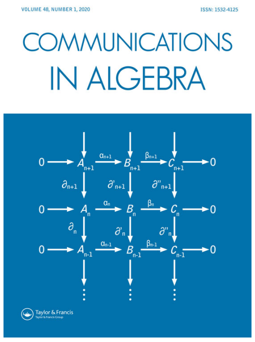

Taylor & Francis
Taylor & Francis Group

Communications in Algebra

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/lagb20

Central units in some integral group rings

Vitor Araujo Garcia & Raul Antonio Ferraz

COMMUNICATIONS IN ALGEBRA®
https://doi.org/10.1080/00927872.2021.1910284

Taylor & Francis
Taylor & Francis Group

Check for updates

Central units in some integral group rings

Vitor Araujo Garcia and Raul Antonio Ferraz

Departamento de Matemática, Universidade de São Paulo, São Paulo, Brazil

ABSTRACT

Let G be a finite group and $\mathbb{Z}G$ be the integral group ring of G. We denote by $U_1(\mathbb{Z}G)$ the group of normalized units of $\mathbb{Z}G$; that is, the units which have augmentation 1, and by $Z(U_1(\mathbb{Z}G))$ the group of normalized central units. Many articles have been written describing the groups $U_1(\mathbb{Z}G)$ and $Z(U_1(\mathbb{Z}G))$ for certain groups G. In this work, we will describe the group of normalized central units of some integral group rings by applying the idea presented in an article by Ferraz and Simón to a wider variety of groups, and we will study some examples of groups that can be treated with this method: metacyclic groups of type $C_{q^m} \rtimes C_{p^n}$; some metacyclic p-groups; some metabelian p-groups and some generalized dihedral groups.

ARTICLE HISTORY
Received 13 November 2020
Revised 9 March 2021
Communicated by Sudarshan Kumar Sehgal

KEYWORDS
Central units; integral group rings; metabelian groups

2020 MATHEMATICS SUBJECT CLASSIFICATION
20C05

1. Introduction

Describing explicitly the group of units of integral group rings is a classical open problem, that has been solved only for some groups, such as cyclic groups of order p^n for some prime numbers p and some integers n (see [2, 7, 8]), groups of type $C_2 \times C_p$ or $C_2 \times C_2 \times C_p$, for some prime numbers p (see [9]) and, using the results of [7] and [13], some elementary abelian groups. See also [5].

The problem of describing explicitly the group of central units of integral group rings $\mathbb{Z}G$ has been solved for some non-abelian groups, such as the alternating groups A_n, for values of n such that the group of central units of $\mathbb{Z}A_n$ has rank 1 (see [1,3]), and groups of type $C_q \rtimes C_p$ (semi-direct product of cyclic groups) for certain values of p and q (see [11]). But there is still a great amount of groups that do not have such a description yet.

In the present paper, we generalize the results obtained in [11] to a wider variety of groups that share properties that allow us to apply the same ideas that the authors used, and we are able to describe explicitly the group of central units of some classes of integral group rings.

First we fix some notations: If $H \leq G$ are groups and H is finite, then $\widehat{H} := \sum_{h \in H} h$ and if $|H|$ is invertible in R, then we denote the idempotent $e_H = \frac{1}{|H|}\widehat{H} \in RG$; if G is a group such that $H \lhd G$ and R is a ring, then $\Delta(G, H)$ denotes the kernel of the ring homomorphism $\pi : RG \to R(G/H)$ that extends linearly the natural projection $G \to G/H$; we also denote ε as the augmentation map. If G is a group and $g \in G$, then $o(g)$ is the order of g in G.

We also remember that a prime number is called regular if it divides its class number. For example, all prime numbers $p < 37$ are regular (see [4], p. 430, Table 9).

Proposition 1.1. (*Proposition* 3.6.7, [15]) *Let R be a ring and H, G groups such that $H \lhd G$. If $|H|$ is invertible in R, we have:*

CONTACT Vitor Araujo Garcia vitorargarcia@hotmail.com Departamento de Matemática, Universidade de São Paulo, Rua do Matão, 1010, 05508-090 - São Paulo, Brazil.

$$RG = RGe_H \bigoplus RG(1 - e_H),$$

with $RGe_H \cong R(G/H)$ *and* $RG(1 - e_H) = \Delta(G, H)$.

In particular, we have that $RG = RGe_{G'} \bigoplus RG(1 - e_{G'})$. In this case, if R is commutative, the first component of the direct sum above will be composed of elements that commute with RG. Then we have the following:

Theorem 1.2. *Let G a finite group, then*

$$Z(U_1(\mathbb{Q}G)) = ((1 + \mathbb{Q}Ge_{G'}) \cap U_1(\mathbb{Q}G)) \times ((1 + \mathbb{Q}G(1 - e_{G'})) \cap Z(U_1(\mathbb{Q}G)))$$

Proof. First, we note that both factors are in $Z(U_1(\mathbb{Q}G))$, because of the paragraph above.

Proposition 1.1 gives us that $(1 + \mathbb{Q}Ge_{G'}) \cap (1 + \mathbb{Q}G(1 - e_{G'})) = \{1\}$.

Now suppose $u \in Z(U_1(\mathbb{Q}G))$. Let us take $u_1 = 1 + (u - 1)e_{G'}, u_2 = 1 + (u - 1)(1 - e_{G'})$. Then we have:

$$u_1u_2 = (1 + (u - 1)e_{G'})(1 + (u - 1)(1 - e_{G'})) =$$
$$= 1 + (u - 1)(1 - e_{G'}) + (u - 1)e_{G'} + (u - 1)e_{G'}(1 - e_{G'}) = 1 + u - 1 = u,$$

because $e_{G'}$ is idempotent.

Then we have the result. □

Remark 1.3. *Considering the morphism* $\pi : \mathbb{Q}G \to \mathbb{Q}G/G'$, *we could take any* $u_1 = 1 + (w - 1)e_{G'}$, *such that* $\pi(w) = \pi(u)$ *in the proof above.*

Now we are able to describe $Z(U_1(\mathbb{Z}G))$ for certain groups G. First we fix some notations: if $g \in G$, then C_g denotes the conjugacy class of g, and γ_g denotes the class sum of g.

Theorem 1.4. *Let G be a finite group such that the following property holds:*

If $x \in G$ *and* $x \notin G'$, *then* $\gamma_x = \widehat{G'}x$.

Then we have that:

$$Z(U_1(\mathbb{Z}G)) = ((1 + \mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G)) \times (U_1(\mathbb{Z}G') \cap Z(\mathbb{Z}G))$$

Proof. We denote by $I_{G'}$ a complete set of representatives of the conjugacy classes of G contained in G', and by $I_{G-G'}$ a complete set representatives of the conjugacy classes of G that don't intersect G' (these are all the possible conjugacy classes, as $G' \lhd G$).

