EXTRACTA MATHEMATICAE Vol. **23**, Núm. 1, 49 – 60 (2008)

# Trivial Units in Commutative Group Algebras

Peter Danchev

13 *General Kutuzov Street, bl.* 7, *floor* 2, *flat* 4, 4003 *Plovdiv, Bulgaria*
*pvdanchev@yahoo.com*

Presented by Avinoam Mann Received December 4, 2006

*Abstract*: Let $G$ be an arbitrary abelian group and let $R$ be a commutative unitary ring of arbitrary characteristic. A necessary and sufficient condition is given for when all units in the group ring $RG$ are trivial provided that either $\mathrm{supp}(G) \cap \mathrm{inv}(R) \neq \emptyset$ or $RG$ is modular. In particular, we establish a comprehensive characterization by finding a criterion when $RG$ has only trivial units provided that $\mathrm{char}(R)$ is a positive number greater than 1. These achievements strengthen results due to Karpilovsky (Arch. Math. Basel, 1983), Herman-Li-Parmenter (Can. Math. Bull., 2005) and the author (Math. Commun., 2005).

*Key words*: normed units, trivial units, group rings, indecomposable rings, reduced rings, idempotents, nilpotents.

AMS *Subject Class.* (2000): 16U60, 16S34, 20K21.

## 1. Introduction

Let $G$ be a multiplicatively written abelian group with the subgroup of torsion $G_t = \coprod_{\forall p} G_p$, where $p$ is a prime integer, and with the set $\mathrm{supp}(G) = \{p : G_p \neq 1\}$. Let $R$ be a commutative ring with identity $1_R$ (such a ring is often called an *unitary ring*), with the multiplicative group $U(R)$ consisting of all invertible elements in $R$, also called units of $R$, with characteristic $\mathrm{char}(R)$ and with the set $\mathrm{inv}(R) = \{p : p \cdot 1_R \in U(R)\}$. If there is no confusion in some concrete situations, for facilitating of the exposition, we shall simply write 1 instead of $1_R$. Traditionally, $RG$ will always denote the group algebra of $G$ over $R$ with the group of normalized (i.e., of augmentation 1) units $V(RG)$. For any set $M$, the symbol $|M|$ denotes its cardinality. Using the standard terminology, $R$ is said to be *indecomposable* if it has no non-trivial idempotents, that are idempotents different from 0 and 1, and $R$ is said to be *reduced* if it does not have non-trivial nilpotents, that are nilpotents different from 0. As usual we shall say that the units in $RG$ are *trivial* precisely when $V(RG) = G$.

We will further quote only those results which are closely related on the

theme presented (the complete bibliography on that subject both in commutative and non-commutative aspects the readers can see in [10], [13], [14] and [15]). And so, the first monumental study on trivial units in commutative group rings was started by G. Higman in [7]. He proved that if $F$ is a field and $G$ is torsion-free (that is $G_t = 1$), then $V(FG) = G$. In [2], because of applicable purposes, we have incidentally extended this result by showing that if $F$ is a field and $G$ is an infinite abelian group, $V(FG) = G$ holds uniquely when $G_t = 1$. Later on, we also have further generalized in [3] this assertion by finding a necessary and sufficient condition when $V(FG) = G$ holds true for an arbitrary abelian group $G$ (see also [13, p. 583, Lemma 1.1]); another strengthening of such a criterion over a field of positive characteristic is established again by us in [4].

