Annals of the University of Bucharest (mathematical series)
(Analele Universităţii Bucureşti. Matematică)
1 (LIX) (2010), 239–244

Units and decompositions in modular group rings of prime characteristic

Peter Danchev

Communicated by Constantin Năstăsescu

Abstract - We give a systematic study of some normalized invertible elements in modular group rings of prime characteristic. In particular, by summarizing some classical results, we also provide more conceptual proofs of recent own results published in An. Univ. Bucureşti, Mat. (2008-2009).

Key words and phrases : units, idempotents, nilpotents, decompositions, group rings.

Mathematics Subject Classification (2000) **:** 16S34, 16U60, 20K10, 20K20, 20K21.

1. Introduction and known facts

Throughout the present paper, suppose R is a commutative unital ring and G is an abelian group written multiplicatively as is customary when discussing group rings; in this way all our groups and subgroups are multiplicative. As usual, RG denotes the group ring of G over R with unit group $U(RG)$ and its subgroup of normalized units $V(RG) = \{\sum_{g\in G} r_g g \in U(RG) \mid \sum_{g\in G} r_g = 1\}$, which will be in the focus of our further interest. Standardly, $U(R)$ and $N(R)$ denote the unit group and the nil-radical of R, respectively, and G_t the torsion subgroup of G with p-component G_p. Imitating [9], we define $\mathbb{P}$ to be the set of all primes which is a subset of the set $\mathbb{N}$ of all naturals, $supp(G) = \{p \in \mathbb{P} \mid G_p \neq 1\}$, $inv(R) = \{p \in \mathbb{P} \mid p \cdot 1_R \in U(R)\}$ and $\emptyset$ the empty set.

Moreover, following [8], we state the so-called *idempotent subgroup* of $V(RG)$. Specifically, we write

$$Id(RG) = \{e_1g_1 + \cdots + e_sg_s | e_i \in R, e_i^2 = e_i, e_ie_j = 0,$$

$$\sum_{1\leq i\leq s} e_i = 1, g_i \in G, 1 \leq i \neq j \leq s \in \mathbb{N}\}.$$

This group is also named *a group of idempotent units*. All other notions and notations are standard and follow essentially those from [8] and [9].

A problem of major interest is to describe the units in commutative group rings, that is, to characterize the group $U(RG)$ up to an isomorphism (see, for instance, [6] and [7]). However, at this stage, this question seems to be insurmountable in general. So, some partial cases, like to characterize all trivial units or more generally all idempotent units, are also very interesting (see, for example, [2], [3] and [5]). A generalization of the idempotent units, called idempotent-nilpotent units, was investigated in [4].

The purpose of this article is to consider one special decomposition of $V(RG)$ that is too close to being all its elements products of idempotent units with p-torsion units. Especially, we obtain a complete answer for rings of prime characteristic, say p. This somewhat generalizes in a more conceptual way the results in [1].

We will now recognize one major assertion that will be used in the sequel.

Theorem 1.1. (see [2]) *Let $G \neq 1$ and let $char(R) = p$ be a prime. Then $V(RG) = Id(RG)$ if and only if $N(R) = 0$ and precisely one of the following clauses holds.*

(i) $G_t = 1$.

(ii) $|G| = 2$ *and for all* $r \in R$: $2r - 1 \in U(R) \iff r^2 = r$.

(iii) $|G| = 3$ *and for all* $r, f \in R$: $1 + 3r^2 + 3f^2 + 3rf - 3r - 3f \in U(R) \iff r^2 = r,\ f^2 = f$ *and* $rf = 0$.

2. Main results

First of all, we recollect some useful statements.

Proposition 2.1. *Suppose that $supp(G) \cap inv(R) \neq \emptyset$. If one has $V(RG) = Id(RG)V_p(RG)$, then $G = G_t$.*

