

Bicyclic units, Bass cyclic units and free groups*

Jairo Z. Gonçalves

Departamento de Matemática
Universidade de São Paulo
São Paulo, 05389-970, Brazil
jzg@ime.usp.br

Ángel del Río

Departamento de Matemáticas
Universidad de Murcia
Campus de Espinardo, Murcia 30100, Spain
adelrio@um.es

Abstract

Let G be a finite group and $\mathbb{Z}G$ its integral group ring. We show that if α is a non-trivial bicyclic unit of $\mathbb{Z}G$, then there are bicyclic units β and γ of different types, such that $\langle \alpha, \beta \rangle$ and $\langle \alpha, \gamma \rangle$ are non-abelian free groups. In case that G is non-abelian of order coprime with 6, then we prove the existence of a bicyclic unit u and a Bass cyclic unit v in $\mathbb{Z}G$, such that for every positive integer m big enough, $\langle u^m, v \rangle$ is a free non-abelian group.

1 Introduction

A *free pair* is by definition a pair formed by two generators of a non-abelian free group. Let G be a finite group. The existence of free pairs in the group of units $U(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$, was firstly proved by Hartley and Pickel [8], provided that G is neither abelian nor a Hamiltonian 2-group (equivalently $U(\mathbb{Z}G)$ is neither abelian nor finite). Their proof is not constructive and this raised the question of exhibiting a concrete free pair. This goal was achieved for non-Hamiltonian groups by Marciniak and Sehgal [12] using bicyclic units, and for Hamiltonian groups (non 2-group) by Ferraz [4] using Bass cyclic units. These results, together with a classical theorem of Bass [2], that states that if G is abelian then the Bass cyclic units generates a subgroups of finite index in $U(\mathbb{Z}G)$, and the more recent ones of Ritter and Sehgal [15] and Jespers and Leal [9], which prove that the group generated by the bicyclic and the Bass cyclic units generates a big portion of $U(\mathbb{Z}G)$, show that these two types of units have an important role in the structure of $U(\mathbb{Z}G)$. As a consequence, several authors have payed attention to the problem of describing the structure of the group generated either by bicyclic units, or Bass cyclic units and more specifically, to the problem of deciding when two bicyclic units or Bass cyclic units form a free pair [3, 7, 10, 16].

The *bicyclic units* of $\mathbb{Z}G$ are the elements of one of the following forms

$$\beta_{x,h} = 1 + (1-h)x(1+h+h^2+\dots+h^{d-1}), \quad \gamma_{x,h} = 1 + (1+h+h^2+\dots+h^{d-1})x(1-h),$$

where $x, h \in G$ and h has order d . Two bicyclic units are of *same type* if both are of type β or both are of type γ . Otherwise they are of *different types*.

The Bass cyclic units of $\mathbb{Z}G$ are the elements of the form

$$u_{k,m}(x) = (1+x+x^2+\dots+x^{k-1})^m + \frac{1-k^m}{d}(1+x+x^2+\dots+x^{d-1}),$$

*Research supported by Capes of Brazil, CNPq grant 303.756/82-5 and Fapesp, Projeto Tematico 00/07.291-0, D.G.I. of Spain and Fundación Séneca of Murcia.

where x is an element of order d and k and m are positive integers such that $\gcd(k, d) = 1$ and $\phi(d) | m$.

One says that a complex number z is *free* or that z is a *free point*, if the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$$

form a free pair¹. Otherwise z is said to be *non-free*. The most classical result on the subject is Sanov Theorem [17] which states that every complex number of modulus at least 4 is free. On the other hand every integer of modulus less than 4 is non-free. For an up-to-date list of results on the matter see [1].

If R is a ring of characteristic 0 then its elements can be considered as belonging to a complex algebra. Indeed, R embeds in $R \otimes_{\mathbb{Z}} \mathbb{C}$, since $_{\mathbb{Z}}\mathbb{C}$ is torsion-free and so it is flat. Thus it makes sense to talk on the transcendency of these elements over any subfield of \mathbb{C} . Moreover, left multiplication by elements of R can be considered as endomorphisms of the underlying vector space structure of the algebra. So we can refer to the eigenvalues of such endomorphism. Note that the eigenvalues do not depend on the algebra where R is included because the minimal polynomial is independent of the algebra. The first result of this paper is the following freeness criteria in terms of free points.

Theorem 1.1. *Let R be a ring of characteristic 0 and a and b elements of R such that $a^2 = b^2 = 0$. Then $(1 + a, 1 + b)$ is a free pair if and only, one of the following conditions hold:*

1. *ab is transcendental (over the rationals).*
2. *ab is algebraic (over the rationals) and one of the eigenvalues of ab is free.*

Notice that every bicyclic unit is of the form $1 + a$ for some $a \in \mathbb{Z}G$ such that $a^2 = 0$ and so Theorem 1.1 can be applied to pairs of bicyclic units. As an application of Theorem 1.1 we show a method to construct many free pairs of bicyclic units and in particular obtain.

Theorem 1.2. *If $\mathbb{Z}G$ has a non-trivial unit α then $\mathbb{Z}G$ has bicyclic units β and γ of different type, such that (α, β) and (α, γ) are free pairs.*

In fact the bicyclic units β and γ of Theorem 1.2 can be explicitly constructed (see Corollary 4.3). The existence of a free pair formed by bicyclic units of different types was already proven in [12]. Another consequence of Theorem 1.1 is a result of Salwa, which states that if a and b satisfy the conditions of Theorem 1.1 and ab is non-nilpotent then $(1 + a, (1 + b)^m = 1 + mb)$ is a free pair for some positive integer m . In Section 5 we discuss the minimal m for which $(1 + a, 1 + mb)$ is a free pair.

Then we consider groups generated by a bicyclic unit and a Bass cyclic unit. Gonçalves and Passman [7] proved recently that if G is a finite non-abelian group of order coprime with 6, then $\mathbb{Z}G$ has a free pair formed by Bass cyclic units. With the same assumptions we also prove:

Theorem 1.3. *If G is a finite non-abelian group of order coprime with 6, then $\mathbb{Z}G$ has a bicyclic unit β and a Bass cyclic unit u such that (u, β^t) is a free pair for any sufficiently large positive integer t .*

The hypothesis of the order of G being coprime with 6, in Theorem 1.3, is partially justified because for the existence of a non-trivial Bass cyclic unit one needs the exponent of the group G not being a divisor of 4 or 6. In the last section of the paper we prove that $\mathbb{Z}S_n$ (respectively, $\mathbb{Z}A_n$) has a free pair formed by a Bass cyclic unit and a bicyclic unit if and only if $n \geq 5$.

¹Some authors define free points by considering $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ as the first matrix. The two definitions are somehow equivalent because z is free under this definition if and only if $2z$ is free under our definition.

2 Proof of Theorem 1.1

For the proof of Theorem 1.1 we first prove some lemmas. The first one was already proved in [6] for $K = \mathbb{C}$ and the same proof works in general. We include a proof for completeness.

Lemma 2.1. *Let K be a field of characteristic 0 and a and b be elements of a K -algebra such that $a^2 = b^2 = 0$. If ab is transcendental over K then $K[a, b]$ is naturally isomorphic to the relatively free algebra $K[x, y | x^2 = y^2 = 0]$.*

Proof. Let f_1, f_2, f_3 and f_4 be polynomials in one variable with coefficients in K such that

$$f_1(ab) + f_2(ab)a + bf_3(ab) + bf_4(ab)a = 0.$$

Multiplying on both sides by ab one has $abf_1(ab)ab = 0$ and hence $f_1 = 0$, by the transcendency of ab over K . Then multiplying by ab on the left and by b on the right, one has $abf_2(ab)ab = 0$ and so $f_2 = 0$. By symmetry one has $f_3 = 0$. Finally multiplying by a on the left and by b on the right one deduces $abf_4(ab)ab = 0$ and this yields $f_4 = 0$.

