# On the unit group of a commutative group ring

Mohamed A. Salim

Department of Math. Sciences,
UAE University - Al-Ain,
United Arab Emirates

Ischia Group Theory , ITALY
April 2014

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 (Theorem of Jennings) that in this case the augmentation ideal

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

is a nilpotent ideal of $RG$ and

$$V(RG) = 1 + \omega(RG).$$

For a finite abelian $p$-group $G$, the invariants and the basis of $V(\mathbb{Z}_p G)$ have been given in

R. Sandling. Units in the modular group algebra of a finite abelian $p$-group. *J. Pure Appl. Algebra*, 33(3):337–346, 1984.

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 our talk we give an explanation of the invariants of $V(RG)$ in the case when $R = \mathbb{Z}_{p^e}$ is the ring of residues modulo $p^e$.

The investigation of the group $V(\mathbb{Z}_{p^e} G)$ was started by:

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

We shall revisit his work 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.

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

M. I. Anokhin.
On some sets of group functions. *Mat. Zametki*, 74(1):3–11, 2003.

B. Hurley and T. Hurley. Group ring cryptography. *Int. J. Pure Appl. Math.*, 69(1):67–86, 2011.

T. Hurley. Convolutional codes from units in matrix and group rings. *Int. J. Pure Appl. Math.*, 50(3):431–463, 2009.

W. Willems. A note on self-dual group codes. *IEEE Trans. Inform. Theory*, 48(12):3107–3109, 2002.

We start to study $V(\mathbb{Z}_{p^e} G)$ with the description of its elements of order $p$.

The next result is well known.

**Lemma**

*If $G$ is a finite abelian $p$-group, then*

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

*where $\mathfrak{I}(H)$ is the ideal of $FG$ generated by the elements $h - 1$ for $h \in H = G[p]$ (i.e. $h$ is an element of order $p$ in $G$).*

But this lemma is not true (!!!) for

$$V(\mathbb{Z}_{p^e} G)[p], \qquad e \geq 2.$$

Now let $G$ be a finite abelian $p$-group and let $R$ be an arbitrary commutative ring of characteristic $p^e$, with $e \geq 2$.

It is easy to see that if $z \in \omega(RG)$ and $c \in G$ is of order $p$, then the nontrivial element

$$c + p^{e-1}z$$

is a unit of order $p$ in $V(RG)$.

Indeed, by the binomial formula

$$\begin{aligned}(c + p^{e-1}z)^p &= \\ &= c^p + \sum_{i=1}^{p-1} \binom{p}{i} c^{p-i}(p^{(e-1)}z)^i + p^{(e-1)p}z^p \\ &= c^p + 0 \\ &= 1.\end{aligned}$$

We can ask whether the converse is true, namely:

Is the following conjecture true?

**Conjecture**

*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 $c \in G$ are of order $p$.*

Using some results of R. Sandling:

R. Sandling. Dimension subgroups over arbitrary coefficient rings. *J. Algebra*, 21:250–265, 1972.

R. Sandling. Units in the modular group algebra of a finite abelian $p$-group. *J. Pure Appl. Algebra*, 33(3):337–346, 1984.

and the paper:

C. Coleman and D. Easdown. Complementation in the group of units of a ring. *Bull. Austral. Math. Soc.*, 62(2):183–192, 2000.

our first result gives an affirmative answer to this question.

## Theorem

*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 the form $u = c + p^{e-1}z$, where $c \in G[p]$ and $z \in \omega(\mathbb{Z}_{p^e}G)$. Moreover,*

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

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

The proof of this result relies heavily on the technics of the following paper.

V. Bovdi and A. Grishkov. Unitary and symmetric units of a commutative group algebra. *subbmited*, pages 1–15, 2013. http://arxiv.org/pdf/1302.5222.pdf

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

## Theorem

*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*

$$V(\mathbb{Z}_{p^e}G) = G \times \mathfrak{U}(\mathbb{Z}_{p^e}G),$$
$$\mathfrak{U}(\mathbb{Z}_{p^e}G) \cong IC_{p^{e-1}} \times \left( \times_{i=1}^{n} s_i C_{p^{d+e-1}} \right),$$

*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 $I = |G| - 1 - (s_1 + \cdots + s_n)$.*

The preprint is available in
http://arxiv.org/pdf/1305.3179v1.pdf