This article was downloaded by:
On: *7 January 2010*
Access details: *Access Details: Free Access*
Publisher *Taylor & Francis*
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Communications in Algebra
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713597239

Group rings R[G] with 3-generated ideals when R is artinian

Souâd Ameziane Hassani [a]; Marco Fontana [b]; Salah-Eddine Kabbaj [c]
[a] Département de Mathémutiques, Faculté des Sciences Suäss, Université S. M. Ben Abdelluh, Fès, Morocco [b] Dipartimento di Matemtica, Terza Universitià degli Studi di Roma, Italy [c] Département de Mathémutiques, Faculté des Sciences Dhar Al-Mehraz, Université S. M. Ben Abdelluh, Fès, Morocco

To cite this Article Hassani, Souâd Ameziane, Fontana, Marco and Kabbaj, Salah-Eddine(1996) 'Group rings R[G] with 3-generated ideals when R is artinian', Communications in Algebra, 24: 4, 1253 — 1280
To link to this Article: DOI: 10.1080/00927879608825637
URL: http://dx.doi.org/10.1080/00927879608825637

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.informaworld.com/terms-and-conditions-of-access.pdf

This article may be used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

COMMUNICATIONS IN ALGEBRA, 24(4), 1253-1280 (1996)

GROUP RINGS $R[G]$ WITH 3-GENERATED IDEALS WHEN R IS ARTINIAN

Souâd AMEZIANE HASSANI
Département de Mathématiques, Faculté des Sciences Saïss, Université S. M. Ben Abdellah, Fès, Morocco.

Marco FONTANA
Dipartimento di Matematica, Terza Università degli Studi di Roma, Italy.

Salah-Eddine KABBAJ
Département de Mathématiques, Faculté des Sciences Dhar Al-Mehraz, Université S. M. Ben Abdellah, Fès, Morocco.

Downloaded At: 16:36 7 January 2010

Let R be a commutative ring with identity. If an ideal I of R can be generated by n elements, then we say that I is *n-generated.* If every ideal of R is n-generated, we say that *the ring R has the n-generator property;* when R has this property then the Krull dimension of R is zero or one [S, Chapter 3, § 1, Theorem 1.2, p. 51].

Considerable interest has been shown in rings with the n-generator property (see for example [C], [Mc], [OV], [S], [Sh1]) and in the problem of determining when a group or monoid ring has the n-generator property, either in general or for a specific choice of n, see [AM], [M1], [M2], [ORV], [OV] and [Sh2].

In this paper, we consider the problem of determining when a group ring $R[G]$ has the 3-generator property, if R is an Artinian principal ideal ring or R has the 2-generator property.

From the restriction on Krull dimension, we have

$$1 \geq \dim R[G] = \dim R + \alpha \, ,$$

Copyright © 1996 by Marcel Dekker, Inc.

where α denotes the torsion free rank of G and $\dim R$ denotes the Krull dimension of R. Since, under our assumptions, $\dim R \leq 1$, we have $\alpha = 0$ or 1. If $\alpha = 0$, then G must be a finite group. If $\alpha = 1$, then $G \simeq \mathbb{Z} \oplus H$, where H is a finite Abelian group and $\mathbb{Z}$ denotes the group of the integers.

Since the case $\alpha = 1$ was considered in [OV, Theorem 5.1], this paper concerns the case $\alpha = 0$, i. e. the case of a finite Abelian group G.

All rings and groups considered in this paper are commutative and the groups are written additively. We refer to [G2] for elementary properties of group rings. If p is a prime integer, then the p-Sylow subgroup of the finite Abelian group G is denoted by G_p.

If I is an ideal in R, then $\mu(I)$ denotes the number of the elements of a minimal set of generators of I.

We recall that, if $R = R_1 \oplus R_2 \oplus ... \oplus R_s$ is a direct sum of rings, then R has the n-generator property if and only if each R_i has the n-generator property. If R is an Artinian ring, then $R = R_1 \oplus R_2 \oplus ... \oplus R_s$, where each R_i is a local Artinian ring. Therefore, in this case, $R[G]$ has the n-generator property if and only if $R_i[G]$ has the n-generator property for each R_i.

If R is an Artinian ring, in order to determine when the group ring $R[G]$ has the n-generator property, by the previous remarks it suffices to consider the cases where R is a field or R is an Artinian local ring which is not a field.

In this paper, we prove the following:

Theorem. *Let R be an Artinian ring with the 2-generator property and let G be a finite abelian group. Then $R[G]$ has the 3-generator property if and only if $R \simeq R_1 \oplus ... \oplus R_s$ where each (R_j, M_j) is a local Artinian ring with the 2-generator property, subject to:*

(A) *Assume R_j is a field of characteristic $p \neq 0$,*

(i) *if $p = 2$ then G_p is a homomorphic image of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^i\mathbb{Z}$, where $i \geq 0$;*

(ii) *if $p = 3$ then G_p is a homomorphic image of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^i\mathbb{Z}$, where $i \geq 0$;*

(iii) *if $p > 3$ then G_p is a cyclic group.*

(B) *Assume (R_j, M_j) is a principal ideal ring which is not a field. If there exist a prime integer p such that $p \mid \mathrm{Ord}(G)$ and $p \in M_j$, then*

(i) *Case: $p = 2$,*

(a) *when $M_j^2 = 0$ then G_p is a cyclic group or $G_p \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$;*

Downloaded At: 16:36 7 January 2010

(b) *when* $M_j^2 \neq 0$, *then* G_p *is a cyclic group.*
More precisely, if $M_j^3 \neq 0$ *then*
(b') $G_p \simeq \mathbb{Z}/2\mathbb{Z}$ *whether* $2 \in M_j^2$;
(b'') $G_p \simeq \mathbb{Z}/2^i\mathbb{Z}$ where $1 \leq i \leq 2$, whether $2 \in M_j \backslash M_j^2$.

(ii) *Case:* $p = 3$,
(a) G_p *is a cyclic group and*
(b) *when* $M_j^3 \neq 0$, *then*
(b') $G_p \simeq \mathbb{Z}/3\mathbb{Z}$ *whether* $3 \in M_j^2$;
(b'') $G_p \simeq \mathbb{Z}/3^i\mathbb{Z}$ *where* $1 \leq i \leq 2$ *whether* $3 \in M_j \backslash M_j^2$.

(iii) *Case:* $p > 3$,
(a) G_p *is a cyclic group and*
(b) *when* $M_j^3 \neq 0$, *then* $p \notin M_j^3$ *and*
(b') $G_p \simeq \mathbb{Z}/p\mathbb{Z}$ *whether* $p \in M_j^2 \backslash M_j^3$;
(b'') $G_p \simeq \mathbb{Z}/p^i\mathbb{Z}$, *where* $1 \leq i \leq 2$, *whether* $p \in M_j \backslash M_j^2$.

(C) *Assume* (R_j, M_j) *has the* 2*-generator property but is not a principal ideal ring. If there exist a prime integer* p *such that* $p \mid \mathrm{Ord}(G)$ and $p \in M_j$, *then*

(i) *Case:* $p = 2$,
(a) G_p *s a cyclic group and* M_j^2 *is a principal ideal; moreover,*
(b) *when* $M_j^2 \neq 0$, *then* $G_p \simeq \mathbb{Z}/2\mathbb{Z}$.

(ii) *Case:* $p \geq 3$,
(a) G_p *is a cyclic group and* M_j^2 *is a principal ideal; moreover,*
(b) *when* $M_j^2 \neq 0$, *then* $G_p \simeq \mathbb{Z}/p\mathbb{Z}$ *and* $M_j^2 \subset (p) \subset M_j$.

§ 1. The coefficient ring of $R[G]$ is an Artinian principal ideal ring

In the present section, we assume that R is an Artinian principal ideal ring and G is a finite Abelian group. In this situation, we intend to charaterize when the group ring $R[G]$ has the 3-generator property, proving the statements (A) and (B) of the Theorem.

Remark 1.1. (1) Assume that F is a field of characteristic p and that G is a torsion group. If $p = 0$, then $F[G]$ is a principal ideal ring. If $p \neq 0$, then $F[G]$ is a principal ideal ring if and only if the p-Sylow subgroup of the finite abelian group G is cyclic [G2, Theorem 19.14].

(2) Let R be a special principal ideal ring (i. e. a local principal ideal ring with nilpotent maximal ideal). Assume that R is not a field and that G is a finite group of

Downloaded At: 16:36 7 January 2010

order m. Then $R[G]$ is a principal ideal ring if and only if m is a unit of R [G2, Theorem 19.15].

Proposition 1.2. [OV, Example 2.6]. *Let F be a field of characteristic $p \neq 0$ and G a finite abelian group then $F[G]$ has the 3-generator property if and only if*

(i) *when $p = 2$, then G_p is a homomorphic image of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^i\mathbb{Z}$ where $i \geq 0$;*

(ii) *when $p = 3$, then G_p is a homomorphic image of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^i\mathbb{Z}$ where $i \geq 0$;*

(iii) *when $p > 3$, then G_p is a cyclic group.* ■

Proposition 1.3. *Assume that G is a non trivial finite 2-group, (R, M) is a local Artinian principal ideal ring which is not a field and $2 \in M$. Then $R[G]$ has the 3-generator property if and only if*

(a) *when $M^2 = 0$ then G is a cyclic group or $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$;*

(b) *when $M^2 \neq 0$, then G is a cyclic group.*

More precisely, if $M^3 \neq 0$, then

(b') *$G \simeq \mathbb{Z}/2\mathbb{Z}$, whether $2 \in M^2$;*

(b") *$G \simeq \mathbb{Z}/2^i\mathbb{Z}$, where $1 \leq i \leq 2$, whether $2 \in M \setminus M^2$.*

Before giving the proof of Proposition 1.3, we need two preliminary results.

Lemma 1.4. *Let R be a ring, G a cyclic group of finite rank m, g a generator of G and a an element in R. If $a(1 - X^g) \in (1 - X^g)^2 R[G]$ then $a = \lambda m$ for some $\lambda \in R$.*

Proof. Since $a(1 - X^g) \in (1 - X^g)^2 R[G]$ then $a(1 - X^g) = \beta(1 - X^g)^2$ for some $\beta \in R[G]$, i. e. $(1 - X^g)(a - \beta(1 - X^g)) = 0$. Therefore, $a - \beta(1 - X^g) \in \mathrm{Ann}_{R[G]}((1 - X^g))$ which is equal to $(1 + X^g + ... + X^{(m-1)g})R$ because $R[G]$ is a free R-module (generated by $\{1, X^g, ..., X^{(m-1)g}\}$). Then $a - \beta(1 - X^g) = \lambda(1 + X^g + ... + X^{(m-1)g})$ for some $\lambda \in R$. Multiplying both sides of this equation by $(1 + X^g + ... + X^{(m-1)g})$, we obtain that $a(1 + X^g + ... + X^{(m-1)g}) = \lambda(1 + X^g + ... + X^{(m-1)g})^2$. Again by the fact that $R[G]$ is a free R-module it is easy to verify that

$$(1 + X^g + ... + X^{(m-1)g})^2 = m(1 + X^g + ... + X^{(m-1)g}).$$

From the previous relations, we deduce that $a = \lambda m$. ■

Lemma 1.5. *Assume that (R, M) is a local Artinian principal ideal ring and G is a*

Downloaded At: 16:36 7 January 2010

finite cyclic group. Let N be the maximal ideal of the local ring $R[G]$. Then $R[G]$ has the 3-generator property if and only if N, N^2 and N^3 are 3-generated.

Proof. Let $M = rR$ and g a generator of G, then we know that $R[G]$ is local with maximal ideal $N = (r, 1 - X^g)$ [G2, Theorem 19.1 and Corollary 19.2]. Suppose that N, N^2 and N^3 are 3-generated. We need to prove that each ideal I of $R[G]$ is 3-generated. By [Sh1, Corollary 4.2.1], it suffices to consider the case where $I \not\subset N^2$. Let $x \in I \backslash N^2$. By [K, Theorem 159], $\mu(N/(x)) = \mu(N) - 1 = 2 - 1 = 1$. Therefore the ring $R[G]/(x)$ is principal, hence $\mu(I/(x)) = 1$, thus $\mu(I) \leq 2$. We conclude that $R[G]$ has the 3-generator property. ■

Proof of Proposition 1.3.

($\Rightarrow$), **(a)**. By assumption $G \simeq \mathbb{Z}/2^{t_1}\mathbb{Z} \oplus \mathbb{Z}/2^{t_2}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/2^{t_s}\mathbb{Z}$ where $0 < t_1 \leq t_2 \leq \ldots \leq t_s$. If $R[G]$ has the 3-generator property, then the homomorphic image $(R/M)[G]$ does also. By Proposition 1.3 (i) (or by [OV, Corollary 2.2]) $s \leq 3$.

