BULLETIN OF THE
GREEK MATHEMATICAL SOCIETY
Volume 56, 2009 (21–28)

Idempotent-Nilpotent Units in Commutative Group Rings

PETER DANCHEV[1]

Keywords and phrases: decompositions, normalized units, nilpotents, idempotents, torsion units, group rings.

Abstract. *Let G be an Abelian group and R a commutative unital ring. Karpilovsky proved in (Arch. Mat. Basel, 1982-1983) that if G is torsion-free, then the group $V(RG)$ of all normalized units in the group ring RG can be decomposed in a special manner as a product of an idempotent unit and a nilpotent unit. We shall show that the converse also holds in some cases, that is, if $V(RG)$ possesses such a special decomposition, then G has to be without torsion elements under certain limitations on R and G. Even more generally, a criterion for the validity of that special decomposition is found only in terms associated with R and G. This encompasses our recent results in (Extr. Math., 2008) and (Kochi J. Math., 2009).*

I. Introduction

Throughout the present paper, suppose that R is a commutative unital (i.e., with identity element) ring with nil-radical $N(R)$ and multiplicative group of units $U(R)$, and G is an Abelian group with torsion part G_t and p-primary component G_p. As usual, RG denotes the group ring of G over R with its group of normalized invertible elements $V(RG)$ and augmentation ideal $I(RG;G)$. Following [11], [12] we also consider the set

$$Id(RG) = \{e_1g_1 + \cdots + e_kg_k | e_i^2 = e_i \in R, e_ie_j = 0, 1 \leq i \neq j \leq k, \sum_i e_i = 1; g_i \in G\}.$$

It is clear that $Id(RG) \leq V(RG)$ because $(e_1g_1+\cdots+e_kg_k)(e_1g_1^{-1}+\cdots+e_kg_k^{-1}) = 1$, and we may write $Id(RG) = \langle e_1g_1 + \cdots + e_kg_k\rangle$, i.e., $Id(RG)$ is generated by such elements described as above since the finite sums and products of orthogonal idempotents are again idempotents.

All other notions and notations are standard and follow essentially those from the survey paper of Karpilovsky [12] or the classical books of Karpilovsky [11] and Sehgal [13].

Karpilovsky showed in [9] and [10] (see [12] too) that if G is torsion-free (i.e., $G_t = 1$) then $V(RG)$ possesses a special decomposition like this:

$$V(RG) = Id(RG) \times (1 + I(N(R)G;G)).$$

[1] *2000 Mathematics Subject Classification*: 16S34, 16U60, 20K10, 20K20, 20K21.

In particular, when R is both indecomposable and reduced, $V(RG) = G$ holds, which generalizes a classical result due to Higman for trivial units.

The purpose of this article, as a culmination of a series of our investigations (see, for instance, [6], [7] and [8]), is to find a necessary and sufficient condition when the above direct decomposition is valid in terms of R and G. The only restriction that we shall use is that RG is of prime characteristic p (i.e., R is in such characteristic).

It is probably worthwhile noticing that many different variants of (direct) decompositions of $V(RG)$ which are explored in details can be found in [1], [2], [3], [4] and [5], respectively. Likewise, in [6] we studied the trivial units in commutative group rings and a complete answer for their existence is given in some general cases; e.g., $char(R)$ is a finite number greater than 1.

II. Decompositions of normalized unit groups

We foremost need a few preliminary technicalities, starting with

Lemma 1. *Let p be a prime. Then*

$$char(R) = p \iff char(R/N(R)) = p \text{ and } char(R) \text{ is a prime number.}$$

Proof. The necessity is obvious.

As for the sufficiency, write $p(1 + N(R)) = p.1 + N(R) = N(R)$, i.e., $p.1 \in N(R)$. Therefore, there exists a natural n such that $(1 + \cdots + 1)^{q^n} = 0$, where $q = char(R)$ and the sum is taken p-times. But this is tantamount to $1+\cdots+1 = 0$ (again p-times) which is precisely $p.1 = 0$. Thus, since $(p, q) = 1$ if $p \neq q$ and hence $q.1 = 0$ inverts in R, which is false, we deduce that $q = p$ and the result follows. □

Lemma 2. *Let $char(R) = p$ be a prime integer. Then the following equality holds*:

$$U(R/N(R)) = \{r + N(R) | r \in U(R)\}.$$

Proof. The inclusion "$\supseteq$" is straightforward because there exist $r, f \in R$ with $rf = 1$ and so $(r + N(R))(f + N(R)) = rf + N(R) = 1 + N(R)$.

