

# BASS CYCLIC UNITS AS FACTORS IN A FREE GROUP IN INTEGRAL GROUP RING UNITS

JAIRO Z. GONÇALVES AND ÁNGEL DEL RÍO

ABSTRACT. Marciniak and Sehgal showed that if  $u$  is a non-trivial bicyclic unit of an integral group ring then there is a bicyclic unit  $v$  such that  $u$  and  $v$  generate a non-abelian free group. A similar result does not hold for Bass cyclic units of infinite order based on non-central elements as some of them have finite order modulo the centre. We prove a theorem that suggests that this is the only limitation to obtain a non-abelian free group from a given Bass cyclic unit. More precisely, we prove that if  $u$  is a Bass cyclic unit of an integral group ring  $\mathbb{Z}G$  of a solvable and finite group  $G$ , such that  $u$  has infinite order modulo the centre of  $U(\mathbb{Z}G)$  and it is based on an element of prime order, then there is a non-abelian free group generated by a power of  $u$  and a power of a unit in  $\mathbb{Z}G$  which is either a Bass cyclic unit or a bicyclic unit.

## 1. INTRODUCTION

Let  $\mathbb{Z}G$  be the integral group ring of the finite group  $G$  over the ring of integers  $\mathbb{Z}$ , and let  $U(\mathbb{Z}G)$  be its group of units. Given  $a \in G$  of order  $d$  and  $k$  and  $m$  positive integers such that  $k^m \equiv 1 \pmod{d}$ , the following is a unit in  $\mathbb{Z}G$ :

$$u_{k,m}(a) = (1 + a + \cdots + a^{k-1})^m + \frac{1 - k^m}{d} (1 + a + \cdots + a^{d-1}).$$

The elements of this form are called Bass cyclic units based on  $a$  and were introduced by Bass in [1]. Recall that the elements of the form

$$1 + (1 - a)g (1 + a + \cdots + a^{d-1}),$$

with  $a$  as above and  $g \in G$ , are also units in  $\mathbb{Z}G$  known as bicyclic units. These two types of units have an important role in  $U(\mathbb{Z}G)$  because for many groups the group generated by all the Bass cyclic units and bicyclic units has finite index in  $U(\mathbb{Z}G)$  [1, 11, 14, 16].

Hartley and Pickel [10] proved that if  $G$  is a finite group then  $U(\mathbb{Z}G)$  is either finite, or abelian or contains a non-abelian free group. The proof of this result is not constructive and this raised the question of giving concrete constructions of non-abelian free subgroups of  $U(\mathbb{Z}G)$ . This goal was reached, using either bicyclic or Bass cyclic units, by combining results of Marciniak and Sehgal [13] and Ferraz [3]. Other constructions of free groups in  $U(\mathbb{Z}G)$  using either Bass cyclic units or bicyclic units can be founded in [2, 6, 7, 8, 12] and [15].

If  $u$  is a non-trivial bicyclic unit then  $\langle u, u^* \rangle$  is a non-abelian free group, where  $-^*$  is the classical involution of  $\mathbb{Z}G$  [13]. However not every non-trivial Bass cyclic

---

2000 *Mathematics Subject Classification.* 20C05, 16S34.

The first author has been partially supported by Grant CNPq 303.756/82-5, and Fapesp Brazil, Proj. Tematico 00/07.291-0 and the second author by the Ministerio de Ciencia y Tecnología of Spain and Fundación Séneca of Murcia.

unit over a non-abelian group is an element of a non-abelian free subgroup of  $U(\mathbb{Z}G)$ . For example, if  $G$  is the dihedral group of order  $2p$ , with  $p$  and odd prime, then all the Bass cyclic units of  $U(\mathbb{Z}G)$  are finite modulo the centre of  $U(\mathbb{Z}G)$  (see Lemma 2.1). In this paper we prove a theorem which suggests that this is basically the only obstacle to construct a non-abelian free group in  $U(\mathbb{Z}G)$  from a given Bass cyclic unit. More precisely in this paper we address the following conjecture which is a natural outgrowth of the result of [6], [7] and [8].

**Conjecture.** Let  $G$  be a finite group. Let  $u$  be a Bass cyclic unit based on a non-central element of prime order. If  $u$  has infinite order modulo the centre of  $U(\mathbb{Z}G)$  then  $\mathbb{Z}G$  contains a Bass cyclic unit or a bicyclic unit  $v$  such that  $\langle u^n, v^n \rangle$  is a non-abelian free group for some integer  $n$ .

Our strategy to attack the conjecture consists in showing that a finite group  $G$  of minimal order for which the conjecture does not hold should satisfy some strong conditions on  $G$ . More precisely, we prove that such a minimal counterexample should be simple. This implies the conjecture for solvable groups. Formally we have

**Main Theorem.** Let  $G$  be a solvable and finite group and let  $a$  be a non-central element of  $G$  of prime order. If  $u$  is a Bass cyclic unit of infinite order based on  $a$  then  $\mathbb{Z}G$  contains a Bass cyclic unit or a bicyclic unit  $v$  such that  $\langle u^n, v^n \rangle$  is a non-abelian free group for some integer  $n$ .

## 2. SOME SIGNIFICANT EXAMPLES

If a Bass cyclic unit of  $U(\mathbb{Z}G)$  belongs to a non-abelian free subgroup of  $U(\mathbb{Z}G)$  then necessarily it should have infinite order modulo the centre of  $U(\mathbb{Z}G)$ . The following lemma characterizes the Bass cyclic units based on elements of prime order satisfying this condition.

**Lemma 2.1.** *Let  $G$  be a finite group,  $a$  an element of  $G$  of prime order  $p$  and let  $u = u_{k,m}(a)$ . Then the following conditions are equivalent:*

- (1)  $u$  has infinite order modulo the centre of  $U(\mathbb{Z}G)$ .
- (2)  $2 \leq k \leq p-2$  and the conjugacy class of  $a$  in  $G$  is not contained in  $\{a, a^{-1}\}$ .

*Proof.* It is well known that  $u = u_{k,m}(a)$  has infinite order if and only if  $2 \leq k \leq p-2$  (see e.g. [7, Section 3]). Thus we may assume that  $u$  has infinite order, and in particular  $p \geq 5$ . We consider three cases:

*Case 1:  $\langle a \rangle$  is not normal in  $G$ .* Then there is  $b \in G$  such that  $\text{Supp}(u^n) \cap \text{Supp}(bu^n b^{-1}) \subseteq \langle a \rangle \cap \langle bab^{-1} \rangle = 1$ , for every  $n \geq 1$ . Since  $u$  has infinite order we deduce that  $u^n \neq bu^n b^{-1}$  and hence  $u$  has infinite order modulo the centre of  $U(\mathbb{Z}G)$ .

*Case 2:  $\langle a \rangle$  is normal in  $G$  but the conjugacy class of  $a$  in  $G$  is not contained in  $\{a, a^{-1}\}$ .* Then there is  $b \in G$  such that  $a^i = bab^{-1}$  with  $i \not\equiv \pm 1 \pmod{p}$ . Let  $t$  be the order of  $i$  modulo  $p$ . By replacing  $b$  by a suitable power of  $b$  one may assume that  $t$  is either 4 or an odd prime dividing  $p-1$ . Let  $H = \langle a, b \rangle = \langle a \rangle \rtimes \langle b \rangle$  and  $K = \langle a, b^t \rangle$ . Then  $K$  is an abelian normal subgroup of index  $t$  in  $H$  and  $K$  has a linear representation  $\lambda$  with  $\lambda(a) = \zeta$ , a  $p$ -th primitive root of unity. Let  $\rho = \lambda^H$ , the representation of  $H$  induced by  $\lambda$ . Then  $\rho(a) = \text{diag}(\zeta, \zeta^i, \zeta^{i^2}, \dots, \zeta^{i^{t-1}})$ . Using

the formulae in [7, Lemma 3.1], for every  $n \geq 1$  we have

$$\rho(u^n) = \rho(u_{k,nm}(a)) = \text{diag}(u_{k,nm}(\zeta), u_{k,nm}(\zeta^i), u_{k,nm}(\zeta^{i^2}), \dots, u_{k,nm}(\zeta^{i^{t-1}})).$$

By [7, Lemma 3.5], we have  $|u_{k,nm}(\zeta)| \neq |u_{k,nm}(\zeta^i)|$ , since  $i \not\equiv \pm 1 \pmod{p}$ . We deduce that  $\rho(u^n)$  is not central in the image of  $\rho$  and therefore  $u^n$  is not central in  $\mathbb{Z}H$ . In particular  $u$  has infinite order modulo the centre of  $U(\mathbb{Z}G)$ .

