Subgrupos Livres e Unidades Centrais no Grupo de Unidades de Alguns Anéis de Grupos.

Raul Antonio Ferraz

TESE APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO GRAU
DE
DOUTOR EM MATEMÁTICA

Área de Concentração: **Álgebra**
Orientador: **Prof. Dr. Jairo Zacarias Gonçalves**

Durante este trabalho, o autor teve o apoio financeiro parcial do CNPq e parcial da FAPESP processo 97/13624-8

Março de 2002

Subgrupos Livres e Unidades Centrais no Grupo de Unidades de Alguns Anéis de Grupos

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Raul Antonio Ferraz e aprovada pela comissão julgadora.

São Paulo, 22 de março de 2002.

Banca examinadora:

Prof. Dr. Jairo Zacarias Gonçalves (Orientador)	- IME - USP
Prof. Dr. Francisco César Polcino Milies	- IME - USP
Prof. Dr. Antonio Paques	- IMECC - UNICAMP
Prof. Dr. Guilherme Augusto de La Rocque Leal	- UFRJ
Prof. Dr. Norai Romeu Rocco	- UNB

Dedicada à memória de *Neuza Steiner Ferraz*
(01/09/1933-02/12/2001)

Agradecimentos

A Deus por me dar saúde, e me reconfortar nos momentos mais díficeis.

Ao meu orientador Prof. Dr. Jairo Zacarias Gonçalves pelo excelente trabalho de orientação e pelo apoio, incentivo, paciência e atenção constantes durante o trabalho.

Aos meus pais Thelmo e Neuza (onde quer que esteja) pelo carinho, amor, afeto, dedicação, atenção, ...enfim, por tudo que sempre fizeram por mim.

Aos meus tios Niuza e Luiz, aos meus primos Suzi e Valdir e aos meus demais familiares pelo apoio incentivo amor e carinho que sempre me dedicaram.

Aos meus amigos Patrícia, Mário e Paul pela hospedagem e pela hospitalidade com que me receberam quando permaneci durante 2 meses no Rio de Janeiro.

Aos amigos de área de álgebra, Profa. Dra. Leilá Maria Vasconcelos Figueredo, Profa.Dra. Maria Lúcia Sobral Singer, Prof. Dr. César Polcino Millies, Prof. Dr.Orlando Stanley Juriaans, Prof. Dr. Michael Dokuchaev, Prof. Dr. Arnaldo Mandel, Prof.Dr.Vítor de Oliveira Ferreira, e Osnel Broche Cristo, que juntamente com meu orientador me ouviram com atenção e paciência expor os resultados da minha tese. Em especial ao Osnel e ao Vítor pelo apoio e companheirismo durante os momentos difíceis neste final de ano.

Aos amigos Daniel, Samuel, Liane, Fernando, Irene, José Antonio, Cecília, Pablo, Marcela, Regina, Cibele, Alice, Leandro, Armando, Paulo José, Marco, Claus, Rodrigo, Major, Lúcia, Bárbara, Gláucio, Clézio, Maité, Mário, Gladys, Maria, Sebastião, Lurdinha, Osmar, Antonio, Thierry, Saraiva e demais amigos pela amizade durante o doutorado.

Ao CNPq pelo apoio financeiro durante os 5 primeiros meses de trabalho na elaboração da Tese, e a FAPESP (processo 97/13624-8) pelo apoio financeiro durante os 43 meses subseqüentes.

Abstract

Let $\mathbb{Z}[G]$ be the group ring of the group G over the ring of rational integers $\mathbb{Z}$, and let $U(\mathbb{Z}[G])$ be its group of units. In [**HP**], Hartley and Pickel prove that if G is a finite group then $U(\mathbb{Z}[G])$ contains a free subgroup except when G is an abelian group or a Hamiltonian 2-group.

In [**G1**],[**G2**],[**G3**], and [**G4**] J.Z.Gonçalves study the existence of free subgroups in the groups of units of group algebras. In [**MS**] Sehgal e Marciniak show how to construct free subgroups in $U(\mathbb{Z}[G])$, provided that there exists a non-normal finite subgroup H in G, using a bicyclic unit and its conjugate.

From another direction Dokuchaev e Gonçalves [**DG1**] show that $U(\mathbb{Z}[G])$, with G a torsion group, does not satisfy a semigroup identity, except when G is an abelian group, or a Hamiltonian 2-group. In this proof, they make use of two units u and v, with v a bicyclic unit, and u a Bass cyclic unit that do not satisfy a special type of semi group identity called R-equation. This result lead us to the following questions:

(1) Do u and v generate a free semigroup in $U(\mathbb{Z}[G])$?
(2) Do u and v generate a free group in $U(\mathbb{Z}[G])$?

Let G_0 be the group generated by u and v. In the first chapter of this Thesis we prove

THEOREM. *The group $G_0 = \langle u, v \rangle$ is isomorphic to $A \rtimes C_\infty$ where A is abelian torsion free and C_∞ infinite cyclic.*

And so we conclude that u and v do not generate a free group in $U(\mathbb{Z}[G])$. We show also u and v do not generate a free semigroup.

In the second chapter we modify the bicyclic unit v. And so with this new unit, when $G = D_n$, the dihedral group of $2n$ elements, the group $\langle u, v \rangle$ contains non-abelian free subgroups. Also, in the second chapter, we construct free groups of rank greater than 2 making use of the bicyclic unit v and the generator of order n of D_n.

In the third chapter we characterize the central units of $U_1(\mathbb{Z}[D_n])$, the group of normalized units of $\mathbb{Z}[D_n]$. Using similar techniques we characterize the central units of $U_1(\mathbb{Z}[DC_n])$, where DC_n denotes the dicyclic group of order $4n$.

Finally in the fourth chapter we construct free subgroups in $U(\mathbb{Z}[G])$, G a hamiltonian group containing an element of odd order using only Bass cyclic units.

Introdução

Sejam G um grupo, $\mathbb{Z}$ o anel dos inteiros, e seja $\mathbb{Z}[G]$ o anel de grupo de G com coeficientes em $\mathbb{Z}$. Em [**HP**] Hartley e Pickel mostraram que a menos que G seja abeliano ou 2-Hamiltoniano, o grupo de unidades de $\mathbb{Z}[G]$, $U(\mathbb{Z}[G])$ contém um grupo livre. Denotaremos por $U_1(\mathbb{Z}[G])$ as unidades de $\mathbb{Z}[G]$ de aumento 1.

Em [**G1**],[**G2**],[**G3**], e [**G4**] J.Z.Gonçalves estudou a existência de grupos livres no grupo de unidades de anéis de grupo. Em [**MS**] Marciniak e Sehgal construiram grupos livres em $U(\mathbb{Z}[G])$ a partir de unidades bicíclicas e do anti-automorfismo *. Até o momento este é o único método explícito de se produzirem unidades que gerem um grupo livre.

A partir de uma direção diferente Dokuchaev e Gonçalves [**DG1**] mostraram que $U(\mathbb{Z}[G])$, com G de torção, não satisfaz uma identidade de semigrupo, a menos que G seja abeliano ou 2-Hamiltoniano. Nesta demonstração são construídas duas unidades u e v, com v bicíclica, e u unidade de Bass, que não satisfazem um tipo específico de identidade de semigrupo, chamado equação-R (R-equation). Este resultado nos leva às seguintes questões:

(1) u e v geram um semigrupo livre em $U(\mathbb{Z}[G])$?
(2) u e v geram um grupo livre em $U(\mathbb{Z}[G])$?

No primeiro capítulo mostraremos que o grupo gerado pelas unidades u e v como construídas em [**DG1**], que chamaremos de G_0 é na verdade metabeliano. Além disso provaremos o

TEOREMA. *O grupo $G_0 = \langle u, v\rangle$ é isomorfo a $A \rtimes C_\infty$ onde A é um grupo abeliano livre e C_∞ denota o grupo cíclico infinito.*

Com isto concluimos que u e v não geram um grupo livre em $U(\mathbb{Z}[G])$. Mostraremos ainda que o semigrupo gerado por u e v não é o semigrupo livre.

Contudo, no segundo capítulo modificaremos um pouco a unidade bicíclica v, em relação a unidade cíclica de Bass u e com isso teremos que no caso em que G é o grupo diedral de $2n$ elementos, que denotaremos por D_n, existirão no subgrupo $\langle u, v\rangle$ grupos livres não abelianos. Ainda no segundo capítulo construiremos grupos livres

de posto maior em D_n gerados a partir da unidade bicíclica v e do gerador de ordem n de D_n que denotaremos por x.

Muito se tem estudado em relação ao grupo de unidades de $\mathbb{Z}[D_n]$, onde D_n é o grupo diedral de ordem $2n$.

Em [**HP2**], Hughes e Pearson caraterizam $U_1(\mathbb{Z}[D_3])$ como um subgrupo de matrizes de $GL_2(\mathbb{Z})$. Em [**Polc**], Polcino caracteriza $U_1(\mathbb{Z}[D_4])$ também como subgrupo de $GL_2(\mathbb{Z})$. Na mesma direção temos os trabalhos de Passman e Smith [**PasSmi**] e Fernandes [**Fer**]. Porém há pouca coisa feita no intuito de caracterizar $U_1(\mathbb{Z}[D_n])$ em termos de geradores e relações. Neste sentido temos em [**PS**], um descrição quando $n = 3$. Afim de aprofundar nossos conhecimentos sobre as unidades de $\mathbb{Z}[D_n]$ caracterizamos no terceiro capítulo as unidades centrais de $U_1(\mathbb{Z}[D_n])$, e aproveitando as mesmas técnicas caracterizamos as unidades centrais de $U_1(\mathbb{Z}[DC_n])$, onde DC_n é o grupo dicíclico de ordem $4n$.

É um resultado bastante conhecido em Teoria de Grupos que se todo subgrupo H de um grupo G é normal então ou G é abeliano ou é hamiltoniano, isto é, G é da forma $K_8 \times A \times E$, onde K_8 é o grupo dos quatérnios de ordem 8, A é um grupo abeliano onde todo elemento tem ordem ímpar, e E é um 2-grupo abeliano elementar. Se A for trivial diremos G é 2-hamiltoniano.

Devido a [**HP**] temos que $U(\mathbb{Z}[G])$ não contém grupos livres se e somente se G é abeliano ou 2-hamiltoniano. Se G for hamiltoniano mas não 2-hamiltoniano, teremos que $U(\mathbb{Z}[G])$ contém grupos livres. Contudo não poderemos usar as técnicas de [**MS**] para construir tais grupos, visto que se G não tem subgrupos não normais $U(\mathbb{Z}[G])$ não terá unidades bicíclicas.

No quarto capítulo construiremos grupos livres em $U(\mathbb{Z}[G])$ quando G é um grupo hamiltoniano, não 2-hamiltoniano, usando apenas unidades cíclicas de Bass.