Let $u \in Z(U_1(\mathbb{Z}G))$. As u is a central element of the group ring, we have that u can be written as following:

$$u = \sum_{a \in I_{G'}} \alpha_a \gamma_a + \sum_{b \in I_{G-G'}} \alpha_b \widehat{G'} b,$$

where $\alpha_s \in \mathbb{Z}$, for all s. We denote by π the ring homomorphism that extends linearly the projection $G \to G/G'$. We have:

$$\pi(u) = \sum_{a \in I_{G'}} \alpha_a |C_a| + |G'| \sum_{b \in I_{G-G'}} \alpha_b b \in U_1(\mathbb{Z}G/G').$$

As $\varepsilon(\pi(u)) = 1$, we have that $\sum_{a \in I_{G'}} \alpha_a |C_a| \equiv 1 (mod |G'|)$. So, we can define the following elements:

$$w_1 := 1 + \left(\frac{\sum_{a\in I_{G'}} \alpha_a |C_a| - 1 + |G'| \sum_{b\in I_{G-G'}} \alpha_b b}{|G'|} \right) \widehat{G'} \in 1 + \mathbb{Z}Ge_{G'}.$$

$$w_2 := \sum_{a\in I_{G'}} \alpha_a \gamma_a - \left(-1 + \sum_{a\in I_{G'}} \alpha_a |C_a| \right) \frac{\widehat{G'}}{|G'|} \in \mathbb{Z}G'.$$

To prove our result, we will verify that $w_1 w_2 = u$. This should be enough, since we would have that $w_1^{-1} = w_2 u^{-1}$ and $w_2^{-1} = w_1 u^{-1}$ (so they are units), and we have that the elements w_1 and u being central imply that w_2 is central.

$$w_1 w_2 = w_2 + \frac{1}{|G'|} \left(\sum_{a\in I_{G'}} \alpha_a |C_a| - 1 + |G'| \sum_{b\in I_{G-G'}} \alpha_b b \right) \widehat{G'} w_2$$

Since $w_2 \in \mathbb{Z}G'$ has augmentation 1, we can write:

$$w_1 w_2 = w_2 + \frac{1}{|G'|} \left(\sum_{a\in I_{G'}} \alpha_a |C_a| - 1 + |G'| \sum_{b\in I_{G-G'}} \alpha_b b \right) \widehat{G'} = u.$$

And our result is proven. □

Let us denote $\mathbb{Z}_n$ the ring of integers modulo n, for all positive integers n. Also, we fix $m := |G'|$ the order of G'. Consider the morphism $\mathbb{Z}G/G' \to \mathbb{Z}_m G/G'$ that extends linearly the natural projection of the coefficients, and we denote $\pi_m : U_1(\mathbb{Z}G/G') \to U(\mathbb{Z}_m G/G')$ the induced group homomorphism on the group of normalized units. We also consider again the ring homomorphism $\pi : \mathbb{Z}G \to \mathbb{Z}(G/G')$, that extends linearly the projection $g \mapsto \bar{g} \in G/G'$.

Then we have the following corollary:

Corollary 1.5. *With the same hypotheses of Theorem 1.4 and the definitions on the paragraph above, we have:*

$$Z(U_1(\mathbb{Z}G)) = W_1 \times W_2,$$

where:

$$W_1 = \left\langle 1 + \frac{(\omega - 1)\widehat{G'}}{m} | \omega \in \pi^{-1}(\ker(\pi_m)) \right\rangle \cong \ker(\pi_m),$$
$$W_2 = (U_1(\mathbb{Z}G') \cap Z(\mathbb{Z}G)).$$

Proof. By the previous theorem, we just need to verify that $W := W_1 = ((1 + \mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G))$ and that $W \cong \ker(\pi_m)$.

Let us take an arbitrary unit of the form $1 + (x-1)e_{G'}, x \in \mathbb{Z}G$. In order to prove that this unit is in W_1, we have to prove that $\pi(x) \in \ker(\pi_m)$.

We have the following: if $x, y \in \mathbb{Z}G$ then

$$(1 + (x-1)e_{G'})(1 + (y-1)e_{G'}) = (1 + (xy-1)e_{G'}).$$

So we have that $(1 + (x-1)e_{G'}) \in U_1(\mathbb{Z}G)$ if, and only if $\pi(x) \in U_1(\mathbb{Z}G/G')$ and $(x-1)e_{G'} \in \mathbb{Z}G$ (that is, it has integer coefficients), due to the isomorphism $\mathbb{Z}Ge_{G'} \cong \mathbb{Z}G/G'$, induced by $ge_{G'} \mapsto \bar{g}$ – in this case, the inverse of $(1 + (x-1)e_{G'})$ would be $(1 + (y-1)e_{G'})$, where $\pi(y) = \pi(x)^{-1}$. This proves that $W_1 \subset ((1 + \mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G))$ (because the domain of π_m consists only of units and, if $\pi(x) \in \ker(\pi_m)$, then $1 + (x-1)e_{G'}$ has only integer coefficients).

Now we prove the other inclusion: suppose $u = 1 + (x-1)e_{G'} \in ((1 + \mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G))$, for a certain $x \in \mathbb{Z}G$. Taking $\{g_i G', i \in I\}$ a complete set of representatives of cosets of G/G', we can assume that there are integers x_i such that x can be written:

$$x = \sum_{i \in I} x_i g_i.$$

From now on we assume that x is written in the form above. If g_i is a coset representative such that $g_i \notin G'$ and $h \in G'$, we have that the coefficient of $g_i h$ in $1 + (x-1)e_{G'}$ is $\frac{x_i}{|G'|}$. If otherwise g_i is a coset representative of the class $\bar{1}$, then the coefficient of $g_i h$ is $\frac{x_i}{|G'|} - \frac{1}{|G'|}$. Therefore we conclude $\pi(x) \in \ker(\pi_m)$, because every coefficient of $(x-1)$ is divisible by $m = |G'|$ so that $1 + (x-1)e_{G'}$ has integers coefficients and by the proof of the first inclusion, we have that $\pi(x)$ is a unit. Thus $x \in \pi^{-1}(\ker(\pi_m))$.

So, we proved the remaining inclusion $((1 + \mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G)) \subset W_1$. Also, $W_1 \cong \ker(\pi_m)$, because $1 + \frac{(\omega_1 - 1)\widehat{G'}}{|G'|} = 1 + \frac{(\omega_2 - 1)\widehat{G'}}{|G'|}$ if, and only if $\pi(\omega_1) = \pi(\omega_2)$.

And our result is proven. □

Now we are ready to apply these results to some concrete examples of groups.

2. Groups of type $C_{q^m} \rtimes C_{p^n}$

In this chapter, we will do something similar to what was done in [11], applying Corollary 1.5. First we fix some notations: given $p \neq q$ odd primes and m, n, r integers such that $1 < r < q^m$, we define for this section

$$G := C_{p^n, q^m, r} = \langle a, b | a^{q^m} = b^{p^n} = 1, bab^{-1} = a^r \rangle.$$

We will need that $r^{p^n} \equiv 1 (mod q^m)$, and it follows that $(r, q) = 1$. We will study only the cases that are non-commutative, so we will assume $r \not\equiv 1 (mod\, q^m)$. These are all the non-commutative possible cases. These groups G are semidirect products $C_{q^m} \rtimes C_{p^n}$.

In [14], the authors presented a set of linearly independent units that generate a subgroup of finite index for the group of central units of the integral group ring of $C_{q^m} \rtimes C_{p^n}$ when the action defining the semidirect product has trivial kernel.

Before we proceed, we will need some facts about the group $C_{p^n, q^m, r}$. First, let us fix the following notation: if $n > 1$ is an integer, we denote $U(\mathbb{Z}_n)$ the group of units of $\mathbb{Z}_n$.

Lemma 2.1. *If $C_{p^n, q^m, r}$ and $C_{p^n, q^m, s}$ are groups as defined above, and if there exists an integer o such that $o(r) = o(s) = p^o$ in $U(\mathbb{Z}_{q^m})$, then $C_{p^n, q^m, r} \cong C_{p^n, q^m, s}$.*

Proof. We know that $U(\mathbb{Z}_{q^m})$ (the group of units of $\mathbb{Z}_{q^m}$) is cyclic, then exists j such that $(j, p) = 1$ and $r^j \equiv s (mod\, q^m)$.

So, $b^j a b^{-j} = a^s$, and b^j generates $\langle b \rangle$ (because $(j, p) = 1$).

Then we have:

$$C_{p^n, q^m, r} = \langle a, b^j | a^{q^m} = b^{p^n} = 1, b^j a b^{-j} = a^s \rangle \cong C_{p^n, q^m, s}$$

□

We will conclude the converse of the above result after we find the conjugacy classes.

