Ann. Sci. Math. Québec **33** (2009), no 1, 39–44

# *G*-UNIPOTENT UNITS IN COMMUTATIVE GROUP RINGS

PETER DANCHEV

RÉSUMÉ. Nous donnons des conditions nécessaires et suffisantes pour que toutes les unités normalisées dans un anneau commutatif de caractéristique $p > 0$ soient des unités $G$-unipotentes. Ceci est la suite de nos travaux récents sur les unités idempotentes dans les anneaux de groupes publiés dans Kochi J. Math. (2009), et améliore nos résultats publiés dans Extracta Math. (2008).

ABSTRACT. We find a necessary and sufficient condition under which all normalized units in a commutative group ring with prime characteristic $p > 0$ are $G$-unipotent units. This continues our recent investigation on idempotent units in commutative group rings published in Kochi J. Math. (2009) and also strengthens our own results from Extracta Math. (2008).

## 1. Introduction

Throughout the present paper, suppose that $RG$ is the group ring of an abelian group $G$ over a commutative unitary (*i.e.*, with identity element) ring $R$. Standardly, we let $V(RG)$ denote the group of normalized units with $p$-torsion part $V_p(RG)$, and $I(RG; G)$ denote the fundamental ideal of $RG$; more generally, for any subgroup $H$ of $G$ and any subring $L$ of $R$ we let $I(LG; H)$ denote the relative augmentation ideal of $LG$ with respect to $H$, generated by the elements $1 - h$, with $h \in H$. Besides, $G_t$ denotes the torsion subgroup of $G$ with $p$-primary component $G_p$, and $U(R)$ and $N(R)$ denote respectively the unit group and the nil-radical of $R$. All other notations and notions are as usual and follow those from [7], [8] and [9].

The classical concept of "trivial units" was studied in [2] and completely resolved in the case of rings with finite characteristic greater than 1 (for some other aspects of trivial units the reader can consult [9]). The purpose of the current article is to generalize this to the so-called $G$-nilpotent units (also termed hereafter $G$-unipotent units).

**Definition 1.** We shall say that the unit $v \in V(RG)$ is a *$G$-unipotent unit* if there exists a decomposition $v = wg$, where $w \in 1 + I(N(R)G; G)$ and $g \in G$.

It is evident that $1 + I(N(R)G; G) \leq V(RG)$, which subgroup we shall call *the $G$-unipotent subgroup*. Moreover, $1 + I(N(R)G; G) \leq V_p(RG)$ whenever char$(R) = p$ is prime.

Reçu le 16 septembre 2008 et, sous forme définitive, le 7 mai 2009.

In this way we shall find a criterion only in terms of $R$ and $G$ which determines when all normalized units in $RG$ are $G$-unipotent units. However, we shall restrict our attention to rings of prime characteristic, say $p$. In particular, when $N(R) = 0$, we shall obtain as an immediate consequence one of our results in [2]. It is noteworthy that our method of proof is at all different to that in [2]. Our statements somewhat enlarge in the subject those from [2], [4], [5] and [6].

## 2. Main results

Before stating and proving our main theorem, we need two preparatory technical lemmas.

**Lemma 2.** *Let $p$ be prime. Then char$(R) = p$ if and only if char$(R/N(R)) = p$ and char$(R)$ is a prime number.*

**Proof.** This follows directly from the classical well-known fact that the characteristic of $R/N(R)$ divides the characteristic of $R$, and the latter is prime. □

**Lemma 3.** *Let char$(R) = p$ be prime. Then the following equality holds:*

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

**Proof.** It is straightforward that the left-hand side contains the right-hand side because there exist $r, f \in R$ with $rf = 1$ and so

$$(r + N(R))(f + N(R)) = rf + N(R) = 1 + N(R).$$

For the converse, given $x = r + N(R) \in U(R/N(R))$, there exists $f + N(R)$ with $f \in R$ such that $(r + N(R))(f + N(R)) = rf + N(R) = 1 + N(R)$. It therefore follows that $rf - 1 \in N(R)$, whence there is $t \in \mathbb{N}$ such that $(rf)^{p^t} - 1 = 0$, *i.e.*, $r^{p^t} f^{p^t} = 1$. This insures that $r \in U(R)$, as required. □

So, we now have at our disposal all the necessary information to prove the following criterion for $G$-unipotent units.

