doi: 10.14232/actasm-013-510-1

Acta Sci. Math. (*Szeged*)
80 (2014), 433–445

On the unit group of a commutative group ring

V. Bovdi and M. Salim

Dedicated to Professor W. Kimmerle on his 60th birthday

Communicated by M. B. Szendrei

Abstract. We investigate the group of normalized units of the group algebra $\mathbb{Z}_{p^e}G$ of a finite abelian p-group G over the ring $\mathbb{Z}_{p^e}$ of residues modulo p^e with $e \geq 1$.

1 Introduction

Let $V(RG)$ be the group of normalized units of the group ring RG of a finite abelian p-group G over a commutative ring R of characteristic p^e with $e \geq 1$. It is well known ([4], Theorem 2.10, p.10) that $V(RG) = 1 + \omega(RG)$, where

$$\omega(RG) = \Big\{ \sum_{g \in G} a_g g \in RG \quad \Big| \quad \sum_{g \in G} a_g = 0 \Big\}$$

is the augmentation ideal of RG.

In the case when $\mathrm{char}(R) = p$ and G is an arbitrary finite (not necessary abelian) p-group, the structure of $V(RG)$ has been studied by several authors (see the survey [3]). For a finite abelian p-group G, the invariants and the basis of $V(\mathbb{Z}_pG)$ has been given by R. Sandling (see [12]). In general, when $\mathrm{char}(R) = p^e$ with $e \geq 2$, the structure of the abelian p-group $V(RG)$ is still not understood.

In the present paper we investigate the invariants of $V(RG)$ in the case when $R = \mathbb{Z}_{p^e}$ is the ring of residues modulo p^e. The question about the bases of $V(\mathbb{Z}_{p^e}G)$

Received January 31, 2013, and in revised form March 5, 2013.
AMS Subject Classifications: 16S34, 16U60, 20C05.
Key words and phrases: group algebra, unitary unit, symmetric unit.
This paper was supported by PPDNF and NRF Grant #31507 at UAEU.

is left open. Our research can be considered as a natural continuation of results of R. Sandling.

Note that the investigation of the group $V(\mathbb{Z}_{p^e}G)$ was started by F. Raggi (see, for example, [10]). We shall revisit his work done in [10] in order to get a more transparent description of the group $V(\mathbb{Z}_{p^e}G)$.

Several results concerning RG and $V(RG)$ have found applications in coding theory, cryptography and threshold logic (see [1, 2, 7, 8, 13]).

2 Main results

We start to study $V(\mathbb{Z}_{p^e}G)$ with the description of its elements of order p. It is easy to see that if $z \in \omega(RG)$ and $c \in G$ is of order p, then $c + p^{e-1}z$ is a nontrivial unit of order p in $\mathbb{Z}_{p^e}G$. We can ask whether the converse is true, namely that every element of order p in $V(\mathbb{Z}_{p^e}G)$ has the form $c + p^{e-1}z$, where $z \in \omega(RG)$ and $c \in G$ of order p. The first result gives an affirmative answer to this question.

Theorem 1. *Let $V(\mathbb{Z}_{p^e}G)$ be the group of normalized units of the group ring $\mathbb{Z}_{p^e}G$ of a finite abelian p-group G, where $e \geq 2$. Then every unit $u \in V(\mathbb{Z}_{p^e}G)$ of order p has a form $u = c + p^{e-1}z$, where $c \in G[p]$ and $z \in \omega(\mathbb{Z}_{p^e}G)$. Moreover,*

$$V(\mathbb{Z}_{p^e}G)[p] = G[p] \times (1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G)),$$

where the order of the elementary p-group $1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G)$ is $p^{|G|-1}$.

A full description of $V(\mathbb{Z}_{p^e}G)$ is given by the next theorem.

Theorem 2. *Let $V(\mathbb{Z}_{p^e}G)$ be the group of normalized units of the group ring $\mathbb{Z}_{p^e}G$ of a finite abelian p-group G with $\exp(G) = p^n$ where $e \geq 2$. Then*

$$V(\mathbb{Z}_{p^e}G) = G \times \mathfrak{L}(\mathbb{Z}_{p^e}G),$$
$$\mathfrak{L}(\mathbb{Z}_{p^e}G) \cong lC_{p^{e-1}} \times \Big(\bigtimes_{i=1}^{n} C_{p^{d+e-1}} \Big),$$

where the nonnegative integer s_i is equal to the difference of

$$|G^{p^{i-1}}| - 2|G^{p^i}| + |G^{p^{i+1}}|$$

and the number of cyclic subgroups of order p^i in the group G and where $l = |G| - 1 - (s_1 + \cdots + s_n)$.