Firstly, we show that the case $s = 3$ is not possible.

Since R is local ring with residue field of characteristic 2 (because $2 \in M$) and $G \simeq \mathbb{Z}/2^{t_1}\mathbb{Z} \oplus \mathbb{Z}/2^{t_2}\mathbb{Z} \oplus \mathbb{Z}/2^{t_3}\mathbb{Z}$ is a finite 2-group, then $R[\mathbb{Z}/2^{t_1}\mathbb{Z} \oplus \mathbb{Z}/2^{t_2}\mathbb{Z} \oplus \mathbb{Z}/2^{t_3}\mathbb{Z}]$ is local with maximal ideal $N := (r, 1 - X^g, 1 - X^h, 1 - X^k)$ where r generates M in R and g (respectively: h, k) is a generator of $\mathbb{Z}/2^{t_1}\mathbb{Z}$ (respectively: $\mathbb{Z}/2^{t_2}\mathbb{Z}$, $\mathbb{Z}/2^{t_3}\mathbb{Z}$) [G2, Theorem 19.1 and Corollary 19.2]. By [N, (5.3) p. 14], the 3 generators of N can be chosen among the elements of the given set of generators of N.

If $N = (r, 1 - X^g, 1 - X^h)$, then by applying the augmentation map $R[\langle k \rangle][\langle g \rangle \oplus \langle h \rangle] \to R[\langle k \rangle]$, we have $1 - X^k \in (r)$ in $R[\langle k \rangle]$. This forces r to be a unit of R: a contradiction.

The argument for $N = (r, 1 - X^g, 1 - X^k)$ and $N = (r, 1 - X^h, 1 - X^k)$ is similar.

If $N = (1 - X^g, 1 - X^h, 1 - X^k)$, then applying the augmentation map $R[\langle g \rangle \oplus \langle h \rangle \oplus \langle k \rangle] \to R$ to $r = a(1 - X^g) + b(1 - X^h) + c(1 - X^k)$ where $a, b, c \in R[\langle g \rangle \oplus \langle h \rangle \oplus \langle k \rangle]$, we obtain $r = 0$ contradicting the hypothesis that R is not a field.

If $s = 2$, then $G \simeq \mathbb{Z}/2^{t_1}\mathbb{Z} \oplus \mathbb{Z}/2^{t_2}\mathbb{Z} = \langle g \rangle \oplus \langle h \rangle$ where $0 < t_1 \leq t_2$. If $R[\langle g \rangle \oplus \langle h \rangle]$ has the 3-generator property, then the homomorphic image $(R/M)[\langle g \rangle \oplus \langle h \rangle]$ does too. By Proposition 1.2 (i) (or by [OV, Proposition 2.1 (a)]) $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^i\mathbb{Z}$, with $i \geq 1$.

Assume $i > 1$, then necessarily $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}]$ has the 3-generator property. Consequently N^2 is 3-generated, where $N := (r, 1 - X^g, 1 - X^h)$, r generates M in R

Downloaded At: 16:36 7 January 2010

and g (respectively, h) is a generator of $\mathbb{Z}/2\mathbb{Z}$ (respectively, $\mathbb{Z}/4\mathbb{Z}$). We note that

$$N^2 = (r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h), (1 - X^g)^2, (1 - X^h)^2)$$

because we are assuming $M^2 = 0$. Moreover, as $\langle g \rangle = \mathbb{Z}/2\mathbb{Z}$ and $2 \in M$, then $(1 - X^g)^2 = 1 - 2X^g + X^{2g} = 2(1 - X^g) \in (r(1 - X^g))$, therefore

$$N^2 = (r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h), (1 - X^h)^2).$$

Suppose that $r(1 - X^g)$ is a redundant generator of the 3-generated ideal N^2. By applying the augmentation map $R[\langle g \rangle][\langle h \rangle] \to R[\langle g \rangle]$ to the equality

$$r(1 - X^g) = ar(1 - X^h) + b(1 - X^g)(1 - X^h) + c(1 - X^h)^2$$

where $a, b, c \in R[\langle g \rangle \oplus \langle h \rangle]$, we obtain that $r(1 - X^g) = 0$ in $R[\langle g \rangle]$, thus $r = 0$ in R: a contradiction. Therefore $r(1 - X^g)$ must appear in a party of 3 generators of N^2. The argument for $r(1 - X^h)$ is similar; so also $r(1 - X^h)$ must appear in a party of 3 generators of N^2.

If $(1 - X^h)^2$ is redundant, then by applying the augmentation map $R[\langle h \rangle][\langle g \rangle] \to R[\langle h \rangle]$ to the equality

$$(1 - X^h)^2 = ar(1 - X^h) + br(1 - X^g) + c(1 - X^g)(1 - X^h)$$

where $a, b, c \in R[\langle g \rangle \oplus \langle h \rangle]$, we obtain $(1 - X^h)^2 = 1 - 2X^h + X^{2h} \in rR[\langle h \rangle]$. This forces r to be a unit in R: a contradiction. Then $(1 - X^h)^2$ must appear in a minimal set of generators of N^2.

The previous argument shows that, if $R[G]$ has the 3-generators property, then $N^2 = (r(1 - X^g), r(1 - X^h), (1 - X^h)^2)$. By passing to the homomorphic image onto $(R/M)[\langle g \rangle \oplus \langle h \rangle]$, we obtain that

$$(1 - X^g)(1 - X^h) \in ((1 - X^h)^2) \text{ in } K[\langle g \rangle \oplus \langle h \rangle],$$

where $K := R/M$ is a field of characteristic 2 (since $2 \in M$). Then, in $K[\langle g \rangle \oplus \langle h \rangle]$ we have $(1 - X^g)(1 - X^h) = \alpha(1 - X^h)^2$, where

$\alpha := a_0X^0 + a_gX^g + a_{g+h}X^{g+h} + a_{g+2h}X^{g+2h} + a_{g+3h}X^{g+3h} + a_hX^h + a_{2h}X^{2h} + a_{3h}X^{3h}$

since a basis for the free K-module $K[\langle g \rangle \oplus \langle h \rangle]$ is given by $\{X^0, X^g, X^{g+h}, X^{g+2h}, X^{g+3h}, X^h, X^{2h}, X^{3h}\}$. Moreover, in $K[\langle g \rangle \oplus \langle h \rangle]$, $(1 - X^h)^2 = 1 - 2X^h + X^{2h} = 1 + X^{2h}$. After setting the corresponding terms equal, from the coefficient of X^0, we obtain $1 = a_0 + a_{2h}$ and, from the coefficient of X^{2h}, we obtain $0 = a_0 + a_{2h}$: a contradiction.

Therefore N^2 is not 3-generated in $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}]$, consequently $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}]$ does not have the 3-generator property.

By the previous argument, we conclude that $s \leq 2$ and if $s = 2$ then $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

($\Leftarrow$), (a). Suppose that $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $M^2 = 0$.

We know that $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$ is a local ring with maximal ideal $N := (r, 1 - X^g, 1 - X^h)$, where r generates M in R and $\langle g \rangle \oplus \langle h \rangle = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ [G2, Theorem 19.1 and Corollary 19.2].

Downloaded At: 16:36 7 January 2010

Step 1. We claim that N, N^2 and N^3 are 3-generated.

We note that

$$N^2 = (r^2, r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h), (1 - X^g)^2, (1 - X^h)^2) =$$
$$= (r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h))$$

since $r^2 = 0$ (because $M^2 = 0$), $(1 - X^g)^2 = 1 - 2X^g + X^{2g} = 2(1 - X^g) \in (r(1 - X^g))$ and $(1 - X^h)^2 = 2(1 - X^h) \in (r(1 - X^h))$ (because $2 \in M$ and 2 is the order of g and h).

By a similar argument, it can be proven that

$$N^3 = (r^3, r^2(1 - X^g), r^2(1 - X^h), r(1 - X^g)(1 - X^h), r(1 - X^g)^2, (1 - X^g)^2(1 - X^h),$$
$$(1 - X^g)(1 - X^h)^2, r(1 - X^h)^2) = (r(1 - X^g)(1 - X^h)).$$

Step 2. Let I be an ideal of $R[G]$, then I is 3-generated.

By [Sh1, Corollary 4. 2.1], it suffices to consider the case where $I \not\subset N^2$.

Let $x \in I \setminus N^2$. Since $x \in N$, then by [K, Theorem 159]

(1.3.1) $\mu(N/(x)) = \mu(N) - 1 = 3 - 1 = 2.$

Now, we claim that

(1.3.2) $\mu((N/(x))^2) \leq 2.$

Since $\mu(N/(x)) = 2$, then

$N = (r, x, 1 - X^g)$ or $N = (r, x, 1 - X^h)$ or $N = (x, 1 - X^g, 1 - X^h)$.

We denote by $\bar{z}$ the class of $z \in R[G]$ modulo (x).

If $N = (r, x, 1 - X^g)$ then $N/(x) = (\bar{r}, \overline{1 - X^g})$ and

$$(N/(x))^2 = (N^2 + (x))/(x) = \left((\bar{r}, \overline{r(1 - X^g)}, \overline{(1 - X^g)^2}\right) = \left(\overline{(r(1 - X^g)}\right)$$

(because $r^2 = 0$ and $(1 - X^g)^2 = 2(1 - X^g) \in (r(1 - X^g))$). Therefore, in this case, obviously $\mu((N/(x))^2) \leq 2$.

The argument for $N = (r, x, 1 - X^h)$ is similar.

If $N = (x, 1 - X^g, 1 - X^h)$ then

$$(N/(x))^2 = (N^2 + (x))/(x) = \left(\overline{r(1 - X^g)}\ \overline{r(1 - X^h)}, \overline{(1 - X^g)(1 - X^h)}\right).$$

Since $r \in N$ then there exist λ, μ, ν in $R[G]$ such that $r = \lambda x + \mu(1 - X^g) + \nu(1 - X^h)$.

If μ is a unit, then

$$(1 - X^g) = \mu^{-1}r - \mu^{-1}\lambda x - \mu^{-1}\nu(1 - X^h)$$

thus, recalling that $r^2 = 0$,

$$r(1 - X^g) = -\mu^{-1}\lambda xr - \mu^{-1}\nu r(1 - X^h)$$

hence $\overline{r(1 - X^g)} \in \left(\overline{r(1 - X^h)}\right)$. Therefore, in this case, $\mu((N/(x))^2) \leq 2$.

If μ is not a unit (i. e. $\mu \in N$), we have

$$r(1 - X^g) = \lambda x(1 - X^g) + \mu(1 - X^g)^2 + \nu(1 - X^g)(1 - X^h).$$

Since $2 \in M = (r)$ then $2 = ar$, where $a \in R$, whence $(1 - X^g)^2 = 2(1 - X^g) =$

Downloaded At: 16:36 7 January 2010

$ar(1 - X^g)$. Therefore:

$$(1 - a\mu)r(1 - X^g) = \lambda x(1 - X^g) + \nu(1 - X^g)(1 - X^h)$$

thus

$$\overline{r(1 - X^g)} \in \left(\overline{(1 - X^g)(1 - X^h)}\right)$$

because $(1 - a\mu)$ is a unit in $R[G]$ (since $R[G]$ is local ring and $\mu \in N$). We conclude that $\mu((N/(x))^2) \leq 2$.

By **(1.3.1)** and **(1.3.2)** and by [Mc, Theorem 1, (6) $\Rightarrow$ (1)] the ring $R[G]/(x)$ has the 2-generator property. Consequently $I/(x)$ is 2-generated, whence I is 3-generated. We conclude that $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$ has the 3-generator property.

In order to complete the proof of $((\Leftarrow)$, (a)) suppose that $M^2 = 0$ and $G \simeq \mathbb{Z}/2^i\mathbb{Z}$, where $1 \leq i$. Then $R[G]$ has the 2-generator property by [OV, Proposition 4.6].

$(\Rightarrow)$, (b). Assume that $R[G]$ has the 3-generator property and that $M^2 \neq 0$. Suppose that G is not cyclic. Then the homomorphic image $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$ of $R[G]$ has the 3-generator property. Consequently N^2 is 3-generated, where N is the maximal ideal of $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$ and $N = (r, 1 - X^g, 1 - X^h)$, with $M = (r)$ and $\langle g \rangle \oplus \langle h \rangle = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

We note that

$$N^2 = (r^2, r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h), (1 - X^g)^2, (1 - X^h)^2) =$$
$$= (r^2, r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h))$$

(because $(1 - X^g)^2 \in (r(1 - X^g))$ and $(1 - X^h)^2 \in (r(1 - X^h))$, since the order of g and h is 2 and $2 \in M = (r)$). As we noticed before, the 3 generators of N^2 can be chosen among the given generators of N^2.