This proves that the elements of the form $(ab)^i, (ab)^i a, b(ab)^i$ and $b(ab)^i a$ are linearly independent over K . Therefore the algebra homomorphism $f : K[x, y | x^2 = y^2 = 0] \rightarrow K[a, b]$ given by $f(x) = a$ and $f(y) = b$ is an isomorphism. \square

Lemma 2.2. *Let $R = R_1 \times \dots \times R_n$ be a direct product of rings, and $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$ be units of R , with $u_i, v_i \in R_i$ for every i . Then (u, v) is a free pair if and only if (u_i, v_i) is a free pair for some i .*

Proof. Without loss of generality we can assume that $n = 2$. The sufficient condition is clear. Assume that neither (u_1, v_1) nor (u_2, v_2) is a free pair. Then there are non-trivial words w_1 and w_2 in the free group on two symbols such that $a_i = w_i(u_i, v_i) = 1$ for $i = 1, 2$. If the commutator $w = w_1 w_2 w_1^{-1} w_2^{-1} \neq 1$ then

$$\begin{aligned} w(u, v) &= (a_1 w_2(u_1, v_1) a_1^{-1} w_2^{-1}(u_1, v_1), w_1(u_2, v_2) a_2 w_1^{-1}(u_2, v_2) a_2^{-1}) \\ &= ((w_2(u_1, v_1) w_2^{-1}(u_1, v_1), w_1(u_2, v_2) w_1^{-1}(u_2, v_2)) = (1, 1) = 1. \end{aligned}$$

Otherwise w_1 and w_2 belongs to a cyclic group and therefore there is $1 \neq w \in \langle w_1 \rangle \cap \langle w_2 \rangle$. Then $w(u, v) = 1$. So in both cases (u, v) is not a free pair. \square

Lemma 2.3. *If $R = M_m(\mathbb{C}) = \mathbb{C}[a, b]$ with $a^2 = b^2 = 0$, then $m \leq 2$. Furthermore $m = 1$ if and only if ab is nilpotent.*

Proof. For a real number α , let $[\alpha]$ denote the greatest integer non greater than α . Consider the elements of R as endomorphisms of \mathbb{C}^n . Then $\dim_{\mathbb{C}} \text{Im}(ab) \leq \text{Im}(a) \leq [\frac{m}{2}]$, because $\text{Im}(a) \subseteq \ker(a)$. Then, by the Cayley-Hamilton Theorem, the degree of the minimal polynomial of ab over \mathbb{C} is $\leq [\frac{m}{2}] + 1$. On the other hand $R = \mathbb{C}[ab] + b\mathbb{C}[ab] + \mathbb{C}[ab]a + b\mathbb{C}[ab]a$. Hence $m^2 = \dim_{\mathbb{C}} \text{End}_{\mathbb{C}}(\mathbb{C}^m) \leq 4([\frac{m}{2}] + 1)$ and so $m \leq 2$. This shows that $m \leq 2$.

If $m = 1$ then clearly ab is nilpotent. By means of contradiction assume that $m = 2$ and ab is nilpotent. After conjugating by some invertible matrix one may assume that $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Then the second row of ab is 0 and, since ab is nilpotent, also the (1,1)-entry is 0. Then $b = \begin{pmatrix} 0 & \mu \\ 0 & 0 \end{pmatrix}$ for some μ . Therefore $ab = ba$, contradicting the assumption $M_2(\mathbb{C}) = \mathbb{C}[a, b]$. \square

Now we prove Theorem 1.1.

Let R be a ring of characteristic 0 and $a, b \in R$ such that $a^2 = b^2 = 0$. By replacing R by $\mathbb{C} \otimes_{\mathbb{Z}} R$ if needed one may assume that R is a \mathbb{C} -algebra. If $ab = ba$ then $\langle 1 + a, 1 + b \rangle$ is not free and 0 is the only eigenvalue of ab , hence the Theorem holds. In the remainder of the proof we assume that $ab \neq ba$.

Assume first that $R = M_2(\mathbb{C}) = \mathbb{C}[a, b]$ and identify R with the ring of endomorphism of a 2-dimensional vector space over \mathbb{C} . Since $\ker(ab) \subseteq \ker(b) \neq 0$, one of the eigenvalues of ab is 0. Let λ be the other eigenvalue. By Lemma 2.3, ab is not nilpotent and so $\lambda \neq 0$. Hence ab is diagonalizable and after some suitable conjugation, one may assume that $ab = \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix}$. Then $\ker(b) = \ker(ab)$ and $\text{Im}(a) = \text{Im}(ab)$ and hence

$$a = \begin{pmatrix} 0 & \mu \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 0 \\ \lambda & 0 \end{pmatrix}$$

for some $0 \neq \mu \in \mathbb{C}$. Conjugating by the matrix $\begin{pmatrix} \frac{1}{\mu} & 0 \\ 0 & 1 \end{pmatrix}$ one may assume that

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 0 \\ \lambda & 0 \end{pmatrix}$$

and so $(1 + a, 1 + b)$ is a free pair if and only if λ is free. Note that ab is transcendental over \mathbb{Q} if and only if so is λ and in this case λ is free.

Now we consider the general case.

If ab is transcendental (over \mathbb{Q}) then, by Lemma 2.1, there is an algebra homomorphism $\mathbb{Q}[a, b] \rightarrow M_2(\mathbb{Q})$ mapping a to $\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and b to $\beta = \begin{pmatrix} 0 & 0 \\ 4 & 0 \end{pmatrix}$. Since 4 is a free-point, $(1 + \alpha, 1 + \beta)$ is a free pair and thus $(1 + a, 1 + b)$ is also a free pair.

Assume now that ab is algebraic (over \mathbb{Q}). We may assume without loss of generality that $R = \mathbb{C}[a, b]$. Then $\dim_{\mathbb{C}} \mathbb{C}[ab] < \infty$ and $R = \mathbb{C}[ab] + b\mathbb{C}[ab] + a\mathbb{C}[ba] + b\mathbb{C}[ab]a$. Thus $\dim_{\mathbb{C}} R \leq 4 \dim_{\mathbb{C}} \mathbb{C}[ab] < \infty$. Therefore, if J denotes the Jacobson radical of R then J is nilpotent and R/J is semisimple. The first implies that $1 + J$ is a nilpotent normal subgroup of the group of units of R . Hence $(1 + J) \cap \langle 1 + a, 1 + b \rangle$ is nilpotent and so $\langle 1 + a, 1 + b \rangle$ is free if and only if $\langle 1 + a + J, 1 + b + J \rangle$ is free. Also from the nilpotency of J it follows that the minimal polynomial of ab divides a power of the minimal polynomial of $ab + J$. We conclude that one may assume without loss of generality that $J = 0$ and so R is semisimple. Then $R = \bigoplus_{i=1}^k A_i$ with $A_i \simeq M_{n_i}(\mathbb{C})$ and $n_i \leq 2$ for every i , by Lemma 2.3. If $x \in R$ and $1 \leq i \leq k$ then x_i denotes the projection of x in A_i .

Assume first that one of the eigenvalues λ of ab is free. Then λ is an eigenvalue of $a_i b_i$ for some $1 \leq i \leq k$. Moreover, $n_i = 2$ because if $n_i = 1$ then $a_i = b_i = 0$. By the first part of the proof, $(1 + a_i, 1 + b_i)$ is a free pair of A_i . Thus $\langle 1 + a, 1 + b \rangle$ is a free pair.

Conversely, assume that $(1 + a, 1 + b)$ is a free pair of R . By Lemma 2.2, there is $1 \leq i \leq k$ such that $(1 + a_i, 1 + b_i)$ is a free pair. Clearly $n_i = 2$ and, by the first part of the proof, one of the eigenvalues of $a_i b_i$ is free. Then one of the eigenvalues of ab is free and this finishes the proof of Theorem 1.1.