Lemma 2.2. *If $o(r) = p^o, o \geq 1$ in $U(Z_{q^m})$, and $0 \leq l < o$, then $r^{p^l} \not\equiv 1 (mod\, q^k)$, for all $0 < k \leq m$.*

Proof. We know that $|U(\mathbb{Z}_{q^m})| = q^{m-1}(q-1), |U(\mathbb{Z}_{q^k})| = q^{k-1}(q-1)$.

Since $r^{p^o} \equiv 1 (mod\, q^m)$, then $p^o | (q-1)$. Furthermore, we also know that $U(\mathbb{Z}_{q^m})$ is cyclic (since q is odd). Let t an integer such that its class modulo q^m generates $U(\mathbb{Z}_{q^m})$. We have that the class modulo q^k of t also generates $U(\mathbb{Z}_{q^k})$.

So, there are i, j such that $(j,p) = (i,p) = 1, r \equiv t^{q^{m-1}\frac{(q-1)j}{p^o}}(mod\, q^k)$ and $r \equiv t^{q^{m-1}\frac{(q-1)i}{p^o}}(mod\, q^m)$ (since $t^{q^{m-1}\frac{(q-1)}{p^o}}$ is a generator of the subgroups of order p^o of $U(\mathbb{Z}_{q^m})$ and of $U(\mathbb{Z}_{q^k})$, and the respective classes of r is in both subgroups).

So, $r^{p^l} \equiv t^{q^{m-1}\frac{(q-1)j}{p^{o-l}}}(mod\, q^k)$. But $q^{k-1}(q-1) \not| q^{m-1}\frac{(q-1)j}{p^{o-l}}$.

So we conclude that $r^{p^l} \not\equiv 1(mod\, q^k)$. □

Lemma 2.3. *Suppose $o(r) = p^o$ in $U(\mathbb{Z}_{q^m})$. Then there is $k \leq m$ such that $(1 - r^i, q^m) = q^k$ if, and only if $p^o|i$.*

In this case, $(1 - r^i, q^m) = q^m$.

Proof. ($\Rightarrow$) $q^k|(1 - r^i)$. So there is y integer such that $1 - r^i = q^k y$. We have:

$$r^i = q^k y + 1$$
$$r^i \equiv 1(mod\, q^k)$$

From Lemma 2.2 we have that $p^o|i$.

($\Leftarrow$) We have $1 - r^i \equiv 0(mod\, q^m)$, then we can take $k = m$. □

Now we will evaluate the conjugacy classes of $C_{p^n,q^m,r}$ and each class sum. Let us fix p^o as the order of r in the group of units of $\mathbb{Z}_{q^m}$:

(1) class $\{\mathbf{1}\}$, with class sum $\mathbf{1}$.

(2) let $1 \leq i \leq q^m - 1, (i,q) = 1$. We evaluate the conjugacy class of a^i:

$$(a^j b^k)a^i(b^{-k}a^{-j}) = a^{ir^k}$$

And we have

$$a^{ir^k} = a^{ir^s} \iff ir^k \equiv ir^s(mod\, q^m)$$

Since $(i,q) = 1$, the above is equivalent to:

$$r^k \equiv r^s(mod\, q^m) \iff k - s \equiv p^o(mod\, q^m)$$

So we have that, in this case, the class of a^i is $\{a^i, a^{ir}, a^{ir^2}, ..., a^{ir^{p^o-1}}\}$, and we denote its sum by γ_i.

In the case $(i,q^m) = q^l$, we have (without loss of generality, we consider $s > k$ below):

$$a^{ir^k} = a^{ir^s} \iff ir^k \equiv ir^s(mod\, q^m) \iff i(r^k - r^s) \equiv 0(mod\, q^m) \iff$$
$$q^{m-l}|(r^k - r^s) = r^k(1 - r^{s-k})$$

Since $(r,q) = 1$, the above is equivalent to:

$$q^{m-l}|(1 - r^{s-k}),$$

which is equivalent to

$$r^{s-k} \equiv 1(mod\, q^{m-l})$$

From Lemma 2.2, we have that the above is equivalent to

$$p^o|(s-k).$$

So in the case $(i,q) \neq 1$ we also have the same format for the conjugacy class of a^i.

(3) If $1 \le i \le p^n - 1, (1 - r^i, q) = 1$. We will find the conjugacy class of b^i:

$$(a^j b^k) b^i (b^{-k} a^{-j}) = a^j b^i a^{-j} = a^j b^i a^{-j} b^{-i} b^i = a^{j(1-r^i)} b^i$$

And we have

$$\begin{aligned} a^{j(1-r^i)} b^i = a^{l(1-r^i)} b^i &\iff \\ j(1 - r^i) \equiv l(1 - r^i)(mod\, q^m) &\iff \\ j \equiv l(mod\, q^m) \end{aligned}$$

Therefore, the class of b^i in this case is $\{b^i, ab^i, a^2 b^i, ..., a^{q^m-1} b^i\}$, and its sum is $\widehat{a} b^i$.

(4) If $1 \le i \le p^n - 1, (1 - r^i, q^m) = q^k$ (from Lemma 2.3), $k = m$). Let us evaluate the conjugacy class of b^i in this case:

$$(a^j b^k) b^i (b^{-k} a^{-j}) = a^{j(1-r^i)} b^i = b^i$$

So, the conjugacy class of b^i in this case is $\{b^i\}$, with sum b^i (this means that b^i is a central element of the group when $(1 - r^i, q) \ne 1$). In fact, the center of the group is generated by such b^i's.

(5) now we evaluate the case of elements of type $a^s b^i$. If $(1 - r^i, q) = 1$, the class appeared in case **(3)**, and in the case $(1 - r^i, q) \ne 1$, we can just use the fact that b^i is central, and we have that the class is $\{a^s b^i, ..., a^{sr^{p^o-1}} b^i\}$, with sum $\gamma_s b^i$.

Note that all the conjugacy classes we evaluated have 1, p^o or q^m elements, proving the reciprocal of Lemma 2.1, that is, if $C_{p^n,q^m,r} \cong C_{p^n,q^m,s}$, then $o(r) = o(s)$ in the group of units of $\mathbb{Z}_{q^m}$.

First we will show that if $o < n$ (remember that o is such that the order of r in the group of units of $\mathbb{Z}_{q^m}$ is p^o), then the assumption of Corollary 1.5 may not follow.

First we notice that $G' = \langle a \rangle$, and that $Z(G) = \langle b^{p^o} \rangle$. To show what we want, we could simply note that the units of $\mathbb{Z}\langle b^{p^o} \rangle$ are all central in $\mathbb{Z}G$ (since b^{p^o} is a central element in G), and if u is such a unit, then $1 + (u - 1)(1 - e_{G'})$ may have non-integer coefficients, for certain value of (p^n, q^m, r). We give an example:

Example: Let $(p^n, q^m) = (81, 19)$ and r such that the order of r in the group of units of $\mathbb{Z}_{19}$ is 9. And we consider the following Hoechsmann's unit (see [16], Chapter 2 for more information about such units):

$$u = (1 + (b^9)^2 + (b^9)^4 + (b^9)^6 + (b^9)^8)(1 + b^9) - \widehat{\langle b^9 \rangle},$$

in this case, one can easily verify that $1 + (u - 1)(1 - e_{G'}) = u - ue_{G'} + e_{G'}$ has non'integer coefficients.

Now we define the following morphism:

$$\pi_{q^m} : U_1(\mathbb{Z}C_{p^o}) \to U_1(\mathbb{Z}_{q^m} C_{p^o})$$

this morphism takes the coefficients to their classes modulo q^m.

