THE NUMBER OF IDEMPOTENTS IN COMMUTATIVE
GROUP RINGS OF PRIME CHARACTERISTIC

P. V. DANCHEV

Abstract. Suppose $R$ is a commutative unitary ring of prime characteristic $p$ and $G$ is a multiplicative abelian group. The cardinality of the set $\text{id}(RG)$ consisting of all idempotent elements in the group ring $RG$, is explicitly calculated only in terms associated with $R$ and $G$ or their sections.

1. Introduction

Throughout this brief paper, we will assume that $R$ is a commutative unitary ring (i.e., a commutative ring containing an identity element 1) of prime characteristic, for instance $p$, and $G$ is an abelian group written multiplicatively as is customary when studying group rings. As usual, $RG$ denotes the group ring of $G$ over $R$, $G_0 = \coprod_p G_p$ denotes the torsion subgroup of $G$ with $p$-primary component $G_p$ and, for any natural number $k$, $\zeta_k$ denotes the primitive $k$th root of unity. Likewise, under the ordinary algebraic operations, $R[\zeta_k]$ designates the free $R$-module over $R$, generated algebraically as a ring (namely as an overring of $R$) by $\zeta_k$, with dimension equal to $[R[\zeta_k] : R]$. All other unexplained notions and notations are standard and follow those from [3].

Traditionally, we put $\text{id}(R)$ and $\text{id}(RG)$ to be the sets of all idempotents in $R$ and $RG$, respectively. Since 0 and 1 are trivial examples of such elements, the inequalities $|\text{id}(RG)| \geq |\text{id}(R)| \geq 2$ hold taking into account that $\text{id}(R) \subseteq \text{id}(RG)$. A question which naturally arises in some aspects of commutative group rings theory (see, e.g., [1] and [2]) is to compute in an explicit form the cardinality $|\text{id}(RG)|$ (in other words, the number of all idempotents being finite or infinite) in a commutative group ring $RG$.

For an arbitrary commutative unitary ring $L$, it was proved in [4] that $|\text{id}(LG)| = 2$ if, and only if, $|\text{id}(L)| = 2$ and $\text{supp}(G) \cap \text{inv}(L) = \emptyset$, where

\[2010 \text{ Mathematics Subject Classification.} \quad 16S34, 16U60, 20K20, 20K21.

Key words and phrases. Groups, rings, idempotents, indecomposable rings, sets, cardinalities.
supp(G) = \{p : G_p \neq 1\} and inv(L) = \{p : p.1 \in L^*\} and L^* denotes the unit group of L (that is the set of all invertible elements in L). However, the mentioned paper does not give any strategy for computing |id(LG)| in the non-trivial case.

So, the purpose of the present short article is to do that but only for rings of prime characteristic. Our computations will mainly depend upon on id(R), of course, as well as on G_0 and its sections.

2. The main result

We begin with some preliminaries. The first statement appeared in both [1] and [2].

Lemma 2.1. ([1], [2]) Let L be a commutative unitary ring. Then L = \bigoplus_{1 \leq i \leq n} L_i, where each L_i is an indecomposable unitary subring of L, if and only if |id(L)| = 2^n.

Theorem 2.2. ([5]) Let P be a commutative indecomposable unitary ring and let F be a finite abelian group of exp(F) \in P^*. Then $PF \cong \bigoplus_{d=\exp(F)} \bigoplus_{a(d)} \mathbb{P}[\zeta_d]$, where $a(d) = \frac{|\{a \in F : \text{order}(a) = d\}|}{[P(\zeta_d) : P]}$, and $\sum_{d=\exp(F)} a(d)[P(\zeta_d) : P] = |F|.$

Proposition 2.3. ([6]) Let P be a commutative indecomposable unitary ring and k \geq 1. Then $P[\zeta_k]$ is also a commutative indecomposable unitary ring.

We now have all the machinery needed to prove the following.

Theorem 2.4. Suppose R is a commutative unitary ring of prime characteristic p and G is an abelian group. Then the following hold:

(1) |id(RG)| = |id(R)| if G_0 = G_p;

(2) |id(RG)| = |id(R)||G_0/G_p| if either |id(R)| \geq \aleph_0 or |G_0/G_p| \geq \aleph_0;

(3) |id(RG)| = 2^{\sum_{d=\exp(G_0/G_p)} \sum_{1 \leq i \leq \log_2 |id(R)|} a_i(d)} if both |id(R)| < \aleph_0 and |G_0/G_p| < \aleph_0,

where $a_i(d) = \frac{|\{g \in G_0/G_p : \text{order}(g) = d\}|}{[R_i(\zeta_d) : R_i]}$ with $R_i = Re_i$ and $\{e_i\}_{1 \leq i \leq n}$ the system of primitive idempotents of R; $n = \log_2 |id(R)|$.

Proof. Letting $e \in id(RG)$, we have $e \in KG$ for some finitely generated subring K of R. Thus $K = R_1 \times \cdots \times R_n$ for some indecomposable subrings $R_i$ of R with 1 \leq i \leq n, and hence $KG = R_1G \times \cdots \times R_nG$. One may observe that id(KG) = id(R_1G) \times \cdots \times id(R_nG) in a set-theoretic sense.
That is why, furthermore, we may assume that $R$ is finitely generated and even indecomposable.