3 Applications of Theorem 1.1

A first application of Theorem 1.1 is the following corollary. The second statement appeared in [16] and a weak version of the third one appeared in [10].

Corollary 3.1. *Let R be a ring of characteristic 0. Let $\alpha = 1 + a$ and $\beta = 1 + b$ be units of R with $a^2 = b^2 = 0$.*

1. *If m and n are positive integers then (α^m, β^n) is a free pair if and only if (α, β^{mn}) is a free pair.*
2. *If ab is not nilpotent then (α, β^m) is a free pair for some positive integer m .*
3. *ab is nilpotent if and only if $\langle 1 + a, 1 + b \rangle$ is nilpotent. Moreover, if ab is algebraic over \mathbb{C} then, $\langle 1 + a, 1 + b \rangle$ is nilpotent if and only if 0 is the only eigenvalue of ab .*

Proof. (1) Is an obvious consequence of Theorem 1.1 because $\alpha^m = 1 + ma$ and $\beta^n = 1 + nb$.

(2) and (3). Firstly assume that ab is nilpotent and let S be the multiplicative semigroup generated by a and b . Then there is a positive number n such that $s^n = 0$ for each $s \in S$. This implies that $1 + S$ is a nilpotent subgroup of the group of units of R . Hence $\langle 1 + a, 1 + b \rangle$ is nilpotent.

Secondly assume that ab is transcendental over \mathbb{Q} . Then (α, β) is a free pair, by Theorem 1.1, and so (2) holds for $m = 1$ and $\langle 1 + a, 1 + b \rangle$ is not nilpotent.

Thirdly assume that ab has a non-zero eigenvalue λ . Let m be a positive integer such that $|m\lambda| \geq 4$. Then $m\lambda$ is an eigenvalue of mab and $m\lambda$ is free by Sanov Theorem. Therefore $(\alpha = 1 + a, \beta^m = 1 + mb)$ is a free pair, by Theorem 1.1, and hence $\langle \alpha, \beta \rangle$ is not nilpotent.

Finally, if ab is algebraic over \mathbb{Q} and 0 is the only eigenvalue of ab then ab is nilpotent. \square

Corollary 3.2. *Let a and b be elements of a finite dimensional \mathbb{C} -algebra A , such that $a^2 = b^2 = 0$. Then $(1 + a, 1 + b)$ is a free pair (resp. $\langle 1 + a, 1 + b \rangle$ is nilpotent) if and only if there is an irreducible representation ρ of A such that one of the eigenvalues of $\rho(ab)$ is free (resp. 0 is the only eigenvalue of $\rho(ab)$ for each irreducible representation ρ of A).*

Proof. It follows from Theorem 1.1 because the set of eigenvalues of an element x of A is the union of the sets of eigenvalues of $\rho(x)$, for ρ running on the irreducible representations of A . \square

Corollary 3.3. *Let G be a finite group, with the property that all the (complex) irreducible characters of G have degree ≤ 3 . Let $\mathbb{C}G$ be the complex group algebra of G , and let $a, b \in \mathbb{C}G$ be such that $a^2 = b^2 = 0$. Then $(1 + a, 1 + b)$ is a free pair (resp. $\langle 1 + a, 1 + b \rangle$ is nilpotent) if and only if $\chi(ab)$ is free for some irreducible character χ of G (resp. $\chi(ab) = 0$ for every irreducible character χ of G).*

Proof. Let ρ be an irreducible representation of G of degree n , $[n/2]$ the greater integer less or equal than $n/2$, and χ the character afforded by ρ . Then $\dim_{\mathbb{C}} \text{Im}(\rho(ab)) \leq \dim_{\mathbb{C}} \text{Im}(\rho(a)) \leq [n/2] \leq 1$, because $\text{Im}(\rho(a)) \subseteq \ker(\rho(a))$ and $n \leq 3$. This shows that the eigenvalues of $\rho(ab)$ are 0 and $\chi(ab)$. Now the result follows from Corollary 3.2. \square

A trace map on a complex algebra A is a \mathbb{C} -linear form $T : A \rightarrow \mathbb{C}$ satisfying the following conditions for $x, y \in A$: $T(xy) = T(yx)$; if x is nilpotent then $T(x) = 0$; and if $0 \neq x = x^2$ then $T(x)$ is a positive real number. For example, the classical trace $\text{tr} : M_n(\mathbb{C}) \rightarrow \mathbb{C}$ is a trace map on $M_n(\mathbb{C})$. An easy argument shows that if T is a trace map on $M_n(\mathbb{C})$ then $T = \alpha \text{tr}$ for some positive real number α (namely $\alpha = T(1)/n$).

Corollary 3.4. [16] *Let R be a ring of characteristic 0 and $a, b \in R$ with $a^2 = b^2 = 0$. If $\mathbb{C} \otimes_{\mathbb{Z}} R$ has a trace map T such that $|T(ab)| \geq 2T(1)$ then $(1 + a, 1 + b)$ is a free pair.*

Proof. By the definition of trace map, ab is not nilpotent. If ab is transcendental over \mathbb{Q} , then the result follows at once from Theorem 1.1.

Otherwise, one may assume that $R = \mathbb{C}[a, b]$. By Lemma 2.3, $R/J \simeq \prod_{i=1}^k M_{n_i}(\mathbb{C})$ with $n_i \leq 2$. Suppose that $n_i = 1$ if $i > l$ and $n_i = 2$, otherwise. Since R is artinian, $T(J) = 0$, because J is nilpotent, and idempotents lift modulo J . Thus T induces a trace map \bar{T} on R/J . For each i , the restriction of \bar{T} to $M_{n_i}(\mathbb{C})$ is a trace map $T_i = \alpha_i \text{tr}$ on $M_{n_i}(\mathbb{C})$. One of the eigenvalues of $a_i b_i$ is 0. If $n_i = 2$, then let λ_i be the other eigenvalue of $a_i b_i$. Then

$$4 \sum_{i=1}^l \alpha_i \leq 2 \sum_{i=1}^k n_i \alpha_i = 2T(1) \leq T(ab) = \sum_{i=1}^k \alpha_i \text{tr}(a_i b_i) = \sum_{i=1}^l \alpha_i \lambda_i$$

and therefore $|\lambda_i| \geq 4$ for some i . Since λ_i is an eigenvalue of ab , $(1+a, 1+b)$ is a free pair by Theorem 1.1. \square

4 Bicyclic units

In this section G stands for an arbitrary group. The notation $H \leq G$ means that H is a subgroup of G . If A is a subset of G then $\langle A \rangle$ denotes the subgroup generated by A . If moreover A is finite then we write $\bar{A} = \sum_{a \in A} a \in \mathbb{Z}G$. If $g \in G$ has finite order then we abbreviate $\bar{g} = \overline{\langle g \rangle}$.

Let H be a finite subgroup of G , $h \in H$ and $x \in G$. Then $(1-h)x\bar{H}$ and $\bar{H}x(1-h)$ are elements of $\mathbb{Z}G$ of square zero and therefore

$$\beta_{x,h,H} = 1 + (1-h)x\bar{H} \quad \text{and} \quad \gamma_{x,h,H} = 1 + \bar{H}x(1-h)$$

are units of $\mathbb{Z}G$. So the bicyclic units of $\mathbb{Z}G$ are the elements of one of the following forms

$$\beta_{x,h} = \beta_{x,h,\langle h \rangle} = 1 + (1-h)x\bar{h} \quad \text{and} \quad \gamma_{x,h} = \gamma_{x,h,\langle h \rangle} = 1 + \bar{h}x(1-h),$$

where $x, h \in G$ and h has finite order.

