Ann. Sci. Math. Québec **33** (2009), no 1, 83–92

GROUP OF NORMALIZED UNITS OF COMMUTATIVE MODULAR GROUP RINGS

TODOR ZH. MOLLOV AND NAKO A. NACHEV

RÉSUMÉ. Soit R un anneau commutatif avec identité de caractéristique p, avec p un nombre premier, et soit G un groupe abélien. Soit $V(RG)$ le groupe des unités normalisées de l'anneau de groupe RG, *i.e.* les unités d'augmentation 1, et soit $S(RG)$ le p-sous-groupe de Sylow du groupe $V(RG)$, *i.e.* la p-composante du groupe $V(RG)$. Dans le présent article, nous donnons quatre conditions et nous démontrons que $V(RG) = GS(RG)$ si et seulement si l'une de ces conditions est satisfaite.

ABSTRACT. Let R be a commutative ring with identity of prime characteristic p and let G be an abelian group. Let $V(RG)$ be the group of normalized units of the group ring RG, *i.e.*, the units of augmentation 1, and let $S(RG)$ be the Sylow p-subgroup of the group $V(RG)$, *i.e.*, the p-component of the group $V(RG)$. In the present paper, we give four conditions and prove that $V(RG) = GS(RG)$ if and only if any one of them is fulfilled.

1. Introduction

Let RG be the group ring of an abelian group G over a commutative ring R with identity of prime characteristic p and let $S(RG)$ be the p-component of the group $V(RG)$ of normalized units of RG. The investigation of the group $S(RG)$ has begun in 1967 with the fundamental papers of Berman [1, 2] in which a complete description of $S(RG)$ (up to isomorphism) was given, when G is a countable abelian p-group and R is a countable perfect field. Further, in 1977 and 1981, Mollov [8, 9] has calculated the Ulm-Kaplansky invariants $f_\alpha(S)$ of the group $S(RG)$ when G is an arbitrary abelian group and R is a field. In 1988, it was proved by May [7] that if G is an abelian p-group and R is a perfect field of prime characteristic p, then $S(RG)$ is simply presented if and only if G is simply presented. Hence, when G is a totally projective abelian p-group and the field R is perfect, the above mentioned Ulm-Kaplansky invariants $f_\alpha(S)$ give a full system of invariants of the group $S(RG)$. Besides, when the ring R is arbitrary, Mollov and Nachev [10] have calculated in 1980 the invariants $f_\alpha(S)$ under the restriction that G is an abelian p-group, and Nachev [12] has calculated in 1995 the invariants $f_\alpha(S)$ without restrictions on the group G and the ring R.

When $G = G_p$, the equality $V(RG) = S(RG)$ holds, while when $G \neq G_p$ the investigation of the group $V(RG)$ is difficult and a full description of $V(RG)$ has not been obtained until now. In this latter situation, a very important problem is the

Reçu le 10 octobre 2008 et, sous forme définitive, le 26 janvier 2009.

following: find necessary and sufficient conditions under which $V(RG) = GS(RG)$. In 2005, Danchev [3, Proposition 5] has provided a partial answer to this question when the ring R has no zero divisors and the group G contains an element of infinite order, and in 2006 Mollov and Nachev [11] have given an answer to this question when the ring R is arbitrary and the torsion subgroup tG of G coincides with G_p. In Theorem 1 of [4] Danchev gives necessary and suffcient conditions for the equality $V(RG) = GS(RG)$ to hold for an arbitrary ring R of prime characteristic p and a group G, but there are imperfections in the proof. In the present paper (see Theorem 4), we provide a transparent complete proof using a more direct approach.

2. Main result

Denote by G_p the p-component of G and by R_p^* the p-component of the unit group R^* of the ring R. Let tG be the torsion subgroup of the group G and let $\langle g\rangle$ be the cyclic subgroup of G generated by $g \in G$.

For our first preliminary result we also denote by (m, n) the greatest common divisor of m and n, for $m, n \in \mathbb{N}$. We shall multiplicatively write the abelian groups. The abelian group terminology is in agreement with Fuchs [5, 6].