Note that Lemma 9 itself can be considered as a separate result.

3 Preliminaries

If H is a subgroup of G, then we denote the left transversal of G with respect to H by $\mathfrak{R}_l(G/H)$. We denote the ideal of FG generated by the elements $h-1$ for $h \in H$ by $\mathfrak{I}(H)$. Furthermore $FG/\mathfrak{I}(H) \cong F[G/H]$ and

$$V(FG)/(1+\mathfrak{I}(H)) \cong V(F[G/H]).$$

Denote the subgroup of G generated by elements of order p^n by $G[p^n]$.

We start with the following well-known results.

Lemma 1. *Let p be a prime and $j = p^l k$, where $(k,p) = 1$. If $l \leq n$, then p^{n-l} is the largest p-power divisor of the binomial coefficient $\binom{p^n}{j}$.*

Proof. If $j = p^l k$ and $(k,p) = 1$, then the statement follows from

$$\binom{p^n}{j} = p^{n-l} \cdot \frac{\prod_{i=1,(i,p)=1}^{j-1}(p^n - i) \cdot \prod_{i=1}^{p^{l-1}k}(p^n - pi)}{(j-1)!k}. \qquad \blacksquare$$

Lemma 2. *Let G be a finite p-group and let R be a commutative ring of characteristic p^e with $e \geq 1$. If $l \geq e$ then*

$$(1-g)^{p^l} = (1-g^{p^s})^{p^{(l-s)}}, \qquad (s = 0, \dots, l-e+1).$$

Proof. See Lemma 2.4 in [6]. $\blacksquare$

Let R be a commutative ring of characteristic p^e with $e \geq 1$. The ideal $\omega(RG)$ is nilpotent ([4], Theorem 2.10, p. 10) and the nth power $\omega^n(RG)$ determines the so-called *nth dimension subgroup*

$$\mathfrak{D}_n(RG) = G \cap (1 + \omega^n(RG)), \qquad (n \geq 1).$$

Lemma 3. (See 1.14, [11].) *Let $e \geq 1$. If G is a finite abelian p-group, then*

$$\mathfrak{D}_n(\mathbb{Z}_{p^e}G) = \begin{cases} G, & \text{if } n = 1; \\ G^{p^{e+i}}, & \text{if } p^i < n \leq p^{i+1}. \end{cases}$$

The next two lemmas are well known.

Lemma 4. *If G is a finite abelian p-group, then*

$$V(\mathbb{Z}_p G)[p] = 1 + \mathfrak{I}(G[p]).$$

Proof. See Lemma 3.3 in [5]. ■

Lemma 5. *Let $U(R)$ be the group of units of a commutative ring R with 1. If I is a nilpotent ideal in R, then*

$$U(R)/(1+I) \cong U(R/I)$$

and the group $(1+I^m)/(1+I^{m+1})$ is isomorphic to the additive group of the quotient I^m/I^{m+1}.

Proof. Note that I is the kernel of the natural epimorphism $\sigma : R \to R/I$. On $U(R)$ the map σ induces the group homomorphism $\tilde{\sigma} : U(R) \to U(R/I)$ which is an epimorphism with kernel $1+I$. Indeed, if $x+I \in U(R/I)$ and $\sigma(w) = (x+I)^{-1}$, then

$$\sigma(xw) = (x+I)(x+I)^{-1} = 1+I.$$

Thus $xw = 1+t$ for some $t \in I$ and $1+t$ is a unit in R, so $w \in U(R)$. Of course $x = w^{-1}(1+t)$ is a unit such that $\tilde{\sigma}(w) = (x+I)^{-1} = x^{-1}+I$. Therefore $\tilde{\sigma}\colon U(R) \to U(R/I)$ is an epimorphism.

Now, let $x, y \in I^m$ and put $\psi(1+x) = x + I^{m+1}$. Then

$$\begin{aligned}\psi((1+x)(1+y)) &= xy + x + y + I^{m+1}\\ &= x + y + I^{m+1} = \psi(1+x) + \psi(1+y),\end{aligned}$$

so ψ is a homomorphism of the multiplicative group $1+I^m$ to the additive group I^m/I^{m+1} with kernel $1+I^{m+1}$. ■