If $a = \sum_{g \in G} a_g g \in \mathbb{C}G$ then the *trace* of a is by definition $T(a) = a_1$. Notice that T is a trace map on $\mathbb{C}G$ as defined in Section 3. This is clear if G is finite because then the trace of the regular representation of $\mathbb{C}G$ is $|G|T$. For a proof for infinite groups see [14, Lemma 1.7 in page 37 and Lemma 3.3 in page 47].

Lemma 4.1. *Let $x, y \in G$ and $H, K \leq G$. Then $\bar{H}x\bar{K} = |H \cap xKx^{-1}| \cdot \overline{HxK}$ and*

$$T(y\bar{H}x\bar{K}) = \begin{cases} |H \cap xKx^{-1}|, & \text{if } y^{-1} \in HxK \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Consider the map $f : H \times K \rightarrow HxK$, given by $f(h, k) = h x k$. Clearly $\bar{H}x\bar{K} = \sum_{y \in HxK} |f^{-1}(y)| y$. It is easy to see that the map $f^{-1}(x) \rightarrow f^{-1}(h x k)$, given by $(h_1, k_1) \mapsto (h h_1, k_1 k)$ is bijective. Using the equality $|H||K| = |HxK| \cap |H \cap xKx^{-1}|$ one deduces that $|f^{-1}(y)| = |H \cap xKx^{-1}|$ for every $y \in HxK$ and hence $\bar{H}x\bar{K} = |H \cap xKx^{-1}| \overline{HxK}$. Then $T(y\bar{H}x\bar{K}) = 0$ if $y^{-1} \notin HxK$ and otherwise $T(y\bar{H}x\bar{K}) = |H \cap xKx^{-1}|$, as asserted. \square

Proposition 4.2. *Let $H \leq K$ be finite subgroups of a group G and let $x \in G$, $h \in H$ and $k \in K$ be such that $x^{-1}hx \notin K$.*

1. *If $x^{-1}kx \notin K$ then $(\beta_{x,h,H}, \gamma_{x^{-1},k,K})$ is a free pair.*
2. *If $xkx^{-1} \notin K$ then $(\beta_{x,h,H}, \beta_{x^{-1},xkx^{-1},xKx^{-1}})$ is a free pair.*

Proof. Let $a = \gamma_{x^{-1},k,K} - 1$ and $b = \beta_{x,h,H} - 1$. Then

$$ab = \overline{K}x^{-1}(1-k)(1-h)x\overline{H} = \overline{K}(1-x^{-1}kx - x^{-1}hx + x^{-1}kx)\overline{H},$$

and using Lemma 4.1 one has

$$\begin{aligned} T(\overline{K}x^{-1}hx\overline{H}) &= T(\overline{K}x^{-1}kx\overline{H}) = 0, \\ T(\overline{K}\overline{H}) &= |H| \quad \text{and} \quad T(\overline{K}x^{-1}kx\overline{H}) \geq 0. \end{aligned}$$

Therefore $T(ab) \geq |H| \geq 2 = 2T(1)$. Then $(\beta_{x,h,H}, \gamma_{x^{-1},k,K})$ is a free pair by Corollary 3.4. Let now $a = \beta_{x,h,H} - 1$ and $b = \beta_{x^{-1},xkx^{-1},xKx^{-1}} - 1$. Then

$$\begin{aligned} ab &= (1-h)x\overline{H}(1-xkx^{-1})x^{-1}\overline{xKx^{-1}} \\ &= x\overline{H}x^{-1}\overline{xKx^{-1}} - hx\overline{H}x^{-1}\overline{xKx^{-1}} - x\overline{H}xkx^{-2}\overline{xKx^{-1}} + hx\overline{H}xkx^{-2}\overline{xKx^{-1}}. \end{aligned}$$

As in the previous case $T(x\overline{H}x^{-1}\overline{xKx^{-1}}) = |H|$ and $T(hx\overline{H}xkx^{-2}\overline{xKx^{-1}}) \geq 0$. Furthermore $(hx)^{-1} \notin Hx^{-1}(xKx^{-1}) = HKx^{-1} = Kx^{-1}$ because $x^{-1}hx \notin K$ and $x^{-1} \notin Hxkx^{-2}(xKx^{-1}) = Hxkx^{-1}Kx^{-1}$, because $xkx^{-1} \notin K = HK$. Thus $1 \notin Hxkx^{-1}K$, hence Lemma 4.1 yields $0 = T(hx\overline{H}x^{-1}\overline{xKx^{-1}}) = T(x\overline{H}xkx^{-2}\overline{xKx^{-1}})$ and so $T(ab) \geq 2$. Again one deduces that $(\beta_{x,h,H}, \beta_{x^{-1},xkx^{-1},xKx^{-1}})$ is a free pair from Corollary 3.4. \square

Theorem 1.2 is a direct consequence of the following.

Corollary 4.3. *Let x and h be elements of a group and assume that h has finite order. Then the following conditions are equivalent.*

- | | |
|---|--|
| (1) $x^{-1}hx \notin \langle h \rangle$. | (5) $(\beta_{x,h}, \beta_{x^{-1},xhx^{-1}})$ is a free pair. |
| (2) $xhx^{-1} \notin \langle h \rangle$. | (6) $(\beta_{x,h}, \gamma_{x^{-1},h})$ is a free pair. |
| (3) $\beta_{x,h} \neq 1$. | (7) $(\gamma_{x,h}, \beta_{x^{-1},h})$ is a free pair. |
| (4) $\gamma_{x,h} \neq 1$. | (8) $(\gamma_{x,h}, \gamma_{x^{-1},xhx^{-1}})$ is a free pair. |

Proof. The equivalence between the first four conditions is obvious. The equivalence with (5) and (6) is a consequence of Proposition 4.2 and the equivalence with (7) and (8) follows by symmetry. \square

5 Examples and questions. Bicyclic units

Corollary 3.1 raised some natural questions. For a finite group G let

$$\begin{aligned} M(G) &= \min\{m \in \mathbb{N} : (\alpha, \beta^m) \text{ is a free pair for every } \alpha = 1 + a \text{ and } \beta = 1 + b \\ &\quad \text{bicyclic units of } \mathbb{Z}G \text{ with } ab \text{ not nilpotent}\}, \\ m(G) &= \min\{m \in \mathbb{N} : (\alpha, \beta^m) \text{ is a free pair for every } \alpha = 1 + a \text{ and } \beta = 1 + b \\ &\quad \text{bicyclic units of the same type of } \mathbb{Z}G \text{ with } ab \text{ not nilpotent}\}. \end{aligned}$$

By Theorem 3.1 one has: G is Hamiltonian if and only if $M(G) = \infty$ if and only if $m(G) = \infty$. (Here we are using the convention that the minimum of the empty set is ∞ .)

Problem 5.1. Compute $M(G)$ and $m(G)$ for some (non-Hamiltonian) finite groups G .

Finding a finite group G with $1 < M(G) \neq \infty$ is easy.

Example 5.2. $M(S_3) = 2$.

Proof. Let S_3 be the symmetric group on three symbols. Recall that S_3 has two linear characters χ_1 and χ_2 and one irreducible character χ_3 of degree 2. Then $6T = \chi_1 + \chi_2 + 2\chi_3$ is the character afforded by the regular representation of G . If $\alpha = 1 + a$ and $\beta = 1 + b$ are bicyclic units then $\chi_1(ab) = \chi_2(ab) = 0$ and therefore $\chi_3(ab) = 3T(ab)$. Then applying Corollary 3.3 one has: If $T(ab) = 0$ then $\chi_3(ab) = 0$ and therefore ab is nilpotent and $\langle \alpha, \beta \rangle$ is a nilpotent group; if $|T(ab)| > 1$ then $|\chi_3(ab)| \geq 4$ and therefore (α, β) is a free pair. Otherwise, (that is if $T(ab) = \pm 1$), then (α, β) is not a free pair (because 3 is non-free) but (α, β^2) is a free pair. This shows that $M(S_3) \leq 2$. To show that the equality holds we exhibit a pair of bicyclic units α and β such that $T(ab) = 1$.