If r^2 is redundant in the set of generators of N^2, then

$r^2 = ar(1 - X^g) + br(1 - X^h) + c(1 - X^g)(1 - X^h)$ where $a, b, c \in R[\langle g \rangle \oplus \langle h \rangle]$.

By applying the augmentation map $R[\langle g \rangle \oplus \langle h \rangle] \rightarrow R$ to the previous equality, we obtain that $r^2 = 0$ contradicting our hypothesis that $M^2 \neq 0$.

If $r(1 - X^g)$ is redundant in the set of generators of N^2, then

$r(1 - X^g) = ar^2 + br(1 - X^h) + c(1 - X^g)(1 - X^h)$,

where $a, b, c \in R[\langle g \rangle \oplus \langle h \rangle]$. By applying the augmentation map $R[\langle g \rangle][\langle h \rangle] \rightarrow R[\langle g \rangle]$ to the previous equality, in $R[\langle g \rangle]$ we obtain that $r(1 - X^g) = r^2(\alpha + \beta X^g)$ where $\alpha, \beta \in R$; thus $r = r^2\alpha$, i. e. $M^2 = M = rR$, whence, by Nakayama's Lemma, $M = 0$: a contradiction.

The argument for $r(1 - X^h)$ is a similar, thus $r(1 - X^h)$ must also appear in a party of 3 generators of N^2.

If $(1 - X^g)(1 - X^h)$ is redundant in the set of generators of N^2, then $(1 - X^g)(1 - X^h) \in (r^2, r(1 - X^g), r(1 - X^h)) \subseteq rR[\langle g \rangle \oplus \langle h \rangle]$. Since $R[\langle g \rangle \oplus \langle h \rangle]$ is a free R-module, this condition yields $1 \in (r)$: a contradiction.

Downloaded At: 16:36 7 January 2010

The previous argument shows that $\{r^2, r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h)\}$ is a minimal set of generators of N^2, whence we reach the contradiction that $R[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$ does not have the 3-generator property.

We conclude that if $M^2 \neq 0$ and if $R[G]$ has the 3-generator property then G must be a cyclic group.

Let g be the generator of G. We know that $R[G]$ is a local ring with maximal ideal $N = (r, 1 - X^g)$ where r generates M [G2, Theorem 19.1 and Corollary.19.2]. Since, by hypoyhesis, $R[G]$ has the 3-generator property then N, N^2 and N^3 are 3-generated. We note that:

$$N^2 = (r^2, r(1 - X^g), (1 - X^g)^2) \text{ and } N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3).$$

It is clear that N, N^2 and N^3 are 3-generated if $M^3 = 0$.

(b'). Suppose $M^3 \neq 0$ and $2 \in M^2$. In order to conclude that $G \simeq \mathbb{Z}/2\mathbb{Z}$, it suffices to prove that $R[\mathbb{Z}/4\mathbb{Z}]$ does not have the 3-generator property, since $R[\mathbb{Z}/2\mathbb{Z}]$ has the 3-generator property (in fact, it has the 2-generator property by [OV, Proposition 4.6]).

We claim that, in $R[\mathbb{Z}/4\mathbb{Z}]$, $N^3 = (r^3, r^2(1 - X^g), r(1- X^g)^2, (1 - X^g)^3)$ may not be generated by 3 elements, where $\mathbb{Z}/4\mathbb{Z} = \langle g \rangle$ and $M = (r)$.

By contradiction, suppose that N^3 is generated by 3 elements. Since $M^3 = (r^3) \neq 0$ and the order of g is strictly bigger than 3, it is clear that r^3 and $(1 - X^g)^3$ must appear in a party of 3 generators extracted from the given set of generators of N^3.

If $r^2(1 - X^g)$ is redundant, then $r^2(1 - X^g) \in (r^3, r(1 - X^g)^2, (1 - X^g)^3)$. By passing to the homomorphic image onto $(R/(r^3))[\langle g \rangle]$, in this ring we have $r^2(1 - X^g) = b(1 - X^g)^2$ where $b \in (R/(r^3))[\langle g \rangle]$. By Lemma 1.4, we have $r^2 = 4\lambda$ for some $\lambda \in R/(r^3)$. Since $2 \in M^2$, we have $r^2 = 0$ in $R/(r^3)$ i. e. $(r^2) = (r^3)$ in R : a contradiction.

If $r(1 - X^g)^2 \in (r^3, r^2(1 - X^g), (1 - X^g)^3)$, by passing to the homomorphic onto $(R/(r^2))[\langle g \rangle]$, in this ring we obtain that $r(1 - X^g)^2 = a(1 - X^g)^3$, where $a \in (R/(r^2))[\langle g \rangle]$. Consequently, in $(R/(r^2))[\langle g \rangle]$ we have

$$\begin{aligned} r(1 - X^g)^3 = a(1 - X^g)^4 &= a(1 - 4X^g + 6X^{2g} - 4X^{3g} + X^{4g}) = \\ &= 2a(1 - 2X^g + 3X^{2g} - 2X^{3g}) \text{ (since the order of } g \text{ is } 4) \\ &= 0 \quad \text{(because } 2 \in M^2 = (r^2)). \end{aligned}$$

Since $(R/(r^2))[\langle g \rangle]$ is a free $R/(r^2)$-module and the order of g is strictly bigger than 3, this equation holds for $r = 0$ in $R/(r^2)$ i. e. $r = r^2$ in R, whence $r = 0$: a contradiction.

The previous argument shows that N^3 is not 3-generated because r^3, $r^2(1 - X^g)$, $r(1 - X^g)^2$ and $(1 - X^g)^3$ must appear in a minimal set of generators of N^3. Thus $R[\mathbb{Z}/4\mathbb{Z}]$ does not have the 3-generator property.

Downloaded At: 16:36 7 January 2010

(b") . Suppose that $R[G]$ has the 3-generator property, $M^3 \neq 0$ and $2 \in M \setminus M^2$. In order to conclude, it suffices to prove that $R[\mathbb{Z}/8\mathbb{Z}]$ does not have the 3-generator property. Let N be the maximal ideal of $R[\mathbb{Z}/8\mathbb{Z}]$, we already know that

$N = (r, 1 - X^g)$, $N^2 = (r^2, r(1 - X^g), (1 - X^g)^2)$ and

$N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3)$.

Suppose that $R[\mathbb{Z}/8\mathbb{Z}]$ has the 3-generator property, then in particular a set of 3 generators can be extracted from the given set of generators of N^3.

Since $M^3 = (r^3) \neq 0$ and the order of g is strictly bigger than 3, it is clear that r^3 and $(1 - X^g)^3$ must appear in each system of 3 generators extracted from the original set of generators of N^3.

If $N^3 = (r^3, r(1 - X^g)^2, (1 - X^g)^3)$, by passing to the homomorphic onto $(R/(r^3))[\mathbb{Z}/8\mathbb{Z}]$, we obtain that $r^2(1 - X^g) = a(1 - X^g)^2$ where $a \in (R/(r^3))[\mathbb{Z}/8\mathbb{Z}]$. By Lemma 1.4 we have $r^2 = 8\lambda$ for some $\lambda \in R/(r^3)$. As $2 \in M = (r)$, then $(r^2) = (r^3)$, therefore $r^2 = 0$: a contradiction.

Let $N^3 = (r^3, r^2(1 - X^g), (1 - X^g)^3)$. Since $(2) = (r)$ because $2 \in M \setminus M^2$, by passing to the homomorphic onto $(R/(r^2))[\mathbb{Z}/8\mathbb{Z}]$, we have $2(1 - X^g)^2 \in ((1 - X^g)^3)$. We know that $(R/(r^2))[\mathbb{Z}/8\mathbb{Z}]$ is $R/(r^2)$-module free, generated by $\{X^{kg} : 0 \leq k \leq 7\}$. Therefore $2(1 - X^g)^2 = (a_0 + a_1X^g + ... + a_7X^{7g})(1 - X^g)^3$, where $a_i \in R/(r^2)$. By setting corresponding terms equal, we obtain the following equations:

X^0	$a_0 - a_5 + 3a_6 - 3a_7$	$= 2$
X^g	$-3a_0 + a_1 - a_6 + 3a_7$	$= 0$
X^{2g}	$3a_0 - 3a_1 + a_2 - a_7$	$= 2$
X^{3g}	$-a_0 + 3a_1 - 3a_2 + a_3$	$= 0$
X^{4g}	$-a_1 + 3a_2 - 3a_3 + a_4$	$= 0$
X^{5g}	$-a_2 + 3a_3 - 3a_4 + a_5$	$= 0$
X^{6g}	$-a_3 + 3a_4 - 3a_5 + a_6$	$= 0$
X^{7g}	$-a_4 + 3a_5 - 3a_6 + a_7$	$= 0$.

After resolving this system, we obtain $2 = 0$ in $R/(r^2)$, i. e. $2 \in M^2$: a contradiction. We conclude that $R[\mathbb{Z}/8\mathbb{Z}]$ does not have the 3-generator property.

($\Leftarrow$), **(b)** . Assume that $M^2 \neq 0$ and thus G is a cyclic group. We want to show that $R[G]$ has the 3-generator property. We recall that $R[G]$ is a local ring [G2, Theorem 19.1 and Corollary 19.2] with ideal maximal $N = (r, 1 - X^g)$, where r generates M and $G = \langle g \rangle$.

Step 1. We claim that N, N^2 and N^3 are 3-generated.

We note that:

$N^2 = (r^2, r(1 - X^g), (1 - X^g)^2)$ and $N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3)$.

If $M^3 = 0$, then it is clear that N, N^2 and N^3 are 3-generated.

Downloaded At: 16:36 7 January 2010

(b'). Assume that $M^3 \neq 0$ and $2 \in M^2$ thus $G \simeq \mathbb{Z}/2\mathbb{Z}$. In this situation, $R[G]$ has the 2-generator property [OV, Theorem 4.1 (b, 2)].

(b"). Assume that $M^3 \neq 0$, $2 \in M \backslash M^2$ and $G \simeq \mathbb{Z}/4\mathbb{Z}$.

For $R[\mathbb{Z}/4\mathbb{Z}]$, we have

$$N = (r, 1 - X^g), \quad N^2 = (r^2, r(1 - X^g), (1 - X^g)^2) \quad \text{and}$$

$$N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3) = (r^3, r(1 - X^g)^2, (1 - X^g)^3)$$

because $r^2(1 - X^g) \in (r(1 - X^g)^2, (1 - X^g)^3)$. As a matter of fact,

$$1 = (1 - X^g + X^g)^4 = 1 + 4(1 - X^g)X^{3g} + 6(1 - X^g)^2X^{2g} + 4(1 - X^g)^3X^g + (1 - X^g)^4$$

i. e. $4(1 - X^g)X^{3g} = -6(1 - X^g)^2X^{2g} - 4(1 - X^g)^3X^g - (1 - X^g)^4$

therefore $4(1 - X^g) \in (2(1 - X^g)^2, (1 - X^g)^3)$. Since (R, M) is local, $M = (r)$ and $2 \in M \backslash M^2$ then $r = 2u$ where u is a unit in R. Consequently, $r^2(1 - X^g) \in (r(1 - X^g)^2, (1 - X^g)^3)$.

Step 2. Each ideal in $R[G]$ is 3-generated.

This statement follows from Step 1 and Lemma 1.5. ■

Proposition 1.6. *Let (R, M) be a local Artinian principal ideal ring not a field, p a prime integer, $p \geq 3$, G is a non trivial finite p-group and $p \in M$. Then $R[G]$ has the 3-generator property if and only if*

(1) *Case $p = 3$,*

(a) *G is a cyclic group; and*

(b) *when $M^3 \neq 0$, then*

(b') *$G \simeq \mathbb{Z}/3\mathbb{Z}$, whether $3 \in M^2$;*

(b") *$G \simeq \mathbb{Z}/3^i\mathbb{Z}$, with $1 \leq i \leq 2$, whether $3 \in M \backslash M^2$.*

(2) *Case $p > 3$,*

(a) *G is a cyclic group; and*

(b) *when $M^3 \neq 0$, then $p \notin M^3$ and*

(b') *$G \simeq \mathbb{Z}/p\mathbb{Z}$, whether $p \in M^2 \backslash M^3$;*

(b") *$G \simeq \mathbb{Z}/p^i\mathbb{Z}$, with $1 \leq i \leq 2$, whether $p \in M \backslash M^2$.*

We establish first a lemma which will be used later several times.