*Case 3: The conjugacy class of  $a$  in  $G$  is contained in  $\{a, a^{-1}\}$ .* By Dirichlet Unit Theorem  $U(\mathbb{Z}[\zeta + \zeta^{-1}])$  has finite index in  $U(\mathbb{Z}[\zeta])$ . Let  $n = [U(\mathbb{Z}[\zeta]) : U(\mathbb{Z}[\zeta + \zeta^{-1}])]$ . We claim that  $u^n$  belongs to the centre of  $U(\mathbb{Z}G)$ . To prove this one may assume that  $G = \langle a, b \rangle$  with  $a^b = a^{-1}$ . Then  $H = \langle a, b^2 \rangle$  is an abelian normal subgroup of index 2 in  $G$  and every non-linear irreducible representation  $\rho$  of  $G$  is of the form  $\lambda^G$  for  $\lambda$  a linear representation of  $H$ . If  $\lambda(a) = 1$  then  $\rho(a) = 1$ . Otherwise  $\rho(a) = \text{diag}(\zeta, \bar{\zeta})$  with  $\zeta$  a primitive  $p$ -th root of unity and  $\rho(bab^{-1}) = \text{diag}(\bar{\zeta}, \zeta)$ . Therefore  $\rho(u) = \text{diag}(\alpha, \bar{\alpha})$  for  $\alpha$  a unit in  $\mathbb{Z}[\zeta]$  and  $\rho(bub^{-1}) = \text{diag}(\bar{\alpha}, \alpha)$ . Hence  $\alpha^n \in \mathbb{R}$  for some  $n$  and hence  $\rho(bu^n b^{-1}) = \text{diag}(\bar{\alpha}^n, \alpha^n) = \alpha^n I = \rho(u^n)$ . This shows that  $\rho(u^n)$  is central in  $\rho(\mathbb{Z}G)$ , for every irreducible representation  $\rho$  of  $G$  and hence  $u^n$  is central in  $U(\mathbb{Z}G)$ .  $\square$

Lemma 2.1 suggests the following definition which will be used in the proof of the Main Theorem: For  $a \in G$ , we denote

$$D_G(a) = \{g \in G : a^g \in \{a, a^{-1}\}\}.$$

Note that  $D_G(a)$  is a subgroup of  $G$  and  $[D_G(a) : C_G(a)] \leq 2$ . The group  $D_G(a)$  might be called something like the ‘‘dihedralizer’’ of  $a$  in  $G$ . Lemma 2.1 can be rephrased as follows: A Bass cyclic unit  $u$  based on an element  $a$  of prime order  $p$  has finite order modulo the centre if and only if either it has finite order or  $D_G(a) = G$ .

Now we consider two examples that show why one needs to consider both Bass cyclic and bicyclic units.

**Example 2.2.** Consider the group  $G = A \rtimes \langle b \rangle$ , where  $A$  is a  $p$ -elementary abelian group, with  $p \geq 5$  prime and  $b$  has order 3, acting faithfully and irreducibly on  $A$ . If  $g \in G \setminus A$  then  $g^3 \in A \cap Z(G) = 1$  and therefore every Bass cyclic unit based on  $g$  has finite order. Therefore, every two Bass cyclic units of infinite order commute, as they belong to  $\mathbb{Z}A$ . This shows the necessity of allowing  $v$  not to be a Bass cyclic unit in the Conjecture stated in the introduction.

For an element  $g$  of order  $d$  in the group  $G$  we use the notation  $\hat{g} = \sum_{i=0}^{d-1} g^i$ .

**Example 2.3.** (Following an idea in [4]) Let  $G = \langle b \rangle \rtimes \langle a \rangle$ , where  $a$  has prime order  $p \geq 5$ ,  $b$  has order  $p^n$ , with  $n \geq 2$ , and  $b^a = b^{1+p^{n-1}}$ . Let  $v = 1 + (1-g)h\hat{g}$  be a non-trivial bicyclic unit of  $U(\mathbb{Z}G)$ . Then  $\langle g \rangle$  is non-normal subgroup of  $G$  and therefore it does not contain  $G' = \langle b^{p^{n-1}} \rangle$ . Then  $\langle g \rangle \cap \langle b \rangle = 1$ , so that  $g^p = 1$ . Thus  $g \in \langle b^j a \rangle$  for some  $j$  such that  $1 = (b^j a)^p = b^{j \frac{(1+p^{n-1})p-1}{p^{n-1}}}$ . As  $(1+p^{n-1})^p \equiv 1+p^n \pmod{p^{n+1}}$  we deduce that  $p^{n-1} | j$  and therefore  $b^j \in G' \subseteq Z(G)$ . Thus  $g = za^t$  for some central element  $z$  with  $z^p = 1$  and  $1 \leq t < p$ . Let  $t'$  be the inverse of  $t$  modulo  $p$ . As  $u_{k,m}(a)$  belongs to the group ring  $\mathbb{Z}\langle a \rangle$ , we can write  $u = u_{k,m}(a) = \sum_{x=0}^{p-1} \alpha_x a^x$  for some integers  $\alpha_x$ . Setting  $w = \sum_{x=0}^{p-1} \alpha_x z^{-t'x}$ , we have

$$\hat{g}u = \hat{g} \sum_x \alpha_x z^{-t'x} g^{t'x} = \hat{g} \sum_x \alpha_x z^{-t'x} = \hat{g}w.$$

As  $w$  is central and  $g$  and  $u$  commute we have

$$u^{-j}v^i u^j = 1 + iw^j u^{-j}(1-g)h\widehat{g}$$

for every  $i, j$ . Using  $\widehat{g}\omega^j u^{-j}(1-g) = \omega^j u^{-j}\widehat{g}(1-g) = 0$ , it is easy to see that  $A = \langle u^{-j}v u^j : j \in \mathbb{Z} \rangle$  is an abelian normal subgroup of  $\langle u, v \rangle$  such that  $\langle u, v \rangle / A$  is cyclic. Thus  $\langle u, v \rangle$  does not contain any non-abelian free group and this shows the necessity of allowing  $v$  not to be bicyclic unit in the Conjecture stated in the introduction.

### 3. FREE GROUPS GENERATED BY A BASS CYCLIC UNIT AND A BICYCLIC UNIT

In this section we prove the Main Theorem for two families of groups which will be the most relevant cases for the proof in the general case.

Throughout this section  $p$  is a prime integer and  $k$  and  $m$  are positive integers with  $k^m \equiv 1 \pmod{p}$  and  $k \not\equiv \pm 1 \pmod{p}$ . We extend the notation of Bass cyclic units and set

$$u(\zeta) = u_{k,m}(\zeta) = (1 + \zeta + \cdots + \zeta^{k-1})^m + \frac{1 - k^m}{p}(1 + \zeta + \cdots + \zeta^{p-1}),$$

for a  $p$ -th root of unity  $\zeta$ . Notice that  $u(1) = 1$  and, if  $\zeta \neq 1$  then  $u(\zeta) = \left(\frac{\zeta^k - 1}{\zeta - 1}\right)^m$ . Moreover, if  $m_1$  is another integer with  $k^{m_1} \equiv 1 \pmod{p}$  then

$$(3.1) \quad u_{k,m}(\zeta)u_{k,m_1}(\zeta) = u_{k,m+m_1}(\zeta).$$

**Lemma 3.1.** *If  $\zeta$  is a primitive  $p$ -th root of unity and  $a$  and  $b$  are integers then  $|u(\zeta^a)| = |u(\zeta^b)|$  if and only if  $a + b \equiv 0 \pmod{p}$ .*

*If moreover,  $p$  divides  $m$  then  $u(\zeta^a) = u(\zeta^b)$  if and only if  $a + b \equiv 0 \pmod{p}$ .*

