Unidades Centrais em Anéis de Grupo

Vitor Araujo Garcia

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Doutor em Ciências

Programa: Matemática

Orientador: Prof. Dr. Raul Antonio Ferraz

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES e do CNPq

São Paulo, fevereiro de 2020

Unidades Centrais em Alguns Anéis de Grupo

Esta versão da tese contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 20/10/2020. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Raul Antonio Ferraz (orientador) - IME-USP
- Prof. Dr. Francisco Cesar Polcino Milies - IME-USP
- Prof. Dr. Antonio Paques - UFRGS
- Prof.ª Dr.ª Patrícia Massae Kitani - UTFPR
- Prof.ª Dr.ª Edite Taufer - UFRGS

Resumo

Garcia, V. A. **Unidades Centrais em Alguns Anéis de Grupo**. 2020. Tese (Doutorado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2020.
Este trabalho tem como objetivo estudar a estrutura do grupo de unidades centrais de certos anéis de grupo integrais, utilizando principalmente as ideias usadas em um artigo publicado em 2016 (Ferraz e Simón, 2016). Também estudamos o grupo de unidades dos anéis de grupo $\mathbb{Z}[\theta_p]A$, onde θ_p é uma raiz primitiva da unidade de ordem p e A é grupo abeliano finito, especialmente quando A tem expoente p.

Palavras-chave: unidades centrais, anel de grupo, anel de grupo integral, lema de Kümmer, primos regulares, grupos metabelianos, grupos abelianos elementares, grupos diedrais generalizados.

Abstract

Garcia, V. A. **Central Units in Group Rings**. 2018. Tese (Doutorado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2018.
The goal of this work is to study the group of central units of certain integral group rings, mainly using the ideas presented in an article from 2016 (Ferraz and Simón, 2016). We also studied the group of units of the group ring $\mathbb{Z}[\theta_p]A$, where θ_p is a primitive p-root of unity and A is a finite abelian group, specially when the exponent of A is p.

Keywords: central units, group ring, integral group ring, Kümmer's lemma, regular primes, metabelian groups, elementar abelian groups, generalized dihedral groups.

Sumário

Introdução

O problema de descrever o grupo de unidades (ou unidades centrais) de um anel de grupo integral, bem como encontrar uma base para a parte livre de tal grupo ou explicitar um subgrupo de índice finito tem sido muito estudado nas últimas décadas (veja, por exemplo, Ferraz e Simón, 2016; Ferraz, 2009; Low, 2008; Cohn e Livingstone, 1965; Ferraz e Kitani, 2015; Ferraz e Marcuz, 2016; Aleev, 1994; Aleev e Panina, 2000).

Muitas bases foram explicitadas com base no trabalho feito por Ferraz, R. A. em 2009, no qual foram explicitadas bases dos grupos de unidades dos anéis de grupo do tipo $\mathbb{Z}C_p$ para certos valores de p. Em 2016 Ferraz e Simón publicaram um artigo no qual eles aplicam o trabalho de 2009 para explicitar bases dos grupos de unidades centrais de anéis de grupo integrais sobre grupos não-abelianos. Neste último trabalho, os métodos usados podem ser aplicados para outros casos de grupos não-abelianos, como veremos no Capítulo 3.

Neste trabalho, apresentaremos alguns resultados que obtivemos na direção descrita no parágrafo anterior, utilizando principalmente a técnica introduzida por Ferraz, R. A. e Simón, J. J. (Ferraz e Simón, 2016).

Também mostraremos como calcular explicitamente um conjunto de geradores para o grupo de unidades dos anéis de grupo do tipo $\mathbb{Z}[\theta_p](C_p \times ... \times C_p)$, onde θ_p é uma raiz primitiva da unidade de ordem p.

Em (Hoechsmann e Sehgal, 1986), é provado que existe uma correspondência entre bases dos grupos de unidades de $Z(C_p \times ... \times C_p)$ e de ZC, onde C percorre todos os subgrupos cíclicos de $C_p \times ... \times C_p$, sempre que p for um número primo regular. Vamos utilizar este resultado para calcular explicitamente uma base para o grupo de unidades centrais de alguns anéis de grupo integrais não comutativos.

Para isso, precisaremos de algumas definições e resultados básicos que serão descritos no capítulo a seguir.

O trabalho está organizado da seguinte forma:

No Capítulo 1, apresentamos brevemente alguns dos conceitos que utilizaremos neste trabalho, incluindo definições e resultados básicos.

No Capítulo 2, vamos listar alguns dos resultados conhecidos e pré-requisitos que serão usados no capítulo seguinte.

No Capítulo 3, vamos enunciar e demonstrar os novos resultados que obtivemos para certos grupos não comutativos.

No Capítulo 4 apresentaremos novos resultados sobre o grupo de unidades de anéis de grupo do tipo $\mathbb{Z}[\theta_p]G$. Um dos resultados será importante para aplicação em exemplos calculados no capítulo anterior.

Logo em seguida, apresentamos a conclusão e alguns problemas para possível investigação futura.

Capítulo 1

Preliminares

1.1 Anéis de Grupo

Definição 1.1.1 (Anel de grupo). *Seja G um grupo e R um anel com* 1. *Definimos RG como sendo o conjunto de todas as somas formais do tipo*

$$\sum_{g\in G} a_g g,$$

onde $a_g \in R, g \in G$, e apenas uma quantidade finita dos a_g´s é diferente de zero.

O conjunto RG definido acima tem uma estrutura de anel com 1, *com as operações de adição e multiplicação definidas da seguinte maneira:*

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g.$$

Se $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g$:

$$\alpha\beta = \sum_{g,h\in G} a_g b_h gh.$$

Com estas operações, RG é chamado ***anel de grupo de*** *G* ***sobre*** *R.*

E definimos o suporte de α: $supp(\alpha) = \{g \in G : a_g \neq 0\}$.

Definição 1.1.2 (Centro de um Anel). *Seja R um anel qualquer. Chamaremos de* centro de R, *e denotaremos por $Z(R)$ o conjunto dos elementos de R que comutam com todos os elementos de R, isto é:*

$$Z(R) = \{r \in R : \forall l \in R, rl = lr\}$$

Chamaremos de unidades centrais de R as unidades que estão em $Z(R)$.

Definição 1.1.3 (Função de Aumento). *A função $\varepsilon : RG \to R$ definida por $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$ é chamada de* função de aumento, *e definimos $U_1(\mathbb{Z}G) = \{x \in U(\mathbb{Z}G) | \varepsilon(x) = 1\}$, e $Z(U_1(\mathbb{Z}G)) = U_1(\mathbb{Z}G) \cap Z(RG)$.*

Vamos usar a notação $U_1(\mathbb{Z}[\theta_p]G) = \{x \in U(\mathbb{Z}[\theta_p]G) | \varepsilon(x) \equiv 1 \ (mod\ \theta_p - 1)\}$, onde θ_p é raiz primitiva da unidade de ordem p.

Sabemos que a função de aumento ε definida acima é um morfismo de anéis e, portanto, esta função restrita às unidades de RG é um morfismo de grupos, com o domínio sendo $U(RG)$, o

contradomínio sendo $U(R)$ e o núcleo sendo $U_1(RG)$. Além disso, é trivial que qualquer unidade de RG é dada por um elemento de $U_1(RG)$ multiplicada por um elemento de $U(R)$. Sendo assim, para conhecer as unidades (ou as unidades centrais) de RG basta conhecer as unidades de aumento 1.

Um fato trivial a respeito de $Z(U_1(RG))$ (respectivamente $(U_1(RG))$) é que este conjunto contém $Z(G)$ (respectivamente, G). A seguir nos concentraremos principalmente no caso em que $R = \mathbb{Z}$.

Vamos utilizar o seguinte resultado:

Teorema 1.1.4 (Aleev, 1994). *Com as notações acima, temos que $Z(U_1(\mathbb{Z}G)) \cong \pm Z(G) \times A_G$, onde A_G é um grupo abeliano livre e de posto finito.*

Sabemos que este posto pode ser calculado dado G: sejam e o expoente de G, $C_g = \{hgh^{-1} | h \in G\}$, $E_g = \bigcup_{(j,e)=1} C_{g^j}$, $D_g = C_g \cup C_{g^{-1}}$, então o número de conjuntos do tipo E_g será denotado por n_e, e o número de conjuntos do tipo D_g será denotado por n_d. Então o posto de A_G é dado por $n_d - n_e$ (a demonstração deste fato se encontra em [Ferraz, 2004]).

Definição 1.1.5 (Grupo de Unidades Simétricas). *Seja $u = \sum_{g \in G} a_g g$ unidade de RG. Dizemos que u é simétrica se $a_g = a_{g^{-1}}$ para todo $g \in G$, e denotamos o grupo de todas as unidades simétricas por $U_*(RG)$ (tais unidades formam um grupo).*

Vamos chamar de ΔG o conjunto dos elementos de RG que estão no núcleo de ε. Temos a seguinte proposição:

Proposição 1.1.6 (Polcino e Sehgal 2002, Proposição 8.3.5). *Se G é grupo abeliano de ordem ímpar, então $U_1(\mathbb{Z}G) \cong G \times U_*(\mathbb{Z}G)$.*

Também vamos precisar do seguinte teorema:

Teorema 1.1.7. *(Maschke) Seja G um grupo. Então o anel de grupo RG é semissimples se, e somente se, valem as seguintes afirmações:*

(i) R é anel semissimples.

(ii) G é finito.

(iii) $|G|$ é invertível em R.

A prova do teorema acima pode ser encontrada em (Polcino e Sehgal, 2002), no teorema 3.4.7.

O conjunto de idempotentes centrais primitivos de $\mathbb{Q}G$ é conhecido quando, por exemplo, G é um grupo abeliano finito. Neste caso, vamos descrever agora quais são esses idempotentes, com base no artigo (Jespers, Leal e Paques, 2003):

Neste caso, os idempotentes são todos os elementos do tipo $\varepsilon(G, N)$, onde N é subgrupo de G tal que G/N é cíclico, e a função ε é definida da seguinte forma:

$$\varepsilon(G, N) = \prod_{\overline{M} \in \mathcal{M}(G/N)} \left(\frac{1}{|N|} \widehat{N} - \frac{1}{|M|} \widehat{M} \right), \text{ se } N \neq G$$

$$\varepsilon(G, G) = \frac{1}{|G|} \widehat{G},$$

onde $\mathcal{M}(G, N)$ é conjunto dos subgrupos minimais de G/N e $\widehat{H} = \sum_{h \in H} h$.

1.2 Primos Regulares

Nesta seção vamos definir o que são primos regulares, enunciar o lema de Kümmer e um corolário que se obtém a partir dele. Aqui vamos fixar θ_p como sendo uma raiz primitiva da unidade de ordem p, $R := \mathbb{Z}[\theta_p]$ e $K := \mathbb{Q}[\theta_p]$.

Definição 1.2.1 (Ideal Fracionário)**.** *Dizemos que I é um ideal fracionário de R se I é um R-submódulo de K tal que existe $r \in R$ com $rI \subset R$. Dizemos que um ideal fracionário é principal se existe $k \in K$ tal que $I = Rk$, o submódulo gerado por k.*

Exemplo 1: qualquer R-submódulo I gerado por k, com $k \in K$ é um ideal fracionário principal de R, pois podemos escrever $k = a/b$, com $a, b \in R$.

Definimos o produto de ideais fracionários da seguinte forma: $IJ = \{a_1b_1 + ... + a_nb_n | a_i \in I, b_i \in J, n \in \mathbb{N}\}$, e este produto resulta em outro ideal fracionário. Assim, o ideal gerado por 1 (que é o próprio R) é um elemento neutro com esta multiplicação.

Temos o seguinte resultado clássico (ver, por exemplo, [Ash, 2003]):

Teorema 1.2.2. *O conjunto de ideais fracionários ($\neq (0)$) de R com a multiplicação definida acima é um grupo abeliano, com elemento identidade $e = R$.*

Vamos denotar o grupo de ideais fracionários (diferentes de (0)) por J, e o subgrupo formado apenas por ideais principais vamos denotar por L. Definimos o grupo de classes como sendo o quociente J/L. Quando este grupo é finito, chamamos a ordem dele de *número de classe*. E dizemos que p é *regular* quando p divide o número de classe correspondente.

É sabido que p é regular para todo primo menor que 100, com exceção de $37, 59$ e 67 (este fato pode ser verificado, por exemplo, a partir do Corolário na página 377 de [Borevich e Shafarevich, 1966]).

Temos também o importante lema, cuja demonstração pode ser encontrada, por exemplo, em [Borevich e Shafarevich, 1966], no capítulo 5:

Lema 1.2.3 (Kummer)**.** *Se p é um número primo regular, e u é unidade de R que é congruente módulo p a algum inteiro, então $u = v^p$, onde v é outra unidade de R.*

Temos que o morfismo natural $\mathbb{Z}C_p \to R$ tem núcleo gerado por $1 + ... + g^{p-1}$ (onde g é gerador do grupo cíclico C_p). Portanto, $U_1(\mathbb{Z}C_p)$ pode ser visto como subgrupo de R (Lema 15.1 de [Sehgal, 1993]), de onde temos o seguinte corolário:

Corolário 1.2.4. *Se p é um primo regular, então o núcleo do homomorfismo natural $U_1(\mathbb{Z}C_p) \to U(\mathbb{Z}_pC_p)$ é dado pelas unidades do tipo u^p, onde $u \in U_1(\mathbb{Z}C_p)$.*

O corolário acima é utilizado implicitamente, por exemplo, no artigo (Hoechsmann e Sehgal, 1986).

No Capítulo 4 vamos enunciar este corolário para domínios mais gerais.

1.3 Extensões p-Ciclotômicas de $\mathbb{Q}$

Nesta seção, vamos considerar p um primo ímpar.

Vamos denotar o anel de polinômios com coeficientes racionais de uma variável por $\mathbb{Q}[x]$. Neste anel, considere o polinômio $f(x) = x^p - 1$. Temos que este polinômio se decompõe em $\mathbb{Q}[x]$:

$$p(x) = (x-1)(1 + x + x^2 + ... + x^{p-1}),$$

e se decompõe em $\mathbb{C}[x]$:

$$p(x) = (x-1)(x - e^{\frac{(2\pi i)}{p}})(x - e^{\frac{2(2\pi i)}{p}})...(x - e^{\frac{(p-1)(2\pi i)}{p}}).$$

Vamos denotar:

$$\Phi_p(x) := 1 + x + x^2 + ... + x^{p-1}.$$

Se p é número primo, então $\Phi_p(x)$ é denominado o p-ésimo polinômio ciclotômico.

