Filomat 26:4 (2012), 719–723
DOI 10.2298/FIL1204719D

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

The number of idempotents in abelian group rings

Peter V. Danchev[a]

[a] *Department of Mathematics, Plovdiv University, Plovdiv 4000, Bulgaria*

Abstract. Suppose that R is a commutative unitary ring of arbitrary characteristic and G is a multiplicative abelian group. Our main theorem completely determines the cardinality of the set $id(RG)$, consisting of all idempotent elements in the group ring RG. It is explicitly calculated only in terms associated with R, G and their divisions. This result strengthens previous estimates obtained in the literature recently.

1. Introduction

Throughout the present short paper, let R be an arbitrary commutative unitary ring and let G be an arbitrary abelian group written multiplicatively as it is customary when investigating group rings. Standardly, RG will always denote the group ring of G over R and $G_0 = \coprod_p G_p$ the maximal torsion part of G with p-primary component G_p. If $M \subset \mathbb{P}$, the set of all primes, without any confusion we shall write $G_p = 1$ whenever we have $\coprod_{p\in M} G_p$ and $M = \emptyset$. For any natural number n, ζ_n denotes the primitive nth root of unity. Likewise, $R[\zeta_n]$ denotes the free R-module, algebraically generated as a ring by ζ_n, with dimension equal to $[R[\zeta_n] : R]$. In other words, $R[\zeta_n]$ is defined in terms of an overring of R. All other unexplained explicitly notions and notations follow those from [4].

Traditionally, we define $id(R)$ and $id(RG)$ to be the sets of all idempotents in R and RG, respectively. Since 0 and 1 are trivial examples of such elements, the inequalities $|id(RG)| \geq |id(R)| \geq 2$ are fulfilled bearing in mind that $id(R) \subseteq id(RG)$. A question, which naturally arises in some aspects of the commutative group algebras theory (see, e.g., [1] and [2]), is to calculate in an explicit form the cardinality $|id(RG)|$ (i.e, the number of all idempotents being finite or infinite) in a commutative group ring RG.

It was proved in [7] that $|id(RG)| = 2$ if and only if $|id(R)| = 2$ and $supp(G) \cap inv(R) = \emptyset$, denoting $supp(G) = \{p : G_p \neq 1\}$ and $inv(R) = \{p : p.1 \in R^*\}$ as well as reserving R^* for the unit group of R (that is, the set of all invertible elements in R). However, this paper does not give any useful strategy for computing $|id(RG)|$ in the nontrivial case. In this respect, in [3] we calculated the cardinality $|id(RG)|$ in terms associated only with R and G, provided that $char(RG) = p$ is a prime integer.

So, the goal of this brief article is to generalize this result for the case of rings of arbitrary characteristic, thus completely solving the indicated problem. Our calculations will substantially depend on $id(R)$, G_0 and its sections. The motivation is also of practical interest in order to obtain some major applications; in fact, group rings and their idempotents are known to have valuable applications in coding theory - see the survey [6] and the monograph [5], Section 9.1.

2010 *Mathematics Subject Classification*. Primary 16S34; Secondary 16U60, 20K20, 20K21

Keywords. Abelian groups, commutative rings, idempotents, indecomposable rings, decompositions, isomorphisms, sets, cardinalities

Received: 22 July 2011; Accepted: 11 August 2011

Communicated by Miroslav Ćirić

Email address: pvdanchev@yahoo.com (Peter V. Danchev)

2. The main result

We begin with some crucial preliminaries.

Lemma 2.1. *Let R be a commutative unitary ring and let $n \in \mathbb{N}$. Then*

$$R = \oplus_{1 \leq i \leq n} L_i,$$

where every L_i is an indecomposable unitary subring of R, if and only if $|id(R)| = 2^n$.

Proof. "Necessity": Since

$$R = \bigoplus_{1 \leq i \leq n} L_i \cong L_1 \times \cdots \times L_n,$$

it is easy to check that $id(R) = id(L_1) \times \cdots \times id(L_n)$ in a set-theoretical sense. But $|id(L_1)| = \cdots = |id(L_n)| = 2$ and hence it follows that $|id(R)| = 2^n$, as stated.