Lemma 1.7. *Let R be a ring, G a cyclic group of finite rank m, g a generator of G and a an element in R. Suppose that m is odd. If $a(1 - X^g)^2 \in ((1 - X^g)^3)$ in $R[G]$, then $a = \lambda m$, for some $\lambda \in R$.*

Proof. Since $a(1 - X^g)^2 \in ((1 - X^g)^3)$ then $a(1 - X^g)^2 = \beta(1 - X^g)^3$, for some $\beta \in R[G]$, i. e. $a(1 - X^g) - \beta(1 - X^g)^2 \in \mathrm{Ann}_{R[G]}(1 - X^g) = (1 + X^g + \ldots + X^{(m-1)g})R$ (cf. also the proof of Lemma 1.4). Therefore

Downloaded At: 16:36 7 January 2010

(1.7.1) $a(1 - X^g) - \beta(1 - X^g)^2 = \lambda'(1 + X^g + ... + X^{(m-1)g})$, for some $\lambda' \in R$. Since β is an element of the free R-module $R[G]$, then $\beta = b_0 + b_1X^g + \cdots + b_{m-1}X^{(m-1)g}$, where $b_i \in$ R for each i . By setting in **(1.7.1)** the corresponding terms equal, we obtain the following equations :

$$
\begin{aligned}
a &= \lambda' + b_0 - 2b_{m-1} + b_{m-2} \\
-a &= \lambda' + b_1 - 2b_0 + b_{m-1} \\
0 &= \lambda' + b_2 - 2b_1 + b_0 \\
0 &= \lambda' + b_3 - 2b_2 + b_1 \\
&\ldots \\
&\ldots \\
0 &= \lambda' + b_{m-1} - 2b_{m-2} + b_{m-3} .
\end{aligned}
$$

After multiplying these equations by $(m - 1)/2, -1 + (m - 1)/2, \ldots , 1, 0, -1, \ldots , -(m - 1)/2$ respectively and adding the resulting equations, we have $a = m(b_{m-2} - b_{m-1})$. Take $\lambda := b_{m-2} - b_{m-1}$. ■

Downloaded At: 16:36 7 January 2010

Proof of Proposition 1.6.

(1) Case: $p = 3$. $(\Rightarrow)$.

(a). By contradiction suppose that G is not cyclic. Since we are supposing that $R[G]$ has the 3-generator property, then also its homomorphic image $R[\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}]$ does. Let $N := (r, 1 - X^g, 1 - X^h)$, where r generates M in R and $\langle g \rangle \oplus \langle h \rangle = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Then N^2 and N^3 are 3-generated in $R[\langle g \rangle \oplus \langle h \rangle]$. We note that:

$$N^2 = (r^2, r(1 - X^g), r(1 - X^h), (1 - X^g)(1 - X^h), (1 - X^g)^2, (1 - X^h)^2) .$$

We know that N^2 can be generated by 3 elements chosen in the previous set of generators of N^2 [N, (5.3) p. 14].

If $(1 - X^g)^2$ is redundant, then in particular $(1 - X^g)^2 = ar^2 + br(1 - X^g) + cr(1 - X^h) + d(1 - X^g)(1 - X^h) + e(1 - X^h)^2$, where $a, b, c, d, e \in R[\langle g \rangle \oplus \langle h \rangle]$. By applying the augmentation map $R[\langle g \rangle][\langle h \rangle] \to R[\langle g \rangle]$, we have $(1 - X^g)^2 = 1 - 2X^g + X^{2g} \in rR[\langle g \rangle]$, since the order of g is strictly bigger than 2 , we reach easily a contradiction.

The argument for $(1 - X^h)^2$ is similar. Consequently $(1 - X^g)^2$ and $(1 - X^h)^2$ must appear in a party of 3 generators extracted from the given set of generators of N^2.

If $(1 - X^g)(1 - X^h) \in (r^2, r(1 - X^g), r(1 - X^h), (1 - X^g)^2, (1 - X^h)^2)$, by passing to the homomorphic image $K[\langle g \rangle \oplus \langle h \rangle]$, where $K := R/(r)$, we obtain that $(1 - X^g)(1 - X^h) = a(1 - X^g)^2 + b(1 - X^h)^2$ where $a, b \in K[\langle g \rangle \oplus \langle h \rangle]$. Therefore $(1 - X^g)^2(1 - X^h) = a(1 - X^g)^3 + b(1 - X^g)(1 - X^h)^2$, hence in $K[\langle g \rangle \oplus \langle h \rangle]$ we have

(1.6.1) $(1 - X^g)^2(1 - X^h) = b(1 - X^g)(1 - X^h)^2,$

because $\langle g \rangle = \mathbb{Z}/3\mathbb{Z}$ and the characteristic of K is 3 . Since $b = b_0 + b_gX^g +$

$b_{g+h}X^{g+h} + b_{g+2h}X^{g+2h} + b_{2g}X^{2g} + b_{2g+h}X^{2g+h} + b_{2g+2h}X^{2g+2h} + b_hX^h + b_{2h}X^{2h}$, then after setting in **(1.6.1)** the corresponding terms equal, we obtain the following system:

$$\begin{aligned}
1 &= b_0 - b_{2g} + 2b_{2g+2h} - b_{2g+h} - 2b_{2h} + b_h\\
-2 &= b_g - b_0 + 2b_{2h} - b_h - 2b_{g+2h} + b_{g+h}\\
2 &= b_{g+h} - b_h + 2b_0 - b_{2h} - 2b_g + b_{g+2h}\\
1 &= b_{2g} - b_g + 2b_{g+2h} - b_{g+h} - 2b_{2g+2h} + b_{2g+h}\\
-1 &= b_{2g+h} - b_{g+h} + 2b_g - b_{g+2h} - 2b_{2g} + b_{2g+2h}\\
-1 &= b_h - b_{2g+h} + 2b_{2g} - b_{2g+2h} - 2b_0 + b_{2h}\\
0 &= b_{g+2h} - b_{2h} + 2b_h - b_0 - 2b_{g+h} + b_g\\
0 &= b_{2g+2h} - b_{g+2h} + 2b_{g+h} - b_g - 2b_{2g+h} + b_{2g}\\
0 &= b_{2h} - b_{2g+2h} + 2b_{2g+h} - b_{2g} - 2b_h + b_0
\end{aligned}$$

It is easy to see that, in the field K of characteristic 3, the previous system has no solutions: a contradiction. Therefore $(1 - X^g)(1 - X^h)$ must appear in a minimal set of 3 generators of N^2.

If $N^2 = ((1 - X^g)(1 - X^h), (1 - X^g)^2, (1 - X^h)^2)$, then particular $r^2 = a(1 - X^g)^2 + b(1 - X^h)^2 + c(1 - X^g)(1 - X^h)$ where $a, b, c \in R[\langle g\rangle \oplus \langle h\rangle]$. By applying the augmentation map $R[\langle g\rangle \oplus \langle h\rangle] \to R$ we have $r^2 = 0$.

The previous argument shows that if $M^2 \neq 0$, then N^2 may not be 3-generated, consequently $R[\langle g\rangle \oplus \langle h\rangle]$ does not have the 3-generator property : a contradiction. Therefore G must be a cyclic group.

If $M^2 = 0$, then we look at N^3, we notice that

$$\begin{aligned}
N^3 = N^2N &= \big((1 - X^g)(1 - X^h), (1 - X^g)^2, (1 - X^h)^2\big)\big(r, 1 - X^g, 1 - X^h\big) =\\
&= \big(r(1 - X^g)(1 - X^h), (1 - X^g)^2(1 - X^h), (1 - X^g)(1 - X^h)^2, r(1 - X^g)^2,\\
&\quad (1 - X^g)^3, r(1 - X^h)^2, (1 - X^h)^3\big) =\\
&= \big(r(1 - X^g)(1 - X^h), (1 - X^g)^2(1 - X^h), (1 - X^g)(1 - X^h)^2, r(1 - X^g)^2,\\
&\quad -3(1 - X^g)X^g, r(1 - X^h)^2, -3(1 - X^h)X^h\big).
\end{aligned}$$

Since $3 \in (r)$ and $(1 - X^g)^2(1 - X^h), (1 - X^g)(1 - X^h)^2 \notin rR[\langle g\rangle \oplus \langle h\rangle]$, then it is easy to show that at least one between $(1 - X^g)^2(1 - X^h)$ and $(1 - X^g)(1 - X^h)^2$ must appear in a party of 3 generators extracted from the original set of generators of N^3. Since g and h have the same role, by passing to the homomorphic image $K[\langle g\rangle \oplus \langle h\rangle]$ where $K = R/(r)$, we obtain again the equation **(1.6.1)**, which is not solvable in K. Therefore, both $(1 - X^g)^2(1 - X^h)$ and $(1 - X^g)(1 - X^h)^2$ must appear in a party of 3 generators of N^3.

Now, suppose that $-3(1 - X^g)X^g \in \big(r(1 - X^g)(1 - X^h), (1 - X^g)^2(1 - X^h), (1 - X^g)(1 - X^h)^2, r(1 - X^g)^2, r(1 - X^h)^2, -3(1 - X^h)X^h\big)$, then by applying the augmentation map $R[\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}] = R[\langle g\rangle][\langle h\rangle] \to R[\langle g\rangle]$, in the last ring we

Downloaded At: 16:36 7 January 2010

have

$$-3(1 - X^g)X^g = (a_0 + a_1X^g + a_2X^{2g})r(1 - X^g)^2, \text{ where } a_0, a_1, a_2 \in R.$$

Thus, after setting the corresponding terms equal, we obtain among other equations the following:

(I) $0 = r(a_0 + a_1 - 2a_2)$

(II) $3 = r(a_0 - 2a_1 + a_2)$

We note that (II) - (I) yields $3 = r(-3a_1 + 3a_2) = 3r(-a_1 + a_2) = 0$, where the last equality holds because $3 \in (r)$ and $r^2 = 0$. Therefore, $\mathrm{ch}(R) = 3$ hence:

$$N^3 = \big(r(1 - X^g)(1 - X^h), (1 - X^g)^2(1 - X^h), (1 - X^g)(1 - X^h)^2, r(1 - X^g)^2, r(1 - X^h)^2\big).$$

Suppose that $r(1 - X^g)^2$ does not appear in a party of 3 generators extracted from the original set of generators of N^3. By applying the augmentation map $R[\langle g\rangle][\langle h\rangle] \to R[\langle g\rangle]$, in $R[\langle g\rangle]$ we have $r(1 - X^g)^2 = 0$. This forces $r = 0$ in R: a contradiction.

The argument for $r(1 - X^h)^2$ is similar. Therefore, we conclude that $(1 - X^g)^2(1 - X^h)$, $(1 - X^g)(1 - X^h)^2$, $r(1 - X^g)^2$ and $r(1 - X^h)^2$ must appear in a minimal set of generators of N^3: a contradiction.

We proved that $-3(1 - X^g)X^g$ must appear in a party of 3 generators extracted from the original set of generators of N^3.

Similarly, we can prove also that $-3(1 - X^h)X^h$ must appear in a party of 3 generators chosen among the given generators of N^3.

Now, we may conclude that N^3 is not 3-generated, because the elements $(1 - X^g)^2(1 - X^h)$, $(1 - X^g)(1 - X^h)^2$, $-3(1 - X^g)X^g$ and $-3(1 - X^h)X^h$ must appear in a minimal set of generators of N^3. Consequently, G is cyclic also when $M^2 = 0$.

(b'). Suppose that $M^3 \neq 0$ and $3 \in M^2$.

The conclusion will follow if we prove that $R[\mathbb{Z}/9\mathbb{Z}]$ does not have the 3-generator property. By contradiction, suppose that the ideal

$$N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3)$$

is 3-generated in $R[\mathbb{Z}/9\mathbb{Z}]$, where r generates M in R and g is a generator of $\mathbb{Z}/9\mathbb{Z}$.

It is clear that r^3 and $(1 - X^g)^3$ must appear in a minimal set of generators extracted from the original set of generators of N^3, since $M^3 \neq 0$ and the order of g is strictly bigger than 3.