As for the converse inclusion "$\subseteq$", choose x to lie in the left hand-side. Hence, we write $x = r + N(R) \in U(R/N(R))$ for some $r \in R$. But there is $f + N(R)$ with $f \in R$ such that $(r + N(R))(f + N(R)) = rf + N(R) = 1 + N(R)$. Consequently, $rf - 1 \in N(R)$. Furthermore, there exists a natural t such that $(rf-1)^{p^t} = (rf)^{p^t} - 1 = r^{p^t} f^{p^t} - 1 = 0$. So, $r^{p^t} f^{p^t} = r.r^{p^t-1} f^{p^t} = 1$ which means that $r \in U(R)$, This gives the desired relation. □

Standardly, define $id(R)$ as the subset of R consisting of all idempotents in R, that is,

$$id(R) = \{e \in R | e^2 = e\}.$$

The following simple technical claim is useful.

Lemma 3. *Let $char(R) = 2$. Then*

$$id(R) \leq R.$$

Proof. Choose $e_1 \in id(R)$ and $e_2 \in id(R)$. Since $(e_1 + e_2)^2 = e_1^2 + e_2^2 = e_1 + e_2$, we have that $e_1 + e_2 \in id(R)$. Obviously, $0, 1 \in id(R)$. Moreover, $(e_1e_2)^2 = e_1^2e_2^2 = e_1e_2$ and thus $e_1e_2 \in id(R)$ as well. This gives our claim. □

Proposition 4. *Let $I \lhd R$ be a nil-ideal and let $char(R) = p$ be a prime natural. Then the maps $\Phi : V(RG) \to V((R/I)G)$ and $\Phi : Id(RG) \to Id((R/I)G)$, induced by the natural map $\varphi : R \to R/I$, are surjective group homomorphisms (= group epimorphisms).*

Proof. The ring epimorphism $\varphi : R \to R/I$ is linearly extended to the group ring epimorphism $\Phi : RG \to (R/I)G$ with kernel IG. Since Φ is a ring homomorphism, its restriction on $V(RG)$ is the group homomorphism $\Phi : V(RG) \to V((R/I)G)$. What we intend to show is that $\Phi(V(RG)) = V((R/I)G)$, that is, for each $w \in V((R/I)G)$ there is $v \in V(RG)$ with the property $\Phi(v) = w$; certainly $v \in RG$. In order to demonstrate this, assume that there is $w' \in V((R/I)G)$ such that $ww' = 1$. So, there exists $v' \in RG$ with $\Phi(v') = w'$. Furthermore, $\Phi(v).\Phi(v') = \Phi(v.v') = 1 = \Phi(1)$ whence $\Phi(v.v' - 1) = 0$. Thus $v.v' - 1 \in IG$, so that there is $m \in \mathbb{N}$ for which $(v.v' - 1)^{p^m} = v^{p^m}.v'^{p^m} - 1 = 0$, i.e., $v^{p^m}.v'^{p^m} = 1$. This ensures that $v \in V(RG)$ as required.

Next, letting $z \in Id((R/I)G)$ we write $z = (r_1 + I)g_1 + \cdots + (r_k + I)g_k$ where $g_1, \cdots, g_k \in G$, $r_1, \cdots, r_k \in R$ with $r_1 + \cdots + r_k - 1 \in I$, $r_i + I = r_i^2 + I$ and $r_ir_j \in I$ for every $1 \leq i \neq j \leq k$. It suffices to show that there exists $y = f_1g_1 + \cdots + f_kg_k$ where $f_1, \cdots, f_k \in R$ with $f_1 + \cdots + f_k = 1$, $f_i = f_i^2$ and $f_if_j = 0$ for each $1 \leq i \neq j \leq k$ such that $\Phi(y) = z$. In fact, $r_1 + \cdots + r_k - 1 \in I$, $r_i - r_i^2 \in I$ and $r_ir_j \in I$. Since we have a finite number of relations and I is a nil-ideal, there is a natural number n such that $(r_1 + \cdots + r_k - 1)^{p^n} = r_1^{p^n} + \cdots + r_k^{p^n} - 1 = 0$, i.e., $r_1^{p^n} + \cdots + r_k^{p^n} = 1$; $r_i^{p^n} - r_i^{2p^n} = 0$, i.e., $r_i^{p^n} = (r_i^{p^n})^2$; $(r_ir_j)^{p^n} = r_i^{p^n}r_j^{p^n} = 0$. Denote $r_i^{p^n} = e'_i$ for all $1 \leq i \leq k$. By what we have just proved $e'_1 + \cdots + e'_k = 1$, $e'_i = e'^2_i$ and $e'_ie'_j = 0$ whenever $1 \leq i \neq j \leq k$. Besides, we observe that $r_i + I = r_i^{p^n} + I = e'_i + I$ whence we select $f_i = e'_i$ for all indices i. That is why, $y = e'_1g_1 + \cdots + e'_kg_k$ with $z = (e'_i + I)g_1 + \cdots + (e'_k + I)g_k = \Phi(e'_1g_1 + \cdots + e'_kg_k)$, as wanted. □

Next, we recollect some basic facts necessary for our presentation.