Lemma 1. *Let R be a commutative ring with identity and $A = \langle a\rangle$ be a cyclic group of order q such that $(q, 6) = 1$. Then the element $x = 1 - a + a^2 \in V(RA)$, i.e., x is a normalized invertible element in the group ring RA.*

Proof. Let k be the least positive solution of the congruence $6k \equiv 1 \pmod q$. It is easy to see that

$$(a^{3n-2} + a^{3n-1})x = a^{3n-2} + a^{3n+1} \tag{1}$$

for $n = 1, 2, \ldots, 2k$. Multiplying the equalities of (1) with an even n by -1 and adding all equalities of (1) we obtain

$$yx = a - a^{6k+1} = a - a^2 = 1 - x,$$

where y is a polynomial of a with integral coefficients. Thus, $y \in RA$ and $x(y+1) = 1$, i.e., x is an invertible element of RA. □

Lemma 2. *Let R be a commutative ring with identity of prime characteristic p and A be a torsion abelian group. If $A_p = 1$ and $V(RA) = A$, then A is a cyclic group either of order 2 or of order 3.*

Proof. Suppose that there is a non-trivial finite subgroup F of A which is different from A. Since $(|F|, p) = 1$ and $\mathrm{char}R = p$, where $|F|$ is the cardinality of F, $|F|$ is an invertible element in R. Consequently, there are idempotents

$$e_1 = \frac{1}{|F|}\sum_{f\in F} f \quad \text{and} \quad e_2 = 1 - e_1.$$

Let $a \in A\backslash F$. We form the element $x = ae_1 + e_2$. Obviously, x is an invertible element and its inverse is $a^{-1}e_1 + e_2$. Thus, $x \in V(RF) \subseteq V(RA) = A$, i.e., $x \in A$. This is a contradiction since $e_1 \neq 0$ and $e_1 \neq 1$. Therefore, A is a cyclic group and the order of A is a prime number q.

We shall prove that either $q = 2$ or $q = 3$. If we suppose that $q \geq 5$, then $(q, 6) = 1$ and, by Lemma 1, the element $x = (1 - a + a^2) \in V(RA) = A$, where $a \in A$. This is a contradiction. Consequently, either $q = 2$ or $q = 3$, *i.e.*, A is a cyclic group either of order 2 or of order 3. $\square$

We recall some well-known definitions. A ring R is called *indecomposable* if it cannot be decomposed into a direct sum of two or more non-trivial ideals of R, or equivalently, if R does not have non-trivial idempotents (*i.e.*, different from 0 and 1).

Let R be a commutative ring with identity of characteristic 2 and let $N(R)$ be the nilradical of R. Further we shall consider the equation

$$X^2 + XY + Y^2 = 1 + N(R) \tag{2}$$

in the quotient ring $R/N(R)$. Clearly, equation (2) has three solutions in $R/N(R)$, namely $(\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})$, where $\overline{\lambda} = \lambda + N(R)$, with $\lambda \in R$. We call these solutions *trivial*.

Lemma 3. *If R is a commutative ring with identity of characteristic 2 and equation (2) has only the trivial solutions in $R/N(R)$, then R is an indecomposable ring.*

Proof. Suppose that $R = I \oplus J$ is a direct sum of non-trivial ideals I and J and $1 = e_1 + e_2$, where $e_1 \in I$ and $e_2 \in J$. Obviously, equation (2) has a solution $(e_1 + N(R), e_2 + N(R))$, which is different from the trivial solutions. Namely, if we suppose that either $e_1 + N(R) = 1 + N(R)$ or $e_1 + N(R) = N(R)$, then we obtain that e_1 is either invertible or nilpotent. This is a contradiction. $\square$

Further, if

$$x = \sum_{i=1}^{n} \alpha_i g_i,$$

with $\alpha_i \in R$ and $g_i \in G$, then we let

$$n(x) = \sum_{i=1}^{n} \alpha_i.$$

We denote by Z_p the prime field of positive characteristic p.

In the next theorem we shall give necessary and sufficient conditions for the equality $V(RG) = GS(RG)$ to hold. This equality is very useful in the investigation of $V(RG)$. As we shall see, in this result the solutions of equation (2) in the quotient ring $R/N(R)$ will play an important role.

Theorem 4. *Let R be a commutative ring with identity of prime characteristic p and G be an abelian group. Then $V(RG) = GS(RG)$ if and only if at least one of the following conditions is fulfilled:*

(1) $G = G_p$;

(2) $G \neq G_p, tG = G_p$ *and the ring R is indecomposable;*

(3) $p = 3, R^* = \langle -1 \rangle \times R_3^*, G = A \times G_3, |A| = 2;$

(4) $p = 2, R^* = R_2^*, G = A \times G_2, |A| = 3$ *and equation* (2) *has only the trivial solutions in* $R/N(R)$.