Proof. Let us assume in a way of contradiction that $G \neq G_t$. Hence there is $g \in G \setminus G_t$. Since the intersection between $supp(G)$ and $inv(R)$ is non-empty, there exists a prime q such that $G_q \neq 1$ and $q = q \cdot 1_R \in U(R)$. Therefore, $e = \frac{1}{q}(1 + a + a^2 + \cdots + a^{q-1})$ is an idempotent, i.e., $e^2 = e$, whenever $a \in G_q$ with the property $a^q = 1$. Next, consider the element $u_g = 1 - e + eg$. Clearly $1 - e + eg \in V(RG)$ because $(1 - e + eg)(1 - e + eg^{-1}) = 1$. So, we can write $1 - e + eg = (r_1b_1 + \cdots + r_sb_s)v_p$ where $r_1b_1 + \cdots + r_sb_s \in Id(RG)$ and $v_p \in V_p(RG)$. We furthermore observe that there is a natural number k such that $u_g^{p^k} = 1 - e + eg^{p^k} = r_1b_1^{p^k} + \cdots + r_sb_s^{p^k}$, that is,

$$1 - q^{-1} - q^{-1}a - q^{-1}a^2 - \cdots - q^{-1}a^{q-1} + q^{-1}g + q^{-1}ag + q^{-1}a^2g + \cdots + q^{-1}a^{q-1}g$$

$$= r_1b_1^{p^k} + \cdots + r_sb_s^{p^k}.$$

It is self-evident that the left hand-side is written in a canonical form, and that because the finite sum of orthogonal idempotents is again an idempotent, which is also orthogonal with the remaining ones that are not members of the sum, we may without loss of generality assume that the right hand-side is in canonical form as well. However, the above equality is impossible since in the left hand-side there is no orthogonal idempotents. This contradiction substantiates our claim that G must be of necessity torsion, as claimed. □

The following technicality is our crucial tool in the reduction of the general case to a well-known particular case established in [3].

Proposition 2.2. *Suppose $char(R) = p$ is a prime integer. The following two points are true.*

(i) $V(RG) = Id(RG)V_p(RG) \iff V(LG) = Id(LG)V_p(LG)$ where $L = R/N(R)$.

(ii) Let $N(R) = 0$. Then $V(RG) = Id(RG)V_p(RG) \iff$ (1) $G_t = G_p$, or (2) $G = G_t \neq G_p$ and $V(R(\coprod_{q\neq p} G_q)) = Id(R(\coprod_{q\neq p} G_q))$.

Proof. (i) Consider the natural map $\varphi : R \to L$. It can be linearly extended in a natural way to the homomorphism $\Phi : RG \to LG$ with kernel $N(R)G$, and its restrictions $\Phi : V(RG) \to V(LG)$, $\Phi : V_p(RG) \to V_p(LG)$ and $\Phi : Id(RG) \to Id(LG)$.

Next, we shall show that in each of these cases Φ is a surjective homomorphism, that is, Φ is an epimorphism. In fact, that each element from LG has a pre-image in RG is straightforward, so we concentrate on the other three cases. Given $v \in V(LG)$, hence by the above comments, there is $z \in RG$ with $\Phi(z) = v$. Since there is $v' \in V(LG)$ with $vv' = 1$ and $z' \in RG$ with $\Phi(z') = v'$, we conclude that $\Phi(zz') = 1 = \Phi(1)$ which ensures that $\Phi(zz' - 1) = 0$. It now follows that $zz' - 1 \in N(R)G \subseteq N(RG)$ and thus $zz' \in 1 + N(RG) \subseteq U(RG)$. Therefore, $z \in U(RG)$. Moreover, the pre-image z can be chosen to be of augmentation 1. Indeed, suppose $(r_1+N(R))g_1+\cdots+(r_s+N(R))g_s \in V(LG)$ with $r_1+\cdots+r_s-1 = \alpha \in N(R)$. Hence it is clear that we can take $z = -\alpha \cdot 1 + r_1g_1 + \cdots + r_sg_s$ which has $aug(z) = -\alpha + r_1 + \cdots + r_s = 1$. Finally, $z \in V(RG)$ as desired. It is worthwhile noticing that we have not used that R has prime characteristic. However, this is needed for proving the surjection $V_p(RG) \to V_p(LG)$. But it plainly follows from the preceding step taking into account that the kernel of $V(RG) \to V(LG)$ in this case is $1 + I(N(R)G; G)$ which is a p-group.

As for the last homomorphism $Id(RG) \to Id(LG)$ it can be processed as follows: Suppose Φ maps $e_1g_1 + \cdots + e_sg_s$ into $(e_1 + N(R))g_1 + \cdots + (e_s + N(R))g_s$ where $e_1 + \cdots + e_s - 1 \in N(R)$, $e_i^2 - e_i \in N(R)$ and $e_ie_j \in N(R)$ whenever $1 \leq i \neq j \leq s \in \mathbb{N}$. Thus there exists a positive integer t such that $e_1^{p^t} + \cdots + e_s^{p^t} = 1$, $(e_i^{p^t})^2 = e_i^{p^t}$ and $e_i^{p^t}e_j^{p^t} = 0$ for all different i and j.