"Sufficiency": It is well known that the set B of all idempotents of R is a Boolean algebra with infima given by $e \wedge f = ef$, suprema given by $e \vee f = e + f - ef$, and complements given by $e' = 1 - e$. But $id(R)$ is finite of cardinality 2^n and is formally (set-theoretically) isomorphic to the Boolean algebra B. Therefore, B is finite. Let $e_1, \cdots, e_n$ be the atoms of B, i.e., the primitive idempotents in R. Moreover, a simple technical manipulation shows that the elements of B are precisely the sums $\sum_{i \in I} e_i$ for subsets $I \subseteq \{1, \cdots, n\}$, and these are all distinct. Thus B has exactly 2^n elements. Consequently, $R = Re_1 \oplus \cdots \oplus Re_n$ where each direct summand $Re_i = L_i$ is an indecomposable ring for $i \in [1, n]$, as asserted. □

Remark 2.2. These subrings $L_i = Re_i$ do not contain the same identity element as that of R; in fact, each indecomposable summand L_i has identity e_i which is a primitive idempotent of R ($1 \leq i \leq n$). Moreover, it is easily verified that all L_i are even ideals of R. A simple check shows also that if the natural number k is invertible in R, then the same can be said of each of the L_i's too.

A similar approach is demonstrated in both [1] and [2].

Theorem 2.3. ([8]) *Suppose that P is a commutative indecomposable unitary ring and F is a finite abelian group of $exp(F) \in P^*$. Then*

$$PF \cong \oplus_{d/exp(F)} \oplus_{a(d)} P[\zeta_d],$$

where $a(d) = \frac{|\{a \in F : order(a) = d\}|}{[P[\zeta_d] : P]}$, and $\sum_{d/exp(F)} a(d)[P[\zeta_d] : P] = |F|$.

Proposition 2.4. ([9]) *Suppose that P is a commutative indecomposable unitary ring and $n \geq 1$. Then $P[\zeta_n]$ is also a commutative indecomposable unitary ring.*

Now we have all the ingredients necessary to prove the following main result, which is in the focus of our investigation.

Theorem 2.5. *Let R be a commutative unitary ring and G an abelian group. Then the following conditions hold:*

(1) $|id(RG)| = |id(R)|$ *if* $supp(G) \cap inv(K) = \emptyset$, *for each indecomposable subring K of R;*

(2) $|id(RG)| = |id(R)| \cdot |G_0 / \coprod_{p \notin inv(K)} G_p|$ *if either* $|id(R)| \geq \aleph_0$ *or* $|G_0 / \coprod_{p \notin inv(K)} G_p| \geq \aleph_0$ *and* $supp(G) \cap inv(K) \neq \emptyset$, *for some indecomposable subring K of R;*

(3) $|id(RG)| = 2^{\sum_{1 \leq i \leq log_2 |id(R)|} \sum_{d/exp(\coprod_{q \in inv(Re_1) \cap inv(Re_i)} G_q)} a_i(d)}$ *if* $|id(R)| < \aleph_0$ *with primitive idempotents* $\{e_1, \cdots, e_n\}$ *and* $1 < |\coprod_{q \in inv(Re_1)} G_q| < \aleph_0$, *where*

$$a_i(d) = \frac{|\{g \in \coprod_{q \in inv(Re_1) \cap inv(Re_i)} G_q : order(g) = d\}|}{[(Re_i)[\zeta_d] : (Re_i)]}.$$

Proof. Letting $e \in id(RG)$, we have $e \in id(FG)$ for some finitely generated subring F of R. Thus one may observe that $id(RG) = \bigcup_{F \leq R} id(FG)$ and $id(R) = \bigcup_{F \leq R} id(F)$. Moreover, one can decompose $F = K_1 \times \cdots \times K_n$ for some indecomposable subrings $K_1, \cdots, K_n$ of F where $n \in \mathbb{N}$. But then $FG = K_1G \times \cdots \times K_nG$, whence it is easily checked that $id(FG) = id(K_1G) \times \cdots \times id(K_nG)$ in a set-theoretic sense. That is why we may further assume that R is finitely generated or even indecomposable.