Proof. (Necessity) Assume that $V(RG) = GS(RG)$. Obviously, either $G = G_p$ or $G \neq G_p$. Suppose first that $G \neq G_p$. We consider the following two subcases: $tG = G_p$ and $tG \neq G_p$.

(a) Let $tG = G_p$. We shall prove that R is an indecomposable ring. Suppose to the contrary that R is decomposable. Therefore, there are orthogonal idempotents e_1 and e_2 of R such that $e_1 + e_2 = 1$. We form the element $x = ge_1 + e_2$, with $g \in G \backslash G_p$. Since $x \in V(RG) = GS(RG)$, we have $x = g_1 s$, with $g_1 \in G$ and $s \in S(RG)$. Consequently, there is $k \in \mathbb{N}$, such that

$$g^{p^k} e_1 + e_2 = x^{p^k} = g_1^{p^k},$$

which is a contradiction, since $g^{p^k} e_1 + e_2$ is an element of RG in a canonical form and this element does not belong to G. Hence R is an indecomposable ring and the conditions of case (2) hold.

(b) Let $tG \neq G_p$.

(b1) We shall prove that $G = tG$ and

$$G = A \times G_p, \quad \text{where } A \neq 1. \tag{3}$$

Since $tG \neq G_p$ and $\mathrm{char} R = p$, there exists an element $a \in tG \backslash G_p$ whose order is $q \geq 2$, with $(q,p) = 1$, and idempotents

$$e_1 = (1/q)(1 + a + \cdots + a^{q-1}) \quad \text{and} \quad e_2 = 1 - e_1. \tag{4}$$

Suppose that $G \neq tG$. Let $g \in G$ be an element of infinite order. Then the element $x = ge_1 + e_2$ belongs to $V(RG) = GS(RG)$ and $x^{p^k} \in G$ for some $k \in \mathbb{N}$. This is a contradiction, since formula (4) for the idempotents e_1 and e_2 implies that x^{p^k} contains at least two non-zero summands in its canonical form. Therefore, $G = tG$ and equality (3) holds.

(b2) We shall prove that

$$R^* = \langle -1 \rangle \times R_p^*. \tag{5}$$

Suppose the contrary, and let $\lambda \in R^*$ be such that $\lambda \notin \langle -1 \rangle \times R_p^*$. We form the element $y = e_1 + \lambda e_2$ which belongs to $V(RG) = GS(RG)$. Consequently, $y = gs$ with $g \in G$ and $s \in S(RG)$. Since, by equality (3), $g = hg_p$, with $h \in A$ and $g_p \in G_p$, there exists $t \in \mathbb{N}$ such that

$$e_1 + \lambda^{p^t} e_2 = y^{p^t} = h^{p^t}.$$

Hence $y^{p^t} \in A$ and, by formula (4),

$$e_1 + \lambda^{p^t} e_2 = (1/q)[(1 + (q-1)\lambda^{p^t}) + (1 - \lambda^{p^t})a + \cdots + (1 - \lambda^{p^t})a^{q-1}], \tag{6}$$

where a and q are chosen as in case (b1). Since $\lambda^{p^t} \neq 1$, the summand $(1 - \lambda^{p^t})a$ in this equality is different from 0. If $q > 2$, then there is at least one non-zero summand in (6) after $(1 - \lambda^{p^t})a$ which is a contradiction, since the right-hand side of (6) is in a canonical form and belongs to A. Consequently, $q = 2$. Then the first summand in the right-hand side of (6) has the form $(1/2)(1 + \lambda^{p^t})$ and must be equal to 0, since the second summand $(1/2)(1-\lambda^{p^t})a$ is different from 0 . Hence $\lambda^{p^t} = -1$, which contradicts the choice of λ. Therefore, (5) holds.

(b3) We shall prove that the prime p can take only the values 2 or 3, *i.e.*, either $p = 2$ or $p = 3$. Suppose that $p \geq 5$. Since $Z_p{}^* \subseteq R^*$ and $|Z_p{}^*| = p-1$, there are elements in $Z_p{}^*$ which, by (5), do not belong to $\langle -1 \rangle \times R_p^* = R^*$. This contradicts (5). Consequently, either $p = 2$ or $p = 3$.