Pela decomposição de $p(x)$ em $\mathbb{C}[x]$ acima, temos que as raízes complexas de $\Phi(x)$ são precisamente as raízes não-triviais da unidade de ordem p.

Assim, denotando $\theta_p := e^{\frac{(2\pi i)}{p}}$, temos que todas as raízes de $\Phi(x)$ são da forma θ_p^n, para algum $1 \leq n \leq p-1$. Assim sendo, temos que o menor corpo que contém $\mathbb{Q}$ e θ_p, que denotaremos por $\mathbb{Q}(\theta_p)$, contém todas as raízes da unidade de ordem p, e é o menor corpo que contém $\mathbb{Q}$ que tem essa propriedade (ou seja, a extensão $\mathbb{Q}(\theta_p)|\mathbb{Q}$ é normal). Para detalhes sobre uma extensão normal ver, por exemplo, [Martin, 2010]).

Definição 1.3.1. *O corpo $\mathbb{Q}(\theta_p)$ definido acima é denominado extensão p-ciclotômica de $\mathbb{Q}$. E o anel $\mathbb{Z}[\theta_p]$ será denominado anel de inteiros p-ciclotômicos.*

Podemos definir automorfismos σ em $\mathbb{Q}(\theta_p)$, induzidos por $\theta_p \mapsto \theta_p^j$, para todo $j = 1, ..., p-1$. O conjunto de todos esses automorfismos é um grupo, com a operação de composição de funções.

O grupo de tais automorfismos será denotado por $Gal(\mathbb{Q}(\theta_p)/\mathbb{Q})$ (para ver como o grupo $Gal(L/K)$ é definido em outras extensões, ver, por exemplo, [Martin, 2010]).

Agora podemos definir o conceito de norma. Primeiro, precisamos do fato de que $\mathbb{Q}(\theta_p)|\mathbb{Q}$ é extensão algébrica e, portanto, $\mathbb{Q}(\theta_p)$ é espaço vetorial de dimensão finita sobre $\mathbb{Q}$. Assim, para todo $x \in \mathbb{Q}(\theta_p)$, definimos $m_x : \mathbb{Q}(\theta_p) \to \mathbb{Q}(\theta_p)$ como sendo $y \mapsto xy$. E temos a seguinte definição:

Definição 1.3.2. *A função $N_{\mathbb{Q}(\theta_p)|\mathbb{Q}} : \mathbb{Q}(\theta_p) \to \mathbb{Q}$, que será denominada norma, é dada por*

$$N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(x) = det(m_x)$$

No caso de a extensão ser p-ciclotômica, temos que:

$$N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(x) = \prod_{\sigma \in Gal(\mathbb{Q}(\theta_p)/\mathbb{Q})} \sigma(x).$$

Que esta função está bem definida (ou seja, que o contradomínio está mesmo correto) pode ser verificado, por exemplo, em (Martin, 2010). Além disso, temos que esta função tem a seguinte propriedade:

$$N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(\alpha\beta) = N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(\alpha) N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(\beta).$$

Assim, segue que se $\alpha \in U(\mathbb{Z}[\theta_p])$, então $N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(\alpha) = \pm 1$, pois ± 1 são os únicos inteiros invertíveis. Mais ainda, se $\alpha \equiv 1\ (mod\ (\theta_p - 1))$, então $N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(\alpha) = 1$.

Capítulo 2

Histórico com Alguns Resultados Conhecidos

Neste capítulo, vamos listar brevemente alguns anéis de grupo dos quais já conhecemos um pouco (ou totalmente) sobre a estrutura do grupo das unidades centrais, que foram relevantes para a construção dos novos resultados que obtivemos.

2.1 Grupos Cíclicos de Ordem Prima

No caso em que $G = C_p$, Raul Antonio Ferraz [Ferraz, 2009] descreveu explicitamente uma base para A_G, quando p é primo ímpar tal que vale a seguinte afirmação:

Seja θ uma raiz p-primitiva da unidade. O conjunto $S = \left\{1+\theta, 1+\theta+\theta^2, ..., 1+\theta+...+\theta^{\frac{p-3}{2}}, -\theta\right\}$ gera o grupo de unidades de $\mathbb{Z}[\theta]$

Tais primos serão chamados de *primos simples* (sabe-se que os primos menores ou iguais que 67 são todos simples [Washington, L. C., Teorema 8.2, páginas 145 e 352]). Nesse caso, denotando por t um gerador do grupo $U(\mathbb{Z}_p)$, s sua inversa módulo p, $k := (ts-1)/p$, g um gerador de C_p e $\hat{g} = 1 + g + ... + g^{p-1}$, definimos:

$$u_i := (1 + g^t + g^{2t} + ... + g^{t(s-1)})(1 + g^{t^i} + g^{2t^i} + ... + g^{(t-1)t^i}) - k\hat{g}.$$

No artigo, Ferraz provou o seguinte teorema:

Teorema 2.1.1. *Seja p um primo simples, e seja A_{C_p} conforme o Teorema 1.1.4, então o conjunto*

$$S_0 = \left\{u_1, ..., u_{\frac{p-3}{2}}\right\}$$

é conjunto de geradores independentes do grupo A_{C_p}.

No artigo citado, o autor utiliza resultados conhecidos sobre o grupo de unidades de $\mathbb{Z}[\theta_p]$, onde θ_p é uma raiz primitiva de ordem p da unidade.

2.2 Grupos Cíclicos de Ordem p^n

Usando inclusive ideias e resultados do artigo citado na seção anterior, Ferraz e Kitani [Ferraz e Kitani, 2015] descreveram uma base para $\mathbb{Z}_{C_{p^n}}$, onde p é qualquer primo ímpar tal que $\varphi(p^n) \leq 67$.

Definindo θ como sendo uma raiz primitiva da unidade de ordem p^n, os autores definiram uma função $\overline{\pi_1} : U_1(\mathbb{Z}C_{p^n}) \to U_1(\mathbb{Z}[\theta])$, onde $U_1(\mathbb{Z}[\theta])$ é grupo de unidades congruentes a 1 módulo $\theta - 1$. Tomando S como sendo o conjunto das unidades do tipo $u_i = (1 + a^t + a^{2t} + ... + a^{(s-1)t})(1 + a^{t^i} + a^{2t^i} + ... + a^{(t-1)t^i}) - \frac{(ts-1)}{p^n}\widehat{a}$, com t um gerador do grupo de unidades dos inteiros módulo p^n e s sua inversa, $1 \leq i \leq \phi(p^n)/2 - 1$, $\langle a \rangle = C_{p^n}$.

Assim, provaram o seguinte teorema:

Teorema 2.2.1. *O grupo $ker(\overline{\pi_1}) \times \langle S \rangle$ gera um complemento para C_{p^n} em $U_1(\mathbb{Z}C_{p^n})$.*

Utilizando este teorema, foram capazes de calcular uma base para o grupo de unidades de $\mathbb{Z}C_{p^n}$ em todos os casos que $\varphi(p^n) \leq 67$.

Vamos utilizar os resultados deste artigo no capítulo seguinte, onde daremos uma descrição breve do resultado principal que eles obtiveram e como utilizar o resultado para calcular as unidades.

2.3 Grupos Metacíclicos

Para p e q primos simples menores que 68 tais que $p|q-1$, Ferraz e Simón descreveram uma base para $Z(U_1(\mathbb{Z}C_{p,q}))$ [Ferraz e Simón, 2016], onde

$$C_{p,q} = \left\langle a, b | a^q = b^p = 1, bab^{-1} = a^r \right\rangle,$$

onde r é qualquer número que não é congruente a 1 módulo p e tal que $r^p \equiv 1 (mod\ p)$.

Neste trabalho, primeiro foram definidos dois subgrupos, W_1 e W_2, da seguinte forma:

$$W_1 = \left\{ 1 + \frac{(\mu - 1)\hat{a}}{q} \right\},$$

onde $\mu \in Ker(\pi_q)$, e $\pi_q : U_1(\mathbb{Z}C_p) \to U_1(\mathbb{Z}_qC_p)$.

$$W_2 = Z(U_1(\mathbb{Z}C_{p,q})) \cap \mathbb{Z}C_q.$$

Neste artigo, provaram que W_1 e W_2 são livres e a base de W_1 foi calculada com ajuda do *software* GAP, tendo em vista os resultados de [Ferraz, 2009] e a descrição dos idempotentes primitivos de $\mathbb{Z}_qC_p$. E a base de W_2 foi calculada tendo em vista uma base de $U_1(\mathbb{Z}C_q)$ também descrita em [Ferraz, 2009] (para primos menores que 66).

Foi provado o seguinte teorema:

Teorema 2.3.1 (Ferraz e Simón, 2016)**.** *Com as notações acima, $Z(U_1(\mathbb{Z}C_{p,q}))$ é igual a $W_1 \times W_2$.*

A demonstração do teorema acima servirá de modelo para provarmos os resultados no capítulo seguinte.

2.4 Grupo Abeliano Elementar Finito

No caso de p ser um primo regular, Hoechsmann e Sehgal provaram o seguinte resultado:

Teorema 2.4.1 (Hoechsmann e Sehgal, 1986). *Seja p um primo regular. Então as unidades de $\mathbb{Z}(C_p \times ... \times C_p) = \mathbb{Z}G$ são todas geradas por unidades dos subanéis do tipo $\mathbb{Z}H$, onde H é subgrupo de G de ordem p.*

Notemos que este resultado junto com o resultado de Ferraz citado na primeira seção deste capítulo nos dá uma descrição completa de grupos abelianos elementares finitos, cuja ordem é a potência de um primo simples e regular.

Para provar este teorema, foi utilizado o corolário do lema de Kümmer e propriedades especiais de funções *exp* e *log* definidas em certos anéis de grupo sobre anéis de inteiros p-ádicos.

Utilizaremos este resultado também nos capítulos seguintes.

2.5 Grupos de Ordem Par

Marcuz e Ferraz publicaram um artigo (Ferraz e Marcuz, 2015) no qual são explicitadas bases para os grupos de unidades de certos anéis do tipo $\mathbb{Z}(C_p \times C_2)$, $\mathbb{Z}(C_p \times C_2 \times C_2)$ e $\mathbb{Z}(C_p \times C_2 \times C_2 \times C_2)$, onde p é um primo simples.

A título de exemplo, vamos descrever brevemente como são as unidades dos anéis de grupo do tipo $\mathbb{Z}(C_p \times C_2) \cong \mathbb{Z}C_{2p}$ que os autores encontraram. Primeiro, vamos fixar algumas notações: $C_p = \langle g \rangle$, $C_2 = \langle a \rangle$, $\rho : U(\mathbb{Z}C_p) \to U(Z_2C_p)$ morfismo natural.

Definimos as seguintes unidades:

$$w_i := (-1)^{\frac{p-3}{2}}(1 - g^{2^{i-1}} + g^{2(2^{i-1})} + ... + (-1)^{\frac{p-3}{2}} g^{\frac{p-3}{2}(2^{i-1})} +$$
$$+(-1)^{\frac{p-3}{2}} g^{\frac{p+3}{2}(2^{i-1})} + ... - g^{(p-2)2^{i-1}} + g^{(p-1)2^{i-1}}),$$

$$u_i(a) = (1 - \beta_i) + \beta_i a,$$

onde $\beta_1 = \frac{1-w_1^2 w_2^{-1}}{2}$, $\beta_i = \delta^{i-1}(\beta_1)$, $1 \leq i \leq \frac{p-3}{2}$, e $\delta : \mathbb{Z}C_p \to \mathbb{Z}C_p$ morfismo que estende $g^i \mapsto g^{2i}$.

Assim, provou-se o seguinte teorema:

Teorema 2.5.1. *Com as notações acima, se a ordem do elemento $\rho(w_1)$ é $2^{\frac{p-1}{2}} - 1$, então:*

$$U(\mathbb{Z}C_{2p}) = \langle -1 \rangle \times \langle g, a \rangle \times \left\langle \left\{ w_i : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \times \left\langle \left\{ u_i(a) : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle.$$

Mais ainda, o conjunto $\left\{ w_1, ..., w_{\frac{p-3}{2}}, u_1(a), ..., u_{\frac{p-3}{2}}(a) \right\}$ é multiplicativamente independente.

Com o teorema acima, os autores foram capazes de calcular, utilizando *softwares*, os casos $p = 5, 7, 11, 13, 19, 23, 29, 53, 59, 61$ e 67. Também mostraram a importância da hipótese do teorema acima, pois verificaram que o caso $p = 37$ não satisfaz a hipótese.

Capítulo 3

Anéis de Grupo Integrais Não-Comutativos

Neste capítulo vamos enunciar e demonstrar em detalhes os resultados novos que obtivemos sobre unidades centrais em anéis de grupos integrais não-comutativos, e aplicações em alguns exemplos. Nos basearemos, principalmente, em ideias do artigo [Ferraz e Simón, 2016].

3.1 Introdução

Vamos começar com a seguinte proposição:

Proposição 3.1.1. *Sejam R um anel e H um subgrupo normal de um grupo G. Se $|H|$ é invertível em R, denotamos $e_H = \frac{1}{|H|}\hat{H}$, e temos:*

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

onde $RGe_H \cong R(G/H)$ e $RG(1-e_H) = \Delta(G, H)$, sendo este último o núcleo do homomorfismo de anéis que estende a projeção $G \to G/H$.

Demonstração:
Ver Proposição 3.6.7 de [Polcino e Sehgal, 2002].

□

Com esta proposição em mente, podemos tomar H como sendo o grupo derivado G'. Neste caso, a primeira componente será formada apenas por elementos comutativos do anel de grupo RG. Sendo assim, temos o seguinte resultado:

Teorema 3.1.2. *Se G é um grupo finito qualquer, temos que*

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

Demonstração:
Primeiro, notemos que ambos os fatores estão em $Z(U_1(\mathbb{Q}G))$, visto que o fator da esquerda só tem elementos do centro de $\mathbb{Q}G$.

Da proposição anterior, temos que $(1 + \mathbb{Q}Ge_{G'}) \cap (1 + \mathbb{Q}G(1 - e_{G'})) = \{1\}$.