Invoking the chief result of [7], every idempotent e from RG is either an idempotent from R, i.e. belongs to $id(R)$, or is nontrivial and lies in $R(\coprod_{q \in inv(R)} G_q)$ provided that $id(R) = \{0, 1\}$. In fact, there are idempotents of the form $e = \frac{1}{|C|} \sum_{c \in C} c$, where $C \leq \coprod_{q \in inv(R)} G_q \leq G_0$ is a finite subgroup such that $|C|$ inverts in some subring P of R. It is evident that $id(RG) = id(RG_0)$ since $supp(G) = supp(G_0)$.

Supposing now that the intersection $supp(G) \cap inv(K)$ is empty for every indecomposable subring K of R, it follows in virtue of the result from [7] mentioned above that $|id(K_iG)| = |id(K_i)| = 2$. Consequently, $|id(FG)| = 2^n = |id(F)|$ and, by what we have already noted, we derive that $|id(RG)| = |id(R)|$, and we are done in this case. Note that in this situation $supp(G) \cap inv(F) = \emptyset$.

Let us now suppose that there exists an indecomposable subring K of R such that $supp(G)$ and $inv(K)$ have non-empty intersection. Without loss of generality we may assume that such a ring K is a member of the decomposition of some finitely generated subring of R. Furthermore, denote $G_0' = \coprod_{q \in inv(K)} G_q$. On the other hand, one may write

$$G_0 = \coprod_{l} G_l = \coprod_{q \in inv(K)} G_q \times \coprod_{p \notin inv(K)} G_p = G_0' \times \coprod_{p \notin inv(K)} G_p.$$

Again from the result of [7] cited above, it is easily verified that $id(KG) = id(KG_0)$. Moreover,

$$KG_0 = (KG_0')\Big(\coprod_{p \notin inv(K)} G_p\Big) = \Big(K\Big(\coprod_{p \notin inv(K)} G_p\Big)\Big)G_0'.$$

Since K is indecomposable, it plainly follows from [7] that so is $K(\coprod_{p \notin inv(K)} G_p)$, whence $id(KG_0) = id(KG_0')$, because $inv(K) = inv(K(\coprod_{p \notin inv(K)}))$. Thus, $id(KG) = id(KG_0')$.

Suppose first that G_0' is infinite. Since K is indecomposable, any its subring with identity contains the identity of K, i.e. it has the same identity. So, in view of [7], it follows that $|id(KG)| = |M|$ where M is the set of all finite subgroups S of G_0'. But $G_0' = \cup_{S \in M} S$ and this assures that $|G_0'| = |M|$. Thus $|id(KG)| = |G_0'|$ if G_0' is infinite. In the case where G_0' is finite, it follows from our arguments presented below that $|id(KG)| = 2^t$, where $t = \sum_{d/exp(G_0')} a(d)$ with

$$a(d) = \frac{|\{g \in G_0' : order(g) = d\}|}{[K[\zeta_d] : K]}.$$

Next, if now one of $id(R)$ or G_0' is infinite, we observe as we have done above that $|id(RG)| \geq \aleph_0$. Therefore, combining both cases, we have

$$|id(RG)| = |id(R)| + |G_0'| = |id(R)| \cdot |G_0'| = max(|id(R)|, |G_0'|),$$

and we are done in this situation.

Finally, let us assume that both $id(R)$ and $G_0 / \coprod_{p \notin inv(K)} G_p \cong G_0'$ are finite, and $supp(G) \cap inv(K) \neq \emptyset$ for some indecomposable subring K of R. Since $id(R)$ is finite, according to Lemma 2.1, R can be decomposed like this:

$$R = \bigoplus_{1 \leq i \leq n} R_i,$$

where each subring $R_i = Re_i$ is indecomposable and $1 \leq i \leq n = log_2|id(R)|$ - thereby $\{e_1, \cdots, e_n\}$ are the primitive idempotents of R.

As aforementioned, we will assume that $K = R_1 = Re_1$ and thus $G_0' = \coprod_{q \in inv(R_1)} G_q$. Clearly $exp(G_0') \in R_1^*$ - note that $G_0' \neq 1$ is tantamount to $supp(G) \cap inv(R_1) \neq \emptyset$.