Sumário

CAPíTULO 1

Subgrupos metabelianos em $U(\mathbb{Z}[G])$

1. Considerações iniciais

Nesta primeira seção daremos definições e fixaremos notações que serão usadas durante o desenvolvimento da tese.

Sejam G um grupo, $\mathbb{Z}$ o anel dos inteiros, denotaremos por $\mathbb{Z}[G]$ o anel de grupo de G com coeficientes em $\mathbb{Z}$. Denotaremos por $U(\mathbb{Z}[G])$ seu grupo de unidades. Além disso se R é um anel unitário denotaremos por $U(R)$ o seu grupo de unidades. Se g for um elemento de ordem finita n em G notaremos por $\hat{g}$ o elemento $\sum_{i=0}^{n-1} g^i$.

Definimos por **morfismo de aumento** o morfismo ε de $\mathbb{Z}[G]$ em $\mathbb{Z}$ dado por

$$\varepsilon(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g.$$

Definimos o **ideal de aumento** como sendo o núcleo do morfismo ε. Dizemos que uma unidade u de $\mathbb{Z}[G]$ é **normalizada** se $\varepsilon(u) = 1$, e denotaremos por $U_1(\mathbb{Z}[G])$ o grupo formado por estas unidades.

Definimos a involução $*$ por

$$(\sum_{g\in G} \alpha_g g)^* = \sum_{g\in G} \alpha_g g^{-1}.$$

Diremos que um elemento α pertencente a $\mathbb{Z}[G]$ é **$*$-simétrico,** ou simplesmente **simétrico,** se $\alpha^* = \alpha$.

Se R é um anel e G um grupo notaremos por $\mathcal{Z}(R)$, e $\mathcal{Z}(G)$, o centro do referido anel R e do referido grupo G.

Denotaremos por $\phi(n)$, a cardinalidade do conjunto $\{0 < j < n | \operatorname{mdc}(j,n) = 1\}$, isto é, a conhecida **função ϕ de Euler** . E notaremos por **i** a quantidade imaginária do corpo de números complexos $\mathbb{C}$.

A propósito $\mathbb{C}$ sempre notará o corpo dos números complexos, assim como $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, e $\mathbb{R}$ sempre notarão o conjunto dos números naturais, o anel dos inteiros, o corpo

dos racionais, e o corpo dos números reais respectivamente. Se n for um natural, notaremos por ζ_n a raiz n-ésima da unidade $e^{\frac{2\pi i}{n}}$. Por $\mathbb{Q}[\zeta_n]$, o corpo ciclotômico gerado por ζ_n, e por $\mathbb{Z}[\zeta_n]$ o seu anel de inteiros algébricos.

No decorrer desta tese usaremos com freqüência duas unidades que iremos descrever mais detalhadamente na próxima seção: As unidades Bicíclicas e as unidades Cíclicas de Bass.

2. Unidades bíciclicas e cíclicas de Bass

Seja G um grupo. Vamos aqui definir duas unidades em $\mathbb{Z}[G]$ que usaremos com bastante freqüencia nesta tese.

A primeira unidade é a unidade bíciclica. Sejam h e g pertencentes a G, tais que g tenha ordem finita, digamos n e que h não normalize $\langle g\rangle$ isto é $hgh^{-1} \notin \langle g\rangle$ (equivalentemente: $h^{-1}gh \notin \langle g\rangle$). Denotaremos por $\hat{g}$ o elemento de $\mathbb{Z}[G]$ dado por $1 + g + \cdots + g^{n-1}$. Seja

$$v = 1 + (1 - g)h\hat{g}.$$

PROPOSIÇÃO 1.1. *O elemento $v \in \mathbb{Z}[G]$ construído acima é uma unidade de ordem infinita de $\mathbb{Z}[G]$. Além disto para todo $r \in \mathbb{Z}$ temos $v^r = 1 + r(1 - g)h\hat{g}$.*

DEMONSTRAÇÃO:

Seja $\alpha = v - 1$ Primeiramente vamos mostrar que v é diferente de 1, ou equivalentemente que

$$\alpha = (1 - g)h\hat{g} \neq 0.$$

$$(1 - g)h\hat{g} = h + hg + \cdots + hg^{n-1} - gh - \cdots - ghg^{n-1}.$$

Concluimos então que para termos $\alpha = 0$ teremos de ter para algum k, $0 \leq k \leq n - 1$, $h = ghg^k$, e portanto $h^{-1}gh \in \langle g\rangle$, o que contradiz a escolha de h e de g. Logo v é diferente de 1.

Do fato que $(1 - g)\hat{g} = 0$ segue que $\alpha^2 = 0$ e portanto segue facilmente

$$v(1 - \alpha) = 1 - \alpha^2 = 1.$$

E portanto v é inversível com inversa $v^{-1} = 1 - \alpha$.

Pelo mesmo motivo temos $v^r = 1 + r\alpha = 1 + r(1-g)h\hat{g} \neq 1$, para todo $r \in \mathbb{Z}$. E assim concluimos a demonstração. □

A unidade v construída acima será chamada de **unidade bicíclica** . Vamos agora analisar unidades contidas em subgrupos cíclicos de ordem finita de G. Seja x um elemento de ordem finita digamos n de G e seja o elemento

$$u = (1 + x + \cdots + x^{j-1})^s - k\hat{x}.$$

Onde $\text{mdc}(j,n) = 1$, $1 < j < n-1$, j^s é côngruo a 1 módulo n, e $k = \frac{j^s-1}{n}$. Podemos observar que $k \in \mathbb{Z}$, e que o aumento de u é 1, visto que o aumento de $\hat{x}$ é n. Vamos a seguinte

PROPOSIÇÃO 1.2. *O elemento u construído acima é uma unidade de ordem infinita em $\mathbb{Z}[G]$. Além disso seja t, o único elemento tal que $1 < t < n-1$ e jt é côngruo a 1, módulo n então*

$$u^{-1} = (1 + x^j + x^{2j} + \cdots + x^{j(t-1)})^s - l\hat{x},$$

onde s e j são os mesmos da definição de u e $l = \frac{t^s-1}{n}$.

DEMONSTRAÇÃO:

Vamos mostrar que u é unidade. Seja $u_1 = (1 + x^j + x^{2j} + \cdots + x^{j(t-1)})^s - l\hat{x}$, com j, s, l, e t como definidos no enunciado da proposição.

Temos de mostrar que $uu_1 = 1$. Vale notar que pelo fato de j^s e jt serem côngruos a 1 módulo n temos que t^s é côngruo a 1 módulo n, e portanto l é um número inteiro, e o aumento de u_1 é 1.

Existe $w \in \mathbb{Z}$, tal que $jt = wn + 1$, temos então

$$(1 + x + \cdots + x^{j-1})(1 + x^j + \cdots + x^{j(t-1)}) =$$
$$1 + x + \cdots + x^{j-1} + x^j + \cdots + x^{j-1+j(t-1)} =$$
$$1 + \cdots + x^{jt-1} = 1 + \cdots + x^{wn} = 1 + w\hat{x}.$$

Temos assim

$$(1 + x + \cdots + x^{j-1})^s(1 + x^j + \cdots + x^{j(t-1)})^s =$$
$$(1 + w\hat{x})^s = 1 + S\hat{x},$$

onde S é um número inteiro, visto que para qualquer potência r maior que 1 temos $\hat{x}^r = n^{r-1}\hat{x}$, e $x \cdot \hat{x} = \hat{x}$.

Desta forma fazendo $A = 1 + x + \cdots + x^{j-1}$ e $B = 1 + x^j + \cdots + x^{j(t-1)}$, teremos

$$uu_1 = (A^s - k\hat{x})(B^s - l\hat{x}) = 1 + S\hat{x} - j^s l\hat{x} - t^s k\hat{x} + lkn\hat{x} =$$
$$1 + (S - j^s l - t^s k + lkn)\hat{x}.$$

Mas como u e u_1 tem aumento igual a 1, uu_1 tem aumento 1, e portanto teremos $(S - j^s l - t^s k + lkn)n = 0$, e conseqüentemente $(S - j^s l - t^s k + lkn) = 0$. Logo $uu_1 = 1$.

Vamos agora mostrar que u tem ordem infinita. Seja τ o morfismo de $\mathbb{Z}[\langle x\rangle]$ em $\mathbb{C}$ definido por $\tau(x^r) = \zeta_n^r = e^{\frac{2\pi ri}{n}}$ e estendido por linearidade.

Vamos então calcular $\tau(u)$

$$\tau(u) = \tau((1 + x + \cdots + x^{j-1})^s - k\hat{x}) =$$
$$(1 + \tau(x) + \cdots + \tau(x^{j-1}))^s - k\tau(\hat{x}).$$

Como $\tau(\hat{x}) = 1 + \zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = 0$, temos que

$$\tau(u) = (1 + \zeta_n + \cdots + \zeta_n^{j-1})^s.$$

Se provarmos que $\tau(u)$ tem ordem infinita teremos que u tem ordem infinita, e para mostrarmos que $\tau(u)$ tem ordem infinita basta mostrar que $1 + \zeta_n + \cdots + \zeta_n^{j-1}$, tem ordem infinita em $\mathbb{C}$. E aqui observamos que

$$(1 + \zeta_n + \cdots + \zeta_n^{j-1})(1 - \zeta_n) = 1 - \zeta_n^j,$$

logo $1 + \zeta_n + \cdots + \zeta_n^{j-1} = \frac{1-\zeta_n^j}{1-\zeta_n}$. Vamos, pois, mostrar que $\gamma = \frac{1-\zeta_n^j}{1-\zeta_n}$ tem ordem infinita.

