Proceedings of the Edinburgh Mathematical Society (2011) **54**, 695–709
DOI:10.1017/S0013091510000428

ALTERNATING UNITS AS FREE FACTORS IN THE GROUP OF UNITS OF INTEGRAL GROUP RINGS

JAIRO Z. GONÇALVES[1] AND PAULA M. VELOSO[1]

[1] *Departamento de Matemática, Universidade de São Paulo, Rua do Matão 1010, Butantã 05508-090, São Paulo (SP), Brazil* (jz.goncalves@usp.br)

[2] *Departamento de Matemática, Universidade Federal de Minas Gerais, Av. Antônio Carlos 6627, PO Box 702, 30161-970 Belo Horizonte (MG), Brazil* (pmv@mat.ufmg.br)

(Received 15 March 2010)

Abstract Let G be a group of odd order that contains a non-central element x whose order is either a prime $p \geqslant 5$ or 3^l, with $l \geqslant 2$. Then, in $\mathcal{U}(\mathbb{Z}G)$, the group of units of $\mathbb{Z}G$, we can find an alternating unit u based on x, and another unit v, which can be either a bicyclic or an alternating unit, such that for all sufficiently large integers m we have that $\langle u^m, v^m\rangle = \langle u^m\rangle * \langle v^m\rangle \cong \mathbb{Z} * \mathbb{Z}$.

Keywords: integral group rings; free groups; units

2010 *Mathematics subject classification:* Primary 20C05
Secondary 20E05

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 $\mathcal{U}(\mathbb{Z}G)$ be its group of units. It is well known [**10**] that unless G is either an abelian or a Hamiltonian 2-group, $\mathcal{U}(\mathbb{Z}G)$ always contains free (non-cyclic) subgroups. The shortcoming of this proof is that it is existential, and does not explicitly present the units of $\mathbb{Z}G$ that generate the free subgroup. More recently, this gap was filled by using bicyclic units [**12**] and by using Bass cyclic units [**2**]. Other instances of construction of free subgroups of $\mathcal{U}(\mathbb{Z}G)$, using either Bass cyclic units or bicyclic units, can be seen in [**1**, **3**, **5**, **6**, **8**, **11**].

Following this trend, we ask if it is possible to find free products in $\mathcal{U}(\mathbb{Z}G)$, where one of the factors is an *alternating unit*.

This is the question that we will pursue in this paper, but let us start by recalling the relevant definitions.

Let $C = \langle x \mid x^n = 1\rangle$ be a cyclic group of order $n > 1$, let $\mathbb{Z}C$ be its integral group ring and let ε be a complex primitive root of unity of order n. The isomorphism $\mathbb{Q}C \simeq \bigoplus_{d\mid n} \mathbb{Q}(\varepsilon^d)$, when restricted to $\mathbb{Z}C$, gives the embedding $\mathbb{Z}C \hookrightarrow \bigoplus_{d\mid n} \mathbb{Z}[\varepsilon^d]$, of

$\mathbb{Z}C$ into the maximal order $\bigoplus_{d|n}\mathbb{Z}[\varepsilon^d]$ of $\mathbb{Q}C$. So, an element u of $\mathbb{Z}C$ is a unit if each component of its image is a unit in $\mathbb{Z}[\varepsilon^d]$.

In $\mathbb{Z}[\varepsilon^d]$ the most common way to produce a unit is the following. If $i \in \mathbb{N}$, $1 < i < n$, $(i, n) = 1$, then

$$\frac{(\varepsilon^i - 1)}{(\varepsilon - 1)} = 1 + \varepsilon + \cdots + \varepsilon^{i-1}$$

is a *cyclotomic unit* in $\mathbb{Z}[\varepsilon]$ with inverse

$$\frac{(\varepsilon - 1)}{(\varepsilon^i - 1)} = \frac{(\varepsilon^{ik} - 1)}{(\varepsilon^i - 1)} = 1 + \varepsilon^i + \cdots + \varepsilon^{i(k-1)},$$

where $ik \equiv 1 \pmod{n}$.

But, if we try to mimic the definition above in $\mathbb{Z}G$, by setting $v = 1+x+\cdots+x^{i-1} \in \mathbb{Z}C$, with $i \in \mathbb{N}$, $1 < i < n$, $(i, n) = 1$, we do not obtain a unit, since the augmentation of v is $i > 1$. So, we need to make a small change in v in order to produce an *alternating unit*.

Let $c > 0$ be an odd integer. Define the polynomial $f_c(Y) \in \mathbb{Z}[Y]$ as

$$f_c(Y) := \frac{Y^c + 1}{Y + 1} = 1 - Y + Y^2 - \cdots + (-1)^{c-1}Y^{c-1} = \sum_{i=0}^{c-1}(-Y)^i.$$

Now, in the finite group G, let $x \in G$ be an element of odd order n, and let $c \in \mathbb{N}$, $1 \leqslant c \leqslant n$ be such that $(c, n) = 1$. If c is odd, then, according to [**13**, Lemma 10.6], the element

$$u_c(x) := f_c(x)$$

is a unit in $\mathbb{Z}G$. If c is even, then, replacing c by $n + c$ (which is an odd number), we still have a unit $u_c(x)$ as before:

$$u_c(x) := f_{n+c}(x).$$

We call this unit the *alternating unit based on the element x and depending on the parameter c*. Notice that, if $n = |\langle x\rangle| < 5$, then the only existing alternating units are trivial units.

Now let g be an element of G of order $n > 1$, and suppose that $h \notin N_G(\langle g\rangle)$, the normalizer of $\langle g\rangle$ in G. Set $\hat{g} = \sum_{i=0}^{n-1} g^i \in \mathbb{Z}G$. Then $\tau = (1 - g)h\hat{g} \in \mathbb{Z}G$ has square 0, but $\tau \neq 0$. The element $v = 1 + \tau$ is called a *bicyclic unit*.

Our main goal is to prove the following.

Theorem 1.1. *Let G be a group of odd order. Suppose that there exists a non-central element $x \in G$ such that the order of x is either a prime $p \geqslant 5$ or of the form 3^l, with $l \geqslant 2$. Then there exist an alternating unit u, based on the element x and dependent on the parameter c, and a unit v, being either a bicyclic unit or an alternating unit, such that for all sufficiently large integers m we have that $\langle u^m, v^m\rangle = \langle u^m\rangle * \langle v^m\rangle \cong \mathbb{Z} * \mathbb{Z}$.*

https://doi.org/10.1017/S0013091510000428 Published online by Cambridge University Press

2. Some lemmas

This section is quite technical, and provides the tools that will be used in § 3.

Our strategy is to prove Theorem 1.1 by induction on $|G|$. The key groups to be considered are groups of minimal order subject to the conditions of the theorem, and they are classified in the lemma below.