With the conjugacy classes evaluated and the morphism above defined, we conclude the following:

Corollary 2.4. *If $o(r) = p^o$ in $U(\mathbb{Z}_{q^m})$, we have that:*

$$Z\left(U_1\left(\mathbb{Z}C_{p^o,q^m,r}\right)\right) = W_1 \times W_2,$$

where:

$$W_1 = \left\{1 + \frac{(\mu - 1)\widehat{a}}{q^m} | \mu \in \ker(\pi_{q^m})\right\} \cong \ker(\pi_{q^m})$$
$$W_2 = Z\big(U_1\big(\mathbb{Z}C_{p^o,q^m,r}\big)\big) \cap U_1(\mathbb{Z}C_{q^m})$$

Proof. By Corollary 1.5, we just have to prove that $G' = \langle a\rangle$. For this, note that $G = \langle a\rangle\langle b\rangle$, so $G' = [G, G] = [\langle a\rangle, \langle b\rangle] \subset \langle a\rangle$.

Furthermore, we have that $aba^{-1}b^{-1} = a^{1-r}$. From Lemma 2.3, we have that a^{1-r} generates $\langle a\rangle$, proving the result. □

Using the results of [7] and [8], we can now evaluate explicitly a basis for W_1 and a basis for W_2 in the cases $(p^o, q^m) = (3, 49), (9, 19) or (9, 37)$ (the other possible cases to evaluate using the results of [7] were already evaluated in [11]). In all cases we will utilize techniques similar to the ones used in [11] to evaluate a basis for W_2. Note that W_1 is trivial in the first case. In the other two cases we use GAP to evaluate W_1, and the code is in Section 4. We will start calculating a basis for W_2.

3. Basis for W_2

In this section, we will describe a basis for W_2 as in Corollary 2.4 when $(p^o, q^m) = (3, 49), (9, 19)$ or $(9, 37)$, and we use the same notations as the previous section. Let us denote $* : \mathbb{Z}G \to \mathbb{Z}G$ the classical involution, given by $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}$. An element $u \in \mathbb{Z}G$ is said to be symmetric if $u^* = u$. We start with the following proposition:

Proposition 3.1. *The units in W_2 are all symmetric.*

Proof. Let $\eta : U_1(\mathbb{Z}C_{q^m}) \to U_1(\mathbb{Z}C_{q^m})$ be the morphism that extends linearly $a \mapsto bab^{-1} = a^r$. We have that $W_2 = \{u \in U_1(\mathbb{Z}C_{q^m}) | \eta(u) = u\}$. We also have that $\eta(x^*) = \eta(x)^*$, for all $x \in \mathbb{Z}C_{q^m}$. Thus, if u is a symmetric unit, then $\eta(u)$ is a symmetric unit too.

Let $u \in W_2$. We have that u may be written uniquely as $u = a^i v$, with $0 \le i \le q^m - 1, v = v^*$. Since $\eta(u) = u$, we have that $a^i v = \eta(a^i v) = \eta(a^i)\eta(v) = a^{ri}\eta(v)$. Since $\eta(v)$ is symmetric and because of the unique expression for the above u, we have that $v = \eta(v)$, and that $a^{ri} = a^i$. So $q^m | (r-1)i$, and by Lemma 2.2, we have that $q \not| (r-1)$, thus $q^m | i$, and we have that $u = v$ proving the result. □

We will start with the cases $(p^n, q^m) = (9, 19)$ or $(9, 37)$, and we will treat the case $(p^o, q^m) = (3, 49)$ separately, since this case is different from the others.

3.1. Basis for W_2 when $(p^n, q^m) = (9, 19)$ or $(9, 37)$

Suppose in this subsection that $(p^n, q^m) = (9, 19)$ or $(9, 37)$. In particular, in these cases we have $m = 1$. We will construct a basis similar to the one presented in [11].

Let $S_0 = \{u_1, u_2, \ldots, u_{\frac{q-3}{2}}\}$ be a linearly independent set of maximum rank in $U_1(\mathbb{Z}C_q)$ (the rank of $U(\mathbb{Z}(C_q))$ follows from [7]), given by:

$$u_i = (1 + a^t + a^{2t} + \ldots + a^{(s-1)t})(1 + a^{t^i} + a^{t^{2i}} + \ldots + a^{(t-1)t^i}) - k\widehat{a},$$

where t is an integer representative of a generator of the units group of $\mathbb{Z}_q$, s is a representative of an inverse of t in this group, and $k = \frac{ts-1}{q}$ (these units are defined in [7]).

In [11], we have the inverses evaluated:

$$u_i^{-1} = (1 + a + a^2 + \dots + a^{t-1})(1 + a^{t^{i+1}} + a^{2t^{i+1}} + \dots + a^{(s-1)t^{i+i}}) - k\widehat{a}.$$

Now we define, for $2 \le i \le \frac{q-3}{2}$, the elements $v_i := u_{i-1}^{-1} u_i$, and $v_1 := u_1$.

Let $S_1 = \{v_1, \dots, v_{\frac{q-3}{2}}\}$. We have $\langle S_0 \rangle = \langle S_1 \rangle$, and similarly to what was evaluated in [11], we have:

$$v_i = (1 + a^{t^i} + a^{t^{2i}} + \dots + a^{(s-1)t^i})(1 + a^{t^i} + a^{2t^i} + \dots + a^{(t-1)t^i}) - k\widehat{a}.$$

With the expression above in mind, let us generalize this definition (of v_i) for all $i \ge 0$. We define the morphism $f : U_1(\mathbb{Z}C_q) \to U_1(\mathbb{Z}C_q)$ as the linear extension of the group homomorphism given by $a \mapsto a^t$. We have:

$$f(v_i) = v_{i+1}; f^{\frac{q-1}{2}}(v_i) = v_{i+\frac{q-1}{2}} = v_i^*.$$

We have that v_i may be written uniquely as $a^{j_i} w_i$, with $w_i = w_i^*$. So we have that:

$$f(w_i) = w_{i+1}; f^{\frac{q-1}{2}}(w_i) = w_i \tag{1}$$

We define $S_* = \{w_1, \dots, w_{\frac{q-3}{2}}\}$, and we have that S_* generates a complement for $\langle a \rangle$ in $U_1(\mathbb{Z}C_q)$.

From (1) we have that, defining $d := (q-1)/2$, then $w_i = w_{i+d}$, for all $i \ge 0$. We state Lemma 4.1 of [11]:

Lemma 3.2. [11] *With the definitions above, we have that* $w_0 w_1 \dots w_{\frac{q-3}{2}} = 1$.

We want to find the elements generated by S_* that are in the center of $\mathbb{Z}G$.

According to Lemma 2.1, from now on, we will consider $r = t^{(q-1)/p^n}$. We have that the map η defined in the proof of Proposition 3.1 can be written as $\eta = f^{\frac{q-1}{p^n}}$. To simplify, we define $l := (q-1)/p^n$. So, we have that $\eta(w_i) = f^l(w_i) = w_{i+l}$. For $1 \le i \le \frac{l}{2} - 1$ we will define the elements $z_i = w_i w_{i+\frac{l}{2}} w_{i+l} \dots w_{i+(p^n-1)\frac{l}{2}}$. In the proof of the next theorem we will prove that all the z_i's are central.

Now, we define the following set:

$$S_\gamma = \{z_1, \dots, z_{\frac{l}{2}-1}\}.$$

We have that the set S_γ is linearly independent, given that S_* is linearly independent.

Theorem 3.3. *With the definitions above (in the cases where $m = 1$), we have* $\langle S_\gamma \rangle = W_2$.