Para finalizar a demonstração, suponha que $u \in Z(U_1(\mathbb{Q}G))$. Então tomamos $u_1 = 1+(u-1)e_{G'}$, $u_2 = 1 + (u-1)(1-e_{G'})$. Vamos provar que u_1 e u_2 são unidades de $\mathbb{Q}G$. Para isso, suponha que $v \in Z(U_1(\mathbb{Q}G))$. Temos:

$$u_1(1+(v-1)e_{G'}) = (1+(u-1)e_{G'})(1+(v-1)e_{G'}) = 1+(v-1+u-1+(u-1)(v-1))e_{G'} =$$

$$= 1+(v-1+u-1-v-u+1+uv)e_{G'} = 1+(uv-1)e_{G'}.$$

Similarmente, temos:

$$u_2(1+(v-1)(1-e_{G'})) = 1+(uv-1)(1-e_{G'}).$$

Em particular, se tomarmos $v = u^{-1}$, temos que $u_1(1+(v-1)e_{G'}) = u_2(1+(v-1)(1-e_{G'})) = 1$ e, portanto, u_1 e u_2 são unidades. Vamos verificar que $u_1u_2 = u$:

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

$$= 1+(u-1)(1-e_{G'})+(u-1)e_{G'}+(u-1)^2e_{G'}(1-e_{G'}) = 1+u-1 = u,$$

visto que $e_{G'}$ é idempotente.

E isso prova o que queremos.

□

Observação 3.1.3. *na demonstração acima, temos que $u_1 = 1+(w-1)e_{G'}$, para todo $w \in \mathbb{Q}G$ cuja imagem pelo morfismo que estende a projeção $G \to G/G'$ é igual à imagem de u pelo mesmo morfismo.*

Agora vamos utilizar as ideias acima para descrever $Z(U_1(\mathbb{Z}G))$ para certos grupos G. Vamos fixar as seguintes notações: se $g \in G$, C_g representa a classe de conjugação de g, e γ_g representa a soma dos elementos de C_g.

Teorema 3.1.4. *Suponha que G é um grupo finito que satisfaz a seguinte propriedade: se $x \notin G'$, então $\gamma_x = \widehat{G'}x$. Então*

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

Demonstração:

Suponha que $u \in Z(U_1(\mathbb{Z}G))$. Como u é elemento central do anel de grupo, temos que u pode ser escrito da seguinte forma:

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

onde $\alpha_s \in \mathbb{Z}$, para todos s, $I_{G'}$ é um conjunto de representantes das classes de conjugação que cobrem G' e $I_{G-G'}$ um conjunto de representantes das classes de conjugação que não intersectam G' (podemos fazer isso pois G' é subgrupo normal). Vamos chamar de φ o homomorfismo de anéis que estende a projeção $G \to G/G'$. Temos:

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

Como $\varepsilon(\varphi(u)) = 1$ (ε sendo a função de aumento), temos que $\sum_{a \in I_{G'}} \alpha_a |C_a| \equiv 1 \ (mod\ |G'|)$. Portanto, podemos definir:

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

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

Para provarmos nosso resultado, vamos verificar que $w_1 w_2 = u$ (isso será suficiente, visto que w_1 é central e tem aumento 1 por construção).

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

Como $w_2 \in \mathbb{Z}G'$ tem aumento 1, podemos escrever:

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

O obtemos, assim, o desejado.

□

Consideremos $\mathbb{Z}G/G' \to \mathbb{Z}_{|G'|}G/G'$ morfismo que estende a projeção natural, e definimos $\pi_{|G'|}$ o morfismo induzido no grupo de unidades de aumento 1. Consideremos também o morfismo de anéis π induzido por $G \to G/G'$. Temos o seguinte corolário do teorema acima:

Corolário 3.1.5. *Com as mesmas hipóteses do teorema anterior e as definições do parágrafo anterior, temos:*

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

onde:

$$W_1 = \left\langle 1 + \frac{(\omega - 1)\widehat{G'}}{|G'|} \mid \pi(\omega) \in ker(\pi_{|G'|}) \right\rangle \cong ker(\pi_{|G'|}),$$

$$W_2 = (U_1(\mathbb{Z}G') \cap Z(\mathbb{Z}G)).$$

Observação 3.1.6. *está implícito no enunciado que $\pi(\omega)$ é unidade de aumento 1, pela definição do domínio de $\pi_{|G'|}$.*

Demonstração:

Pelo teorema anterior, basta verificar que $W := W_1 = ((1 + \mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G))$ e que isto é isomorfo a $ker(\pi_{|G'|})$.

Podemos tomar um elemento arbitrário da forma $1+(x-1)e_{G'}$, com $x \in \mathbb{Z}G$.

Também temos o seguinte: se $x, y \in \mathbb{Q}G$ então

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

Então temos que para $(1+(x-1)e_{G'}) \in U_1\mathbb{Z}G$, é necessário e suficiente que $\pi(x)$ seja unidade de $U_1(\mathbb{Z}G/G')$ tal que $(x-1)e_{G'} \in \mathbb{Z}G$ (isto é, tenha coeficientes inteiros), devido ao isomorfismo $\mathbb{Z}Ge_{G'} \cong \mathbb{Z}G/G'$, que é induzido por $ge_{G'} \mapsto \overline{g}$.

Também temos que, tomando $\{g_i,\ i \in I\}$ conjunto de representantes das coclasses em G/G', podemos supor que x é da forma:

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

Daí, temos que $\pi(x) \in ker(\pi_{|G'|})$, pois cada coeficiente de $x-1$ precisa ser divisível por $|G'|$.

Assim provamos que $W_1 = ((1+\mathbb{Z}Ge_{G'}) \cap U_1(\mathbb{Z}G))$. Também fica claro que $W_1 \cong ker(\pi_{|G'|})$, visto que $1+\frac{(\omega_1-1)\widehat{G'}}{|G'|} = 1+\frac{(\omega_2-1)\widehat{G'}}{|G'|}$ se, e somente se, $\pi(\omega_1) = \pi(\omega_2)$.

Assim, concluímos nosso resultado.

□

Vamos agora aplicar o teorema acima em alguns casos e descrever explicitamente o grupo de unidades centrais de alguns anéis de grupo.

Vamos mostrar mais adiante que existem grupos metacíclicos para os quais o resultado não vale (para ilustrar a importância da hipótese do teorema).

3.2 Produto Semidireto de Cíclicos cujas Ordens São Potências de Primos Distintos

Na Seção 2.3 vimos que são conhecidos resultados para os grupos do tipo $C_{p,q}$, que é equivalente ao produto semidireto $C_q \rtimes C_p$. É sabido que este é o único caso de produto semidireto entre os grupos C_q e C_p.

Faremos um processo similar para encontrar resultados sobre a estrutura do grupo de unidades centrais de certo produto semidireto entre os grupos C_{q^m} e C_{p^n}, aplicando o Corolário 3.1.5. Vamos assim definir o seguinte grupo, dados p e q primos ímpares distintos e $1 < r < q^m$:

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

Vale dizer que no artigo (Jespers, Olteanu, del Río e Gelder, 2013), é construído um conjunto de unidades linearmente independentes que geram subgrupo de índice finito para o grupo de unidades acima, quando a ação que define o produto semidireto tem núcleo trivial.

Notemos que para que o grupo acima esteja bem definido, precisamos que $r^{p^n} \equiv 1\ (mod\ q^m)$, de onde temos que $(r,q) = 1$. Além disso, vamos apenas trabalhar com o caso em que o grupo acima é não-comutativo, portanto também vamos supor $r \not\equiv 1\ (mod\ q^m)$. Esses são todos os produtos semidiretos não-abelianos possíveis.

Para podermos prosseguir, vamos precisar de alguns fatos a respeito dos grupos definidos acima.

Lema 3.2.1. *Se s e r são inteiros que tornam produtos semidiretos de ordem p^nq^m os grupos $C_{p^n,q^m,r}$ e $C_{p^n,q^m,s}$, e se existe inteiro o tal que $o(r) = o(s) = p^o$ no grupo de unidades de $\mathbb{Z}_{q^m}$, então $C_{p^n,q^m,r} \cong C_{p^n,q^m,s}$.*

Demonstração:

Sabemos que $U(\mathbb{Z}_{q^m})$ (o grupo de unidades de $\mathbb{Z}_{q^m}$) é cíclico e, portanto, existe j tal que $(j,p) = 1$ e $r^j \equiv s \ (mod\ q^m)$.

Assim, $b^jab^{-j} = a^s$, e b^j gera $\langle b\rangle$ (pois $(j,p) = 1$).

Então:

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

□

A recíproca do resultado acima nós concluiremos após calcular as classes de conjugação do grupo.

Lema 3.2.2. *Seja $o, l \in \mathbb{Z}$, $o \geq 1$, $0 \leq l < o$ e $o(r) = p^o$ em $U(Z_{q^m})$, então $r^{p^l} \not\equiv 1 \ (mod\ q^k)$, para todo $k \leq m$.*

Demonstração:

Sabemos que $|U(\mathbb{Z}_{q^m})| = q^{m-1}(q-1)$, $|U(\mathbb{Z}_{q^k})| = q^{k-1}(q-1)$.

Como $r^{p^o} \equiv 1 \ (mod\ q^m)$, então $p^o|(q-1)$. Além disso, também sabemos que $U(\mathbb{Z}_{q^m})$ é cíclico (pois q é ímpar). Seja t um inteiro cuja classe módulo q^m gera $U(\mathbb{Z}_{q^m})$. Temos que a classe módulo q^k de t também gera $U(\mathbb{Z}_{q^k})$.

Assim, existem i, j tais que $(j,p) = (i,p) = 1, r \equiv t^{q^{m-1}\frac{(q-1)j}{p^o}} \ (mod\ q^k)$ e $r \equiv t^{q^{m-1}\frac{(q-1)i}{p^o}} \ (mod\ q^m)$ (pois $t^{q^{m-1}\frac{(q-1)}{p^o}}$ é gerador dos subgrupos de ordem p^o de $U(\mathbb{Z}_{q^m})$ e de $U(\mathbb{Z}_{q^k})$, e r pertence a ambos os subgrupos).

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

Portanto $r^{p^l} \not\equiv 1 \ (mod\ q^k)$.

□

Lema 3.2.3. *Se $o(r) = p^o$ em $U(\mathbb{Z}_{q^m})$, então $(1 - r^i, q^m) = q^k$, para algum $k \leq m$ se, e somente se $p^o|i$.*

E nesse caso, $(1 - r^i, q^m) = q^m$.

Demonstração:

($\Rightarrow$) Nesse caso, $q^k|(1 - r^i)$. Então existe y inteiro tal que $1 - r^i = q^ky$. Temos:

$$r^i = q^ky + 1$$

$$r^i \equiv 1 \ (mod\ q^k)$$

Pelo Lema 3.2.2 temos que $p^o|i$.

($\Leftarrow$) Nesse caso, temos $1 - r^i \equiv 0 \ (mod\ q^m)$, e portanto podemos tomar $k = m$.

□

Agora vamos calcular as classes de conjugação do grupo $C_{p^n,q^m,r}$ e as somas de cada classe. Vamos fixar p^o como sendo a ordem de r no grupo de unidades de $\mathbb{Z}_{q^m}$:

(1) classe $\{1\}$, cuja soma é 1.

(2) seja $1 \leq i \leq q^m - 1$, $(i, q) = 1$. Vamos calcular a classe de conjugação de a^i:

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

E temos

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

Como $(i, q) = 1$, a congruência acima é equivalente a:

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

Portanto temos que a classe de a^i nesse caso é $\{a^i, a^{ir}, a^{ir^2}, ..., a^{ir^{p^o-1}}\}$, e denotaremos sua soma por γ_i.

No caso em que $(i, q^m) = q^l$, temos (sem perda de generalidade, abaixo consideramos $s > k$):

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

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

Como $(r, q) = 1$, temos que:

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

E pelo lema 3.2.2, temos que

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

Portanto, no caso $(i, q) \neq 1$ também teremos a mesma forma da classe de conjugação de a^i.

(3) Se $1 \leq i \leq p^n - 1$, $(1 - r^i, q) = 1$, vamos encontrar a classe de conjugação de b^i:

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

E temos

$$a^{j(1-r^i)} b^i = a^{l(1-r^i)} b^i \iff$$

$$j(1 - r^i) \equiv l(1 - r^i) \ (mod\ q^m) \iff$$

$$j \equiv l \ (mod\ q^m)$$

Sendo assim, a classe de b^i nesse caso é $\{b^i, ab^i, a^2 b^i, ..., a^{q^m-1} b^i\}$, e sua soma será $\widehat{a} b^i$.

(4) Se $1 \leq i \leq p^n - 1$, $(1 - r^i, q^m) = q^k$ (pelo Lema 3.2.3), $k = m$). Vamos calcular a classe de conjugação de b^i nesse caso:

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

Assim, a classe de conjugação de b^i nesse caso é $\{b^i\}$, e a soma é b^i (isso significa que b^i é elemento central do grupo, quando $(1-r^i, q) \neq 1$). De fato, temos que o centro do grupo é o subgrupo gerado por b^i.

(5) agora vamos calcular um elemento qualquer do tipo $a^s b^i$. No caso em que $(1-r^i, q) = 1$, esta classe já apareceu no item **(3)**, e no caso $(1-r^i, q) \neq 1$, basta utilizar o fato de que b^i é central, e temos que a classe é $\{a^s b^i, ..., a^{sr^{p^o-1}} b^i\}$, e a soma é $\gamma_s b^i$.

Note que todas as classes de conjugação que calculamos têm tamanho 1, p^o ou q^m, provando a recíproca do Lema 3.2.1, isto é, se $C_{p^n,q^m,r} \equiv C_{p^n,q^m,s}$, então $o(r) = o(s)$ no grupo de unidades de $\mathbb{Z}_{q^m}$.

Vamos, em primeiro lugar, mostrar que se $o < n$ (lembrando que o é tal que a ordem de r no grupo de unidades de $\mathbb{Z}_{q^m}$ é p^o), a tese do Corolário 3.1.5 pode não valer.