(b4) We shall prove that in equality (3) A is a cyclic group either of order 2 or of order 3. Namely, we consider $V(Z_pA) \leq V(RA) \leq V(RG) = GS(RG)$, *i.e.*, $V(Z_pA) \leq GS(RG)$. However, $V(Z_pA)$ does not contain p-elements. Therefore, $V(Z_pA) \subseteq G$ and $V(Z_pA) \bigcap G = A$, *i.e.*, $V(Z_pA) = A$. Then Lemma 2 implies that A is a cyclic group either of order 2 or of order 3 and, by case (b3), either $p = 2$ or $p = 3$. Consequently, by equality (3), if $p = 3$, then A is a cyclic group of order 2 and if $p = 2$, then A is a cyclic group of order 3. These results show that the conditions of case (3) and of case (4), eventually without the last condition of case (4), are fulfilled.

(b5) Let $p = 2$. We shall prove that the last condition of case (4) holds, *i.e.*, that equality (2) has only the trivial solutions in $R/N(R)$. Since $p = 2$, it follows from equality (3) that $G = A \times G_2$, with $|A| = 3$. Let $A = \langle a \rangle$ and let

$$(\overline{\lambda}, \overline{\mu}), \quad \text{with } \lambda, \mu \in R, \tag{7}$$

be a solution of equation (2) in $R/N(R)$. Substituting $\overline{\lambda}$ and $\overline{\mu}$ in equation (2) gives

$$\lambda^2 + \lambda\mu + \mu^2 = 1 + r, \tag{8}$$

where $r \in N(R)$. We consider the element

$$x = 1 + \mu + (1+\lambda)a + (1+\lambda+\mu)a^2. \tag{9}$$

Obviously, $n(x) = 1$. We shall prove that $x \in V(RG)$. Namely, we consider the element

$$y = 1 + \mu + (1+\lambda+\mu)a + (1+\lambda)a^2.$$

Then $xy = 1+ra+ra^2$, where, by (8), $r = \lambda^2+\lambda\mu+\mu^2+1$ and $r \in N(R)$. Thus, xy is an invertible element. Hence x is an invertible element and $x \in V(RG) = GS(RG)$. Consequently, we can represent x in the form $x = a^k h$, where $a \in A$, $h \in S(RG)$ and $x^{2^n} \in A$ for some $n \in \mathbb{N}$. Using (9) we get

$$x^{2^n} = 1 + \mu^{2^n} + (1+\lambda^{2^n})a^{2^n} + (1+\lambda^{2^n}+\mu^{2^n})a^{2^{n+1}}. \tag{10}$$

We note that $a^{2^n} = a$ if n is even and $a^{2^n} = a^2$ if n is odd. We consider the following cases:

(i) Suppose that $x^{2^n} = 1$. Then equality (10) implies that $\mu^{2^n} = 0$ and $\lambda^{2^n} = 1$, *i.e.*, $\mu \in N(R)$ and $\lambda \in (1+N(R)$. Therefore, solution (7), namely $(\overline{\lambda}, \overline{\mu})$, coincides with the trivial solution $(\overline{1}, \overline{0})$ of equation (2).

(ii) Suppose that $x^{2^n} = a$ or $x^{2^n} = a^2$. Then $\mu^{2^n} = 1$, *i.e.*, $\mu \in (1+N(R))$ and either $1+\lambda^{2^n} = 1$ or $\lambda^{2^n} = 1$, *i.e.*, either $\lambda \in N(R)$ or $\lambda \in (1+N(R))$. Consequently, solution (7), namely $(\overline{\lambda}, \overline{\mu})$, is a trivial solution of equation (2), *i.e.*, equation (2) has only the trivial solutions in $R/N(R)$.

This proves the necessity.

(Sufficiency) Suppose that the condition of case (1) holds. Then $G = G_p$ and consequently $V(RG) = S(RG) \subseteq GS(RG)$. Hence, $V(RG) = GS(RG)$.

If the condition of case (2) holds, then $G \neq G_p$, $tG = G_p$ and the ring R is indecomposable. Then, by Mollov and Nachev [11], $V(RG) = GS(RG)$.