Let $f_e\colon \mathbb{Z}_{p^e} \to \mathbb{Z}_{p^{e-1}}$ $(e \geq 2)$ be a ring homomorphism determined by

$$f_e(a+(p^e)) = a + (p^{e-1}) \qquad (a \in \mathbb{Z}).$$

Clearly $\mathbb{Z}_{p^e}/(p^{e-1}\mathbb{Z}_{p^e}) \cong \mathbb{Z}_{p^{e-1}}$ and the homomorphism f_e can be linearly extended to the group ring homomorphism

$$\overline{f_e}\colon \mathbb{Z}_{p^e}G \to \mathbb{Z}_{p^{e-1}}G. \tag{1}$$

Let us define the map $\mathfrak{r}\colon \mathbb{Z}_{p^e} \to \mathbb{Z}$ to be the map with the property that for any integer α with $0 \leq \alpha < p^e - 1$ we have $\mathfrak{r}^{-1}(\alpha) = \overline{\alpha} \in \mathbb{Z}_{p^e}$. Obviously, $\mathbb{Z}_{p^e} \ni \gamma_g = \alpha_g + p^{e-1}\beta_g$, where $0 \leq \mathfrak{r}(\alpha_g) < p^{e-1}$. Hence any $x \in \mathbb{Z}_{p^e}G$ can be written as

$$x = \sum_{g\in G} \gamma_g g = \sum_{g\in G} \alpha_g g + p^{e-1} \sum_{g\in G} \beta_g g, \tag{2}$$

where $\mathrm{red}_p(x) = \sum_{g\in G} \alpha_g g \in \mathbb{Z}_{p^e}G$ is called the *p-reduced part* of x.

It is easy to see, that $\mathfrak{Ker}(\overline{f_e}) = p^{e-1}\mathbb{Z}_{p^e}G$ and $(\mathfrak{Ker}(\overline{f_e}))^2 = 0$, so by (1) and (2) we obtain that

$$\mathbb{Z}_{p^e}G\Big/(p^{e-1}\mathbb{Z}_{p^e}G) \cong \mathbb{Z}_{p^{e-1}}G.$$

Since $p^{e-1}\mathbb{Z}_{p^e}G$ is a nilpotent ideal by Lemma 5,

$$U(\mathbb{Z}_{p^e}G)/(1+p^{e-1}\mathbb{Z}_{p^e}G) \cong U(\mathbb{Z}_{p^{e-1}}G).$$

Clearly, $1+p^{e-1}\mathbb{Z}_{p^e}G$ is an elementary abelian p-group of order

$$|1+p^{e-1}\mathbb{Z}_{p^e}G| = \frac{|V(\mathbb{Z}_{p^e}G)|\cdot|U(\mathbb{Z}_{p^e})|}{|V(\mathbb{Z}_{p^{e-1}}G)|\cdot|U(\mathbb{Z}_{p^{e-1}})|} = \frac{p^{e(|G|-1)}\cdot p}{p^{(e-1)(|G|-1)}} = p^{|G|}.$$

Furthermore, if $u \in V(\mathbb{Z}_{p^e}G) = 1+\omega(\mathbb{Z}_{p^e}G)$, then

$$u = \mathrm{red}_p(u) + p^{e-1}\sum_{g\in G}\beta_g(g-1),$$

where $\mathrm{red}_p(u) = 1+\sum_{g\in G}\alpha_g(g-1)$ is a unit and $0 \le \mathfrak{r}(\alpha_g) < p^{e-1}$. It follows that

$$u = \mathrm{red}_p(u)(1+p^{e-1}z), \qquad (z\in\omega(\mathbb{Z}_{p^e}G)). \tag{3}$$

Lemma 6. *Let* $\overline{f_e}\colon V(\mathbb{Z}_{p^e}G) \to V(\mathbb{Z}_{p^{e-1}}G)$ *be the group homomorphism naturally obtained from* (1)*. Then* $\mathfrak{Ker}(\overline{f_e}) = 1+p^{e-1}\omega(\mathbb{Z}_{p^e}G)$ *is an elementary abelian* p*-group of order* $p^{|G|-1}$ *and*

$$V(\mathbb{Z}_{p^e}G)/(1+p^{e-1}\omega(\mathbb{Z}_{p^e}G)) \cong V(\mathbb{Z}_{p^{e-1}}G). \tag{4}$$

Proof. Let $u \in V(\mathbb{Z}_{p^e}G)$. Then by (3) we have that

$$\overline{f_e}(u) = 1+\sum_{g\in G}(\alpha_g + (p^{e-1}))(g-1) \in V(\mathbb{Z}_{p^{e-1}}G),$$

so $V(\mathbb{Z}_{p^e}G)/(1+p^{e-1}W) \cong V(\mathbb{Z}_{p^{e-1}}G)$, where $W \subseteq \omega(\mathbb{Z}_{p^e}G)$. It is easy to check that $1+p^{e-1}W$ is an elementary abelian p-group of order

$$|1+p^{e-1}W| = \frac{|V(\mathbb{Z}_{p^e}G)|}{|V(\mathbb{Z}_{p^{e-1}}G)|} = \frac{p^{e(|G|-1)}}{p^{(e-1)(|G|-1)}} = p^{|G|-1}.$$

Clearly, $|p^{e-1}\omega(\mathbb{Z}_{p^e}G)| = |p^{e-1}W| = p^{|G|-1}$ and consequently

$$1+p^{e-1}W = 1+p^{e-1}\omega(\mathbb{Z}_{p^e}G).$$

The proof is complete. ∎

4 Proof of the Theorems

Proof of Theorem 1. Use induction on e. The base of the induction is: $e = 2$.

