PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 7, July 2017, Pages 2771–2783
http://dx.doi.org/10.1090/proc/13631
Article electronically published on April 4, 2017

FREE PRODUCTS IN THE UNIT GROUP OF THE INTEGRAL GROUP RING OF A FINITE GROUP

GEOFFREY JANSSENS, ERIC JESPERS, AND DORYAN TEMMERMAN

(Communicated by Pham Huu Tiep)

ABSTRACT. Let G be a finite group and let p be a prime. We continue the search for generic constructions of free products and free monoids in the unit group $\mathcal{U}(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$. For a nilpotent group G with a non-central element g of order p, explicit generic constructions are given of two periodic units b_1 and b_2 in $\mathcal{U}(\mathbb{Z}G)$ such that $\langle b_1, b_2\rangle = \langle b_1\rangle \star \langle b_2\rangle \cong \mathbb{Z}_p \star \mathbb{Z}_p$, a free product of two cyclic groups of prime order. Moreover, if G is nilpotent of class 2 and g has order p^n, then also concrete generators for free products $\mathbb{Z}_{p^k} \star \mathbb{Z}_{p^m}$ are constructed (with $1 \leq k, m \leq n$). As an application, for finite nilpotent groups, we obtain earlier results of Marciniak-Sehgal and Gonçalves-Passman. Further, for an arbitrary finite group G we give generic constructions of free monoids in $\mathcal{U}(\mathbb{Z}G)$ that generate an infinite solvable subgroup.

1. Introduction

The representation theory over some ring R of a finite group G is currently studied through the modules over its group ring RG. In this perspective it is natural to ask whether RG determines the underlying group G, i.e., if $RG \cong RH$, then is $G \cong H$? This question is called the isomorphism problem for group rings. In case $R = \mathbb{Z}$ the problem remained open until the surprising counterexample by Hertweck in 2001 [7]. However for many classes of groups the isomorphism problem has a positive answer over $\mathbb{Z}$. One main obstruction towards a positive solution is the lack of information on how rigid G lies inside $\mathbb{Z}G$ or more precisely inside $\mathcal{U}(\mathbb{Z}G)$, the unit group of $\mathbb{Z}G$. Several conjectures have been made in this direction, such as the Zassenhaus conjectures, and consequently one started the search for generic constructions of elements in $\mathcal{U}(\mathbb{Z}G)$ and one investigates the algebraic structure of the group generated by these units.

Only a few generic constructions are known. The most important are the so-called Bass units and the bicyclic units. With these elements at hand, it is a natural problem to determine "how large" the group B generated by the Bass and bicyclic units is compared to $\mathcal{U}(\mathbb{Z}G)$. Furthermore, one would like to determine the relations between these units. Jespers and Leal [9] proved that for many finite groups G the

Received by the editors July 8, 2016.
2010 *Mathematics Subject Classification.* Primary 16U60, 20C05, 16S34, 20E06; Secondary 20C10, 20C40.
Key words and phrases. Group ring, unit group, free product, generic units.
The first and third authors were supported by Fonds voor Wetenschappelijk Onderzoek (Flanders).
The second author was supported by Onderzoeksraad of Vrije Universiteit Brussel and Fonds voor Wetenschappelijk Onderzoek (Flanders).

group B is of finite index in $\mathcal{U}(\mathbb{Z}G)$; earlier results of this type were obtained by Ritter and Sehgal (see for example [14]). The groups G excluded are those that have a non-commutative fixed point free image and those for which the rational group algebra $\mathbb{Q}G$ does have an exceptional simple epimorphic image. The latter are by definition the non-commutative division algebras which are not a positive-definite quaternion algebra and matrix algebras $M_2(D)$ over a division algebra of the type $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-d})$ or a quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$. Moreover, in [3], Eisele, Kiefer and Van Gelder reduced the number of exceptional cases by showing that the only cases that can occur as an epimorphic image of a rational groups algebra $\mathbb{Q}G$ are $d = 1, 2, 3$ and $(a, b) = (-1, -1), (-1, -3), (-2, -5)$. For a state-of-the-art article we refer to [10].

In recent years there have been many investigations determining whether there are any non-trivial relations between two given units that are Bass units or bicyclic units. It turns out that in many cases two such elements generate a non-cyclic free group. In this context, a result of Hartley and Pickel [6] states that $\mathcal{U}(\mathbb{Z}G)$ contains a non-cyclic free group except if G is abelian or a Hamiltonian 2-group. Actually, it turns out that these cases correspond with $\mathcal{U}(\mathbb{Z}G)$ being abelian-by-finite, which in its turn is exactly the case when the unit group is solvable-by-finite (see [10, Corollary 5.5.7]).

An explicit construction of a free subgroup of the unit group was given by Marciniak and Sehgal in [12]: it is shown that any non-trivial bicyclic unit together with its image under the classical involution (which also is a bicyclic unit) generate a non-cyclic free group. Since then many more constructions of two bicyclic units, or two Bass units, or a Bass together with a bicyclic unit generating a free group have been discovered. For a survey we refer to [5, 11]. In [4], Gonçalves and Passman showed that $\mathcal{U}(\mathbb{Z}G)$ contains a free product $\mathbb{Z}_p \star \mathbb{Z}$ (with p a prime number) if and only if G contains a non-central element of order p. Moreover, when this occurs, the $\mathbb{Z}_p$-part of the free product can be taken to be a suitable non-central subgroup of G of order p. The proof of this result makes use of an earlier work of Passman [13] on the existence in $\mathrm{PSL}_n(R)$ (with R a commutative integral domain of characteristic zero) of a free product $G \star \mathbb{Z}$ when G is a finite subgroup of $\mathrm{PSL}_n(R)$. In the proofs of all these results, the element of infinite order is used in order to apply Tits alternative type techniques. We point out that this generator of the infinite cyclic part is only shown to exist, but no explicit constructions are obtained.

Note that if $p \neq 2$, then a group contains $\mathbb{Z}_p \star \mathbb{Z}$ if and only if it contains a group $\mathbb{Z}_p \star \mathbb{Z}_p$. Hence, a natural problem is to give explicit generic constructions of units $b_1, b_2 \in \mathcal{U}(\mathbb{Z}G)$ such that $\langle b_1, b_2\rangle \cong \mathbb{Z}_p \star \mathbb{Z}_p$. As such, one also obtains a generic construction of a unit $b = b_2b_1b_2$ such that $\langle b_1, b\rangle \cong \mathbb{Z}_p \star \mathbb{Z}$, provided $p \neq 2$. So far, such a result has not been obtained mainly because of the lack of generic constructions of non-trivial torsion units. However, recently in [1], V. Bovdi introduced very interesting torsion units.

In this paper we make use of these torsion units, we simply call them Bovdi units, to give the first (generic) constructions of free products of two finite cyclic groups in $\mathcal{U}(\mathbb{Z}G)$ provided G is a finite nilpotent group. Moreover, for an arbitrary finite group G, we also deal with the problem of producing infinite solvable subgroups in $\mathcal{U}(\mathbb{Z}G)$ (that are not virtually nilpotent) using non-trivial Bass and bicyclic units and construct generators of a non-cyclic free submonoid in these groups.