On the other hand, Karpilovsky obtained in [8] and [9] a criterion when a group ring element of a torsion-free group over an arbitrary commutative coefficient ring must be a unit. Moreover, in [9] he enlarged the Higman's attainment by arguing that if $G \neq 1$ is torsion-free, then $V(RG) = G$ holds only when $R$ is reduced and indecomposable. Here we shall try to improve this statement of Karpilovsky for an arbitrary abelian group $G$. To this goal, we shall use a theorem due to Nachev-Mollov from [12] which describes the isomorphic structure of $V(RG)$ when $G$ is finite and $R$ is indecomposable such that $\exp(G) \cdot 1_R \in U(R)$. So, the aim of the present paper is to provide an almost final analysis of the trivial units in commutative group rings, namely to describe when $V(RG) = G$ holds valid exclusively only in terms of $R$ and $G$, where $R$ possesses some minimal limitations and $G$ is arbitrary; especially we shall require the set $\mathrm{inv}(R) \cap \mathrm{supp}(G)$ to be non-empty (whence in $RG$ there are non-trivial idempotents (e.g. [1] or [11])) or the characteristic of $R$ is a positive integer $\geq 2$ or $RG$ is a modular group ring. We thus answer [4, Problem 1]. The essence in the proof of our main affirmation is that in the group ring there exist idempotents which complicated its structure. It is worthwhile noticing that in [14] is considered a special situation of group rings without idempotents, named $G$-adapted, that are extensions of the integral group ring $\mathbb{Z}G$, when $G$ is a finite abelian group (see [6] too). Specifically, the ring of coefficients is taken to be an integral domain of characteristic zero and if $p/|G|$ then $p \cdot 1_R \notin U(R)$, i.e., $p \notin \mathrm{inv}(R)$ and therefore $\mathrm{supp}(G) \cap \mathrm{inv}(R) = \emptyset$. By the way, note that in [16] is posed the following terminology: the abelian group $G$ is said to be $R$-favorable provided that $G_R = \coprod_{p \in \mathrm{inv}(R)} G_p = 1$ or, equivalently, $\mathrm{supp}(G) \cap \mathrm{inv}(R) = \emptyset$.

## 2. The main result

Before stating our general criterion for trivial units in $RG$ under some restrictions on $R$ and $G$, we formulate the major instrument needed for the finite case of $G$ in our theorem (see [12]).

Theorem. (Mollov-Nachev, 2004) *Let $G$ be a finite abelian group with exponent $n$ and let $R$ be a commutative indecomposable ring with identity in which the number $n$ is an invertible element. Then*

$$U(R) \times V(RG) \cong \coprod_{d/n} \coprod_{a(d)} U(R[\zeta_d])$$

*where $a(d) = |\{g \in G : \text{order}(g) = d\}|/(R[\zeta_d] : R)$ with $(R[\zeta_d] : R)$ the dimension of the free $R$-module $R[\zeta_d]$ over $R$, and $\zeta_d$ is a fixed root of an irreducible divisor of the cyclotomic polynomial $\Phi_d(x)$ over $R$.*

Since the above isomorphism can be taken to be canonical, i.e., that maps $U(R)$ isomorphically onto $U(R)$ or, in other words, to preserve the augmentation (see, for instance, [11]) hereafter, under the above circumstances on $R$ and $G$,

$$V(RG) \cong \coprod_{2 \leq d, d/n} \coprod_{a(d)} U(R[\zeta_d]).$$

The object here is to find a suitable criterion in appropriate terms associated only with $R$ and $G$. Before doing that, we need the following preparatory technicality.

Proposition. *Let $|G| = 3$ and $\text{char}(R) = 2$. Then $V(RG) = G$ if and only if $U(R) = 1$ and for each pair $(a, b) \in R$ the equality $a^2 + b^2 + ab + 1 = 0$ implies that $(a, b) = (1, 1)$ or $(a, b) = (1, 0)$ or $(a, b) = (0, 1)$.*

*Proof.* Firstly, suppose that $V(RG) = G$. If assume in a way of contradiction that there is $1 \neq r \in U(R)$, then it is an easy technical exercise to check that $u_r = 1 + (1 + r)g + (1 + r)g^2$ is a non-trivial unit with the inverse $u_r^{-1} = 1 + (1 + r^{-1})g + (1 + r^{-1})g^2 = u_{r^{-1}}$. On the other hand, each normalized element in $RG$ is of the form $1 + r + f + rg + fg^2$ for some $r, f \in R$. It is a straightforward matter to verify that

$$\begin{aligned}(1 + r + f + rg + fg^2)&(1 + r + f + fg + rg^2) \\ &= 1 + (r + r^2 + f + f^2 + rf)g + (r + r^2 + f + f^2 + rf)g^2 .\end{aligned}$$

Thus $1+r+f+rg+fg^2$ is a unit with inverse element $1+r+f+fg+rg^2$ precisely when $r+r^2+f+f^2+rf=0$. To be a trivial unit, it must be that both $r$ and $f$ are either 0 or 1. Moreover, this equation can be equivalently written as $(1+r)^2+(1+f)^2=(1+r)(1+f)+1$. Consequently, $a=1+r$ and $b=1+f$ do work.