If $r^2(1 - X^g) \in (r^3, r(1 - X^g)^2, (1 - X^g)^3)$. By passing to the homomorphic image onto $(R/(r^3))[\mathbb{Z}/9\mathbb{Z}]$, in this ring we obtain that $r^2(1 - X^g) = \beta(1 - X^g)^2$, where $\beta \in (R/(r^3))[\mathbb{Z}/9\mathbb{Z}]$. By Lemma 1.4, in the ring $R/(r^3)$ we have that $r^2 = 9\lambda$, for some $\lambda \in R/(r^3)$. Since, we are assuming $3 \in M^2$, then $M^2 = M^3$, whence (by Nakayama's Lemma) $M^2 = 0$, contradicting the hypothesis $M^3 \neq 0$.

Downloaded At: 16:36 7 January 2010

The previous argument shows that, when $R[\mathbb{Z}/9\mathbb{Z}]$ is 3-generated then $N^3 = (r^3, r^2(1 - X^g), (1 - X^g)^3)$, hence $r(1 - X^g)^2 \in N^3$. Therefore, passing modulo $r^2R[\mathbb{Z}/9\mathbb{Z}]$, in this quotient ring we obtain $r(1 - X^g)^2 = \rho(1 - X^g)^3$ where $\rho \in (R/(r^2))[\mathbb{Z}/9\mathbb{Z}]$. By Lemma 1.7, $r = 9\lambda$ for some $\lambda \in R/(r^2)$ i. e. $r = 0$ in $R/(r^2)$, since $3 \in M^2$. We deduce that $(r) = (r^2)$ in R : a contradiction.

In conclusion, we proved that, if $M^3 \neq 0$ and $3 \in M^2$, $R[\mathbb{Z}/9\mathbb{Z}]$ does not have the 3-generator property.

(b"). Suppose that $M^3 \neq 0$ and $3 \in M \backslash M^2$.

We note that the condition that $3 \in M \backslash M^2$ (i. e. $(3) = (r) = M$) implies the conclusion, if we prove that $R[\mathbb{Z}/27\mathbb{Z}]$ does not have the 3-generator property. By contradiction, suppose that $R[\mathbb{Z}/27\mathbb{Z}]$ has the 3-generator property. In particular, the ideal N^3 is 3-generated, where $N := (3, (1 - X^g))$ is the maximal ideal of $R[\mathbb{Z}/27\mathbb{Z}]$ and g is a generator of $\mathbb{Z}/27\mathbb{Z}$. We note that:

$$N^2 = (9, 3(1 - X^g), (1 - X^g)^2) \quad \text{and} \quad N^3 = (27, 9(1 - X^g), 3(1 - X^g)^2, (1 - X^g)^3).$$

Since $M^3 \neq 0$ and the order of g is strictly bigger than 3, then 27 and $(1 - X^g)^3$ must appear in a minimal set of 3 generators extracted from the given set of generators of N^3.

If $9(1 - X^g)$ is redundant, passing modulo $27R[\mathbb{Z}/27\mathbb{Z}]$, then, in the ring $(R/(27))[\mathbb{Z}/27\mathbb{Z}]$ we obtain $9(1 - X^g) = \beta(1 - X^g)^2$ (where $\beta \in (R/(27))[\mathbb{Z}/27\mathbb{Z}]$). By Lemma 1.4, we have $9 = 27\lambda$ for some $\lambda \in R/(27)$. Therefore, $9 \in (27)$ in R, hence $M^2 = M^3$: a contradiction.

Since we are supposing that $R[\mathbb{Z}/27\mathbb{Z}]$ has the 3-generator property then the previous argument implies that $N^3 = (27, 9(1 - X^g), (1 - X^g)^3)$, i. e. $3(1 - X^g)^2 \in N^3$. Passing to the quotient ring modulo $9R[\mathbb{Z}/27\mathbb{Z}]$, we obtain $3(1 - X^g)^2 = \beta(1 - X^g)^3$, where $\beta \in (R/(9))[\mathbb{Z}/27\mathbb{Z}]$. By Lemma 1.7, we have $3 = 27\lambda$ for some $\lambda \in R/(9)$, whence $M = M^3$: a contradiction.

In conclusion, $R[\mathbb{Z}/27\mathbb{Z}]$ does not have the 3-generator property.

(1) Case $p = 3$. $(\Leftarrow)$.

(a). Assume that G is a cyclic group. We want to show that $R[G]$ has the 3-generator property. Since $R[G]$ is a local ring [G2, Theorem 19.1 and Corollary 19.2] with ideal maximal $N := (r, 1 - X^g)$, where r generates M and $G = \langle g \rangle$, by Lemma 1.6 it suffices to prove that N, N^2 and N^3 are 3-generated. We note that:

$$N^2 = (r^2, r(1 - X^g), (1 - X^g)^2) \quad \text{and} \quad N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3).$$

It is clear that N, N^2 and N^3 are 3-generated when $M^3 = 0$.

Suppose that **(b)** holds, i. e. $M^3 \neq 0$.

(b'). In case $3 \in M^2$, we need to prove that N^3 is 3-generated in $R[\mathbb{Z}/3\mathbb{Z}]$.

Downloaded At: 16:36 7 January 2010

We note that $(1 - X^g)^3 = -3(1 - X^g)X^g \in (r^2(1 - X^g))$, hence $N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2)$.

(b"). In case $3 \in M\backslash M^2$, the conclusion will follow if we prove that N^3 is 3-generated in $R[\mathbb{Z}/p^2\mathbb{Z}]$, with $p = 3$. We note that:

$$\begin{aligned} 1 &= (1 - X^g + X^g)^{p^2} = \textstyle\sum_0^{p^2} C(p^2, i)(1 - X^g)^i X^{(p^2 - i)g} = \\ &= X^{gp^2} + p^2(1 - X^g)X^{(p^2-1)g} + C(p^2, 2)(1 - X^g)^2 X^{(p^2-2)g} + \\ &\quad + (1 - X^g)^3(\textstyle\sum_3^{p^2} C(p^2, i)(1 - X^g)^{(i-3)} X^{(p^2 - i)g} , \end{aligned}$$

where $C(x, y) := \binom{x}{y}$, and x and y are integers with $x > 0$ and $y \geq 0$.

Since $\mathrm{Ord}(g) = p^2$, then

$$\begin{aligned} p^2(1 - X^g) &= - C(p^2, 2)(1 - X^g)^2 X^{(p^2-1)g} + \\ &\quad - (1 - X^g)^3(\textstyle\sum_3^{p^2} C(p^2, i)(1 - X^g)^{(i-3)} X^{(p^2 - i + 1)g} , \end{aligned}$$

hence $p^2(1 - X^g) \in (p(1 - X^g)^2, (1 - X^g)^3)$, because p divides $C(p^2, i)$, for $i \geq 2$. Since $p \in M\backslash M^2$, i. e. $(p) = M = (r)$, we have $r^2(1 - X^g) \in (r(1 - X^g)^2, (1 - X^g)^3)$. Then $N^3 = (r^3, r(1 - X^g)^2, (1 - X^g)^3)$.

(2) Case $p > 3$. $(\Rightarrow)$.

By [OV, Proposition 3.5] we have that G is a cyclic group (i. e. (a)) and, when $M^3 \neq 0$, then $G \simeq \mathbb{Z}/p^i\mathbb{Z}$ with $i \leq 2$ (i. e. part of (b)).

We show that $R[\mathbb{Z}/p^2\mathbb{Z}]$ does not have the 3-generator property when $p \in M^2$.

By contradiction suppose that $p \in M^2$ and that the ideal $N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3)$ is 3-generated in $R[\mathbb{Z}/p^2\mathbb{Z}]$. We know that in this case N^3 can be generated by 3 elements chosen among the elements of the given set generators of N^3. Since $M^3 \neq 0$ and the order of g is strictly bigger than 3, then, it is clear that r^3 and $(1 - X^g)^3$ must appear in a minimal set of generators of N^3.

If $r^2(1 - X^g) \in (r^3, r(1 - X^g)^2, (1 - X^g)^3)$, then, by passing to the homomorphic image onto $(R/(r^3))[\mathbb{Z}/p^2\mathbb{Z}]$, in this ring we have $r^2(1 - X^g) = \beta(1 - X^g)^2$ where $\beta \in (R/(r^3))[\mathbb{Z}/p^2\mathbb{Z}]$. By Lemma 1.4, we have $r^2 = p^2\lambda$ for some $\lambda \in R/(r^3)$. Since $p \in M^2$, we have $r^2 = 0$ in $R/(r^3)$ i. e. $M^2 = M^3$ in R: a contradiction.

Since we are supposing that N^3 is 3-generated, then the previous argument shows that $N^3 = (r^3, r^2(1 - X^g), (1 - X^g)^3)$, i. e. $r(1 - X^g)^2 \in N^3$, by passing to the homomophic image onto $(R/(r^2))[\mathbb{Z}/p^2\mathbb{Z}]$, in this ring we have $r(1 - X^g)^2 = a(1 - X^g)^3$, where $a \in (R/(r^2))[\mathbb{Z}/p^2\mathbb{Z}]$. By Lemma 1.7, we have $r = p^2\lambda$, for some $\lambda \in R/(r^2)$, whence $r = 0$ in $(R/(r^2))$, i. e. $M = M^2$ in R: a contradiction.

The previous argument shows that, if $p \in M^2$, then N^3 is not generated by 3 elements, hence $R[\mathbb{Z}/p^2\mathbb{Z}]$ does not have the 3-generator property.

Downloaded At: 16:36 7 January 2010

In order to complete the proof of part **(b)**, we assume $p \in M^3$. We show that $R[\mathbb{Z}/p\mathbb{Z}]$ does not have the 3-generator property.

With the same argument as before, we can conclude that r^3 and $(1 - X^g)^3$ must appear in a minimal set of 3 generators of $N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3)$.

If $r^2(1 - X^g) \in (r^3, r(1 - X^g)^2, (1 - X^g)^3)$ then, by passing to the homomophic image onto $(R/(r^3))[\mathbb{Z}/p\mathbb{Z}]$, in this ring we have $r^2(1 - X^g) = a(1 - X^g)^2$, with $a \in (R/(r^3))[\mathbb{Z}/p\mathbb{Z}]$. Since $p \in M^3$, by Lemma 1.4 we have $r^2 = 0$ in $R/(r^3)$, i. e. $M^2 = M^3$: a contradiction.

If $r(1 - X^g)^2 \in (r^3, r^2(1 - X^g), (1 - X^g)^3)$, then, by passing to the homomophic image onto $(R/(r^2))[\mathbb{Z}/p\mathbb{Z}]$, in this ring we have $r(1 - X^g)^2 = b(1 - X^g)^3$ with $b \in (R/(r^2))[\mathbb{Z}/p\mathbb{Z}]$. By Lemma 1.7, we have $r = p\lambda$ for some $\lambda \in R/(r^2)$ and since $p \in M^3$, then we reach a contradiction.

In conclusion, when $p \in M^3$, N^3 is not 3-generated, consequently $R[\mathbb{Z}/p\mathbb{Z}]$ does not have the 3-generator property.

(2) Case: $p > 3$. ($\Leftarrow$).

(a). Assume that G is a cyclic group. Since $R[G]$ is a local ring with maximal ideal $N := (r, 1 - X^g)$ where r generates M and $G = \langle g \rangle$ [G2, Theorem 19.1 and Corollary 19.2] then, by Lemma 1.5, it suffices to prove that N, N^2 and N^3 are 3-generated. We note that:

$N^2 = (r^2, r(1 - X^g), (1 - X^g)^2)$ and $N^3 = (r^3, r^2(1 - X^g), r(1 - X^g)^2, (1 - X^g)^3)$.

It is clear that N, N^2 and N^3 are 3-generated when $M^3 = 0$.

(b). Suppose $M^3 \neq 0$.

(b''). With the same argument as for the case $p = 3$, we prove that $R[\mathbb{Z}/p^2\mathbb{Z}]$ has the 3-generator property, when $p \in M \backslash M^2$.

(b'). Suppose that $p \in M^2 \backslash M^3$. In this case, $M^2 = (r^2) = (p)$, i. e. $p = ur^2$ where u is a unit of R. We need to prove that N^3 is 3-generated in $R[\mathbb{Z}/p\mathbb{Z}]$. We note :

$$1 = (1 - X^g + X^g)^p = X^{pg} + p(1 - X^g)X^{(p-1)g} + \sum_2^p C(p, i)(1 - X^g)^i X^{(p-i)g} =$$

$$= 1 + p(1 - X^g)X^{(p-1)g} + \sum_2^p C(p, i)(1 - X^g)^i X^{(p-i)g} .$$

Therefore

$$p(1 - X^g) = - C(p, 2)(1 - X^g)^2 X^{(p-1)g} - (1 - X^g)^3 (\sum_3^p C(p, i)(1 - X^g)^{i-3} X^{(p+1-i)g}) .$$

Since $p \mid C(p, 2)$, then $p(1 - X^g) \in (p(1 - X^g)^2), (1 - X^g)^3)$. Consequently $r^2(1 - X^g) \in (r(1 - X^g)^2, (1 - X^g)^3)$, whence $N^3 = (r^3, r(1 - X^g)^2, (1 - X^g)^3)$. ■

Proof of the Theorem: (A) and (B).