Throughout the paper G denotes a finite group and for a subset H of G we put $\widetilde{H} = \sum_{h\in H} h \in \mathbb{Z}G$ and $\widehat{H} = \frac{1}{|H|}\widetilde{H} \in \mathbb{Q}G$. If H is a subgroup, then $\widehat{H}$ is an idempotent. In case $H = \langle g\rangle$ we simply denote these elements by $\widetilde{g}$ and $\widehat{g}$ respectively. The classical involution on a group algebra KG is the K-linear map defined by $g \mapsto g^{-1}$, for $g \in G$. By ω we denote the augmentation map $KG \to K$. The free product of two groups H and K is denoted by $H \star K$. By $o(g)$ we denote the order of $g \in G$ and a cyclic group of order n (possibly n is infinite) we will denote by C_n.

2. Preliminaries

In order to construct free monoids and free products of cyclic groups in $\mathcal{U}(\mathbb{Z}G)$, we will make use of representations of the finite groups G and hence of matrix epimorphic images of the complex group algebra $\mathbb{C}G$. Therefore we begin with some technical lemmas on constructions of free products in matrix algebras. By E_{ij} we denote the elementary matrix with 1 in position (i,j) and zeros elsewhere. We start with three lemmas. The first and the third can be found in [11, pages 2,3] and the second is easily verified.

Lemma 2.1. *Suppose z_1, z_2, w_1, w_2 are non-zero elements in a field F. Then, there exists $U \in GL_2(F)$ such that $E_{12}(z_1)^U = E_{12}(w_1)$ and $E_{21}(z_2)^U = E_{21}(w_2)$ if and only if $z_1z_2 = w_1w_2$.*

Lemma 2.2. *Let n be a positive integer and $\zeta_n = e^{\frac{2\pi i}{n}}$ be a complex primitive n-th root of unity. If k is a positive integer such that $k \neq 0 \bmod n$, then $|\sum_{i=0}^{k-1}\zeta_n^i| \geq 1$; and this inequality is strict if and only if $k \neq \pm 1 \bmod n$.*

A useful tool for proving that the group generated by two subgroups is actually a free product is the well-known Ping-Pong Lemma.

Lemma 2.3. (Ping-Pong Lemma). *Suppose G_1 and G_2 are non-trivial subgroups of a group G with $|G_1| > 2$. If G acts on a set P and P_1 and P_2 are two non-empty and distinct subsets of P such that $g(P_i) \subseteq P_j$ for every non-trivial $g \in G_i$ and $\{i,j\} = \{1,2\}$, then $\langle G_1, G_2\rangle \cong G_1 \star G_2$.*

This Ping-Pong Lemma allows one to construct a free product of cyclic groups in $GL_n(\mathbb{C})$ and thus we obtain the following Sanov-like result.

Proposition 2.4. *Let n and m be positive integers and let $\zeta_n = e^{\frac{2k_n\pi i}{n}}$ and $\zeta_m = e^{\frac{2k_m\pi i}{m}}$ be primitive complex roots of unity of order n and m respectively (k_n and k_m are integers such that $1 \leq k_n \leq n$, $1 \leq k_m \leq m$). Put $z_{k_n} = \sum_{j=0}^{k_n-1} e^{\frac{2j\pi i}{n}}$, $z_{k_m} = \sum_{j=0}^{k_m-1} e^{\frac{2j\pi i}{m}}$ and suppose $u, v \in \mathbb{C}$. If either n or m is not 2 and $|uv| \geq 4|z_{k_n}z_{k_m}|$, or $n = m = 2$ and u or v is non-zero, then the following isomorphisms hold:*

$$\langle \begin{bmatrix} \zeta_n & u \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \zeta_m & 0 \\ v & 1 \end{bmatrix} \rangle \cong C_{i_n} \star C_{i_m} \cong \langle \begin{bmatrix} 1 & u \\ 0 & \zeta_n \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ v & \zeta_m \end{bmatrix} \rangle,$$

where $i_t = t$ if $t \neq 1$ and $i_1 = \infty$.

Proof. It is clear that $\langle \begin{bmatrix} \zeta_n & u \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \zeta_m & 0 \\ v & 1 \end{bmatrix} \rangle \cong \langle \begin{bmatrix} 1 & 0 \\ u & \zeta_n \end{bmatrix}, \begin{bmatrix} 1 & v \\ 0 & \zeta_m \end{bmatrix} \rangle$. So we only will prove the first isomorphism.

Put $A = \begin{bmatrix} \zeta_n & u \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} \zeta_m & 0 \\ v & 1 \end{bmatrix}$. Clearly, $\langle A \rangle \cong C_{i_n}$ and $\langle B \rangle \cong C_{i_m}$.

We first deal with the case that either n or m is not 2 and $|uv| \geq 4|z_{k_n} z_{k_m}|$. Suppose first that $k_n = k_m = 1$ and thus $1 = z_{k_n} = z_{k_m}$. By Lemma 2.1 we may assume $|u| \geq 2|z_{k_n}| = 2$ and $|v| \geq 2|z_{k_m}| = 2$. The group $\langle A, B \rangle$ acts via Möbius transformations on $\mathbb{C}$. The Möbius transformations determined by A and B are resprectively:

$$\varphi_A : z \mapsto \zeta_n z + u \quad \text{and} \quad \varphi_B : z \mapsto \frac{\zeta_m z}{vz+1}.$$

One easily verifies that for any positive integer k the following equalities hold:

$$\varphi_A^k(z) = \zeta_n^k z + \sum_{i=0}^{k-1} \zeta_n^i u \quad \text{and} \quad \varphi_B^k(z) = \frac{\zeta_m^k z}{\left(\sum_{i=0}^{k-1} \zeta_m^i\right) vz + 1}.$$

Consider in $\mathbb{C}$ the following regions $P_1 = \{z \in \mathbb{C} \mid |z| < 1\}$ and $P_2 = \{z \in \mathbb{C} \mid |z| > 1\}$ of $\mathbb{C}$. If $z \in P_1$ and $1 \leq k < n$ (or k a positive integer if $n = 1$), then by Lemma 2.2 $|\sum_{i=0}^{k-1} \zeta_n^i| \geq 1$ and hence

$$|\varphi_A^k(z)| \; = \; |\zeta_n^k z + \sum_{i=0}^{k-1} \zeta_n^i u| \; \geq \; |\sum_{i=0}^{k-1} \zeta_n^i u| - |\zeta_n^k z| \; \geq \; |u| - |z| \; > \; 1.$$

So, $(\langle A \rangle \backslash \{1\})(P_1) \subseteq P_2$. Similarly one shows that $(\langle B \rangle \backslash \{1\})(P_2) \subseteq P_1$. Lemma 2.3 (here we use that either n or m is not 2) yields that

$$\langle A, B \rangle = \langle A \rangle \star \langle B \rangle \cong C_{i_n} \star C_{i_m}.$$

