Can. J. Math., Vol. XXVIII, No. 5, 1976, pp. 954–960

INTEGRAL GROUP RINGS WITH NILPOTENT UNIT GROUPS

CÉSAR POLCINO MILIES

Introduction. Let R be a ring with unit element and G a finite group. We denote by RG the group ring of the group G over R and by $U(RG)$ the group of units of this group ring.

The study of the nilpotency of $U(RG)$ has been the subject of several papers. First, J. M. Bateman and D. B. Coleman showed in [**1**] that if G is a finite group and K a field, then $U(KG)$ is nilpotent if and only if either char $K = 0$ and G is abelian or char $K = p \neq 0$ and G is the direct product of a p-group and an abelian group.

Later K. Motose and H. Tominaga [**6**] corrected a small gap in the proof of the theorem above and obtained a similar result for group rings of finite groups over artinian semisimple rings (which must be commutative for $U(RG)$ to be nilpotent).

For group rings over commutative rings of non-zero characteristic it is possible to obtain a natural generalization of the theorem in [**1**]. (See I. I. Khripta [**5**] or C. Polcino [**7**]).

In this paper we study the nilpotency of $U(\mathbf{Z}G)$ where $\mathbf{Z}$ is the ring of rational integers. In Section 2 we consider also group rings over rings of p-adic integers. A brief account of the results in that section was given in [**7**].

1. Units of integral group rings.

Proposition 1. *Let G be a non abelian finite group. If $U(\mathbf{Z}G)$ is nilpotent then G is a Hamiltonian group.*

Proof. Suppose that G is not Hamiltonian. Then, there exist elements a, $b \in G$ such that $a^{-1}ba$ is not a power of b. Let n be the order of b and $u = (1 - b)a(1 + b + \ldots + b^{n-1})$.

Now, $u \neq 0$ and $u^2 = 0$ so $\alpha_0 = 1 + u$ is a unit in $\mathbf{Z}G$ whose inverse is $\alpha_0^{-1} = 1 - u$. Inductively, we define:

(1) $\alpha_k = [\alpha_{k-1}, b] = \alpha_{k-1}b\alpha_{k-1}^{-1}b^{-1}.$

It follows, by an induction argument, that:

(2) $\alpha_{k-1} = 1 + (1 - b)^{k-1}u.$

Set $\Gamma = a(1 + b + \ldots + b^{n-1})$. We then have:

(3) $(1 - b)^{k-1}u = (1 - b)^k\Gamma = \Gamma - \binom{k}{1}b\Gamma + \ldots + (-1)^k b^k\Gamma.$

Received July 8, 1975 and in revised form, May 4, 1976.

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press

For an arbitrary element $\alpha = \sum_{g \in G} a_g \cdot g \in \mathbf{Z}G$ let the support of α be the set:

$$\operatorname{supp}(\alpha) = \{g \in G | a_g \neq 0\}.$$

Now, if $r = \min\{x \in \mathbf{Z} | x > 0, b^x \Gamma = \Gamma\}$ it is easy to see that $\operatorname{supp}(b^h) \cap \operatorname{supp}(b^k \Gamma) \neq \phi$ if and only if $h \equiv k \pmod r$ and in this case $b^h \Gamma = b^k \Gamma$. So (3) may be written in the form:

$$(4) \qquad (1 - b)^{k-1}. u = x_0 \Gamma + x_1 b \Gamma + \ldots + x_{r-1} b^{r-1} \Gamma,$$

with $x_s = \sum_{i \geqq 0} (-1)^{s+ir} \binom{k}{s + ir}$, where the sum runs over all integers $i \geqq 0$ such that $s + ir \leqq k$.

Now, since all summands in the right-hand member of (4) have disjoint support, if we prove that all coefficients x_s, $0 \leqq s \leqq r - 1$, cannot vanish simultaneously, it will follow that $(1 - b)^{k-1} \neq 0$.

To see this, let ξ be a primitive root of unity of order r. Then

$$(1 - \xi)^n = x_0 + x_1 \xi + \ldots + x_{r-1} \xi^{r-1}.$$

If they could vanish simultaneously we would have $\xi = 1$.

Finally, (2) shows that we have found a sequence of commutators that are never 1 so $U(\mathbf{Z}G)$ is not nilpotent. This completes the proof.