Theorem. ([7]) *Let K be a commutative unital ring of prime characteristic p and G a non-identity Abelian group. Then $V(KG) = Id(KG)$ if and only if $N(K) = 0$ and one of the following clauses holds:*

(1) $G_t = 1$;
(2) $|G| = 2 = p$ and K is Boolean;
(3) $|G| = 2$, $\forall\ r \in K : 2r - 1 \in U(K) \iff r^2 = r$;
(4) $|G| = 3$, $\forall\ (r, f) \in K : 1 + 3r^2 + 3f^2 + 3rf - 3r - 3f \in U(K) \iff r^2 = r$, $f^2 = f$ and $rf = 0$.

Proposition. ([2]) *Let char(R)=p be a prime and $G_p = 1$. Then the following formula is true*:

$$V_p(RG) = 1 + I(N(R)G; G)$$

Now, we have at our disposal all the machinery needed to proceed by proving

Theorem 5. *Let R be a commutative unital ring of prime characteristic p and let G be a non-identity Abelian group. Then $V(RG) = Id(RG) \times (1 + I(N(R)G; G))$ if and only if one of the following conditions holds:*

(a) $G_t = 1$;
(b) $|G| = p = 2$ and $R = id(R) + N(R)$;
(c) $|G| = 2$, $\forall\ r \in R : 2r - 1 \in U(R) \iff r^2 = r$;
(d) $|G| = 3$, $\forall\ (r, f) \in R : 1+3r^2+3f^2+3rf-3r-3f \in U(R) \iff r^2-r \in N(R)$, $f^2 - f \in N(R)$ and $rf \in N(R)$.

Proof. First of all, we emphasize that every $x \in 1 + I(N(R)G; G)$ can be written in canonical form as $x = 1 + f + \sum_{g\in G\setminus\{1\}} f_g g$, where $f, f_g \in N(R)$ and $f + \sum_{g\in G\setminus\{1\}} f_g = 0$.

The situation when $G_t = 1$ was handled in [9]-[12]. So, assume further that $G_t \neq 1$.

We shall differ two basic cases.

Case 1: $G = G_p$ (Notice that $G_p \neq 1$ since otherwise $G = 1$ which is false.)

Foremost, let $V(RG)$ be decomposed as given in the text of the theorem. We claim that $|G| = 2$. In order to demonstrate this, assume the contrary that $|G| \geq 3$. Hence, we construct the element $1 + b - h \in V(RG)$ where $b, h \in G \setminus \{1\}$ with $b \neq h$. Thus we write

$$1 + b - h = (1 + f + \sum_{g\in G\setminus\{1\}} f_g g)(e_1c_1 + \cdots + e_kc_k)$$

where $f, f_g \in N(R)$ with $f + \sum_{g\in G\setminus\{1\}} f_g = 0$; $e_1, \cdots, e_k$ are pair-wise orthogonal idempotents in R with $e_1 + \cdots + e_k = 1$ and $c_1, \cdots, c_k \in G$. If we assume that $e_i \neq 0$ for some $1 \leq i \leq k$, then by multiplying both sides of the foregoing equality with e_i, we obtain that

$$e_i + e_i b - e_i h = (e_i + e_i f)c_i + \sum_{g\in G\setminus\{1\}} f_g e_i g c_i$$

Clearly, the elements in the two sides are in canonical forms as well. Therefore, $e_i = f_{g'} e_i \in N(R)$ for some $g' \in G\setminus\{1\}$ and thus $e_i = 0$. So, without loss of generality, we may assume that $e_1 = 1$ and $e_2 = \cdots = e_k = 0$.

Furthermore,

$$1 + b - h = (1 + f)c_1 + \sum_{g\in G\setminus\{1\}} f_g g c_1$$

But since $\pm 1 \notin N(R)$, this record is impossible. Consequently, $|G| < 3$, i.e., $|G| = 2$ with $G = \langle h | h^2 = 1\rangle = \{1, h | h^2 = 1\}$, whence $p = 2 = char(R)$ as claimed.