Para isso, notemos primeiro que $G' = \langle a \rangle$, e que $Z(G) = \langle b^{p^o} \rangle$. Para verificar o que queremos, basta notar que as unidades de $\mathbb{Z}\langle b^{p^o} \rangle$ são todas centrais em $\mathbb{Z}G$ (pois b^{p^o} é elemento central em G), e se u for uma tal unidade, então $1 + (u-1)(1-e_{G'})$ pode ter coeficientes não-inteiros, para certos valores de (p^n, q^m, r). Vamos dar um exemplo a seguir:

Exemplo: Sejam $(p^n, q^m) = (81, 19)$ e r tal que a ordem de r no grupo de unidades de $\mathbb{Z}_{19}$ é 9. Então tomemos a unidade de Hoechsmann dada por:

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

nesse caso, verifica-se facilmente que $1+(u-1)(1-e_{G'}) = u - ue_{G'} + e_{G'}$ tem coeficientes não-inteiros.

Agora definimos o seguinte morfismo:

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

que apenas leva os coeficientes inteiros na sua classe módulo q^m.

Agora que calculamos todas as classes de conjugação e definimos o morfismo acima, concluímos a seguinte implicação do Corolário 3.1.5:

Corolário 3.2.4. *Com as notações que estamos utilizando, temos que*

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

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

Demonstração:

Basta provar que $G' = \langle a \rangle$. Para isso, notemos que $G = \langle a \rangle \langle b \rangle$, portanto $G' = [\langle a \rangle, \langle b \rangle] \subset \langle a \rangle$.

Além disso, temos $aba^{-1}b^{-1} = a^{1-r}$. Pelo Lema 3.2.3, temos que a^{1-r} gera $\langle a \rangle$, provando assim o que queremos.

□

Com os resultados conhecidos de [Ferraz, 2009] e [Ferraz e Kitani, 2015], podemos agora calcular, explicitamente, uma base para W_1 e W_2 nos casos $(p^o, q^m) = (3, 49),\ (9, 19)$ *ou* $(9, 37)$. Nos 3 casos

vamos utilizar métodos semelhantes aos utilizados por [Ferraz e Simón, 2016] para calcular uma base para W_2. Notemos que W_1 no primeiro caso é o grupo trivial. Nos outros 2 casos vamos utilizar o software GAP para calcular W_1. Nós vamos começar calculando uma base para W_2.

3.2.5 Base para W_2

Antes, vamos precisar da seguinte proposição:

Proposição 3.2.6. *As unidades em W_2 são simétricas.*

Demonstração:

Seja η morfismo que estende $a \mapsto bab^{-1} = a^r$. Temos que $W_2 = \{u \in U_1(\mathbb{Z}C_{q^m}) | \eta(u) = u\}$. Também temos que $\eta(x^*) = \eta(x)^*$, para todo $x \in \mathbb{Z}C_{q^m}$. Portanto, se u for unidade simétrica, então $\eta(u)$ também é.

Seja $u \in W_2$. Temos que u pode ser escrito de forma única como sendo $u = a^i v$, com $0 \leq i \leq q^m - 1$, $v = v^*$. Como $\eta(u) = u$, temos que $a^i v = \eta(a^i v) = \eta(a^i)\eta(v) = a^{ri}\eta(v)$, como $\eta(v)$ é simétrica e pela unicidade da expressão para u, temos que $v = \eta(v)$, e que $a^{ri} = a^i$. Então $q^m | (r-1)i$, e pelo Lema 3.2.2, temos que $q \not| (r-1)$, portanto $q^m | i$ e temos que $u = v$, provando assim o que queríamos.

□

Vamos começar pelos casos $(p^n, q^m) = (9, 19)$ ou $(9, 37)$ (e a ordem de r no grupo de unidades de C_{q^m} é p^n). Em particular, nesses casos, temos que $m = 1$. Já vamos fazer uma construção semelhante à feita em [Ferraz e Simón, 2016].

Seja $S_0 = \left\{u_1, u_2, ..., u_{\frac{q-3}{2}}\right\}$ conjunto l.i. de posto máximo de $U_1(\mathbb{Z}C_q)$, dada por:

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

onde t é representante inteiro de um gerador do grupo de unidades de $\mathbb{Z}_q$, s é representante de uma inversa de t nesse grupo, e $k = \dfrac{ts-1}{q}$ (unidades definidas em [Ferraz, 2009]).

Temos, conforme calculado, por exemplo, em [Ferraz e Simón, 2016], que qualquer unidade desse tipo tem inversa dada por:

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

Vamos definir, para $2 \leq i \leq \frac{q-3}{2}$, $v_i := u_{i-1}^{-1} u_i$, e $v_1 := u_1$.

Seja $S_1 = \left\{v_1, ..., v_{\frac{q-3}{2}}\right\}$. Temos que $\langle S_0 \rangle = \langle S_1 \rangle$, e conforme calculado em [Ferraz e Simón, 2016], temos:

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

Com esta expressão acima, generalizamos esta definição para todo $i \geq 0$. Vamos definir o morfismo f como sendo extensão do morfismo de grupos dado por $a \mapsto a^t$. Temos:

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

Temos que v_i pode ser escrito de forma única como $a^{j_i} w_i$, com $w_i = w_i^*$. Assim, temos que:

$$f(w_i) = w_{i+1};\ f^{\frac{q-1}{2}}(w_i) = w_i \tag{3.2.1}$$

Definimos $S_* = \left\{w_1, ..., w_{\frac{q-3}{2}}\right\}$, e temos que S_* gera um complemento para $\langle a\rangle$ em $U_1(\mathbb{Z}C_q)$.

Por 3.2.1 temos que, definindo $d := (q-1)/2$, então $w_i = w_{i+d}$, para todo $i \geq 0$. Vamos enunciar o Lema 4.1 de [Ferraz e Simón, 2016]:

Lema 3.2.7. *(Ferraz e Simón) Com as definições acima, temos que* $w_0 w_1 ... w_{\frac{q-3}{2}} = 1$.

Queremos encontrar os elementos gerados por S_* que estão no centro de $\mathbb{Z}G$ e, pela Proposição 3.2.6, tais elementos formam W_2.

A partir de agora, vamos supor $r = t^{(q-1)/p^n}$ (podemos fazer isso, pelo lema 3.2.1). Desta forma, temos que $\eta = f^{\frac{q-1}{p^n}}$. Para simplificar, vamos definir $l := (q-1)/p^n$. Assim, temos que $\eta(w_i) = f^l(w_i) = w_{i+l}$. Para $1 \leq i \leq \frac{l}{2} - 1$ vamos definir os elementos $z_i = w_i w_{i+\frac{l}{2}} + w_{i+l} + ... + w_{i+(p^n-1)\frac{l}{2}}$, e o conjunto $S_\phi = \{z_1, ..., z_{\frac{l}{2}-1}\}$. Temos que o conjunto S_ϕ é l.i., pelo fato de que S_* o é.

Teorema 3.2.8. *Com as definições acima (nos casos em que* $m = 1$*), temos* $\langle S_\phi\rangle = W_2$.

Demonstração:

Vamos começar provando que $S_\phi \subset W_2$. Temos:

$$\eta(w_i) = w_{i+l};$$

$$\eta(w_{i+l}) = w_{i+2l};$$

$$\vdots$$

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

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

Como $2d = p^n l$, então $i + \frac{(p^n+1)}{2}l = i + d + \frac{l}{2}$, e como $w_i = w_{i+d}$, temos (a partir das equações acima):

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

E como $\eta(w_i) = w_{i+l}$, temos:

$$\eta(w_{i+\frac{l}{2}}) = w_{i+\frac{3l}{2}};$$

$$\eta(w_{i+\frac{3l}{2}}) = w_{i+\frac{5l}{2}};$$

$$\vdots$$

$$\eta(w_{i+\frac{(p^n-4)l}{2}}) = w_{i+\frac{(p^n-2)l}{2}};$$

$$\eta(w_{i+\frac{(p^n-2)l}{2}}) = w_{i+\frac{p^n l}{2}} = w_{i+d} = w_i.$$

Daí, temos que:

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

$$= w_{i+l}w_{i+\frac{3l}{2}}...w_{i+\frac{(p^n-1)l}{2}}w_iw_{i+\frac{l}{2}} = z_i.$$

Acabamos de provar que $\langle S_\phi\rangle \subset W_2$. Vamos agora demonstrar a outra inclusão.

Suponha que $u \in W_2$. Pela Proposição 3.2.6, temos que u é simétrica e, portanto, podemos escrever $u = w_1^{r_1}...w_{d-1}^{r_{d-1}}$, para certos inteiros r_i, visto que S_* gera o grupo das unidades simétricas em $\mathbb{Z}C_q$. Temos:

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

pois para $i \geq d-l$, temos $i+l \geq d$, por isso substitui-se $i+l$ por $i+l-d$ no índice dos w's.

Pela Proposição 3.2.7 temos que $w_0 = w_1^{-1}...w_{d-1}^{-1}$, então temos:

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

Como u é central, temos $u = \eta(u)$. Além disso, S_* é conjunto l.i., portanto os expoentes dos w_i's em u são iguais aos de $\eta(u)$. Em particular, temos que $r_l = -r_{d-l}$, $r_{2l} = r_l - r_{d-l} = -2r_{d-l}$. Por indução temos que, para todo inteiro $j \geq 1$, $r_{jl} = -jr_{d-l}$ (pois $r_{jl} = r_{(j-1)l} - r_{d-l}$).

Também temos que $r_{\frac{l}{2}} = r_{d-\frac{l}{2}} - r_{d-l}$. Como $d - \frac{l}{2} = \frac{p^n-1}{2}l$ e $r_{jl} = -jr_{d-l}$, temos que $r_{l/2} = -\frac{p^n-1}{2}r_{d-l} - r_{d-l} = -\frac{p^n+1}{2}r_{d-l}$. Além disso, $r_{\frac{3l}{2}} = r_{\frac{l}{2}} - r_{d-l} = -\frac{p^n+3}{2}r_{d-l}$. Por indução temos que, se m é ímpar, então $r_{\frac{ml}{2}} = r_{\frac{(m-2)l}{2}} - r_{d-l} = -\frac{p^n+m}{2}r_{d-l}$.

Usando a fórmula acima para $m = p^n - 2$, temos que $r_{m\frac{l}{2}} = -(p^n-1)r_{d-l}$, no entanto, para este valor de m, temos que $m\frac{l}{2} = d - l$. Portanto, concluímos que $r_{d-l} = -(p^n-1)r_{d-l}$, donde temos que $r_{d-l} = 0$. Podemos, assim, escrever:

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

Comparando os expoentes dos fatores de u e $\eta(u)$, temos que $r_i = r_{i+jl}$, para todos $i, j \geq 1$ (quando o índice estiver definido). Também temos que $r_i = r_{i+d-l} = r_{i+\frac{(p^n-2)l}{2}}$, e pela fórmula que concluímos anteriormente neste mesmo parágrafo, temos $r_{i+\frac{(p^n-2)l}{2}} = r_{i+\frac{(p^n-4)l}{2}} = ... = r_{i+\frac{l}{2}}$.

Daí concluímos que $r_i = r_{i+\frac{l}{2}} = r_{i+l} = ... = r_{i+\frac{(p^n-1)l}{2}}$, e $u = z_1^{r_1}...z_{\frac{l}{2}-1}^{r_{\frac{l}{2}-1}}$, como queríamos.

□

Agora falta fazer o caso $(p^n, q^m) = (3, 49)$. Neste caso $n = 1$ e $m = 2$. Os casos anteriores foram essencialmente repetição do que foi feito em [Ferraz e Simón, 2016]. Neste caso o procedimento é praticamente o mesmo, porém será feito para dois tipos diferentes de unidades de $\mathbb{Z}C_{q^m}$, conforme descreveremos a seguir.

Pelo artigo [Ferraz e Kitani, 2015], temos que, se $\phi(q^2) \leq 66$, então $ker(\overline{\pi_1}) \times \langle S\rangle$ gera complemento para $\langle a\rangle$, onde $\overline{\pi_1} : U_1(\mathbb{Z}C_{q^2}) \to U_1(\mathbb{Z}[\theta])$, θ é uma raiz q^2-primitiva da unidade e $U_1(\mathbb{Z}[\theta])$ são unidades congruentes a 1 módulo $\theta - 1$ de $\mathbb{Z}[\theta]$, S é o conjunto das unidades $u_i = (1 + a^t + a^{2t} + ... + a^{(s-1)t})(1 + a^{t^i} + a^{2t^i} + ... + a^{(t-1)t^i}) - \frac{(ts-1)}{q^2}\widehat{a}$, com t um gerador do grupo de unidades dos inteiros módulo q^2 e s sua inversa, $1 \leq i \leq \phi(q^2)/2 - 1$.

Vamos utilizar as unidades u_i e tomar $r = t^{\frac{\phi(q^m)}{p^n}}$. Desta maneira temos, de forma análoga ao que foi feito nos casos anteriores, obtemos os conjuntos S_0, formado por elementos do tipo $v_i = u_{i-1}^{-1}u_i$, para $1 < i \leq \phi(q^2)/2 - 1$, $v_1 = u_1$. Temos que os elementos v_i são escritos como

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

Novamente vamos chamar de f a função que estende $a \mapsto a^t$. Temos, de forma análoga ao que fizemos nos casos anteriores, que $f(v_i) = v_{i+1}$, $f^{\phi(q^2)/2}(v_i) = v_{i+\phi(q^2)/2} = v_i^*$. Novamente, sabemos que existe único w_i tal que $v_i = a^{j_i}w_i$, e w_i é simétrico. E definimos o conjunto $S_* = \{w_1, ..., w_{\phi(q^2)/2-1}\}$ de unidades simétricas l.i.. Temos que $f(w_i) = w_{i+1}$ e $f^{\phi(q^2)/2}(w_i) = w_i$. Temos o seguinte lema, análogo ao lema 3.2.7:

Lema 3.2.9. *Com as definições acima,* $w_0...w_{\frac{\phi(q^2)}{2}-1} = 1$

Demonstração:

Vamos utilizar as propriedades da função f. Definindo $u = w_0...w_{\phi(q^2)/2-1}$, temos:

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

Além disso:

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

$$= \prod_{j=1}^{\phi(q^2)} \overline{\pi_1}(u) = (\overline{\pi_1}(u))^{\phi(q^2)} = \overline{\pi_1}(u^{\phi(q^2)}).$$

Como u é uma unidade de aumento 1, temos que $N_{\mathbb{Q}(\theta)|\mathbb{Q}}(\overline{\pi_1}(u)) = 1$.