Conversely, by modifying the same well-known idea as in [6, Proposition 3] (see [5, Proposition 3.1] too), we conclude that the identity $V(RG)=G$ holds. In fact, write $G=\langle g : g^3=1\rangle$ whence $RG=R\langle g\rangle$. It is plainly seen that all normed units in $RG$ are of the type $u=1+a+b+ag+bg^2$ for some $a,b\in R$. In the quotient ring $R\langle g\rangle/\langle 1+g+g^2\rangle\cong R[y]$, where $y^3=1$, $y\neq 1$ and $1+y+y^2=0$, we observe that the isomorphic image of $u$ is the unit

$$v=1+a+b+ay+by^2=1+a+b+ay+b(1+y)=1+a+(a+b)y\,.$$

Now, since $v$ is a unit, for any element $r+fy\in R[y]$ with $r,f\in R$ we can find $c+dy\in R[y]$ with $c,d\in R$ such that $v(c+dy)=r+fy$. But

$$\begin{aligned} v(c+dy)&=(1+a+(a+b)y)(c+dy)\\ &=(1+a)c+(a+b)d+((a+b)c+(1+b)d)y=r+fy \end{aligned}$$

implies that the system

$$\begin{aligned} (1+a)c+(a+b)d&=r\\ (a+b)c+(1+b)d&=f \end{aligned}$$

in the variables $c$ and $d$ has a solution in $R$ for each $r\in R$ and $f\in R$. Therefore, the determinant $D$ of the coefficient matrix arising from the above system must be a unit of $R$. Thus $D=1+a+b+ab+a^2+b^2\in U(R)=1$, hence $a+b+ab+a^2+b^2=0$. Finally, we replace $a$ with $1+a$ and $b$ with $1+b$ and thereby the foregoing conditions are necessary for the existence only of trivial units. ∎

Now, we are ready to proceed by proving the following chief affirmation (notice that when $\mathrm{supp}(G)=\emptyset$, i.e., $G_t=1$, we wish apply [9] to get the claim when $V(RG)=G$).

Main Theorem. *Suppose that $G$ is an abelian group and $R$ is a commutative unitary ring such that either* $\mathrm{supp}(G)\cap\mathrm{inv}(R)\neq\emptyset$ *or* $\mathrm{char}(R)$ *divides the orders of torsion elements in $G$. Then, $V(RG)=G$ $\Longleftrightarrow$*

(1) *$G=1$; or*

(2) *$G \neq 1$, $R$ is indecomposable and reduced, and one of the following conditions holds:*

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

(2.2) $|G| = 3$, $|U(R)| = 1$, $\mathrm{char}(R) = 2$ *and for each pair* $(a, b) \in R$ *the equality* $a^2 + b^2 + ab + 1 = 0$ *implies* $(a, b) = (1, 1)$ *or* $(a, b) = (1, 0)$ *or* $(a, b) = (0, 1)$;

(2.3) $|G| = |R| = 2$.

*Proof.* Foremost, we clearly observe that $V(RG) = 1$ if and only if $G = 1$. Assume now that $G \neq 1$. If there is $e \in R$ so that $e^2 = e$ and $e \neq \{0, 1\}$, we construct the element $u_e = 1 + e(g - 1) = 1 - e + eg$ where $1 \neq g \in G$. Apparently, $u_e^{-1} = 1 - e + eg^{-1}$ exists and $u_e \in V(RG)$ but $u_e \notin G$. So, $R$ must be indecomposable provided that $V(RG) = G$. Note that in [9] it was considered the normed unit $e + (1 - e)g$ to show that $R$ has to be indecomposable.

Let us now there exists $0 \neq r \in R$ such that $r^k = 0$ for some natural $k$. We choose the element $v_r = 1 - rg$ where $1 \neq g \in G$. Since $1 - (rg)^k = 1$, one can decompose

$$(1 - rg)(1 + rg + r^2g^2 + \cdots + r^{k-1}g^{k-1}) = 1\,.$$

Hence $1-rg$ is a unit in $RG$ different from $r'g'$ for any $r' \in U(R)$ and $g' \in G$. In fact, assume the contrary that $1 - rg = r'g'$. Hence, $1 = rg + r'g'$. Thus $r = 0$ or $r = 1$ if $g \neq g'$ whereas $r + r' = 1$ if $g = g'$. Then $1 - rg = (1 - r)g = g - rg$ implies that $g = 1$. But all of these variants are impossible and that is why $R$ must be reduced as well provided $V(RG) = G$.