Now, we intend to prove that $R = id(R) + N(R)$ where in virtue of Lemma 3 we have $id(R) \leq R$. In doing that, choose $r \in R \setminus \{0, 1\}$ and write again

$$1 + r - rh = (1 + f - fh)(eh + 1 - e).$$

After some minor technical steps this is equivalent to $1 + r - rh = (1 - e + f) + (e - f)h$. Consequently, $r = f - e \in N(R) + id(R)$, as required.

Conversely, assume that the conditions in (b) are satisfied. If $v \in V(RG)$ is an arbitrary element, then v is of the form $v = 1 + r - rh$, where $r \in R$ and $h \in G$ with $h^2 = 1$. But $r = f + e$, where $f \in N(R)$ and $e \in id(R)$, so that we subsequently obtain $v = 1+f+e+(f+e)h = 1+f+e+(e+fe+f+ef)h = 1+f+e+(1+e)fh+(1+f)eh = (1+f)eh+(1+f)(1+e)+ef+(1+e)fh = (1+f)eh+(1+f)(1+e)+efh^2+(1+e)fh = (1 + f + fh)(1 + e + eh) \in (1 + I(N(R)G; G))Id(RG)$, as stated.

Case 2: $G \neq G_p$.

Hence there exists $h \in G\setminus G_p$. Let first again $V(RG)$ have the direct decomposition from the text of the theorem. We assert that $G_p = 1$. To show this, assume the contrapositive, i.e., that there is $1 \neq g_p \in G_p$. So, we write

$$1 + h - hg_p = (1 + f + \sum_{g\in G\setminus\{1\}} f_g g)(e_1c_1 + \cdots + e_kc_k)$$

where the symbols from the right hand-side are already described above.

If we assume that $e_i \neq 0$ for some $1 \leq i \leq k$, then by multiplying both sides of the preceding equality with e_i, we derive that

$$e_i + e_ih - e_ihg_p = (e_i + e_if)c_i + \sum_{g\in G\setminus\{1\}} f_ge_igc_i$$

Because the elements in the two sides are also in canonical forms, we deduce that $e_i = f_{g'}e_i \in N(R)$ for some $g' \in G \setminus \{1\}$ whence $e_i = 0$. Furthermore, with no harm of generality, we may assume that $e_1 = 1$ and $e_2 = \cdots = e_k = 0$.

Consequently,

$$1 + h - hg_p = (1 + f)c_1 + \sum_{g\in G\setminus\{1\}} f_ggc_1$$

Since $\pm 1 \notin N(R)$, this record is possible only when $g_p = 1$. This assures our assertion that $G_p = 1$.

Next, because by what we have just argued above $G_p = 1$, an appeal to the previously listed Proposition gives that $V_p(RG) = 1 + I(N(R)G; G)$, so that $V(RG) = Id(RG) \times V_p(RG)$; note also that $1 + I(N(R)G; G) \leq V_p(RG)$ and thus $V(RG) = Id(RG)\times(1+I(N(R)G; G)) \subseteq Id(RG)\times V_p(RG)$ since $Id(RG)\cap V_p(RG) = Id_p(RG) = Id(RG_p) = 1$. Finally, $V(RG) = Id(RG) \times V_p(RG)$ really follows.

Moreover, we claim that

$$V(RG) = Id(RG) \times V_p(RG) \iff V((R/N(R))G) = Id((R/N(R))G).$$

Indeed, consider the natural map $\phi : R \to R/N(R)$ which linearly induces both the ring and group homomorphisms $\Phi : RG \to (R/N(R))G$ with kernel $N(R)G$, which is a nil-ideal, $\Phi : V(RG) \to V((R/N(R))G)$ and $\Phi : Id(RG) \to Id((R/N(R))G)$ with $\Phi : G \to G$ formally true (i.e., it is the identity). The first one is obviously surjective, while the second and third ones are also surjective owing to Proposition 4. Likewise, $\Phi : V_p(RG) \to V_p((R/N(R))G) = 1$ taking into account that $G_p = 1$.

And so, since as observed above the maps are actually epimorphisms, $V(RG) = V_p(RG) \times Id(RG)$ obviously implies that

$$V((R/N(R))G) = \Phi(V(RG)) = \Phi(V_p(RG).Id(RG)) = \Phi(V_p(RG)).\Phi(Id(RG)) =$$

$$= \Phi(Id(RG)) = Id((R/N(R))G)$$

as desired.

(We pause to note that only the inclusion $\Phi(Id(RG)) \subseteq Id((R/N(R))G)$ is enough because $Id((R/N(R))G) \subseteq V((R/N(R))G)$; however for completeness we used the fact that Φ acts epimorphically on $Id(RG)$ as well.)