*Proof.* The first statement is proved in [7, Lemma 3.5]. Assume that  $a + b \equiv 0 \pmod{p}$ . If  $a \equiv 0 \pmod{p}$  then  $u(\zeta^{ak}) = 1 = u(\zeta^{bk})$ . Otherwise

$$u(\zeta^b) = \left(\frac{\zeta^{-ak} - 1}{\zeta^{-a} - 1}\right)^m = \left(\frac{\zeta^{-ak}}{\zeta^{-a}} \cdot \frac{\zeta^{ak} - 1}{\zeta^a - 1}\right)^m = u(\zeta^a).$$

□

**Lemma 3.2.** *Let  $\zeta_0, \dots, \zeta_{q-1}$  be a list of  $p$ -th roots of unity such that  $\zeta_j \notin \{\zeta_i, \overline{\zeta_i}\}$  for some  $1 \leq i, j \leq q-1$ . Let  $k$  and  $m$  be integers with  $k \not\equiv \pm 1 \pmod{p}$  and  $k^m \equiv 1 \pmod{p}$ . Consider the diagonal matrix  $S = \text{Diag}(u(\zeta_0), \dots, u(\zeta_{q-1}))$  and the matrix*

$$\tau = \begin{pmatrix} \zeta_0 - \zeta_1 & \zeta_0 - \zeta_1 & \cdots & \zeta_0 - \zeta_1 \\ \zeta_1 - \zeta_2 & \zeta_1 - \zeta_2 & \cdots & \zeta_1 - \zeta_2 \\ \cdots & \cdots & \cdots & \cdots \\ \zeta_{q-1} - \zeta_0 & \zeta_{q-1} - \zeta_0 & \cdots & \zeta_{q-1} - \zeta_0 \end{pmatrix}.$$

*Then  $\langle S^n, (1 + \tau)^n = 1 + n\tau \rangle$  is free non-abelian for some  $n$ .*

*Proof.* Let  $M_+$  and  $M_-$  be the maximum and minimum of  $\{|u(\zeta_0)|, \dots, |u(\zeta_{q-1})|\}$ . By assumption and Lemma 3.1,  $M_- \neq M_+$ . Let  $X = \{0, 1, 2, \dots, q-1\}$ ,  $X_{\pm} = \{i \in X : |u(\zeta_i)| = M_{\pm}\}$  and  $X_0 = X \setminus (X_+ \cup X_-)$ .

We consider  $S$  and  $\tau$  as endomorphisms of  $V = \mathbb{C}^q$ . Let  $\{e_0, \dots, e_{q-1}\}$  be the standard basis of  $V$ . Let  $V_+$ ,  $V_-$  and  $V_0$  be the subspaces of  $V$  generated by  $\{e_i : i \in X_+\}$ ,  $\{e_i : i \in X_-\}$  and  $\{e_i : i \in X_0\}$ , respectively. Then  $V = V_+ \oplus V_0 \oplus V_-$  is an  $S$ -decomposition of  $V$  in the sense of [7]. Let  $K$  and  $I$  denote the kernel and image of  $\tau$ .

By (3.1), one may assume without loss of generality that  $p$  divides  $m$ . By Lemma 3.1, this implies that if  $|u(\zeta_i)| = |u(\zeta_j)|$  then  $u(\zeta_i) = u(\zeta_j)$ . Thus  $W = (V_+ \cap K) \oplus (V_- \cap K)$  is invariant under the action of  $S$  and  $\tau$  and hence they induce endomorphisms  $\bar{S}$  and  $\bar{\tau}$  of  $\bar{V} = V/W$ . To finish the proof we prove that  $\bar{\tau}$  and  $\bar{S}$  satisfies the assumptions of Theorem 2.7 in [7].

The kernel and image of  $\bar{\tau}$  are  $K_1 = \bar{\tau}^{-1}(W)$  and  $\bar{I}$  (we are using the standard bar notation for reduction modulo  $W$ ). Let  $\bar{V} = \bar{V}_+ \oplus \bar{V}_- \oplus \bar{V}_0$  be the  $\bar{S}$ -decomposition of  $\bar{V}$ . Then the dimension of  $\bar{V}_\pm \simeq V_\pm / (V_\pm \cap W) = V_\pm / (V_\pm \cap K)$  is 1, because  $K$  is a hyperplane of  $V$  but  $e_i \notin K$  and  $S(e_i) = u(\zeta_i)e_i \notin K$  for every  $i \in X_\pm$ . Thus  $\bar{V}_\pm \cap K_1 = 0$ . Moreover  $\bar{I}$  is 1-dimensional generated by  $\bar{\Psi}$ , with  $\Psi = (\zeta_0 - \zeta_1, \zeta_1 - \zeta_2, \dots, \zeta_{q-1} - \zeta_0)$ .

It only remains to prove that  $\bar{I} \cap (\bar{V}_0 \oplus \bar{V}_\pm) = 0$  or equivalently  $\bar{\Psi} \notin \bar{V}_0 \oplus \bar{V}_\pm$ . By symmetry we prove  $\bar{\Psi} \notin \bar{V}_0 \oplus \bar{V}_+$ . Otherwise  $\Psi = v + w_+ + w_-$  for some  $v \in V_0$ ,  $w_+ \in V_+$  and  $w_- \in V_- \cap K$ . Thus the projection of  $\Psi$  onto  $V_-$  belongs to  $K$ . That is,  $\sum_{i \in X_-} (\zeta_i - \zeta_{i+1}) = 0$ , where the subindexes are considered modulo  $q$ . Now we delete from the equality above the zero summands and move the negative expression to the right side and add up the equal terms obtaining

$$(3.2) \quad n_1 \lambda_1 + n_2 \lambda_2 = \sum_{i=1}^k m_i \mu_i \quad \text{and} \quad n_1 + n_2 = \sum_{i=1}^k m_i,$$

where  $\{\lambda_1, \lambda_2\} = \{\zeta_i : i \in X_-, \zeta_i \neq \zeta_{i+1}\}$ ,  $\{\mu_1, \dots, \mu_k\} = \{\zeta_{i+1} : i \in X_-, \zeta_i \neq \zeta_{i+1}\}$ , the  $\mu_i$ 's are pairwise different,  $n_i$  is the cardinality of  $\{j : \lambda_i = \zeta_j \neq \zeta_{j+1}\}$ , for  $i = 1, 2$ , and  $m_i$  is the cardinality of  $\{j \in X_- : \zeta_j \neq \zeta_{j+1} = \mu_i\}$ . Moreover  $\lambda_1$  and  $\lambda_2$  are complex conjugate and  $n_1$  and  $n_2$  are non-negative with at least one of them positive. We may assume without loss of generality that  $n_1 > 0$  and if  $n_2 \neq 0$  then  $\lambda_1 \neq \lambda_2$ . Let  $\text{tr}$  denotes the Galois trace of the extension  $\mathbb{Q}(\xi)/\mathbb{Q}$ , where  $\xi$  is a primitive  $p$ -th root of unity. Recall that  $\text{tr}(1) = p - 1$  and  $\text{tr}(\zeta) = -1$ , for every primitive  $p$ -th root of unity  $\zeta$ . If  $n_2 = 0$  then  $\mu_i \neq \lambda_1$  for every  $i$  and applying  $\text{tr}$  on

$$n_1 = \sum_{i=1}^k m_i \mu_i \lambda_1^{-1}$$

we obtain  $n_1(p-1) < 0$ , yielding a contradiction. Thus  $n_2 \neq 0$  and so  $\lambda_1 = \bar{\lambda}_2 \neq \lambda_2$ . Now, applying  $\text{tr}$  on the left equation of (3.2) we obtain

$$-\sum_{i=1}^k m_i = -n_1 - n_2 = \sum_{i=1}^k m_i \text{tr}(\mu_i)$$

and hence  $\mu_i \neq 1$  for every  $i$ . This, together with (3.2), and the fact that the set of  $p$ -th primitive roots of unity is linearly independent over the rationals, implies that every  $\mu_i$  is either  $\lambda_1$  or  $\lambda_2 = \bar{\lambda}_1$ . However, by assumption there is  $0 \leq j \leq p-1$  such that  $\zeta_j \notin \{\lambda_1, \bar{\lambda}_2\}$ . If  $j$  is the first element satisfying this condition then  $\mu_i = \zeta_j \notin \{\lambda_1, \bar{\lambda}_2\}$  for some  $i$ .  $\square$