Put $H = G[p]$. Any $u \in V(\mathbb{Z}_{p^e}G)[p]$ can be written as

$$u = c_1 x_1 + \cdots + c_t x_t,$$

where $c_1, \dots, c_t \in \mathfrak{R}_l(G/H)$ and $x_1, \dots, x_t \in \mathbb{Z}_{p^2}H$.

First, assume that $c_i \notin H$ for any $i = 1, \dots t$. Clearly,

$$\overline{f_2}(u) = c_1\overline{f_2}(x_1) + c_2\overline{f_2}(x_2) + \cdots + c_t\overline{f_2}(x_t) \in V(\mathbb{Z}_pG). \tag{5}$$

Since $\overline{f_2}(u) \in 1 + \mathfrak{I}(H)$ (see Lemma 4), we have that $c_j \in H$ for some j, by (5), a contradiction.

Consequently, we can assume that $c_1 = 1 \in H$, $x_1 \neq 0$ and $1 \in \operatorname{Supp}(x_1)$. This yields that

$$\begin{aligned}\overline{f_2}(u) = \overline{f_2}(x_1 - \chi(x_1)) + c_2\overline{f_2}(x_2 - \chi(x_2)) + \cdots + c_t\overline{f_2}(x_t - \chi(x_t)) +\\ + \overline{f_2}(\chi(x_1)) + c_2\overline{f_2}(\chi(x_2)) + \cdots + c_t\overline{f_2}(\chi(x_t)) \in V(\mathbb{Z}_pG).\end{aligned}$$

Clearly, either $\overline{f_2}(u) = 1$ or $\overline{f_2}(u)$ has order p. Lemma 4 ensures that

$$\begin{aligned} f_2(\chi(x_1)) \equiv 1 \pmod{p}, \qquad \text{and}\\ f_2(\chi(x_2)) \equiv \cdots \equiv f_2(\chi(x_t)) \equiv 0 \pmod{p}.\end{aligned}$$

It follows that u can be written as

$$u = 1 + \sum_{i=1}^{t} c_i \sum_{h \in G[p]} \beta_h^{(i)}(h-1) + pz, \qquad (z \in \mathbb{Z}_{p^2}G). \tag{6}$$

We can assume that $z = 0$. By Lemma 3 we have that

$$G = \mathfrak{D}_1(G) \supset \mathfrak{D}_2(G) = \mathfrak{D}_3(G) = \cdots = \mathfrak{D}_p(G) = G^{p^2},$$

so (6) can be rewritten as

$$u = 1 + \sum_{i=1}^{t} c_i \sum_{h \in G[p]\setminus \mathfrak{D}_p} \beta_h^{(i)}(h-1) + w,$$

where $w \in \omega^2(\mathbb{Z}_{p^2}G)$. Then, by the binomial formula,

$$\begin{aligned}1 = u^p \equiv 1 + p\sum_{i=1}^{t} c_i \sum_{h \in G[p]\setminus \mathfrak{D}_p} \beta_h^{(i)}(h-1) +\\ + \binom{p}{2}\Big(\sum_{i=1}^{t} c_i \sum_{h \in G[p]\setminus \mathfrak{D}_p} \beta_h^{(i)}(h-1)\Big)^2 + \cdots \pmod{\omega^2(\mathbb{Z}_{p^2}G)}.\end{aligned}$$

It follows that

$$p\sum_{i=1}^{t} c_i \sum_{h\in G[p]\setminus\mathfrak{D}_p} \beta_h^{(i)}(h-1) \equiv 0 \pmod{\omega^2(\mathbb{Z}_{p^2}G)}$$

and $\beta_h^{(i)} \equiv 0 \pmod{p^2}$ for any $h \in G[p] \setminus \mathfrak{D}_p$. Hence by (6),

$$u = 1 + w, \qquad (w \in \omega^2(\mathbb{Z}_{p^2}G)).$$

Again, by Lemma 3, we have that

$$G^{p^2} = \mathfrak{D}_p(G) \supset \mathfrak{D}_{p+1}(G) = \mathfrak{D}_{p+2}(G) = \cdots = \mathfrak{D}_{p^2}(G) = G^{p^3}$$