Para tanto, basta demonstrar que seu módulo é diferente de 1. Digamos que $\zeta_n = a_1 + b_1\mathbf{i}$, com a_1 e b_1 em $\mathbb{R}$ e $\zeta_n^j = a_2 + b_2\mathbf{i}$ com a_2 e b_2 em $\mathbb{R}$. Como $|\zeta_n| = |\zeta_n^j| = 1$, temos que $a_1^2 + b_1^2 = a_2^2 + b_2^2 = 1$, e assim temos

$$\left|\frac{1 - \zeta_n^j}{1 - \zeta_n}\right|^2 = \frac{|1 - \zeta_n^j|^2}{|1 - \zeta_n|^2} =$$
$$\frac{(1 - a_1 - b_1\mathbf{i})(1 - a_1 + b_1\mathbf{i})}{(1 - a_2 - b_2\mathbf{i})(1 - a_2 + b_2\mathbf{i})} = \frac{1 + a_1^2 + b_1^2 - 2a_1}{1 + a_2^2 + b_2^2 - 2a_2} = \frac{2 - 2a_1}{2 - 2a_2} = \frac{1 - a_1}{1 - a_2}.$$

Donde concluimos que $|\gamma| = 1$ somente se $a_1 = a_2$. Mas como $a_1^2 + b_1^2 = a_2^2 + b_2^2$, teríamos $b_2 = \pm b_1$ e portanto ou $\zeta_n^j = \zeta_n$, e portanto $j = 1$, ou $\zeta_n = \overline{\zeta_n} = \zeta_n^{n-1}$ e portanto $j = n - 1$, casos descartados na construção de u, e portanto concluimos a demonstração. □

Se $s = \phi(n)$, temos $j^{\phi(n)}$ côngruo a 1 módulo n, e portanto podemos construir a unidade

$$u = (1 + x + \cdots + x^{j-1})^{\phi(n)} - k\hat{x},$$

onde $k = \frac{j^{\phi(n)}-1}{n}$. Diremos nesta situação que u é uma **unidade cíclica de Bass.**Se s for diferente de $\phi(n)$ diremos que u é uma **unidade cíclica de Bass modificada.**

Além disso temos que se j for igual a 1 ou a $n-1$ o elemento

$$u = (1 + x + \cdots + x^{j-1})^{s} - k\hat{x},$$

como construído acima será uma unidade trivial de $\mathbb{Z}[G]$. De fato, se $j = 1$, temos que $u = 1$. Vamos então ao caso $j = n - 1$. Se $n = 2$, temos $1 = n - 1$. Portanto, podemos supor n diferente de 2. E claramente se $(n-1)^s$ é côngruo a 1 módulo n, com $n > 2$ temos que s é par. Com estas considerações temos

$$u = (1 + x + \cdots + x^{n-2})^{s} - k\hat{x} = (\hat{x} - x^{n-1})^{s} - k\hat{x}.$$

Temos $x\hat{x} = \hat{x}$, e $\hat{x}^r = n^{r-1}\hat{x}$, para todo natural não nulo r. Segue daí que para algum $R \in \mathbb{Z}$,

$$u = R\hat{x} + (-x)^{(n-1)s} - k\hat{x} = x^{(n-1)s} + (R - k)\hat{x}.$$

E por construção u tem aumento 1, logo $1 + (R-k)n = 1$, e temos portanto $R - k = 0$, e portanto $u = x^{(n-1)s}$.

OBSERVAÇÃO 1.3. *Para podermos construir uma unidade cíclica de Bass (ou de Bass modificada), precisamos de um número j primo com n, tal que $1 < j < n-1$. Portanto precisamos que existam pelo menos 3 elementos menores que n, relativamente primos com n. Ou seja precisamos $\phi(n) \geq 3$. Logo se $n = 1, 2, 3, 4$, ou 6, não poderemos construir unidades cíclicas de Bass (nem cíclicas de Bass modificadas) a partir do elemento x.*

3. O grupo G_0

Seja G um grupo e seja $\mathbb{Z}[G]$ o anel de inteiros sobre este grupo. Suponha que existam g e h neste grupo G tais que h não normalize $\langle g \rangle$, e que a ordem de g, que denotaremos por n seja igual a 5 ou maior que 6.

Seja a unidade bicíclica

$$v = 1 + (1 - g)h\hat{g}$$

E a unidade cíclica de Bass

$$u = (1 + g + \cdots + g^{j_0-1})^{\phi(n)} - k_0\hat{g}.$$

com k_0 e j_0 nas condições da proposição 1.2.

Em [DG1] Gonçalves e Dokuchaev estudaram o subgrupo G_0 de $U_1(\mathbb{Z}[G])$ gerado pelas unidades v e u construídas acima. Neste artigo os autores demonstram o seguinte

TEOREMA 1.4. *O subgrupo G_0, gerado pelas unidades u e v como construídas acima não satisfaz a nenhuma identidade de semi-grupo.*

Tendo em vista este teorema ficam as questões:

O grupo G_0 é livre gerado livremente por u e v?

Os elementos u e v geram um semigrupo livre ?

Demonstraremos nesta seção que para qualquer grupo G e quaisquer elementos u e v construídos como acima o subgrupo G_0 de $U(\mathbb{Z}[G])$ é metabeliano e portanto u e v não geram um grupo livre. Também demonstraremos que u e v não geram um semigrupo livre em $U_1(\mathbb{Z}[G])$.

Primeiramente vale lembrar que como o aumento de u é 1, $\hat{g}u = u\hat{g} = \hat{g}$, e que daí temos $\hat{g}u^j = u^j\hat{g} = \hat{g}$, para j em $\mathbb{Z}$. Portanto

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

E do fato que $v^k = 1 + k(1-g)h\hat{g}$, para k inteiro, temos

$$u^j v^k u^{-j} = 1 + ku^j(1-g)h\hat{g}$$

TEOREMA 1.5. *Seja G um grupo finito, e seja $\mathbb{Z}[G]$, o anel de grupo de G sobre o anel dos inteiros. Suponha que em G existam dois elementos g e h com as condições acimas citadas, e que portanto dêem origem às unidades u e v construídas como acima em $U(\mathbb{Z}[G])$. Então o subgrupo $G_0 = \langle u, v\rangle$ é um subgrupo metabeliano de $U(\mathbb{Z}[G])$.*

DEMONSTRAÇÃO:

Basta mostrar que G_0 possui um subgrupo abeliano A normal, tal que $\frac{G_0}{A}$ também é abeliano. Tomemos $A = \langle u^j v u^{-j} | j \in \mathbb{Z}\rangle$. A é claramente um subgrupo normal de G_0. Vamos mostrar que A é abeliano. Para tanto basta mostrar que os geradores de A comutam. Como vimos acima temos:

$$u^j v u^{-j} = 1 + u^j(1-g)h\hat{g}.$$

Assim para 2 geradores arbitrários de A, $u^{j_1} v u^{-j_1}$, e $u^{j_2} v u^{-j_2}$, temos

$$u^{j_1} v u^{-j_1} \cdot u^{j_2} v u^{-j_2} = (1 + u^{j_1}(1-g)h\hat{g})(1 + u^{j_2}(1-g)h\hat{g}) =$$
$$(1 + (u^{j_1} + u^{j_2})(1-g)h\hat{g}) = u^{j_2} v u^{-j_2} \cdot u^{j_1} v u^{-j_1}.$$

Donde concluimos que A é abeliano. Do fato de $v \in A$, temos que $\langle A, u\rangle = G_0$. Logo $\frac{G_0}{A} = \langle \overline{u}\rangle$ é um grupo cíclico, portanto abeliano. Logo G_0 é metabeliano. □

Usando a equação $u^j v^k u^{-j} = 1 + k u^j (1-g)h\hat{g}$, com j e k inteiros, podemos demonstrar a seguinte

PROPOSIÇÃO 1.6. *O subgrupo $A = \langle u^j v u^{-j} | j \in \mathbb{Z}\rangle$ de G_0 é livre de torção.*

DEMONSTRAÇÃO.

Para facilitar a notação vamos notar por v_j o elemento $u^j v u^{-j}$. Seja agora $a \in A$, $a = {v_{j_1}}^{k_1} \cdots {v_{j_s}}^{k_s}$, com $a \neq 1$. Temos

$$a = 1 + (k_1 u^{j_1} + \cdots + k_s u^{j_s})(1-g)h\hat{g}.$$

Se $a \neq 1$ então

$$(k_1 u^{j_1} + \cdots + k_s u^{j_s})(1-g)h\hat{g} \neq 0,$$

assim temos para todo $m \in \mathbb{Z}, m \neq 0$

$$m(k_1 u^{j_1} + \cdots + k_s u^{j_s})(1-g)h\hat{g} \neq 0.$$

Logo para $m \neq 0$ temos

$$a^m = {v_{j_1}}^{mk_1} \cdots {v_{j_s}}^{mk_s} = 1 + m(k_1 u^{j_1} + \cdots + k_s u^{j_s})(g-1)h\hat{g} \neq 1.$$

E portanto A é livre de torção. □

Vamos mostrar agora que G_0 é livre de torção.

PROPOSIÇÃO 1.7. *O grupo G_0 é o produto semi-direto de A por $\langle u\rangle$, logo $\frac{G_0}{A} \simeq \langle u\rangle$. Por conseqüência temos que G_0 é livre de torção.*

DEMONSTRAÇÃO:

A é normal em G_0. Como $G_0 = \langle A, u\rangle$ e A é normal em G_0, temos $G_0 = A \cdot \langle u\rangle$. Basta mostrar portanto, que $A \cap \langle u\rangle = 1$. Para isto tomemos $a \in A \cap \langle u\rangle$. Como $a \in A$, a é da forma

$$a = 1 + (k_1 u^{s_1} + \cdots + k_t u^{s_t})(1-g)h\hat{g},$$

com k_i's e s_i's pertencentes a $\mathbb{Z}$. Como u tem suporte em $\langle g \rangle$ temos que $a-1$ tem o suporte no conjunto H,

$$H = \{g^i h g^j | i, j \in \mathbb{Z}\}.$$

Por outro lado se $a \in \langle u \rangle$, a, e conseqüentemente $a-1$ tem suporte em $\langle g \rangle$. Vamos mostrar que

$$H \cap \langle g \rangle = \emptyset.$$

De fato, se supormos que $g^i h g^j = g^r$, com $i, j, r \in \mathbb{Z}$ teremos $h = g^{r-i-j}$, e portanto $h \in \langle g \rangle$, o que por construção é absurdo. Logo concluimos que $H \cap \langle g \rangle = \emptyset$. Assim temos que o suporte de $a-1$ é vazio, e portanto $a = 1$. Assim

$$G_0 = A \rtimes \langle u \rangle,$$

e claro, $\frac{G_0}{A} \simeq \langle u \rangle$.

Para obtermos que G_0 é livre de torção basta tomarmos um elemento $w \in G_0$ com ordem finita. Seja f a aplicação canônica de G_0 em $\frac{G_0}{A}$. Como w é de torção temos que $f(w)$ também o é, mas como $\frac{G_0}{A} \simeq \langle u \rangle$, e $\langle u \rangle$ é livre de torção temos $f(w) = 1$, e portanto $w \in A$. Pela proposição anterior A é livre de torção, logo $w = 1$. Portanto G_0 é livre de torção. □

Vamos agora caracterizar melhor o grupo A, e conseqüentemente o grupo G_0. Antes faremos dois lemas auxiliares.