**Proposition 3.3.** *Let  $G$  be a finite group,  $A$  and abelian normal subgroup of  $G$  and let  $a \in A$  and  $b \in G$ . Assume that the order of  $a$  is prime, say  $p$ , and  $b \notin D_G(a)$ . Let  $u = u_{k,m}(a)$  be a Bass cyclic unit with  $k \not\equiv \pm 1 \pmod{p}$  (in particular,  $p \geq 5$ ) and  $v = 1 + (1-b)\widehat{ab}$ . Then  $\langle u^n, v^n \rangle$  is free non-abelian for some  $n$ .*

*Proof.* Let  $\phi$  be a linear representation of  $A$  and let  $\chi = \phi^G$ , the representation induced by  $\phi$  on  $G$ . For every  $i = 0, 1, \dots, q-1$  let  $\zeta_i = \phi(a^{b^i})$ . Then  $S = \chi(u)$  and  $\tau = \chi(v-1)$  are as in Lemma 3.2. Thus to prove the lemma it is enough to show that  $A$  has a representation for which not all the  $\zeta_i$  are either equal or conjugate. If  $a^b \notin \langle a \rangle$  then  $A = A_1 \times A_2$  for two subgroups of  $A$  with  $a \in A_1$  and  $a^b \in A_2$ . Thus  $A$  has a linear representation  $\phi$  with  $a \in \ker \phi$  and  $a^b \notin \ker \phi$ . Otherwise,  $a^b = a^i$ , with  $i \not\equiv \pm 1 \pmod{p}$ . Moreover,  $A$  has a linear representation  $\phi$  with  $\phi(a) = \zeta$  a primitive  $p$ -th root of unity. Then  $\zeta_0 = \phi(a) = \zeta$  and  $\zeta_1 = \phi(a^b) = \zeta^i$  are neither equal nor complex conjugate.  $\square$

**Proposition 3.4.** *Let  $\langle a \rangle$  be a cyclic group of prime order  $p$  acting faithfully and irreducibly on a non-cyclic elementary abelian  $q$ -group  $B$ , with  $q \neq p$ , and let  $1 \neq b \in B$  and let  $G = B \rtimes \langle a \rangle$  the corresponding semidirect product. If  $u = u_{k,m}(a)$  has infinite order module the centre of  $U(\mathbb{Z}G)$  and  $v = 1 + (1-ba)\widehat{aba}$  then  $\langle u^n, v^n \rangle$  is a non-abelian free group for some integer  $n$ .*

*Proof.* As  $B$  is non-cyclic it has a non-trivial linear character  $\chi$  of  $B$ , with  $\chi(b) = 1$ . Let  $\rho = \chi^G$  the induced representation and set  $\gamma_i = \chi(b^{a^i})$  for  $i \in \mathbb{Z}$ . Since the action of  $a$  on  $B$  is irreducible  $b^{a^i} \notin \ker(\chi)$  for some  $i$  and therefore, not all the  $\gamma_i$ 's are equal.

For every  $i \geq 0$  we set  $\delta_i = \prod_{j=0}^{i-1} \gamma_j$ . Note that  $\delta_0 = 1$ , because the empty product is interpreted as 1. Moreover  $\delta_p = \gamma(\prod_{i=0}^{p-1} b^{a^i}) = \gamma(1) = 1$ , because  $\prod_{i=0}^{p-1} b^{a^i} \in Z(G) = 1$ . As not all the  $\gamma$ 's are equal, not all the  $\delta$ 's are equal.

We also define  $\epsilon_{i,j} = \prod_{x=i}^{j-1} \gamma_x$ , where for  $j < i$  we interpret the product as  $\gamma_i \gamma_{i+1} \dots \gamma_{p-1} \gamma_0 \gamma_1 \dots \gamma_{j-1}$ .

Using  $\gamma_p = \delta_p = 1$  allows to consider the subindices of the  $\gamma_i$ 's,  $\delta_i$ 's and  $\epsilon_{i,j}$ 's as elements in  $\mathbb{Z}/p\mathbb{Z}$ . We also label the rows and columns of a  $p \times p$  matrix by elements of  $\mathbb{Z}/p\mathbb{Z}$ . Accordingly, for  $0 \leq i, j < p$ , let  $e_{i,j}$  denote the matrix having 1 at the  $(i, j)$ -entry and zeroes elsewhere. Then

$$\rho(b) = \text{diag}(\gamma_0, \gamma_1, \dots, \gamma_{p-1}) = \sum_{i=0}^{p-1} \gamma_i e_{i,i}$$

and

$$\rho(a) = \sum_{i=0}^{p-1} e_{i,i+1}, \quad \text{and} \quad \rho(ba) = \sum_{i=0}^{p-1} \gamma_i e_{i,i+1}.$$

Thus

$$\rho((ba)^j) = \sum_{i=0}^{p-1} \gamma_i \gamma_{i+1} \dots \gamma_{i+j-1} e_{i,i+j} = \sum_{i=0}^{p-1} \epsilon_{i,i+j} e_{i,i+j}.$$

Note that the non-zero entries of  $\rho((ba)^j)$  appears in different positions for different values of  $j$ . So,

$$\rho(\widehat{ba}) = \rho(1 + ba + (ba)^2 + \dots + (ba)^{p-1}) = \sum_{i,j} \epsilon_{i,j} e_{i,j} = (\epsilon_{i,j}).$$

The 0-th column of  $\rho(\widehat{ba})$  is

$$\begin{pmatrix} \epsilon_{0,0} \\ \epsilon_{1,0} \\ \epsilon_{2,0} \\ \vdots \\ \epsilon_{p-1,0} \end{pmatrix} = \begin{pmatrix} 1 \\ \gamma_1 \cdots \gamma_{p-1} \\ \gamma_2 \cdots \gamma_{p-1} \\ \vdots \\ \gamma_{p-1} \end{pmatrix}.$$

Using that  $\gamma_0 \cdots \gamma_{p-1} = 1$  we obtain that the  $i$ -th column of  $\rho(\widehat{ba})$  is

$$\begin{pmatrix} \epsilon_i \\ \epsilon_{1,i} \\ \epsilon_{2,i} \\ \vdots \\ \epsilon_{i-1,i} \\ \epsilon_{i,i} \\ \epsilon_{i+1,i} \\ \vdots \\ \epsilon_{p-1,i} \end{pmatrix} = \begin{pmatrix} \gamma_0 \cdots \gamma_{i-1} \\ \gamma_1 \cdots \gamma_{i-1} \\ \gamma_2 \cdots \gamma_{i-1} \\ \vdots \\ \gamma_{i-1} \\ 1 \\ \gamma_{i+1} \cdots \gamma_{p-1} \gamma_0 \cdots \gamma_{i-1} \\ \vdots \\ \gamma_{p-1} \gamma_0 \cdots \gamma_{i-1} \end{pmatrix} = \gamma_0 \cdots \gamma_{i-1} \begin{pmatrix} 1 \\ \gamma_1 \gamma_2 \cdots \gamma_{p-1} \\ \vdots \\ \gamma_{i-1} \cdots \gamma_{p-1} \\ \gamma_i \cdots \gamma_{p-1} \\ \gamma_{i+1} \cdots \gamma_{p-1} \\ \vdots \\ \gamma_{p-1} \end{pmatrix}.$$