We say that G is a *p-critical group* if G has a non-central element of order p and, for all proper subgroups H of G, the elements of H of order p are central in H [**5**].

We start with the following lemma.

Lemma 2.1. *Let G be a finite group of odd order, possessing an element $a \in G \setminus \mathcal{Z}(G)$ such that the order of a is either a prime number $p \geqslant 5$ or $3^r \geqslant 9$, and that, for every proper subgroup or proper homomorphic image H of G, the elements of H of order $p \geqslant 5$ or $3^r \geqslant 9$ are central in H. Then one of the following statements holds.*

(1) *G is the semidirect product $G = B \rtimes A$ of the abelian group B by the cyclic group $A = \langle a\rangle$ of order $p \geqslant 5$. Furthermore, either $B = \langle b\rangle$ is cyclic of order $p^{n+1} \geqslant p^2$ with $b^a = b^{1+p^n}$, or $B = \langle b\rangle \times \langle z\rangle$, with z central of order p and $b^a = bz$.*

(2) *G is the semidirect product $G = P \rtimes Q$ of the elementary abelian p-group P, with $p \geqslant 5$, by the cyclic group Q of prime order $q \neq p$, and Q acts irreducibly on P as a group of order q.*

(3) *G is the semidirect product $G = Q \rtimes P$ of the q-group Q, q a prime, by the cyclic group P of order $p \neq q$, $p \geqslant 5$; P acts faithfully and irreducibly on the Frattini quotient $Q/\Phi(Q)$ and P centralizes $\Phi(Q)$.*

(4) *G is one of the following 3-groups:*

 (i) $G = \langle a, b \mid a^{3^r} = b^3 = 1,\ b^{-1}ab = a^{1+3^{r-1}}\rangle$, $r \geqslant 2$;

 (ii) $G = \langle a, b \mid a^{3^r} = b^{3^s} = c^3 = 1,\ c = (a,b), (a,c) = (b,c) = 1\rangle$.

Proof. Among all groups G satisfying the hypotheses of the lemma, take one with minimal order, with $a \in G$ being the non-central element. There exists $b \in G$ such that $(a,b) = a^{-1}b^{-1}ab \neq 1$. By hypothesis, $\langle a, b\rangle$ cannot be a proper subgroup of G, so $G = \langle a, b\rangle$. We have the following possibilities.

(a) $|\langle a\rangle| = p \geqslant 5$, p a prime number: in this case, G is a p-critical group and, thus, according to [**5**, Proposition 2.3], G is either (1), (2) or (3).

(b) $|\langle a\rangle| = 3^r \geqslant 9$: if $|\langle b\rangle| = p$ is a prime number not equal to 3, then G is again p-critical (G is either (1), (2) or (3)).

So, we can assume that $|\langle b\rangle| = 3^s$. If G is not a 3-group, then take $w \in G$ such that $|\langle w\rangle| = p$ is a prime number not equal to 3. If $w \notin \mathcal{Z}(G)$, then we are again in the p-critical case, and G is either of type (1), (2) or (3).

Therefore, we can assume that $W = \langle w\rangle$ is central.

We claim that G/W is abelian.

Otherwise, denoting by $^{-}: G \to G/W$ the canonical epimorphism, we have, by hypothesis, that $|\langle \bar{a} \rangle| = |\langle \bar{b} \rangle| = 3$, and $a^3 \in W$. Since the order of w is p, the possibilities for the order of a are either 3 or $3p$, which go against the hypothesis that the order of a is $3^r \geqslant 9$.

So G/W is abelian, and $(a,b) = w$. Therefore, $|\langle a \rangle|$ is the least common multiple between the orders of b^{-1} and w, which is $3^s p$: a contradiction again.

The conclusion is that if G is not p-critical for $p \geqslant 5$, then G is a 3-group. So, from now on we assume that G is a 3-group.

It may be the case that G contains a cyclic subgroup of index 3. Then by [**9**, Theorem 12.5.1], G is of type (a).

Thus, we can assume that G has no maximal cyclic subgroup.

Let $a \in G$ be a non-central element of order $3^r \geqslant 9$ and let $b \in G$ be an element of order 3^s such that $(a,b) \neq 1$. Then $G = \langle a, b \rangle$, and $\langle a \rangle$ is contained in a maximal subgroup H of G, such that $H \lhd G$ and $[G : H] = 3$. This implies that H contains all conjugates of a, and in particular $C = \langle a^g \mid g \in G \rangle$ is a normal abelian subgroup of G, and since $G = \langle a, b \rangle$, it follows that $G = \langle C, b \rangle$. Since G is non-abelian, b cannot centralize C, but $b \in N_G(C)$.

Set $c := (a,b) = a^{-1}a^b$. Then $c \in C$, and c is a commutator of G of order $3^l \leqslant 3^r$.

We have two possibilities.

(I) $\langle a^{-1} \rangle \cap \langle a^b \rangle = \{1\}$: in this case the order of c is equal the order of a, which is $3^r \geqslant 9$.

We claim that c is central in G.

Indeed, let $g \in G$ and let L be a maximal subgroup of G containing g. Then $L \lhd G$ and, since G/L is cyclic of order 3, it follows that $c \in G' \subseteq L$. Notice that, by hypothesis, c is central in L; thus, we conclude that $cg = gc$, and $\langle c \rangle = Z$ is central in G.

Let $^{-} : G \to G/C$ denote the canonical epimorphism, and let 3^m be the order of $\bar{b}$. If $m > 1$, set $\tilde{b} := b^{3^{m-1}}$. Then, since c is central, we have $\tilde{c} := c^{3^{m-1}} = (a, \tilde{b}) = (a, b^{3^{m-1}}) \neq 1$, and $\tilde{c}^3 = 1$. So, if we substitute b by $\tilde{b}$, we have the new relations $a^{3^r} = \tilde{b}^{3^{s'}} = 1$, $(a, \tilde{b}) = \tilde{c}$, $\tilde{c}^3 = 1$, as in (i).

(II) $\langle a^{-1} \rangle \cap \langle a^b \rangle \neq \{1\}$: the inequality of the intersection above means that b normalizes $\langle a \rangle$. So, substituting, if necessary, b by one of its powers, we can assume that b normalizes $\langle a \rangle$ and b^3 centralizes a. Therefore, $a^b = a^{1+3^{r-1}}$, $c = a^{-1}a^{1+3^{r-1}}$ and $c^3 = 1$. But we cannot guarantee that $b^3 = 1$. If this is not so, certainly $b^3 = a^{3s}$, and the element we are looking for is $b' = a^{-s}b$. This is case (b).

□

We must prove Theorem 1.1 for each group type in Lemma 2.1 and the technique we use is as follows. Consider a suitable representation of $\mathbb{C}G$ and regard the units in $\mathcal{U}(\mathbb{C}G)$ as non-singular linear operators in a complex vector space. We obtain free groups for the powers of the operators involved after the following setting is established.