and (6) can be rewritten as

$$u = 1 + \sum_{i=1}^{t} c_i \sum_{h\in\mathfrak{D}_p\setminus\mathfrak{D}_{p^2}} \beta_h^{(i)}(h-1) + w,$$

where $w \in \omega^3(\mathbb{Z}_{p^2}G)$. This yields

$$\begin{aligned} 1 = u^p \equiv 1 + p\sum_{i=1}^{t} c_i \sum_{h\in\mathfrak{D}_p\setminus\mathfrak{D}_{p^2}} \beta_h^{(i)}(h-1) + \\ + \binom{p}{2}\Big(\sum_{i=1}^{t} c_i \sum_{h\in\mathfrak{D}_p\setminus\mathfrak{D}_{p^2}} \beta_h^{(i)}(h-1)\Big)^2 + \cdots \pmod{\omega^3(\mathbb{Z}_{p^2}G)}. \end{aligned}$$

As before, it follows that

$$p\sum_{i=1}^{t} c_i \sum_{h\in\mathfrak{D}_p\setminus\mathfrak{D}_{p^2}} \beta_h^{(i)}(h-1) \equiv 0 \pmod{\omega^3(\mathbb{Z}_{p^2}G)}$$

and $\beta_h^{(i)} \equiv 0 \pmod{p^2}$ for any $h \in \mathfrak{D}_p \setminus \mathfrak{D}_{p^2}$. Therefore,

$$u = 1 + w, \qquad (w \in \omega^3(\mathbb{Z}_{p^2}G)).$$

By continuing this process we obtain that $u = 1 + pv$, because the augmentation ideal $\omega(\mathbb{Z}_{p^2}G)$ is nilpotent.

Now assume that the statement of our lemma is true for $\mathbb{Z}_{p^{e-1}}G$. This means that for a unit u of the form (3) we get $\beta_h^{(i)} = p^{e-2}\alpha_h^{(i)}$ and

$$u = 1 + \sum_{i=1}^{t} c_i \sum_{h\in G[p]} p^{e-2}\alpha_h^{(i)}(h-1),$$

so

$$1 = u^p = 1 + p\sum_{i=1}^{t} c_i \sum_{h\in G[p]} p^{e-2}\alpha_h^{(i)}(h-1)$$

and $\alpha_h^{(i)} \equiv 0 \pmod p$. The proof is complete. ∎

Lemma 7. *Let G be a finite abelian p-group. Then*

$$V(\mathbb{Z}_{p^e}G) = G \times \mathfrak{L}(\mathbb{Z}_{p^e}G)$$

and the following conditions hold:

(i) *if $e \geq 2$, then $\overline{f_e}(\mathfrak{L}(\mathbb{Z}_{p^e}G)) = \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)$;*

(ii) *if $e \geq 2$, then $\mathfrak{Ker}(\overline{f_e}) = 1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G) = \mathfrak{L}(\mathbb{Z}_{p^e}G)[p]$ and*

$$\mathfrak{L}(\mathbb{Z}_{p^e}G)/(1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G)) \cong \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G); \tag{7}$$

(iii) *$\mathfrak{L}(\mathbb{Z}_{p^e}G)[p] \cong \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)[p]$ for $e \geq 3$.*

Proof. If $e = 1$, then there exists a subgroup $\mathfrak{L}(\mathbb{Z}_pG)$ of $V(\mathbb{Z}_pG)$ (see [9], Theorem 3) such that $V(\mathbb{Z}_pG) = G \times \mathfrak{L}(\mathbb{Z}_pG)$.

Assume $V(\mathbb{Z}_{p^{e-1}}G) = G \times \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)$. Consider the homomorphism

$$\overline{f_e} : V(\mathbb{Z}_{p^e}G) \to V(\mathbb{Z}_{p^{e-1}}G) = G \times \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G).$$

Denote the preimage of $\mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)$ in $V(\mathbb{Z}_{p^e}G)$ by $\mathfrak{L}(\mathbb{Z}_{p^e}G)$. Clearly, $\overline{f_e}(g) = g$ for all $g \in G$ and

$$\mathfrak{Ker}(\overline{f_e}) = 1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G) \leq \mathfrak{L}(\mathbb{Z}_{p^e}G).$$

If $x \in \mathfrak{L}(\mathbb{Z}_{p^e}G) \cap G$, then

$$G \ni \overline{f_e}(x) \in \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G) \cap G = \langle 1 \rangle,$$

so $x = 1$. Hence $\mathfrak{L}(\mathbb{Z}_{p^e}G) \cap G = \langle 1 \rangle$ and $G \times \mathfrak{L}(\mathbb{Z}_{p^e}G) \subseteq V(\mathbb{Z}_{p^e}G)$. Since

$$\overline{f_e}(G \times \mathfrak{L}(\mathbb{Z}_{p^e}G)) = V(\mathbb{Z}_{p^{e-1}}G)$$

and $\mathfrak{Ker}(\overline{f_e}) \subseteq G \times \mathfrak{L}(\mathbb{Z}_{p^e}G)$, we have that $V(\mathbb{Z}_{p^e}G) = G \times \mathfrak{L}(\mathbb{Z}_{p^e}G)$ by properties of the homomorphism.