No entanto, pelo artigo [Ferraz e Kitani, 2015], sabemos que $u^j \notin ker(\overline{\pi_1})$ se $u \neq 1$, para todo $j \geq 1$ (pois $\langle S \rangle \cap ker(\overline{\pi_1})$ é trivial).

Assim, temos $u = 1$, como desejamos.

□

Assim, definimos $d := \phi(q^2)/2$, $l = \phi(q^2)/p^n$, e definimos o conjunto $S_\phi = \{z_1, ..., z_{l/2-1}\}$, onde $z_i = w_i w_{i+l/2} w_{i+l} ... w_{i+(p^n-1)l/2}$. De modo análogo ao que fizemos nos casos anteriores, temos que $S_\phi \subset W_2$. Neste caso não temos a igualdade, pois ainda precisamos considerar as unidades em $ker(\overline{\pi_1})$. No entanto, as unidades z_i que encontramos aqui formam uma base para o grupo de unidades centrais em $\mathbb{Z}G$ que estão em $\langle S_* \rangle$, de modo análogo ao que fizemos nos casos anteriores. E sabemos que $ker(\overline{\pi_1}) \times \langle S_* \rangle$ gera um complemento para $\langle a \rangle$ no grupo $U_1(\mathbb{Z}C_{q^2})$.

Consideremos a função $f_1 : U_1(\mathbb{Z}C_q) \to U_1(\mathbb{Z}_q)$. A partir de agora vamos considerar que q é um primo regular (é o caso se $q = 7$). Assim sendo, pelo lema de Kümmer, temos $ker(f_1) = \{u^q | u \in U_1(\mathbb{Z}C_q)\}$. Vamos denotar $h = a^q$, assim h é gerador de C_q. Portanto, utilizando as unidades simétricas de $\mathbb{Z}C_q$ encontradas a partir das unidades de Hoechsmann (fizemos este procedimento nos casos anteriores), que nós vamos chamar de $\tilde{w_i}$, temos que $ker(f_1) = \langle \tilde{w_i}^q \rangle_{i=1,...,(q-3)/2}$. Para facilitar notação, vamos chamar $\mu_i = \tilde{w_i}^q$. Assim, temos que as unidades μ_i são da forma $1 + qx_i = 1 + q(c_{0,i} + c_{1,i}h + ...c_{q-1,i}h^{q-1})$, onde $c_{j,k}$ são inteiros.

Vamos definir as unidades $\rho_i = 1 + c_{0,i}\widehat{h} + c_{1,i}a\widehat{h} + c_{2,i}a^2\widehat{h} + ... + c_{q-1,i}a^{q-1}\widehat{h}$. Pelo artigo [Ferraz e Kitani, 2015], temos $ker(\overline{\pi_1})$ é gerado pelas unidades $\rho_i, i = 1, ..., (q-3)/2$ que são l.i. e simétricas. Daí, concluímos que as unidades de $ker(\overline{\pi_1})$ são precisamente todos os elementos do tipo:

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

onde $1 + d_0 + d_1 h + ... + d_{q-1}h^{q-1}$ é gerado pelo conjunto dos μ_i's.

De forma análoga ao que fizemos nos casos anteriores, vamos definir unidades $\tilde{z}_i$, para $1 \leq i \leq \frac{(q-1)}{2p} - 1$, dados por

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

Observação 3.2.10. *aqui, $(q-1)/2p$ desempenha o mesmo papel que l desempenhou nos casos anteriores.*

Observação 3.2.11. *no caso $q = 7, p = 3$ que nós estamos trabalhando, o conjunto dos $\tilde{z}_i$'s é vazio, pois $\frac{(q-1)}{2p} - 1 = 0$. Isso acontece devido ao fato de que o posto do grupo de unidades centrais de $\mathbb{Z}C_{3,7}$ é zero (ver, por exemplo, a fórmula do posto calculada em [Ferraz e Simón, 2008]). Mas vamos continuar com o argumento para que o método seja o mais geral possível, podendo servir, por exemplo, para encontrar geradores de um subgrupo de índice finito do grupo $Z(U_1(\mathbb{Z}G))$ no futuro.*

Com este procedimento, temos que as unidades $\tilde{z}_i$ formam uma base do grupo de unidades em $\mathbb{Z}C_q$ que estão em $Z(\mathbb{Z}C_{p,q})$ (aqui $C_{p,q}$ visto como subgrupo de G) e, consequentemente, em $Z(\mathbb{Z}G)$.

Portanto, concluímos que uma base para as unidades em $ker(\overline{\pi_1})$ que estão em $Z(\mathbb{Z}G)$ é formado por unidades do tipo

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

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

Fazendo um procedimento análogo ao que fizemos nos casos anteriores, temos que as unidades z_i e ζ_j formam uma base para W_2.

Observação 3.2.12. *no caso $q = 7, p = 3$ que nós estamos estudando, temos apenas as unidades z_i, pelo motivo já observado anteriormente.*

3.2.13 Base para W_1

Vamos começar provando a seguinte proposição, análoga à proposição 2.1 de [Ferraz e Simón, 2016]:

Proposição 3.2.14. *Com as mesmas notações do corolário 3.2.4, temos que $ker(\pi_{q^m})$ só tem unidades simétricas.*

Demonstração:

Seja $u \in ker(\pi_{q^m})$. Temos, pela Proposição 1.1.6 que existe uma potência de b, digamos, b^j, e w unidade simétrica tal que $u = b^j w$.

Então $1 = \pi_{q^m}(b^j w) = \pi_{q^m}(b^j)\pi_{q^m}(w) = b^j \pi_{q^m}(w)$, de onde concluímos que $\pi_{q^m}(w) = b^{-j}$, mas este último é unidade simétrica, de onde concluímos que $b^{-j} = 1$ e, portanto, $u = w$.

□

Ainda precisamos calcular W_1 nos casos $(p^o, q^m) = (9, 19)$ ou $(9, 37)$ (nestes casos temos $m = 1$). Pelo corolário 3.5.6 de [Polcino e Sehgal, 2002], temos que $\mathbb{Z}_q C_{p^o} \cong (\mathbb{Z}_q)^{p^o}$ (pois r é uma raiz primitiva da unidade de ordem p^o em $\mathbb{Z}C_q$).

Precisamos calcular o núcleo da função $\pi_{q^m} (= \pi_q)$. Pela observação acima, temos que o expoente de $\mathbb{Z}_q C_{p^o}$ é $q - 1$. E pelo artigo [Ferraz e Kitani, 2015], temos que o conjunto $S = \{s_1 = -1 + b - b^2 + b^3 + b^6 - b^7 + b^8, s_2 = 1 - b + b^2 + b^7 - b^8\}$ gera $U^*(\mathbb{Z}C_9)$, o grupo das unidades simétricas, onde b é gerador de C_9. Assim, basta nós calcularmos todas as combinações $s_1^i s_2^j$, com $0 \leq i, j \leq q - 2$, para os possíveis valores de q (no nosso caso, 19 ou 37), e assim teremos calculado geradores do núcleo de $ker(\pi_q)$ para cada caso. Usamos o programa GAP, com o seguinte código:

```
1 G := CyclicGroup(IsPermGroup,9);
2 R := GroupRing(GF(19),G);
3 b := R.1;
4
5 s1 := -b^0 + b - b^2 + b^3 + b^6 - b^7 + b^8;
6 s2 := b^0 - b + b^2 + b^7 - b^8;
7
8 r := b^0;
9 s := b^0;
10
11 for i in [0..17] do
12     s := b^0;
13     for j in [0..17] do
14         if r*s = b^0 then
15             Print("i = ", i, "; j = ", j, "\n");
16         fi;
17         s := s2*s;
18     od;
19     r := s1*r;
20 od;
```

No código acima fizemos o caso $q = 19$ mas, trocando 19 por 37 e 17 por 35 no código acima, obtemos o código para o caso $q = 37$.

Caso $q = 19$:

Obtivemos a seguinte saída:

i = 0; j = 0

i = 6; j = 6

i = 12; j = 12

Daí concluímos que, no caso $q = 19$, o núcleo da função é gerado por $\{s_1^6 s_2^6, s_1^{18}\}$, pois a segunda linha da saída gera a unidade dada pela terceira linha.

Caso $q = 37$:

Obtivemos a seguinte saída:

i = 0; j = 0

i = 12; j = 12

i = 24; j = 24

Daí concluímos que, no caso $q = 37$, o núcleo da função é gerado por $\{s_1^{12} s_2^{12}, s_1^{36}\}$, pois a segunda linha da saída gera a unidade dada pela terceira linha.

E assim terminamos esta seção.

3.3 p-Grupos Metacíclicos

Nesta seção, vamos considerar o grupo $G_n = \left\langle a, b | a^{p^2} = b^{p^n} = 1, bab^{-1} = a^{p+1} \right\rangle$, que é produto semidireto $C_{p^2} \rtimes C_{p^n}$.

O centro de G_n é $\{1, a^p, a^{2p}, ..., a^{(p-1)p}\}$. As classes de conjugação de elementos não centrais desse grupo são bem conhecidas, e as listamos da seguinte maneira:

(1) a classe de a^i, para $p \nmid i$ é $\{a^i, a^{i+p}, a^{i+2p}, ..., a^{i+(p-1)p}\}$, e a soma dos elementos dessa classe é $\gamma_i := \widehat{Z(G_n)}a^i$.

(2) a classe de $a^s b^i$ é $\{a^s b^i, a^{p+s} b^i, a^{2p+s} b^i, ..., a^{(p-1)p+s} b^i\}$, e a soma dos elementos dessa classe é $\Gamma_{i,s} := \widehat{Z(G_n)}a^s b^i$.

Também temos que $G' = Z(G_n) = \langle a^p \rangle$. Assim, temos que G_n satisfaz às condições do Corolário 3.1.5.

Vamos definir o seguinte morfismo:

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

que apenas leva os coeficientes inteiros na sua classe módulo p.

Agora temos o seguinte teorema:

Teorema 3.3.1. *Com as notações utilizadas até agora nesta seção, temos que*

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

onde

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

$$W_2 = U_1(\mathbb{Z}Z(G_n)) \cong U_1(\mathbb{Z}C_p)$$

Observação 3.3.2. *aqui, estamos enxergando o domínio de $\pi_{p,n}$ como sendo $U_1(\mathbb{Z}G_n/G'_n) = U_1(\mathbb{Z}G_n/\langle a^p \rangle)$, e podemos tomar w como sendo qualquer representante no anel de grupo $\mathbb{Z}G_n$.*

Demonstração:

Segue diretamente do Corolário 3.1.5, e temos que a imagem de w_i em $U_1(\mathbb{Z}G_n/G'_n)$ é o que define u_i (lembrando que $Z(G_n) = G'_n$).

□

No próximo capítulo, vamos calcular o núcleo da função $\pi_{p,1}$ quando p é um primo regular e provaremos que ele é precisamente o conjunto $\{u^p | u \in U_1(\mathbb{Z}C_p \times C_p)\}$ (ver o Teorema 4.2.4), dando uma outra demonstração de um caso particular do resultado principal de (Hoechsmann, 1989).

3.4 p-Grupos Metabelianos

Nesta seção, vamos trabalhar com grupos do tipo $(C_p)^n \rtimes C_p$, onde $(C_p)^n$ é o produto direto de n cópias de C_p.

No caso $n = 2$, temos um grupo conhecido:

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

E também pode ser visto como o seguinte grupo multiplicativo de matrizes:

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

Tal grupo é conhecido como grupo de Heisenberg.

Sendo que o isomorfismo entre G e H descritos acima é dado por

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

Voltando para o caso geral, vamos definir os seguintes grupos, para $n \geq 2$:

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

De maneira análoga ao que acontece no caso $n = 2$, temos que $Z(H_n) = \langle a_1 \rangle = H_n'$, e a classe de conjugação de um elemento do tipo $g = a_2^{i_2} ... a_n^{i_n} b^j$ é o conjunto $\{g, a_1 g, a_1^2 g, ..., a_1^{p-1} g\}$.

Portanto, temos que os conjuntos do tipo H_n satisfazem às condições do Corolário 3.1.5.

Vamos definir as funções $\tilde{\pi}_{p,n} : U_1(\mathbb{Z}(C_p)^n) \to U_1(\mathbb{Z}_p(C_p)^n)$, que leva os coeficientes na sua classe módulo p. Temos o seguinte teorema:

Teorema 3.4.1. *Com as mesmas notações usadas acima, temos que*

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

onde:

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

$$W_2 = U_1(\mathbb{Z}Z(H_n)) \cong U_1(\mathbb{Z}C_p)$$

Observação 3.4.2. *de modo análogo ao que fizemos no Teorema 3.3.1, estamos considerando o domínio de $\tilde{\pi}_{p,n}$ como sendo $U_1(\mathbb{Z}H_n/H_n')$, e podemos tomar w como sendo qualquer representante dele no anel de grupo $\mathbb{Z}H_n$.*

Demonstração:

Pelos parágrafos anteriores, temos que H_n satisfaz às hipóteses do Corolário 3.1.5, portanto, de forma análoga ao Teorema 3.3.1, segue diretamente do Corolário 3.1.5.

□

No próximo capítulo, vamos calcular o núcleo da função $\tilde{\pi}_{p,n}$ quando p é um primo regular, e provaremos que ele é precisamente o conjunto $\{u^p | u \in U_1(\mathbb{Z}(C_p)^n)\}$ (ver o Teorema 4.2.4), provando um caso particular do resultado principal de (Hoechsmann, 1989).

Assim sendo, seremos capazes de exibir explicitamente uma base para o grupo de unidades centrais para uma classe infinita de anéis de grupos integrais não comutativos, utilizando os resultados do Capítulo 2. Mais especificamente, para os anéis de grupo do tipo $\mathbb{Z}H_n$, sempre que p for um primo regular menor que 68.

3.5 Grupos Diedrais Generalizados

Vamos considerar H grupo abeliano finito com $|H|$ ímpar e os grupos do tipo:

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

onde $C_2 = \langle g \rangle$ e o produto semidireto é definido pelo morfismo ψ, dado por:

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

Observação 3.5.1. *Não precisamos que $|H|$ seja ímpar para definir tais grupos, mas precisaremos disso para provar o teorema que seguirá nesta seção. Os grupos do tipo G_H são chamados de grupos diedrais generalizados.*

Observação 3.5.2. *No caso em que H é grupo cíclico de ordem ímpar n, temos que G_H é o grupo diedral D_{2n}, e este caso foi feito na tese de doutorado de Ferraz (Ferraz, 2002).*

Desta forma, temos que se $x \in H$, então $xgx^{-1} = x^2 g$ e, como $|H|$ é ímpar, temos que $x \in H \mapsto x^2$ é sobrejetora (sobre H), portanto $G'_H = H$.