LEMA 1.8. *Seja O_k um anel de inteiros algébricos, digamos com corpo de frações K extensão algébrica de $\mathbb{Q}$. Se μ é uma unidade de O_k então existe um polinômio mônico minimal $p \in \mathbb{Z}[x]$ com coeficiente independente ± 1 tal que $p(\mu) = 0$.*

DEMONSTRAÇÃO:

Como μ é inteiro algébrico, é conhecido o fato que o polinômio minimal mônico satisfeito por μ em $\mathbb{Q}[x]$, que chamaremos p tem coeficientes em $\mathbb{Z}[x]$, digamos $p(x) = a_m x^m + \cdots + a_0$, com $a_m = 1$ e $a_i \in \mathbb{Z}$, para todo i. Vamos mostrar que $a_0 = \pm 1$. Como $p(\mu) = 0$ temos:

$$\mu^m + \cdots + a_1 \mu + a_0 = 0.$$

Se multiplicarmos a equação acima por μ^{-m} e chamarmos $\omega = u^{-1}$ teremos:

$$1 + a_{m-1}\omega + \cdots + a_1\omega^{m-1} + a_0\omega^m = 0$$

Se existisse um polinômio q em $\mathbb{Q}[x]$ de grau menor que m tal que $q(\omega) = 0$, usando raciocínio análogo ao acima teríamos um polinômio $q_1(x)$, de mesmo grau de q tal que $q_1(\mu) = 0$. Absurdo pois p é o polinômio mônico minimal de μ. Logo concluimos que $p_1(x) = 1 + a_{m-1}x + \cdots + a_1x^{m-1} + a_0x^m$ é um polinômio minimal que satisfaz $p_1(\omega) = 0$. Ora ω também é inteiro algébrico, logo o polinômio mônico minimal que ω satisfaz em $\mathbb{Q}[x]$ tem coeficientes inteiros e o mesmo grau de p_1. Assim como o coeficiente independente de p_1 é 1 temos que o coeficiente dominante de p_1 será uma unidade de $\mathbb{Z}$, isto é $a_0 = \pm 1$. □

LEMA 1.9. *A unidade cíclica de Bass u construída acima satisfaz um polinômio mônico $p(x)$ em $\mathbb{Z}[x]$, que tem o coeficiente independente igual a ± 1.*

DEMONSTRAÇÃO:

Seja ψ a inclusão canônica de $\mathbb{Z}[\langle g\rangle]$ em $\bigoplus_{d|n} \mathbb{Z}[\zeta_d]$, que leva g em

$$\psi(g) = (1, \zeta_{d_2}, \ldots, \zeta_n),$$

onde d_i são os divisores de n (n é a ordem de g), e ζ_{d_i} são as raizes d-ésimas primitivas da unidade.

Seja ψ_{d_i} a composta de ψ com a projeção canônica π_{d_i} de $\bigoplus_{d|n} \mathbb{Z}[\zeta_d]$ em $\mathbb{Z}[\zeta_{d_i}]$.

Claramente $\psi_{d_i}(u)$ é inversível em $\mathbb{Z}[\zeta_{d_i}]$ para cada d_i, e como $\mathbb{Z}[\zeta_{d_i}]$ é um anel de inteiro algébricos, temos pelo lema anterior que $\psi_{d_i}(u)$ satisfaz um polinômio mônico $p_{d_i}(x)$ com coeficiente independente igual a ± 1 em $\mathbb{Z}[x]$.

Se tomarmos $p(x) = \prod_{d|n} p_d(x)$ teremos que $p(u) = 0$, com p polinômio mônico em $\mathbb{Z}[x]$ e com coeficiente independente igual a ± 1. □

Notaremos por C_∞ o grupo cíclico infinito, e por C_∞^m o produto direto de m cópias de C_∞, isto é

$$C_\infty^m = \underbrace{C_\infty \times \cdots \times C_\infty}_{m \text{ vezes}}.$$

Vamos agora ao seguinte

TEOREMA 1.10. *O subgrupo A de G_0, descrito acima, é finitamente gerado e portanto é abeliano livre. Isto é $A = C_\infty^m$, para algum m natural. Conseqüentemente*

$$G_0 \simeq C_\infty^m \rtimes C_\infty.$$

DEMONSTRAÇÃO:

Voltaremos a utilizar aqui a notação $v_i = u^i v u^{-i}$. Pelo lema 1.9 temos que u satisfaz um polinômio mônico $p(x)$ em $\mathbb{Z}[x]$ tal que $p(x)$ tem coeficiente independente igual a ± 1.

Digamos que p tenha grau s. Então

$$u^s = a_{s-1}u^{s-1} + a_{s-2}u^{s-2} + \cdots + a_1 u + a_0.$$

Temos portanto que

$$v_s = u^s v u^{-s} = 1 + u^s(1-g)h\hat{g} =$$
$$1 + (a_{s-1}u^{s-1} + a_{s-2}u^{s-2} + \cdots + a_1 u + a_0)(1-g)h\hat{g} =$$
$$u^{s-1}v^{a_{s-1}}u^{1-s}u^{s-2}v^{a_{s-2}}u^{-(s-2)}\cdots uv^{a_1}u^{-1}v^{a_0} =$$
$$v_{s-1}^{a_{s-1}}v_{s-2}^{a_{s-2}}\cdots v_1^{a_1}v^{a_0}.$$

Assim temos $v_s \in A_0 = \langle v_{s-1}, v_{s-2}, \ldots, v_1, v_0\rangle$, Vamos agora usar indução para provar que para $t > s$, temos $v_t \in A_0$. Vamos supor que para todo t', $0 \leq t' < t$, $v_{t'} \in A_0$. Temos

$$v_t = u^t v u^{-t} = 1 + u^t(1-g)h\hat{g}.$$

Agora temos

$$u^t = u^{t-s}u^s = u^{t-s}(a_{s-1}u^{s-1} + a_{s-2}u^{s-2} + \cdots + a_1 u + a_0) =$$
$$= a_{s-1}u^{t-1} + a_{s-2}u^{t-2} + \cdots + a_1 u^{t-s+1} + a_0 u^{t-s}.$$

E assim

$$v_t = 1 + (a_{s-1}u^{t-1} + a_{s-2}u^{t-2} + \cdots + a_1 u^{t-s+1} + a_0 u^{t-s})(1-g)h\hat{g} =$$
$$= v_{t-1}^{a_{s-1}}v_{t-2}^{a_{s-2}}\cdots v_{t-s+1}^{a_1}v_{t-s}^{a_0}.$$

Pela hipótese de indução temos que $v_{t-1}, \ldots, v_{t-s}$, pertencem a A_0. Logo v_t pertence a A_0.

Seja agora $v_{-1} = u^{-1}vu$.

$$u^{s-1} = a_{s-1}u^{s-2} + a_{s-2}u^{s-3} + \cdots + a_1 + a_0 u^{-1}.$$

Como $a_0 = \pm 1$, temos

$$u^{-1} = \pm u^{s-1} \mp a_{s-1}u^{s-2} \mp a_{s-2}u^{s-3} \mp \cdots \mp a_1,$$

e portanto concluimos de forma análoga ao caso anterior, que $u^{-1}vu$ pertence a $A_0 = \langle v_{s-1}, v_{s-2}, \ldots, v_1, v_0\rangle$.

Por um argumento de indução temos que $u^J v u^{-J}$ pertence a A_0, para todo $J < 0$. Logo concluimos que $A = A_0$. Como A é livre de torção e finitamente gerado A é abeliano livre de posto m para algum m natural.

Tendo em vista os resultados anteriores podemos concluir que

$$G_0 \simeq C_\infty^m \rtimes C_\infty. \ \square$$

Vale ressaltar aqui que estamos provando apenas que $m \leq s$, e não a igualdade. Usaremos este resultado para demonstrar o seguinte

TEOREMA 1.11. *Sejam G um grupo, $\mathbb{Z}[G]$ o anel de inteiros sobre G, u e v construídas como acima. Então u e v não geram um semigrupo livre em $U(\mathbb{Z}[G])$, independentemente da escolha de G, dos elementos $h, g \in G$ e do inteiro j_0, utilizados na construção de u e v.*

DEMONSTRAÇÃO

Seja $v_j = u^j v u^{-j}$. Como vimos no teorema 1.10 para algum s, teremos

$$v_s = v_0^{r_0} v_1^{r_1} \cdots v_{s-1}^{r_{s-1}}.$$

Sejam $0 \leq i_1 < i_2 < \cdots < i_m < s$, todos os índices para os quais r_{i_k} é positivo, e $0 \leq j_1 < j_2 < \cdots < j_l < s$, todos os índices para os quais r_{j_k} é negativo.

Usaremos a notação $h_k = r_{i_k}$, para k entre 1 e m, e $t_k = -r_{j_k}$ para k entre 1 e l. Vale notar que os h_k´s e os t_k´s são positivos. Teremos então

$$v_{j_1}^{t_1} \cdots v_{j_l}^{t_l} v_s = v_{i_1}^{h_1} \cdots v_{i_m}^{h_m}.$$

Escrevendo cada v_i como $u^i v u^{-i}$ teremos

$$u^{j_1} v^{t_1} u^{j_2 - j_1} \cdots u^{j_l - j_{l-1}} v^{t_l} u^{s - j_l} v u^{-s} = u^{i_1} v^{h_1} u^{i_2 - i_1} \cdots u^{i_m - i_{m-1}} v^{h_m} u^{-i_m}.$$

Multiplicando os dois lados a direita por u^s teremos

$$u^{j_1} v^{t_1} u^{j_2 - j_1} \cdots u^{j_l - j_{l-1}} v^{t_l} u^{s - j_l} v = u^{i_1} v^{h_1} u^{i_2 - i_1} \cdots u^{i_m - i_{m-1}} v^{h_m} u^{s - i_m}.$$

Por construção temos que para cada k, $j_k - j_{k-1} > 0$ e cada $i_k - i_{k-1} > 0$. Além disso s é maior que i_m e que j_l, e portanto $s - i_m > 0$, e $s - j_l > 0$. E como citado anteriormente os t_k´s e os h_k´s são positivos. Tendo isto em vista temos que u e v satisfazem a igualdade não trivial de semi-grupo

$$x^{j_1} y^{t_1} x^{j_2 - j_1} \cdots x^{j_l - j_{l-1}} y^{t_l} x^{s - j_l} y = x^{i_1} y^{h_1} x^{i_2 - i_1} \cdots x^{i_m - i_{m-1}} y^{h_m} x^{s - i_m}$$

e portanto não geram um semi grupo livre em $U(\mathbb{Z}[G])$. $\square$

CAPíTULO 2

Grupos livres em $U(\mathbb{Z}[D_n])$

No primeiro capítulo trabalhamos com uma unidade cíclica de Bass u e uma unidade bicíclica v, com $u \in \mathbb{Z}[\langle g \rangle]$ e v da forma $1 + (1-g)h\hat{g}$, com $hgh^{-1} \notin \langle g \rangle$. E concluimos que o grupo gerado por u e v não continha subgrupos livres.

Neste próximo capítulo trabalharemos com uma unidade cíclica de Bass, (ou cíclica de Bass modificada), u, que será gerada a partir do grupo $\langle x \rangle$, e com uma unidade bicíclica v, da forma $1+(1-y)x\hat{y}$. Isto é o elemento que gera a unidade cíclica de Bass, está agora no "meio"e não nas pontas do termo $(1-y)x\hat{y}$. Mostraremos que quando G é o grupo diedral de ordem $2n$ que denotaremos por D_n, o grupo gerado por $\langle u, v \rangle$ contém um subgrupo livre.