**Theorem 4.** *Let $R$ be a commutative unitary ring with char$(R) = p$ prime, and let $G \neq 1$ be an abelian group. Then $V(RG) = (1 + I(N(R)G; G)) \times G$ if and only if $R$ is indecomposable and one of the following conditions holds:*

(a) $G_t = 1$;

(b) $|G| = p = 2$, $R = L + N(R)$, *and* $L \leq R$, *with* $|L| = 2$;

(c) $|G| = 2$ *and* $U(R) = \pm 1 + N(R)$;

(d) $|G| = 3$, $p = 2$, $U(R) = 1 + N(R)$ *and, for each pair of elements* $a, b \in R$, *we have* $a^2 + b^2 + ab + 1 \in N(R)$ *if and only if* $1 + a \in N(R)$ *and* $1 + b \in N(R)$; $1 + a \in N(R)$ *and* $b \in N(R)$; *or* $a \in N(R)$ *and* $1 + b \in N(R)$.

**Proof.** First of all, we emphasize that every element $x$ 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 $f + \sum_{g \in G \setminus \{1\}} f_g = 0$. Also, every element $y$ in $1 + I(RG; G_p)$ can be written in canonical form as $y = \sum_{g \in G} r_g g$, where $r_g \in R$ with $\sum_{g \in aG_p} r_g = 1$, when $a \in G_p$; or $\sum_{g \in aG_p} r_g = 0$, when $a \notin G_p$, for any $a \in G$ of this sum.

The situation when $G$ is torsion-free was exhausted in [5] and [6]; see [8] as well. We therefore will assume in the sequel that $G_t \neq 1$.

Now, suppose that there is a non-trivial idempotent $r$ in $R$, that is $r^2 = r$ and $r \notin \{0, 1\}$. Hence $1 - r + rh \in V(RG)$ with inverse $1 - r + rh^{-1}$ whenever $1 \neq h \in G$ and thus we write

$$1 - r + rh = \left(1 + f + \sum_{g \in G \setminus \{1\}} f_g g\right) a = (1 + f)a + \sum_{g \in G \setminus \{1\}} f_g g a,$$

where $f, f_g \in N(R)$, with $f + \sum_{g \in G \setminus \{1\}} f_g = 0$ and $a \in G$. Since these two elements are both in canonical form, we easily obtain that either $r \in N(R)$ or $r \in 1 + N(R)$. This forces at once that either $r = 0$ or $r = 1$, which is a contradiction. This substantiates the claim that $R$ has no non-trivial idempotents.

Next, we distinguish some basic cases:

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

First, assume that $V(RG)$ can be decomposed as above. Then, if $|G| \geq 3$, we have $1 + b - h \in V(RG)$ whenever $b, h \in G \setminus \{1\}$, with $b \neq h$. So, we write

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

where $f, f_g \in N(R)$, with $f + \sum_{g \in G \setminus \{1\}} f_g = 0$ and $a \in G$. However, it is apparent that this relation is impossible since $\pm 1 \notin N(R)$. Thereby, $|G| = 2 = p$.

Furthermore, if $r \in R \setminus \{0, 1\}$ and $h \in G \setminus \{1\}$, then $1 + r - rh \in V(RG)$ and hence

$$1 + r - rh = (1 + f)a + \sum_{g \in G \setminus \{1\}} f_g g a$$

where $f, f_g \in N(R)$, with $f + \sum_{g \in G \setminus \{1\}} f_g = 0$ and $a \in G$. This immediately guarantees that $r \in N(R)$ or $r \in 1 + N(R)$. Therefore, $R = L + N(R)$ where $L = \{0, 1\} \leq R$.