If the condition of case (3) holds, let $A = \langle a \rangle$. We form the idempotents $e_1 = (1/2)(1+a)$ and $e_2 = (1/2)(1-a)$ of RG, *i.e.*, $e_1 = -1-a$ and $e_2 = -1+a$. Therefore, $ae_1 = e_1$ and $ae_2 = -e_2$. Then

$$RG = RGe_1 \oplus RGe_2 = RG_3e_1 \oplus RG_3e_2.$$

If $x \in V(RG)$, then $x = \lambda e_1 + \mu e_2$, where $\lambda, \mu \in RG_3$ are such that λ and μ are invertible elements. Consequently, $n(x) = n(\lambda) = 1$. Hence $\lambda \in S(RG_3)$. Since μ is an invertible element of RG_3, we have $n(\mu) \in R^* = \langle -1 \rangle \times R_3^*$, *i.e.*,

$$n(\mu) = \pm\alpha,$$

with $\alpha \in R_3^*$. On the one hand, if $n(\mu) = \alpha$, then $x \in S(RG) \subseteq GS(RG)$. On the other hand, if $n(\mu) = -\alpha$, then

$$x = \lambda e_1 + \mu e_2 = \lambda a e_1 - \mu a e_2 = a(\lambda e_1 - \mu e_2) \in GS(RG).$$

Then both cases imply $V(RG) \subseteq GS(RG)$, *i.e.*, $V(RG) = GS(RG)$.

Finally, assume that the condition of case (4) holds and let $A = \langle a \rangle$. We shall prove that $V(RG) = GS(RG)$. It is easy to see that the system

$$\{1, a, a^2, g-1, a(g-1), a^2(g-1) \mid g \in G_2 \backslash \{1\}\}$$

is a basis of the R-algebra RG. Hence, if $x \in V(RG)$, then x can be written as

$$x = x_0 + x_1,$$

where

$$\left\{ \begin{aligned} & x_0 = \alpha_0 + \alpha_1 a + \alpha_2 a^2, \quad \text{with } \alpha_i \in R, \\ & x_1 = \sum_{i=0}^{2} \sum_{g \in G_2 \backslash \{1\}} x_{a^i g} a^i (g-1), \quad \text{with } x_{a^i g} \in R. \end{aligned} \right. \tag{11}$$

Since x_1 is a nilpotent element, there is n such that $x^{2^n} = x_0^{2^n}$. Therefore, x_0 is an invertible element. In view of the fact that $n(x) = 1$ and $n(x_1) = 0$, we have $n(x_0) = 1$. Consequently, $x_0 \in V(RA)$. Then

$$x = x_0(1 + {x_0}^{-1}x_1),$$

where $(1 + {x_0}^{-1}x_1) \in S(RG)$.

We shall prove that $x_0 \in AS(RG)$. Hence it will follow that $x \in GS(RG)$, *i.e.*, $V(RG) = GS(RG)$. For this sake we let $\lambda = 1 + \alpha_1$ and $\mu = 1 + \alpha_0$, *i.e.*, $\alpha_0 = 1 + \mu, \alpha_1 = 1 + \lambda$. Since $\alpha_0 + \alpha_1 + \alpha_2 = 1$, we have $\alpha_2 = 1 + \lambda + \mu$. If we substitute α_0, α_1 and α_2 in equality (11) we get

$$x_0 = 1 + \mu + (1+\lambda)a + (1+\lambda+\mu)a^2. \tag{12}$$

We form the idempotents $e_1 = 1 + a + a^2$ and $e_2 = a + a^2$. Therefore,

$$a^2 e_2 + a e_2 = e_2. \tag{13}$$

It is easy to see, using (11), that $x_0 = e_1 + (\lambda + \mu a)e_2$. Consequently, $(\lambda + \mu a)e_2$ is an invertible element in RAe_2. Since the map $a \to a^2$ is an automorphism of the group A, the extension of this map gives an automorphism of RAe_2. Therefore, $\lambda e_2 + \mu a^2 e_2$ is an invertible element of RAe_2. Hence the product

$$(\lambda e_2 + \mu a e_2)(\lambda e_2 + \mu a^2 e_2) = (\lambda^2 + \lambda\mu + \mu^2)e_2$$

is an invertible element of Re_2, where, to obtain of this equality, we used equality (13). Hence $(\lambda^2 + \lambda\mu + \mu^2) \in R^* = R_2^* = \{1\} + N(R)$. This equality implies that $\overline{\lambda}^2 + \overline{\lambda}\overline{\mu} + \overline{\mu}^2 = \overline{1}$, *i.e.*, $(\overline{\lambda}, \overline{\mu})$ is a solution of equation (2). Consequently, $(\overline{\lambda}, \overline{\mu})$ is a trivial solution of equation (2), *i.e.*, one of the following conditions holds:

(i) $\overline{\lambda} = \overline{1}$ and $\overline{\mu} = \overline{0}$,

(ii) $\overline{\lambda} = \overline{0}$ and $\overline{\mu} = \overline{1}$,

(iii) $\overline{\lambda} = \overline{1}$ and $\overline{\mu} = \overline{1}$.