As for the converse, given that $V((R/N(R))G) = Id((R/N(R))G)$ and choose an arbitrary $v \in V(RG)$. Hence $\Phi(v) = w \in Id((R/N(R))G)$ and in accordance with

Proposition 4 there exists $u \in Id(R)$ such that $\Phi(u) = w$. Therefore, $\Phi(v) = \Phi(u)$ and thereby $\Phi(v - u) = 0$ ensures that $v - u = d \in N(R)G$. Thus $v = u + d = u(1 + du^{-1}) \in Id(RG)V_p(RG)$, as required. So, the claim sustained.

Furthermore, invoking to the main result from [7] (compare with the Theorem quoted above), combined with Lemmas 1 and 2 plus some folklore ring-theoretical facts, we conclude that clauses (a)-(d) are satisfied and vice versa. □

Remark. It is worth noting that condition (2) is decidable from condition (3) as well as (b) is symmetrically decidable from (c) but, however, for the sake of completeness we listed them. In fact, the first is self-evident. As for the second one, supposing $r \in R$ is an arbitrary element, we have $r^2 - r \in N(R)$. So, there is $n \in \mathbb{N}$ with $r^{2.2^n} - r^{2^n} = r^{2^{n+1}} - r^{2^n} = 0$ (note that $char(R) = 2$) and hence $(r^{2^n})^2 = r^{2^n} = e$ is an idempotent. But $(r - e)^{2^n} = r^{2^n} - e = 0$ and so $r - e \in N(R)$. Finally, $r \in id(R) + N(R)$, which leads to $R = id(R) + N(R)$ as expected.

As an immediate consequence, we yield the following assertion.

Corollary 6. ([8]) *Suppose R is a commutative unital ring of prime characteristic p and $G \neq 1$ is an Abelian group. Then $V(RG) = G \times (1 + I(N(R)G; G))$ if and only if R is indecomposable and the following hold:*

(a) $G_t = 1$;
(b) $|G| = p = 2$ and $R = L + N(R)$ where $|L| = 2$;
(c) $|G| = 2$, $\forall\, r \in R : 2r - 1 \in U(R) \iff r^2 = r$;
(d) $|G| = 3$, $\forall\, (r, f) \in R : 1+3r^2+3f^2+3rf-3r-3f \in U(R) \iff r^2-r \in N(R)$, $f^2 - f \in N(R)$ and $rf \in N(R)$.

Proof. That $id(R) = \{0, 1\}$ follows as in [8]. Thus $Id(RG) = G$ and we apply Theorem 5 to finish our arguments. □

Remark. Note that these four conditions (a)-(d) are absolutely equivalent to the corresponding ones from [8].

REFERENCES

[1] P. Danchev, *On a decomposition formula in commutative group rings*, Miskolc Math. Notes **6**(2) (2005), 153-159.

[2] ——— , *On a decomposition equality in modular group rings*, Vlad. Math. J. **9**(2) (2007), 3-8.

[3] ——— , *A note on decompositions in abelian group rings*, An. St. Univ. Ovidius Const. - Math. **16**(1) (2008), 73-76.

[4] ——— , *A note on a formula of May concerning normed units in abelian group rings*, Bull.

Allahabad Math. Soc. **23**(1) (2008), 155-158.

[5] ______ , *Note on a decomposition of normalized unit groups in abelian group algebras*, Bull. Allahabad Math. Soc. **23**(2) (2008), 365-368.

[6] ______ , *Trivial units in commutative group algebras*, Extr. Math. **23**(1) (2008), 49-60.

[7] ______ , *Idempotent units in commutative group rings*, Kochi Math. J. **4** (2009), 61-66.

[8] ______ , *G-Nilpotent units in commutative group rings*, Ann. Sci. Math. Quebec, to appear.

[9] G. Karpilovsky, *On units in commutative group rings*, Arch. Math. (Basel) **38** (1982), 420-422.

[10] ______ , *On finite generation of unit groups of commutative group rings*, Arch. Math. (Basel) **40** (1983), 503-508.

[11] ______ , Unit Groups of Group Rings, Longman Sci. and Techn., Harlow 1989.

[12] ______ , *Units of commutative group algebras*, Expo. Math. **8** (1990), 247-287.

[13] S. Sehgal, Topics in Group Rings, Marcel Dekker, New York 1978.

Peter Danchev
13, General Kutuzov Street
block 7, floor 2, flat 4
4003 Plovdiv, Bulgaria
E-mail: pvdanchev@yahoo.com