Conversely, when (b) holds, $G = \{1, g\}$ and $R = \{0, 1\} + N(R)$. It is immediate from the canonical form mentioned previously that $G \cap (1 + I(N(R)G; G)) = 1$. If $x \in V(RG)$, then either $x$ or $xg$ is equal to $(1 - r) + rg = 1 + r(g - 1)$, for some $r \in N(R)$. Therefore, $x \in G \times (1 + I(N(R)G; G))$, as required.

Case 2: $G \neq G_p$.

First, let $V(RG)$ be decomposed as above. Hence

$$V_p(RG) = (1 + I(N(R)G; G)) \times G_p.$$

Since $G_p \subseteq 1 + I(RG; G_p) \subseteq V_p(RG)$, with the aid of the modular law we easily obtain that

$$\begin{aligned} 1 + I(RG; G_p) &= [(1 + I(N(R)G; G)) \times G_p] \cap (1 + I(RG; G_p)) \\ &= G_p \times [(1 + I(N(R)G; G)) \cap (1 + I(RG; G_p))]. \end{aligned}$$

But, it is a routine technical exercise to verify that

$$(1 + I(N(R)G; G)) \cap (1 + I(RG; G_p)) = 1 + I(N(R)G; G_p)$$

by comparison of the two canonical forms described above of each element belonging to the intersection. Thus, $1 + I(RG; G_p) = G_p \times (1 + I(N(R)G; G_p))$ and we claim that this is equivalent to $G_p = 1$. In fact, since there is $h \in G \setminus G_p$ we consider the element $1 + h - hg_p$ where $g_p \in G_p$ is an arbitrary element.

Thereby we write in canonical forms

$$1 + h - hg_p = a_p \left(1 + f + \sum_{g\in G\setminus\{1\}} f_g g\right) = (1 + f)a_p + \sum_{g\in G\setminus\{1\}} f_g g a_p$$

where $f, f_g \in N(R)$, with $f + \sum_{g\in G\setminus\{1\}} f_g = 0$ and $a_p \in G_p$. Since $\pm 1 \notin N(R)$ this relationship is possible uniquely when $g_p = a_p = 1$ and $f = f_g = 0$ for every $g \in G \setminus \{1\}$. So, the claim sustained.

(We pause to note that, in view of [1], we may also write

$$V_p(RG) = M[N(R); \textstyle\prod(G/G_p)] \times (1 + I(RG; G_p)),$$

where

$$\begin{aligned} M\left[N(R); \textstyle\prod(G/G_p)\right] &= \left\{1 + \sum_{g\in\prod(G/G_p)} r_g g \;\middle|\; r_g \in N(R), \sum_{g\in\prod(G/G_p)} r_g = 0\right\} \\ &\subseteq 1 + I(N(R)G; G) \end{aligned}$$

with $\prod(G/G_p)$ a complete set of representatives of $G$ with respect to $G_p$ containing the same identity as that of $G$.)

Consequently, $V_p(RG) = 1 + I(N(R)G; G)$ and $V(RG) = G \times V_p(RG)$ because $G \cap V_p(RG) = G_p = 1$. We shall further demonstrate that the last direct decomposition is equivalent to the equality

$$V((R/N(R))G) = G$$

which is crucial. Indeed, let us consider the natural map $\varphi : R \to R/N(R)$. It linearly induces an extension to the $R$-algebra surjection $\Phi : RG \to (R/N(R))G$, with kernel $N(R)G$ which is a nil-ideal, and whose restriction on $V(RG)$ is the group epimorphism $\Phi : V(RG) \to V((R/N(R))G)$ formally sending $G$ onto $G$. By applying $\Phi$ on both sides of $V(RG) = G \times V_p(RG)$ we deduce the desired relation $V((R/N(R))G) = G$ because $\Phi$ maps $V_p(RG)$ onto $V_p((R/N(R))G) = 1$ bearing in mind that $G_p = 1$.