Let F be a locally compact field with a real absolute value $|\cdot|$ and let V be a finite-dimensional F-vector space. If T is a non-singular, diagonalizable operator on V, we say that $V = X_+ \oplus X_0 \oplus X_-$ is a *T-decomposition* of V if there exist real numbers $r > s > 0$ with $X_+ \neq 0$ (the subspace spanned by the eigenvectors of T corresponding to the eigenvalues of absolute value greater than or equal to r), $X_- \neq 0$ (the subspace spanned by the eigenvectors of T corresponding to the eigenvalues of absolute value less than or equal to s) and with X_0 the span of the remaining eigenvectors. We use $1\mathbb{Z}$ to denote the set of integral multiples of 1 in F. So, if $\operatorname{Char} F = p > 0$, then $|1\mathbb{Z} \setminus 0| = 1$; and if $\operatorname{Char} F = 0$, then $1\mathbb{Z} = \mathbb{Z}$. The hypothesis $|1\mathbb{Z} \setminus 0| \geqslant 1$ in the theorem below excludes the case of p-adic fields.

Now, we can state the following result.

Theorem 2.2 (Gonçalves and Passman [6, Theorem 2.7]). *Let V be a finite-dimensional F-vector space and let $S, T\colon V \to V$ be two non-singular operators. Suppose S is diagonalizable with an S-decomposition given by $V = X_+ \oplus X_0 \oplus X_-$. Furthermore, suppose $T = 1 + a\tau$ is a generalized transvection, where $a \in F$, $\tau\colon V \to V$ is a non-zero operator of square zero with $\mathcal{I} = \tau(V) = \operatorname{Im}\tau$ and $\mathcal{K} = \ker\tau$. Assume also that $|1\mathbb{Z} \setminus 0| \geqslant 1$. If the four intersections $X_\pm \cap \mathcal{K}$ and $\mathcal{I} \cap (X_\pm \oplus X_0)$ are trivial, then, for all sufficiently large integers n and all $a \in F$ of sufficiently large absolute value, we have $\langle S^n, T\rangle = \langle S^n\rangle * \langle T\rangle$.*

Theorem 2.3 (Gonçalves and Passman [6, Corollary 4.1]). *Let V be a finite-dimensional F-vector space and let $S, T\colon V \to V$ be two non-singular operators on V. Suppose that S and T are both diagonalizable with $V = X_+ \oplus X_0 \oplus X_-$ and $V = Y_+ \oplus Y_0 \oplus Y_-$ being S- and T-decompositions of V, respectively. Assume that $\dim X_+ = \dim X_- = r = \dim Y_+ = \dim Y_+$ and consider the four projections $\sigma_+\colon V \to X_+$, $\sigma_-\colon V \to X_-$, $\tau_+\colon V \to Y_+$ and $\tau_-\colon V \to Y_-$. If the idempotent conditions $\operatorname{rank}\sigma_i\tau_j = r = \tau_j\sigma_i$ hold for all $i, j \in \{+,-\}$, then $\langle S^m, T^m\rangle = \langle S^m\rangle * \langle T^m\rangle$, for all sufficiently large positive integers m.*

Looking into the conditions of Theorems 2.2 and 2.3, we see that we must know precisely what the absolute values of the eigenvalues of an alternating unit are. This is our next task.

Lemma 2.4. *Let n be an odd integer, $n \geqslant 5$, and let $\varepsilon = \exp(2\pi\mathrm{i}/n)$ be a primitive complex nth root of unity. Let c be an integer $1 < c < n$ coprime to n and let a be any integer. If $u_c(x)$ is the alternating unit based on x with parameter c, then*

(i) $|u_c(\varepsilon^a)| = \left|\dfrac{\cos(\pi ca/n)}{\cos(\pi a/n)}\right| = \left|\dfrac{\varepsilon^{ac/2} + \varepsilon^{-ac/2}}{\varepsilon^{a/2} + \varepsilon^{-a/2}}\right|,$

(ii) *the largest absolute value of $|u_c(\varepsilon^a)|$ occurs when $2a \equiv \pm 1 \pmod{n}$.*

(iii) *the smallest absolute value of $|u_c(\varepsilon^a)|$ occurs when $2a \equiv \pm c^{-1} \pmod{n}$.*

Proof. (i), (ii) Our goal is to find the integer a that maximizes $|u_c(\varepsilon^a)|$; clearly, we may assume that $0 \leqslant a < n$. Since $|\varepsilon^a| = 1$, it is easy to see that

$$|u_c(\varepsilon^a)| = \left|\frac{\varepsilon^{ca}+1}{\varepsilon^a+1}\right| = \left|\frac{\varepsilon^{ac/2}+\varepsilon^{-ac/2}}{\varepsilon^{a/2}+\varepsilon^{-a/2}}\right| = \left|\frac{\cos(\pi ca/n)}{\cos(\pi a/n)}\right|.$$

From the above expression, we see that we may replace c by $n+c$ if necessary, and thus assume that c is odd. Furthermore, we may replace a by $n-a$ if necessary, and thus assume that $\frac{1}{2}(n+1) \leqslant a < n$.

Set $z := a/n$. Since c is odd, we have that

$$|u_c(\varepsilon^a)| = \left|\frac{\cos(\pi cz)}{\cos(\pi z)}\right| = \left|\frac{\sin(\pi c(z-\frac{1}{2}))}{\sin(\pi(z-\frac{1}{2}))}\right| = \left|\frac{\sin(\pi cx)}{\sin(\pi x)}\right|,$$

where $x := z - \frac{1}{2}$.

Now, $(n+1)/2 \leqslant a < n$; so $1/2 + 1/2n \leqslant z < 1$ and $r := 1/2n \leqslant x < 1/2$. Since $1 < c < n$, we have that $0 < r < 1/2c$, and [**6**, Lemma 3.3] implies that the largest value of $|u_c(\varepsilon^a)|$ occurs when $x = r = 1/2n$ or, equivalently, when $a = (n+1)/2$. Another possibility for a is obtained by replacing a by $n - a = (n-1)/2$.

(iii) $|u_c(\varepsilon^a)|$ has a minimum, as a function of a, precisely when $|u_c(\varepsilon^a)^{-1}|$ has a maximum.

If $bc \equiv 1 \pmod n$ and $x^n = 1$, then

$$u_c(x)^{-1} = \frac{x+1}{x^c+1} = \frac{y^b+1}{y+1} = u_b(y) = u_b(x^c),$$

where $y = x^c$.