Every Hamiltonian group G can be written as a direct product $G = T_1 \times T_2 \times Q$ where T_1 is an abelian group such that every element in T_1 is of odd order, T_2 is an abelian group of exponent 2 and Q a quaternion group of order 8. In what follows a and b will denote two elements of G that are generators of Q, verifying the relations:

$$a^4 = 1; a^2 = b^2; b^{-1} a b = a^{-1}.$$

LEMMA 1. *Let $G = T \times Q$ where T is an abelian group and Q a quaternion group of order* 8. *If T contains an element of order* 3 *then $U(\mathbf{Z}G)$ is not nilpotent.*

Proof. Suppose T contains an element g of order 3. Then

$$(5) \qquad u = 1 + (225(2 - g - g^2) + 390(bg^2 - bg))(1 - b^2)$$

is a unit in $\mathbf{Z}G$ whose inverse is

$$u^{-1} = 1 + (225(2 - g - g^2) - 390(bg^2 - bg))(1 - b^2)$$

(See A. A. Bovdi [**3**, Lemma 10]).

Since g commutes with a and $aba^{-1} = b^3$, $ab^2a^{-1} = b^2$, it follows that $au^{-1}a^{-1} = u$. Thus, setting $\alpha_1 = [u, a]$, $\alpha_k = [\alpha_{k-1}, a]$ it is easily seen by induction that $\alpha_k = u^{2^k}$.

Finally if u were a unit of finite order, writing $u = \sum_{g \in G} u_g g$ we would have $u_1 = 0$ (see S. D. Berman [**2**, Lemma 2]) or S. Takahashi [**9**]) but formula (5) shows that this is not the case.

Thus we have found a sequence of commutators that is never equal to 1; hence $U(\mathbf{Z}G)$ is not nilpotent.

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press

LEMMA 2. *Let $G = T \times Q$ where T is an abelian group and Q a quaternion group of order 8. If T contains an element of prime order $p > 3$, then $U(\mathbf{Z}G)$ is not nilpotent.*

Proof. Suppose that T contains an element g of prime order $p > 3$. Let $H = (g) \times (a)$. The decomposition of $\mathbf{Q}H$ as direct sum of bilateral ideals is

$$\mathbf{Q}H = I_1 \oplus \ldots \oplus I_6,$$

where the idempotent elements e_i such that $I_i = \mathbf{Q}H \cdot e_i$, $1 \leqq i \leqq 6$, are:

$$\text{(6)} \quad \begin{aligned} e_1 &= \frac{1}{4p}(1 + a + a^2 + a^3)(1 + g + \ldots + g^{p-1}), \\ e_2 &= \frac{1}{4p}(1 - a + a^2 - a^3)(1 + g + \ldots + g^{p-1}), \\ e_3 &= \frac{1}{2p}(1 - a^2)(1 + g + \ldots + g^{p-1}), \\ e_4 &= \frac{1}{4p}(1 + a + a^2 + a^3)(p - 1 - g - \ldots - g^{p-1}), \\ e_5 &= \frac{1}{4p}(1 - a + a^2 - a^3)(p - 1 - g - \ldots - g^{p-1}), \\ e_6 &= \frac{1}{2p}(1 - a^2)(p - 1 - g - \ldots - g^{p-1}). \end{aligned}$$

Berman has also shown that $\xi = gae_6 \in I_6$ is a primitive root of unity of order $4p$ and that identifying $\mathbf{Q} = \mathbf{Q}e_6 \subset I_6$ we have $I_6 = \mathbf{Q}(\xi)$. He also observed that if s stands for the number of residue classes modulo $4p$ in $\mathbf{Q}(\xi)$ that are relatively prime with $4p$, then:

$$\text{(7)} \quad u = e_1 + \ldots + e_5 + (1 + ga + g^2a^2)^s e_6 = e_1 + \ldots + e_5 + (1 + \xi + \xi^2)^s e_6$$

is a unit in $\mathbf{Z}H$.

Since $[\mathbf{Q}(\xi) : \mathbf{Q}] = 2(p - 1)$, u can be written in the form:

$$\text{(8)} \quad u = e_1 + \ldots + e_5 + f(\xi)e_6,$$

where $f \in \mathbf{Z}[X]$ with degree$(f) < 2(p - 1)$ and f contains non zero terms of both odd and even order (see again Berman [**2**, Lemma 9]).