Now, in case (i), we have $\lambda = 1 + r_1$ and $\mu = r_2$, with $r_1, r_2 \in N(R)$, and (12) implies that $x_0 = 1 + r_2 + r_1 a + (r_1 + r_2)a^2$. Hence $x_0 \in S(RA) \subseteq AS(RG)$. In case (ii), we have $\lambda = r_1$ and $\mu = 1 + r_2$, with $r_1, r_2 \in N(R)$, and equality (12) implies that $x_0 = a[1 + r_1 + (r_1 + r_2)a + r_2 a^2]$. Hence $x_0 \in AS(RA)$. Finally, in the case (iii), we have $\lambda = 1 + r_1$ and $\mu = 1 + r_2$, with $r_1, r_2 \in N(R)$, and equality (12) implies that $x_0 = a^2(1 + r_1 + r_2 + r_2 a + r_1 a^2)$. Hence $x_0 \in AS(RA)$. The theorem is proved. □

In order to characterize the property $V(RG) = GS(RG)$, Danchev mentions in Theorem 1 of [4] the contradictory condition (2.2):

$$R = L + N(R), 1_R \in L \leq R, |L| = 2, G = G_p \times C, C \leq G, \text{ and } |C| = 2.$$

As a matter of fact, since L is a subring of R and $1_R \in L$, L contains the elements $0, 1_R, \ldots, (p-1)1_R$. Then $|L| = 2$ implies $p = 2$. Therefore, $G = G_2 \times C$ is a 2-group which contradicts the condition of case (2) $G \neq G_p$ in Theorem 1 of [4].

In the following proposition we prove that if case (3) of Theorem 4 holds, then the ring R is indecomposable.

Proposition 5. *If $p = 3$ and $R^* = \langle -1 \rangle \times R_3^*$, then the ring R is indecomposable.*

Proof. Assume that the ring R is decomposable. Therefore, there exist two non-trivial orthogonal idempotents e_1 and e_2 such that $e_1 + e_2 = 1$. Then $e_1 - e_2 \in \langle -1 \rangle$ since $(e_1 - e_2)^2 = e_1 + e_2 = 1$. There are two possible cases to consider:

(i) If $e_1 - e_2 = 1$, then $e_1 + e_2 = 1$ implies $2e_2 = 0$ which is a contradiction.

(ii) If $e_1 - e_2 = -1$, then $e_1 + e_2 = 1$ implies $2e_1 = 0$ which is also a contradiction.

Therefore, the ring R is indecomposable. □

Let $Z_2[x]$ be a polynomial ring of x with coefficients from Z_2 and let $(f(x), g(x))$ be the greatest common divisor of $f(x)$ and $g(x)$ in $Z_2[x]$. In connection with the condition of case (4) of Theorem 4 and Lemma 3 we give an example, formulated as a proposition, which shows that there is an indecomposable ring R, of characteristic 2, satisfying $R^* = R_2^*$ and such that equation (2) has a non-trivial solution in $R/N(R)$. Consequently, the condition in case (4) of Theorem 4 for the solutions of equation (2) is essential. Besides, for this ring R of characteristic 2 the converse of Lemma 3 is not true.

Proposition 6. *Let $A = Z_2[x]$ and y be a root of the equation*

$$y^2 + xy + (x^2 + 1) = 0. \tag{14}$$

Then $R = A[y]$ is an indecomposable ring of characteristic 2, $R^* = R_2^*$ and equation (2) *has more than three solutions in $R/N(R)$.*

Proof. Obviously, A and R are rings of characteristic 2 and $A^* = 1$. It is not hard to see that the left-hand side of equation (14) is an indecomposable polynomial over $A = Z_2[x]$, and the A-algebra $R = A[y]$ has $\{1, y\}$ as an A-basis. We divide the proof in several steps.