Now set $x := \varepsilon^a$. Then $u_c(\varepsilon^a)^{-1} = u_b(\varepsilon^{ac})$, which has a maximum when $2ac \equiv \pm 1 \pmod n$. So, the solution for the minimum problem is $2a \equiv \pm c^{-1} \equiv b \pmod n$, as claimed. □

Lemma 2.5. *Let $p \geqslant 5$ be a prime. Consider $n := p^d$ and $\varepsilon = \exp(2\pi \mathrm{i}/n)$ a primitive complex nth root of unity. Assume c is a positive integer with $c \not\equiv 0, \pm 1 \pmod n$. Then we have that*

(i) $|u_c(\varepsilon^a)| = |u_c(\varepsilon^b)|$ *if and only if* $a \equiv \pm b \pmod n$,

(ii) $u_c(\varepsilon^a) = u_c(\varepsilon^b)$ *if and only if* $a \equiv b \pmod n$.

Proof. (i) Since p is odd, each primitive root of unity of order n is a square. So we may replace a and b by $2a$ and $2b$, respectively.

From the hypothesis, we have that

$$|u_c(\varepsilon^{2a})| = \left|\frac{\varepsilon^{ca}+\varepsilon^{-ca}}{\varepsilon^a+\varepsilon^{-a}}\right| = \left|\frac{\varepsilon^{cb}+\varepsilon^{-cb}}{\varepsilon^b+\varepsilon^{-b}}\right| = |u_c(\varepsilon^{2b})|.$$

Since

$$u_c(\varepsilon^{2a}) = \frac{\cos(\pi c 2a/n)}{\cos(\pi 2a/n)}$$

is a real number, we have that

$$\frac{\varepsilon^{ca}+\varepsilon^{-ca}}{\varepsilon^{a}+\varepsilon^{-a}}=\kappa\frac{\varepsilon^{cb}+\varepsilon^{-cb}}{\varepsilon^{b}+\varepsilon^{-b}},\quad \text{where } \kappa=\pm 1.$$

We have two cases.

Case 1 ($\kappa = 1$).

$$\varepsilon^{ca+b}+\varepsilon^{-ca-b}+\varepsilon^{ca-b}+\varepsilon^{-ca+b}=\varepsilon^{cb+a}+\varepsilon^{-cb-a}+\varepsilon^{cb-a}+\varepsilon^{-cb+a}$$

From [**6**, Lemma 3.5 (i)], we have that

- $ca+b\equiv\pm(cb+a)$ or
- $ca+b\equiv\pm(cb-a)$.

In the first case, then, either $(c-1)a\equiv(c-1)b$ (and $a\equiv b$), or $(c+1)a\equiv(c+1)(-b)$ (and then $a\equiv -b$).

In the latter case, we also have that $ca-b\equiv\pm(cb+a) \pmod n$. So,

$$\begin{aligned} ca+b&\equiv\pm(cb-a) \pmod n,\\ ca-b&\equiv\pm(cb+a) \pmod n. \end{aligned}$$

If the two $\pm$ signs in the equations above disagree, then, adding them, we have $2ca\equiv 2a$, which is absurd. Therefore, the $\pm$ signs must agree, and we have $2ca\equiv 2cb$, which implies $a\equiv b \pmod n$.

Case 2 ($\kappa = -1$).

$$\varepsilon^{ca+b}+\varepsilon^{-ca-b}+\varepsilon^{ca-b}+\varepsilon^{-ca+b}+\varepsilon^{cb+a}+\varepsilon^{-cb-a}+\varepsilon^{cb-a}+\varepsilon^{-cb+a}=0. \tag{2.1}$$

Let $\Phi_p(X)$ denote the pth cyclotomic polynomial over $\mathbb{Q}$.

Notice that, if $p\geqslant 11$, then the degree of $\Phi_p(X)$ is $p-1$, which is greater than 9; so the equation above is not possible.

Now we may suppose $p<11$. Let $f(X)$ denote the polynomial in $\mathbb{Q}[X]$ obtained by replacing ε by X in (2.1). Then $\Phi(X)$ should divide $f(X)$ and the left-hand side of (2.1) would have n terms, where n is a multiple of 5 (if $p=5$) or 7 (if $p=7$): a contradiction.

(ii) If $u_c(\varepsilon^a)=u_c(\varepsilon^b)$, then, in particular, we have that $|u_c(\varepsilon^a)|=|u_c(\varepsilon^b)|$, which, by part (i), implies that $a\equiv\pm b \pmod n$.

As in (i), we replace a and b by $2a$ and $2b$, respectively. Then we have, from the definition of an alternating unit and the hypothesis, that

$$\begin{aligned} u_c(\varepsilon^{2a})&=\frac{\varepsilon^{2ca}+1}{\varepsilon^{2a}+1}\\ &=\frac{\varepsilon^{ca}(\varepsilon^{ca}+\varepsilon^{-ca})}{\varepsilon^{a}(\varepsilon^{a}+\varepsilon^{-a})} \end{aligned}$$

https://doi.org/10.1017/S0013091510000428 Published online by Cambridge University Press

$$\begin{aligned} &= \varepsilon^{(c-1)a}\left(\frac{\varepsilon^{ca}+\varepsilon^{-ca}}{\varepsilon^{a}+\varepsilon^{-a}}\right) \\ &= \varepsilon^{(c-1)b}\left(\frac{\varepsilon^{cb}+\varepsilon^{-cb}}{\varepsilon^{b}+\varepsilon^{-b}}\right) \\ &= u_c(\varepsilon^{2b}). \end{aligned}$$

Suppose that $a \equiv -b \pmod n$, with $a \not\equiv 0 \pmod n$. Thus, $\varepsilon^{a(c-1)} = \varepsilon^{b(c-1)}$, i.e. $\varepsilon^{(a-b)(c-1)} = 1$, or $\varepsilon^{2a(c-1)} = 1$, which implies that $n|a$: a contradiction. □

Lemma 2.6. *Let $d \geqslant 2$ be an integer. Consider $n := 3^d$, $\varepsilon = \exp(2\pi \mathrm{i}/n)$ a primitive complex nth root of unity, and $t := 1+3^{d-1}$. Assume c is a positive integer with $(c,3)=1$. If the equality*

$$\varepsilon^{c+t}+\varepsilon^{c-t}+\varepsilon^{-c+t}+\varepsilon^{-c-t}=\varepsilon^{ct+1}+\varepsilon^{-ct+1}+\varepsilon^{ct-1}+\varepsilon^{-ct-1}$$

holds, then each term on the left-hand side equals exactly one term on the right-hand side.

Proof. Denote by tr the Galois trace in the field extension $\mathbb{Q}(\varepsilon)|\mathbb{Q}$ divided by 3^{d-1}. We have that $\operatorname{tr} 1 = 2$, $\operatorname{tr}\varepsilon^{3^{d-1}} = -1$ and $\operatorname{tr}\varepsilon^{3^i} = 0$ for $0 \leqslant i \leqslant d-2$.