Proof. Let us start by proving that $S_\gamma \subset W_2$. We have:

$$\eta(w_i) = w_{i+l};$$
$$\eta(w_{i+l}) = w_{i+2l};$$
$$\vdots$$
$$\eta\left(w_{i+\frac{(p^n-3)}{2}l}\right) = w_{i+\frac{(p^n-1)}{2}l};$$
$$\eta\left(w_{i+\frac{(p^n-1)}{2}l}\right) = w_{i+\frac{(p^n+1)}{2}l}.$$

Since $2d = p^n l$, then $i + \frac{(p^n+1)}{2} l = i + d + \frac{l}{2}$, and since $w_i = w_{i+d}$, we have (following the equations above):

$$\eta\left(w_{i+\frac{(p^n-1)}{2}l}\right) = w_{i+\frac{l}{2}}.$$

And since $\eta(w_i) = w_{i+l}$, we have:

$$\eta(w_{i+\frac{l}{2}}) = w_{i+\frac{3l}{2}};$$
$$\eta(w_{i+\frac{3l}{2}}) = w_{i+\frac{5l}{2}};$$
$$\vdots$$
$$\eta\left(w_{i+\frac{(p^n-4)l}{2}}\right) = w_{i+\frac{(p^n-2)l}{2}};$$
$$\eta\left(w_{i+\frac{(p^n-2)l}{2}}\right) = w_{i+\frac{p^n l}{2}} = w_{i+d} = w_i.$$

From that, we have:

$$\eta(z_i) = \eta\left(w_i w_{i+\frac{l}{2}} w_{i+l} w_{i+\frac{3l}{2}} \dots w_{i+\frac{(p^n-1)l}{2}}\right) = \\ = w_{i+l} w_{i+\frac{3l}{2}} \dots w_{i+\frac{(p^n-1)l}{2}} w_i w_{i+\frac{l}{2}} = z_i.$$

And it's proven that $\langle S_\gamma \rangle \subset W_2$. We prove now the other inclusion.

Suppose $u \in W_2$. From proposition 3.1, we have that u is symmetric and, therefore, we can write $u = w_1^{r_1} \dots w_{d-1}^{r_{d-1}}$, for certain integers r_i, since S_* generates the group of symmetric units of $\mathbb{Z}C_q$. We have:

$$\eta(u) = \eta(w_1)^{r_1} \dots \eta(w_{d-1})^{r_{d-1}} = w_{1+l}^{r_1} \dots w_{d-1}^{r_{d-l-1}} w_0^{r_{d-l}} w_1^{r_{d-l+1}} \dots w_{l-1}^{r_{d-1}},$$

since for $i \geq d-l$ we have $i+l \geq d$, we substitute $i+l$ by $i+l-d$ in the index of the w's.

By proposition 3.2 we have that $w_0 = w_1^{-1} \dots w_{d-1}^{-1}$, so we have:

$$\eta(u) = w_1^{r_{d-l+1}-r_{d-l}} \dots w_{l-1}^{r_{d-1}-r_{d-l}} w_l^{-r_{d-l}} \dots w_{d-1}^{r_{d-l-1}-r_{d-l}}.$$

Since u is central, we have $u = \eta(u)$. Furthermore, S_* is a linearly independent set, then the exponents of the w_i's in u are the same as in $\eta(u)$. In particular, we have that $r_l = -r_{d-l}, r_{2l} = r_l - r_{d-l} = -2r_{d-l}$. By induction, we get that for every integer $j \geq 1, r_{jl} = -jr_{d-l}$ (since $r_{jl} = r_{(j-1)l} - r_{d-l}$).

We also have that $r_{\frac{l}{2}} = r_{d-\frac{l}{2}} - r_{d-l}$. Since $d - \frac{l}{2} = \frac{p^n-1}{2} l$ and $r_{jl} = -jr_{d-l}$, we have that $r_{l/2} = -\frac{p^n-1}{2} r_{d-l} - r_{d-l} = -\frac{p^n+1}{2} r_{d-l}$. Furthermore, $r_{\frac{3l}{2}} = r_{\frac{l}{2}} - r_{d-l} = -\frac{p^n+3}{2} r_{d-l}$. By induction we have that, if m is odd, then $r_{\frac{ml}{2}} = r_{\frac{(m-2)l}{2}} - r_{d-l} = -\frac{p^n+m}{2} r_{d-l}$.

Using the formula above for $m = p^n - 2$, we get $r_{m\frac{l}{2}} = -(p^n-1) r_{d-l}$, however, for this value of m, we have that $m\frac{l}{2} = d - l$. Therefore, we conclude that $r_{d-l} = -(p^n-1) r_{d-l}$, and we get that $r_{d-l} = 0$. So we can write:

$$\eta(u) = w_1^{r_{d-l+1}} w_2^{d-l+2} \dots w_{\frac{l}{2}-1}^{r_{d-\frac{l}{2}-1}} w_{\frac{l}{2}+1}^{r_{d-\frac{l}{2}+1}} \dots w_{l-1}^{r_{d-1}} w_{l+1}^{r_1} \dots w_{d-1}^{r_{d-l-1}}.$$

Comparing the exponents of the factors of u and $\eta(u)$, we get $r_i = r_{i+jl}$, for all $i, j \geq 1$ (such that the index makes sense). We also get that $r_i = r_{i+d-l} = r_{i+\frac{(p^n-2)l}{2}}$, and by the formula we concluded before, in this same paragraph, we have that $r_{i+\frac{(p^n-2)l}{2}} = r_{i+\frac{(p^n-4)l}{2}} = \dots = r_{i+\frac{l}{2}}$.

Then $r_i = r_{i+\frac{l}{2}} = r_{i+l} = \dots = r_{i+\frac{(p^n-1)l}{2}}$, and $u = z_1^{r_1} \dots z_{\frac{l}{2}-1}^{r_{\frac{l}{2}-1}}$, as we wanted. □

3.2. Basis for W_2 when $(p^n, q^m) = (3, 49)$

Now we will work with the case $(p^n, q^m) = (3, 49)$. In this case $n = 1$ and $m = 2$. The previous cases are essentially a repetition of what was done in [11]. From now on, the procedure is basically the same, but it will be done with two different types of units of $\mathbb{Z}C_{q^m}$, as we will describe below.

From [8], we have that, if $\phi(q^2) \leq 66$, then $\ker(\overline{\pi_1}) \times \langle S\rangle$ generates a complement for $\langle a\rangle$ in $U_1(\mathbb{Z}C_{q^2})$, where $\overline{\pi_1} : U_1(\mathbb{Z}C_{q^2}) \to U_1(\mathbb{Z}[\theta])$, θ is a q^2-primitive root of unit and $U_1(\mathbb{Z}[\theta])$ are units congruent to 1 modulo $\theta - 1$ (units of $\mathbb{Z}[\theta]$), S is the set of units $u_i = (1 + a^t + a^{2t} + ... + a^{(s-1)t})(1 + a^{t^i} + a^{2t^i} + ... + a^{(t-1)t^i}) - \frac{(ts-1)}{q^2}\widehat{a}$, where t generates the group of units of integers modulo q^2 and s its inverse, $1 \leq i \leq \phi(q^2)/2 - 1$.

Let us use the units u_i and set $r = t^{\frac{\phi(q^m)}{p^n}}$. This way, analogously to what was done in the other cases, we get the set S_0, consisting of elements $v_i = u_{i-1}^{-1}u_i$, for $1 \leq i \leq \phi(q^2)/2 - 1, v_1 = u_1$. We have that the elements v_i are written as

$$v_i = (1 + a^{t^i} + a^{t^{2i}} + ... + a^{(s-1)t^i})(1 + a^{t^i} + a^{2t^i} + ... + a^{(t-1)t^i}) - \frac{(ts-1)}{q^2}\widehat{a}.$$

We will now call $f : U_1(\mathbb{Z}C_{q^m}) \to U_1(\mathbb{Z}C_{q^m})$ the map that extends linearly $a \mapsto a^t$. Again we have that (like in the previous cases) $f(v_i) = v_{i+1}, f^{\phi(q^2)/2}(v_i) = v_{i+\phi(q^2)/2} = v_i^*$. Again, we know that there is only one w_i such that $v_i = a^{j_i}w_i$, and w_i is symmetric. We define the set $S_* = \{w_1, ..., w_{\phi(q^2)/2-1}\}$ of symmetric linearly independent units. We have that $f(w_i) = w_{i+1}$ and $f^{\phi(q^2)/2}(w_i) = w_i$. We have the following lemma, analogous to Lemma 3.2:

Lemma 3.4. *With the definitions above,* $w_0...w_{\frac{\phi(q^2)}{2}-1} = 1$.