Next we consider arbitrary ζ_n and ζ_m, for $n \neq 1 \neq m$ (and we still work under the assumption $n \neq 2$ or $m \neq 2$). Clearly,

$$\begin{bmatrix} e^{\frac{2\pi i}{n}} & z_{k_n}^{-1} u \\ 0 & 1 \end{bmatrix}^{k_n} = A \quad \text{and} \quad \begin{bmatrix} e^{\frac{2\pi i}{m}} & 0 \\ z_{k_m}^{-1} v & 1 \end{bmatrix}^{k_m} = B.$$

Because $|z_{k_n}^{-1} u z_{k_m}^{-1} v| \geq \left| \frac{4|z_{k_n} z_{k_m}|}{z_{k_n} z_{k_m}} \right| = 4$, the conditions for the first part of the proof are satisfied for the matrices $\begin{bmatrix} e^{\frac{2\pi i}{n}} & z_{k_n}^{-1} u \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} e^{\frac{2\pi i}{m}} & 0 \\ z_{k_m}^{-1} v & 1 \end{bmatrix}$. Hence, they generate a group isomorphic to $C_{i_n} \star C_{i_m}$. Since k_n and k_m are coprime to n and m respectively, $\langle A, B \rangle = \langle \begin{bmatrix} e^{\frac{2\pi i}{n}} & z_{k_n}^{-1} u \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} e^{\frac{2\pi i}{m}} & 0 \\ z_{k_m}^{-1} v & 1 \end{bmatrix} \rangle$ and thus the result follows in this case.

The case where $n = m = 2$ has a more direct proof. Indeed, in this case $A = \begin{bmatrix} -1 & u \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ v & 1 \end{bmatrix}$, and these are elements of order 2. Also, $B^{-1}(AB)B = BABB = BA = (AB)^{-1}$, showing that B acts on AB by inversion. So, $\langle A, B \rangle$ is the infinite dihedral group and thus isomorphic with $C_2 \star C_2$. $\square$

The following lemma is an easy consequence of the proposition but it is essential for the remainder of the paper.

Lemma 2.5. *We use notation as in Proposition* 2.4. *Let r be a positive integer different from* 2. *Suppose $A = (A_{ij}) \in \mathrm{GL}_r(\mathbb{C})$ is a lower triangular matrix of order i_n with $A_{11} = 1$ and $A_{22} = \zeta_n$ and $B = D + dE_{12} \in \mathrm{GL}_r(\mathbb{C})$ a matrix of order*

i_m *with* D *a diagonal matrix,* $D_{11} = 1$ *and* $D_{12} = \zeta_m$*. If* $|A_{21}d| \geq 4|z_{k_n} z_{k_m}|$*, then* $\langle A, B\rangle \cong C_{i_n} \star C_{i_m}$*.*

Proof. Let $L_r = \{(a_{ij}) \in GL_r(\mathbb{C}) \mid a_{ij} = 0 \text{ if } j > i \text{ and } j > 2\}$, a subgroup of $GL_r(\mathbb{C})$. Obviously the map $R : L_r \to GL_2(\mathbb{C})$ defined by $(a_{ij}) \mapsto \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is a group homomorphism. Clearly, A and B are in L_r. Also, by the assumptions, $R(A) = \begin{bmatrix} 1 & 0 \\ A_{21} & \zeta_n \end{bmatrix}$ and $R(B) = \begin{bmatrix} 1 & d \\ 0 & \zeta_m \end{bmatrix}$. The assumption $|A_{21}d| \geq 4|z_{k_n} z_{k_m}|$ and Proposition 2.4 yield that $\langle R(A), R(B)\rangle \cong C_{i_n} \star C_{i_m}$. Since A has order i_n and B has order i_m we obtain that $\langle A, B\rangle \cong C_{i_n} \star C_{i_m}$. $\square$

3. Solvable subgroups and free sub-semigroups

In this section we first construct subgroups of $\mathcal{U}(\mathbb{Z}G)$ that are abelian-by-finite and solvable of length 2. We will give explicit generators for such groups; the construction of these generators is a generalization of the bicyclic units (seen from another perspective, they are products of a bicyclic unit with a trivial unit). Modifying the bicyclic units differently, we next will construct solvable-by-finite subgroups of $\mathcal{U}(\mathbb{Z}G)$ that are not nilpotent-by-finite. By the well-known result of Rosenblatt [15] such groups contain a free submonoid of rank 2. Actually, we give explicit generators of such monoids.

We begin by recalling some definitions and notation (we use the same notation as in [10]). The bicyclic units in $\mathbb{Z}G$ are the unipotent units of the type

$$b(g, \tilde{h}) = 1 + (1-h)g\tilde{h} \quad \text{and} \quad b(\tilde{h}, g) = 1 + \tilde{h}g(1-h),$$

where $g, h \in G$. These units are non-trivial (i.e. they do not belong to G) if $g \notin N_G(\langle h\rangle)$, the normalizer of $\langle h\rangle$ in G. The Bass units are the units of the type

$$u_{k,m}(g) = (1 + g + \cdots + g^{k-1})^m + \frac{1-k^m}{o(g)}\tilde{g},$$

where $g \in G$ and k, m are positive integers such that $k^m \equiv 1 \bmod o(g)$, and $1 \leq k < n$. In [1] V. Bovdi introduced the following beautiful new units in $\mathbb{Z}G$ by modifying the bicyclic unit construction and as such constructed units that are often periodic units:

$$b_k(g, \tilde{h}) = h^k + (1-h)g\widetilde{h} \quad \text{and} \quad b_k(\tilde{h}, g) = h^k + \widetilde{h}g(1-h),$$

with $g, h \in G$ and k a positive integer. Clearly $b_{o(h)}(g, \tilde{h}) = b(g, \tilde{h})$, $b_{o(h)}(\tilde{h}, g) = b(\tilde{h}, g)$, $b_k(g, \tilde{h}) = h^k b(h^{-k}g, \tilde{h})$ and $b_k(\tilde{h}, g) = h^k b(\tilde{h}, h^{-k}g) = h^k b(\tilde{h}, g)$. So, again these units are non-trivial precisely when g does not belong to $N_G(\langle h\rangle)$. We call these units the *Bovdi units.* Also, as remarked in Problem 4 in [8], if a unit

$$b_k(g, \tilde{h}) = h^k + (h-1)g\widetilde{h}$$

(respectively $b_k(\tilde{h}, g) = h^k + \widetilde{h}g(h-1)$) is of finite order, then it is rationally conjugate to h^k. This easily follows from Lemma 37.6 in [16], which says that two elements of $\mathcal{U}(\mathbb{Z}G)$ of the same finite order are rationally conjugate if all irreducible representations of G coincide on both elements. We recall a lemma from [1] where it is shown when a Bovdi unit is of finite order. For the sake of completeness a proof is included.

Lemma 3.1. *Let $g, h \in G$ and suppose that $g \notin N_G(\langle h \rangle)$. Suppose m is the smallest positive integer such that $g \in N_G(\langle h^m \rangle)$. For an integer $1 \leq k < o(h)$, the elements $b_k(g, \tilde{h})$ and $b_k(\tilde{h}, g)$ are units in $\mathbb{Z}G$ and*

(1) if $(k, m) = 1$, then $o(b_k(g, \tilde{h})) = o(b_k(\tilde{h}, g)) = o(h^k)$,
(2) else both $b_k(g, \tilde{h})$ and $b_k(\tilde{h}, g)$ have infinite order.