Let $\sigma = (1, 2, 3)$, $\tau = (1, 2)$ and consider the bicyclic units $\alpha = \gamma_{\sigma, \tau} = 1 + a$ and $\beta = \beta_{\sigma^2, \sigma\tau} = 1 + b$. We see that $T(ab) = 1$ by using Lemma 4.1 and noticing that $1, \tau, \sigma^2 \in \langle \tau \rangle \langle \sigma\tau \rangle = \{1, \tau, \sigma\tau, \sigma^2\}$, $\sigma^2\tau \notin \langle \tau \rangle \langle \sigma\tau \rangle$, $\langle \tau \rangle \cap \sigma^2 \langle \sigma\tau \rangle \sigma^{-2} = \langle \tau \rangle \cap \langle \sigma\tau \rangle = \{1\}$, $\langle \tau \rangle \cap \tau \langle \sigma\tau \rangle \tau^{-1} = \langle \tau \rangle \cap \langle \sigma^2\tau \rangle = \{1\}$ and

$$ab = \bar{\tau}(1 - \sigma\tau\sigma^2 - \sigma\sigma\tau\sigma^2 + \sigma\tau\sigma\tau\sigma^2)\bar{\sigma\tau} = \bar{\tau}(1 - \sigma^2\tau - \tau + \sigma^2)\bar{\sigma\tau}.$$

□

Finding a finite group G such that $1 < m(G) \neq \infty$ is more difficult. For example, if D_{2n} denotes the dihedral group of order $2n$ and n is prime then $m(D_{2n}) = 1$ [10]. This has been recently generalized by Jiménez [11] who, using Corollary 3.3, have shown that $m(D_{2n}) \leq 2$ for every n and, if 12 does not divide n , then $m(D_{2n}) = 1$. In fact the result of Jiménez shows that if 12 divides n then $m(D_{2n}) = 1$ if and only if $2\sqrt{3}$ is free, and otherwise $m(D_{2n}) = 2$. More examples of finite groups G with $m(G) = 1$ can be founded in [3]. Since we still do not know if $2\sqrt{3}$ is free it is not clear whether dihedral groups provides examples of non Hamiltonian groups G for which $m(G) > 1$. We found that S_4 provides such an example as an application of Corollary 3.3.

Example 5.3. $m(S_4) = 2$.

Proof. Having in mind that each irreducible character of S_4 takes values on the integers and that an integer m is free if and only if $|m| \geq 4$, it is not difficult to compute $m(S_4)$ using Corollary 3.3 and an algebraic software package. First, compute all the bicyclic units of one type: there are 157. Then compute $\chi(ab)$ for all the pairs $(\alpha = 1 + a, \beta = 1 + b)$ of bicyclic units. It turns out that either $\chi(ab) = 0$ for all the irreducible characters χ of S_4 or there is an irreducible character χ such that $|\chi(ab)| \geq 2$. In the former case $\langle \alpha, \beta \rangle$ is nilpotent and in the latter (α, β^2) is a free pair. This shows that $m(S_4) \leq 2$ and in fact the equality holds because there is a pair $(\alpha = 1 + a, \beta = 1 + b)$ such that $|\chi(ab)|$ is either 0 or 2 for each irreducible character χ . For the readers convenience we give a computer-free proof.

We choose the following set of generators of S_4 .

$$\sigma = (1, 2, 3), \quad \tau = (1, 2), \quad \mu = (1, 2)(3, 4), \quad \nu = (1, 3)(2, 4).$$

Let $\pi : \mathbb{Z}S_4 \rightarrow \mathbb{Z}S_3$ be the ring homomorphism which acts as the identity on S_3 and maps μ and ν to 1. Let χ_1, χ_2 and χ_3 be the three irreducible characters of S_3 (Example 5.2). Then S_4 has two linear characters, $\theta_1 = \chi_1 \circ \pi$ and $\theta_2 = \chi_2 \circ \pi$; one irreducible character of degree 2, $\theta_3 = \chi_3 \circ \pi$; and two irreducible characters θ_4 and θ_5 of degree 3. Observe also that $\theta_i(g) \in \mathbb{Z}$ for each $g \in S_4$ and $i \leq 5$. Furthermore $\theta_1(g) \equiv \theta_2(g) \equiv 1 \pmod{2}$, $\theta_4(g) \equiv \theta_5(g) \not\equiv \theta_3(g) \pmod{2}$ and if $\theta_3(g)$ is odd then g is a 3-cycle.

Let $\alpha = 1 + a$ and $\beta = 1 + b$ be bicyclic units of the same type of $\mathbb{Z}S_4$ such that ab is not nilpotent but (α, β) is not a free pair. Then $\pi(\alpha)$ and $\pi(\beta)$ are powers of bicyclic units

of $\mathbb{Z}S_3$ and $(\pi(\alpha), \pi(\beta))$ is not a free pair. Since $m(S_3) = 1$, $\pi(ab)$ is nilpotent and thus $0 = \theta_1(ab) = \theta_2(ab) = \theta_3(ab)$. Therefore the number of 3-cycles in the support of ab is even and thus $\theta_4(ab) \equiv \theta_5(ab) \equiv \theta_1(ab) = 0 \pmod{2}$. Since ab is not nilpotent, either $\theta_4(ab) \neq 0$ or $\theta_5(ab) \neq 0$ and thus the absolute value of one of them is at least 2. Then either $2\theta_4(ab)$ or $2\theta_5(ab)$ is free and so (α, β^2) is a free pair. This proves that $m(S_4) \leq 2$.

To show $m(S_4) = 2$ we consider the bicyclic units

$$\alpha = \beta_{\mu\tau, \nu} = 1 + a \quad \text{and} \quad \beta = \beta_{\mu\nu\sigma^2\tau, \nu\sigma} = 1 + b.$$

As in Example 5.2 we prove that (α, β) is not a free pair by showing that $\theta(x)$ is non-free for every irreducible character χ of S_4 . Obviously $\theta_1(ab) = \theta_2(ab) = 0$. Furthermore $\pi(b) = 0$ because $\pi(\nu\sigma) = \sigma$ generates a normal subgroup of S_3 , and thus $\theta_3(ab) = 0$. Now a straightforward computation shows that $\theta_4(ab) = -\theta_5(ab) = \pm 2$, which is non-free. \square

The previous computations raised the following.

Question 5.4. Is there a positive integer m such that $m(G) \leq m$, for every non-Hamiltonian finite group G ? Is $m(G) \leq 2$ for every non-Hamiltonian finite group G ?

6 Proof of Theorem 1.3

The proof of Theorem 1.3 uses the following Theorem of Gonçalves and Passman [7].

Theorem 6.1. *Let V be a finite dimensional vector space V over \mathbb{C} and S and τ endomorphisms of V . Assume that $\tau^2 = 0$ and S is diagonalizable. Let r_+ and r_- be the maximum and minimum of the absolute values of the eigenvalues of S . Let V_+ (resp. V_-) be the subspace generated by the eigenvectors of V with eigenvalue of modulus r_+ (resp. r_-) and V_0 the subspace generated by the remaining eigenvectors.*

If the four intersections $V_{\pm} \cap \ker(\tau)$ and $\text{Im}(\tau) \cap (V_0 \oplus V_{\pm})$ are trivial then $(S^s, (1 + \tau)^t)$ is the free product of $\langle S^s \rangle$ and $\langle (1 + \tau)^t \rangle$ for sufficiently large positive integers s and t .

Let d, k and m be positive integers such that k and d are relatively prime, and m a multiple of $\phi(d)$. Here ϕ stands for the Euler function. Since $k^m \equiv 1 \pmod{d}$ the polynomial

$$u_{k,m,d}(X) = (1 + X + X^2 + \dots + X^{k-1})^m + \frac{1 - k^m}{d}(1 + X + X^2 + \dots + X^{d-1})$$

has integral coefficients.