Além disso, temos que se $y \notin G'_H$, então a soma dos elementos da classe de conjugação de y é $\gamma_y = \widehat{G'_H} y$.

Assim, temos satisfeitas as hipóteses do Corolário 3.1.5, e temos imediatamente o seguinte teorema:

Teorema 3.5.3. *Se G_H é o grupo definido acima, onde H é grupo abeliano finito com $|H|$ ímpar, então $Z(U_1(\mathbb{Z}G_H))$ é o grupo de unidades simétricas $U_1^*(\mathbb{Z}H)$.*

Demonstração:

Pelo Corolário 3.1.5, temos $Z(U_1(\mathbb{Z}G_H)) = W_1 \times W_2$, onde W_1 é congruente a um subgrupo de $U(\mathbb{Z}G_H/G'_H) \cong U(\mathbb{Z}C_2)$, que é trivial. Portanto, a única parcela não trivial é W_2.

Este, por sua vez, compreende as unidades centrais de $U_1(\mathbb{Z}H)$ que comutam com G_H. Como $gxg^{-1} = x^{-1}$, temos que $u \in W_2$ se, e somente se u é unidade simétrica em $Z(U_1(\mathbb{Z}H))$, de onde temos o resultado desejado.

□

Podemos, em particular tomar H como sendo um grupo abeliano de ordem ímpar cujo grupo de unidades nós já conhecemos (ver, por exemplo, o Capítulo 2). Neste caso temos, imediatamente, por exemplo, o resultado para o grupo diedral D_{2n}, onde n é ímpar, obtendo um caso particular para um resultado publicado na tese de doutorado de Ferraz (Ferraz, 2002).

Capítulo 4

Anéis de Grupo Comutativos

Neste capítulo, vamos estudar o grupo de unidades de alguns anéis de grupo do tipo $\mathbb{Z}[\theta_p](C_p)^n$, onde θ_p é uma raiz primitiva da unidade de ordem p, obtendo resultados análogos aos obtidos em (Hoechsmann e Sehgal, 1986) e (Hoechsmann, Sehgal, Weiss, 1985).

Também vamos apresentar demonstração alternativa para um caso particular do resultado principal de (Hoechsmann, 1989), e mostrar aplicações do mesmo para calcular os exemplos G_n e H_n do capítulo anterior.

4.1 Anel de Grupo sobre Inteiros p-Ciclotômicos

Temos, pelo Teorema 3.5.4 de (Polcino e Sehgal, 2002), que $\mathbb{Q}[\theta_p]C_p \cong p\mathbb{Q}(\theta_p) = \mathbb{Q}(\theta_p) \oplus ... \oplus \mathbb{Q}(\theta_p)$ (p somas de $\mathbb{Q}(\theta_p)$), onde cada um dos termos é dado por um idempotente primitivo do anel de grupo $\mathbb{Q}(\theta_p)C_p$, isto é, para cada componente simples $S_i \cong \mathbb{Q}(\theta_p)$ existe um idempotente e_i tal que $S_i = \mathbb{Q}(\theta_p)C_p e_i$, o ideal gerado por e_i.

Além disso, temos que a imagem de $\mathbb{Z}[\theta_p]C_p$ por este isomorfismo está contida em $p\mathbb{Z}[\theta_p]$ - uma maneira de justificar isso é observar que os idempotentes primitivos são os elementos da forma $e_i = (h\theta_p^i)^0 + (h\theta_p^i)^1 + ... + (h\theta_p^i)^{p-1}$, $i = 0, ..., p-1$, onde h é gerador de C_p, portanto a imagem de θ_p em cada componente é um elemento diferente de 1 que é raiz p-ésima da unidade, portanto temos que a imagem de $\mathbb{Z}[\theta_p]C_p$ em cada componente é, de fato, $\mathbb{Z}[\theta_p]$.

Assim sendo, podemos considerar $\mathbb{Z}[\theta_p]C_p$ como subanel de $p\mathbb{Z}[\theta_p]$.

Devido ao fato de que a imagem de h em cada componente também é um elemento $\neq 1$ que é raiz p-ésima da unidade temos que, em particular, para cada componente i existe j tal que $g\theta_p^j \mapsto \theta_p$ na componente i.

Também concluímos com isso que a imagem do isomorfismo restrito ao grupo de unidades de $\mathbb{Z}[\theta_p]C_p$ está contida no grupo de unidades de $p\mathbb{Z}[\theta_p]$.

Além disso, temos que $U_1\mathbb{Z}C_p \cong U_1\mathbb{Z}[\theta_p]$, onde $U_1(\mathbb{Z}[\theta_p])$ representa o grupo de unidades de $\mathbb{Z}[\theta_p]$ congruentes a 1 módulo $\theta_p - 1$ (ver, por exemplo, Lemma 15.1 de [Sehgal, 1993]).

Vamos denotar por $U_1(p\mathbb{Z}[\theta_p])$ o conjunto $pU_1(\mathbb{Z}[\theta_p])$, e vamos denotar por $U_1(\mathbb{Z}[\theta_p]C_p)$ o conjunto das unidades cujo aumento é congruente a 1 módulo $(\theta_p - 1)$.

Com as informações acima em mente, podemos enunciar o seguinte resultado:

Lema 4.1.1. *Com as notações acima, temos que* $U_1(\mathbb{Z}[\theta_p]C_p) \leq U_1(p\mathbb{Z}[\theta_p])$. *Além disso, se* $u \in U_1(p\mathbb{Z}[\theta_p])$, *então* u^p *é unidade de* $U_1(\mathbb{Z}[\theta_p]C_p)$.

Demonstração:

Primeiro, vamos lembrar que existe a decomposição de $\mathbb{Q}[\theta_p]C_p$ como sendo $p\mathbb{Q}[\theta_p]$.

A primeira parte do teorema nós temos do fato de que $g\theta_p^j \mapsto \theta_p$, em cada termo da decomposição, para certos j, ou seja, $g \mapsto \theta_p^{1-j}$ para cada termo da decomposição, para certos $j \in \mathbb{Z}$. Assim sendo, se $\varepsilon(u) \equiv 1\ (mod\ (\theta_p - 1))$, então a imagem de u em cada componente de $p\mathbb{Z}[\theta_p]$ é uma unidade congruente a 1 módulo $\theta_p - 1$.

Com as notações acima, e denotando por g um gerador de C_p, se e_i's $(i = 0, ..., p-1)$ forem os idempotentes relativos aos termos $\mathbb{Q}[\theta_p]$ da soma de Wedderburn-Artin, podemos tomar, sem perda de generalidade, uma unidade básica $u = (1 + (\theta_p - 1)v)e_0 + e_1 + ... + e_{p-1}$, onde $v \in \mathbb{Z}[\theta_1]C_p$.

Assim sendo, temos:

$$u^p = ((1 + (\theta_p - 1)v)e_0 + e_1 + ... + e_{p-1})^p =$$

$$= (1 + (\theta_p - 1)v)^p e_0 + e_1 + ... + e_{p-1}$$

Vamos tomar $e_i = \frac{1}{p}(1 + \theta_p^{(p-1)^i} g + \theta_p^{(p-2)^i} g^2 + ... + \theta_p^{1^i} g^{p-1})$, se $i > 0$, $e_0 = \widehat{C_p}$ (ou seja, todos têm denominador p) o conjunto de todos os idempotentes primitivos de $\mathbb{Q}[\theta_p]C_p$ portanto, para provarmos a segunda parte do lema, basta provar que $(1 + (\theta_p - 1)v)^p - 1 \equiv 0(mod\ p)$. Temos:

$$(1 + (\theta_p - 1)v)^p - 1 \equiv 1 + (\theta_p - 1)^p v^p - 1 \equiv (\theta_p - 1)^p v^p (mod\ p),$$

e temos:

$$(\theta_p - 1)^p \cong (\theta_p)^p + (-1)^p \cong 0(mod\ p),$$

pois p é ímpar.

Assim, temos o desejado.

□

Do lema acima, temos que o quociente do grupo $U_1(p\mathbb{Z}[\theta_p])$ pelo grupo $U_1(\mathbb{Z}[\theta_p]C_p)$ é abeliano elementar finito, para todo primo p.

A partir de agora, considere $A := C_p \times C_p = \langle g \rangle \times \langle h \rangle$.

Dado G um grupo qualquer, denotemos por $\dot{U}_1(G)$ o grupo de unidades de aumento 1 de $\mathbb{Z}G$ módulo torção.

Vamos definir morfismos semelhantes aos que aparecem no começo do artigo [Hoechsmann, Sehgal, Weiss, 1985], mas primeiro vamos apresentar os morfismos definidos no artigo citado:

O primeiro morfismo é dado por

$$\delta : \prod_C \dot{U}_1 C \to \dot{U}_1(A),$$

onde $A = C_p \times C_p$, e C percorre todos os subgrupos cíclicos não triviais de A. Esse morfismo estende a inclusão $g \in C \mapsto g \in A$.

Antes de apresentar o outro morfismo, lembremos que $\mathbb{Q}A \to (\bigoplus_{i=1}^{n} \mathbb{Q}(\theta_p)) \oplus \mathbb{Q}$, onde n é o número de subgrupos cíclicos não triviais de A, pelo Corolário 3.5.5 de (Polcino e Sehgal, 2002). Assim, temos o segundo morfismo dado por:

$$\xi : \dot{U}_1(A) \to \prod_K \dot{U}_1 K,$$

onde K denota cada fator da decomposição de Wedderburn - Artin acima (com exceção do último fator, dado por $\mathbb{Q}$) - faz sentido devido ao isomorfismo entre $U_1\mathbb{Z}C_p$ e $U_1\mathbb{Z}[\theta]$) - aqui estamos usando notação de produto por se tratar do grupo de unidades. Este morfismo é dado pela restrição do isomorfismo $\mathbb{Q}C_p \times C_p \to \mathbb{Q}\bigoplus_{i=1}^{p+1}\mathbb{Q}(\theta_p)$.

No artigo acima citado, prova-se o seguinte:

Teorema 4.1.2. *O conúcleo da composição $\gamma = \xi \circ \delta$ tem ordem dada por p^N, onde $N = \frac{p-3}{4}(p+1)$.*

Vale notar que o posto do grupo de unidades de $\mathbb{Z}C_p$ é $\frac{p-3}{2}$ (este posto aparece, por exemplo, em [Ferraz, 2009]).

Vamos denotar por $\dot{V}(C_p)$ o grupo de unidades $U_1\mathbb{Z}[\theta_p]C_p$ módulo torção, onde este último representa o conjunto das unidades cujo aumento é congruente a 1 módulo $(\theta_p - 1)$.

Seja

$$\sigma : \dot{U}_1(A) \to \dot{V}(C_p),$$

dado por $g \mapsto \theta_p$, e seja

$$l : \dot{V}(C_p) \to \prod_L \dot{U}_1(L)$$

morfismo natural, onde os L são dados pelas componentes da decomposição de Wedderburn - Artin de $\mathbb{Q}(\theta_p)C_p$.

Vamos também fixar os idempotentes primitivos de $\mathbb{Q}(\theta_p)C_p$ como sendo

$$e_i = (h\theta_p^i)^0 + ... + (h\theta_p^i)^{p-1}, i = 0, ..., p-1,$$

e vamos fixar os idempotentes primitivos de $\mathbb{Q}A$ como sendo

$$E_j = \frac{1}{p}\widehat{hg^j} - \frac{1}{p^2}\widehat{A}, j = 0, ..., p-1,$$

$$E_p = \frac{1}{p}\widehat{g} - \frac{1}{p^2}\widehat{A},$$

$$E_{p+1} = \frac{1}{p^2}\widehat{A}$$

(tais idempotentes foam calculados, por exemplo, em [Jespers, Leal e Paques, 2003]).

Com os idempotentes acima fixados, dado $u \in \dot{U}_1(A)$, temos que

$$u = u_0E_0 + ... + u_pE_p + E_{p+1},$$

para certos u_i unidades de $\mathbb{Z}C_p$ de aumento 1. O coeficiente de E_{p+1} é o aumento de u, por isso é 1.

Temos que, para $j = 0, ..., p-1$, podemos tomar u_j como sendo $\varphi_j(u)$, dada por $h \mapsto g^{-j}$ (ou $h \mapsto \theta_p^{-j}$, se considerar cada componente como sendo $\mathbb{Q}(\theta_p)$), ao passo que u_p pode ser tomada

como $\varphi_p(u)$, que é dada por $g \mapsto 1$. Assim sendo, temos que

$$\sigma(u) = u_0 e_0 + ... + u_{p-1} e_{p-1},$$

e podemos enxergar cada u_i como sendo uma unidade em $\dot{U}C_p$.

Temos o seguinte lema:

Lema 4.1.3. *O núcleo de $\sigma \circ \delta$ é o conjunto das unidades cuja imagem por δ é do tipo $E_0 + ... + E_{p-1} + (u(h))^p E_p + E_{p+1}$, onde $u(h)$ é uma unidade de $\mathbb{Z}\langle h \rangle$.*

Demonstração:

Sejam $u_1(h), ..., u_{\frac{p-3}{2}}(h)$ unidades que formam uma base para $\dot{U}_1\mathbb{Z}\langle h \rangle$.