Proof. Recall that for a positive integer t we have

$$b_k(g, \tilde{h})^t = (h^k)^t + \left(\sum_{i=0}^{t-1} (h^k)^i \right) (1-h) g \tilde{h}.$$

Because $g \notin \langle h \rangle$, we have that $(h^k)^t \notin \mathrm{Supp}(\left(\sum_{i=0}^{t-1} (h^k)^i \right) (1-h) g \tilde{h})$ and thus $(h^k)^t \in \mathrm{Supp}(b_k(g, \tilde{h})^t)$. In particular, if $b_k(g, \tilde{h})$ is torsion, then $(h^k)^{o(b_k(g, \tilde{h}))} = 1$ and $o(h^k) \mid o(b_k(g, \tilde{h}))$.

Note that the minimality assumption on m implies that $m | o(h)$. A straightforward calculation then yields

$$\begin{aligned} (b_k(g, \tilde{h}))^{o(h^k)} &= (h^k)^{o(h^k)} + \left(\sum_{i=0}^{o(h^k)-1} (h^k)^i \right) (1-h) g \tilde{h} \\ &= 1 + t \left(\sum_{i=0}^{\frac{m}{(k,m)}-1} (h^{(k,m)})^i \right) (1-h) g \tilde{h}, \end{aligned} \tag{3.1}$$

for some positive integer t.

To prove part (1), assume $(k, m) = 1$. Since $g \in N_G(\langle h^m \rangle)$, we then get that $\left(\sum_{i=0}^{\frac{m}{(k,m)}-1} (h^{(k,m)})^i \right) (1-h) g \tilde{h} = (1-h^m) g \tilde{h} = 0$. Hence, $(b_k(g, \tilde{h}))^{o(h^k)} = 1$ and thus $o(b_k(g, \tilde{h})) | o(h^k)$. So, by the above $o(b_k(g, \tilde{h})) = o(h^k)$. This proves part (1).

To prove part (2), assume $(k, m) \neq 1$. We give a proof by contradiction. So suppose $b_k(g, \tilde{h})$ has finite order. By the first part of the proof,

$$1 = (h^k)^{o(h^k)} \in \mathrm{Supp}(b_k(g, \tilde{h})^{o(h^k)}).$$

The Berman-Higman Theorem therefore yields that $(b_k(g, \tilde{h}))^{o(h^k)} = 1$. So, by (3.1), $\left(\sum_{i=0}^{\frac{m}{(k,m)}-1} (h^{(k,m)})^i \right) (1-h) g \tilde{h} = 0$. Thus, $g \in N_G(\langle h^{(k,m)i+1} \rangle)$ for some $0 \leq i < \frac{m}{(k,m)}$; in contradiction with the minimality of m. This proves part (2) for $b_k(g, \tilde{h})$. The proof for $b_k(\tilde{h}, g)$ is similar. $\square$

Proposition 3.2. *Let G be a finite group and $g, h \in G$. Let $u = b_k(g, \tilde{h})$ be a Bovdi unit and $w = b(g, \tilde{h})$ a bicyclic unit. Then, the group $\langle u, u^w \rangle$ is abelian-by-finite and solvable of length at most 2. Similarly, if $b_k(\tilde{h}, g)$ is a Bovdi unit and $v = b(\tilde{h}, g)$, then $\langle b_k(\tilde{h}, g), (b_k(\tilde{h}, g))^v \rangle$ is an abelian-by-finite (and solvable) group.*

Proof. We prove the first part. Put $n = o(h)$. Write the Pierce decomposition of $\mathbb{Q}G$ with respect to the non-central idempotent $e = \widehat{h}$ in a natural matrix form as follows:

$$\mathbb{Q}G = \begin{bmatrix} (1-e)\mathbb{Q}G(1-e) & (1-e)\mathbb{Q}Ge \\ e\mathbb{Q}G(1-e) & e\mathbb{Q}Ge \end{bmatrix}.$$

Note that $u = wh^k$ and $u^w = h^k w$,

$$w = \begin{bmatrix} 1-e & (1-h)nge \\ 0 & e \end{bmatrix} \quad \text{and} \quad h^k = \begin{bmatrix} h^k(1-e) & 0 \\ 0 & e \end{bmatrix}.$$

Hence

$$u = \begin{bmatrix} h^k(1-e) & (1-h)nge \\ 0 & e \end{bmatrix} \quad \text{and} \quad u^w = \begin{bmatrix} h^k(1-e) & h^k(1-h)nge \\ 0 & e \end{bmatrix}.$$

So, $\langle u, u^w \rangle$ is a subgroup of $\begin{bmatrix} \langle h \rangle(1-e) & (1-e)\mathbb{Q}Ge \\ 0 & e \end{bmatrix} = H$. Clearly, this group H contains the abelian group $N = \begin{bmatrix} 1-e & (1-e)\mathbb{Q}Ge \\ 0 & e \end{bmatrix}$ as a normal subgroup and $H/N \cong \langle h \rangle$. So, H, and thus also $\langle u, u^w \rangle$, is an abelian-by-finite group. The result follows. □

Note that the group constructed in the previous proposition is finite if the Bovdi unit is trivial. Furthermore it is infinite cyclic if $h^k = 1$.

The proposition implies that $\langle u, u^w \rangle$ does not contain a free group or free monoid (since nilpotent-by-finite groups have polynomial growth) if u is not a trivial Bovdi unit and $h^k \neq 1$. In particular $\langle u, u^w \rangle \not\cong C_t \star C_t$ for $t \geq 3$ or $t = \infty$ since otherwise it would contain $\langle uu^w, u^w u \rangle$, a free group of rank 2. We point this out due to [1] where it is asserted that $\langle u, u^w \rangle \cong C_t \star C_t$. However in the case $o(h) = 2$ and k is odd, then $\langle u, u^w \rangle \cong C_2 \star C_2$. Indeed, if $o(h) = 2$, then by Lemma 3.1 also $o(u^w) = o(u) = 2$. Moreover, $uu^w = wh^{2k}w = w^2$ has infinite order. Since $(u^w)^{-1}(uu^w)u^w = u^w u = (uu^w)^{-1}$ we get that $\langle u, u^w \rangle = \langle uu^w, u^w \rangle \cong \mathbb{Z} \rtimes C_2 \cong C_2 \star C_2$ as claimed.