Notice that the Bass cyclic units of $\mathbb{Z}G$ are the elements of the form $u_{k,m}(x) = u_{k,m,d}(x)$, where x is an element of order d in the group G and k and m satisfy the above conditions. If ξ is a complex root d -th root of unity then $u_{k,m,d}(\xi) = u_{k,m}(\xi)$ is a well defined unit of $\mathbb{Z}[\xi]$. Using this it is easy to see that the Bass cyclic units of $\mathbb{Z}G$ belong to $U(\mathbb{Z}G)$. See [7] and [18] for other properties of Bass cyclic units. Notice that $u_{k,m}(x)$ is determined by k modulo d , and hence one can assume that $1 \leq k \leq d - 1$. Moreover $u_{1,m}(x) = 1$, $u_{d-1,m}(x) = x^{(d-1)m}$ and $u_{k,m}(x)^a = u_{k,am}(x)$, for each integer a [7, Lemma 3.1]. Therefore the set of Bass cyclic units of $\mathbb{Z}G$ is closed under taking powers and $u_{k,m}(x)$ has finite order if and only if $k \equiv \pm 1 \pmod{d}$.

Let G be a finite group of order coprime with 6. We have to show that $\mathbb{Z}G$ has a free pair formed by a bicyclic unit and a Bass cyclic unit. We start with a reduction argument.

Claim 1. *One may assume that the group $G = A \rtimes X$ where $X = \langle x \rangle$ has prime order (say p), and one of the following conditions hold:*

1. A is cyclic of prime power order.
2. A is an elementary abelian p -group of order p^2 .
3. A is an elementary abelian q -group, with q prime distinct from p , and X acts faithfully and irreducibly on A .

Notice that if Theorem 1.3 holds for some subgroup or some epimorphic image of G then it also holds for G . This is clear if H is a subgroup of G because a Bass cyclic unit (respectively, bicyclic unit) of $\mathbb{Z}H$ is also a Bass cyclic unit (respectively, bicyclic unit) of $\mathbb{Z}G$. Assume that H is an epimorphic image of G , u_1 is a Bass cyclic unit of $\mathbb{Z}H$ and β_1 is a bicyclic unit of $\mathbb{Z}H$ such that (u_1, β_1^s) is free for s sufficiently large. Then $\mathbb{Z}G$ has a Bass cyclic unit u and a bicyclic unit β such that u projects to u_1^k and β projects to β_1^l for some $k, l \geq 0$ [7, Lemma 3.2]. Thus (u, β^s) is a free pair of $\mathbb{Z}G$, for s sufficiently large. Thus arguing by induction to prove Theorem 1.3, one may assume without loss of generality that all the proper subgroups and proper epimorphic images of G are abelian. Then a theorem of [13] shows that the group G is as stated in the claim. This proves Claim 1.

So, in the remainder we assume that G is as in Claim 1, with $p, q \geq 5$, and we refer to cases (1), (2) and (3), depending on which condition holds. Since G is non-abelian, X is not normal in G , and therefore $x^a \notin X$ for some $a \in A$ that will be fixed until the end of the proof. For example, in Case (1), a can be a generator of A . In Case (2) one can take $a \in A$ such that $Z(G) = \langle b = a^x a^{-1} \rangle$. In Case (3), $Z(G) = 1$, and thus every non-trivial element of A satisfies the required condition.

Let x and a be as above and let q be the order of a . (Notice that this notation is compatible with the notation in Case (3); in Case (1) q is a power of p and; in Case (2) $q = p$.) We fix $2 \leq k \leq q - 2$ (recall that $q \geq 5$) and let

$$u = u_{k,m}(a), \quad \text{and} \quad \beta = 1 + (1 - x)a\hat{x}$$

for m a multiple of $\phi(d)$. Later on we will specify some additional condition on m . Notice that u and β have infinite order.

Claim 2. There is a linear representation χ of A such that the induced representation $\rho = \chi^G$ is irreducible, $\rho((a, x)) \neq 1$ and in Case (3), either $|A| = q$ or $a \in \ker(\chi)$.

Since the commutator $(a, x) \neq 1$, there is an irreducible representation (necessarily non-linear) ρ of G such that $\rho((a, x)) \neq 1$. All the non-linear irreducible representations of G are induced from linear representations of A and so the claim is clear except for the exceptional case (3) with $|A| \neq q$. In this case A has a maximal subgroup B containing a and so there is a linear representation χ of A with $\ker(\chi) = B$. Since X acts irreducibly on A and the subgroups G' and $C = \langle a^{x^i} : i = 0, 1, \dots, p-1 \rangle$ of A are invariant under this action, one has $A = G' = C$. The first equality implies that χ^G is irreducible and the second that $a^{x^i} \notin \ker(\chi)$ for some i . Therefore $\rho(a) = \text{diag}(\chi(a) = 1, \chi(a^x), \chi(a^{x^2}), \dots, \chi(a^{x^{p-1}})) \neq \text{diag}(\chi(a^x), \chi(a^{x^2}), \dots, \chi(a^{x^{p-1}}), \chi(a)) = \rho(a^x)$ and thus $\rho((a, x)) \neq 1$, as wanted. This proves Claim 2.

For the remainder of the proof we fix a linear representation χ of A satisfying the conditions of Claim 2 and put $\zeta_i = \chi(a^{x^i})$ and $\rho = \chi^G$. Then $\rho(a) = \text{diag}(\zeta_0, \zeta_1, \dots, \zeta_{p-1})$ is a non-scalar matrix, i.e. the set $\Lambda = \{\zeta_i : i = 0, 1, \dots, p-1\}$ has at least two different elements. In fact

Claim 3. If $|\Lambda| \neq p$ then Case (3) holds and $|A| \neq q$ and so Λ contains 1 (and another different element).

Furthermore, in Case (1) ζ_i and ζ_{i+1} are not complex conjugate for each $0 \leq i < p$ (where the subindexes are considered as elements in \mathbb{Z}_p , the ring of integers modulo p).

We consider the three cases separately.

In Case (1), $a^x = a^r$ for some integer r coprime with p and such that the multiplicative order of r modulo the order of a is p . Therefore $\zeta_i = \zeta_0^{r^i}$ and $\zeta_0 \mapsto \zeta_0^r$ induces an automorphism σ of $\mathbb{Q}(\zeta_0)$ ($= \mathbb{Q}(\zeta_i)$) of order p . This implies that $|\Lambda| = p$. Moreover, if ζ_i and ζ_{i+1} are complex conjugate then σ has order 2 yielding a contradiction with $p \geq 5$.

In Case (2), $Z(G) = G' = \langle b = a^x a^{-1} \rangle$. Then $\zeta_i = \xi^i \zeta_0$, where $\xi = \chi(b)$ is a primitive p -th root of unity, and again $|\Lambda| = p$.

In Case (3) with $|A| \neq q$, $1 = \chi(a) = \zeta_0 \in \Lambda$, by the construction of χ . If $|A| = q$ then χ is injective and thus the ζ_i 's are pairwise different. Indeed, if $0 \leq i < j \leq p-1$ then x^{j-i} is a generator of X . Then $a^{x^{j-i}} \neq a$, so $\zeta_i = \chi(a^{x^i}) \neq \chi(a^{x^j}) = \zeta_j$. This finishes the proof of Claim 3.