(ii) Clearly the epimorphism $\overline{f_e}$ $(e \geq 2)$ satisfies (7) by construction.

(iii) Let $e \geq 3$. From (ii) we have

$$\mathfrak{Ker}(\overline{f_e}) = 1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G) = \mathfrak{L}(\mathbb{Z}_{p^e}G)[p]$$

and $|1 + p^{e-1}\omega(\mathbb{Z}_{p^e}G)| = p^{|G|-1}$ (see Lemma 6). It follows that

$$|\mathfrak{L}(\mathbb{Z}_{p^e}G)[p]| = |\mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)[p]| = p^{|G|-1},$$

so the proof is finished. ∎

Lemma 8. *Let $e \geq 2$. If $u \in \mathfrak{L}(\mathbb{Z}_{p^e}G)$, then*

$$|u| = p \cdot |\overline{f_e}(u)|. \tag{8}$$

Proof. Let $|u| = p^m$. By Theorem 1 we obtain that $u^{p^{m-1}} = 1 + p^{e-1}z$ for some $z \in \omega(\mathbb{Z}_{p^e}G)$, and $\overline{f_e}(u^{p^{m-1}}) = 1$, so the statement follows by induction. ∎

Lemma 9. *Let $d \geq 1$ and $0 \neq y \in \mathbb{Z}_{p^e}G$. Then $(1+p^d y)^{p^{e-d}} = 1$ and the following conditions hold:*

(i) *if $p^{e-1}y \neq 0$, then the unit $1 + p^d y$ has order p^{e-d}, except when*

$$p = 2, \quad d = 1 \quad \text{and} \quad y^2 \notin 2\mathbb{Z}_{2^e}G;$$

(ii) *if $p^{e-1}y = 0$ then $y = p^s z$, where $p^{e-1}z \neq 0$, and the unit $1 + p^{d+s}z$ has order p^{e-d-s}.*

Proof. Let $j = p^l k$ and $(k,p) = 1$. By Lemma 1, the number $p^{e+(j-1)d-l}$ is the largest p-power divisor of $\binom{p^{e-d}}{j}p^{jd}$ for $j \geq 1$. Since

$$\begin{aligned} e - d - l + p^l kd \geq e - d - l + p^l d = e + (p^l - 1)d - l \geq e + p^l - 1 - l \geq e; \\ dp^{e-d} \geq d + p^{e-d} \geq d + e - d \geq e, \end{aligned}$$

the number p^e divides the natural numbers $\binom{p^{e-d}}{j}p^{jd}$ and $p^{dp^{e-d}}$. Using these inequalities, we have

$$(1+p^d y)^{p^{e-d}} = 1 + \textstyle\sum_{j=1}^{p^{e-d}} \binom{p^{e-d}}{j} p^{jd} \cdot y^j + p^{dp^{e-d}} \cdot y^{p^{e-d}} = 1.$$

Therefore, the order of $1 + p^d y$ is a divisor of p^{e-d}.

Assume that $(1+p^d y)^{p^{e-d-1}} = 1$. Since

$$dp^{e-d-1} \geq d + p^{e-d-1} \geq d + 1 + (e - d - 1) \geq e,$$

we obtain that

$$\begin{aligned} (1+p^d y)^{p^{e-d-1}} &= 1 + \sum_{j=1}^{p^{e-d-1}-1} \binom{p^{e-d-1}}{j} p^{jd} y^j + p^{dp^{e-d-1}} \cdot y^{p^{e-d-1}} \\ &= 1 + \sum_{j=1}^{p^{e-d-1}-1} \binom{p^{e-d-1}}{j} p^{jd} y^j = 1 \end{aligned}$$

and $\sum_{j=1}^{p^{e-d-1}-1}\binom{p^{e-d-1}}{j}p^{jd}y^j=0$. This yields that

$$p^{e-1}y=-\binom{p^{e-d-1}}{2}p^{2d}y^2-\sum_{j=3}^{p^{e-d-1}-1}\binom{p^{e-d-1}}{j}p^{jd}y^j. \qquad (9)$$