In order to construct free monoids in $\mathcal{U}(\mathbb{Z}G)$ we generalize the Bovdi units via the use of an arbitrary unit in $\mathbb{Z}\langle h \rangle$ (instead of h^k). More precisely, for $g, h \in G$ and $u(h) \in \mathcal{U}(\mathbb{Z}\langle h \rangle)$ define

$$b(u(h), g, \tilde{h}) = u(h) + (1-h)g\tilde{h} \quad \text{and} \quad b(u(h), \tilde{h}, g) = u(h) + \tilde{h}g(1-h).$$

Clearly, $b(u(h), g, \tilde{h}) = u(h)(1 + (1-h)(u(h))^{-1}g\tilde{h})$ and thus it is a unit. Similarly, $b(u(h), \tilde{h}, g)$ is a unit. We now show that the $\mathbb{Q}$-algebra generated by h and $a = (1-h)g\tilde{h}$ is contained in a (generalized) upper triangular matrix algebra. By a theorem of Perlis and Walker, $\mathbb{Q}\langle h \rangle \cong \prod_{d|o(h)} \mathbb{Q}(\zeta_d)$, where ζ_d denotes a primitive d-th-root of unity. Thus, there exists a primitive idempotent $f \in \mathbb{Q}\langle h \rangle$ such that $\mathbb{Q}\langle h \rangle f \cong \mathbb{Q}(\zeta_n)$, with $n = o(h)$. Note that $a^2 = 0$ and $au = \omega(u)a$ for any $u \in \mathbb{Q}\langle h \rangle$. An easy computation shows that the map

$$\varphi \;:\; \mathbb{Q}\langle h \rangle \oplus \mathbb{Q}\langle h \rangle a \to \begin{bmatrix} \mathbb{Q}(\zeta_n) & \mathbb{Q}(\zeta_n) \\ 0 & \mathbb{Q} \end{bmatrix}, \tag{3.2}$$

defined by

$$u_1 + u_2 a \mapsto \begin{bmatrix} u_1 f & u_2 f \\ 0 & \omega(u_1) \end{bmatrix}$$

is a $\mathbb{Q}$-algebra morphism. Hence, if $u(h)$ is a unit of $\mathbb{Z}\langle h \rangle$ of augmentation 1, then $\varphi(b(u(h), g, \tilde{h}))$ is a matrix of the type $\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$, with $x, y \in \mathbb{Q}(\zeta_n)$.

In order to show that two specific matrices of such a type generate a free monoid, we need, for a field K (for our purposes it is sufficient to consider the case that

$K = \mathbb{C}$), a criterion when two elements of the group of affine transformations of the K-line

$$\mathbb{A}(K) = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \mid x \in K^{\times}, y \in K \right\},$$

generate a free monoid. This is stated in the following free monoid variant of the Ping-Pong Lemma (see for example [2, Lemma 2.1]). Note that there are essentially two types of transformations–those with $x = 1$, a translation which has no fix-points, and those with $x \neq 1$, a transformation with fix-point $\frac{y}{1-x}$–and this can be seen as a homothety about this point with scaling factor x.

Lemma 3.3. (Ping-Pong Lemma for Monoids). *If $A, B \in \mathbb{A}(\mathbb{C})$ are homotheties with different fixed points, have respective scaling factors x and y and $|x|, |y| \leq \frac{1}{3}$, then A and B generate a free monoid of rank 2.*

Actually the lemma is valid in the more general context of the affine group $\mathbb{A}(K)$ over a (non-) archimedean local field K. In case of a non-archimedean field K the condition on the scaling factors has to be replaced by $|x|, |y| < 1$.

The following result is stated for finite groups. It is clear from the proof that it remains valid for arbitrary groups G provided H is a finite subgroup of G.

Theorem 3.4. *Let H be a subgroup of a finite group G. Suppose $h \in H$ with $o(h) = n$ and assume $\alpha \in \mathbb{Z}G$ is such that $s = 1 + (1-h)\alpha\widetilde{H} \neq 1$. Let ζ be a primitive n-th root of unity. Suppose $b_1 = u_{k_1,m_1}(h)$ and $b_2 = u_{k_2,m_2}(h)$ are two non-trivial Bass units (so, $1 < k_1, k_2 < n-1$, $(k_1, n) = (k_2, n) = 1$, $k_1^{m_1} \equiv 1 \bmod n$ and $k_2^{m_2} \equiv \bmod n$). If, for $i \in \{1, 2\}$,*

$$m_i \geq \log_{\left|\frac{\zeta^{k_i}-1}{\zeta-1}\right|} 3 \quad \textit{and} \quad \left(\frac{\zeta^{k_1}-1}{\zeta-1}\right)^{m_1} \neq \left(\frac{\zeta^{k_2}-1}{\zeta-1}\right)^{m_2},$$

then

$$\{b_1 + (1-h)\alpha\widetilde{H}, b_2 + (1-h)\alpha\widetilde{H}\} \qquad \textit{and} \qquad \{b_1 s, b_2 s\}$$

generate free monoids of rank 2 that are contained in a solvable group.

In particular, $\langle b(u_{k_1,m_1}(h), g, \tilde{h}), b(u_{k_2,m_2}(h), g, \tilde{h})\rangle$ is a free monoid of rank 2 if $g \notin N_G(\langle h \rangle)$.

Proof. Put $a = (1-h)\alpha\widetilde{H}$. Then, $a^2 = 0$ and $a\beta = \omega(\beta)a$ for all $\beta \in \mathbb{Q}H$. Let $f \in \mathbb{Q}\langle h \rangle$ be a primitive central idempotent such that $\mathbb{Q}\langle h \rangle f \cong \mathbb{Q}(\zeta)$. Again, as in (3.2) we have a $\mathbb{Q}$-algebra morphism $\varphi : \mathbb{Q}\langle h \rangle \oplus \mathbb{Q}\langle h \rangle a \to \begin{bmatrix} \mathbb{Q}(\zeta) & \mathbb{Q}(\zeta) \\ 0 & \mathbb{Q} \end{bmatrix}$ with $u_1 + u_2 a \mapsto \begin{bmatrix} u_1 f & u_2 f \\ 0 & \omega(u_1) \end{bmatrix}$. Since $b_i f = \mu_{k_i,m_i}(\zeta) = \left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{m_i}$ and $\omega(b_i) = 1$ we obtain that

$$\varphi(b_i + a) = \begin{bmatrix} \left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{m_i} & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \varphi(b_i s) = \begin{bmatrix} \left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{m_i} & \left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{m_i} \\ 0 & 1 \end{bmatrix}.$$

The inverses of these images are

$$\begin{bmatrix} \left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{-m_i} & -\left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{-m_i} \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{-m_i} & -1 \\ 0 & 1 \end{bmatrix}$$

respectively. As elements of $\mathbb{A}(\mathbb{C})$ they have respective fixed points

$$f_i = \frac{-\left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{-m_i}}{1-\left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{-m_i}} = \frac{-1}{\left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{m_i}-1} \quad \text{and} \quad g_i = \frac{-1}{1-\left(\frac{\zeta^{k_i}-1}{\zeta-1}\right)^{-m_i}}.$$

By assumption, $f_1 \neq f_2$ and $g_1 \neq g_2$. Moreover, from the assumption that $m_i \geq \log_{\left|\frac{\zeta^{k_i}-1}{\zeta-1}\right|} 3$, we know that $\left|\frac{\zeta^{k_i}-1}{\zeta-1}\right|^{-m_i} \leq 3^{-1}$. Therefore, by Lemma 3.3, the homotheties $\varphi(b_1+a)^{-1}$ and $\varphi(b_2+a)^{-1}$, respectively $\varphi(b_1 s)^{-1}$ and $\varphi(b_2 s)^{-1}$, generate a free monoid (and thus also $\varphi(b_1+a)$ and $\varphi(b_2+a)$, respectively $\varphi(b_1 s)$ and $\varphi(b_2 s)$). Hence, $\{b_1+a, b_2+a\}$ and $\{b_1 s, b_2 s\}$ generate free monoids as well. Note that these monoids are contained in a solvable group. $\square$

We include a couple of remarks on the assumptions concerning m_1 and m_2. The restrictions on m_i are clearly satisfied if one takes $k_1 \neq k_2$ arbitrary (and keeping the requirement that the Bass units are non-trivial) and $m_1 = m_2 = m$ large enough. The latter is allowed as one may replace the Bass units by powers because $u_{k,m}(g)u_{k,n}(g) = u_{k,m+n}(g)$.