Denoting $e_i^{p^t}=e_i'$ for every $1\leq i\leq s$, we observe that $\Phi(e_1'g_1+\cdots+e_s'g_s)=(e_1'+N(R))g_1+\cdots+(e_s'+N(R))g_s=(e_1+N(R))g_1+\cdots+(e_s+N(R))g_s$ because each $e_i+N(R)$ is an idempotent and hence $e_i+N(R)=(e_i+N(R))^{p^t}=e_i^{p^t}+N(R)=e_i'+N(R)$ for any i with $1\leq i\leq s$. This substantiates our claim that $\Phi: Id(RG)\to Id(LG)$ is, in fact, surjective.

So, we are ready to prove the equivalence.

"$\Rightarrow$". By taking Φ in both sides of $V(RG)=Id(RG)V_p(RG)$ and by what we have shown above that $\Phi(V(RG))=V(LG), \Phi(Id(RG))=Id(LG)$ and $\Phi(V_p(RG))=V_p(LG)$, we directly yield that $V(LG)=Id(LG)V_p(LG)$ as stated.

"$\Leftarrow$". Conversely, write $V(LG)=Id(LG)V_p(LG)$ and choose an arbitrary element $x\in V(RG)$. Hence there is $y\in V(LG)$ such that $\Phi(x)=y$. But $y=zv_p$ where $z\in Id(LG)$ and $v_p\in V_p(LG)$. Again by what we have established above, there are $u\in Id(RG)$ and $u_p\in V_p(RG)$ such that $\Phi(u)=z$ and $\Phi(u_p)=v_p$. Thus $\Phi(x)=\Phi(u)\Phi(u_p)=\Phi(uu_p)$, and hence $\Phi(xu^{-1}u_p^{-1})=1$. This ensures that $xu^{-1}u_p^{-1}\in ker\Phi=1+I(N(R)G;G)\subseteq V_p(RG)$ which implies that $x\in Id(RG)V_p(RG)$ as required.

(ii) Denote $G'=\coprod_{q\neq p}G_q$.

"$\Rightarrow$". If G is p-mixed, i.e., $G_t=G_p$, we are done. So, assume that $G_t\neq G_p$. We next claim that G is torsion and to this aim we consider two situations. First, if $supp(G)\cap inv(R)\neq\emptyset$ we apply Proposition 2.1 to infer that G is torsion, indeed. If now $supp(G)\cap inv(R)=\emptyset$, then because $char(R)=p$ is a prime integer, we deduce that $inv(R)=\{q\neq p|p\in\mathbb{P}\}$, that is the set of all primes but p, and $supp(G)=\{p\}$, that is the set of a single element p. Consequently, $G_t=G_p$ which is a contradiction. Finally, $G=G_t$ as expected.

Furthermore, given $x\in V(RG')$ whence $x\in Id(R(G'\times G_p))V_p(RG)=Id(RG')Id(RG_p)V_p(RG)=Id(RG')Id_p(RG)V_p(RG)=Id(RG')V_p(RG)$. Thus $x=yz$ where $y\in Id(RG')\subseteq V(RG')$ and $z\in V_p(RG)$. But $xy^{-1}\in V(RG')\cap V_p(RG)=V_p(RG')=1$ and hence $x=y\in Id(RG')$ as required. So we conclude that either $G'=1$ or $G'\neq 1$, $G=G_p\times G'$ and $V(RG')=Id(RG')$ as asserted.

"$\Leftarrow$". Write $G=G_p\times G'$, hence it is easily checked that $V(RG)=V(RG')V_p(RG)=Id(RG')V_p(RG)=Id(RG)V_p(RG)$ because $Id(RG')\subseteq Id(RG)$. This substantiates our claim.

By the way, note that $Id(RG)=Id(R(G_p\times G'))=Id(RG_p)Id(RG')=Id_p(RG)Id(RG')\subseteq Id(RG')V_p(RG)$ whence we obtain $Id(RG)V_p(RG)=Id(RG')V_p(RG)$. □

We now have at our disposal all the machinery needed to prove the following chief result.