Assume that $p^{e-1}y\neq 0$. Since $j=p^lk$, where $(k,p)=1$, the number $p^{e+(j-1)d-1-l}$ is the largest p-power divisor of $\binom{p^{e-d-1}}{j}p^{jd}$ for $j\geq 2$ by Lemma 1. Put

$$m=(j-1)d-1-l,$$

and consider the following cases:

1. Let $l=0$. Then $m=(k-1)d-1-l$ and $k\geq 2$, so $m\geq 0$.
2. Let $l>1$. Then $j=p^lk\geq p^l\geq 4$ and

$$\begin{aligned} m&=(p^lk-1)d-1-l\\ &\geq (p^l-1)-1-l=p^l-2-l\geq (p^l+l)-l-2=p^l-2\geq 0.\end{aligned}$$

3. Let $l=1$. Then $pk>2$ unless $p=2$ and $d=1$. If $p=2$ and $d=1$ we have $m=(pk-1)2-2=2pk-4\geq 0$.

In all cases $m\geq 0$ unless $p=2$, $d=1$ and $y^2\notin 2\mathbb{Z}_{2^e}G$. Therefore

$$p^{e+(j-1)d-1-l}\geq p^e$$

and by (9), we get $p^{e-1}y=0$, a contradiction. Hence, the order of the unit $1+p^dy$ is p^{e-d}. The proof of part (i) is finished.

If $p^{e-1}y=0$ then $y=p^sz$, where $p^{e-1}z\neq 0$, so by part (i), the unit $1+p^{d+s}z$ has order p^{e-d-s}. ∎

Corollary 1. *If $G=\langle a\mid a^2=1\rangle$ then*

$$V(\mathbb{Z}_{2^e}G)=G\times\langle 1+2(a-1)\rangle\cong C_2\times C_{2^{e-1}}.$$

Proof. Indeed, $(a-1)^2=-2(a-1)$, so $|1+2(a-1)|=2^{e-1}$. ∎

Proof of Theorem 2. Let $|V(\mathbb{Z}_pG)[p]|=p^r$ and $\exp(G)=p^n$. Assume that

$$V(\mathbb{Z}_pG)=\langle b_1\rangle\times\cdots\times\langle b_r\rangle, \qquad (10)$$

where $|\langle b_j\rangle|=p^{c_j}$. The number $r=\operatorname{rank}_p(V)$ is called the *p-rank of* $V(\mathbb{Z}_pG)$. Obviously

$$V(\mathbb{Z}_pG)[p]=\langle b_1^{p^{c_1-1}}\rangle\times\langle b_2^{p^{c_2-1}}\rangle\times\cdots\times\langle b_r^{p^{c_r-1}}\rangle.$$

Put $H = G[p]$. Since $V(\mathbb{Z}_pG)[p] = 1 + \mathfrak{I}(H)$ (see Lemma 4), p^r equals the number of the elements of the ideal $\mathfrak{I}(H)$. It is well known (see [4], Lemma 2.2, p.7) that a basis of $\mathfrak{I}(H)$ consists of

$$\{u_i(h_j - 1) \mid u_i \in \mathfrak{R}_l(G/H), \quad h_j \in H \setminus 1\}$$

and the number of such elements is $\frac{|G|}{|H|}(|H| - 1) = |G| - |G^p|$. Hence

$$r = \mathrm{rank}_p(V) = |G| - |G^p|.$$

Since $V(\mathbb{Z}_pG)^p = V(\mathbb{Z}_pG^p)$, we have $\mathrm{rank}_p(V(\mathbb{Z}_pG)^p) = |G^p| - |G^{p^2}|$. It follows that the number of cyclic subgroups of order p in $V(\mathbb{Z}_pG)$ (see (10)) is

$$(|G| - |G^p|) - (|G^p| - |G^{p^2}|) = |G| - 2|G^p| + |G^{p^2}|.$$

Repeating this argument, one can easily see that the number of elements of order p^i in $V(\mathbb{Z}_pG)$ is equal to

$$|G^{p^{i-1}}| - 2|G^{p^i}| + |G^{p^{i+1}}|, \qquad (i = 1, \dots, n). \tag{11}$$

Recall that $V(\mathbb{Z}_pG) = G \times \mathfrak{L}(\mathbb{Z}_pG)$ (see [9], Theorem 3) is a finite abelian p-group and $\mathfrak{L}(\mathbb{Z}_pG)$ has a decomposition

$$\mathfrak{L}(\mathbb{Z}_pG) \cong \bigtimes_{d=1}^{n} s_d C_{p^d} \qquad (s_d \in \mathbb{N}), \tag{12}$$

where $\mathrm{rank}_p(\mathfrak{L}(\mathbb{Z}_pG)) = r = s_1 + \dots + s_n$ and $\exp(G) = p^n$. The number s_i is equal to the difference of (11) and the number of cyclic subgroups of order p^i in the direct decomposition of the group G.