We show first that there is a term on the right-hand side that is equal to ε^{c+t}. We multiply both sides of the equality by ε^{-c-t}, obtaining

$$1+\varepsilon^{-2t}+\varepsilon^{-2c}+\varepsilon^{-2(c-t)}=\varepsilon^{ct+1-c-t}+\varepsilon^{-ct+1-c-t}+\varepsilon^{ct-1-c-t}+\varepsilon^{-ct-1-c-t}.$$

We may assume, without loss of generality, that c is odd (by replacing c by $c+n$ if necessary). Computing the trace on both sides of the equality we obtain $\operatorname{tr} 1 = 2$, $\operatorname{tr}\varepsilon^{-2t} = \operatorname{tr}\varepsilon^{-2c} = 0$ for $(2c,3)=(2t,3)=1$. Notice that $\operatorname{tr}\varepsilon^{-2(c-t)} = -1$ in the worst situation. In any situation, the trace is positive on the left-hand side of the equation; thus, there must exist some ε^i on the right-hand side of the equation with $\operatorname{tr}\varepsilon^i > 0$, which implies $\operatorname{tr}\varepsilon^i = 1$.

We cancel out the equal terms on both sides of the equation and repeat the process, getting the result. □

Lemma 2.7. *Let $d \geqslant 2$ be an integer. Consider $n := 3^d$, $\varepsilon = \exp(2\pi \mathrm{i}/n)$ a primitive complex nth root of unity, and $t := 1+3^{d-1}$. Assume c is a positive integer with $(c,3)=1$. The equality*

$$\varepsilon^{c+t}+\varepsilon^{c-t}+\varepsilon^{-c+t}+\varepsilon^{-c-t}+\varepsilon^{ct+1}+\varepsilon^{-ct+1}+\varepsilon^{ct-1}+\varepsilon^{-ct-1}=0$$

is impossible.

Proof. The cyclotomic polynomial of ε over $\mathbb{Q}$ is $\Phi_{3^d} = X^{2\cdot 3^{d-1}} + X^{3^{d-1}} + 1$. Set

$$f(X) = X^{3^b}(X^{c+t}+X^{c-t}+X^{-c+t}+X^{-c-t}+X^{ct+1}+X^{-ct+1}+X^{ct-1}+X^{-ct-1}),$$

with b chosen so that $f(X) \in \mathbb{Z}[X]$.

Since $f(\varepsilon)=0$, it follows that $f(X) = \Phi_{3^d}(X)g(X)$, for some $g(X) \in \mathbb{Z}[X]$. But then we would have $f(1) = \Phi_{3^d}(1)g(1)$, i.e. $8 = 3\cdot k$, with $k \in \mathbb{Z}$: a contradiction. □

Lemma 2.8. *Let $d \geqslant 2$ be an integer. Consider $n := 3^d$, $\varepsilon = \exp(2\pi \mathrm{i}/n)$ a primitive complex nth root of unity, and $t := 1 + 3^{d-1}$. Assume c is a positive integer with $c \not\equiv 0 \pmod{n}$. Then $|u_c(\varepsilon)|$, $|u_c(\varepsilon^t)|$ and $|u_c(\varepsilon^{t^2})|$ are all distinct.*

Proof. Since n is odd, each primitive root of unity of order n is a square. So, we may replace a and b by $2a$ and $2b$, respectively.

Suppose, by contradiction, that $|u_c(\varepsilon)| = |u_c(\varepsilon^t)|$. Notice that this implies that $|u_c(\varepsilon^t)| = |u_c(\varepsilon^{t^2})|$ and that $|u_c(\varepsilon^{t^2})| = |u_c(\varepsilon)|$. Then we would have

$$|u_c(\varepsilon)| = \left|\frac{\varepsilon^c + \varepsilon^{-c}}{\varepsilon + \varepsilon^{-1}}\right| = \left|\frac{\varepsilon^{ct} + \varepsilon^{-ct}}{\varepsilon^t + \varepsilon^{-t}}\right| = |u_c(\varepsilon^t)|.$$

Since

$$u_c(\varepsilon^{2a}) = \frac{\cos(\pi c 2a/n)}{\cos(\pi 2a/n)}$$

is a real number, we have that

$$\frac{\varepsilon^c + \varepsilon^{-c}}{\varepsilon + \varepsilon^{-1}} = \kappa \frac{\varepsilon^{ct} + \varepsilon^{-ct}}{\varepsilon^t + \varepsilon^{-t}}, \quad \text{where } \kappa = \pm 1.$$

We have two cases.

Case 1 ($\boldsymbol{\kappa = -1}$).

$$\varepsilon^{c+t} + \varepsilon^{-c-t} + \varepsilon^{c-t} + \varepsilon^{-c+t} + \varepsilon^{ct+1} + \varepsilon^{-ct-1} + \varepsilon^{ct-1} + \varepsilon^{-ct+1} = 0,$$

which, by Lemma 2.7, is impossible; so this case is excluded.

Case 2 ($\boldsymbol{\kappa = 1}$).

$$\varepsilon^{c+t} + \varepsilon^{-c-t} + \varepsilon^{c-t} + \varepsilon^{-c+t} = \varepsilon^{ct+1} + \varepsilon^{-ct-1} + \varepsilon^{ct-1} + \varepsilon^{-ct+1}.$$

From Lemma 2.6, it follows that

- $c + t \equiv \pm(ct + 1)$ or
- $c + t \equiv \pm(ct - 1)$.

In the first case, either $c - 1 \equiv (c - 1)t \pmod{n}$ (and $1 \equiv t \pmod{n}$, which does not happen as $t = 1 + 3^{d-1}$) or $c + 1 \equiv (c + 1)(-t) \pmod{n}$ (and then $1 \equiv -t \pmod{n}$, which does not happen either).

In the latter case, we also have that $c - t \equiv \pm(ct + 1) \pmod{n}$. So,

$$\begin{aligned} c + t &\equiv \pm(ct - 1) \pmod{n}, \\ c - t &\equiv \pm(ct + 1) \pmod{n}. \end{aligned}$$

If the two $\pm$ signs in the equations above disagree, then, adding them, we have $2c \equiv 2$, which is absurd. And if the $\pm$ signs agree, we have $2c \equiv 2ct$, which implies $t \equiv 1 \pmod{n}$, which is not possible either.

We conclude that $|u_c(\varepsilon)| \neq |u_c(\varepsilon^t)|$, which implies that $|u_c(\varepsilon^t)| \neq |u_c(\varepsilon^{t^2})|$ and that $|u_c(\varepsilon^{t^2})| \neq |u_c(\varepsilon)|$, as desired. □

3. Bicyclic and alternating units

As we declared initially, we intend to prove Theorem 1.1 by induction on $|G|$. Therefore, we need to know how to lift alternating units from homomorphic images of $\mathbb{Z}G$ back to $\mathbb{Z}G$. The next proposition deals with this.