(a) We shall prove that $N(R) = 0$. Suppose the contrary. Then there exists an element $v \in N(R)$, with $v \neq 0$, such that $v^2 = 0$. The element v has the form $v = a(x) + b(x)y$, with $a(x), b(x) \in Z_2[x]$. The equality

$$v^2 = a^2(x) + b^2(x)y^2 = a^2(x) + b^2(x)(xy + x^2 + 1) = 0$$

implies that $b^2(x)x = 0$ and, since the ring $Z_2[x]$ does not have zero divisors, we have $b^2(x) = 0$. Therefore, $b(x) = 0$ and $a(x) = 0$. Consequently, $v = a(x) + b(x)y = 0$ which is a contradiction. Therefore $N(R) = 0$.

(b) Equation (2) has a solution $X = x$ and $Y = y$, where $x, y \in R = A[y]$, *i.e.*, equation (2) has a non-trivial solution in $R/N(R)$.

(c) Now we shall prove that $R^* = 1 = R_2^*$ by the using $N(R) = 0$. Suppose to the contrary that there exists $(a(x) + b(x)y) \in R^*$, with $a(x), b(x) \in Z_2[x]$, such that $a(x) + b(x)y \neq 1$, *i.e.*, the following condition holds:

$$\text{either } a(x) \neq 1 \text{ or } b(x) \neq 0. \tag{$*$}$$

Then there exists $(a_1(x) + b_1(x)y) \in R^*$, with $a_1(x), b_1(x) \in Z_2[x]$, such that

$$(a(x) + b(x)y)(a_1(x) + b_1(x)y) = 1, \tag{15}$$

i.e.,

$$a(x)a_1(x) + (a(x)b_1(x) + a_1(x)b(x))y + b(x)b_1(x)(x^2 + xy + 1) = 1.$$

Since $\{1, y\}$ is a basis of $R = A[y]$,

$$\begin{cases} a(x)a_1(x) + (x^2 + 1)b(x)b_1(x) = 1, \\ a(x)b_1(x) + a_1(x)b(x) + b(x)b_1(x)x = 0. \end{cases} \tag{16}$$

If $b(x) = 0$, then (16) implies that $a(x) = a_1(x) = 1$, which contradicts the condition $(*)$. If $b_1(x) = 0$, then again (16) implies that $a(x) = a_1(x) = 1$ and from the second equation of (16) we get $b(x) = 0$, which, together with $a(x) = 1$, contradicts the condition $(*)$. Consequently, $b(x) \neq 0$ and $b_1(x) \neq 0$. Now we write the second equation of (16) in the form

$$b(x)a_1(x) = (a(x) + b(x)x)b_1(x). \tag{17}$$

Since the greatest common divisor $(b(x), a(x) + b(x)x) = (b(x), a(x)) = 1$, where the second equality follows from (15), equation (17) implies that $b(x)$ divides $b_1(x)$. In an analogous manner, (15) implies that $(a_1(x), b_1(x)) = 1$. Therefore, we get from

(17) that $b_1(x)$ divides $b(x)$. Since $b_1(x)$ and $b(x)$ are monic polynomials, we have $b_1(x) = b(x)$. Hence $b_1(x) = b(x) \neq 0$ and (17) implies that $a_1(x) = a(x) + b(x)x$. We substitute $a_1(x)$ and $b_1(x)$ in the first equation of (16) with $a(x) + b(x)x$ and $b(x)$, respectively, and obtain

$$a^2(x) + a(x)b(x)x + (x^2 + 1)b^2(x) = 1. \tag{18}$$

If deg$(a(x)) = -\infty$, *i.e.*, $a(x) = 0$, then the left and the right-hand sides of (18) have degrees at least 2 and 0, respectively, which is a contradiction. If deg$(a(x)) = 0$, then $a(x) = 1$ and by comparing the degrees of the left and the right-hand sides of (18) we get a contradiction. Let $n = \deg(a(x)) \geq 1$. Then, in the left-hand side of (18), there are two of the first three summands whose degrees are equal. Consequently, letting deg$(b(x)) = k$, we have three cases:

(i) The first two summands in the left-hand side of (18) have equal degrees, *i.e.*, $2n = n + k + 1$.

(ii) The first and the third summands in the left-hand side of (18) have equal degrees, *i.e.*, $2n = 2k + 2$.