Therefore all the columns of  $\rho(\widehat{ba})$  are proportional to the first column and hence the rank of  $\rho(\widehat{ba})$  is 1 and hence the rank of  $\tau = \rho(v-1)$  is at most 1. In fact it is 1 because

$$\begin{aligned} \tau &= \left( \sum_{i=0}^{p-1} e_{i,i} - \gamma_i e_{i,i+1} \right) \sum_{j=0}^{p-1} e_{j,j+1} \left( \sum_{k,l} \epsilon_{k,l} e_{k,l} \right) = \sum_{i,j} (\epsilon_{i+1,j} - \gamma_i \epsilon_{i+2,j}) e_{i,j} \\ &= \sum_{i,j} (\gamma_{i+1} - \gamma_i) \epsilon_{i+2,j} e_{i,j} \neq 0, \end{aligned}$$

as not all the  $\gamma_i$ 's are equal. Hence the kernel of  $\tau$  coincides with the nullspace of  $\rho(\widehat{ba})$  and this is equal to the nullspace of any non-zero row of  $\rho(\widehat{ba})$ , for example we can take the first row. In other words,

$$K = \ker(\tau) = \{(x_0, \dots, x_{p-1}) : x_0 + \delta_1 x_1 + \cdots + \delta_{p-1} x_{p-1} = 0\}$$

and the image of  $\tau$  is spanned by

$$\Psi = ((\gamma_1 - \gamma_0) \epsilon_{2,0}, (\gamma_2 - \gamma_1) \epsilon_{3,0}, \dots, (\gamma_0 - \gamma_{p-1}) \epsilon_{1,0}).$$

Let  $\zeta$  be a  $p$ -th primitive root of unity and consider the Vandermonde matrix

$$U = V(1, \zeta, \zeta^2, \dots, \zeta^{p-1}) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^{2 \cdot 2} & \cdots & \zeta^{2(p-1)} \\ 1 & \zeta^3 & \zeta^{3 \cdot 2} & \cdots & \zeta^{3(p-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \zeta^{(p-1)} & \zeta^{(p-1) \cdot 2} & \cdots & \zeta^{(p-1)(p-1)} \end{pmatrix}.$$

The  $i$ -th column  $v_i$  of  $U$  is an eigenvector of  $\rho(a)$  with eigenvalue  $\zeta^i$ . So it is also an eigenvector of  $A = \rho(u)$  with eigenvalue  $u(\zeta^i)$ . Let  $\alpha$  and  $\beta$  be such that  $|u(\zeta^\beta)| \leq |u(\zeta^j)| \leq |u(\zeta^\alpha)|$ , for every  $j$ . So, if  $V_+ = \mathbb{C}v_\alpha + \mathbb{C}v_{-\alpha}$ ,  $V_- = \mathbb{C}v_\beta + \mathbb{C}v_{-\beta}$  and  $V_0 = \sum_{i \notin \{\pm\alpha, \pm\beta\}} \mathbb{C}v_i$  then  $V = V_+ \oplus V_0 \oplus V_-$  is an  $A$ -decomposition of  $V$ .

As  $K$  is a hyperplane of the representing space  $V = \mathbb{C}^p$  and  $V_+$  and  $V_-$  have dimension 2 we have  $K \cap V_+ \neq 0 \neq K \cap V_-$ . However we can play the same trick as in the proof of Lemma 3.2, by assuming that  $m$  is a power of  $p$ , so that,  $u_{k,m}(\zeta^i) = u_{k,m}(\zeta^{-i}) \in \mathbb{R}$  for every  $i$ . So  $V_+$  and  $V_-$  are the eigenspaces of  $A$  corresponding to the eigenvalues  $u(\zeta^\alpha)$  and  $u(\zeta^\beta)$ , respectively. Thus  $W = K \cap V_+ \oplus K \cap V_-$  is invariant under the action of  $A$  and  $\tau$ . Hence there are induced endomorphisms  $\bar{A}$  and  $\bar{\tau}$  of  $\bar{V} = V/W$ . The kernel of  $\bar{\tau}$  is  $\tau^{-1}(W)$  and the image is generated by  $\bar{\Psi}$ .

If  $\xi$  is a primitive  $q$ -root of unity then  $\mathbb{Q}(\xi) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$  and thus the minimal polynomial of  $\zeta$  over  $\mathbb{Q}(\xi)$  is  $1 + x + x^2 + \dots + x^{p-1}$ . Hence, as not all the  $\delta_i$ 's are equal, we have  $\sum_{j=0}^{p-1} \delta_j \zeta^{ij} \neq 0$  for every  $1 \leq i < p$ , or equivalently  $v_i \notin K$  for every  $i$ . In particular,  $v_{\pm i_{\pm}} \notin K$  and hence both  $K \cap V_+$  and  $K \cap V_-$  have dimension 1.

To finish the proof it is enough to check that  $\bar{A}$  and  $\bar{\tau}$  satisfies the conditions of [7, Theorem 2.7] and for that it only remains to show that  $\bar{\Psi} \notin \bar{V}_0 \oplus \bar{V}_{\pm}$ . By symmetry, we prove  $\bar{\Psi} \notin \bar{V}_0 \oplus \bar{V}_+$ . By means of contradiction assume that  $\bar{\Psi} \in \bar{V}_0 \oplus \bar{V}_+$ . Then the projection  $\Psi_-$  of  $\Psi$  onto  $V_-$ , via the  $A$ -decomposition, belongs to  $K$ . The inverse of the matrix  $U$  is  $\bar{U}/p$ , where the entries of  $\bar{U}$  are the conjugates of the entries of  $U$ . This implies that the projection of the column vector  $x$  onto  $V_-$  is  $U(e_{\beta,\beta} + e_{-\beta,-\beta})\bar{U}x/p$ . We first calculate

$$\begin{aligned} U(e_{\beta,\beta} + e_{-\beta,-\beta})\bar{U} &= \left( \sum_{i,j} \zeta^{ij} e_{i,j} \right) (e_{\beta,\beta} + e_{-\beta,-\beta}) \left( \sum_{k,l} \zeta^{-kl} e_{k,l} \right) \\ &= \sum_{i,l} (\zeta^{i\beta} \zeta^{-\beta l} + \zeta^{-i\beta} \zeta^{\beta l}) e_{i,l} \\ &= \sum_{i,l} (\zeta^{(i-l)\beta} + \zeta^{(l-i)\beta}) e_{i,l}. \end{aligned}$$

Therefore

$$p\Psi_- = U(e_{\beta,\beta} + e_{-\beta,-\beta})\bar{U}\Psi = \begin{pmatrix} \sum_j (\zeta^{-j\beta} + \zeta^{j\beta})(\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0} \\ \sum_j (\zeta^{(1-j)\beta} + \zeta^{(j-1)\beta})(\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0} \\ \vdots \\ \sum_j (\zeta^{(p-1-j)\beta} + \zeta^{(j-p-1)\beta})(\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0} \end{pmatrix}$$

So  $\Psi_- \in K$  if and only if  $\sum_{i,j} \delta_i (\zeta^{(i-j)\beta} + \zeta^{(j-i)\beta})(\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0} = 0$ , if and only if  $\sum_{i,j} \delta_{j+i} (\zeta^{i\beta} + \zeta^{-i\beta})(\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0} = 0$  if and only if

$$\sum_i \left( \sum_j (\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0}(\delta_{j+i} + \delta_{j-i}) \right) \zeta^{i\beta} = 0$$

if and only if  $\alpha_i = \sum_j (\gamma_{j+1} - \gamma_j)\epsilon_{j+2,0}(\delta_{j+i} + \delta_{j-i})$  is independent of  $i$ .