Also note that for the restriction $m_i \geq \log_{\left|\frac{\zeta^{k_i}-1}{\zeta-1}\right|} 3$ to be fulfilled it is necessary that $\left|\frac{\zeta^{k_i}-1}{\zeta-1}\right| \neq 1$. Because of Lemma 2.2 this is equivalent to $k_i \neq \pm 1 \bmod |g|$ (i.e. the Bass units constructed are non-trivial).

4. Free product of cyclic groups

In this section we will give an explicit construction via Bovdi units of a free product $C_p \star C_p$ in the unit group of the integral group ring of a finite nilpotent group G. We first deal with groups of class 2. In this case we prove a more general statement.

Theorem 4.1. *Let G be a finite nilpotent group of class 2 and let $g, h \in G$. Assume $o(h) = p^n$, with p a prime number, and $g \notin N_G(\langle h^{p^i}\rangle)$ for all $0 \leq i < n$. Then, for any $1 \leq l, t \leq p^n$,*

$$\langle b_l(g, \widetilde{h}), b_t(\widetilde{h}, g^{-1})\rangle \cong C_{n_l} \star C_{n_t} \cong \langle b_l(g, \widetilde{h}), b_t(g, \widetilde{h})^{\star}\rangle,$$

a free product of cyclic groups, where $n_l = o(b_l(g, \widetilde{h}))$ and $n_t = o(b_t(\widetilde{h}, g^{-1}))$ (see Lemma 3.1).

Proof. Without loss of generality we may assume that $G = \langle g, h\rangle$. Since G has nilpotency class 2, $c = [g, h^{-1}]$ is central and has p-power order, say p^m with $m \leq n$ (and similarly $o(c) \leq o(g)$). Clearly, $(h^{p^m})^g = c^{p^m} h^{p^m} = h^{p^m}$ and thus $g \in N_G(\langle h^{p^m}\rangle)$. The assumptions therefore imply that $n \leq m$ and thus $n = m$. So $o(h) = o(c)$ and hence the normalizer assumption on g yields that $\langle h\rangle \cap \langle c\rangle = \{1\}$. So $\langle h, c\rangle = \langle h\rangle \times \langle c\rangle$.

We will now construct a concrete irreducible complex representation of G so that the proposed Bovdi units will be represented by matrices to which Lemma 2.5 can be applied. To do so, first note that if $g^i h^j \in \mathcal{Z}(G)$, then $1 = [g, g^i h^j] = [g, g^i][g, h^j] = [g, h]^j = c^{-j}$ and $1 = [h, g^i h^j] = [h, g^i]^{h^j}[h, h^j] = [h, g]^i = c^i$. Because $o(h) = o(c)$ this implies that $\mathcal{Z}(G) = \langle g^{o(c)}, c\rangle$ and $G/\mathcal{Z}(G) = \langle \overline{g}\rangle \times \langle \overline{h}\rangle \cong C_{o(c)} \times C_{o(c)}$.

Since $\mathcal{Z}(G)$ is a 2-generated abelian group with $o(c)$ a p-power, there is an isomorphism $\varphi : \mathcal{Z}(G) \to C_{p^\alpha} \times C_k$, for some non-negative integers α and k. Without loss of generality, we may choose α and k such that $\varphi(c) = (c_\alpha, c_\beta)$ and $o(c) = o(c_\alpha)$. Set $K = \varphi^{-1}(1 \times C_k)$, a subgroup of $\mathcal{Z}(G)$. Then $\langle c \rangle$ embeds faithfully in $\mathcal{Z}(G)/K \cong C_{p^\alpha}$. Let H be a subgroup of $\mathcal{Z}(G)$ that is minimal for properly containing K. It is well known and easily verified that $\varepsilon = \hat{K} - \hat{H}$ is a primitive idempotent of $\mathbb{Q}\mathcal{Z}(G)$ and $\mathbb{Q}\mathcal{Z}(G)\varepsilon \cong \mathbb{Q}(\zeta_{p^\alpha})$ (see for example Lemma 3.3.2 in [10]). Under this isomorphism c is mapped onto the primitive $p^{o(c)}$-th root of unity $\zeta_{p^{o(c)}}$.

We next show that $\mathbb{Q}G\varepsilon$ is a simple algebra. This follows at once from the description of primitive central idempotents in strongly monomial groups; for example nilpotent groups (Section 3.5 in [10]). However, in this case this can be shown easily. To do so, write $\mathbb{Q}G\varepsilon = \sum_{t\in T} \mathbb{Q}\mathcal{Z}(G)\varepsilon t$, with T a transversal of $\mathcal{Z}(G)$ in G. Let $z = \sum_{t\in T} \alpha_t \varepsilon t \in \mathcal{Z}(\mathbb{Q}G\varepsilon)$, with each $\alpha_t \in \mathbb{Q}\mathcal{Z}(G)\varepsilon$. The centrality of z means that $\sum_{t\in T} \alpha_t\varepsilon t = (\sum_{t\in T} \alpha_t t)^s = \sum_{t\in T} (\alpha_t t)^s = \sum_{t\in T} \alpha_t t^s = \sum_{t\in T} \alpha_t [s, t^{-1}]t$ for all $s \in T$. Since $[s, t^{-1}] \in \mathcal{Z}(G)$ and because $\mathbb{Q}\mathcal{Z}(G)\varepsilon$ is a field, we obtain that $\alpha_t t\varepsilon = \alpha_t[s, t^{-1}]t$ for all $s, t \in T$. If $t \notin \mathcal{Z}(G)$, then there exists $s \in T$ so that $\varepsilon \neq [s, t^{-1}]\varepsilon$. Hence, $\alpha_t = 0$ if $t \notin \mathcal{Z}(G)$. So, $\mathcal{Z}(\mathbb{Q}G\varepsilon) = \mathbb{Q}\mathcal{Z}(G)\varepsilon \cong \mathbb{Q}(\zeta_{p^\alpha})$, a field. Thus the semisimple algebra $\mathbb{Q}G\varepsilon$ indeed is simple and has center isomorphic to $\mathbb{Q}(\zeta_{p^\alpha})$.