If R is an Artinian principal ideal ring, then $R \simeq R_1 \oplus \ldots \oplus R_s$, where each (R_j, M_j) is a local Artinian principal ideal ring [J, Vol. II, Theorem 7.15]. It is easy to

Downloaded At: 16:36 7 January 2010

see that $R[G]$ has the n-generator property if and only if each $R_j[G]$ has the n-generator property.

(A). If R_j is a field then it suffices to apply Proposition 1.2 (and Remark 1.1 (1)).

(B). Assume that R_j is not a field. It is proved in [G2, Theorem 19.15] that $R_j[G]$ is a principal ideal ring if R_j is a principal ideal ring and the order of G is a unit in R_j. Therefore, we can suppose that there exists a local Artinian principal ideal ring R_j in which the order of G is not a unit. For simplicity, we denote (R_j, M_j) by (R, M).

Since the order of G is not a unit in R, then

$$\text{Ord}(G) = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} \in M \text{ , where } p_i \text{ is a prime integer.}$$

Therefore, there exists $p \in \{p_1, p_2, \dots, p_t\}$ such that $p \in M$, whence p is the characteristic of R/M. Let $G = G_p \oplus H$, where H is a finite group and $p \nmid \text{Ord}(H)$.

($\Rightarrow$). If $R[G]$ has the 3-generator property, then its homomorphic image $R[G_p]$ does also. Now, it suffices to apply Propositions 1.3 and 1.6.

($\Leftarrow$). For the case $G = G_p$, it suffices to apply Propositions 1.3 and 1.6. For the general case, $R[G] = R[H][G_p]$. We notice that $R[H]$ is an Artinian ring [G2, Theorem 20.7]. Since the order of H is a unit in R, then $R[H] = A_1 \oplus \dots \oplus A_q$ where each (A_i, N_i) is a local Artinian principal ideal ring, $1 \leq i \leq q$, [G2, Theorem 19.15]. Furthermore, $MR[H]$ is equal to the nilradical of $R[H]$ by [G2, Corollary 9.18].

We claim that, for $k \geq 2$, $M^k = 0$ implies that $N_i^k = 0$, for each i.

As a matter of fact, for $k = 2$, let $z \in N_i^2$ then, without loss of generality, $z = xy$ where $x, y \in N_i = \text{Nil}(A_i)$ (A_i is an Artinian ring). Henceforth, there exists $n > 0$ such that $x^n = y^n = 0$, thus $(0, \dots, 0, x, 0, \dots, 0), (0, \dots, 0, y, 0, \dots, 0) \in \text{Nil}(R[H])$. We conclude that $(0, \dots, 0, xy, 0, \dots, 0) \in (\text{Nil}(R[H])^2) = (MR[H])^2 = M^2R[H] = 0$, then $z = xy = 0$. A similar argument applies for $k \geq 3$.

Therefore for each i, $A_i[G_p]$ has the 3-generator property by Propositions 1.2, 1.3, and 1.6. Hence $R[G]$ has the 3-generator property. ■

§ 2. The coefficient ring of $R[G]$ has the 2-generator property

Let G be a finite abelian group and R a commutative ring. In this section we assume that the coefficient ring R of the group ring $R[G]$ has the 2-generator property. We will show the statement (C) of the Theorem.

Downloaded At: 16:36 7 January 2010

Proposition 2.1. *Let p be a prime integer and G a non-trivial finite p-group. Assume that (R, M) is an Artinian local ring with the 2-generator property, but R is not a principal ideal ring, and that $p \in M$. Then $R[G]$ has the 3-generator property if and only if*

(i) *Case: $p = 2$,*

(a) *G is a cyclic group and M^2 is a principal ideal; moreover,*

(b) *when $M^2 \neq 0$, then $G \simeq \mathbb{Z}/2\mathbb{Z}$.*

(ii) *Case: $p \geq 3$,*

(a) *G is a cyclic group and M^2 is a principal ideal; moreover,*

(b) *when $M^2 \neq 0$, then $G \simeq \mathbb{Z}/p\mathbb{Z}$ and $M^2 \subset (p) \subset M$.*

Proof.

($\Rightarrow$). Since (R, M) has the 2-generator property but it is not a principal ideal ring, then $M = (u, v)$, with $u, v \in R$, is not a principal ideal [G1, Ex. 8, p. 33].

If $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, then it is easy to see that the maximal ideal N of $R[G]$ is minimally generated by 4 elements; more precisely, $N = (u, v, 1 - X^g, 1 - X^h)$, where $\langle g \rangle \oplus \langle h \rangle = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ (cf. also [G2, proof of Theorem 19.1]). The previous argument shows that G is a cyclic group, for each $p \geq 2$.

Let $G = \mathbb{Z}/p^i\mathbb{Z}$, $i \geq 1$, and let g be a generator of G.

Since $M^2 = (u^2, v^2, uv)$ is 2-generated, if M^2 is not principal, then we can find a minimal set of two generators of M^2, extracted from the given set $\{u^2, v^2, uv\}$. Therefore we can assume either $M^2 = (u^2, v^2)$ or $M^2 = (u^2, uv)$, since u, v have the same role. For simplicity, we write $M^2 = (a, b)$ where $a = u^2$ and $b \in \{v^2, uv\}$.

Since $R[G]$ has the 3-generator property and G is cyclic, by passing to a quotient group, we can assume that $R[\mathbb{Z}/p\mathbb{Z}]$ has the 3-generator property.

Let $N = (u, v, (1 - X^g))$ be the maximal ideal of $R[\mathbb{Z}/p\mathbb{Z}]$, with $\langle g \rangle = \mathbb{Z}/p\mathbb{Z}$, then $N^2 = (a, b, u(1 - X^g), v(1 - X^g), (1 - X^g)^2)$. Since $R[\langle g \rangle]$ has the 3-generator property, then N^2 possedes a minimal set of 3 generators extracted from the given one.

If a does not appear in a minimal set of generators, then

$a = \alpha b + \beta u(1 - X^g) + \gamma v(1 - X^g) + \delta(1 - X^g)^2$ where $\alpha, \beta, \gamma, \delta \in R[\langle g \rangle]$.

By applying the augmentation map, we have $a \in (b)$ in R: a contradiction.

The argument for b is similar. Then a and b must appear in a minimal set of 3 generators of N^2.

(i): Case: $p = 2$.

(a). Assume that $M^2 = (a, b)$ is not principal. We have

$$(1 - X^g)^2 = 2(1 - X^g) \in (u(1 - X^g), v(1 - X^g)),$$

Downloaded At: 16:36 7 January 2010

because $2 \in M = (u, v)$. Then, it is easy to see that $N^2 = (a, b, u(1 - X^g), v(1 - X^g))$.

If $N^2 = (a, b, v(1 - X^g))$ then, passing to the quotient ring modulo $vR[G]$, we obtain $u(1 - X^g) = \lambda u^2$, where $\lambda \in (R/(v))[G]$. Since $(R/(v))[G]$ is a free $R/(v)$-module, then necessarly we have $u \in (u^2)$ in $R/(v)$, hence $u = 0$ in $R/(v)$. This fact implies that $M = (u, v) = (v)$: a contradiction.

If $N^2 = (a, b, u(1 - X^g))$ then, passing to the quotient ring modulo $uR[G]$, we obtain $v(1 - X^g) = 0$ or $v(1 - X^g) \in (v^2)$ in $(R/(u))[G]$, according to $b = uv$ or $b = v^2$. Since $(R/(u))[G]$ is a free $R/(u)$-module, in both cases we have $v = 0$ in $R/(u)$, whence $M = (u, v) = (u)$: a contradiction.

In conclusion, if $p = 2$, then M^2 is principal.

(ii) : Case: $p \geq 3$.

(a). Since the order of g is strictly bigger than 2, it is clear that $(1 - X^g)^2$ must appear in a minimal set of 3 generators extracted from the given set of generators of N^2. Therefore, if $R[G]$ has the 3-generator property then

$$N^2 = (a, b, (1 - X^g)^2).$$

Since $u(1 - X^g) \in N^2$ then, passing to the quotient ring modulo M^2, we obtain that $u(1 - X^g) = c(1 - X^g)^2$, where $c \in (R/M^2)[G]$. By Lemma 1.5, in R/M^2 we have $u = \lambda p$ for some $\lambda \in (R/M^2)$. This forces $p \in M \backslash M^2$ and λ to be invertible in R/M^2. As a matter of fact, if $u = 0$ in R/M^2 then $u \in M^2 = (a, b)$. In this case, it is easy to see that $M = (u, v) = (u^2, v) = (u^3, v) = ... = (v)$, since R is an Artinian ring. Therefore, we contradict the fact that M is not a principal ideal.

The previous argument shows that $(u) = (p)$ in R/M^2

In a similar way, we can prove that $(v) = (p)$ in R/M^2. Therefore $(u) = (v)$ in the quotient ring R/M^2, thus $u = \alpha v + \beta a + \gamma b$ with $\alpha, \beta, \gamma \in R$. This fact implies that $M = (u, v) = (u^2, v) = (u^3, v) = ... = (v)$, since R is an Artinian ring: a contradiction.

The previous argument shows in both cases ((i) and (ii)) that M^2 is a principal ideal.

(b). Now, we want to prove that if $M^2 \neq 0$ then, for every prime p, $R[\mathbb{Z}/p^2\mathbb{Z}]$ does not have the 3-generator property.

Let $M^2 = (\alpha)$, $\mathbb{Z}/p^2\mathbb{Z} = \langle g \rangle$ and let $N = (u, v, (1 - X^g))$ be the maximal ideal of $R[\mathbb{Z}/p^2\mathbb{Z}]$. By contradiction, assume that $R[\mathbb{Z}/p^2\mathbb{Z}]$ has the 3-generator property. In particular, the ideal $N^2 = (\alpha, u(1 - X^g), v(1 - X^g), (1 - X^g)^2)$ possesses a minimal set of 3 generators, extracted from the original set of generators.

Since $M^2 \neq 0$ and the order of g is strictly bigger than 2, it is clear that α and $(1 - X^g)^2$ must appear in a minimal set of 3 generators.

Downloaded At: 16:36 7 January 2010

If $N^2 = (\alpha, u(1 - X^g), (1 - X^g)^2)$ then, passing to the quotient ring modulo $(\alpha, u)R[\langle g \rangle]$, we have $v(1 - X^g) = t(1 - X^g)^2$ where $t \in (R/(\alpha, u))[\langle g \rangle]$. By Lemma 1.5, in $R/(\alpha, u)$ we have $v = p^2\lambda$, for some $\lambda \in (R/(\alpha, u))$. Since $p^2 \in M^2 = (\alpha)$, then $v = 0$ in $R/(\alpha, u)$. Therefore $(u, v) = (u, \alpha)$, and this implies that $(u, v) = (u)$, because R is an Artinian ring: a contradiction.

With a similar argument, we may prove that N^2 contains properly $(\alpha, v(1 - X^g), (1 - X^g)^2)$.

In conclusion, we proved that, if $M^2 \neq 0$, $R[\mathbb{Z}/p^2\mathbb{Z}]$ does not have the 3-generator property, for each p.

In order to conclude the proof of **(b)** in case **(ii)**, we start to prove

Claim 1: $R[\mathbb{Z}/p\mathbb{Z}]$ does not have the 3 generator property, when $M^2 \neq 0$, $p \in M^2$ and $p \geq 3$.

By contradiction, we can assume that, $N^2 = (\alpha, u(1 - X^g), v(1 - X^g), (1 - X^g)^2)$ is 3-generated, having a set of 3 generators extracted from the given one.

If $u(1 - X^g) \in (\alpha, v(1 - X^g), (1 - X^g)^2)$ then, by passing to the homomorphic image onto $(R/(\alpha, v))[\mathbb{Z}/p\mathbb{Z}]$ and by using Lemma 1.5, we have $u \in (v, \alpha)$, since $p \in M^2 = (\alpha)$. Therefore $(u, v) = (v, \alpha) = (v)$: a contradiction.

Since u and v have the same role, we may conclude that $u(1 - X^g)$ and $v(1 - X^g)$ must appear in a minimal set of 3 generators extracted from the original set of generators of N^2.