Temos que $u_1(hg^j), ..., u_{\frac{p-3}{2}}(hg^j)$ forma uma base para $\dot{U}_1\mathbb{Z}\langle hg^j \rangle$, e $u_1(g), ..., u_{\frac{p-3}{2}}(g)$ para $\dot{U}_1\mathbb{Z}\langle g \rangle$. Temos:

$$\sigma(u_i(hg^j)) = u_i(\theta_p^j)e_0 + u_i(\theta_p^{j-1})e_1 + ... + u_i(\theta_p^{j-p+1})e_{p-1}$$

Portanto, temos:

$$\sigma\left(\prod_{j=0}^{p-1}(u_i(hg^j))\right) = \left(\prod_{j=0}^{p-1}(u_i(\theta_p^j))e_0\right) + ... + \left(\prod_{j=0}^{p-1}(u_i(\theta_p^{j-p+1}))e_{p-1}\right),$$

em cada componente, temos que um dos fatores é igual a 1 e os demais são todos os conjugados algébricos de $u_i(\theta_p)$. portanto, podemos escrever a expressão acima do seguinte modo:

$$N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(u_i(\theta_p))e_0 + ... + N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(u_i(\theta_p))e_{p-1} = 1$$

E temos, analogamente, que

$$\prod_{j=0}^{p-1}(u_i(hg^j)) = E_0 + ... + E_{p-1} + (u_i(h))^p E_p + E_{p+1}$$

Portanto, sabemos que todas as unidades do tipo $E_0 + ... + E_{p-1} + (u(h))^p E_p + E_{p+1}$ estão no núcleo de σ. Pelas observações que precedem o lema, temos que todas as unidades do núcleo devem ter a forma $E_0 + ... + E_{p-1} + vE_p + E_{p+1}$, para certo $v \in U_1(\mathbb{Z}\langle h \rangle)$. Portanto, basta provar que se $u = E_0 + ... + E_{p-1} + vE_p + E_{p+1} \in Im(\delta)$, então $v = w^p$, para alguma unidade w.

Podemos escrever, para certos $a_i \in \mathbb{Z}$, $v = u_1(h)^{a_1}...u_{\frac{p-3}{2}}(h)^{a_{\frac{p-3}{2}}}$.Temos que:

$$u^p = \left(\prod_{j=0}^{p-1}(u_1(hg^j))\right)^{a_1} ... \left(\prod_{j=0}^{p-1}(u_{\frac{p-3}{2}}(hg^j))\right)^{a_{\frac{p-3}{2}}}.$$

No entanto, como $rank(\dot{U}_1(A)) = rank(\prod_C \dot{U}_1 C) = rank(\prod_K \dot{U}_1 K) = (p+1)(p-3)/2$ e o conúcleo de $\xi \circ \delta$ é finito (pelo Teorema 4.1.2), temos que o conjunto formado pelas $(p+1)(p-3)/2$ unidades $u_i(g), u_i(hg^j)$, $i = 1, ..., (p-3)/2, j = 0, ..., p-1$ é l.i. e gera a imagem de δ. Portanto, como $u \in Im(\delta)$, temos que $p|a_i$, para todo i.

Isso conclui nossa demonstração.

□

Com essas informações em mente, provemos o seguinte resultado:

Teorema 4.1.4. *O conúcleo de $l \circ \sigma \circ \delta$ é abeliano elementar e tem ordem $p^{\frac{p-3}{4}(p-1)}$.*

Demonstração:

A primeira afirmação segue do lema 4.1.3, pois aplicando funções do tipo $h^i g^j \mapsto h^a g^b$ em $\prod_{j=0}^{p-1}(u_i(hg^j))$, temos que na imagem de $\sigma \circ \delta$ existem todas as unidades do tipo:

$$\sum_{i \neq j}(e_i) + u^p e_j,\ j = 0, ..., p-1.$$

A segunda afirmação segue imediatamente de 4.1.2 e do fato de que $\sigma(u_0(g)E_0 + ... + u_{p-1}(g)E_{p-1} + u_p(h)E_p + E_{p+1}) = u_0(\theta_p)e_0 + ... + u_{p-1}(\theta_p)e_{p-1}$.

□

Observação 4.1.5. *seja K o núcleo da função natural $\dot{U}_1\mathbb{Z}C_p \to \mathbb{Z}_pC_p$. Analisando os coeficientes, vemos facilmente que se $u(\theta_p) \in K$, então $ue_i + \sum_{i \neq j} e_j$ é unidade de $\mathbb{Z}[\theta_p]C_p$. Pela demonstração do teorema anterior, temos que unidades desse tipo estão na imagem de $\sigma \circ \delta$ somente quando o coeficiente não trivial é uma unidade elevada a p. Portanto, se K contém elementos não triviais que não são unidades elevadas a p, então $\sigma \circ \delta$ não é sobrejetora.*

Antes, vamos enunciar o seguinte teorema, cuja prova se encontra em [Low, 2008], e que vamos utilizar na prova do nosso próximo teorema:

Teorema 4.1.6. *(Low, 2008) Dado o seguinte diagrama, onde G é grupo finito, sendo $\pi : g \mapsto 1$, $\sigma : g \mapsto \theta_p$, $\alpha : \theta_p \mapsto \overline{1}$, onde g é gerador de C_p,*

$$\begin{array}{ccc} U_1(\mathbb{Z}C_p \times G) & \xrightarrow{\pi} & U_1(\mathbb{Z}G) \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \rho} \\ U_1(\mathbb{Z}[\theta_p]G) & \xrightarrow{\alpha} & U_1(\mathbb{Z}_pG) \end{array}$$

Temos que σ restrita ao núcleo de π é isomorfismo sobre o núcleo de α.

Agora podemos provar o seguinte resultado:

Teorema 4.1.7. *Com as mesmas notações do Teorema 4.1.6, se G é p-grupo abeliano finito, temos que σ é função sobrejetora.*

Demonstração:

Seja $u \in U_1(\mathbb{Z}[\theta_p]G)$. Vamos provar que $u \in Im(\sigma)$. Considere $\eta : \mathbb{Z}[\theta_p]G \to \mathbb{Z}[\theta_p]G$ endomorfismo induzido por $g \mapsto g^p$, para todo $g \in G$.

Primeiro, vamos provar que $\eta(u)u^{-p} \in Im(\sigma)$: com efeito, podemos escrever

$$u = \sum_{g \in G} a_g g,$$

onde os a_g estão em $\mathbb{Z}[\theta_p]$. Assim, temos:

$$\alpha(u^p) = \alpha(u)^p = \left(\sum_{g\in G} \overline{a_g} g\right)^p,$$

como $\mathbb{Z}_pG$ é anel comutativo de característica p, temos:

$$\alpha(u^p) = \sum_{g\in G} \overline{a_g^p} g^p = \sum_{g\in G} \overline{a_g} g^p = \alpha(\eta(u)),$$

Portanto, $\eta(u)u^{-p} \in ker(\alpha)$ e, pelo Teorema 4.1.6, temos que $\eta(u)u^{-p} \in Im(\sigma)$.

Agora definimos, para $1 \leq s \leq p-1$, os morfismos $\psi_s : \mathbb{Z}[\theta_p]G \to \mathbb{Z}[\theta_p]G$ dados por $\theta_p \mapsto \theta_p^s$.

Assim, temos que $u\psi_s(u)^{-1} \in ker(\alpha)$, pois $\alpha(u) = \alpha(\psi_s(u))$, portanto, pelo Teorema 4.1.6 temos que $u\psi_s(u)^{-1} \in Im(\sigma)$, para todo $1 \leq s \leq p-1$.

Definimos a seguinte unidade:

$$v = \prod_{s=1}^{p-1} \psi_s(u).$$

Temos que $\psi_s(v) = v$, para todo $1 \leq s \leq p-1$. Assim, se escrevermos v como sendo

$$v = z_0 + \sum_{i=1}^{p-1} z_i \theta_p^i,$$

onde $z_j \in \mathbb{Z}G$, temos:

$$v = \psi_s(v) = z_0 + \sum_{i=1}^{p-1} z_i \theta_p^{si}.$$

Escrevendo $z_j = \sum_{g\in G} a_{j,g} g$, com $a_{j,g} \in \mathbb{Z}$ temos, para todos $g \in G$, $1 \leq s \leq p-1$:

$$a_{0,g} + \sum_{i=1}^{p-1} a_{i,g}\theta_p^i = a_{0,g} + \sum_{i=1}^{p-1} a_{i,g}\theta_p^{si},$$

ou seja, $a_{0,g} + \sum_{i=1}^{p-1} a_{i,g}\theta_p^i$ (que é o coeficiente de g da unidade v) é fixo pela ação do grupo $Gal(\mathbb{Q}(\theta_p)/\mathbb{Q})$, de onde temos, pela correspondência dada pelo Teorema Fundamental da Teoria de Galois, que

$$a_{0,g} + \sum_{i=1}^{p-1} a_{i,g}\theta_p^i \in \mathbb{Q},$$

logo $v \in \mathbb{Z}G \subset \mathbb{Z}(C_p \times G)$, portanto $v \in Im(\sigma)$ (pois temos $v = \sigma(v)$).

Então temos $v \in Im(\sigma)$, $\eta(u)u^{-p} \in Im(\sigma)$ e, para todo $1 \leq s \leq p-1$, temos $u\psi_s(u)^{-1} \in Im(\sigma)$. Com estas informações em mente, temos:

$$Im(\sigma) \ni \prod_{s=1}^{p-1} u\psi_s(u)^{-1} = u^{p-1}v^{-1},$$

como $v, v^{-1} \in Im(\sigma)$, temos $u^{p-1} \in Im(\sigma)$, e como $\eta(u)u^{-p} \in Im(\sigma)$, então temos:

$$u^{-1}\eta(u) \in Im(\sigma).$$

Analogamente temos que:

$$(\eta^{n-1}(u))^{-1}(\eta^n(u)) \in Im(\sigma).$$

No entanto, tomando $E = p^e$ como sendo o expoente de G, temos $\eta^e(u) \equiv 1 \ (mod \ (\theta_p - 1))$, portanto $\eta^e(u) \in ker(\alpha)$ e, pelo Teorema 4.1.6, $\eta^e(u) \in Im(\sigma)$, de onde temos que $\eta^{e-1}(u) \in Im(\sigma)$.

Deste último temos, analogamente, que $\eta^{e-2}(u) \in Im(\sigma)$. Continuado indutivamente, temos $\eta(u) \in Im(\sigma)$ e, portanto, $u \in Im(\sigma)$, como queríamos demonstrar.

□

Assim sendo, se p é primo regular ≤ 67, temos um conjunto de geradores do grupo $U_1\mathbb{Z}[\theta_p](C_p)^n$, utilizando os resultados de (Ferraz, 2009).

Na próxima seção, vamos calcular o núcleo de σ.

4.2 Corolários do Lema de Kümmer

Vamos considerar nesta seção p um número primo regular. Lembramos que a partir do lema de Kümmer, podemos concluir que as unidades de $\mathbb{Z}C_p$ que são congruentes a 1 módulo p são precisamente aquelas que são da forma u^p.

Em 1989, Hoechsmann provou o seguinte :

Teorema 4.2.1. *(Hoechsmann, 1989) Se p é um primo regular ímpar, A é um p-grupo abeliano finito, e u unidade simétrica de aumento 1 em $\mathbb{Z}A$ tal que $u \equiv 1 \ (mod \ p)$, então existe v unidade simétrica de aumento 1 tal que $u = \eta(v)v^{-p}$, onde η é endomorfismo que estende $g \mapsto g^p$, para todo $g \in A$.*

Vamos dar uma outra demonstração para o caso que A é abeliano elementar finito (isto é, para anéis do tipo $\mathbb{Z}C_p \times ... \times C_p$) mais à frente (ver Teorema 4.2.4), e vamos calcular o núcleo de σ (definida como no Teorema 4.1.6) neste caso.

Fixemos as notações: $\mathcal{G}_2 = C_p^{n-1}$ (produto direto de $(n-1)$ cópias de C_p) e $\mathcal{G} = C_p \times \mathcal{G}_2 = \langle h \rangle \times \mathcal{G}_2$. Temos que $\mathcal{G}$ tem $k = p^{n-1} + p^{n-2} + ... + p + 1$ subgrupos cíclicos não triviais, pois cada elemento de $\mathcal{G}$ está contido em um grupo cíclico de ordem p, e todos os subgrupos cíclicos têm apenas o elemento 1 na sua intersecção dois a dois, portanto temos, chamando de k a quantidade de subgrupos cíclicos não triviais, que $(p-1)k+1 = p^n$, donde temos que $k = p^{n-1}+p^{n-2}+...+p+1$. Analogamente, temos que $\mathcal{G}_2$ tem $p^{n-2} + ... + p + 1$ subgrupos cíclicos não triviais. Vamos fixar então $k = p^{n-1} + p^{n-2} + ... + p + 1$ e $k_2 = p^{n-2} + ... + p + 1$.

Temos os seguintes isomorfismos

$$\mathbb{Q}\mathcal{G} \cong \mathbb{Q} \oplus k\mathbb{Q}(\theta_p)$$

$$\mathbb{Q}(\theta_p)\mathcal{G}_2 \cong p^{n-1}\mathbb{Q}(\theta_p).$$

A partir disso, temos que

$$rank(U_1(\mathbb{Z}\mathcal{G}_2)) = rank(U_1(\mathbb{Z}\mathcal{G})) - \frac{p-3}{2}k_2.$$

Sejam $\langle c_i\rangle_{i=1,...,k_2}$ os subgrupos cíclicos não triviais de $\mathcal{G}_2$. Então os subgrupos cíclicos não triviais de $\mathcal{G}$ são precisamente os grupos $\langle h^j c_i\rangle$ e $\langle h\rangle$, com $0 \leq j \leq p-1, 1 \leq i \leq k_2$.

Se $\{u_1(h), ..., u_{\frac{p-3}{2}}(h)\}$ é complemento para $\langle h\rangle$ em $U_1(\mathbb{Z}\langle h\rangle)$, temos por [Hoechsmann e Sehgal, 1986] que o conjunto $\mathcal{B} = \{u_1(h^j c_i), ..., u_{\frac{p-3}{2}}(h^j c_i)\}_{i,j} \cup \{u_1(h), ..., u_{\frac{p-3}{2}}(h)\}$ $(0 \leq j \leq p-1, 1 \leq i \leq k_2)$. gera complemento para $\mathcal{G}$ em $U_1(\mathbb{Z}\mathcal{G})$. Vamos provar que $\mathcal{B}$ é conjunto linearmente independente. Mas precisamos, primeiro, do seguinte resultado:

Teorema 4.2.2. *(Higman, Ayoub) Seja G um grupo abeliano e seja G_0 seu subgrupo de torção. Então:*

$$U(\mathbb{Z}G) = \pm G \times F,$$

onde F é grupo abeliano livre cujo posto é dado do seguinte modo:

$$\frac{1}{2}(|G_0| - 2l + m + 1), \text{ se } G \text{ é finito,}$$

$$0, \text{ se } G_0^4 = 1 \text{ ou } G_0^6 = 1$$

$$|G_0|, \text{ caso contrário,}$$

onde $G_0^i = \{g^i : g \in G_0\}$, m é o número de subgrupos cíclicos de G_0 de ordem 2, l é o número de subgrupos cíclicos de G_0.