Because $[G : \mathcal{Z}(G)] = o(c)^2$ we get that $\mathbb{Q}G\varepsilon = M_{o(c)}(\mathbb{Q}(\zeta_{p^\alpha}))$, a matrix ring of degree $o(c)$. In order to describe explicitly this representation, we first note that the following non-zero elements:

$$E_{ii} = \widehat{h^{g^{i-1}}}\varepsilon,$$

with $1 \leq i \leq o(c)$, form a complete set of orthogonal primitive idempotents of this matrix ring. For this it is sufficient to show the orthogonality and this follows from the fact that if $1 \leq j, i \leq o(c)$ with $i \neq j$, then $o(c^{i-j}) | o(c^{i-1}h) = o(c)$, $\widehat{c^{i-j}}\varepsilon = 0$ and thus

$$\begin{aligned}
E_{ii}E_{jj} &= \widehat{h^{g^{i-1}}}\varepsilon\, \widehat{h^{g^{j-1}}}\varepsilon = \widehat{c^{i-1}h}\, \widehat{c^{j-1}h}\varepsilon \;=\; c^{i-j}\widehat{(c^{j-1}h)}\;\; \widehat{c^{j-1}h}\varepsilon \\
&= \frac{1}{o(c)} \sum_{k=0}^{o(c)-1} ((c^{i-j})^k (c^{j-1}h)^k)\;\; \widehat{c^{j-1}h}\varepsilon \\
&= \frac{1}{o(c)} \sum_{k=0}^{o(c)-1} (c^{i-j})^k \;\; \widehat{c^{j-1}h}\varepsilon \\
&= \widehat{c^{i-j}}\varepsilon\, \widehat{c^{j-1}h}\varepsilon \\
&= 0.
\end{aligned}$$

We present some arithmetic concerning these idempotents.

(1) $hE_{ii} = E_{ii}h$ and $hE_{11} = E_{11}$.
(2) $E_{ii}g = \widehat{h^{g^{i-1}}}\varepsilon g = g\widehat{h^{g^i}}\varepsilon = gE_{i+1,i+1}$, where the indices are taken modulo $o(c)$.
(3) $hE_{ii} = hg^{-(i-1)}g^{i-1}E_{ii} = g^{-(i-1)}c^{i-1}hE_{11}g^{i-1} = c^{i-1}g^{-(i-1)}E_{11}g^{i-1} = c^{i-1}E_{ii}$.

Now, for any $1 \leq i, j \leq o(c)$, put

$$E_{ij} = E_{ii} g^{j-i} E_{jj}.$$

Then, $E_{ij}E_{ji} = E_{ii}g^{j-i}E_{jj}E_{jj}g^{i-j}E_{ii} = E_{ii}g^{j-i}g^{i-j}E_{ii} = E_{ii}$. Hence, $\{E_{ij} \mid 1 \leq i, j \leq o(c)\}$ is a complete set of matrix units of the matrix ring $\mathbb{Q}G\varepsilon = M_{o(c)}(\mathbb{Q}(\zeta_{p^\alpha}))$.

With respect to these matrix units we will now represent the elements $u = b_l(g, \widetilde{h})\varepsilon$ and $v = b_t(\widetilde{h}, g^{-1})\varepsilon$ as matrices (the calculations for $\langle b_l(g, \widetilde{h}), b_t(g, \widetilde{h})^\star \rangle$ are similar, but are left to the reader as an exercise). The (i, j)-th position in the matrix of the representation of u is determined as follows:

$$\begin{aligned} E_{ii}uE_{jj} &= E_{ii}(h^l + (1-h)g\widetilde{h})E_{jj} = h^l E_{ii}E_{jj} + (1-h)E_{ii}g\widetilde{h}E_{jj} \\ &= h^l E_{ii}E_{jj} + (1-h)g\widetilde{h}E_{i+1,i+1}E_{jj}. \end{aligned}$$

So, if $i = j$, then $E_{ii}uE_{ii} = h^l E_{ii}$ and thus $E_{11}uE_{11} = h^l E_{11} = E_{11}$. On the other hand, if $i + 1 = j$, then

$$E_{ii}uE_{jj} = (1-h)g\widetilde{h}E_{jj} = o(h)(1-h)g\widehat{h}E_{jj} = o(h)(1-h)gE_{11}E_{jj},$$

which is zero if $j \neq 1$. If $i \neq j$ and $i+1 \neq j$, then $E_{ii}uE_{jj} = 0$. This shows that the non-diagonal entries of the matrix representation of u are 0, except the $(o(c), 1)$-position. By the previous calculations, the value at this point is determined as follows:

$$\begin{aligned} E_{o(c),o(c)}uE_{11} &= o(h)(1-h)gE_{11} = o(h)(1-h)E_{o(c),o(c)}gE_{11} \\ &= o(h)(1-c^{-1})E_{o(c),o(c)}gE_{11} \\ &= o(h)(1-c^{-1})E_{o(c),1}. \end{aligned}$$

A similar calculation and reasoning yields for v:

$$E_{ii}vE_{jj} = h^t E_{ii}E_{jj} + \widetilde{h}g^{-1}(1-h)E_{i-1,i-1}E_{jj},$$

which is zero everywhere except on the $(1, o(c))$-position and on the diagonal. Explicitly

$$E_{11}vE_{o(c),o(c)} = o(h)(1-c^{-1})E_{1,o(c)}.$$

Through the explicit morphism to $M_{o(c)}(\mathbb{Q}(\zeta_{p^\alpha}))$ the elements u and v have $o(h)(1-\zeta_{o(c)}^{-1})$ on position $(o(c), 1)$ and $(1, o(c))$ respectively since c is mapped to $\zeta_{o(c)}$. Moreover, position $(o(c), o(c))$ u has value $\zeta_{o(c)}^{-l}$ because

$$h^l E_{o(c),o(c)} = c^{l(o(c)-1)}E_{o(c),o(c)},$$

and v has value $\zeta_{o(c)}^{-t}$. Because $|o(h)(1-\zeta_{o(c)}^{-1})| \geq 2$, these matrices satisfy the conditions for Lemma 2.5, so $\langle u, v\rangle$ has $C_{o(u)} \star C_{o(v)}$ as an epimorphic image. Then also $\langle u, v\rangle \cong C_{o(u)} \star C_{o(v)}$. $\square$

The previous result will be used to prove our main result of this section.

Theorem 4.2. *Let G be a finite nilpotent group, $g, h \in G$ such that $g \notin N_G(\langle h\rangle)$. If $o(h) = p$ (a prime number) and $1 \leq k, l \leq p-1$, then*

$$\langle b_k(g, \tilde{h}), b_l(g, \tilde{h})^*\rangle \cong C_p \star C_p \cong \langle b_k(g, \tilde{h}), b_l(\tilde{h}, g^{-1})\rangle.$$

Conversely, if $\mathcal{U}(\mathbb{Z}G)$ contains a subgroup isomorphic with $C_p \star C_p$, then there exist $g, h \in G$ satisfying the assumptions of the first part of the statement.