We use induction on $e \geq 2$ to prove that

$$\mathfrak{L}(\mathbb{Z}_{p^e}G) \cong lC_{p^{e-1}} \times \Big(\bigtimes_{d=1}^{n} s_d C_{p^{d+e-1}} \Big), \tag{13}$$

where $l = |G| - 1 - r$ and where $s_1, \dots, s_n \in \mathbb{N}$ are from (12).

The base of the induction is: $e = 2$. According to Lemma 7, the kernel of the epimorphism $\overline{f_e}$ is $\mathfrak{Ker}(\overline{f_e}) = 1 + p\omega(\mathbb{Z}_{p^2}G)$, which consists of all elements of order p in $\mathfrak{L}(\mathbb{Z}_{p^2}G)$ and $|1 + p\omega(\mathbb{Z}_{p^2}G)| = p^{|G|-1}$ by Lemma 6. Hence

$$\exp(\mathfrak{L}(\mathbb{Z}_{p^2}G)) = p \cdot \exp(\mathfrak{L}(\mathbb{Z}_pG)) = p^{n+1}$$

and the finite abelian p-group $\mathfrak{L}(\mathbb{Z}_{p^2}G)$ has a decomposition

$$\mathfrak{L}(\mathbb{Z}_{p^2}G) \cong lC_p \times \Big(\bigtimes_{d=1}^{n} s_d C_{p^{d+1}} \Big),$$

where $s_1, \dots, s_n \in \mathbb{N}$ are from (12), and where $l = |G| - 1 - r$ by Lemma 6.

Assume that

$$\mathfrak{L}(\mathbb{Z}_{p^{e-1}}G) \cong lC_{p^{e-2}} \times \Big(\bigtimes_{d=1}^{n} s_d C_{p^{d+e-2}} \Big).$$

Using Lemma 8, we get

$$\exp(\mathfrak{L}(\mathbb{Z}_{p^e}G)) = p \cdot \exp(\mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)) = p^{n+e-1}$$

and $\mathfrak{L}(\mathbb{Z}_{p^e}G)[p] \cong \mathfrak{L}(\mathbb{Z}_{p^{e-1}}G)[p]$ with $e > 2$, by Lemma 7(iii). Now, again as before, we obtain (13). The proof is complete. ∎

References

[1] N. N. Aĭzenberg, A. A. Bovdi, E. I. Gergo and F. E. Geche, Algebraic aspects of threshold logic, *Cybernetics*, **2** (1980), 26–30.

[2] M. I. Anokhin, On some sets of group functions, *Mat. Zametki*, **74** (2003), 3–11.

[3] A. Bovdi, The group of units of a group algebra of characteristic p, *Publ. Math. Debrecen*, **52** (1998), 193–244.

[4] A. A. Bovdi, Group rings, Kiev.UMK VO (1988), 155 (in Russian).

[5] V. Bovdi and A. Grishkov, Unitary and symmetric units of a commutative group algebra, *Proc. Edinburgh Math. Soc.*, to appear.

[6] C. Coleman and D. Easdown, Complementation in the group of units of a ring, *Bull. Austral. Math. Soc.*, **62** (2000), 183–192.

[7] B. Hurley and T. Hurley, Group ring cryptography, *Int. J. Pure Appl. Math.*, **69** (2011), 67–86.

[8] T. Hurley, Convolutional codes from units in matrix and group rings, *Int. J. Pure Appl. Math.*, **50** (2009), 431–463.

[9] D. L. Johnson, The modular group-ring of a finite p-group, *Proc. Amer. Math. Soc.*, **68** (1978), 19–22.

[10] F. Raggi C, Las unidades en anillos de gruppo con coefficientes em K_{p^n}, $\mathbb{Z}_{p^n}$ and $\widehat{F}_{p^n}$, *Anales del Inst. de Mat.de la UNAM*, **10** (1977), 29–65.

[11] R. Sandling, Dimension subgroups over arbitrary coefficient rings, *J. Algebra*, **21** (1972), 250–265.

[12] R. Sandling, Units in the modular group algebra of a finite abelian p-group, *J. Pure Appl. Algebra*, **33** (1984), 337–346.

[13] W. Willems, A note on self-dual group codes, *IEEE Trans. Inform. Theory*, **48** (2002), 3107–3109.

V. Bovdi, Department of Math. Sciences, UAE University - Al-Ain, United Arab Emirates; *e-mail*: vbovdi@gmail.com

M. Salim, Department of Math. Sciences, UAE University - Al-Ain, United Arab Emirates; *e-mail*: MSalim@uaeu.ac.ae