(iii) The second and the third summands in the left-hand side of (18) have equal degrees, *i.e.*, $n + k + 1 = 2k + 2$.

For all these cases, we obtain $k = n - 1$. Let

$$a(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n \quad \text{and} \quad b(x) = d_0x^k + d_1x^{k-1} + \cdots + d_k,$$

with $c_i, d_j \in Z_2$ and $c_0 = d_0 = 1$. Then, on the one hand, the summand in the left-hand side of (18) of degree $2n$ has coefficient $c_0^2 + c_0d_0 + d_0^2 = 1$ and, on the other hand, this coefficient $c_0^2 + c_0d_0 + d_0^2$ must be equal to 0. This is a contradiction.

(d) We shall prove that the ring $R = A[y]$ is indecomposable. Suppose the contrary. Then R has a non-trivial idempotent $e = a(x)+b(x)y$, where $a(x), b(x) \in Z_2[x]$ (*i.e.*, different from 0 and 1). If $b(x) = 0$, then we get that either $e = a(x) = 0$ or $e = a(x) = 1$, which is a contradiction. Therefore, $b(x) \neq 0$ and $e^2 = e$ implies that $a^2(x) + b^2(x)y^2 = a(x) + b(x)y$, *i.e.*,

$$a^2(x) + b^2(x)xy + b^2(x)x^2 + b^2(x) = a(x) + b(x)y.$$

Hence $b^2(x)x = b(x)$, *i.e.*, $b(x)x = 1$, which is a contradiction, since $b(x) \in Z_2[x]$ is a non-zero polynomial of x. This completes the proof. $\square$

Acknowledgements. Research partially supported by the fund “NI" of University of Plovdiv, Bulgaria. The authors are grateful to the referee for the valuable suggestions.

References

[1] S. D. Berman, *Group algebras of countable abelian p-groups*, Dokl. Akad. Nauk SSSR **175** (1967) no. 3, 514–516.

[2] S. D. Berman, *Group algebras of countable abelian p-groups*, Publ. Math. Debrecen **14** (1967), 365–405.

[3] P. V. Danchev, *Warfield invariants in abelian group rings*, Extracta Math. **20** (2005), no. 3, 233–241.

[4] P. V. Danchev, *On a decomposition of normalized units in abelian group algebras*, An. Univ. Bucureşti Mat. **57** (2008), no. 2, 133–138.

[5] L. Fuchs, *Infinite abelian groups*, Vol. I, Pure and Applied Mathematics, Vol. 36, Academic Press, New York-London, 1970, xi+290 pp.

[6] L. Fuchs, *Infinite abelian groups*, Vol. II, Pure and Applied Mathematics, Vol. 36-II, Academic Press, New York-London, 1973, ix+363 pp.

[7] W. May, *Modular group algebras of simply presented abelian groups*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 403–409.

[8] T. Z. Mollov, *Ulm invariants of the Sylow p-subgroups of the group algebras of the abelian groups over a field of characteristic p*, Sixth Congress of the Bulgarian Mathematicians, Varna, Reports Abstracts, Section **A2** (19977), p. 2.

[9] T.Z. Mollov, *Ulm invariants of Sylow p-subgroups of group algebras of abelian groups over a field of characteristic p*, PLISKA Stud. Math. Bulgar. **2** (1981), 77–82.

[10] T. Z. Mollov and N. A. Nachev, *The Ulm-Kaplansky invariants of the group of normed units of a modular group ring of a primary abelian group*, Serdica **6** (1980), no. 3, 258–263.

[11] T. Z. Mollov and N. A. Nachev, *Unit groups of commutative modular group rings*, C. R. Acad. Bulgare Sci. **59** (2006), no. 6, 589–592.

[12] N. A. Nachev, *Invariants of the Sylow p-subgroup of the unit group of a commutative group ring of characteristic p*, Comm. Algebra **23** (1995), no. 7, 2469–2489.

T. Z. MOLLOV, DEPT. OF ALGEBRA, U. OF PLOVDIV, 24 TZAR ASSEN STR., 4000 PLOVDIV, BULGARIA.
mollov@uni-plovdiv.bg

N. A. NACHEV, DEPT. OF ALGEBRA, U. OF PLOVDIV, 24 TZAR ASSEN STR., 4000 PLOVDIV, BULGARIA.
nachev@uni-plovdiv.bg