Proof. We will use the properties of f. Setting $u = w_0...w_{\phi(q^2)/2-1}$, we have:

$$f(u) = w_0...w_{\phi(q^2)/2-1} = u.$$

Furthermore:

$$N_{\mathbb{Q}(\theta)|\mathbb{Q}}(\overline{\pi_1}(u)) = \prod_{\sigma \in Gal(\mathbb{Q}(\theta)|\mathbb{Q})} \sigma(\overline{\pi_1}(u)) = \prod_{j=1}^{\phi(q^2)} \overline{\pi_1}(f^j(u)) =$$
$$= \prod_{j=1}^{\phi(q^2)} \overline{\pi_1}(u) = (\overline{\pi_1}(u))^{\phi(q^2)} = \overline{\pi_1}(u^{\phi(q^2)}),$$

where $N_{\mathbb{Q}(\theta)|\mathbb{Q}}$ denotes the field norm.

Since u is an unit with augmentation 1, we get $N_{\mathbb{Q}(\theta)|\mathbb{Q}}(\overline{\pi_1}(u)) = 1$.

However, from [8], we know that $u^j \notin \ker(\overline{\pi_1})$ if $u \neq 1$, for all $j \geq 1$ (since $\langle S\rangle \cap \ker(\overline{\pi_1})$ is trivial).

And we get $u = 1$, as desired. □

So, we define $d := \phi(q^2)/2, l = \phi(q^2)/p^n$, and we define the set $S_\gamma = \{z_1, ..., z_{l/2-1}\}$, where $z_i = w_i w_{i+l/2} w_{i+l} ... w_{i+(p^n-1)l/2}$. As we did in the previous cases, we have that $S_\gamma \subset W_2$. In this case we do not have equality, because we still need to consider units in $\ker(\overline{\pi_1})$. However, the units z_i that we just found form a basis for the group of central units of $\mathbb{Z}G$ that are in $\langle S_*\rangle$, analogously to what we did in the previous cases. And we know that $\ker(\overline{\pi_1}) \times \langle S_*\rangle$ generates a complement for $\langle a\rangle$ in the group $U_1(\mathbb{Z}C_{q^2})$.

Now we consider the map $f_1 : U_1(\mathbb{Z}C_q) \to U(\mathbb{Z}_q C_q)$ that sends the coefficients to theirs classes modulo q. From now on we will consider q a regular prime (remember $q = 7$ is regular). So, by Kümmer's Lemma, we have that $\ker(f_1) = \{u^q | u \in U_1(\mathbb{Z}C_q)\}$ (see [13]). Let us denote $h = a^q$, so that h is a generator of a group isomorphic to C_q. Thus, utilizing the symmetric units of $\mathbb{Z}\langle h\rangle\mathbb{Z}C_q$ obtained from the Hoechsmann units (analogous to the w_i units we had in the previous cases), that we will denote now by $\tilde{w}_i$, we have that $\ker(f_1) = \langle \tilde{w}_i{}^q\rangle_{i=1,...,(q-3)/2}$.

To simplify notation, we will denote $\mu_i = \tilde{w}_i{}^q$. So, we have that the units μ_i are of the form $1 + qx_i = 1 + q(c_{0,i} + c_{1,i}h + ...c_{q-1,i}h^{q-1})$, where $c_{j,k}$ are integers.

Now we define the units $\rho_i = 1 + c_{0,i}\widehat{h} + c_{1,i}a\widehat{h} + c_{2,i}a^2\widehat{h} + \ldots + c_{q-1,i}a^{q-1}\widehat{h}$. From [8], we have that $\ker(\overline{\pi_1})$ is generated by the units $\rho_i, i = 1, \ldots, (q-3)/2$ that are linearly independent and symmetric. Thus, we conclude that the units in $\ker(\overline{\pi_1})$ are precisely all the elements generated by units of the following type:

$$1 + (d_0 + d_1 a + \ldots + d_{q-1}a^{q-1})\widehat{h},$$

where $1 + d_0 + d_1 h + \ldots + d_{q-1}h^{q-1}$ is generated by the μ_i's.

Similarly to what we did previously, we define the units $\tilde{z}_i$, for $1 \leq i \leq \frac{(q-1)}{2p} - 1$, given by

$$\tilde{z}_i = \tilde{w}_i \tilde{w}_{i+\frac{(q-1)}{2p}} \tilde{w}_{i+\frac{(q-1)}{p}} \ldots \tilde{w}_{i+(p-1)\frac{(q-1)}{2p}}.$$

Remark 3.5. *Here, $(q-1)/2p$ plays the same role that l played in the previous cases.*

Remark 3.6. *In the case $q = 7, p = 3$ that we are studying now, the set of the $\tilde{z}_i$'s is empty, since $\frac{(q-1)}{2p} - 1 = 0$. This happens due to the fact that the rank of the group of central units of $\mathbb{Z}C_{3,7}$ is zero (see the formula for the rank in [10]). But we will continue with the argument anyway, so that the method will be as general as possible, allowing one to find generators of a group o finite index in $Z(U_1(\mathbb{Z}G))$ in the future.*

With this procedure, we have that the units $\tilde{z}_i$ form a basis for the group of units of $\mathbb{Z}C_q$ that are in $Z(\mathbb{Z}C_{p,q})$ (here $C_{p,q}$ is seen as a subgroup of G) and, consequently, in $Z(\mathbb{Z}G)$.

Therefore, we conclude that a basis for the group of units in $\ker(\overline{\pi_1})$ that are in $Z(\mathbb{Z}G)$ is formed by the units below:

$$\zeta_i = 1 + (d_{0,i} + d_{1,i}a + \ldots + d_{q-1,i}a^{q-1})\widehat{h},$$

where $\tilde{z}_i{}^q = 1 + d_{0,i} + d_{1,i}h + \ldots + d_{q-1,i}h^{q-1}$.

With a procedure analogous to that we did before, we have that the units z_i and ζ_j form a basis for W_2.

Remark 3.7. *In our case $q = 7, p = 3$, we only have the units z_i, for the reason mentioned above.*

4. Basis for W_1

We start by proving the following proposition, analogous to Proposition 2.1 from [11]:

Proposition 4.1. *With the same notations of Corollary 2.4, we have that $\ker(\pi_{q^m})$ has only symmetric units.*

Proof. Let $u \in \ker(\pi_{q^m})$. We have that there is a power of b, say, b^j, and w symmetric unit such that $u = b^j w$.

Then $1 = \pi_{q^m}(b^j w) = \pi_{q^m}(b^j)\pi_{q^m}(w) = b^j \pi_{q^m}(w)$, so we get that $\pi_{q^m}(w) = b^{-j}$, but this is symmetric, so $b^{-j} = 1$ and, therefore, $u = w$. □

We still need to evaluate W_1 in the cases $(p^o, q^m) = (9, 19)$ or $(9, 37)$ (in these cases we have $m = 1$). By Corollary 3.5.6 of [15], we have that $\mathbb{Z}_q C_{p^o} \cong (\mathbb{Z}_q)^{p^o}$ (since r is a primitive root of unity of order p^o in $\mathbb{Z}C_q$).