For  $i = 0$  we have

$$\begin{aligned}
 \alpha_0 &= 2 \sum_j \delta_j (\gamma_{j+1} - \gamma_j) \epsilon_{j+2,0} = 2 \left( \sum_j \delta_j \gamma_{j+1} \epsilon_{j+2,0} - \sum_j \delta_j \gamma_j \epsilon_{j+2,0} \right) \\
 &= 2 \left( \sum_j \prod_{0 \leq k < p-1, k \neq j} \gamma_k - \sum_j \prod_{0 \leq k < p-1, k \neq j+1} \gamma_{k+1} \right) \\
 &= 2 \left( \sum_j \gamma_j^{-1} - \sum_j \gamma_{j+1}^{-1} \right) = 0.
 \end{aligned}$$

Hence, if  $\Psi_- \in K$  then  $\alpha_i = 0$  for every  $i$ . In particular for  $i = 1$  we have

$$\begin{aligned}
 0 &= \alpha_1 = \sum_j (\delta_{j+1} + \delta_{j-1}) (\gamma_{j+1} - \gamma_j) \epsilon_{j+2,0} \\
 &= \sum_j (\delta_{j+1} \gamma_{j+1} \epsilon_{j+2,0} + \delta_{j-1} \gamma_{j+1} \epsilon_{j+2,0} - \delta_{j+1} \gamma_j \epsilon_{j+2,0} - \delta_{j-1} \gamma_j \epsilon_{j+2,0}) \\
 &= \sum_j (1 + \gamma_{j-1}^{-1} \gamma_j^{-1} - \gamma_j \gamma_{j+1}^{-1} - \gamma_{j-1}^{-1} \gamma_{j+1}^{-1}) \\
 &= p + \sum_j \gamma_j^{-1} \gamma_{j+1}^{-1} - \sum_j \gamma_j \gamma_{j+1}^{-1} - \sum_j \gamma_j^{-1} \gamma_{j+2}^{-1}
 \end{aligned}$$

If  $\text{tr}$  denotes the trace of the extension  $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ , where  $\zeta_q$  is a  $q$ -th root of unity then  $\text{tr}(\zeta_q^i) = (q-1)$  if  $q$  divides  $i$  and it is  $-1$  otherwise. Therefore applying  $\text{tr}$  in the previous expression we obtain

$$\begin{aligned}
 0 &= p(q-1) + n_1(q-1) - (p-n_1) - n_2(q-1) + (p-n_2) - n_3(q-1) + (p-n_3) \\
 &= pq + (n_1 - n_2 - n_3)q,
 \end{aligned}$$

where  $n_i$  is the cardinality of  $X_i$  for

$$\begin{aligned}
 X_1 &= \{j \in \mathbb{Z}_p : \zeta_j = \zeta_{j+1}^{-1}\}, \\
 X_2 &= \{j \in \mathbb{Z}_p : \zeta_j = \zeta_{j+1}\} \text{ and} \\
 X_3 &= \{j \in \mathbb{Z}_p : \zeta_j = \zeta_{j+2}^{-1}\}.
 \end{aligned}$$

On the other hand, if  $j \in X_2 \cap X_3$  then  $\zeta_{j+1} \in X_1$ . Hence  $j \mapsto j+1$  is an injective map  $X_2 \cap X_3 \rightarrow X_1$ . So  $p = n_2 + n_3 - n_1 \leq |X_2| + |X_3| - |X_2 \cap X_3| = |X_2 \cup X_3|$  and therefore  $X_2 \cup X_3 = \mathbb{Z}_p$ . If  $X_2 = \emptyset$  then  $\zeta_{j+2} = \zeta_j^{-1}$  for every  $j$ . Using that  $p$  is odd one deduces that  $\zeta_j = \zeta_0 = 1$ , for every  $j$ . Thus  $X_2 \neq \emptyset$ , i.e.  $\gamma_{j_0} = \gamma_{j_0+1}$  for some  $j_0$ . Now using that  $\gamma_{j-1}$  is either  $\gamma_j$  or  $\gamma_{j+1}$  for every  $j$ , we deduce that  $\gamma_j$  is either  $\gamma_{j_0}$  or  $\gamma_{j_0}^{-1}$  for every  $j$ . As  $\gamma_0 = 1$ , we deduce that  $\gamma_j = 1$  for every  $j$  and this yields the final contradiction.  $\square$

#### 4. DIHEDRAL $p$ -CRITICAL ELEMENTS AND PROOF OF THE MAIN THEOREM

Recall that [6] defines  $G$  as being  $p$ -critical provided that:

- (1)  $G$  has a non-central element of order  $p$ ; and
- (2) for all proper subgroups  $H$  of  $G$ , the elements of  $H$  of order  $p$  are central in  $H$ .

Here we will need a sharper definition, the criticality being associated to an element. We say that  $a$  is *dihedral  $p$ -critical in  $G$*  if it satisfies the following conditions:

- (C1)  $a$  has order  $p$  and  $D_G(a) \neq G$ .
- (C2) If  $H$  is a proper subgroup of  $G$ , and  $a \in H$ , then  $D_H(a) = H$ .
- (C3) If  $\bar{G}$  is a proper quotient of  $G$  then  $D_{\bar{G}}(\bar{a}) = \bar{G}$ . (Here we use the standard bar notation.)

Our next goal is to classify finite groups with a dihedral  $p$ -critical element. We start with some easy consequences of the definition.

**Lemma 4.1.** *If  $a$  is dihedral  $p$ -critical in  $G$  then*

- (1) *Every proper subgroup of  $G$  containing  $a$  is contained in  $D_G(a)$ .*
- (2) *If  $b \in G \setminus D_G(a)$  then  $G = \langle a, b \rangle$ .*
- (3) *If  $N$  is a non-trivial normal subgroup of  $G$  then  $G' \subseteq \langle a, N \rangle$ .*

*Proof.* (1) and (2) are consequences of (C2). By (2),  $G = \langle a, b \rangle$  for some  $b \in G$ . Let  $N$  be a non-trivial normal subgroup of  $G$ . By condition (C3),  $a^g \in aN \cup a^{-1}N$  for every  $g \in G$  and hence  $[G, a] \subseteq N \cup a^2N$ . Thus  $[g, a]^h = a^{gh}(a^h)^{-1} \in \langle a, N \rangle$  for every  $g, h \in G$ . This shows that  $\langle a, N \rangle$  contains  $M = \langle [G, a]^g : g \in G \rangle$ . Since  $G/M$  is abelian, because  $G = \langle a, b \rangle$ , we deduce that  $G' \subseteq \langle a, N \rangle$ .  $\square$

The notation  $\langle g \rangle_n$  represents a cyclic group of order  $n$  generated by  $g$ . If  $i$  and  $n$  are coprime integers then  $o_n(i)$  denotes the order of  $i$  modulo  $n$ .

**Proposition 4.2.** *Let  $a$  be a dihedral  $p$ -critical element of a finite group  $G$ . Then one of the following conditions holds:*

- (1)  $G = \langle a \rangle_p \rtimes \langle b \rangle_q$ , for  $q$  either 4 or an odd prime such that  $a^b = a^i$  and  $q = o_p(i)$ .
- (2)  $G = (\langle a \rangle_p \times \langle z \rangle_p) \rtimes \langle b \rangle_p$ , with  $z \in Z(G)$  and  $a^b = za$ .
- (3)  $G = \langle b \rangle_{p^n} \rtimes \langle a \rangle_p$ , with  $n \geq 2$  and  $b^a = b^{1+p^{n-1}}$ .
- (4)  $G = (\langle a \rangle_p \times \langle z \rangle_p) \rtimes \langle b \rangle_2$ , with  $z \in Z(G)$  and  $a^b = za^{-1}$ .
- (5)  $G = A \rtimes \langle b \rangle_q$ , where  $A$  is an elementary abelian non-cyclic  $p$ -group containing  $a$ , with  $q \neq p$  prime and the action of  $\langle b \rangle$  on  $A$  is irreducible and faithful.
- (6)  $G = (\langle a \rangle_p \times \langle a_1 \rangle_p) \rtimes \langle b \rangle_4$ , with  $a^b = a_1$  and  $a_1^b = a^{-1}$ .
- (7)  $G = B \rtimes \langle a \rangle_p$ , where  $B$  is an elementary abelian  $q$ -group and the action of  $\langle a \rangle$  on  $B$  is faithful and irreducible.
- (8)  $G$  is simple.

*Proof.* We set  $D = D_G(a)$  and  $C = C_G(a)$  and fix an element  $b \in G \setminus D_G(a)$ . Notice that  $g^2 \in C$  for every  $g \in D$  and, by Lemma 4.1,  $D$  is the unique maximal subgroup of  $G$  containing  $a$ .