Furthermore, we deduce that

$$RG = \bigoplus_{1\le i\le n} R_iG,$$

and

$$RG'_0 \cong \bigoplus_{1\le i\le n} R_iG'_0.$$

and, as a consequence, by what we have shown above

$$id(RG) = id(R_1G) \times \cdots \times id(R_iG) = id(R_1G'_0) \times \cdots \times id(R_iG'_0) = id(RG'_0)$$

written in a set-theoretical sense.

On the other hand, for any $i \in (1, n]$, we have the equalities

$$\begin{aligned} R_iG'_0 &= R_i\Big(\coprod_{q\in inv(R_1)} G_q\Big) = \Big(R_i\Big(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q\Big)\Big)\Big(\coprod_{q\in inv(R_1)\setminus inv(R_i)} G_q\Big) \\ &= \Big(R_i\Big(\coprod_{q\in inv(R_1)\setminus inv(R_i)} G_q\Big)\Big)\Big(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q\Big). \end{aligned}$$

Since R_i is indecomposable, it follows from [7] that the same can be said of the ring $R_i(\coprod_{q\in inv(R_1)\setminus inv(R_i)} G_q)$. Moreover $inv(R_i(\coprod_{q\in inv(R_1)\setminus inv(R_i)} G_q)) = inv(R_i)$, and hence

$$id(R_iG'_0) = id\Big(R_i\Big(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q\Big)\Big).$$

Note that if $inv(R_1) \cap inv(R_i) = \emptyset$ we write $\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q = 1$ and so this forces at once that

$$\Big|id\Big(R_i\Big(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q\Big)\Big)\Big| = |id(R_i)| = 2,$$

for each i with $1 < i \le n$ which satisfies the above intersection requirement.

Since $exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q) \in R_i^*$, by Theorem 2.3, we obtain

$$R_i\Big(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q\Big) \cong \bigoplus_{d/exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q)} \oplus_{a_i(d)} R_i[\zeta_d]$$

where

$$a_i(d) = \frac{|\{g \in \coprod_{q\in inv(R_1)\cap inv(R_i)} G_q : order(g) = d\}|}{[R_i[\zeta_d] : R_i]}.$$

However, Proposition 2.4 tells us that the ring extensions $R_i[\zeta_d]$ are indecomposable as well, and their number is $\sum_{d/exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q)} a_i(d)$. That is why

$$R\Big(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q\Big) \cong \bigoplus_{1\le i\le n} \bigoplus_{d/exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q)} \bigoplus_{a_i(d)} R_i[\zeta_d] = \bigoplus_{d/exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q)} \bigoplus_{1\le i\le n} \bigoplus_{a_i(d)} R_i[\zeta_d].$$

Thus we conclude that the number of all irreducible summands is equal to

$$\sum_{d/exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q)} \sum_{1\le i\le log_2|id(R)|} a_i(d) = \sum_{1\le i\le log_2|id(R)|} \sum_{d/exp(\coprod_{q\in inv(R_1)\cap inv(R_i)} G_q)} a_i(d).$$

Finally, we again apply Lemma 2.1 to obtain the desired equality, which completes the proof in all generality. □

Acknowledgment

The author is grateful to the referee for comments which have helped to improve the text.

References

[1] P. Danchev, Warfield invariants in commutative group rings, J. Algebra Appl. 8 (2009) 829–836.
[2] P. Danchev, Maximal divisible subgroups in modular group rings of p-mixed abelian groups, Bull. Braz. Math. Soc. 41 (2010) 63–72.
[3] P. Danchev, The number of idempotents in commutative group rings of prime characteristic, Sarajevo J. Math. 7 (2011).
[4] G. Karpilovsky, Commutative Group Algebras, Marcel Dekker, New York, 1983.
[5] A.V. Kelarev, Ring Constructions and Applications, World Scientific, River Edge, NJ, 2002.
[6] A.V. Kelarev, P. Solé, Error-correcting codes as ideals in group rings, Contemporary Mathematics 273 (2001) 11-18.
[7] W. May, Group algebras over finitely generated rings, J. Algebra 39 (1976) 483–511.
[8] T. Mollov, N. Nachev, Unit groups of commutative group rings, Commun. Algebra 34 (2006), 3835–3857.
[9] N. Nachev, Nilpotent elements and idempotents in commutative group rings, Commun. Algebra 33 (2005) 3631–3637.