Theorem 2.1. *Suppose $char(R)=p$ is a prime integer. Then $V(RG)=$*

$Id(RG)V_p(RG)$ if and only if exactly one of the following clauses is valid.

(i) $G_t = G_p$.

(ii) $G = G_p \times G_2$, $|G_2| = 2$ *and for all* $r \in R$: $2r - 1 \in U(R) \iff r^2 - r \in N(R)$.

(iii) $G = G_p \times G_3$, $|G_3| = 3$ *and for all* $r, f \in R$: $1 + 3r^2 + 3f^2 + 3rf - 3r - 3f \in U(R)$ *if and only if* $r^2 - r \in N(R)$, $f^2 - f \in N(R)$ *and* $rf \in N(R)$.

Proof. According to Proposition 2.2 (i), we may without loss of generality assume that R is reduced, i.e., $N(R) = 0$. So, in view of Proposition 2.2 (ii) we deduce that either $G_t = G_p$, which is exactly point (i), or $G = G_t \neq G_p$ and $V(RG') = Id(RG')$ where we put $G' = \coprod_{q \neq p} G_q$. Therefore, the theorem from [2] stated in Section I plus some folklore ring theoretic and group theoretic facts allow us to infer that points (ii) and (iii) hold too. □

Remark 2.1. It is worthwhile noticing that the ring part in point (c) is equivalent to the condition that the equation $X^2 + XY + Y^2 = 1 + N(R)$ has only trivial solutions in $R/N(R)$.

As an immediate consequence, we derive the following.

Corollary 2.1. (see [1]) *Let* $char(R) = p$ *be a prime. Then* $V(RG) = GV_p(RG)$ *if and only if* $G = G_p$ *or* $G \neq G_p$, R *is indecomposable and at most one of the following is valid.*

(i) $G_t = G_p$.

(ii) $p = 3$, $U(R) = \pm 1 + N(R)$ *and* $G = G_3 \times G_2$ *with* $|G_2| = 2$.

(iii) $p = 2$, $U(R) = 1 + N(R)$, *the equation* $x^2 + xy + y^2 = 1 + N(R)$ *possesses only trivial solutions in* $R/N(R)$ *and* $G = G_2 \times G_3$ *with* $|G_3| = 3$.

Proof. What we need to show is that R is indecomposable whenever G is not p-torsion that is a routine exercise. In fact, if $g \in G \setminus G_p$ and $r \in id(R) \setminus \{0, 1\}$, then $1 - r + rg \in V(RG)$ and so we can write $1 - r + rg = av_p$ for some $a \in G$ and $v_p \in V_p(RG)$. Thus there is $k \in \mathbb{N}$ such that $1 - r + rg^{p^k} = a^{p^k}$, which is obviously wrong. This shows that $id(R) = \{0, 1\}$ as wanted. Furthermore, Theorem 2.1 manifestly works. □

We close the work with two challenging problems.

Problem 1. Find a necessary and sufficient condition for the truthfulness of the equality

$$V(RG) = Id(RG)V_t(RG).$$

Problem 2. Find a criterion for the validity of the equalities

$$V(RG) = Id(RG)V(RG_p)$$

and

$$V(RG) = Id(RG)V(RG_t).$$

Acknowledgments

The author is gratefully thankful to the referee for his/her suggestions that improved the presentation of the article.

References

[1] P.V. DANCHEV, On a decomposition of normalized units in abelian group algebras, *An. Univ. Bucureşti Mat.*, **57** (2008), 133-138.

[2] P.V. DANCHEV, Idempotent units in commutative group rings, *Kochi J. Math.*, **4** (2009), 61-66.

[3] P.V. DANCHEV, On idempotent units in commutative group rings, *An. Univ. Bucureşti Mat.*, **58** (2009), 17-22.

[4] P.V. DANCHEV, Idempotent-nilpotent units in commutative group rings, *Bull. Greek Math. Soc.*, **56** (2009), 21-28.

[5] P.V. DANCHEV, Idempotent units of commutative group rings, *Commun. Algebra*, **38** (2010), 4649-4654.

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

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

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

[9] W.L. MAY, Group algebras over finitely generated rings, *J. Algebra*, **39** (1976), 483-511.

Peter Danchev

13, General Kutuzov Str., bl. 7, fl. 2, ap. 4

4003 Plovdiv, Bulgaria

E-mail: pvdanchev@yahoo.com