The representations of u and β by ρ are

$$S = \rho(u) = \text{diag}(u_{k,m}(\zeta_0), u_{k,m}(\zeta_1), \dots, u_{k,m}(\zeta_{p-1})) = \text{diag}(u_0, u_1, \dots, u_{p-1})$$

and $\rho(\beta) = 1 + \tau$ with

$$\tau = \begin{pmatrix} \zeta_0 - \zeta_1 & \zeta_0 - \zeta_1 & \dots & \zeta_0 - \zeta_1 \\ \zeta_1 - \zeta_2 & \zeta_1 - \zeta_2 & \dots & \zeta_1 - \zeta_2 \\ \vdots & \vdots & & \vdots \\ \zeta_{p-1} - \zeta_0 & \zeta_{p-1} - \zeta_0 & \dots & \zeta_{p-1} - \zeta_0 \end{pmatrix}.$$

Since not all the ζ_i are equal, τ has rank 1 with image generated by

$$\Psi = \begin{pmatrix} \zeta_0 - \zeta_1 \\ \zeta_1 - \zeta_2 \\ \vdots \\ \zeta_{p-1} - \zeta_0 \end{pmatrix},$$

and kernel

$$K = \ker(\tau) = \left\{ \begin{pmatrix} x_0 \\ \vdots \\ x_{p-1} \end{pmatrix} : x_0 + \dots + x_{p-1} = 0 \right\}.$$

Let r_+ and r_- be the maximum and minimum of $\{|u_i| : i = 0, 1, \dots, p-1\}$ and set $X_+ = \{i : |u_i| = r_+\}$, $X_- = \{i : |u_i| = r_-\}$ and $X_0 = \mathbb{Z}_p \setminus (X_+ \cup X_-)$. Let $\{e_1, \dots, e_n\}$ be the canonical basis of $V = \mathbb{C}^p$, the representation space of ρ . Let V_* be the span $\{e_i : i \in X_*\}$ for $* = +, -$ or 0 . Notice that this notation agrees with that of Theorem 6.1.

Claim 4: $\mathbb{Z}_p \neq X_+$ (equivalently $\mathbb{Z}_p \neq X_-$).

The order d of $\rho(a)$ is a divisor of q and so it is a prime power. Moreover $\Lambda \subseteq L$ where L is the set of d -th roots of unity. By [7, Lemma 3.5(ii)], if $x, y \in L$ then $|u_{k,m}(x)| = |u_{k,m}(y)|$ if and only if x and y are either equal or conjugate. If $\mathbb{Z}_p = X_+$ then Λ has either one element or it has two different conjugate elements. This contradicts Claim 3, and so $\mathbb{Z}_p \neq X_+$. This proves Claim 4.

At this point it is tempting to try to show that S and τ satisfy the conditions of Theorem 6.1. Unfortunately this is not the case in general. For example, in Case (3) some of the ζ_i 's may be equal (for example, this is the case if $q < p$) and this may provide some non-trivial elements in $V_+ \cap K$.

As we mentioned above, we are going to be more specific on the the integer m used in the definition of $u = u_{k,m}(a)$. Namely, we are going to impose that m is a multiple of q , the order of a . Let ξ be a primitive q -th root of unity. If $|u_{k,m}(\xi^a)| = |u_{k,m}(\xi^b)|$ then $b \equiv \pm a \pmod{q}$ ([7, Lemma 3.5]). If moreover $a \not\equiv 0 \pmod{q}$ then $u_{k,m}(\xi^b) = \left(\frac{\xi^{bk}-1}{\xi^b-1}\right)^m = \left(\frac{\xi^{bk}}{\xi^b} \cdot \frac{\xi^{ak}-1}{\xi^a-1}\right)^m = \left(\frac{\xi^{ak}-1}{\xi^a-1}\right)^m = u_{k,m}(\xi^a)$. In particular, $\{\zeta_i : i \in X_+\}$ and $\{\zeta_i : i \in X_-\}$ have cardinality 1. This implies that $W = (V_+ \cap K) \oplus (V_- \cap K)$ is invariant under the action of S and hence the endomorphisms S and τ of V induce endomorphisms \bar{S} and $\bar{\tau}$ of $\bar{V} = V/W$.

We are going to use the standard bar notation for reduction modulo W . Then, as we will see below, $\bar{V} = \bar{V}_+ \oplus \bar{V}_0 \oplus \bar{V}_-$ is a decomposition of \bar{V} with respect to \bar{S} as in Theorem 6.1.

Claim 5: \bar{S} and $\bar{\tau}$ satisfy the hypothesis of Theorem 6.1.

The kernel and image of $\bar{\tau}$ are $K_1 = \overline{\tau^{-1}(W)}$ and $I_1 = \bar{I}$, respectively. 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 $S(e_i) = \zeta_i e_i \notin K$ for each $i \in X_\pm$. This shows that $\bar{V}_\pm \cap K_1 = 0$.

To prove that $I_1 \cap (\bar{V}_0 \oplus \bar{V}_\pm) = 0$ we only have to show that $\bar{\Psi} \notin \bar{V}_0 \oplus \bar{V}_\pm$, and due to symmetry, only that $\bar{\Psi} \notin \bar{V}_0 \oplus \bar{V}_+$. If this is not so, then $\Psi = v + w_+ + w_-$ for some $v \in V_0$, $w_+ \in V_+$ and $w_- \in V_- \cap K$. Thus the projection of Ψ on V_- belongs to K . That is, $\sum_{i \in X_-} (\lambda - \zeta_{i+1}) = \sum_{i \in X_-} (\zeta_i - \zeta_{i+1}) = 0$, where λ is the unique element of the form ζ_i , with $i \in X_-$. Now we delete from the equality above the neighbor zero summands, that is the ones in which $\lambda = \zeta_{i+1}$. Passing the negative expressions to the right side and adding up the equal terms, we obtain $n\lambda = \sum_{i=1}^k m_i \mu_i$, for n the cardinalty of $\{i \in X_- : \zeta_{i+1} \neq \lambda\}$, m_i non-negative integers and μ_1, \dots, μ_i, q -th roots of unity different from λ . Moreover $n > 0$, because $\mathbb{Z}_p \neq X_-$. Let tr denotes the Galois trace of the extension $\mathbb{Q}(\xi)/\mathbb{Q}$ and write $q = p^r$, with p prime. Let ε be a q -th root of unity. Then $\text{tr}(\varepsilon) = p^{r-1}(p-1)$ if $\varepsilon = 1$, $\text{tr}(\varepsilon) = -p^{r-1}$ if ε has order p and $\text{tr}(\varepsilon) = 0$ otherwise. Thus $\text{tr}(\lambda^{-1}\mu_i) \leq 0$ for each i and hence $0 < n(p-1)p^{n-1} = \text{tr}(n) = \sum_{i=1}^k m_i \text{tr}(\lambda^{-1}\mu_i) \leq 0$, which yields a contradiction. This finishes the proof of Claim 5.

By Claim 5, $(\bar{S}^s, (1 + \bar{\tau})^t)$ is the free product of $\langle \bar{S}^s \rangle$ and $\langle (1 + \bar{\tau})^t \rangle$ for s and t sufficiently large. Thus (u^s, β^t) the free product of $\langle u^s \rangle$ and $\langle \beta^t \rangle$. Since u and β have infinite order, (u^s, β^t) is a free pair formed by a Bass cyclic unit and a power of a bicyclic unit of $\mathbb{Z}G$. This finishes the proof of Theorem 1.3.

7 Examples and questions. Bass cyclic and bicyclic units

If $u_{k,m}(a)$ is a Bass cyclic unit of infinite order then $k \not\equiv \pm 1 \pmod{d}$, where d is the order of a and hence d is not a divisor of 4 nor 6. Therefore, if G has a free pair in which one of the elements is a Bass cyclic unit, and the other is a power of a bicyclic unit, then G has a non central element whose order does not divide neither 4 nor 6 (for $\mathbb{Z}G$ to have a non-central Bass cyclic unit of infinite order) and G is not Hamiltonian (for $\mathbb{Z}G$ to have a non-trivial bicyclic unit). This justifies partially the hypothesis in Theorem 1.3 (and in [7, Theorem 4.7]) of G having order coprime to 6 and suggest the following question.