Proposition 3.1. *Let* $^{-}\colon \mathbb{Z}G \to \mathbb{Z}H$ *be the group ring homomorphism obtained by extending linearly the group epimorphism* $^{-}\colon G \to H$. *If* $u_c(\bar{y})$ *is an alternating unit of* $\mathbb{Z}H$, *then there exist an element* x *in* G *such that the order of* x *and the order of* $\bar{y}$ *have the same prime factors, and there exists an alternating unit* $u_c(x)$ *such that* $\overline{u_c(x)} = u_c(\bar{x}) = u_c(\bar{y})$.

Proof. Let N be the kernel of $^{-}\colon G \to H$, so $G/N \simeq H$. Suppose $\bar{y}$ has order m in H, with $m = p_1^{k_1} \cdots p_r^{k_r}$, where $p_1, \dots, p_r$ are r distinct primes. Then m is the smallest integer such that $y^m \in N$, with $y \in G$ a pre-image of $\bar{y}$. Let a be the smallest integer such that $y^{ma} = 1$. If $a = 1$ or if a is a product of powers of the p_i, then we are done (take $x = y$). Otherwise, we may suppose that $(a, m) = 1$ (in fact, if $(a, m) \neq 1$, write $a = a'\mu$, where $p_i | \mu$ if $p_i | a$, and a' is not divisible by any of the p_i. Define $m' := m\mu$. Now, $(a', m') = 1$, and we may replace a by a' and m by m'). There exist $d, e \in \mathbb{Z}$ such that $ad + me = 1$. Take $x := y^{ad}$; so, the p_i are the only prime factors of the order of x, and $\bar{y} = \bar{y}^{ad+me} = \bar{y}^{ad}\bar{y}^{me} = \bar{y}^{ad} = \bar{x}$, since $y^{me} \in N$. Thus, $u_c(\bar{x}) = u_c(\bar{y})$, as we wanted. □

Below we state and prove the lemma that will be used in proving case (3) of Lemma 2.1.

Lemma 3.2. *Let* $P = \langle x \rangle$ *be a cyclic group of prime order* p *that acts faithfully and irreducibly on an elementary abelian* q*-group* Q, *with* $q \neq p$ *a prime. Consider the group* $G = Q \rtimes P$. *If* $p \geqslant 5$ *and* $q \geqslant 3$, *then for any* $1 \neq y \in Q$ *there exist suitable alternating units* $u = u_c(x)$ *and* $v = u_c(x^y)$ *in* $\mathcal{U}(\mathbb{Z}G)$, *such that for all sufficiently large integers* m *we have that* $\langle u^m, v^m \rangle$ *is a free group of* $\mathcal{U}(\mathbb{Z}G)$.

Proof. Take $y \in Q \setminus \{1\}$. By [**7**, Lemma 2.6], the elements $y^{1+x}, y^{1+x^2}, \dots, y^{1+x^{p-1}}$ cannot be all P-conjugates to y^{1+x}. In other words, there exist $t \in \{1, 2, \dots, p-1\}$ with y^{1+x} not P-conjugate to y^{1+x^t}. Since $(y^{1+x})^{x^{-1}} = y^{1+x^{-1}}$, it is clear that $t \neq 1, p-1$. Thus, $2 \leqslant t \leqslant p-2$, and we take $c \in \mathbb{Z}$ a positive integer such that

$$c \equiv \frac{t-1}{t+1} \pmod{p}.$$

Of course, $c \not\equiv 0 \pmod{p}$ and, since $t \equiv (1-c)/(1+c) \pmod{p}$, we have that $c \not\equiv \pm 1 \pmod{p}$. Therefore, we may assume that $2 \leqslant c \leqslant p-2$.

We now consider the alternating units $u = u_c(x)$, $v = u_c(y^{-1}xy) = y^{-1}u_c(x)y$, and argue exactly as in [**6**, Lemma 4.6]. □

Now, we prove the claim of Theorem 1.1 for each group type in Lemma 2.1. In fact, the proofs of cases (1)–(3) are given in [**3**, § 6], so here we will only give a brief sketch of them.

https://doi.org/10.1017/S0013091510000428 Published online by Cambridge University Press

Proposition 3.3. *Let G be a finite group of odd order, possessing an element $x \in G \setminus \mathcal{Z}(G)$ such that the order of x is either a prime number $p \geqslant 5$ or $3^r \geqslant 9$ and that, for every proper subgroup or proper homomorphic image H of G, the elements of H of order $p \geqslant 5$ or $3^r \geqslant 9$ are central in H. Then there exist an alternating unit u based on the element x and depending on a parameter c and a unit v, being either a bicyclic unit or an alternating unit, such that for all sufficiently large integers m we have that $\langle u^m, v^m\rangle = \langle u^m\rangle * \langle v^m\rangle = \mathbb{Z} * \mathbb{Z}$.*

Proof. We know that G is one of the group types of Lemma 2.1.

As before, cases (1)–(3) refer to G being a p-critical group, whereas in case (4) G belongs to the families described in Lemma 2.1 (a) and (b).

(1) $G = B \rtimes A$ is as in case (1) of Lemma 2.1.

We consider further subcases depending on the group B.

- $B = \langle b\rangle$ is cyclic of order $p^{n+1} \geqslant p^2$ with $b^a = b^{1+p^n}$. Let ε be a complex primitive root of unity of order p^{n+1}. Consider the map $\lambda\colon \mathbb{C}B \to \mathbb{C}$ given by $\lambda(b) := \varepsilon$, which induces the representation $\theta := \lambda^G\colon \mathbb{C}G \to M_p(\mathbb{C})$. We have that $\theta(b) = \mathrm{diag}(\varepsilon, \varepsilon^t, \ldots, \varepsilon^{t^{p-1}})$, with $t = 1 + p^n$, and

$$\theta(a) = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{pmatrix}.$$

  Let us also choose $c \in \mathbb{N}$, with $(c, p) = 1$ and set $u := u_c(b)$, $v := u_c(a)$.

  Now, arguing as in [**6**, Lemma 4.3], we find $m_0 \in \mathbb{N}$, such that for all integers $m > m_0$ we have $\langle u_c(a)^m, u_c(b)^m\rangle = \langle u_c(a)^m\rangle * \langle u_c(b)^m\rangle$.

  At this point, is important to mention that no power of the alternating unit $u_c(a)$ can be a factor in a free product by a bicyclic unit in $\mathcal{U}(\mathbb{Z}G)$. The same argument, given in [**4**, Example 2.3], applies here.

- $B = \langle b\rangle \times \langle z\rangle$, with z central of order p and $b^a = bz$.