We shall now show that:

$$u^{-1}b^{-1}ub = e_1 + \ldots + e_5 + f_1(\xi)e_6,$$

where $f_1 \in \mathbf{Z}[X]$ satisfies the same conditions as f above.

In fact, it is easy to see that $b^{-1}e_ib = e_i$, $1 \leqq i \leqq 6$, thus:

$$\text{(9)} \quad b^{-1}ub = e_1 + \ldots + e_5 + b^{-1}f(\xi)be_6.$$

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press

Let $h \in \mathbf{Z}[X]$ be the polynomial formed by the odd terms of f. Since $b^{-1}a^ib = a^i$ if i is even, $b^{-1}a^ib = a^{i+2}$ if i is odd and $(1 - a^2)e_6 = 2e_6$, it follows that:

(10) $b^{-1}ub = e_1 + \ldots + e_5 + (f(\xi) - 2h(\xi))e_6.$

Now, $u^{-1} \in \mathbf{Z}H$ so it is integral over $\mathbf{Z}$ and there exists $f^* \in \mathbf{Z}[X]$ such that degree$(f^*) < 2(p - 1)$, $f(\xi) \cdot f^*(\xi) = 1$ and

(11) $u^{-1} = e_1 + \ldots + e_5 + f^*(\xi)e_6.$

From (10) and (11) we get:

(12) $u^{-1}bub = e_1 + \ldots + e_5 + (1 - 2f^*(\xi)h(\xi))e_6$

Let $f_1(\xi) = 1 - 2f^*(\xi)h(\xi)$ (after reducing to a polynomial of degree less than $2(p - 1)$). We must still show that f_1 has non-zero terms of both even and odd degree.

First, suppose that f_1 contains no terms of odd order. Then, we would have $f_1(\xi) = f_1(-\xi)$, i.e.:

(13) $1 - 2f^*(\xi)h(\xi) = 1 + 2f^*(-\xi)h(\xi)$

where degree$(h) < 2(p - 1)$; hence $h(\xi) \neq 0$ and (13) gives:

(14) $-f^*(\xi) = f^*(-\xi)$

Since ξ is a primitive root of unity of order $4p$, there exists a $\mathbf{Q}$-automorphism ϕ of $\mathbf{Q}(\xi)$ that takes ξ to $-\xi$ so $f^*(-\xi) = f(-\xi)^{-1}$ and (14) gives $f(\xi) = -f(-\xi)$, a contradiction.

Now suppose $f_1(\xi)$ contains no terms of even order. We would then have $f_1(\xi) = -f_1(-\xi)$, i.e.:

$$1 - 2f^*(\xi)h(\xi) = -1 - 2f^*(-\xi)h(\xi),$$

so

(15) $1 = (f^*(\xi) - f^*(-\xi))h(\xi)$

If $k \in \mathbf{Z}[X]$ denotes the polynomial formed by the even terms of f^*, (15) can be written in the form

$$1 = 2k(\xi)h(\xi)$$

and $1/2$ would be an algebraic integer.

Finally, if we define $u_0 = u$, $u_k = [u_{k-1}{}^{-1}, b^{-1}]$ a repetition of the argument above shows that this is a sequence of commutators that are never equal to 1 so $U(\mathbf{Z}G)$ is not nilpotent.

THEOREM 1. *Let G be a finite group. Then $U(\mathbf{Z}G)$ is nilpotent if and only if G is commutative or a Hamiltonian 2-group.*

Proof. If $U(\mathbf{Z}G)$ is nilpotent, from Proposition 1, G is either commutative or a Hamiltonian group of the form $G = T_1 \times T_2 \times Q$. Lemmas 1 and 2 show that T_1 must be trivial, hence G is a 2-group.

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press

Now, if G is commutative so is $U(\mathbf{Z}G)$, and G. Higman ([**4**, Theorem 11]) has shown that, for non-abelian groups, $U(\mathbf{Z}G) = \{\pm 1\} \times G$ if and only if G is a Hamiltonian 2-group. Thus, the converse follows trivially.

THEOREM 2. *Let G be a non-abelian finite group. Then the following are equivalent:*

(i) *$U(\mathbf{Z}G)$ is nilpotent.*
(ii) *$U(\mathbf{Z}G)$ is periodic.*
(iii) *$U(\mathbf{Z}G) = \{\pm 1\} \times G$.*
(iv) *G is a Hamiltonian 2-group.*

Proof. After the previous results it remains only to prove that if $U(\mathbf{Z}G)$ is periodic, then G is a Hamiltonian 2-group.