Conversely, choose $v \in V(RG)$, hence there is $w \in V((R/N(R))G) = G$ such that $\Phi(v) = w$. But $w = \Phi(w)$, whence $\Phi(v) = \Phi(w)$, *i.e.*, $\Phi(v - w) = 0$. This means $v - w \in \ker\Phi = N(R)G$, that is $v \in G + N(R)G$ and $v = g + z$, where $g \in G$ and $z \in N(R)G$. Finally, we have $v = g(1 + g^{-1}z) \in GV_p(RG)$, as required. Thus $V(RG) = GV_p(RG)$ and, because $G \cap V_p(RG) = G_p = 1$, we derive the equality $V(RG) = G \times V_p(RG)$, as expected.

Henceforth, we wish to apply [2] in order to obtain $|G| = |U(R/N(R))| = 2$ or $|G| = 3$, $U(R/N(R)) = 1$ and, for each pair $a', b' \in R/N(R)$, we have that

${a'}^2+{b'}^2+a'b'+1'=0'$ gives $(a',b')=(1',1')$ or $(a',b')=(1',0')$ or $(a',b')=(0',1')$, where $0'$ and $1'$ are respectively the zero and the identity elements in $R/N(R)$. We now refer to Lemmas 2 and 3 which combined with some folklore ring-theoretical facts allow to infer that either $U(R)=\pm 1+N(R)$, or $p=2$, $U(R)=1+N(R)$ and the equation $a^2+b^2+ab+1=0$ possesses only trivial solutions in $R$. Thus (c) and (d) follow at once. The opposite assertion that both (c) and (d) independently imply $V(RG)=(1+I(N(R)G;G))\times G$ follows in the same manner since $G_p=1$. □

**Remark 5.** In the case when $G_t\neq 1$ and $G_p=1$, we may now illustrate another approach in order to show that $|G|\leq 3$. In fact, suppose that $G_t\neq 1$ and $G_p=1$ where $p=\mathrm{char}(R)$. Then $G_q\neq 1$ for some prime $q\neq p$. Let $g\in G$ be of order $q$. If $q\geq 5$, then the element

$$u=(1+g)^{q-1}-\frac{2^{q-1}-1}{q}(1+g+\cdots+g^{q-1})$$

is a non-$G$-unipotent unit of $V(RG)$. This follows from the argument that can be found in the proof of [4, Proposition 8] saying that at least two of the coefficients of $u$ are forced to be units of $R$, so it cannot be placed in the canonical form required in order to be a $G$-unipotent unit.

If $G$ is not cyclic of order $q$, let $e$ be an idempotent of $R\langle g\rangle$ other than 0 or 1 and whose coefficients lie in the prime subring $\mathbb{Z}_p$ of $R$. Then $e$ has at least two non-zero coefficients, and every non-zero coefficient of $e$ is a unit of $R$. Suppose that $h\in G\setminus\langle g\rangle$. Then $v=(1-e)+eh$ lies in $V(RG)\setminus\{1\}$, with inverse $v^{-1}=(1-e)+eh^{-1}$. But $v$ is not a $G$-unipotent unit because we cannot find $c\in G$ for which $vc$ lies in the canonical form of $1+I(N(R)G;G)$.

As a direct consequence, we derive the following result from [2].

**Corollary 6.** ([2]) *Let $G\neq 1$ and char$(R)=p$ be prime. Then $V(RG)=G$ if and only if $R$ is indecomposable and reduced, and one of the following holds:*

(a) $G_t=1$;

(b) $|G|=|R|=2$;

(c) $|G|=|U(R)|=2$;

(d) $|G|=3$, $U(R)=1$ *and the equation* $a^2+b^2+ab+1=0$ *has only the trivial solutions in $R$ that are* $(a,b)=(1,1)$, $(a,b)=(1,0)$ *and* $(a,b)=(0,1)$.