Question 7.1. Let G be a non-Hamiltonian group with an element whose order does not divide neither 4 nor 6. Does $\mathbb{Z}G$ have a free pair formed by a Bass cyclic and a power of a bicyclic unit?

Remark 7.2. Notice that if G is non-abelian and has a central element a of order d with $d \nmid 4$ and $d \nmid 6$, then G has also a non-central element satisfying the same condition. Indeed, assume that every non-central element of G has order dividing either 4 or 6. Let b a non-central element of maximal order n , and so $n = 2, 3, 4$ or 6 . Then $a^i b$ is non-central and therefore the order of $a^i b$ divides 4 or 6 for each i . This implies that $\langle a \rangle \cap \langle b \rangle \neq 1$ and thus $n \neq 2, 3$. Furthermore $d = 2^k 3^l$ for some $k, l \geq 0$. If $n = 6$ then the orders of $a^{3^l} b$ and $a^{2^k} b$ are multiple of $2^k \cdot 3$ and $2 \cdot 3^l$, respectively, and this yields a contradiction because either $k \geq 2$ or $l \geq 2$. This shows that the order of b is 4 and the order of ab is at most 4. Then $b^3 \notin \langle a \rangle$ and so the order of ab divides 4. Thus the order of a divides 4, contradicting the hypothesis.

Notice that if either A_n or S_n satisfies the hypothesis of Question 7.1 then $n \geq 5$. Thus to give an affirmative answer to Question 7.1 for symmetric and alternating groups, it is enough to show that $\mathbb{Z}A_5$ has a free pair formed by a power of a bicyclic unit, and a Bass cyclic unit.

The group A_5 can be defined by generators and relations as

$$A_5 = \langle a, b \mid a^2 = b^3 = (ba)^5 = 1 \rangle$$

and one can take $a = (1, 2)(3, 4)$ and $b = (1, 3, 5)$, so that $c = ba = (1, 2, 3, 4, 5)$. Take the irreducible representation ϕ of A_5 given by

$$A = \phi(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \phi(b) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $\xi = e^{\frac{2\pi i}{5}}$, a primitive 5-th root of unity, and set $F = \mathbb{Q}(\xi)$. Let $\sigma \in \text{Gal}(F/\mathbb{Q})$ be given by $(\sigma(\xi) = \xi^2)$. Notice that σ generates $\text{Gal}(F/\mathbb{Q})$ and one has

$$C = \phi(c) = BA = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Consider $\text{Gal}(F/\mathbb{Q})$ acting componentwise on F^4 . Let $v_0 = (\xi^2, \xi, \xi^4, \xi^3)$ and $v_i = \sigma^i(v_0)$. Then $Cv_0 = \xi v_0$, that is v_0 is an eigenvector of C with eigenvalue ξ . Therefore v_i is also an eigenvector of C with eigenvalue $\sigma^i(\xi) = \xi^{2^i}$. This implies that v_i is an eigenvector of the Bass cyclic unit $S = u_{2,4}(C) = \phi(u_{2,4}(c))$ with eigenvalue $\lambda_i = \sigma^i(u_{2,4}(\xi)) = 1 + \xi^{2^i}$. Now $|\lambda_1| = |\lambda_3| > |\lambda_2| = |\lambda_4|$ and so $F^4 = V_+ \oplus V_-$, where $V_+ = \langle v_1, v_3 \rangle$ and $V_- = \langle v_2, v_4 \rangle$.

Let now

$$\tau = \phi((1-a)b(1+a)) = \begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -2 & -2 & -3 & -3 \\ 2 & 2 & 3 & 3 \end{pmatrix}.$$

Then $K = \ker(\tau) = \text{Im}(\tau) = \{(x_1, x_2, x_3, x_4) : x_1 + x_2 = x_3 + x_4 = 0\}$. Let $\delta_1, \delta_2 \in F$ be such that $\delta_1 v_1 + \delta_2 v_3 = (\delta_1 \xi^2 + \delta_2 \xi^3, \delta_1 \xi + \delta_2 \xi^4, \delta_1 \xi^4 + \delta_2 \xi, \delta_1 \xi^3 + \delta_2 \xi^2) \in K$. Then $\delta_1(\xi^2 + \xi) + \delta_2(\xi^3 + \xi^4) = \delta_1(\xi^4 + \xi^3) + \delta_2(\xi + \xi^2) = 0$ and so $\delta_1 = \delta_2 = 0$, because $(\xi^4 + \xi^3) - (\xi^2 + \xi) = -2\xi^2 - 2\xi - 1 \neq 0$.

This shows that $K \cap X_+ = 0$. Since σ leaves K invariant and interchanges V_+ and V_- one obtains that $K \cap X_- = 0$. Therefore S and τ (considered as endomorphisms of complex vector spaces) satisfy the hypotheses of Theorem 6.1. Thus $(S^n = \phi(u_{2,4}(c)^n), \phi(\beta_{a,b})^m = (1 + \tau))^m$ is a free pair for some n and m , and we conclude that $(u_{2,4}(c)^n = u_{2,4n}(c), (\beta_{a,b})^m)$ is a free pair of $\mathbb{Z}A_5$, formed by a Bass cyclic unit and a power of a bicyclic unit. So we have shown.

Theorem 7.3. $\mathbb{Z}A_n$ (resp. $\mathbb{Z}S_n$) contains a free pair formed by a power of a bicyclic unit and a Bass cyclic unit, if and only if $n \geq 5$.

Acknowledgements. In this paper we have used many ideas which Donald Passman generously shared with us. We would like to thank him and also thank the referee for pointing out an error in a previous version of the proof of Theorem 1.3.

References

- [1] J. Bamberg, *Non-free points for groups generated by a pair of 2×2 matrices*, J. London Math. Soc. (2) 62 (2000) 795–801.
- [2] H. Bass, *The Dirichlet unit theorem, induced characters and Whitehead groups of finite groups*, Topology 4 (1966) 391–410.
- [3] A. Dooms, E. Jespers and M. Ruiz, *Free groups and subgroups of finite index in the unit group of an integral group ring*, preprint.
- [4] R. Ferraz, *Free subgroups in the units of $\mathbb{Z}[K_8 \times C_p]$* , Comm. Algebra 31 (2003), no. 9, 4291–4299.
- [5] J.Z. Gonçalves and A. Mandel, *Free subgroups in the group of units of a twisted group algebra*, Comm. Algebra 29(5) (2001) 2231–2238.
- [6] J.Z. Gonçalves and D.S. Passman, *Free subgroups of units in algebras of characteristic 0*, unpublished.
- [7] J.Z. Gonçalves and D.S. Passman, *Linear groups and group rings*, J. Algebra 295 (2006), 94–118. (Erratum, J. Algebra 307 (2007), 930–931)
- [8] 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.
- [9] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math. 78 (1993), no. 3, 303–315.
- [10] 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.
- [11] V. Jiménez, *A trigonometric inequality and its application to the theory of integral group rings*, Comm. Algebra, to appear.
- [12] Z.S. Marciniak and S.K. Sehgal, *Constructing free subgroups of integral group rings*, Proc. AMS 125 (1997) 1005–1009.
- [13] G. Miller and H. Moreno, *Non-abelian groups in which every subgroup is abelian*, Trans. AMS 4 (1903) 398–404.

- [14] D.S. Passman, *The algebraic structure of group rings*, Interscience, New York, 1977.
- [15] 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.
- [16] A. Salwa, *On free subgroups of units of rings*, *Proc. AMS* 127 (1999) 2569-2572.
- [17] I.N. Sanov, *The property of certain representatoin of free groups*, *Dokl. AN SSSR* 57 (1947) 657-659.
- [18] S.K. Sehgal, *Units in integral group rings*, Longman Scientific & Technical, Pitman Monographs, *Surveys in Pure and Applied Mathematics* 69, 1993.