*Case 1:* Assume that  $G' = \langle a \rangle$ . Then  $a^b = a^i$  for some  $i \not\equiv \pm 1 \pmod{p}$ . Let  $t = o_p(i)$ . If  $q$  is a prime divisor of  $t$  then  $\langle a, b^q \rangle$  is a proper subgroup of  $G$  and hence  $a^{i^q} = a^{b^q} = a^{\pm 1}$ . Hence either  $t = 4$  or  $t$  is an odd prime. If  $r$  is a prime divisor of the order of  $b$  which is coprime with  $t$  then  $\langle a, b^r \rangle$  is again a proper subgroup of  $G$  not contained in  $D$ , yielding a contradiction. Thus  $G = \langle a \rangle_p \rtimes \langle b \rangle_{q^k}$  and either  $q = o_p(i)$  is an odd prime or  $q = 2$ ,  $k \geq 2$  and  $o_p(i) = 4$ . In the first case  $k = 1$ , because otherwise  $1 \neq b^q \in Z(G)$  and  $G/\langle b^q \rangle = \langle \bar{a} \rangle_p \rtimes \langle \bar{b} \rangle_{q^{k-1}}$ , with  $\bar{a}^{\bar{b}} = \bar{a}^i$  and  $i \not\equiv \pm 1 \pmod{p}$ , contradicting (C3). In the second case  $b^4 \in Z(G)$  and a similar argument shows that in this case  $k = 2$ . Thus  $G$  is as in (1).

*Case 2: Assume that  $G' \neq \langle a \rangle$  and  $Z(G) \neq 1$ .* By property (3) of Lemma 4.1,  $G'$  is contained in  $\langle a, z \rangle = \langle a \rangle \times \langle z \rangle$  for every  $1 \neq z \in Z(G)$ . Therefore, if  $H$  and  $K$  are two different minimal subgroups of  $Z(G)$  then  $G' \subseteq \langle a, H \rangle \cap \langle a, K \rangle = \langle a \rangle$ , contradicting the assumption  $G' \neq \langle a \rangle$ . Hence  $Z(G)$  has a unique minimal subgroup, or equivalently,  $Z(G)$  is cyclic of prime power order, say  $q^k$  with  $q$  prime. By (C1) and (C3) we deduce that  $a^b = a^{\pm 1}z$ , with  $z$  a central element of order  $q$ . In particular,  $p = q$ .

Assume first that  $a^b = az$ . Then  $b^{-p}ab^p = z^pa = a$  and hence  $b^p \in Z(G)$ . If  $b^p = 1$  then  $G = (\langle a \rangle_p \times \langle z \rangle_p) \rtimes \langle b \rangle_p$  and  $G$  is as in (2). Otherwise,  $b$  has order  $p^n$  with  $n \geq 2$ . Then  $\langle b^{p^{n-1}} \rangle$  is the only minimal subgroup of  $Z(G)$  and replacing  $b$  by a suitable power if needed, one may assume that  $z = b^{p^{n-1}}$ . So  $b^a = b^{1+p^{n-1}}$  and  $G$  is as in case (3).

Assume otherwise that  $a^b = a^{-1}z$ . Then  $a^{b^2} = (a^{-1}z)^b = az^{-1}z = a$ , i.e.  $b^2 \in Z(G)$ . Then  $b^2 = 1$  because otherwise  $\langle a, b^p \rangle$  is a proper subgroup of  $G$  and  $a^{b^p} = a^{-1}z \notin \{a, a^{-1}\}$ , contradicting (C2). Then  $G = (\langle a \rangle_p \times \langle z \rangle_p) \rtimes \langle b \rangle_2$ , and  $G$  satisfies the conditions of (4).

*Case 3.  $Z(G) = 1$  and  $D$  is normal in  $G$ .* In particular  $G$  is not a  $p$ -group and  $a^g \in D$  for all  $g \in G$ . Hence  $(a^g)^2 \in C$  and since  $p$ , the order of  $a$ , is odd,  $a^g \in C$ . Thus  $A = \langle a^g : g \in G \rangle$  is a non-trivial elementary abelian normal  $p$ -subgroup of  $G$ . Hence  $G' \subseteq A \subseteq D$ . Since  $D$  is the unique maximal subgroup of  $G$  containing  $a$ ,  $G/A$  is a cyclic  $q$ -group for some prime  $q \neq p$ . Let  $b \in G$  be a generator of  $G$  modulo  $A$ . Then  $D = \langle A, b^q \rangle$  and hence  $b^{2q} \in C$ . The last implies that  $b^{2q} \in Z(G) = 1$ . Therefore  $G = A \rtimes \langle b \rangle$  and, by the definition of  $A$ , it is a minimal  $\langle b \rangle$ -module. By Masche's Theorem, the action of  $\langle b \rangle$  on  $A$  is irreducible. On the other hand  $[G : A]$  is a power of  $q$  and  $q \neq p$ . Thus the order of  $b$  is either  $q$  or  $4$ . If  $A$  is cyclic then  $G$  is as in (1). If  $A$  is non-cyclic and  $b$  as prime order then  $G$  is as in (5). Finally, if  $A$  is non-cyclic and  $b$  has order  $4$  then  $a^{b^2} = a^{-1}$ , because otherwise  $\langle b^2 \rangle$  is a proper central subgroup of  $G$  and if  $\bar{G} = G/\langle b^2 \rangle$  then  $\bar{a} \notin D_{\bar{G}}(\bar{a})$ . Therefore  $A = \langle a \rangle \times \langle a_1 \rangle$  and  $a_1 = a^b$  and  $a_1^b = a^{-1}$  and condition (6) holds.

*Case 4.  $Z(G) = 1$  and  $D$  is not normal in  $G$ .* In particular  $G'$  is not contained in  $D$ . Thus  $\langle G', a \rangle$  is a subgroup of  $G$  containing  $a$  and not contained in  $C$ . Using (C2) once more we have  $G = \langle G', a \rangle$ . Therefore  $\langle a, N \rangle = G$  for every normal subgroup  $N$  of  $G$ . If  $G$  is simple then condition (8) holds. Otherwise, for every proper non-trivial normal subgroup  $N$  of  $G$  we have  $G = N \rtimes \langle a \rangle$ . Therefore  $1 \neq G' \subseteq N$  and hence  $N = G'$ , is the unique minimal normal subgroup of  $G$ . Then  $G' = S_1 \times \dots \times S_k$  with  $S_1, \dots, S_k$  minimal normal subgroups of  $G'$ . We claim that  $G'$  is abelian. Otherwise,  $S_1, \dots, S_k$  are the only minimal normal subgroups of  $G'$  [9, Proposition 3.2] and hence the action of  $\langle a \rangle$  permutes the  $S_i$  transitively (and, in particular,  $k = p$ ). If  $1 \neq b \in S_1$  then  $H = \langle b \rangle \times \langle b^a \rangle \times \langle b^{a^2} \rangle \times \dots \times \langle b^{a^{p-1}} \rangle$  is a proper subgroup of  $G'$  which is invariant under the action of  $a$ . Therefore  $H \rtimes \langle a \rangle$  is a proper subgroup of  $G$  containing  $a$  and not contained in  $D$ , contradicting condition (C2). We conclude that  $G'$  is abelian and hence  $G'$  is an elementary abelian  $q$ -group, for  $q \neq p$  prime and the action of  $\langle a \rangle$  is faithful and irreducible. So condition (7) holds.  $\square$

Finally we are ready to prove the Main Theorem which is an obvious consequence of the following.

**Theorem 4.3.** *Let  $\mathcal{C}$  be a class of finite groups which is closed under subgroups and epimorphic images. Let  $G$  be a group of minimal order in the class  $\mathcal{C}$  which is*

a counterexample to the conjecture stated at the introduction and let  $u = u_{k,m}(a)$  be a Bass cyclic unit of  $G$  based in  $a$ , witnessing this fact. Then  $a$  is dihedral  $p$ -critical in  $G$  and  $G$  is simple.