As $M^2 \neq 0$ and the order of g is strictly bigger than 2, it is clear that also α and $(1 - X^g)^2$ must appear in a minimal set of 3 generators of N^2: a contradiction.

In conclusion, we proved that $R[\mathbb{Z}/p\mathbb{Z}]$ does not have the 3-generator property, when $M^2 \neq 0$ and $p \in M^2$

Claim 2: Assume that $M^2 \neq 0$ and $R[\mathbb{Z}/p\mathbb{Z}]$ has the 3-generator property, then $M^2 \subset (p) \subset M$.

We know (Claim 1) that, in this situation, $p \in M \setminus M^2$ i. e. $p = cu + dv$ where c or d is a unit in R. Therefore $M = (p, u)$ (respectively, $M = (p, v)$) if d (respectively, c) is a unit in R. Since in a local Noetherian ring every set of generators contains a minimal set of generators [N, (5.3), p. 14], then we may assume $M^2 = (\alpha)$, where $\alpha \in \{p^2, pa_0, a_0^2\}$ and $a_0 = u$ (respectively, $a_0 = v$) if d (respectively, c) is a unit in R.

We can assume that $M^2 = (a_0^2)$, otherwise the conclusion is obvious. We note that:

$$N = (u, v, (1 - X^g) \quad \text{and} \quad N^2 = (a_0^2, u(1 - X^g), v(1 - X^g), (1 - X^g)^2).$$

Moreover:

Downloaded At: 16:36 7 January 2010

$$1 = (1 - X^g + X^g)^p = X^{pg} + p(1 - X^g)X^{(p-1)g} +$$
$$+ (1 - X^g)^2(\textstyle\sum_2^p \ C(p, i)(1 - X^g)^{i-2}X^{(p-i)g}) .$$

Since $\mathrm{Ord}(\langle g \rangle) = p$, then

$$(cu + dv)(1 - X^g) = p(1 - X^g) = - (1 - X^g)^2(\textstyle\sum_2^p \ C(p, i)(1 - X^g)^{i-2}X^{(p-i+1)g}) .$$

- If d is a unit in R, we have :

$$v(1 - X^g) = - d^{-1}cu(1 - X^g) - (1 - X^g)^2(\textstyle\sum_2^p \ d^{-1}C(p, i)(1 - X^g)^{i-2}X^{(p-i+1)g}) .$$

•• If c is a unit in R, we have:

$$u(1 - X^g) = - c^{-1}dv(1 - X^g) - (1 - X^g)^2(\textstyle\sum_2^p \ c^{-1}C(p, i)(1 - X^g)^{i-2}X^{(p-i+1)g}) .$$

Therefore, $N^2 = (a_0^2, u(1 - X^g), (1 - X^g)^2)$, if d is a unit in R or $N^2 = (a_0^2, v(1 - X^g), (1 - X^g)^2)$, if c is a unit in R.

- Assume that d is a unit in R. In this situation $a_0 = u$, therefore:

$$N^3 = N^2N = (u^2, u(1 - X^g), (1 - X^g)^2)(u, v, (1 - X^g)) =$$
$$= (u^3, u^2(1 - X^g), u(1 - X^g)^2, (1 - X^g)^3)$$

because we proved above that $v(1 - X^g) \in (u(1 - X^g), (1 - X^g)^2)$, that $v \in (p, u)$ and that $pu \in M^2 = (u^2)$, whence $u^2v \in (pu^2, u^3) = (u^3)$.

If $u(1 - X^g)^2$ is redundant then, by passing to the homomorphic image onto $(R/(u^2))[\mathbb{Z}/p\mathbb{Z}]$ and by applying Lemma 1.8, we have $u = \lambda p$ for some $\lambda \in R/(u^2)$. If $\lambda \in M/M^2$, then we have $u \in M^2$ whence $M = (u, v) = (u^2, v) = (v)$: a contradiction (because M is not a principal ideal). Therefore λ is a unit in R/M^2. Consequently, since $M^2 = (u^2)$, then

$$p = \ell u + wu^2 \text{ for some } w \in R \text{ and } \ell \in R \text{ such that } \ell + M^2 = \lambda^{-1},$$

whence $M = (u, p) = (u)$: a contradiction. The previous argument shows that $u(1 - X^g)^2$ must appear in a minimal set of generators of N^3.

Claim 2, case 1: Assume $M^3 \neq 0$.

It is clear that u^3 must appear in a minimal set of generators of N^3.

Moreover, for $p > 3$, it is easy to see that also $(1 - X^g)^3$ must appear in a minimal set of generators of N^3.

For $p = 3$, we know that $(1 - X^g)^3 = -3X^g(1 - X^g)$. If $(1 - X^g)^3 \in (u^3, u^2(1 - X^g), u(1 - X^g)^2)$, then $3(1 - X^g) \in uR[\mathbb{Z}/3\mathbb{Z}]$. Since $R[\mathbb{Z}/3\mathbb{Z}]$ is a free R-module, we have $3 \in (u)$, whence $M = (u, 3) = (u)$: a contradiction.

The previous argument shows that if d is a unit in R, then $N^3 = (u^3, u(1 - X^g)^2, (1 - X^g)^3)$. Since $u^2(1 - X^g) \in N^3$ then, by passing to the homomorphic image onto $(R/(u^3))[\mathbb{Z}/p\mathbb{Z}]$ and by using the Lemma 1.5, in $R/(u^3)$ we have $u^2 = \lambda p$ for some $\lambda \in R/(u^3)$. Therefore, $u^2 \in (p, u^3)$, hence $(p, u^2) = (p, u^3) = ... = (p)$, because R is an Artinian ring. Whence $u^2 \in (p)$, thus $M^2 \subset (p)$.

Downloaded At: 16:36 7 January 2010

Claim 2, case 2: Assume $M^3 = 0$.

We suppose, by contradiction, that $M^2 = (u^2) \not\subset (p)$. Since $p^2 \in M^2 = (u^2)$, then there exists an element $a \in M$ such that $p^2 = au^2 = 0$ (because $M^2 \not\subset (p)$ and $M^3 = 0$). Moreover, $pu \in M^2 = (u^2)$, thus there exists $b \in M$ such that $pu = bu^2 = 0$ (because $M^2 \not\subset (p)$ and $M^3 = 0$). Therefore $p^2 = pu = 0$.

Let $I := N^2 + (p)$.

Since d is a unit, we proved already that $N^2 = (u^2, u(1 - X^g), (1 - X^g)^2)$, thus

$$I = (p, u^2, u(1 - X^g), (1 - X^g)^2).$$

We claim that $\mu(I) = 4$.

Assume that $\mu(I) \leq 3$. Since the order of g is strictly bigger than 2, it is clear that $(1 - X^g)^2$ must appear in a party of 3 generators (extracted from the original set of generators) of the ideal I.

Suppose that p (respectively, u^2) is redundant then $p \in (u^2, u(1 - X^g), (1 - X^g)^2)$ (respectively, $u^2 \in (p, u(1 - X^g), (1 - X^g)^2)$). By applying the augmentation map $R[G] \to R$ we have $p \in (u^2) = M^2$ (respectively, $M^2 = (u^2) \subset (p)$). This is absurd because $p \in M \setminus M^2$ (respectively, $M^2 \not\subset (p)$). Therefore p and u^2 must appear in a party of 3 generators (extracted from the original set of generators) of the ideal I.

Therefore $u(1 - X^g) \in (p, u^2, (1 - X^g)^2)$. After passing to the quotient ring modulo $(p, u^2)R[G]$, we obtain in $(R/(p, u^2))[G]$ that $u(1 - X^g) = \lambda(1 - X^g)^2)$ where $\lambda \in R/(p, u^2))[G]$. By Lemma 1.5, in $R/(p, u^2)$, we have $u = \mu p$ for some $\mu \in R/(p, u^2)$. Therefore in the ring R, $u \in (p, u^2)$, whence $(p, u) = (p, u^2) = (p, u^3) = ... = (p)$. This is absurd, because $M = (p, u)$ is not principal. We conclude that $M^2 \subset (p)$.

•• We recall that if c is a unit in R, then $a_0 = v$, $M^2 = (v^2)$ and $N = (v^2, v(1 - X^g), (1 - X^g)^2)$. *Mutatis mutandis*, by a similar argument as before we can prove that $M^2 \subset (p)$.

($\Leftarrow$). In the present situation, we know that $R[G]$ is a local ring with maximal ideal $N = (u, v, 1 - X^g)$ where u and v are the generators of M and g is a generator of the cyclic group G [G2, Theorem 19.2].

Step 1: We claim that N, N^2 and N^3 are 3-generated.

If $M^2 = (\alpha)$, then

$$N^2 = (\alpha, u(1 - X^g), v(1 - X^g), (1 - X^g)^2)$$

$$N^3 = (\alpha u, \alpha(1 - X^g), u(1 - X^g)^2, v(1 - X^g)^2, (1 - X^g)^3).$$

It is clear that N, N^2 and N^3 are 3-generated, if $M^2 = 0$.

Assume $M^2 \neq 0$, hence $G \cong \mathbb{Z}/p\mathbb{Z}$.

(i) : Case: $p = 2$.

Downloaded At: 16:36 7 January 2010

We note that $(1 - X^g)^2 = 2(1 - X^g) \in (u(1 - X^g), v(1 - X^g))$, because $2 \in M = (u, v)$. Therefore, $N^2 = (\alpha, u(1 - X^g), v(1 - X^g))$ and $N^3 = (\alpha u, \alpha(1 - X^g))$, thus N, N^2 and N^3 are 3-generated.

(ii) : Case: $p \geq 3$.

Since $p \in M \backslash M^2$ then $p = cu + dv$, where c or d is a unit in R.

• We may assume that d is a unit in R. By an argument used above, we can prove that $v(1 - X^g) \in (u(1 - X^g), (1 - X^g)^2)$, whence $N^2 = (\alpha, u(1 - X^g), (1 - X^g)^2)$ is 3-generated. Moreover, $N^3 = (\alpha u, \alpha(1 - X^g), u(1 - X^g)^2, (1 - X^g)^3)$.

By hypothesis, $M^2 = (\alpha) \subset (p) \subset M$. By a routine argument, we can prove that

$$p(1 - X^g) = -(1 - X^g)^2(\sum_2^p C(p, i)(1 - X^g)^{i-2} X^{(p-i+1)g}).$$

Since $p | C(p, i)$, for $i = 2, \ldots\ldots, p - 1$, then $p(1 - X^g) = p\lambda(1 - X^g)^2 - X^g(1 - X^g)^p$ for some $\lambda \in R[G]$. From the fact that $M^2 \subset (p) \subset M = (u, v)$, we deduce that :

$$\alpha(1 - X^g) \in (p(1 - X^g)^2, (1 - X^g)^3) \subseteq (u(1 - X^g)^2, v(1 - X^g)^2, (1 - X^g)^3).$$

Moreover, since we are assuming that d is a unit of R, we already observed that $v(1 - X^g) \in (u(1 - X^g), (1 - X^g)^2)$. Hence, $\alpha(1 - X^g) \in (u(1 - X^g)^2, (1 - X^g)^3)$, thus $N^3 = (\alpha u, u(1 - X^g)^2, (1 - X^g)^3)$ is 3-generated.

•• If c is a unit in R, then *mutatis mutandis* we can prove that N^2 and N^3 are 3-generated.

Step 2 : Let I be an ideal of $R[G]$, we claim that I is 3-generated.

By [Sh1, Corollary 4. 2.1], it suffices to consider the case where $I \not\subset N^2$.

Let $x \in I \backslash N^2$, then

(2.1.1) $\mu(N/(x)) = \mu(N) - 1 = 2$ [K, Theorem 159].

We claim that:

(2.1.2) $\mu((N/(x))^2) \leq 2$.

Since $N = (u, v, 1 - X^g)$ and $\mu(N/(x)) = 2$, then

$N = (u, v, x)$ or $N = (u, x, 1 - X^g)$ or $N = (v, x, 1 - X^g)$.

◆ Assume $M^2 = 0$.

If $N = (u, v, x)$ then $(N/(x))^2 = (0)$, thus $\mu((N/(x))^2) \leq 2$.

If $N = (u, x, 1 - X^g)$, then in the ring $R[G]/xR[G]$ we have:

$$(N/(x))^2 = \left(\overline{(1 - X^g)^2}, \overline{u(1 - X^g)}\right)$$

thus $\mu((N/(x))^2) \leq 2$.

The argument for $N = (v, x, 1 - X^g)$ is similar.

◆ Assume $M^2 \neq 0$.

(i) : Case: $p = 2$.