**Proof.** Suppose that $RG$ contains only trivial units. Then $R$ does not have non-trivial nilpotents since otherwise $0\neq r\in N(R)$ ensures that $1+r-rg=1+r(1-g)\in V(RG)\setminus G$ whenever $1\neq g\in G$, because $r(1-g)\in N(R)G$ is nilpotent and the sum of a unit and a nilpotent element is again a unit. Therefore, since $N(R)=0$, $V(RG)=G$ is obviously equivalent to $V(RG)=G\times[1+I(N(R)G;G)]$. Hereafter, we use Theorem 4 to infer that points (a)-(d) are valid.

In order to argue that char$(R)$ is 3 in case (c) and it is 2 in case (d), we use the fact that whenever char$(R)=p$ is prime, the prime subring of $R$ is a copy of $\mathbb{Z}/p\mathbb{Z}$, and thus $|U(R)|\geq p-1$. So, in case (d), $|U(R)|=1$ forces char$(R)=2$. In case (c), the condition $|U(R)|=2$ then implies char$(R)=2$ or char$(R)=3$. But, when

$|G| = 2$ and char$(R) = 2$, the only time we will have $V(RG) = G$ is in case (b), so char$(R) = 3$ in case (c) as wanted. $\square$

**Remark 7.** Note that $V(RG) = 1 + I(N(R)G; G)$ if and only if $G = 1$ since $G \cap (1 + I(N(R)G; G)) = 1$.

## 3. Concluding discussion

A problem of challenging interest is to find a criterion in terms associated with $R$ and $G$ when all normalized units in $RG$ are $G$-unipotent units, without the restriction on the characteristic of $R$ to be a prime number. This may be generalized to the following.

**Problem 8.** Find a necessary and sufficient condition when the equality

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

holds, provided that $Id(RG)$ is the idempotent subgroup of $V(RG)$; see, *e.g.*, [3].

This will be the subject of another study.

*Acknowledgement.* The author is very thankful to the referee for the numerous expert suggestions made.

## References

[1] P. Danchev, *Commutative group algebras of σ-summable abelian groups*, Proc. Amer. Math. Soc. **125** (1997), no. 9, 2559–2564.

[2] P. Danchev, *Trivial units in commutative group algebras*, Extracta Math. **23** (2008), no. 1, 49–60.

[3] P. Danchev, *Idempotent units in commutative group rings*, Kochi J. Math. **4** (2009), no. 1, 61–68.

[4] A. Herman, Y. Li and M. M. Parmenter, *Trivial units for group rings with G-adapted coefficient rings*, Canad. Math. Bull. **48** (2005), no. 1, 80–89.

[5] G. Karpilovsky, *On units in commutative group rings*, Arch. Math. (Basel) **38** (1982), no. 5, 420–422.

[6] G. Karpilovsky, *On finite generation of unit groups of commutative group rings*, Arch. Math. (Basel) **40** (1983), no. 6, 503–508.

[7] G. Karpilovsky, *Unit groups of group rings*, Pitman Monographs and Surveys in Pure and Applied Mathematics, **47** Longman Scientific & Technical, Harlow; copublished with John Wiley & Sons, Inc., New York, 1989, xiv+393 pp.

[8] G. Karpilovsky, *Units of commutative group algebras*, Exposition. Math. **8** (1990), no. 3, 247–287.

[9] S. K. Sehgal, *Topics in group rings*, Monographs and Textbooks in Pure and Applied Math., **50** Marcel Dekker, Inc., New York, 1978. vi+251 pp.

P. Danchev, 13, General Kutuzov Street, bl. 7, fl. 2, ap. 4, 4003 Plovdiv, Bulgaria.
pvdanchev@yahoo.com