  Let ε be a complex primitive root of unity of order p. Consider the map $\lambda\colon \mathbb{C}B \to \mathbb{C}$ given by $\lambda(b) := \varepsilon$, $\lambda(z) := \varepsilon$, which induces the representation $\theta := \lambda^G\colon \mathbb{C}G \to M_p(\mathbb{C})$. We have that $\theta(b) = \mathrm{diag}(\varepsilon, \varepsilon^2, \ldots, \varepsilon^p = 1)$ and

$$\theta(a) = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{pmatrix}.$$

Also, choose $c \in \mathbb{N}$ such that $(c,p)=1$ and set $u := u_c(b)$, $\tau := (1-a)b\hat{a}$ and $v := 1+\tau$. Then $S := \theta(u) = \operatorname{diag}(u_c(\varepsilon), u_c(\varepsilon^2), \dots, 1)$ and

$$T := \theta(v) = I_p + \begin{pmatrix} \varepsilon-\varepsilon^2 & \varepsilon-\varepsilon^2 & \cdots & \varepsilon-\varepsilon^2 \\ \varepsilon^2-\varepsilon^3 & \varepsilon^2-\varepsilon^3 & \cdots & \varepsilon^2-\varepsilon^3 \\ \vdots & \vdots & \ddots & \vdots \\ 1-\varepsilon & 1-\varepsilon & \cdots & 1-\varepsilon \end{pmatrix},$$

where I_p denotes the $p \times p$ identity matrix.

We have that

$$\mathcal{I} := \operatorname{Im}\tau = \begin{pmatrix} \varepsilon-\varepsilon^2 \\ \varepsilon^2-\varepsilon^3 \\ \vdots \\ 1-\varepsilon \end{pmatrix},$$

and $\mathcal{K} := \ker\tau = \{(z_0, z_1, \dots, z_{q-1}) \mid z_0 + z_1 + \cdots + z_{q-1} = 0\}$.

Let $\mathfrak{B} = \{e_0, e_1, \dots, e_{p-1}\}$ be the canonical basis of $\mathbb{C}^p$, and let r_+ and r_- be, respectively, the maximum and the minimum of the absolute values of the eigenvalues of S. Let $i_\pm = \{i \mid |u_c(\varepsilon_i)| = r_\pm\}$ and let X_+ be the span of the set $\{e_i \mid i \in i_+\}$. Let X_- be the span of the set $\{e_i \mid i \in i_-\}$, and let X_0 be the span of the remaining canonical vectors.

Notice that the dimensions of both X_+ and X_- are 2, while the dimension of $\mathcal{K}$ is 1, so Theorem 2.2 cannot be applied. We defer the proof until the next case.

(2) $G = P \rtimes Q$, with P an elementary abelian p-group and Q the cyclic group of order $q \neq p$, and Q acts irreducibly on P as a group of order q.

Take $x \in P$, with x of order $p \geqslant 5$ and not central in G, and $y \in Q \setminus \{1\}$.

By [**3**, § 6, Claim 2], there is a linear representation λ of P such that the induced representation $\theta = \lambda^G$ is irreducible, $\theta((x,y)) \neq 1$, and either $|P| = p$ or $x \in \ker(\lambda)$.

Fix a representation λ of P as above and let its induced representation be $\theta = \lambda^G$. Set $\varepsilon_i := \lambda(x^{y^i})$. Notice that all the ε_i are pth roots of unity, not necessarily distinct. As in [**3**, § 6, Claim 2], the set $Z = \{\varepsilon_i;\ i = 0, \dots, q-1\}$ contains at least two different elements when $|P| \neq p$. On the other hand, if $|P| = p$, then λ is injective and thus the ε_i are pairwise distinct.

We have that $\theta(x) = \operatorname{diag}(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{q-1})$ and

$$\theta(y) = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{pmatrix}.$$

https://doi.org/10.1017/S0013091510000428 Published online by Cambridge University Press

Now, choose $c \in \mathbb{N}$ such that $(c,p) = 1$ and set $u := u_c(x)$ and $v := 1 + \tau$. Then $S := \theta(u) = \mathrm{diag}(u_c(\varepsilon_0), u_c(\varepsilon_1), \dots, u_c(\varepsilon_{q-1}))$ and

$$T := \theta(v) = I_q + \begin{pmatrix} \varepsilon_0 - \varepsilon_1 & \varepsilon_0 - \varepsilon_1 & \cdots & \varepsilon_0 - \varepsilon_1 \\ \varepsilon_1 - \varepsilon_2 & \varepsilon_1 - \varepsilon_2 & \cdots & \varepsilon_1 - \varepsilon_2 \\ \vdots & \vdots & \ddots & \vdots \\ \varepsilon_{q-1} - \varepsilon_0 & \varepsilon_{q-1} - \varepsilon_0 & \cdots & \varepsilon_{q-1} - \varepsilon_0 \end{pmatrix},$$

where I_q denotes the $q \times q$ identity matrix.

Finally, argue as in [**3**, § 6, Claims 3–5].

That reasoning applies to the present case and also to the former one, and so we conclude that convenient homomorphic images $\bar{S}$ and $\bar{T}$ of the maps S and T satisfy the hypothesis of Theorem 2.2. Thus, there exists $m_0 \in \mathbb{N}$ such that, for all integers $m > m_0$, we have that $\langle T^m, S^m \rangle = \langle T^m \rangle * \langle S^m \rangle \cong \mathbb{Z} * \mathbb{Z}$ and so $\langle u_c(x)^m, v^m \rangle$ is a non-abelian free subgroup of $\mathcal{U}(\mathbb{Z}G)$ for sufficiently large $m \in \mathbb{Z}$.

(3) $G = Q \rtimes P$, with Q a q-group and P a cyclic group of order $p \neq q$, where P acts faithfully and irreducibly on the Frattini quotient $Q/\Phi(Q)$ and P centralizes $\Phi(Q)$.

Since alternating units and bicyclic units can be lifted (by Proposition 3.1), we can replace Q by $\bar{Q} := Q/\Phi(Q)$, and G by $\bar{G} := \bar{Q} \rtimes P$, and so assume that $\Phi(Q) = 1$, and that $\langle x \rangle = P$ acts faithfully and irreducibly on the elementary abelian q-group Q. From the fact that $p \geqslant 5$, by Lemma 3.2, there exist $y \in Q$ and a pair of alternating units $u := u_c(x)$ and $v := u_c(x^y)$ in $\mathcal{U}(\mathbb{Z}G)$ such that $\langle u^m, v^m \rangle$ is a non-abelian free subgroup of $\mathcal{U}(\mathbb{Z}G)$ for sufficiently large $m \in \mathbb{Z}$.

(4) We will only give the proof of case (a), for case (b) goes along the same lines.