If $N = (u, v, x)$, then in the ring $R[G]/xR[G]$ it is trivial that

$$N/(x) = (\bar{u}, \bar{v}) \qquad (N/(x))^2 = (\overline{u^2}, \overline{uv}, \overline{v^2}) = (\bar{\alpha})$$

Downloaded At: 16:36 7 January 2010

therefore $\mu((N/(x))^2) \leq 2$.

If $N = (u, x, 1 - X^g)$, then it is easy to see that

$$(N/(x))^2 = (N^2 + (x))/(x) = \left(\overline{\alpha},\ \overline{u(1-X^g)},\ \overline{v(1-X^g)}\right)$$

Since $v \in N$, then there exist $\lambda, \mu, \gamma \in R[G]$ such that

(2.1.3) $$v = \lambda u + \mu x + \gamma(1 - X^g).$$

If γ is a unit in $R[G]$, then $(1 - X^g) = \gamma^{-1}v - \gamma^{-1}\lambda u - \gamma^{-1}\mu x$, thus

$u(1 - X^g) = \gamma^{-1}uv - \gamma^{-1}\lambda u^2 - \gamma^{-1}\mu ux$ and

$v(1 - X^g) = \gamma^{-1}v^2 - \gamma^{-1}\lambda uv - \gamma^{-1}\mu vx$

whence $(N/(x))^2 = (\overline{\alpha})$ and, obviously, $\mu((N/(x))^2) \leq 2$.

If γ is not a unit in $R[G]$, since by hypothesis $2 \in M = (u, v)$, then $2 = cu + dv$, with c, d in R.

From **(2.1.3)** we have:

$$\begin{aligned} v(1 - X^g) &= \lambda u(1 - X^g) + \mu x(1 - X^g) + \gamma(1 - X^g)^2 = \\ &= \lambda u(1 - X^g) + \mu x(1 - X^g) + 2\gamma(1 - X^g) = \\ &= \lambda u(1 - X^g) + \mu x(1 - X^g) + \gamma(cu + dv)(1 - X^g) \end{aligned}$$

thus

$$(1 - \gamma d)v(1 - X^g) = (\lambda + \gamma c)(u(1 - X^g)) + \mu x(1 - X^g).$$

Since $(1 - \gamma d)$ is a unit in $R[G]$, because $R[G]$ is a local ring and γ is not a unit in $R[G]$, then, in the ring $R[G]/xR[G]$, $\overline{v(1-X^g)} \in \left(\overline{u(1-X^g)}\right)$. Therefore

$$(N/(x))^2 = \left(\overline{\alpha},\ \overline{u(1-X^g)}\right)$$

hence $\mu((N/(x))^2) \leq 2$.

The argument for $N = (v, x, 1 - X^g)$ is similar.

(ii) : Case: $p \geq 3$.

Let $p = cu + dv$.

- We assume that d is a unit in R, since c or d is a unit in R.

In this situation $N = (u, v, 1 - X^g) = (u, p, 1 - X^g)$. Since $\mu(N/(x)) = 2$, then

$N = (u, p, x)$ or $N = (p, x, 1 - X^g)$ or $N = (u, x, 1 - X^g)$.

If $N = (u, p, x)$, then obviously $(N/(x))^2 = (\overline{u}, \overline{p})^2 = \left(\overline{u^2}, \overline{p^2}, \overline{up}\right) = (\overline{\alpha})$, thus $\mu((N/(x))^2) \leq 2$.

If $N = (p, x, 1 - X^g)$ then, in the ring $R[G]/xR[G]$, $N/(x) = \left(\overline{p}, \overline{(1-X^g)}\right)$ and $(N/(x))^2 = \left(\overline{p^2}, \overline{p(1-X^g)}, \overline{(1-X^g)^2}\right) = \left(\overline{p^2}, \overline{(1-X^g)^2}\right)$ because we have already shown that $p(1 - X^g) \in (1 - X^g)^2R[G]$. Therefore, also in this case, $\mu((N/(x))^2) \leq 2$.

If $N = (u, x, 1 - X^g)$, then it is easy to see that $(N/(x))^2 = \left(\overline{\alpha}, \overline{u(1-X^g)}, \overline{(1-X^g)^2}\right)$. Since $p \in N$, then

(2.1.4) $p = \lambda u + \mu x + \gamma(1 - X^g)$ where $\lambda, \mu, \gamma \in R[G]$.

If λ is a unit, then $u(1 - X^g) = \lambda^{-1}p(1 - X^g) - \lambda^{-1}\mu x(1 - X^g) - \lambda^{-1}\gamma(1 - X^g)^2$. Since $p(1 - X^g) \in (1 - X^g)^2R[G]$ then, in the ring $R[G]/xR[G]$, $\overline{u(1-X^g)} \in \left(\overline{(1-X^g)^2}\right)$. Therefore $(N/(x))^2 = \left(\overline{\alpha}, \overline{(1-X^g)^2}\right)$, thus $\mu((N/(x))^2) \leq 2$.

If γ is a unit, then $(1 - X^g) = \gamma^{-1}p - \gamma^{-1}\lambda u - \gamma^{-1}\mu x$ and thus

$$u(1 - X^g) = \gamma^{-1}pu - \gamma^{-1}\lambda u^2 - \gamma^{-1}\mu xu$$

then, in the ring $R[G]/xR[G]$, $\overline{u(1-X^g)} \in \left(\overline{up}, \overline{u^2}\right) \subseteq (\overline{\alpha})$. Therefore, also in this case, $(N/(x))^2 = \left(\overline{\alpha}, \overline{(1-X^g)^2}\right)$, whence $\mu((N/(x))^2) \leq 2$.

If both λ and γ are not units, then $\lambda, \gamma \in N = (u, x, 1 - X^g)$. From **(2.1.4)** we deduce immediately that there exists λ', μ', γ' and δ' in $R[G]$ such that

$$p = \lambda' u^2 + \mu' x + \gamma' u(1 - X^g) + \delta'(1 - X^g)^2.$$

By hypothesis, $M^2 = (\alpha) \subset (p) \subset M$, then there exists $m \in M$ such that $\alpha = mp$. Moreover $u^2 \in M^2 = (\alpha)$, thus there exists $a' \in R$ such that $u^2 = a'\alpha$.

Therefore

$$\alpha = mp = \lambda' m a' \alpha + \mu' m x + \gamma' m u(1 - X^g) + \delta' m(1 - X^g)^2$$

hence

$$(1 - \lambda' m a')\alpha = \mu' m x + \gamma' m u(1 - X^g) + \delta' m(1 - X^g)^2$$

with $\lambda' m a' \in MR[G] \subseteq N$. Since $(1 - \lambda' m a')$ is a unit in $R[G]$ then, in the ring $R[G]/xR[G]$, $\overline{\alpha} \in \left(\overline{u(1-X^g)}, \overline{(1-X^g)^2}\right)$. From this fact, we deduce that $(N/(x))^2 = \left(\overline{u(1-X^g)}, \overline{(1-X^g)^2}\right)$, whence $\mu((N/(x))^2) \leq 2$.

We have proved that $N/(x)$ and $(N/(x))^2$ are 2-generated in $R[G]/(x)$, therefore by [Mc, Theorem 1, (6) $\Rightarrow$ (1)] the ring $R[G]/(x)$ has the 2-generator property. Consequently, the ideal $I/(x)$ is 2-generated, thus I is 3-generated. This concludes the proof that $R[G]$ has the 3-generator property, when d is a unit in R.

•• If c is a unit in R, *mutatis mutandis* we can conclude that each ideal I of $R[G]$ is 3-generated. ■

Proof of Theorem: (C).

We recall that, if R is an Artinian ring, then $R \cong R_1 \oplus \ldots \oplus R_s$, where each (R_j, M_j) is a local Artinian ring. Moreover, it is well known that $R[G]$ has the n-generator property if and only if each $R_j[G]$ has the n-generator property. By using [G2, Theorem 19.15] and [OV, Proposition 4.5], we know also that $R_j[G]$ has the 2-generator property if R_j has the 2-generator property and the order of G is a unit in R_j. Suppose that there exists j, $1 \leq j \leq s$, such that the order of G is not a unit in R_j. We denote simply by (R, M) the local ring (R_j, M_j).

Downloaded At: 16:36 7 January 2010

Assume that (R, M) has the 2-generator property but it is not a principal ideal ring. Since the order of G is not a unit in R, then

$$\text{Ord}(G) = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} \in M \text{ , where } p_i \text{ is a prime integer.}$$

Therefore, there exists $p \in \{p_1, p_2, \ldots, p_t\}$ such that $p \in M$, whence p is the characteristic of R/M. Let $G = G_p \oplus H$, where H is a finite group and $p \nmid \text{Ord}(H)$.

($\Rightarrow$). If $R[G]$ has the 3-generator property, then the homomorphic image $R[G_p]$ does also, whence the conclusion follows from Proposition 2.1.

($\Leftarrow$). For the case $G = G_p$, it suffices to apply Proposition 2.1. For the general case $G = G_p \oplus H$, then $R[G] = R[H][G_p]$. We notice that $R[H]$ is an Artinian ring [G2, Theorem 20.7]. Since the order of H is a unit in R, then $R[H]$ has the 2-generator property [OV, Proposition 4.5] thus $R[H] \simeq A_1 \oplus \ldots \oplus A_q$ where each (A_i, N_i) is a local Artinian ring with the 2-generator property, $1 \leq i \leq q$. Furthermore, $MR[H]$ is equal to the nilradical of $R[H]$ [G2, Corollary 9.18].

We know that, when $k \geq 2$, $M^k = 0$ implies $N_i^k = 0$ for each i (cf. the proof of (A) and (B)). Therefore, for each i, $A_i[G_p]$ has the 3-generator property by Remark 1.1 and Propositions 1.2, 1.3, 1.6 and 2.1. Hence $R[G]$ has the 3-generator property. ■

ACKNOWLEDGEMENTS

The second author (MF) was partially supported by research funds of the *Ministero dell'Università e della Ricerca Scientifica e Tecnologica* and by a grant N. 9300856.CT01 of the *Consiglio Nazionale delle Ricerche*.

This work was done while the third author (SEK) was visiting the *Terza Università di Roma* in the Spring and Autumn of 1994, supported by a grant of the *Consiglio Nazionale delle Ricerche*.

The authors are indebted to the referee for pointing out a gap that affected a previous version of the proofs of Propositions 1.3, 1.6 and 2.1.

REFERENCES

[AG] J. T. Arnold - R. Gilmer. The dimension theory of commutative semigroup rings. Houston J. Math. **2** (1976), 299 - 313.

[AM] J. T. Arnold - R. Matsuda. The n-generator property for semigroup rings. Houston J. Math. **12** (1986), 345 - 356.

Downloaded At: 16:36 7 January 2010

[C] I. S. Cohen. Commutative rings with restricted minimum condition. Duke Math. **17** (1950), 27 - 42.

[G1] R. Gilmer. *Multiplicative ideal theory*. Dekker, New York 1972.

[G2] R. Gilmer. *Commutative semigroup rings*. Chicago Lectures in Mathematics. Univ. Chicago Press 1984.

[J] N. Jacobson. *Basic Algebra*. Freeman 1985, 1989.

[K] I. Kaplansky. Commutative rings. The University of Chicago Press 2nd print (1974)

[M1] R. Matsuda. Torsion free abelian semigroup rings,V. Bull. Fac. Sci. Ibaraki Univ. **11** (1979), 1-37.

[M2] R. Matsuda. *N*-generator property of a polynomial ring. Bull. Fac. Sci. Ibaraki Univ. **16** (1984), 17-23.

[Mc] K. R. McLean. Local ring with bounded ideals. J. Algebra **74** (1982), 328-332.

[N] M. Nagata. *Local ring*. Interscience, New York 1962.

[ORV] J. Okon - D. Rush - P. Vicknair. Semigroup rings with two generated ideals. J. London Math. Soc. **45** (1992), 417-432.

[OV] J. Okon - P. Vicknair. Group rings with *n*-generated ideals. Comm. Algebra **20** (1992), 189-217.

[S] J. D. Sally. *Number of generators of ideals in local rings*. Lectures Notes in Pure and Applied Mathematics **35**, Marcel Dekker New York, 1978.

[Sh1] A. Shalev. On the number of generators of ideals in local rings. Adv. Math. **59** (1986), 82-94.

[Sh2] A. Shalev. Dimension subgroup, nilpotency indices and the number of generators of ideals in p-group algebras. J. Algebra **129** (1990), 412-438.

Received: December 1994

Revised: October 1995 and December 1995

Downloaded At: 16:36 7 January 2010