Proof. Write $g = g_p x$ with $(o(x), p) = 1$ and let G_p denote the Sylow p-subgroup of G. Since G is nilpotent, $g_p \notin N_{G_p}(\langle h \rangle)$. So, in order to prove the first part of the statement, without loss of generality, we may assume that $G = \langle g, h \rangle$ is a p-group. We prove the result by induction on the nilpotency class of G. Let $u = b_k(g, \tilde{h})$ and $v = b_k(\tilde{h}, g^{-1})$. If the class is 2, then the result holds by Theorem 4.1. So, assume that the class of G is more than 2. Let $\overline{G} = G/\mathcal{Z}(G)$ and denote by $\overline{\alpha}$ the natural image of $\alpha \in \mathbb{Z}G$ in $\mathbb{Z}\overline{G}$. Clearly $\overline{h}$ has order p. Also, $\overline{g} \notin N_{\overline{G}}(\langle \overline{h} \rangle)$. Indeed, otherwise $\langle \overline{h} \rangle$ is a normal subgroup of $\overline{G}$. In particular since $\overline{G}$ is nilpotent, some $\overline{h}^k$ would be central in $\overline{G} = \langle \overline{g}, \overline{h} \rangle = \langle \overline{g}, \overline{h}^k \rangle$. This would imply that $\overline{G}$ is commutative, a contradiction with the fact that G is not of nilpotency degree 2. So, the assumptions are inherited in the group $\overline{G}$. The induction hypothesis yields that $\langle \overline{u}, \overline{v} \rangle \cong C_p \star C_p$. Hence, since u and v have order p, also $\langle u, v \rangle \cong C_p \star C_p$.

A similar proof can be given for the statement $\langle b_k(g, \tilde{h}), b_l(g, \tilde{h})^* \rangle \cong C_p \star C_p$.

For the converse, assume that all cyclic subgroups of G of order p are normal. In this case, Gonçalves and Passman, in [4, Lemma 1.3], have shown that all units of order p in $\mathcal{U}(\mathbb{Z}G)$ are trivial. In particular, $C_p \star C_p$ would not be a subgroup of $\mathcal{U}(\mathbb{Z}(G))$, a contradiction. $\square$

We immediately get the following Marciniak-Seghal type result.

Corollary 4.3. *Let G be a finite nilpotent group, $g, h \in G$ such that $g \notin N_G(\langle h \rangle)$ and $o(h) = p \neq 2$. Then $\langle b_k(g, \tilde{h})\, b_l(g, \tilde{h})^*, b_l(g, \tilde{h})^* b_k(g, \tilde{h}) \rangle$ is a free group of rank 2.*

Also the earlier mentioned result of Gonçalves and Passman is a consequence in case G is a finite nilpotent group.

Corollary 4.4. *Let G be a finite nilpotent group and suppose $h \in G$ is a non-central element of order $p \neq 2$. Then a subgroup isomorphic to $C_p \star C_\infty$ exists in $\mathcal{U}(\mathbb{Z}G)$ and can be explicitly constructed. Moreover there exists a unit $w \in \mathcal{U}(\mathbb{Z}G)$ such that $\langle h, w \rangle \cong C_p \star C_\infty$.*

Proof. Because h is not central and of order p, the subgroup $\langle h \rangle$ is not normal in G. Hence there exists $g \in G$ such that $g \notin N_G(\langle h \rangle)$. So, by Theorem 4.2, $\langle u, u^* \rangle \cong \langle u \rangle \star \langle u^* \rangle \cong C_p \star C_p$ with $u = b_1(g, \tilde{h})$. Clearly,

$$\langle u, u^* u u^* \rangle \cong \langle u \rangle \star \langle u^* u u^* \rangle \cong C_p \star C_\infty.$$

As mentioned earlier, there exists a rational unit v such that $u^v = h$. Since $v^{-1}(\mathbb{Z}G)v$ is a $\mathbb{Z}$-order in $\mathbb{Q}G$, the unit group of this order and $\mathcal{U}(\mathbb{Z}G)$ are commensurable (see for example [10, Lemma 4.6.9]). Hence, for some positive integer m, we get that $((u^* u u^*)^v)^m \in \mathcal{U}(\mathbb{Z}G)$. So $\langle u^v, ((u^* u u^*)^v)^m \rangle = \langle h, (u^* u u^*)^v)^m \rangle \cong C_p \star C_\infty$. Hence, the result follows. $\square$

References

[1] V. Bovdi, *Free subgroups in group rings*, arXiv:1406.6771, 2014, preprint.

[2] Emmanuel Breuillard, *On uniform exponential growth for solvable groups*, Pure Appl. Math. Q. **3** (2007), no. no. 4, Special Issue: In honor of Grigory Margulis., 949–967. MR2402591

[3] Florian Eisele, Ann Kiefer, and Inneke Van Gelder, *Describing units of integral group rings up to commensurability*, J. Pure Appl. Algebra **219** (2015), no. no. 7, 2901–2916. MR3313511

[4] J. Z. Gonçalves and D. S. Passman, *Embedding free products in the unit group of an integral group ring*, Arch. Math. (Basel) **82** (2004), no. no. 2, 97–102. MR2047662

[5] Jairo Z. Gonçalves and Ángel Del Río, *A survey on free subgroups in the group of units of group rings*, J. Algebra Appl. **12** (2013), no. no. 6, 1350004, 28. MR3063443

[6] B. Hartley and P. F. Pickel, *Free subgroups in the unit groups of integral group rings*, Canad. J. Math. **32** (1980), no. 6, 1342–1352. MR604689

[7] Martin Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. (2) **154** (2001), no. no. 1, 115–138. MR1847590

[8] *Mini-Workshop: Arithmetik von Gruppenringen*, Oberwolfach Rep. **4** (2007), no. no. 4, 3209–3239. Abstracts from the mini-workshop held November 25–December 1, 2007; Organized by Eric Jespers, Zbigniew Marciniak, Gabriele Nebe and Wolfgang Kimmerle; Oberwolfach Reports. Vol. 4, no. 4. MR2463649

[9] Eric Jespers and Guilherme Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math. **78** (1993), no. no. 3, 303–315. MR1206159

[10] E. Jespers and Á. del Río, *Group ring groups. Volume 1: Orders and generic constructions of units*, De Gruyter, Berlin, 2016.

[11] E. Jespers and Á. del Río, *Group ring groups. Volume 2: Structure theorems of unit groups*, De Gruyter, Berlin, 2016.

[12] Zbigniew S. Marciniak and Sudarshan K. Sehgal, *Constructing free subgroups of integral group ring units*, Proc. Amer. Math. Soc. **125** (1997), no. no. 4, 1005–1009. MR1376998

[13] D. S. Passman, *Free products in linear groups*, Proc. Amer. Math. Soc. **132** (2004), no. no. 1, 37–46. MR2021246

[14] Jürgen Ritter and Sudarshan K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. **324** (1991), no. no. 2, 603–621. MR987166

[15] Joseph Max Rosenblatt, *Invariant measures and growth conditions*, Trans. Amer. Math. Soc. **193** (1974), 33–53. MR0342955

[16] S. K. Sehgal, *Units in integral group rings*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 69, Longman Scientific and Technical, Harlow; copublished in the United States with John Wiley and Sons, Inc., New York, 1993. With an appendix by Al Weiss. MR1242557

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Elsene, Belgium

E-mail address: Geoffrey.Janssens@vub.be

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Elsene, Belgium

E-mail address: Eric.Jespers@vub.be

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Elsene, Belgium

E-mail address: Doryan.Temmerman@vub.be