1. O grupo de Möbius e o morfismo φ

Nesta seção introduziremos o grupo de Möbius $\mathcal{M}$, e com ele o morfismo φ que será de grande importância na demonstração do principal teorema do capítulo.

Seja $\mathbb{C}$ o corpo dos números complexos, e seja $\mathcal{M}$ o grupo das funções de $\mathbb{C} \cup \{\infty\}$ em $\mathbb{C} \cup \{\infty\}$ que podem ser escritas como

$$f(z) = \frac{az+b}{cz+d},$$

com a, b, c, e d pertencentes a $\mathbb{C}$, e $ad - bc \neq 0$, com a operação de grupo dada pela composição de funções.

Com a hipótese que $ad - bc \neq 0$ temos que de fato cada f é inversível e o grupo $\mathcal{M}$ está bem definido. Denominaremos tal grupo como **grupo de Möbius** .

Seja agora $GL_2(\mathbb{C})$ o grupo das matrizes 2×2 inversíveis sobre $\mathbb{C}$.

PROPOSIÇÃO 2.1. *A função* Υ *de* $GL_2(\mathbb{C})$ *em* $\mathcal{M}$ *dada por*

$$\Upsilon \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} (z) = \frac{x_{11}z + x_{12}}{x_{21}z + x_{22}}$$

é um morfismo sobrejetor de grupos. Além disso o núcleo de Υ *é igual ao centro de* $GL_2(\mathbb{C})$. *Temos portanto que*

$$\mathcal{M} \simeq \frac{GL_2(\mathbb{C})}{\mathcal{Z}(GL_2(\mathbb{C}))} \simeq PGL_2(\mathbb{C}).$$

DEMONSTRAÇÃO: Ver [**Ahl**], página 76.

Seja D_n o grupo diedral de $2n$ elementos

$$\left\langle x, y | x^n = 1, y^2 = 1, yxy^{-1} = x^{-1} \right\rangle.$$

Vamos agora construir um morfismo que relacionará o grupo de unidades $U(\mathbb{Z}[D_n])$ do anel $\mathbb{Z}[D_n]$ com o grupo $\mathcal{M}$ definido acima. Para isto construiremos um morfismo σ entre $Z[D_n]$ e $M_2(\mathbb{C})$, que por sua vez está relacionado com o morfismo τ que construiremos abaixo.

Seja $\langle x \rangle \subseteq D_n$ o grupo cíclico de ordem n contido em D_n Seja $\zeta_n \in \mathbb{C}$, $\zeta_n = e^{\frac{2\pi i}{n}}$. Denotaremos por τ o morfismo de $\mathbb{Z}[\langle x \rangle]$ em $\mathbb{C}$ definido da seguinte forma

$$\tau(x) = \zeta_n,$$

estendido por linearidade a $\mathbb{Z}[C_n]$. Seja agora o morfismo de grupos σ de D_n em $GL_2(\mathbb{C})$ dado por:

$$\sigma(x) = M_x = \begin{pmatrix} \tau(x) & 0 \\ 0 & \tau(x)^{-1} \end{pmatrix},$$

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

Como $\tau(x)^n = 1$ temos facilmente que $M_x^n = 1$, $M_y^2 = 1$, e que $M_y M_x M_y^{-1} = M_x^{-1}$, e que portanto σ é morfismo de grupos. Podemos estender então σ a um morfismo de anéis entre $\mathbb{Z}[D_n]$ e $M_2(\mathbb{C})$. Vale notar que

$$\sigma(x^k y) = \begin{pmatrix} 0 & \tau(x)^k \\ \tau(x)^{-k} & 0 \end{pmatrix}$$

e

$$\sigma(x^l) = \begin{pmatrix} \tau(x)^l & 0 \\ 0 & \tau(x)^{-l} \end{pmatrix},$$

com k e l inteiros. Assim seja w um elemento de $\mathbb{Z}[D_n]$ digamos $w = \beta + \gamma y$, onde β e γ pertencem a $\mathbb{Z}[\langle x \rangle]$, e seja $*$ a involução que leva x em x^{-1} estendida a $\mathbb{Z}[\langle x \rangle]$, teremos

$$\sigma(w) = \sigma(\beta + \gamma y) = \begin{pmatrix} \tau(\beta) & \tau(\gamma) \\ \tau(\gamma^*) & \tau(\beta^*) \end{pmatrix}.$$

Além disso como $\zeta_n^{-1} = \overline{\zeta_n}$, onde $^-$ denota a conjugação em $\mathbb{C}$ e $^-$ é $\mathbb{Z}$-linear temos que $\tau(\delta^*) = \overline{\tau(\delta)}$ para todo $\delta \in \mathbb{Z}[\langle x \rangle]$, e portanto temos

$$\sigma(w) = \sigma(\beta + \gamma y) = \begin{pmatrix} \tau(\beta) & \tau(\gamma) \\ \overline{\tau(\gamma)} & \overline{\tau(\beta)} \end{pmatrix}.$$

Vale notar que σ restrita a $U(\mathbb{Z}[D_n])$ tem imagem em $GL_2(\mathbb{C})$ e que portanto podemos definir o morfismo $\varphi = \Upsilon \circ \sigma$ de $U(\mathbb{Z}[D_n])$ em $\mathcal{M}$. Tendo em vista as observações anteriores teremos que se $w = \beta + \gamma y$ pertencer a $U(\mathbb{Z}[D_n])$, teremos

$$\varphi(w)z = \Upsilon \begin{pmatrix} \tau(\beta) & \tau(\gamma) \\ \overline{\tau(\gamma)} & \overline{\tau(\beta)} \end{pmatrix}(z) = \frac{\tau(\beta)z + \tau(\gamma)}{\overline{\tau(\gamma)}z + \overline{\tau(\beta)}}.$$

A função φ definida acima ocupará posição central no teorema principal da seção. Podemos notar que a imagem de φ em $\mathcal{M}$ é composta por elementos da forma

$$f(z) = \frac{az + b}{\overline{b}z + \overline{a}},$$

com a e b elementos de $\mathbb{C}$. Motivados por este fato, faremos aqui a seguinte

PROPOSIÇÃO 2.2. *Sejam* $S^1 = \{z \in \mathbb{C} | |z| = 1\}$ *e* $f(z)$ *uma aplicação de Möbius da forma*

$$f(z) = \frac{az + b}{\overline{b}z + \overline{a}},$$

com a *e* b *pertencentes a* $\mathbb{C}$. *Então temos* $f(S^1) = S^1$, *isto é se* z *pertencente a* $\mathbb{C}$ *tem módulo* 1, *então* $f(z)$ *terá módulo* 1.

DEMONSTRAÇÃO:

Basta demonstrar que $|z| = 1$ implica $|f(z)| = 1$, ou equivalentemente que $|z|^2 = z\bar{z} = 1$ implica $|f(z)|^2 = f(z)\overline{f(z)} = 1$.

$$f(z)\overline{f(z)} = \left(\frac{az + b}{\overline{b}z + \overline{a}}\right)\left(\frac{\overline{a}z + \overline{b}}{b\overline{z} + a}\right) =$$

$$\frac{|a|^2|z|^2 + a\bar{b}z + b\overline{az} + |b|^2}{|b|^2|z|^2 + \bar{b}az + \bar{a}b\bar{z} + |a|^2} =$$
$$\frac{|a|^2 + a\bar{b}z + b\overline{az} + |b|^2}{|b|^2 + \bar{b}az + \bar{a}b\bar{z} + |a|^2} = 1.\square$$

2. Unidades Cíclicas de Bass não centrais em $U(\mathbb{Z}[D_n])$

Nesta seção estudaremos quando o grupo de unidades de $\mathbb{Z}[D_n]$ contém unidades cíclicas de Bass não centrais. Quando não as contiver como construiremos unidades cíclicas de Bass modificadas não centrais.

OBSERVAÇÃO 2.3. *Um elemento ω pertencente a $\mathbb{Z}[\langle x\rangle]$ será central em $\mathbb{Z}[D_n]$, se e somente se comutar com y. Como $yxy^{-1} = x^{-1}$, temos a igualdade $y\omega y^{-1} = \omega^*$, para todo ω em $\mathbb{Z}[\langle x\rangle]$. Logo concluimos que ω será central em $\mathbb{Z}[D_n]$, se e somente se ω for igual a ω^*.*

Motivados por esta observação faremos o seguinte lema

LEMA 2.4. *Seja $u_s = (1 + x + \cdots + x^{j-1})^s - k\hat{x}$ uma unidade cíclica de Bass ou cíclica de Bass modificada. Temos*

$$u_s^* = x^{(1-j)s}u_s.$$

DEMONSTRAÇÃO: Se notarmos que $\hat{x}^* = \hat{x}$, e $x^\delta k\hat{x} = k\hat{x}$, para todo δ inteiro temos

$$u_s^* = (1 + x^{-1} + \cdots + x^{1-j})^s - k\hat{x} =$$
$$[x^{1-j}(1 + x + \cdots + x^{j-1})]^s - k\hat{x} =$$
$$x^{(1-j)s}[(1 + x + \cdots + x^{j-1})^s - k\hat{x}] = x^{(1-j)s}u_s \ \square$$

Vamos agora a uma proposição que nos garante a existência de unidades cíclicas de Bass que não são centrais, quando n é ímpar.

PROPOSIÇÃO 2.5. *Sejam n um inteiro ímpar maior ou igual a 5, D_n o grupo diedral de $2n$ elementos, e x um elemento de ordem n em D_n. A unidade cíclica de Bass $u_2 = (1 + x)^{\phi(n)} - k\hat{x}$ é não central em $U_1(\mathbb{Z}[D_n])$, onde k denota $\frac{2^{\phi(n)}-1}{n}$.*

DEMONSTRAÇÃO:

Pela observação 2.3 basta mostrar que $u_2 \neq u_2^*$. Pelo lema 2.4 temos $u_2^* = x^{-\phi(n)}u_2$. Ora se $u_2 = u_2^*$ teríamos

$$x^{-\phi(n)}u_2 = u_2.$$

Como u_2 é inversível, teríamos $x^{-\phi(n)} = 1$, o que implicaria que n divide $\phi(n)$. Absurdo, pois $n > \phi(n)$. Logo u_2 não é central em $U_1(\mathbb{Z}[D_n])$ □

Vamos agora demonstrar que existem unidades cíclicas de Bass não centrais em D_n, mesmo com n par, desde que n não seja uma potência de 2.