We first observe that if $U(\mathbf{Z}G)$ is periodic and $\alpha, \beta \in \mathbf{Z}G$ are elements such that $\alpha\beta = 0$ then $\beta\alpha = 0$. In fact, if $\beta\alpha \neq 0$, since $(\beta\alpha)^2 = 0$ it follows that $u = 1 + \beta\alpha$ is a unit in $\mathbf{Z}G$ and it is easy to see that $u^n = 1 + n\beta\alpha$. Thus u would be a unit of infinite order. Now, the proof of Theorem 10 in Higman [**4**] can be carried out in this case to show that G must be Hamiltonian.

Finally, write $G = T_1 \times T_2 \times Q$ as above. If T_1 were not trivial, it would contain an element g of order $p \geqq 3$ and taking $H = (g) \times (a)$, it follows from [**4**, Theorems 3 and 6] that $\mathbf{Z}H$ would contain a unit of infinite order.

2. Units of group rings over p-adic integers. In this section we shall denote by J_{p^n} the ring of integers modulo p^n. If $p > 0$ is a prime number and G is a finite p-group, it follows from I. I. Khripta [**5**] or C. Polcino [**7**] that $U(J_{p^n}G)$ is nilpotent.

LEMMA 3. *Let $p > 0$ be a prime number and G a finite p-group. The epimorphism $\phi_{mn}^* : J_{p^n}G \rightarrow J_{p^m}G$ induced by the natural morphism $\phi_{mn} : J_{p^n} \rightarrow J_{p^m}$ yields by restriction an epimorphism of the groups of units.*

Proof. Let α be a unit in $J_{p^m}G$ with inverse α^{-1} and let α^* be any inverse image of α. We will show that α^* is a unit in $J_{p^n}G$.

In fact, if α' is any inverse image of α^{-1} we have:

$$\alpha^*\alpha' = 1 + u$$

$$\alpha'\alpha^* = 1 + v$$

where both u and v belong to $\operatorname{Ker}(\phi_{mn}^*) = p^m J_{p^n}G$; thus u and v are both nilpotent, so $1 + u$, $1 + v$ are invertible elements. Let β and γ be their respective inverses Then:

$$(\gamma\alpha')\alpha^* = \alpha^*(\alpha'\beta) = 1,$$

so $\gamma\alpha' = \alpha'\beta = \alpha^{*-1}$ and α^* is a unit in $J_{p^n}G$.

LEMMA 4. *Let G be a non-abelian, finite, p-group and $n = 2m > 0$ an integer. Then the class of nilpotency of $U(J_{p^n}G)$ is greater than $m/2$.*

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press

Proof. It is easy to see that there exist $a, b \in G$ such that $ab^p = b^pa$ and $ab^i \neq b^ia$ for all integers i, $1 \leqq i \leqq p - 1$.

We define:

$$(16) \quad (a - b)^{(1)} = ab - ba$$
$$(a - b)^{(k)} = (a - b)^{(k-1)}b - b(a - b)^{(k-1)}$$

An induction argument shows that:

$$(17) \quad (a - b)^{(k)} = ab^k - \binom{k}{1}bab^{k-1} + \binom{k}{2}b^2ab^{k-2} + \ldots + (-1)^kb^ka$$

Since $b^rab^{k-r} = b^sab^{k-s}$ if and only if $r \equiv s \pmod{p}$ we can write:

$$(18) \quad (a - b)^{(k)} = x_0ab^k + x_1bab^{k-1} + \ldots + x_{p-1}b^{p-1}ab^{k-p+1}$$

with $x_s = \sum_{i\geqq 0}(-1)^{s+ip}\binom{k}{s + ip}$, where the sum runs over all integers $i \geqq 0$ such that $s + ip \leqq k$. Again, not all x_s, $0 \leqq s \leqq p - 1$, vanish simultaneously so, if p^e is the greatest power of p that divides every coefficient in the right-hand member of (18), we have:

$$(19) \quad (a - b)^{(k)} = p^e\gamma \quad \text{where } \gamma \notin p \cdot J_{p^n}G,$$

with $e < k$ since $|x_s| < \sum_{i=0}^{k}\binom{k}{i} = 2^k \leqq p^k$.