Proof of "$\Rightarrow$" in *semi-simple case*. Let now $V(RG) = G$ with $\mathrm{supp}(G) \cap \mathrm{inv}(R) \neq \emptyset$, whence $G_t \neq 1$. Suppose for a moment, in a way of contradiction, $|G| \geq \aleph_0$, hence $G$ must be mixed or infinite torsion. Choose $C \leq G_t$ with $|C| < \aleph_0$ so that $\mathrm{supp}(C) \cap \mathrm{inv}(R) \neq \emptyset$. Clearly, such a choice is possible because otherwise $\mathrm{supp}(G) \cap \mathrm{inv}(R) = \emptyset$ which is a contradiction with our initial assumption. Since there is $\{0, 1\} \neq e \in RC$ so that $e^2 = e$ (e.g. cf. [1] or [11]), one can construct the element $u_e = 1 + e(g - 1)$ where $g \in G \setminus C$. It is readily seen that $eg \neq e$ and that $u_e \notin G$ because $u_e$ is written in canonical form. Moreover, it is easily checked that $u_e^{-1} = 1 + e(g^{-1} - 1)$ exists and hence $u_e \in V(RG)$ secures $V(RG) > G$ which is the wanted contradiction. Thus, we conclude that this implies $|G| < \aleph_0$, whence $G = G_t$. We claim that $|G|$ is of prime order, say $p$. In fact, once again we assume in a way

of contradiction that there exists a proper subgroup $P < G$, hence one may choose $g \in G \setminus P$. Furthermore, we repeat the same procedure as above demonstrated. Indeed, since $P$ can be chosen so that $\mathrm{supp}(P) \cap \mathrm{inv}(R) \neq \emptyset$, we construct $u_g = 1 + e(g-1)$, where $\{0,1\} \neq e^2 = e \in RP$. It is apparent that $eg \neq e$, whence $u_g$ is written canonically. It is obvious that $u_g \notin G$ and a simple technical exercise to verify that $u_g^{-1} = u_{g^{-1}}$ exists in an explicit form. Thus $u_g \in V(RG) \setminus G$, which is against our assumption $V(RG) = G$. Finally, we infer that $G$ does not possess proper subgroups, as claimed. Thus, owing to the listed above formula from Mollov-Nachev's theorem, we conclude that either

$$V(RG) \cong \times_{p-1} U(R)$$

when $\zeta_p \in R$ since simple calculations lead us to $a(p) = p-1$ bearing in mind that $(R[\zeta_p] : R) = 1$ or

$$V(RG) \cong U(R[\zeta_p])$$

when $\zeta_p \notin R$ since plain computations lead us to $a(p) = 1$ taking into account that $(R[\zeta_p] : R) = p-1$. In fact, we know from module theory that $(R[\zeta_p] : R)$ divides $p-1$, whence $(R[\zeta_p] : R) \leq p-1$. If we assume that $(R[\zeta_p] : R) < p-1$, we obtain in virtue of the above Mollov-Nachev's theorem that $V(RG) \cong \times_{a(p)} U(R[\zeta_p])$ where $a(p) \geq 2$. Because $U(R[\zeta_p])$ has at least $p$ totally different units, that are $1, \zeta_p, \ldots, \zeta_p^{p-1}$, we observe by this isomorphism formula that $V(RG)$ has at least $p^2$ totally different units which contradicts our assumption that $V(RG) = G$. Thus $(R[\zeta_p] : R) = p-1$ holds, indeed. (Note that the same reasoning was applied but not in an explicit form in [3, p. 145, Case 2]. There, under the requirement that $V(FG) = G$, the polynomial $1 + x + \cdots + x^{q-1}$ was irreducible over the finite field $F$ of non-zero characteristic $p \neq q$, where $q = |G|$.)

That is why, in the first case, $|V(RG)| = |U(R)|^{p-1}$ and consequently $V(RG) = G$ being equivalent to $|V(RG)| = |G|$ is possible only when $p = |U(R)|^{p-1}$. This diophantine equation has unique solutions $p = |U(R)| = 2$.