Let $G = \langle x, y \mid x^{3^l} = 1 = y^3 = 1, x^y = x^{1+3^{l-1}} \rangle$, let ε be a complex primitive root of unity of order 3^l, and set $t := 1 + 3^{l-1}$.

Consider the map $\theta \colon \mathbb{C}G \to M_3(\mathbb{C})$, with $\theta(x) = \mathrm{diag}(\varepsilon, \varepsilon^t, \varepsilon^{t^2})$ and

$$\theta(y) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

It is easy to check that $\theta(x)$ and $\theta(y)$ satisfy the same relations as x and y, so θ is indeed a representation of $\mathbb{C}G$.

Also, choose $1 < c \in \mathbb{N}$ such that $(c, 3^l) = 1$, and set $u := u_c(x)$, $\tau := (1-y)x\hat{y}$ and $v := 1 + \tau$. Then $S := \theta(u) = \mathrm{diag}(u_c(\varepsilon), u_c(\varepsilon^t), u_c(\varepsilon^{t^2}))$ and

$$T := \theta(v) = I_3 + \begin{pmatrix} \varepsilon - \varepsilon^t & \varepsilon - \varepsilon^t & \varepsilon - \varepsilon^t \\ \varepsilon^t - \varepsilon^{t^2} & \varepsilon^t - \varepsilon^{t^2} & \varepsilon^t - \varepsilon^{t^2} \\ \varepsilon^{t^2} - \varepsilon & \varepsilon^{t^2} - \varepsilon & \varepsilon^{t^2} - \varepsilon \end{pmatrix},$$

where I_3 denotes the 3×3 identity matrix.

We have that the eigenvalues of S are all distinct (by Lemma 2.8). Let r_+ and r_- be the maximum and the minimum of the absolute values of the eigenvalues of S, and let

i_+ and i_- be defined as $i_\pm = \{i \mid |u_c(\varepsilon^{t^i})| = r_\pm\}$. Let $\mathfrak{B} = \{e_0, e_1, e_2\}$ be the canonical basis of $V := \mathbb{C}^3$. Let us denote by $X_+ \neq 0$ the span of e_{i_+}, by $X_- \neq 0$ the span of e_{i_-}, and by X_0 the span of the remaining canonical vector.

We have that

$$\mathcal{I} := \operatorname{Im}\tau = \begin{pmatrix} \varepsilon - \varepsilon^t \\ \varepsilon^t - \varepsilon^{t^2} \\ \varepsilon^{t^2} - \varepsilon \end{pmatrix},$$

and $\mathcal{K} := \ker\tau = \{(z_0, z_1, z_2) \mid z_0 + z_1 + z_2 = 0\}$.

We easily check that $X_\pm \cap \mathcal{K} = \mathcal{I} \cap (X_\pm \oplus X_0) = 0$. So, by Theorem 2.2, there exists $m_0 \in \mathbb{N}$ such that, for all integers $m > m_0$ we have $\langle T^m, S^m\rangle = \langle T^m\rangle * \langle S^m\rangle \cong \mathbb{Z} * \mathbb{Z}$. Therefore, $\langle u^m, v^m\rangle \cong \mathbb{Z} * \mathbb{Z}$ also. □

We are ready to prove Theorem 1.1.

Proof of Theorem 1.1. The proof is by induction on $|G|$.

If G has a proper non-abelian subgroup H satisfying the hypothesis of the theorem, then by induction $\mathbb{Z}H$ contains an alternating unit $u_c(x)$, based on an element $x \in H$ of order n, with $(c, n) = 1$, and a unit v, either alternating or bicyclic, such that for all sufficiently large integers m we have that $\langle u_c(x)^m, v^m\rangle$ is a free group. So the result is proved in this situation, since these units are units of $\mathbb{Z}G$.

Now, suppose that G has a proper non-abelian homomorphic image H satisfying the hypothesis of the theorem. By induction, there exist in $\mathbb{Z}H$ an alternating unit $u_c(\bar{y})$, based on a non-central element $\bar{y} \in H$, and a unit $\bar{v}$, either alternating or bicyclic, such that for all sufficiently large integers m we have that $\langle u_c(\bar{y})^m, \bar{v}^m\rangle$ is a free group. Since alternating units can be lifted, by Proposition 3.1, and bicyclic units also, the result holds for $\mathbb{Z}G$. □

Remark 3.4. Alternating units behave similarly to Bass cyclic units. So, [**6**, Theorem 4.7] remains true if we substitute in its statement 'Bass cyclic units' by 'alternating units'.

Acknowledgements. J.Z.G. was supported by Grant CNPq 303.756/82-5 and by FAPESP-Brazil, Projeto Temático 00/07.291-0. P.M.V. was supported by FAPESP post-doctoral scholarship 06/59817-2. The authors are indebted to Professor Donald Passman for many enlightening conversations.

References

1. A. Dooms, E. Jespers and M. Ruiz, Free groups and subgroups of finite index in the unit group of an integral group ring, *Commun. Alg.* **35** (2007), 2879–2888.
2. R. A. Ferraz, Free subgroups in the units of $\mathbb{Z}[K_8 \times C_p]$, *Commun. Alg.* **31** (2003), 4291–4299.
3. J. Z. Gonçalves and A. del Rio, Bicyclic units, Bass cyclic units and free groups, *J. Group Theory* **11** (2008), 247–265.
4. J. Z. Gonçalves and A. del Rio, Bass cyclic units as factors in a free group, *Int. J. Alg. Computat.*, in press.

5. J. Z. Gonçalves and D. S. Passman, Embedding free products in the unit group of an integral group ring, *Arch. Math.* **82** (2004), 97–102.
6. J. Z. Gonçalves and D. S. Passman, Linear groups and group rings, *J. Alg.* **295** (2006), 94–118.
7. J. Z. Gonçalves and D. S. Passman, Involutions and free pairs of bicyclic units in integral group rings, *J. Group Theory* **13** (2010), 721–742.
8. J. Z. Gonçalves and P. M. Veloso, *Special units, unipotent units and free groups in group algebras*, Contemporary Mathematics, Volume 499, pp. 127–140 (American Mathematical Society, Providence, RI, 2009).
9. M. Hall, *The theory of groups* (Macmillan, New York, 1959).
10. B. Hartley and P. F. Pickel, Free subgroups in the unit groups of integral group rings, *Can. J. Math.* **32** (1980), 1342–1352.
11. E. Jespers, A. del Rio and M. Ruiz, Groups generated by two bicyclic units in integral group rings, *J. Group Theory* **5** (2002), 493–511.
12. Z. S. Marciniak and S. K. Sehgal, Constructing free subgroups of integral group rings, *Proc. Am. Math. Soc.* **125** (1997), 1005–1009.
13. S. K. Sehgal, *Units in integral group rings* (Longman, New York, 1993).