We need to evaluate the kernel of $\pi_{q^m}(= \pi_q)$. By the above, we have that the exponent of $\mathbb{Z}_q C_{p^o}$ is $q-1$. By [8], we have that the set

$$S = \{s_1 = -1 + b - b^2 + b^3 + b^6 - b^7 + b^8, s_2 = 1 - b + b^2 + b^7 - b^8\}$$

generates $U^*(\mathbb{Z}C_9)$, the group of symmetric units, where b is a generator of C_9. Thus, we just have to evaluate all pairs $s_1^i s_2^j$, with $0 \le i, j \le q-2$, for the possible values of q (in our case, 19 or 37), and so we will have generator of $\ker(\pi_q)$ for each case. We used GAP, with the following code:

```
G := CyclicGroup(IsPermGroup,9);
R := GroupRing(GF(19),G);
b := R.1;

s1 := −b ^ 0 + b − b^2 + b^3 + b^6 − b^7 + b^8;
s2 := b^0 − b + b^2 + b^7 − b^8;

r := b^0;
s := b^0;

for i in [0.17] do
    s := b^0;
    for j in [0.17] do
        if r * s = b^0 then
            Print("i =", i," ; j =", j," \n");
        fi;
        s: = s2 * s;
    od;
    r: = s1 * r;
od;
```

In the code above we did the case $q = 19$ but, changing 19 for 37 and 17 for 35 in the code, we obtain the case $q = 37$.

Case $q = 19$:

We got the following outcome:

i = 0; j = 0
i = 6; j = 6
i = 12; j = 12

It means that the algorithm found the following elements in the kernel: $s_1^0 s_2^0, s_1^6 s_2^6, s_1^{12} s_2^{12}$. Thus, in the case $q = 19$, the kernel is generated by $\{s_1^6 s_2^6, s_1^{18}\}$.

Case $q = 37$:

We got the following outcome:
i = 0; j = 0
i = 12; j = 12
i = 24; j = 24

It means that the algorithm found the following elements in the kernel: $s_1^0 s_2^0, s_1^{12} s_2^{12}, s_1^{24} s_2^{24}$. Thus, in the case $q = 37$, the kernel is generated by $\{s_1^{12} s_2^{12}, s_1^{36}\}$.
And so we finish this section.

5. Some metacyclic p-groups

Throughout this section, we consider p an odd prime number. First, we need the following theorem:

Theorem 5.1. [12] *If p is a regular odd prime number, A is a finite abelian p-group, and u is a symmetric unit with augmentation 1 in $\mathbb{Z}A$ such that $u \equiv 1 (mod\, p)$, then there is a symmetric unit*

v with augmentation 1 such that $u = \eta(v)v^{-p}$, where $\eta : \mathbb{Z}A \to \mathbb{Z}A$ is an endomorphism that extends linearly $g \mapsto g^p$, for all $g \in A$.

In this chapter, we will consider the groups $G_n = \langle a, b | a^{p^2} = b^{p^n} = 1, bab^{-1} = a^{p+1} \rangle$ (this can be seen as a semidirect product $C_{p^2} \rtimes C_{p^n}$).

The center of G_n is $\{1, a^p, a^{2p}, ..., a^{(p-1)p}\}$. the conjugacy classes of non-central elements are listed below:

(1) the class of a^i, for $p \nmid i$ is $\{a^i, a^{i+p}, a^{i+2p}, ..., a^{i+(p-1)p}\}$, and its sum is $\gamma_i := \widehat{Z(G_n)}a^i$.

(2) the class of $a^s b^i$ is $\{a^s b^i, a^{p+s}b^i, a^{2p+s}b^i, ..., a^{(p-1)p+s}b^i\}$, and its sum is $\Gamma_{i,s} := \widehat{Z(G_n)}a^s b^i$.

We also have that $G' = Z(G_n) = \langle a^p \rangle$. So, we have that G_n satisfies the hypothesis of Corollary 1.5.

Now we define the following morphism:

$$\pi_{p,n} : U_1(\mathbb{Z}(C_p \times C_{p^n})) \to U_1(\mathbb{Z}_p(C_p \times C_{p^n})),$$

that takes the coefficients to their classes modulo p.

We have the following theorem:

Theorem 5.2. *With the notations above, we have that*

$$Z(U_1(\mathbb{Z}G_n)) = W_1 \times W_2,$$

where

$$W_1 = \left\langle 1 + \frac{(w-1)\widehat{Z(G_n)}}{p} | w \in \ker(\pi_{p,n}) \right\rangle \cong \ker(\pi_{p,n})$$
$$W_2 = U_1(\mathbb{Z}Z(G_n)) \cong U_1(\mathbb{Z}C_p)$$

Remark 5.3. *Here, we are considering the domain of $\pi_{p,n}$ as $U_1(\mathbb{Z}G_n/G'_n) = U_1(\mathbb{Z}G_n/\langle a^p \rangle)$, and we can take w as any representative in the group ring $\mathbb{Z}G_n$.*

Proof. It follows immediately from Corollary 1.5, and we have that the image of w_i in $U_1(\mathbb{Z}G_n/G'_n)$ is what defines u_i (remember that $Z(G_n) = G'_n$). □

By Theorem 5.1 we get that the kernel of $\pi_{p,1}$ when p is a regular prime is precisely the set $\{u^p | u \in U_1(\mathbb{Z}C_p \times C_p)\}$. So, using the results of [7] and the following theorem by Hoechsmann, we get explicitly the group of central units of G_n for regular primes p that are less than 68.

Theorem 5.4. [13] *Let p a regular prime. So, the units of $\mathbb{Z}(C_p \times \cdots \times C_p) = \mathbb{Z}G$ are all generated by the units of subrings of the type $\mathbb{Z}H$, where H is a subgroup of G of order p.*

By Theorem 5.1 we get that the kernel of $\pi_{p,1}$ when p is a regular prime is precisely the set $\{u^p | u \in U_1(\mathbb{Z}C_p \times C_p)\}$. So, using the results of [7] and by Theorem 5.1, we get explicitly the group of central units of G_n for regular primes p that are less than 68. Let us give an example:

We consider $n = 1$, $p = 5$. We know that $Z(G_n) = \langle a^p \rangle \cong C_p$. From [7], we have that $u(b) := b^4 + b - 1$ generates a complement for C_5 in $U_1\mathbb{Z}C_5$. We have:

$$W_2 = \langle a^p \rangle \times \langle (a^p)^4 + (a^p) - 1 \rangle = \langle a^p \rangle \times \langle u(a^p) \rangle$$

Set $V = \{u(a)^p, u(ab)^p, u(ab^2)^p, ..., u(ab^{p-1})^p, u(b)^p\}$. By Theorems 5.4 and 5.1, we have that

$$W_1 = \left\langle 1 + \frac{(w-1)\widehat{a^p}}{p} | w \in V \right\rangle$$

6. Other metabelian p-Groups

In this chapter, we are going to study groups of type $(C_p)^n \rtimes C_p$, where $(C_p)^n$ is the direct product of n copies of C_p.

In the case $n = 2$, we get a very well known group:

$$G = \langle a, b, c | a^p = b^p = c^p = 1, ab = ba, ac = ca, cbc^{-1}b^{-1} = a \rangle$$

It can also be seen as the following matrix group:

$$H = \left\langle \begin{bmatrix} 1 & k & i \\ 0 & 1 & j \\ 0 & 0 & 1 \end{bmatrix} | i, j, k \in \mathbb{Z}_p \right\rangle$$

This is known as the Heisenberg group.