As for the second case, one can illustrate the following trick. Note that our approach used here is totally different from this in [3] because the concrete estimation of $|U(R[\zeta_p])|$ in the case when $R$ is not a field is difficult. And so, since $\zeta_p \notin R$, we derive that $p \geq 3$; otherwise if $p = 2$ we observe that $\zeta_2 = \pm 1 \in R$ which is impossible. Moreover, if we assume that $-1 \neq 1$, we observe that ${\zeta_p}^s \neq -1$ whenever $0 \leq s \leq p-1$. This is so because $p$ is odd. Consequently, there are $p+1$ different units in $U(R[\zeta_p])$, namely $-1, 1, \zeta_p, \ldots, {\zeta_p}^{p-1}$, and thus $V(RG) \neq G$. That is why, $V(RG) = G$ yields that $-1 = 1$ whence $\mathrm{char}(R) = 2$. Therefore, $L = \{0,1\}$ is a subfield of $R$ and

$V(RG) = G$ obviously forces that $V(LG) = G$. Furthermore, [3] applies to show that $|G| = 3$. Notice also that $p \cdot 1_R = 1_R \in U(R)$, i.e., $p \in \text{inv}(R)$, since $(2, p) = 1$ and $p = 2k+1$ where $k \geq 1$. Henceforth, we wish apply Proposition to infer the validity of this point.

Proof of "$\Leftarrow$" in *semi-simple case*. That conditions (2.1) and (2.2) will imply $V(RG) = G$ follows either by the previously listed isomorphism description of $V(RG)$ or by Proposition.

*Modular case.* Finally, let $\text{char}(R)$ divides the orders of elements in $G_t$. For instance, let $\text{char}(R) = q$ whence $G_q \neq 1$ while $G_p = 1$ for each other prime $p \neq q$. By considering the element $1 + r(1 - g)$, where $r \in R$ and $g \in G_q$, we infer that $V(RG) = G$ is true when and only when $r = \{0, 1\}$, hence $\text{char}(R) = 2$ with $|R| = 2$, and $|G| = 2$. ∎

*Remark.* First of all, we note that in condition (2.1) we must have $\text{char}(R) = 3$ since $2 \cdot 1_R \in U(R) = \{1, -1\}$ and thus $2 = -1$, that is, $3 = 0$.

Second, an interesting example of a ring $R$ of characteristic 0 for which $\text{supp}(G) \cap \text{inv}(R) \neq \emptyset$, i.e., whose satisfies the condition from Theorem, is $R = \mathbb{Z}[\frac{1}{p}]$, where $G_p \neq 1$.

It is also noteworthy that $V(RG)$ being only with trivial units implies that $R$ is indecomposable and reduced, even in the case where $G$ is not commutative. One only needs to observe that the above two constructions of nontrivial units in these different situations do not make use of commutativity of $G$, but only the fact that $R$ commutes with $G$ in $RG$.

As a major consequence of Main Theorem we deduce the following.

COROLLARY. *Let $G$ be an abelian group and $R$ a commutative unitary ring of prime characteristic $p$. Then $V(RG) = G$ if and only if $R$ is indecomposable and reduced and at most one of the following conditions holds:*

(a) $G_t = 1$;

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

(c) $|G| = 3, |U(R)| = 1$ *and for each pair* $(a, b) \in R$ *the equality* $a^2 + b^2 + ab + 1 = 0$ *possesses only trivial solutions in* $R$;

(d) $|G| = |R| = 2$.

*Proof.* That $R$ has to be without idempotents and nilpotents follows as given above.

Condition (a) was done in [9].