*Proof.* Let  $\mathcal{C}$ ,  $G$  and  $u = u_{k,m}(a)$  be as in the statement of the theorem. Then  $a$  has prime order, say  $p$  and  $u$  has infinite order modulo the centre of  $U(\mathbb{Z}G)$ . By Lemma 2.1,  $a \in G \setminus D_G(a)$ , so that  $a$  satisfies condition (C1). Let  $H$  be a proper subgroup of  $G$  containing  $a$ . By the minimality of  $|G|$ ,  $u$  has finite order modulo the centre of  $U(\mathbb{Z}H)$  and hence  $a \in D_H(a)$ , that is  $a$  satisfies condition (C2). Finally, let  $\bar{G}$  be a proper epimorphic image of  $G$  such that  $D_{\bar{G}}(\bar{a}) \neq \bar{G}$ . By Lemma 2.1,  $\bar{a}$  is a Bass cyclic unit, of infinite order modulo the centre of  $U(\mathbb{Z}\bar{G})$ , based on  $\bar{a}$ . By the minimality of  $|G|$ ,  $\langle \bar{u}^n, w^n \rangle$  is a non-abelian free group for some  $w$ , which is either a Bass cyclic unit or a bicyclic unit in  $\mathbb{Z}\bar{G}$ . Then  $w = \bar{v}^m$ , for  $v$  either a Bass cyclic unit or a bicyclic unit of  $\mathbb{Z}G$  and some  $m$ . Thus  $\langle u^{nm}, v^{nm} \rangle$  is free non-abelian contradicting the assumption. This proves that  $a$  satisfies condition (C3). Thus  $a$  is dihedral  $p$ -critical in  $G$ .

Therefore  $G$  is one of the groups of Proposition 4.2. The groups of type (1), (2), (4), (5) or (6) satisfy the hypothesis of Proposition 3.3 and the groups of type (7) satisfy the hypothesis of Proposition 3.4. So  $G$  is not of any of these types because otherwise  $\langle u^n, v^n \rangle$  is free non-abelian for some bicyclic unit  $v$ . Therefore, to prove that  $G$  is simple we have to show that  $G$  is not of type (3). This is the group  $G = \langle a, b \rangle$  of Example 2.3 for which we have seen that for every bicyclic unit  $v$ ,  $\langle u, v \rangle$  is metabelian and therefore  $\langle u^n, v^n \rangle$  is not free for any  $n$ . However, by the proof of [7, Lemma 4.3], if  $v = u_{r,s}(b)$  is any Bass cyclic unit based on  $b$  with  $r \not\equiv \pm 1 \pmod{p^n}$  then  $\langle u^n, v^n \rangle$  is free non-abelian for some integer  $n$ , contradicting the assumption. We conclude that  $G$  is simple.  $\square$

**Final remarks:** 1. Observe that if  $G$  is one of the groups of types (1)-(7) in Proposition 4.2 then  $a$  is dihedral  $p$ -critical. However if  $G$  is a non-abelian simple group and  $a$  is an element of prime order  $p$  then  $a$  is not necessarily dihedral  $p$ -critical. For example, the only alternating group with a dihedral  $p$ -critical element, with  $p \geq 5$ , is  $A_5$  and the dihedral 5-critical elements of  $A_5$  are the 5-cycles. Indeed, assume that  $a$  is a dihedral  $p$ -critical element in  $A_n$  with  $p \geq 5$ . Then  $a$  is a product of disjoint  $p$ -cycles and one may assume that  $a = (1, 2, \dots, p)(p+1, p+2, \dots, 2p) \dots ((k-1)p, (k-1)p+1, \dots, kp)$  with  $kp \leq n$ . Since  $b = (3, 4, 5) \notin D_{A_n}(a)$  then  $A_n = \langle a, b \rangle$  and therefore  $k = 1$  and  $n = p$ . Let  $i$  be a generator of the group of units of the field  $\mathbb{Z}_p$ , with  $p$  elements. Then  $a^i$  is a  $p$ -cycle and therefore there is  $\sigma \in S_p$  such that  $a^\sigma = a^i$ . Thus  $a^{i^2} = a^{\sigma^2} \in \langle a \rangle$  and hence  $\sigma^2$  belongs to  $N = N_{A_p}(a)$ , the normalizer of  $\langle a \rangle$  in  $A_p$ . As  $N$  is a proper subgroup of  $A_p$  containing  $a$ ,  $N \subseteq D_G(a)$  and so  $a^{i^2}$  is either  $a$  or  $a^{-1}$ . Hence  $i^2 \equiv \pm 1 \pmod{p}$ . As the order of  $i$  in  $\mathbb{Z}_p$  is  $p-1$ , necessarily  $i^2 \equiv -1 \pmod{p}$  and  $p = 5$ . Finally, to prove that  $a = (1, 2, 3, 4, 5)$  is dihedral 5-critical in  $A_5$  notice that  $N = N_{A_5}(a) = \langle a, (2, 5)(3, 4) \rangle = D_{A_5}(a)$  and  $G = \langle a, b \rangle$  for every  $b \in G \setminus N$ . This proves the claim.

A computer search, using GAP [5], showed that if  $q < 100$  is a prime integer then  $\text{PSL}(2, q)$  contains a dihedral  $p$ -critical element for some  $p \geq 5$  if and only if  $q = 5, 13, 37, 41, 43, 61, 67, 73, 79$  or  $97$ . For example,  $\text{PSL}(2, 5) \simeq A_5$ , so that, by the previous paragraph, the elements of order 5 in  $\text{PSL}(2, 5)$  are dihedral 5-critical. In  $\text{PSL}(2, 13)$  every element of order 7 is dihedral 7-critical and these are the only dihedral  $p$ -critical elements of  $\text{PSL}(2, 13)$  for  $p \geq 5$ .

We have also checked using GAP that the Mathieu simple groups have not dihedral  $p$ -critical elements with  $p \geq 5$ .

2. We believe that the conjecture stated in the introduction is true. By Theorem 4.3, it is enough to prove it for simple groups with a dihedral  $p$ -critical element with  $p \geq 5$ . By the previous remark, it is natural to expect that few simple groups have a dihedral  $p$ -critical element with  $p \geq 5$ . If this is true one could try to classify them and then prove the conjecture for those simple groups. Unfortunately we do not know how to classify the simple groups having dihedral  $p$ -critical elements.

3. One could also ask whether the conjecture is true for Bass cyclic units with infinite order modulo the centre based on elements of order non necessarily prime. Unfortunately our techniques does not seem to apply in this more general situation.

#### REFERENCES

- [1] H. Bass, *The Dirichlet unit theorem, induced characters and Whitehead groups of finite groups*, Topology 4 (1966) 391–410.
- [2] A. Dooms, E. Jespers and M. Ruiz, *Free groups and subgroups of finite index in the unit group of an integral group ring*, Comm. Algebra 35 no. 9 (2007) 2879–2888.
- [3] R. Ferraz, *Free subgroups in the units of  $\mathbb{Z}[K_8 \times C_p]$* , Comm. Algebra 31 no. 9 (2003) 4291–4299.
- [4] ———, *Groups generated by a Bass-cyclic unit and a bicyclic unit in the units of  $\mathbb{Z}[G]$* , J. Group Theory 7 (2004) 421–430.
- [5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2006, (<http://www.gap-system.org>).
- [6] J. Z. Goncalves and D. S. Passman, *Embedding free products in the unit group of an integral group ring*. Archiv der Mathematik 82 (2004) 97–102.
- [7] ———, *Linear groups and group rings*. J. Algebra 295 (2006), 94–118.
- [8] J. Z. Goncalves and Á. del Río, *Bicyclic units, Bass cyclic units and free groups*. J. Group Theory 11 (2008), 247–265.
- [9] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of finite simple groups*. Math. Surveys and Monographs V 40, N 1, 1994. AMS, Providence, RI.
- [10] 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.
- [11] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math. 78 no. 3 (1993) 303–315.
- [12] E. Jespers, Á. del Río and M. Ruiz, *Groups generated by two bicyclic units in integral group rings*, J. Group Theory 5 (2002), no. 4, 493–511.
- [13] Z.S. Marciniak and S.K. Sehgal, *Constructing free subgroups of integral group rings*, Proc. AMS 125 (1997) 1005–1009.
- [14] J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. 324 (1991), no. 2, 603–621.
- [15] A. Salwa, *On free subgroups of units of rings*, Proc. AMS 127 (1999) 2569–2572.
- [16] S.K. Sehgal, *Units in integral group rings*, Longman Scientific & Technical, Pitman Monographs, Surveys in Pure and Applied Mathematics 69, 1993.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SÃO PAULO, 05508-090, BRAZIL  
*E-mail address:* [jz.goncalves@usp.br](mailto:jz.goncalves@usp.br)

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE MURCIA, MURCIA 30100, SPAIN  
*E-mail address:* [adelrio@um.es](mailto:adelrio@um.es)