PROPOSIÇÃO 2.6. *Seja $n = 2^s r$, com r um número ímpar maior que 1, s maior ou igual a 1 e $n \neq 6$. Então existe uma unidade cíclica de Bass u em $\mathbb{Z}[D_n]$ tal que u não é central.*

DEMONSTRAÇÃO:

Como $\text{mdc}(r, 2^s) = 1$ temos que $\phi(n) = \phi(2^s)\phi(r) = 2^{s-1}\phi(r)$

E pelo teorema do resto chinês temos que existe j, $0 \leq j \leq n$, tal que

$$j \equiv 2 \bmod r$$

e

$$j \equiv 1 \bmod 2^s.$$

Queremos primeiramente mostrar que $j \neq 1$, $j \neq n-1$ e $\text{mdc}(j, n) = 1$. Claramente temos que $j \neq 1$. Para concluirmos que $\text{mdc}(j, n) = 1$ basta mostrar que $\text{mdc}(j, r) = 1$ e que $\text{mdc}(j, 2^s) = 1$. A primeira igualdade é conseqüência da primeira congruência juntando o fato que 2 não divide r, e a segunda igualdade é conseqüência imediata da segunda congruência. Resta mostrar que $j \neq n-1$.

Se r é diferente de 3 segue como conseqüência da primeira congruência. Agora se $r = 3$ teremos pelo fato que $n \neq 6$, que s é maior ou igual a 2 e portanto segue da segunda congruência que j é diferente de $n-1$.

Então para este j temos a unidade cíclica de Bass

$$u = (1 + x + \cdots + x^{j-1})^{\phi(n)} - k\hat{x}.$$

Onde k e $\hat{x}$ são os como definidos convencionalmente. Mostraremos agora que u não é central. Para tanto basta mostrar que $u \neq u^*$.

Pelo lema 2.4 temos $u^* = x^{-(j-1)\phi(n)}u$, logo temos que mostrar que $x^{-(j-1)\phi(n)} \neq 1$, ou equivalentemente mostrar que n não divide $(j-1)\phi(n)$. Para tanto basta mostrar que r não divide $(j-1)\phi(n) = (j-1)2^s\phi(r)$. Como $\text{mdc}(2, r) = 1$ basta mostrar que r não divide $(j-1)\phi(r)$.

Como j é côngruo a 2 módulo r, $j-1$ será côngruo a 1 módulo r. Conseqüentemente $(j-1)\phi(r)$ será côngruo a $\phi(r)$ módulo r. Por outro lado como $\phi(r) < r$, teremos que r não divide $(j-1)\phi(r)$. Assim n não divide $(j-1)\phi(n)$. Donde concluimos que u não é central. □

Já quando temos n uma potência de 2, digamos $n = 2^r$ temos que toda unidade cíclica de Bass é central. De fato:

Se tomarmos um j ímpar $j < n$ teremos a unidade cíclica de Bass

$$u = (1 + x + \cdots + x^{j-1})^{\phi(n)} - k\hat{x}.$$

Sabemos que $u^* = x^{(j-1)\phi(n)}u$. Do fato que $j-1$ é par e $\phi(n) = 2^{r-1}$, temos que n divide $(j-1)\phi(n)$, e portanto $u = u^*$ logo u é central.

Para termos uma unidade que faça o mesmo papel que a unidade cíclica de Bass nos casos anteriores usaremos o fato que para todo j ímpar, e $r \geq 3$, temos que $j^{2^{r-2}} = j^{\frac{n}{4}}$ é côngruo a 1 módulo $n = 2^r$. Em particular $3^{\frac{n}{4}}$ é côngruo a 1 módulo n. Podemos então construir a unidade cíclica de Bass modificada

$$u_2 = (1 + x + x^2)^{\frac{n}{4}} - k_2\hat{x},$$

onde $k_2 = \frac{3^{\frac{n}{4}}-1}{n}$.

Pela proposição 1.2, temos que u_2 é unidade. Pelo lema 2.4 segue que $u_2^* = (x^2)^{\frac{n}{4}}u_2 = x^{\frac{n}{2}}u_2$. Como a ordem de x é n temos que $u_2^* \neq u_2$. Logo u_2 é uma unidade cíclica de Bass modificada não central.

3. O Teorema Central

Nesta seção iremos demonstrar o principal teorema do capítulo, isto é o teorema que nos permite construir subgrupos livres em $\langle u, v\rangle$. Vamos antes enunciar um lema que nos será útil na demonstração do teorema principal. Conhecido como lema do ping-pong. Uma demonstração detalhada deste resultado pode ser encontrada em [**Harpe**]. Denotaremos o produto livre de dois grupos G_1 e G_2 por $G_1 * G_2$.

LEMA 2.7. *[Klein]*

Sejam G um grupo agindo em um conjunto S, Γ_1, Γ_2, dois subgrupos de G e seja Γ o subgrupo gerado por eles. Assuma que Γ_1 contém pelo menos 3 elementos. Suponha também que existem 2 sub-conjuntos não vazios de S, S_1 e S_2 tais que S_2 não está contido em S_1, que $\gamma_1(S_1) \subset S_2$ para todo $\gamma_1 \in \Gamma_1 - \{1\}$, e $\gamma_2(S_2) \subset S_1$, para todo $\gamma_2 \in \Gamma_2 - \{1\}$. Então $\Gamma = \Gamma_1 * \Gamma_2$.

Vamos agora ao teorema central.

TEOREMA 2.8. *Seja n um número igual a 5 ou maior que 6 e seja D_n o grupo diedral de ordem $2n$*

$$D_n = \left\langle x, y | x^n = 1 = y^2, yxy^{-1} = x^{-1} \right\rangle.$$

Tomemos a unidade bíciclica $v = 1 + (1-y)x(1+y)$ *e uma unidade cíclica de Bass ou cíclica de Bass modificada da forma* $u = (1 + x + \cdots + x^{j-1})^m - k_m\hat{x}$, *ambas em* $\mathbb{Z}[D_n]$, *com* j, k_m *e* m *satisfazendo as condições da proposição 1.2.*

Para um r *adequado temos*

$$\frac{\langle u, v^r\rangle}{\mathcal{Z}(\langle u, v^r\rangle)} = \langle \overline{u}\rangle * \langle \overline{v^r}\rangle\,,$$

onde $\mathcal{Z}(\langle u, v^r\rangle)$ *denota o centro de* $\langle u, v^r\rangle$, *e* $^-$, *denota a imagem pelo morfismo canônico. Como conseqüência podemos afirmar que* v^r *e* uv^ru *formam um par livre em* $U(\mathbb{Z}[D_n])$.

DEMONSTRAÇÃO:

Utilizaremos o morfismo φ definido acima, demonstrando que $\langle \varphi(u), \varphi(v^r)\rangle \subset \mathcal{M}$ é o produto livre $\langle \varphi(u)\rangle * \langle \varphi(v^r)\rangle$ para um r adequado, e depois provaremos que o núcleo de φ restrita ao grupo $\langle \varphi(u), \varphi(v^r)\rangle$ é o centro de $\langle \varphi(u), \varphi(v^r)\rangle$.

Vamos primeiramente calcular $\varphi(u^t)$, e $\varphi(v^t)$, para t um número inteiro. Temos

$$\varphi(u^t)(z) = \frac{\tau(u)^t z}{\overline{\tau(u)^t}},$$

visto que suporte de u está contido em $\langle x\rangle$. Como $\tau(\hat{x}) = 0$, temos $\tau(u) = \tau(1 + \zeta_n + \cdots + \zeta_n^{j-1})^m$, e portanto $\tau(u^t) = \tau(1 + \zeta_n + \cdots + \zeta_n^{j-1})^{tm}$, assim

$$\frac{\tau(u)^t z}{\overline{\tau(u)^t}} = \frac{(1 + \zeta_n + \cdots + {\zeta_n}^{j-1})^{tm} z}{\overline{(1 + \zeta_n + \cdots + {\zeta_n}^{j-1})^{tm}}} = \frac{(1 + \zeta_n + \cdots + {\zeta_n}^{j-1})^{tm} z}{(1 + {\zeta_n}^{-1} + \cdots + {\zeta_n}^{1-j})^{tm}} =$$

$$= \frac{(1 + \zeta_n + \cdots + {\zeta_n}^{j-1})^{tm} z}{\zeta_n^{(1-j)tm}(1 + \zeta_n + \cdots + {\zeta_n}^{j-1})^{tm} z} = {\zeta_n}^{(j-1)tm} z.$$

Vamos agora calcular $\varphi(v^t)$:

$$v^t = 1 + t(1-y)x(1+y) = (1 + t(x - x^{-1})) + t(x - x^{-1})y$$

Assim se chamarmos $c' = x - x^{-1}$, e $c = \tau(c') = \tau(x) - \tau(x^{-1})$ e notarmos que $\overline{c} = -c$, temos que $v^t = (1 + tc') + tc'y$ e portanto

$$\varphi(v^t)(z) = \frac{(1+tc)z + tc}{-tcz + (1-tc)},$$

para todo $t \in \mathbb{Z}$. Daqui em diante dividiremos a demonstração em 3 partes:

Primeira Parte: $\langle \varphi(u), \varphi(v^r) \rangle \simeq \langle \varphi(u) \rangle * \langle \varphi(v^r) \rangle$, com n ímpar.

Denotemos por $S^1 = \{z \in \mathbb{C} || z| = 1\}$. Pela proposição 2.2 temos $\varphi(u)(S^1) = S^1$, e $\varphi(v)(S^1) = S^1$. Vamos agora tomar 2 subconjuntos disjuntos de S^1,

$$\mathcal{P} = \{z \in S^1 | z = e^{\mathrm{i}\theta}, \frac{\pi(n-1)}{n} < \theta < \frac{\pi(n+1)}{n}\},$$

e

$$\mathcal{Q} = \{z \in S^1 | z = e^{\mathrm{i}\theta}, 0 \leq \theta < \frac{\pi(n-1)}{n}, \ ou, \ \frac{\pi(n+1)}{n} < \theta \leq 2\pi\}$$

Vale notar que $\mathcal{P} \cap \mathcal{Q} = \emptyset$, e que o grupo $\langle v^r \rangle$ tem ordem infinita, para todo $r \neq 0$. Assim, se provarmos que $\varphi(u^t)(\mathcal{P}) \subset \mathcal{Q}$ para t entre 0 e a ordem de $\varphi(u)$, que denotaremos por k e que $\varphi(v^{rs})(\mathcal{Q}) \subset \mathcal{P}$ para todo $s \in \mathbb{Z}, s \neq 0$ e r com módulo suficientemente grande, teremos pelo lema do ping pong que

$$\langle \varphi(u), \varphi(v^r) \rangle = \langle \varphi(u) \rangle * \langle \varphi(v^r) \rangle .$$

Começaremos mostrando que $\varphi(u^t)(\mathcal{P}) \subset \mathcal{Q}$ para $0 < t < o(\varphi(u)) = k$, onde $k = o(\varphi(u))$ denota a ordem de $\varphi(u)$.

Como $\varphi(u)(z) = {\zeta_n}^{(j-1)m} z$ basta mostrar que para todo $z \in \mathcal{P}$ temos ${\zeta_n}^t z \in \mathcal{Q}$ desde que $0 < t < n$. Vale lembrar que $\zeta_n = e^{\frac{2\pi \mathrm{i}}{n}}$.