Let us now for a moment $G$ is infinite with $G_t \neq 1$. We claim that $\mathrm{supp}(G) \cap \mathrm{inv}(R) = \emptyset$. In fact, assume the converse, i.e., that the intersection is non-empty. By what we have demonstrated in the corresponding part of Main Theorem, we obtain that this contradicts $V(RG) = G$, thus substantiating our claim. Since $\mathrm{inv}(R)$ contains all primes but $p$, we derive that $G_t = G_p$. Furthermore, we appeal to [8] (see also [10]) to infer that $V(RG) = GV_p(RG)$. Thus, $V(RG) = G$ is obviously equivalent to $V_p(RG) = G_p$. By considering the elements $1 + g - gg_p$ where $1 \neq g \in G \setminus G_p$ and $1 \neq g_p \in G_p$ when $G \neq G_p$, and $1 + g - h$ where $g, h \in G \setminus \{1\}$ with $g \neq h$ when $G = G_p$, we deduce that our assumption that $G$ is infinite is impossible. That is why, $G$ must be of necessity finite, hence $G = G_t$. As showed in the corresponding part of Main Theorem, we may conclude that $G$ is cyclic of prime order $q \neq p$ when $G_q \neq 1$ for some prime $q$, because $\mathrm{inv}(R)$ contains all primes but $p$ and, therefore, $\mathrm{supp}(G) \cap \mathrm{inv}(R) \neq \emptyset$ guarantees the existence of nontrivial idempotents in $RG$. Henceforth, the method described in the proof of Main Theorem works to derive that (b) and (c) hold. Note that in (c) it follows that $\mathrm{char}(R) = 2$, i.e., $p = 2$ since otherwise $p \geq 3$ will force that $2 \in \mathrm{inv}(R)$, that is, $2 \cdot 1_R \in U(R) = 1_R$ and hence $1 = 0$ which is wrong.

As for (d), if $G = G_p$ is finite, it is readily checked that $|R| = |G| = 2$ is the only possible situation. ∎

We are now able to extend the last consequence to the following

THEOREM. *Suppose that $G$ is an abelian group and $R$ is a commutative unitary ring of finite characteristic more than 1. Then $V(RG) = G$ if and only if $R$ is indecomposable and reduced and precisely one of the conditions holds:*

(a') $G_t = 1$;

(b') $|G| = 2$ *and for each pair* $(a, b) \in R$ *the relation* $a^2 - b^2 \in U(R)$ *implies* $(a, b) = (1, 0)$ *or* $(a, b) = (0, 1)$;

(c') $|G| = 3$ *and for each pair* $(a, b) \in R$ *the relation* $3(a^2+b^2+ab-a-b)+1 \in U(R)$ *implies* $(a, b) = (0, 0)$ *or* $(a, b) = (1, 0)$ *or* $(a, b) = (0, 1)$;

(d') $|G| = |R| = 2$.

*Proof.* As previously demonstrated $R$ does not have idempotents and nilpotents. The case when $G$ is torsion-free was handled in [9]. Let us now we assume incidentally that $G$ is infinite with non-identity $G_t$. Since $\mathrm{char}(R)$ is finite, there exists a natural $n$ with the property $nR = 0$. Therefore, there is

a subring $P \leq R$, containing the same identity, so that $\mathrm{char}(P)$ is a prime; specifically $P$ is of the form $mR$ for some positive integer $m$ that depends on $n$. Furthermore, $V(RG) = G$ forces at once that $V(PG) = G$ which, as we have seen in the proof of Corollary, is impossible. That is why, $G$ has to be finite. Hereafter, we wish apply [6, Proposition 1, Proposition 3 and Proposition 8] by replacing in Proposition 3 elements $a \to a - 1$ and $b \to -b$ to deduce that points (a')–(d') are true. ∎

Comments. Here we shall give some more detailed explanations for the validity of the equality $(R[\zeta_p] : R) = p - 1$ outside the equality $V(RG) = G$. Indeed, let me denote the finite field with $m$ elements ($m$ a prime power) by $F(m)$ and let $z$ be a primitive $p$-th root of unity for whatever prime $p$ is being discussed above ($p$ not dividing $m$). Galois theory tells us that the degree $(F(m)(z) : F(m))$ of $F(m)(z)$ over $F(m)$ divides $p - 1$. Our question is: if $z$ is not in $F(m)$, when will it be true that the degree is precisely $p - 1$?

For $p = 2$, the question does not arise since $z$ lies in $F(m)$.

For $p = 3$, it is always true. The degree must be greater than 1 but less than 3. We emphasize that this is actually the case in our Main Theorem. Notice also the well-known classical fact that the polynomial $1 + x + x^2$ is irreducible over the field $\mathbb{Z}/2\mathbb{Z}$.