Now, taking into account [4], every idempotent $e$ from $RG$ is either an idempotent from $R$, i.e. belongs to $\text{id}(R)$, or is non-trivial and lies in $R(\coprod_{q \neq p} G_q)$ provided $\text{id}(R) = \{0, 1\}$. In fact, there are idempotents of the form $e = \frac{1}{|C|} \sum_{c \in C} c$, where $C \leq \coprod_{q \neq p} G_q \leq G_0$ is a finite subgroup such that $|C|$ inverts in $R$.

If now $G$ is $p$-mixed, that is $G_0 = G_p$, it is readily seen that $\text{supp}(G) \cap \text{inv}(R) = \emptyset$ since $\text{inv}(R)$ contains all primes but $p$. Consequently, applying the aforementioned result of [4], the only idempotents in $RG$ are those from $R$ and we are finished in that case.

Next, if one of $\text{id}(R)$ or $G_0/G_p \cong \coprod_{q \neq p} G_q$ is infinite, we observe via the above that $|\text{id}(RG)| \geq N_0$. Notice that $\text{id}(RG) = \text{id}(RG_0)$ since $\text{supp}(G) = \text{supp}(G_0)$. But $RG_0 = R(\coprod_{q \neq p} G_q)G_p$ and hence as in the previous paragraph $\text{id}(RG_0) = \text{id}(R(\coprod_{q \neq p} G_q)) = \text{id}(R(G_0/G_p))$. Therefore, we have $|\text{id}(RG)| = \max(|\text{id}(R)|, |M|)$, where $M$ is the set of all finite subgroups $F$ of $\coprod_{q \neq p} G_q$. But $\coprod_{q \neq p} G_q = \bigcup_{F \in M} F$ and, if $G_0/G_p$ is infinite, this ensures that $|\coprod_{q \neq p} G_q| = |M|$. Moreover, if $\text{id}(R)$ is infinite, $R$ contains an infinite number of indecomposable subrings which number equals to $|\text{id}(R)|$. So, we are done in this case.

Let us assume now that both $\text{id}(R)$ and $G_0/G_p \cong \coprod_{q \neq p} G_q$ are finite. Since $\coprod_{q \neq p} G_q$ is pure in $G_0$ being its direct factor and $G_0$ is pure in $G$, it follows that $\coprod_{q \neq p} G_q$ is pure in $G$. So, one may write $G = (\coprod_{q \neq p} G_q) \times M \cong (G_0/G_p) \times M$ for some subgroup $M \cong G/\coprod_{q \neq p} G_q$ of $G$ which is obviously $p$-mixed because $M_0 = (G/\coprod_{q \neq p} G_q)_0 = G_0/\coprod_{q \neq p} G_q \cong G_p$. Therefore $RG \cong (R(G_0/G_p))M$ and from point (a) it is easily verified that $\text{id}(RG) = \text{id}(R(G_0/G_p)) = \text{id}(R(\coprod_{q \neq p} G_q))$.

On the other hand, since $\text{id}(R)$ is finite, $R$ can be decomposed as follows:

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

where each $R_i$ is indecomposable with the same characteristic $p$ and $1 \leq i \leq n = \log_2 |\text{id}(R)|$ by Lemma 2.1. Furthermore, we deduce that

$$R \left( \coprod_{q \neq p} G_q \right) \cong \oplus_{1 \leq i \leq n} R_i \left( \coprod_{q \neq p} G_q \right).$$

Since $\coprod_{q \neq p} G_q$ is of finite exponent which inverts in $R$, according to Theorem 2.2, we have

$$R_i \left( \coprod_{q \neq p} G_q \right) \cong \oplus_{d \mid \exp(G_0/G_p)} \oplus_{a_i(d)} R_i[\zeta_d]$$
where $a_i(d) = \frac{|\{g \in \bigcup_{p \neq q} G_q : \text{order}(g) = d\}|}{|R_i[G_q : R_i]|}$. But due to Proposition 2.3, the ring extensions $R_i[G_q]$ are also indecomposable and their number is $\sum_{d \div \exp(G_0/G_p)} a_i(d)$. That is why

$$R\left( \bigoplus_{q \neq p} G_q \right) \cong \bigoplus_{1 \leq i \leq n} \bigoplus_{d \div \exp(G_0/G_p)} \bigoplus_{1 \leq i \leq n} \bigoplus_{a_i(d)} R_i[G_q].$$

Thus we conclude that the number of all irreducible summands equals to $\sum_{d \div \exp(G_0/G_p)} \sum_{1 \leq i \leq |\text{id}(R)|} a_i(d)$. Finally, we apply Lemma 2.1 again to obtain the desired equality, as asserted.

A question which immediately arises is the following.

**Problem.** For any commutative unitary ring $L$ and any abelian group $G$ calculate $\text{id}(LG)$.

**References**