Podemos notar com facilidade que $f_n(z) = \zeta_n z$, é uma rotação de ângulo $\frac{2\pi}{n}$ radianos, a mesma medida em radianos do ângulo formado pelos pontos ${\zeta_n}^{\frac{n-1}{2}}, 0$, e ${\zeta_n}^{\frac{n+1}{2}}$. Assim se dividirmos S^1 em n ângulos de mesma medida

$$\mathcal{P}_k = \{z \in S^1 | z = e^{\mathrm{i}\theta}, \frac{2\pi(k-1)}{n} < \theta < \frac{2\pi k}{n}\},$$

teremos que a rotação f_n age em $\{\mathcal{P}_1, \ldots, \mathcal{P}_n\}$ da seguinte forma para $0 \leq j_1 < n$,

$$f_n^{j_1}(\mathcal{P}_{j_2}) = \mathcal{P}_{j_1 + j_2},$$

se $j_1 + j_2 \leq n$, e

$$f_n^{j_1}(\mathcal{P}_{j_2}) = \mathcal{P}_{j_1 + j_2 - n},$$

se $j_1 + j_2 > n$, em particular para todo j_1, $0 < j_1 < n$, temos $f_n^{j_1}(\mathcal{P}_{j_2}) \neq \mathcal{P}_{j_2}$.

É fácil notar que $\mathcal{P} = \mathcal{P}_{\frac{n+1}{2}}$ e que $\mathcal{P}_i$´s estão contidos em $\mathcal{Q}$, sempre que $i \neq \frac{n+1}{2}$. Assim concluimos que para $0 < t < n$ temos

$$\zeta_n^t(\mathcal{P}) \subset \mathcal{Q}$$

e portanto $\varphi(u)^t(\mathcal{P}) \subset \mathcal{Q}$, sempre que $0 < t < k$.

Vamos agora mostrar que para $r \in \mathbb{Z}$ com módulo suficientemente grand temos $\varphi(v^{rs})(\mathcal{Q}) \subset \mathcal{P}$, para todo $s \in \mathbb{Z}, s \neq 0$.

Para tanto usaremos a bijeção ω definida de $\mathbb{C} \cup \{\infty\}$ em $\mathbb{C} \cup \{\infty\}$:

$$\omega(z) = \left(\frac{\zeta_n^{\frac{n-1}{2}} + 1}{\zeta_n^{\frac{n-1}{2}} - 1}\right)\frac{z-1}{z+1}$$

Para facilitar a notação vamos denotar $\alpha = \frac{\zeta_n^{\frac{n-1}{2}}+1}{\zeta_n^{\frac{n-1}{2}}-1}$. Vale notar que $\omega^{-1}(z) = \frac{\alpha+z}{\alpha-z}$.

É conhecido que transformações do tipo $\frac{az+b}{cz+d}$ levam circunferências de $\mathbb{C}$ ou em outras circunferências ou em retas. Vamos analisar $\omega(S^1)$:

$\omega(-1) = \alpha\frac{-1-1}{-1+1} = \frac{-2}{0} = \infty$.

Assim temos que $\omega(S^1)$ é uma reta mais o ponto do infinito. Vamos mostrar que é a reta real mais o ponto do infnto:

$$\omega(1) = \alpha\frac{1-1}{1+1} = 0.$$

$$\omega(\zeta_n^{\frac{n-1}{2}}) = \alpha\frac{\zeta_n^{\frac{n-1}{2}} - 1}{\zeta_n^{\frac{n-1}{2}} + 1} = \alpha\alpha^{-1} = 1.$$

$$\omega(\zeta_n^{\frac{n+1}{2}}) = \alpha\frac{\zeta_n^{\frac{n+1}{2}} - 1}{\zeta_n^{\frac{n+1}{2}} + 1} = \alpha\frac{\zeta_n^{\frac{n+1}{2}}(1 - \zeta_n^{\frac{n-1}{2}})}{\zeta_n^{\frac{n+1}{2}}(1 + \zeta_n^{\frac{n-1}{2}})} = \alpha(-\alpha^{-1}) = -1.$$

Assim $0, 1$, e -1 pertencem a $\omega(S^1)$ e portanto temos que $\omega(S^1)$ é a reta real mais o ponto do infinito. Como $1 \in \mathcal{Q}$, os elementos $\zeta_n^{\frac{n-1}{2}}$ e $\zeta_n^{\frac{n+1}{2}}$ são os pontos de fronteira entre $\mathcal{P}$ e $\mathcal{Q}$ e ω é contínua para $z \neq -1$ temos que $\omega(\mathcal{Q}) =]-1, 1[$ e $\omega(\mathcal{P}) = (\mathbb{R} \setminus [-1, 1]) \cup \{\infty\}$. Vamos mostrar que

$$\omega \circ \varphi(v^{rs}) \circ \omega^{-1}(]-1, 1[) \subset (\mathbb{R} \setminus [-1, 1]) \cup \{\infty\},$$

para r com módulo suficientemente grande, e $s \neq 0$.

$$\omega \circ \varphi(v^{rs}) \circ \omega^{-1}(z) =$$
$$\omega \circ \varphi(v^{rs})(\frac{\alpha+z}{\alpha-z}) =$$
$$\omega\left(\frac{(1+rsc)(\frac{\alpha+z}{\alpha-z})+rsc}{(-rsc)(\frac{\alpha+z}{\alpha-z})+1-rsc}\right) =$$
$$\omega\left(\frac{\alpha+z+rscz+rsc\alpha+rsc\alpha-rscz}{-rsc\alpha-rscz+\alpha-z-rsc\alpha+rscz}\right) =$$
$$\omega\left(\frac{\alpha+z+2rsc\alpha}{\alpha-z-2rsc\alpha}\right) =$$
$$\alpha\left(\frac{\frac{\alpha+z+2rsc\alpha}{\alpha-z-2rsc\alpha}-1}{\frac{\alpha+z+2rsc\alpha}{\alpha-z-2rsc\alpha}+1}\right) =$$
$$\alpha\left(\frac{\alpha+z+2rsc\alpha-\alpha+z+2rsc\alpha}{\alpha+z+2rsc\alpha+\alpha-z-2rsc\alpha}\right) =$$
$$\alpha\left(\frac{2z+4rsc\alpha}{2\alpha}\right) = z+2rsc\alpha$$

Se tomarmos $r \geq |\frac{1}{c\alpha}|$ teremos $|rsc\alpha| \geq 1$, para todo $s \neq 0$, e portanto

$$\omega \circ \varphi(v^{rs})\omega^{-1}(]-1,1[) \subset \mathbb{R} \setminus [-1,1],$$

para todo $s \neq 0$.

E como ω é uma bijeção, concluimos que $(\varphi(v^r))^s(\mathcal{Q}) \subset \mathcal{P}$, para todo $s \neq 0$.

Desta forma usando o lema do ping-pong (2.7), temos que

$$\langle \varphi(u), \varphi(v^r) \rangle = \langle \varphi(u) \rangle * \langle \varphi(v^r) \rangle .$$

Segunda Parte: $\langle \varphi(u) \rangle * \langle \varphi(v^r) \rangle$, com n par.

Basicamente a demonstração segue os mesmos moldes do caso ímpar. Seja $l = \frac{n}{2}$. Aqui usaremos outros subconjuntos de S^1 a saber $\mathcal{P}^*$ e $\mathcal{Q}^*$:

$$\mathcal{P}^* = \{z \in S^1 | z = e^{i\theta}, \frac{\pi(n-2)}{n} < \theta < \frac{\pi(n+2)}{n}\},$$

e

$$\mathcal{Q}^* = \{z \in S^1 | z = e^{i\theta}, 0 \leq \theta < \frac{\pi(n-2)}{n}, \text{ ou, } \frac{\pi(n+2)}{n} < \theta \leq 2\pi\}.$$

Começaremos mostrando que $\varphi(u^t)(\mathcal{P}^*) \subset \mathcal{Q}^*$ para $0 < t < k = o(\varphi(u))$, onde $o(\varphi(u))$ denota a ordem de $\varphi(u)$.

Seja $g_n(z) = \zeta_n^2(z)$. Como $\varphi(u)(z) = \zeta_n{}^{(j-1)m} z$ e $j-1$ é par, temos $\langle \varphi(u) \rangle \subset \langle g_n \rangle$, e portanto é suficiente mostrar que para todo $z \in \mathcal{P}^*$ temos $g_n^t(z) = \zeta_n^{2t} z \in \mathcal{Q}^*$, com $0 < t < \frac{n}{2} = l$.

Seja

$$P_j^* = \{z \in S^1 | z = e^{\mathrm{i}\theta}, \frac{\pi(n-2)}{n} + \frac{4\pi(j-1)}{n} < \theta < \frac{\pi(n-2)}{n} + \frac{4\pi j}{n}\}.$$

Como no caso n ímpar temos que g_n age em $\{\mathcal{P}_1^*, \ldots, \mathcal{P}_l^*\}$ da seguinte forma

$$g_n^{j_1}(\mathcal{P}_{j_2}^*) = \mathcal{P}_{j_1+j_2}^*,$$

se $j_1 + j_2 \leq l$, e

$$g_n^{j_1}(\mathcal{P}_{j_2}^*) = \mathcal{P}_{j_1+j_2-l}^*,$$

se $j_1 + j_2 > l$.

Temos que $\mathcal{P}_1^* = \mathcal{P}^*$, e que para todo $j \neq 1$, $j \leq l$, $\mathcal{P}_j^*$ está contido em $\mathcal{Q}^*$.

Assim temos que para todo $0 < t < l$, $g_n^t(\mathcal{P}^*) \subset \mathcal{Q}^*$.

A demonstração que $\varphi(v^{rs})(\mathcal{Q}^*) \subset \mathcal{P}^*$ para um r adequado, e $s \neq 0$, é bastante similar ao caso n ímpar. Tomemos a função

$$\omega_2(z) = \left(\frac{\zeta_n^{\frac{n-2}{2}} + 1}{\zeta_n^{\frac{n-2}{2}} - 1} \right) \frac{z-1}{z+1}.$$

Cálculos similares ao caso anterior, mostram que $\omega(-1) = \infty$, $\omega_2(1) = 0$, $\omega_2(\zeta_n^{\frac{n-2}{2}}) = 1$, $\omega_2(\zeta_n^{\frac{n+2}{2}}) = -1$.

Se tomarmos $\alpha_2 = \frac{\zeta_n^{\frac{n-2}{2}}+1}{\zeta_n^{\frac{n-2}{2}}-1}$ de forma análoga ao caso anterior teremos

$$\omega_2 \circ \varphi(v^{rs}) \circ \omega_2{}^{-1}(z) = z + 2rsc\alpha_2.$$

Assim tomando $r \geq |\frac{1}{c\alpha_2}|$, temos

$$\varphi(v^{rs})(\mathcal{Q}^*) \subset \mathcal{P}^*,$$

para $s \neq 0$.