For $p = 5$, we get various behaviors depending on $m$. For example, for $F(2)$ the degree must be 4 since $F(16)$ is the lowest degree extension of $F(2)$ whose multiplicative group (cyclic of order 15) has order divisible by 5. On the other hand, the reader can verify that 19 is the first prime $q$ such that we get a false result for $F(q)$ since $F(361)$ has a multiplicative group of order divisible by 5 and is the smallest prime $q$ such that $q - 1$ is not divisible by 5 and $q^2 - 1$ is divisible by 5; thus the degree is 2.

In general, for a prime $p$, if we want degree $p - 1$ over $F(m)$, then $p$ should not divide $m^d - 1$ for any divisor $d$ of $p - 1$ smaller than $p - 1$.

For $R$ an indecomposable reduced ring of characteristic $q$, $R$ will contain a maximal algebraic extension field $F$ of $F(q)$. The question for $R$ would then be the same as for $F$. It depends on how much of $F(q)(z)$ lies in $F$.

Note that by results on primes in arithmetic sequences, for a fixed prime $p$ no smaller than 5, there will be infinitely many primes $q$ for which the degree over $F(q)$ is $p - 1$ and infinitely many for which it is smaller.

In characteristic 0, it depends on how much of the cyclotomic field $\mathbb{Q}(z)$ is contained in the field under consideration.

We would like to mention also that each finite commutative ring with identity and without nontrivial nilpotent and idempotent elements is a field. Indeed, by the classical structure theorem for Artinian rings, any finite commutative ring $R$ is a direct product of finitely many local rings. Because $R$ has no nontrivial idempotents, there is only one factor, i.e., $R$ must be local, say with unique maximal ideal $M$. As finite commutative rings are zero-dimensional, $M$ must be the only prime ideal of $R$, and so since $R$ has no nonzero nilpotent elements $M$ has to be 0. Since 0 is a maximal ideal of $R$, any such $R$ is, in fact, a field. Another confirmation of the last fact may be like this: Since $R$ is Artinian with zero nil-radical, it is semi-simple. Then it must be a direct product of fields. But it is indecomposable, hence it is a field, indeed. Thus, even more, every Artinian commutative unitary ring with no idempotents and nilpotents has to be a field.

Now, if we assume for a moment in our theorem that $R$ is Artinian (in particular finite), since it is of necessity without nontrivial idempotents and nilpotents, according to the statements alluded to above, we deduce that $R$ must be a field. Henceforth, the method in [3] works successfully to obtain $|R| = 2$ provided that $\mathrm{char}(R) = 2$.

Let $\mathrm{id}(R)$ designate the set of all idempotents in $R$, that is $\mathrm{id}(R) = \{e \in R : e^2 = e\}$. It is easily seen that $\mathrm{id}(R)$ is a ring, so that $\mathrm{id}(R) \leq R$, provided $\mathrm{char}(R) = 2$. Certainly, $|\,\mathrm{id}(R)| = 2$ whenever $R$ is indecomposable.

It is noteworthy that the equation $a^2 + b^2 + ab + 1 = 0$ perhaps possesses nontrivial solutions in $R$ (i.e., solutions different from $(1,1), (1,0)$ and $(0,1)$) even when $\mathrm{char}(R) = 2, U(R) = 1$ and $\mathrm{id}(R) = \{0,1\}$. The following example gives a recent progress in this (compare with the concluding discussion in [6]). Let $G$ be of order 3 and $\mathrm{char}(R) = 2$. If $RG$ has only trivial solutions of this equation, and $a$ is an element of $R$ other than 0 or 1, then one can see from our conditions that $a$ cannot be either an idempotent or a unit, and that $a$ cannot be algebraic over the field of two elements $\mathbb{F}_2$ (because then $R$ would contain a proper field extension of $\mathbb{F}_2$ and hence a nontrivial unit), nor can $a$ be nilpotent over $\mathbb{F}_2$ (because this would imply the existence of a nontrivial idempotent). So this should force $\mathbb{F}_2[a]$ to be isomorphic to the polynomial ring. Now, if we let $b$ be a new variable that commutes with $a$ and we form the ring $R' = \mathbb{F}_2[a,b]/(a^2 + b^2 + ab + 1)$, then $R'G$ has nontrivial units. So, an interesting example would be any ring $R$ for which $\mathbb{F}_2[a] < R < P \cong R'$. Furthermore, any commutative unitary ring $S$ for which $SG$ has nontrivial units should contain a subring which is isomorphic to a homomorphic image

of $R'$ in which $a$ and $b$ do not vanish. So it will be helpful to know whether $R'$ has nontrivial units, idempotents, or nilpotent elements.