Set:

$$(20) \quad \alpha = 1 - p^ma,\ \beta = 1 - pb,$$
$$\alpha_1 = [\alpha^{-1}, \beta^{-1}],\ \alpha_k = [\alpha_{k-1}{}^{-1}, \beta^{-1}]$$

Again, an induction argument shows that:

$$(21) \quad \alpha_k = 1 + (-1)^{k+1}p^{m+k}(1 + \textstyle\sum_{h=1}^{2m-1} x_hp^hb^h)(a - b)^{(k)}$$

where $x_h \in J_{p^n}$, $1 \leqq h \leqq 2m - 1$. It follows from Lemma 3 that

$$1 + \textstyle\sum_{h=1}^{2m-1} x_hp^hb^h \in U(J_{p^n}G),$$

thus $\alpha_k = 1$ if and only if $p^{m+k}(a - b)^{(k)} = 0$.

From (19) we have $p^{m+k}(a - b)^{(k)} = p^{m+k+e} \cdot \gamma$, where $\gamma \notin pJ_{p^n}G$; thus $\alpha_k = 1$ if and only if $m + k + e \geqq 2m$. Hence, if $k \leqq m/2$ then $\alpha_k \neq 1$ and the class of nilpotency of $U(\mathbf{Z}G)$ is greater than $m/2$.

THEOREM 3. *Let $\mathbf{Z}_p$ be the ring of p-adic integers and G a finite group. Then $U(\mathbf{Z}_pG)$ is nilpotent if and only if G is abelian.*

Proof. Since $\mathbf{Z}_p = \varprojlim \{J_{p^n}\}$, it follows as in Raggi [**8**] that $\mathbf{Z}_pG = \varprojlim \{J_{p^n}G\}$ and $U(\mathbf{Z}_pG) = \varprojlim \{U(J_{p^n}G)\}$.

Suppose that $U(\mathbf{Z}_pG)$ is nilpotent. Then G is also nilpotent and it will suffice to show that every Sylow subgroup of G is abelian. Since we have shown in

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press

Lemma 3 that the morphisms $\phi_{mn} : U(J_{p^n}G) \to U(J_{p^m}G)$ are onto, the morphisms:

$$\phi_n : U(\mathbf{Z}_pG) \to U(J_{p^n}G)$$

are also onto.

The nilpotency of $U(J_pG)$ implies that all q-Sylow subgroups of G, with $q \neq p$, must be abelian (see J. M. Bateman and D. B. Coleman [**1**]). Also, the class of nilpotency of all the groups $U(J_{p^n}G)$ is bounded above by the class of nilpotency of $U(\mathbf{Z}_pG)$; hence, after Lemma 4, also the p-Sylow subgroup of G must be abelian. The converse is trivial.

References

1. J. M. Bateman and D. B. Coleman, *Group algebras with nilpotent unit groups*, Proc. Amer. Math. Soc. *19* (1968), 448–449.

2. S. D. Berman, *On the equation $x^m = 1$ in an integral group ring*, Ukrain. Mat. Ž *7* (1955), 253–261.

3. A. A. Bovdi, *The periodic normal divisors of the multiplicative group of a group ring II*, Sibirsk. Mat. Ž *11* (1970), 492–511.

4. G. Higman, *The units of group rings*, Proc. London Math. Soc. *46* (1940), 231–248.

5. I. I. Khripta, *The nilpotency of the multiplicative group of a group ring*, Mat. Zametki *11* (1972), 191–200.

6. K. Motose and H. Tominaga, *Group rings with nilpotent unit groups*, Math. J. Okayama Univ. *14* (1969), 43–46.

7. C. Polcino Milies, *The nilpotency of the group of units of a group ring*, Atas da 3ª. Escola de Álgebra, 1974, to appear.

8. F. F. Raggi Cardenas, *Las unidades en anillos de grupo con coeficientes en K_{p^n}, Z_{p^n} y $\hat{Z}_p$*, Anales Inst. Mat. Univ. Nac. Aut. México *10* (1970), 29–65.

9. S. Takahashi, *Some properties of the group ring over rational integers of a finite group*, Notices Amer. Math. Soc. *12* (1965), 463.

Instituto de Matemática e Estatística,
Universidade de São Paulo,
São Paulo, Brasil

https://doi.org/10.4153/CJM-1976-092-4 Published online by Cambridge University Press