The isomorphism between G and H is given by

$$(a^i, b^j, c^k) \mapsto \begin{bmatrix} 1 & k & i \\ 0 & 1 & j \\ 0 & 0 & 1 \end{bmatrix}.$$

Back to the general case, we will define the following groups, for $n \geq 2$:

$$H_n = \langle a_1, ..., a_n, b | a_1^p = ... = a_n^p = b^p = 1; a_i a_j = a_j a_i, \forall i, j \geq 1; \\ a_1 b = b a_1; b a_k b^{-1} a_k^{-1} = a_1, \forall k \geq 2 \rangle$$

Analogous to what happens in the case $n = 2$, we have that $Z(H_n) = \langle a_1 \rangle = H_n'$, and the conjugacy class of an element of type $g = a_2^{i_2} ... a_n^{i_n} b^j$ is the set $\{g, a_1 g, a_1^2 g, ..., a_1^{p-1} g\}$.

Thus, the groups H_n satisfy the hypothesis of Corollary 1.5.

Let us define the map $\tilde{\pi}_{p,n} : U_1(\mathbb{Z}(C_p)^n) \to U_1(\mathbb{Z}_p(C_p)^n)$, that takes the coefficients to their classes modulo p. We have the following:

Theorem 6.1. *With the same notations used above, we have that*

$$Z(U_1(\mathbb{Z}H_n)) = W_1 \times W_2,$$

where:

$$W_1 = \left\langle 1 + \frac{(w-1)\widehat{\langle a_1 \rangle}}{p} | w \in \ker(\tilde{\pi}_{p,n}) \right\rangle \cong \ker(\tilde{\pi}_{p,n})$$
$$W_2 = U_1(\mathbb{Z}Z(H_n)) \cong U_1(\mathbb{Z}C_p)$$

Remark 6.2. *Here we are considering the domain of $\tilde{\pi}_{p,n}$ as $U_1(\mathbb{Z}H_n/H_n')$, and we could take w as any representative of it in the group ring $\mathbb{Z}H_n$.*

Proof. It follows immediately from Corollary 1.5, analogous to the result of the previous section.

We also give an example of how to apply this to a concrete case:

With $p = 5$ and $n = 2$, we take $u(b) = b^4 + b - 1$. So, we have:

$$W_2 = \langle a_1 \rangle \times \langle u(a_1) \rangle,$$

and setting $V = \{u(a_1)^p, u(a_1b)^p, u(a_1b^2)^p, ..., u(a_1b^{p-1})^p, u(b)^p\}$, we have by Theorem 5.1:

$$W_1 = \left\langle 1 + \frac{(w-1)\widehat{a_1^p}}{p} | w \in V \right\rangle$$

With this example we conclude this section.

7. Some generalized dihedral groups

We will consider H a finite abelian group such that $|H|$ is odd, and we define the following groups:

$$G_H := H \rtimes_\psi C_2,$$

where $C_2 = \langle g \rangle$ and the semidirect product is defined by the morphism ψ, given by:

$$x \in H \mapsto \psi(x) := gxg^{-1} = x^{-1}.$$

Remark 7.1. *We don't need $|H|$ to be odd to define such groups, but we need this to prove the theorem in this chapter. The groups of type G_H are called Generalized Dihedral groups.*

Remark 7.2. *In the case of H a cyclic group of odd order n, we have that G_H is the dihedral group D_{2n}, this case is covered in the Ph. D. thesis of Ferraz* [6]

Now, if $x \in H$, then $xgx^{-1} = x^2g$ and, since $|H|$ is odd, we have that $x \in H \mapsto x^2$ is surjective (over H), therefore $G'_H = H$.

Furthermore, we have that if $y \notin G'_H$, then the sum of the conjugacy class of y is $\gamma_y = \widehat{G'_H}y$.

So, we have satisfied the hypothesis of Corollary 1.5, and we have immediately the following theorem:

Theorem 7.3. *If G_H is the group defined above, where H is a finite abelian group with $|H|$ odd, then $Z(U_1(\mathbb{Z}G_H))$ is the group of symmetric units $U_1^*(\mathbb{Z}H)$.*

Proof. By Corollary 1.5, we have $Z(U_1(\mathbb{Z}G_H)) = W_1 \times W_2$, where W_1 is isomorphic to a subgroup of $U(\mathbb{Z}G_H/G'_H) \cong U(\mathbb{Z}C_2)$, which is trivial. Thus, the only non-trivial factor is W_2.

But W_2 is formed by the units of $U_1(\mathbb{Z}H)$ that commute with G_H. Since $gxg^{-1} = x^{-1}$, we have that $u \in W_2$ if, and only if u is a symmetric unit in $Z(U_1(\mathbb{Z}H))$, and we have our result proven. □

Funding

The first author was partially supported by CNPq.

ORCID

Vitor Araujo Garcia http://orcid.org/0000-0001-6150-5633

References

[1] Aleev, R. Z. (1994). Higman's central unit theorem, units of integral group rings and Fibonacci numbers. *Int. J. Algebra Comput.* 04(03):309–358. DOI: 10.1142/S0218196794000038.
[2] Aleev, R. Z., Panina, Z. (2000). The units of cyclic groups of order 7 and 9. *Rus. Math.* 43:80–83.

[3] Aleev, R. Z., Sokolov, V. V. (2009). On central unit groups of integral group rings of alternating groups. *Proc. Steklov Inst. Math.* 267(S1):S1–S9. DOI: 10.1134/S0081543809070013.
[4] Borevich, Z. I., Shafarevich, I. R. (1966). *Number Theory, Pure and Applied Mathematics*. Cambridge, MA: Academic Press.
[5] Cohn, J. A., Livingstone, D. (1965). On the structure of group algebras. *Can. J. Math.* 17:583–593. DOI: 10.4153/CJM-1965-058-2.
[6] Ferraz, R. A. (2002). *Subgrupos Livres e Unidades Centrais No Grupo de Unidades de Alguns Anéis de Grupos*. São Paulo: Universidade de São Paulo.
[7] Ferraz, R. A. (2009). Units of $\mathbb{Z}C_p$, *Groups, Rings and Group Rings, Contemporary Mathematics*, Vol. 499. Providence, RI: American Mathematical Society, pp. 107–119.
[8] Ferraz, R. A., Kitani, P. M. (2015). Units of $\mathbb{Z}C_{p^n}$. *Commun. Algebra* 43:4936–4950.
[9] Ferraz, R. A., Marcuz, R. (2016). Units of $\mathbb{Z}(C_p \times C_2)$ and $\mathbb{Z}(C_p \times C_2 \times C_2)$. *Commun. Algebra* 44(2): 851–872.
[10] Ferraz, R. A., Simón, J. J. (2008). Central units in metacyclic integral group rings. *Commun. Algebra* 36(10): 3708–3722. DOI: 10.1080/00927870802158028.
[11] Ferraz, R. A., Simón, J. J. (2016). Central units in $\mathbb{Z}C_{p,q}$. *Commun. Algebra* 44(5):2264–2275.
[12] Hoechsmann, K. (1989). Généralization d'un lemme de Kummer. *Can. Math. Bull.* 32(4):486–489.
[13] Hoechsmann, K., Sehgal, S. K. (1986). Units in regular elementary abelian group rings. *Arch. Math.* 47(5): 413–417. DOI: 10.1007/BF01189981.
[14] Jespers, E., Olteanu, G., del Río, Á., Gelder, I. V. (2013). Group rings of finite strongly monomial groups: Central units and primitive idempotents. *J. Algebra* 387:99–116. DOI: 10.1016/j.jalgebra.2013.04.020.
[15] Polcino Milies, C., Sehgal, S. K. (2002). *An Introduction to Group Rings*. Amsterdam: Kluwer Academic Publishers.
[16] Sehgal, S. K. (1993). *Units in Integral Group Rings*. London: Longman Scientific & Technical.