We also emphasize that the conditions on $R$ listed in Proposition assure the lack of nontrivial idempotents in $R$.

A question of ring-theoretical interest is to describe the structure of those rings whose unit groups are given in the statement of Main Theorem and its two corollaries. However, this concrete exhibition is the theme of some other research work.

We close with a discussion concerning certain homomorphisms. Consider the natural map $\phi : R \to R/I$ where $I \lhd R$. It can be linearly extended to a group ring surjective homomorphism (= epimorphism) $\Phi : RG \to (R/I)G$ with kernel $IG$. This induces the group homomorphisms $\Phi : V(RG) \to V((R/I)G)$ and $\Phi : V_p(RG) \to V_p((R/I)G)$ which are the identity on $G$. Notice that the latter one is an epimorphism for an arbitrary (maximal) ideal $I$; besides the first one is also an epimorphism when $I$ is a nil-ideal; for example $I = N(R)$. Consequently, in that case, $V(RG) = G$ assures that $V((R/N(R))G) = G$ since $\Phi(G) = G$. However, there is no a real advantage in this, although $R/N(R)$ is without nilpotent elements.

Correction. Although it is clear from the context, we would like to specify that in [2, Lemma 4] the integral domain $R$ is of non-zero, whence prime, characteristic.

In closing, we state (see [5], [6] and [14] as well)

Problem. Describe when $V(RG) = G$ provided that $\operatorname{supp}(G) \cap \operatorname{inv}(R) = \emptyset$ or, in particular, $\operatorname{inv}(R) = \emptyset$. (For instance $R = \mathbb{Z}$ is such a ring, and the question was already settled in [7] and [10], respectively.) According to the results of this article, the only outstanding case would be when $\operatorname{char}(R) = 0$, $G_t \neq 1$ and $\operatorname{supp}(G) \cap \operatorname{inv}(R) = \emptyset$.

Acknowledgements

The author would like to thank Professors Allen Herman and David Dobbs for valuable communications. The author also expresses his sincere thanks to the anonymous expert referees for their numerous suggestions leading to an improvement of the present manuscript.

## References


[1] D.B. Coleman, Idempotents in group rings, *Proc. Amer. Math. Soc.* **17** (4) (1966), 962.

[2] P.V. Danchev, Warfield invariants in abelian group rings, *Extracta Math.* **20** (3) (2005), 233 – 241.

[3] P.V. Danchev, On the trivial units in finite commutative group rings, *Math. Commun.* **10** (2) (2005), 143 – 147.

[4] P.V. Danchev, A note on trivial units in abelian group rings, *An. Univ. Bucureşti Mat.* **54** (2) (2005), 229 – 234.

[5] A. Herman, Y. Li, Trivial units for group rings over rings of algebraic integers, *Proc. Amer. Math. Soc.* **134** (3) (2006), 631 – 635.

[6] A. Herman, Y. Li, M.M. Parmenter, Trivial units for group rings with $G$-adapted coefficient rings, *Canad. Math. Bull.* **48** (1) (2005), 80 – 89.

[7] G. Higman, The units of group rings, *Proc. Lond. Math. Soc.* **46** (1940), 231 – 248.

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

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

[10] G. Karpilovsky, "Unit Groups of Group Rings", Longman Scientific & Technical, Harlow, 1989.

[11] W.L. May, Group algebras over finitely generated rings, *J. Algebra* **39** (1976), 483 – 511.

[12] T.Zh. Mollov, N.A. Nachev, Unit groups of commutative group rings, *Compt. Rend. Acad. Bulg. Sci.* **57** (5) (2004), 9 – 12.

[13] D.S. Passman, "The Algebraic Structure of Group Rings", Wiley – Interscience, New York-London-Sydney, 1977.

[14] J. Ritter, S.K. Sehgal, Trivial units in $RG$, *Math. Proc. R. Ir. Acad.* **105** (1) (2005), 25 – 39.

[15] S.K. Sehgal, "Topics in Group Rings", Marcel Dekker, Inc., New York, 1978.

[16] W.D. Ullery, On isomorphism of group algebras of torsion abelian groups, *Rocky Mountain J. Math.* **22** (3) (1992), 1111 – 1122.