A demonstração do lema acima pode ser encontrada em (Karpilovsky, 1983 - Teorema 4.5).

Vamos calcular o posto de F no caso $G = \mathcal{G}$. Neste caso, já sabemos que $l = (p^n - 1)/(p-1) + 1$ (os subgrupos cíclicos de ordem p e o trivial). Temos:

$$rank(F) = \frac{1}{2}\left(p^n - 2\left(\frac{p^n - 1}{p-1} + 1\right) + 1\right) = \frac{1}{2}\left(p^n - 2(1 + p + ... + p^{n-1} + 1) + 1\right) =$$

$$= \frac{1}{2}(p-3)(1 + p + ... + p^{n-1}) = \frac{1}{2}(p-3)(l-1).$$

Assim, como o conjunto $\mathcal{B}$ tem $\frac{1}{2}(p-3)(l-1)$ elementos e é gerador, então é linearmente independente.

Temos o seguinte lema, análogo ao que obtivemos na demonstração do Lema 4.1.3:

Lema 4.2.3. *Se $g \in \mathcal{G}_2$ e $u(c_i) \in U_1(\mathbb{Z}\langle c_i\rangle)$, então $u(c_i)u(\theta_p c_i)...u(\theta_p^{p-1} c_i) = 1$*

Demonstração:

Temos que o elemento $\theta_p^j c_i \in \mathbb{Z}[\theta_p]G$ é levado em cada componente simples (que é isomorfa a $\mathbb{Z}[\theta_p]$) a um inteiro ciclotômico x tal que $x^p = 1$. Portanto, nesta componente, temos que $\theta_p^j c_i \mapsto \theta_p^k$, para certo $0 \leq k \leq p-1$.

Fixamos uma componente simples qualquer. Se para todo j temos que $\theta_p^j c_i \mapsto 1$, então é claro que, nesta componente, temos que $u(c_i)u(\theta_p c_i)...u(\theta_p^{p-1} c_i) \mapsto 1$. Assim sendo, podemos supor que existe j tal que $\theta_p^j c_i \mapsto \theta_p^k$, para certo $0 < k \leq p-1$, neste caso, temos que $u(c_i)u(\theta_p c_i)...u(\theta_p^{p-1} c_i) \mapsto N_{\mathbb{Q}(\theta_p)|\mathbb{Q}}(u(\theta_p^k)) = 1$.

Portanto, em cada componente simples, o produto $u(c_i)u(\theta_p c_i)...u(\theta_p^{p-1} c_i) \mapsto 1$, e isso prova o lema.

□

Com a relação que nós temos entre os postos dos grupos de unidades, e utilizando a mesma notação que utilizamos no teorema 4.1.6, com $G = \mathcal{G}_2$, temos que:

$$ker(\sigma) = \left\langle u_j(c_i)u_j(hc_i)...u_j(h^{p-1}c_i)\right\rangle_{i,j}.$$

Portanto o conjunto dos $u_j(\theta^l c_i)$ com $j = 1, ..., (p-3)/2$, $i = 1, ..., k_2$, $l = 0, ..., p-2$ é linearmente independente e gera um complemento para $\langle \theta_p, \mathcal{G}_2\rangle$ em $U_1(\mathbb{Z}[\theta_p]\mathcal{G}_2)$.

Portanto, utilizando as notações do teorema 4.1.6, se $u \in U_1(\mathbb{Z}[\theta_p]\mathcal{G}_2)$ é tal que $u \in ker(\alpha)$ e $u \in U_1(\mathbb{Z}\mathcal{G}_2)$, então u pode ser escrito como $u = \prod_{i,j} u_j(c_i)^{k_{i,j}}$. Pelo teorema 4.1.6, temos que existe $v \in U_1(\mathbb{Z}\mathcal{G})$ tal que $v \in ker(\pi)$ e $u = \sigma(v)$.

Portanto, temos que existe $w \in ker(\sigma)$ tal que $v = w\prod_{i,j} u_j(c_i)^{k_{i,j}}$. Como $w \in ker(\sigma)$ e $v \in ker(\pi)$, temos imediatamente que $w = \prod_{i,j}\left(u_j(c_i)^{-k_{i,j}/p}u_j(hc_i)^{-k_{i,j}/p}...u_j(h^{p-1}c_i)^{-k_{i,j}/p}\right)$, de onde concluímos que $p|k_{i,j}$, para todos i, j.

Então acabamos de provar o seguinte resultado:

Teorema 4.2.4. *Se p é primo regular e $\pi_p : U_1(\mathbb{Z}C_p \times ... \times C_p) \to U_1(\mathbb{Z}_pC_p \times ... \times C_p)$ é a projeção natural dos coeficientes em $\mathbb{Z}_p$, então $ker(\pi_p) = \{u^p | u \in U_1(\mathbb{Z}C_p \times ... \times C_p)\}$.*

Como aplicação do teorema acima, vamos calcular o grupo de unidades centrais de $\mathbb{Z}G_n$ e $\mathbb{Z}H_n$ definidos no capítulo anterior, para certos valores de p e n (no caso dos grupos do tipo H_n, poderíamos calcular o grupo de unidades centrais para qualquer $n \geq 2$).

4.2.5 Aplicação ao Anel de Grupo $\mathbb{Z}G_n$

Vamos recordar a definição de G_n:
$G_n = \left\langle a, b | a^{p^2} = b^{p^n} = 1, bab^{-1} = a^{p+1}\right\rangle$
E pelo Teorema 3.3.1, temos que o grupo de unidades centrais de aumento 1 de $\mathbb{Z}G_n$ é $W_1 \times W_2$, onde

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

$$W_2 = U_1(\mathbb{Z}Z(G_n)) \cong U_1(\mathbb{Z}C_p),$$

onde $\pi_{p,n} : U_1(\mathbb{Z}(C_p \times C_{p^n})) \to U_1(\mathbb{Z}_p(C_p \times C_{p^n}))$ é a projeção natural, e estamos enxergando o domínio desta função como sendo $U_1(\mathbb{Z}G_n/G_n') = U_1(\mathbb{Z}G_n/\langle a^p\rangle)$, e podemos tomar w como sendo qualquer representante no anel de grupo $\mathbb{Z}G_n$.

Agora vamos tomar $n = 1, p = 5$. Sabemos que $Z(G_n) = \langle a^p\rangle \cong C_p$. Pelo artigo (Ferraz, 2009), temos que $u(b) := b^4 + b - 1$ gera complemento para C_5 em $U_1\mathbb{Z}C_5$. Temos:

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

Pelos teoremas 2.4.1 e 4.2.4, temos que:

$$W_1 = \left\langle 1 + \frac{(w-1)\widehat{a^p}}{p} \mid w = \prod_{i,j} (u(a^i b^j)^{pk_{i,j}}), i, j, k_{i,j} \in \mathbb{Z} \right\rangle$$

4.2.6 Aplicação ao Anel de Grupo $\mathbb{Z}H_n$

Vamos recordar a definição de H_n:

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

E pelo teorema 3.4.1, temos que o grupo de unidades centrais de aumento 1 em $\mathbb{Z}H_n$ é dado por $W_1 \times W_2$, onde

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

$$W_2 = U_1(\mathbb{Z}Z(H_n)) \cong U_1(\mathbb{Z}C_p),$$

onde $\tilde{\pi}_{p,n} : U_1(\mathbb{Z}(C_p)^n) \to U_1(\mathbb{Z}_p(C_p)^n)$ projeta os coeficientes em $\mathbb{Z}_p$.

Analogamente à subseção anterior, considerando $p = 5$ e $n = 2$, vamos tomar $u(b) = b^4 + b - 1$. Então, temos:

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

e também temos, pelo Teorema 4.2.4:

$$W_1 = \left\langle 1 + \frac{(w-1)\widehat{\widehat{a_1}}}{p} \mid w = \prod_{i,j} (u(a_1^i b^j)^{pk_{i,j}}), i, j, k_{i,j} \in \mathbb{Z} \right\rangle$$

Concluímos, assim, este capítulo.

Conclusão

Neste trabalho, fomos capazes de provar teorema estrutural para o grupo de unidades centrais de certos anéis de grupo $\mathbb{Z}G$. Mais precisamente, para aqueles grupos G tais que a soma da classe de conjugação de todo elemento $g \notin G'$ é exatamente $\widehat{G'}g$.

Pudemos aplicar este resultado a algumas classes de anéis de grupo, o que nos permitiu calcular explicitamente o grupo de unidades centrais de alguns anéis de grupo não-comutativos.

Também obtivemos alguns resultados para o grupo de unidades de $\mathbb{Z}[\theta_p]A$ onde A é abeliano finito, especialmente quando A é elementar, e utilizamos algumas propriedades deste anel e um teorema devido a Low, R. para provar um corolário do conhecido lema de Kümmer, sendo este corolário um caso particular do resultado principal de (Hoechsmann, 1989). Isto possibilitou calcular explicitamente o grupo de unidades centrais de todos os anéis de grupo do tipo $\mathbb{Z}H_n$, e calculamos explicitamente o caso em que $p = 5$ e $n = 2$, para exemplificar como fazer isso.

Ficam algumas perguntas para possível investigação futura:

1 - Quais os grupos que satisfazem à hipótese do Teorema 3.1.5 ?

2 - Exibir o grupo de unidades centrais de $\mathbb{Z}C_{p^n,q^m,r}$ quando a ordem de $\overline{r}$ é menor que p^n em $\mathbb{Z}_q$.

3 - No caso em que p não é regular, como calcular o núcleo de $U(\mathbb{Z}C_p) \to U(\mathbb{Z}_pC_p)$?

4 - Calcular o grupo de unidades centrais de um anel de grupo $\mathbb{Z}G$ quando G não é metabeliano (em todos os casos que fizemos, G é metabeliano).

Assim encerramos o texto principal do trabalho.

Bibliografia

[Aleev, 1994] Aleev, R. Z., *Higman's central unit theorem, units of integral group rings and Fibonacci numbers*, Int. J. of Alg. and Comp. 4, 3 (1994), 309-358,

[Aleev e Panina] Aleev, R. Z., Panina, Z., *The units of cyclic groups of order 7 and 9*, Rus. Math. 43, (2000), 80 - 83,

[Ash, 2003] Ash, Robert B., *A Course In Algebraic Number Theory*, Dover Books on Mathematics, 2003.

[Borevich e Shafarevich, 1966] Borevich, Z. I., Shafarevich, I. R., *Number Theory*, Pure and Applied Mathematics, Academic Press (1966)

[Cohn e Livingstone, 1965] Cohn, J. A., Livingstone, D., *On the structure of group algebras*, Canadian Journal of Mathematics, 17 (1965), 583 - 593,

[Ferraz, 2004] Ferraz, R. A., *Simple components and central units in group algebras.* Journal of Algebra, v. 279, n.1, p. 191-203, 2004.

[Ferraz, 2009] Ferraz, R. A., *Units of* $\mathbb{Z}C_p$, Groups, Rings and Group Rings, Contemporary Mathematics - American Mathematical Society, Providence, RI, (2009), v. 499, 107 - 119,

[Ferraz, 2002] Ferraz, R., A., *Subgrupos livres e unidades centrais no grupo de unidades de alguns anéis de grupos*, Universidade de São Paulo, 2002.

[Ferraz e Kitani, 2015] Ferraz, R. A., Kitani, P. M., *Units of* $\mathbb{Z}C_{p^n}$, Communications in Algebra, v. 43, 4936 - 4950.

[Ferraz e Marcuz, 2016] Ferraz, R.A., Marcuz, R., *Units of* $\mathbb{Z}(C_p \times C_2)$ *and* $\mathbb{Z}(C_p \times C_2 \times C_2)$, Communications in Algebra, v. 44, I. 2, (2016) 851 - 872,

[Ferraz e Simón, 2008] Ferraz, R. A., Simón, J. J., *Central units in metacyclic integral group rings*, Communications in Algebra, 36: 3708 - 3722, (2008),

[Ferraz e Simón, 2016] Ferraz, R. A., Simón, J. J., *Central units in* $\mathbb{Z}C_{p,q}$, Communications in Algebra, 44:5, 2264 - 2275 (2016),

[Hoechsmann, 1989] Hoechsmann, K., *Généralization d'un lemme de Kummer*, Canad. Math. Bull. Vol. 32 (4), 1989

[Hoechsmann e Sehgal, 1986] Hoechsmann, K., Sehgal, S. K., *Units in regular elementary abelian group rings*, Arch. Math., Vol. 47, 413 - 417 (1986),

[Hoechsmann, Sehgal, Weiss, 1985] Hoechsmann, K., Sehgal, S., K, Weiss, A., *Cyclotomic units and the unit group of an elementary abelian group ring*, Arch. Math., Vol. 45, 5 - 7 (1985),

[Jespers, Leal e Paques, 2003] Jespers, E., Leal, G., Paques, A., *Central idempotents in the rational group algebra of a finite nilpotent group*, Journal of Algebra and Its Applications Vol. 2, No. 1 (2003) 57-62

[Jespers, Olteanu, del Río e Gelder, 2013] Jespers, E, Olteanu, G., del Río, Á., Gelder, I. V., *Group rings of finite strongly monomial groups: Central units and primitive idempotents*, Journal of Algebra, Volume 387, 99-116, August 2013.

[Karpilovsky, 1983] Karpilovsky, G., *Commutative Group Algebras*, Marcel Dekker, Inc. (1983)

[Lang, 1990] Lang, S., *Cyclotomic Fields I and II*, Combined Second Edition, Springer (1990),

[Low, 2008] Low, R. M., *On the units of the integral group ring* $\mathbb{Z}[G \times C_p]$, Journal of Algebra and Its Applications, vol. 7, no. 3, 393 - 403 (2008).

[Martin, 2010] Martin, Paulo Agozzini. *Grupos, Corpos e Teoria de Galois*. [S.l: s.n.], 2010.

[Polcino e Sehgal, 2002] Polcino Milies, C., Sehgal, S. K., *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.

[Sehgal, 1993] Sehgal, S. K., *Units in Integral Group Rings*, Longman Scientific and Technical, 1993.

[Washington, L. C.] *Introduction to Cyclotomic Fields*, Springer Verlag, New York, 1980.