Assim usando o lema 2.7 temos

$$\langle \varphi(u), \varphi(v^r) \rangle \cong \langle \varphi(u) \rangle * \langle \varphi(v^r) \rangle .$$

Terceira Parte: $\ker\varphi|_{\langle u,v^r\rangle} = \mathcal{Z}(\langle u, v^r\rangle)$

Sejam $\psi = \varphi|_{\langle u,v^r\rangle}$ e k a ordem de $\psi(u)$. Sabemos que $\psi(u^k) = \tau(u^k)/\overline{\tau(u^k)} = 1$. Logo $\tau(u^k) = \overline{\tau(u^k)} = \tau((u^k)^*)$. Daí temos que $(u^k)^* - u^k$ pertence ao núcleo de τ.

Por 2.4, $(u^k)^* = x^{-mk(j-1)}u^k$. Logo $\tau(1 - x^{-mk(j-1)}) = 0$ e conseqüentemente $\zeta_n^{-mk(j-1)} = 1$. Isto implica que n divide $-mk(j-1)$, $x^{-mk(j-1)} = 1$, e $(u^k)^* = u^k$. Por 2.3 temos que u^k é central.

Assim, todo elemento de $\langle u, v^r\rangle$ é da forma $u^{kw}\nu(u, v^r)$ onde w é um inteiro e ν é um elemento do grupo $C_k * C_\infty$. Como já vimos $\psi(\nu(u, v^r)) = \nu(\psi(u), \psi(v^r)) \neq 1$ a menos que $\nu = 1$. Logo o núcleo de ψ é igual a $\langle u^k\rangle$. E assim concluimos que $\ker\psi \subset \mathcal{Z}(\langle u, v^r\rangle)$.

Claramente temos que $\mathcal{Z}(\langle u, v^r\rangle)$ está contido no núcleo de ψ, pois a imagem de ψ não admite elementos centrais não triviais. Portanto temos que o núcleo de ψ é igual ao centro de $\langle u, v^r\rangle$. E assim temos:

$$\frac{\langle u, v^r\rangle}{\mathcal{Z}(\langle u, v^r\rangle)} = \frac{\langle u, v^r\rangle}{\ker(\psi)} \simeq Im(\psi) \simeq \langle\overline{u}\rangle * \langle\overline{v^r}\rangle .\square$$

4. Grupos livres de posto maior em $U(\mathbb{Z}[D_n])$

Nesta seção construiremos grupos livres de posto maior em D_n, com n maior igual a 3. Usando a unidade bicíclica v construída acima e o elemento x de D_n, faremos uma separação entre o caso ímpar e o caso par.

Começaremos com o caso ímpar.

PROPOSIÇÃO 2.9. *Seja n um número ímpar, $n \neq 1$ e seja D_n o grupo diedral de ordem $2n$*

$$D_n = \langle x, y | x^n = 1 = y^2, yxy^{-1} = x^{-1}\rangle .$$

Tomemos a unidade bíciclica $v = 1 + (1 - y)x(1 + y)$ em $\mathbb{Z}[D_n]$. Para um r adequado, temos

$$\langle x, v^r\rangle = \langle x\rangle * \langle v^r\rangle .$$

DEMONSTRAÇÃO:

Utilizaremos aqui o mesmo morfismo φ das seções anteriores, obtendo

$$\varphi(x)(z) = \frac{\tau(x)}{\overline{\tau(x)}} = \frac{\zeta_n z}{\zeta_n^{-1}} = \zeta_n^2 z.$$

Como n é ímpar temos que a ordem de $\varphi(x)$ é n.

Usando parte da demonstração do teorema 2.8 e o mesmo r temos que

$$\langle \varphi(x), \varphi(v^r) \rangle = \langle \varphi(x) \rangle * \langle \varphi(v^r) \rangle .$$

Vamos mostrar que o núcleo de $\psi = \varphi|_{\langle x, v^r \rangle}$ é trivial. Tomemos um elemento $a \neq 1$ de $\langle x, v^r \rangle$. Ele será da forma

$$a = x^{i_1} v^{rj_1} \cdots x^{i_s},$$

Com $0 < s$, $0 < i_k < n$, a menos que $k = 1$ ou $k = s$, $0 \leq k_1, k_s < n$ e $j_k \neq 0$. Temos

$$\psi(a) = \psi(x)^{i_1} \psi(v^r)^{j_1} \cdots \psi(x)^{i_s} \neq 1,$$

visto que a ordem de $\psi(x)$ é igual a n. Logo ψ é injetora e portanto

$$\langle x, v^r \rangle \simeq \langle \psi(x), \psi(v^r) \rangle \simeq \langle \psi(x) \rangle * \langle \psi(v^r) \rangle \simeq \langle x \rangle * \langle v^r \rangle . \square$$

Vamos agora construir explicitamente grupos livres de posto n:

TEOREMA 2.10. *Sejam n,x,v e r como no teorema anterior. Os elementos $v^r, xv^rx^{-1}, \ldots, x^{n-1}v^rx^{1-n}$, geram (livremente) um grupo livre de posto n em $U(\mathbb{Z}[D_n])$.*

DEMONSTRAÇÃO:

Sejam $v_i = x^i v^r x^{-i}$, $0 \leq i \leq n-1$. Podemos notar que $v_i^k = x^i v^{rk} x^{-i}$. Vamos mostrar que

$$v_{j_1}^{s_1} v_{j_2}^{s_2} \cdots v_{j_k}^{s_k} \neq 1,$$

sempre que $j_i \neq j_{i+1}$, $s_i \neq 0$, e $k \neq 0$.

De fato,

$$v_{j_1}^{s_1} v_{j_2}^{s_2} \cdots v_{j_k}^{s_k} = x^{j_1} v^{rs_1} x^{j_2 - j_1} v^{rs_2} \cdots x^{j_k - j_{k-1}} v^{rs_k} x^{-j_k}$$

Segue de $j_i \neq j_{i-1}$ que $j_i - j_{i-1} \neq 0$ e de $0 \leq j_i \leq n-1$ que $-n < j_i - j_{i-1} < n$. Portanto temos $x^{j_i - j_{i-1}} \neq 1$. Do fato de $s_i \neq 0$ temos que $v^{rs_i} \neq 1$. Assim como $\langle x, v^r \rangle = \langle x \rangle * \langle v^r \rangle$, temos

$$v_{j_1}^{s_1} v_{j_2}^{s_2} \cdots v_{j_k}^{s_k} \neq 1,$$

e portanto $v_0, v_1, \ldots, v_{n-1}$ geram um grupo livre em $U(\mathbb{Z}[D_n]) \square$.

Diferentemente do caso ímpar, onde construimos grupos livres de posto n no caso par construiremos grupos livres de posto $n/2$. Vamos a uma proposição auxiliar.

PROPOSIÇÃO 2.11. *Seja n um número par, digamos $n = 2l$, $n \neq 2$ e seja D_n o grupo diedral de ordem $2n$*

$$D_n = \langle x, y | x^n = 1 = y^2, yxy^{-1} = x^{-1} \rangle .$$

Tomemos a unidade bíciclica $v = 1 + (1 - y)x(1 + y)$ em $\mathbb{Z}[D_n]$.

Para o mesmo morfismo φ, e o mesmo r do teorema 2.8 teremos

$$\frac{\langle x, v^r \rangle}{\mathcal{Z}(\langle x, v^r \rangle)} = \frac{\langle x, v^r \rangle}{\langle x^l \rangle} = \langle \bar{x} \rangle * \langle \overline{v^r} \rangle .$$

DEMONSTRAÇÃO:

Temos $\varphi(x)(z) = \frac{\tau(x)}{\tau(x)} = \zeta_n^2 z$. Logo $o(\varphi(x)) = l$. Já vimos na demonstração do teorema 2.8 que $\varphi(x)$ e $\varphi(v^r)$ geram um produto livre isomorfo a $C_l * C_\infty$.

Seja $\psi = \varphi|_{\langle x, v^r \rangle}$. Vamos mostrar que

$$\langle x^l \rangle = \mathcal{Z}(\langle x, v^r \rangle) = \ker \psi.$$

Como a imagem de ψ não admite elementos centrais não triviais, temos que $\mathcal{Z}(\langle x, v^r \rangle)$ está contido em $\ker \psi$. Como x^l é central em $\mathbb{Z}[D_n]$, temos que $x^l \in \mathcal{Z}(\langle x, v^r \rangle)$. Vamos mostrar agora que $\ker \psi \subset \langle x^l \rangle$.

Seja $\omega \in \langle x, v^r \rangle$, $\omega = x^{i_1} v^{rs_1} \cdots v^{rs_{k'}} x^{i_{k'+1}}$. Como x^l é central temos

$$\omega = x^{tl} x^{i_1} v^{rs_1} \cdots v^{rs_k} x^{i_{k+1}},$$

com $k \leq k'$, t inteiro, $0 < i_2, \ldots, i_k < l$, $0 \leq i_1, i_{k+1} < l$ e $j_1, \ldots, j_k \neq 0$. Se $\psi(\omega) = 1$, teremos

$$1 = \psi(x^{tl} x^{i_1} v^{rs_1} \cdots v^{rs_k} x^{i_{k+1}}) = \varphi(x)^{i_1} \varphi(v^r)^{s_1} \cdots \varphi(v^r)^{s_k} \varphi(x)^{i_{k+1}}.$$

E como $\varphi(x)$ e $\varphi(v^r)$ geram um produto livre temos $k = 0$ e $i_1 = 0$. Donde concluimos $\omega = x^{tl}$.

Logo temos que $\ker \psi \subset \langle x^l \rangle$, concluindo assim a demonstração. □

COROLÁRIO 2.12. *Seja $\omega \in \langle x, v^r \rangle$, $\omega = x^{i_1} v^{rs_1} \cdots x^{i_k} v^{rs_k} x^{i_{k+1}}$. Suponhamos que $k \geq 1$, $s_1, \ldots, s_k$ sejam não nulos e que l não divida $i_2, \ldots, i_k$. Então $\omega \neq 1$.*

DEMONSTRAÇÃO:

Aplicando a função ψ e usando a proposição 2.11, teremos

$$\psi(\omega) = \psi(x)^{i'_1} \psi(v^r)^{s_1} \cdots \psi(x)^{i'_k} \psi(v^r)^{s_k} \psi(x)^{i'_{k+1}},$$

onde cada i'_j é côngruo a i_j módulo l. Logo l não divide $i'_2, \ldots, i'_k$. Por 2.11 segue $\psi(\omega) \neq 1$, e conseqüentemente $\omega \neq 1$. □

Vamos agora construir explicitamente grupos livres de posto l:

TEOREMA 2.13. *Sejam n, l, x, v e r como na proposição 2.11. Os elementos $v^r, xv^rx^{-1}, \ldots, x^{l-1}v^rx^{1-l}$, geram (livremente) um grupo livre de posto l em $U(\mathbb{Z}[D_n])$*

DEMONSTRAÇÃO:

Notaremos por $v_i = x^i v^r x^{-i}$, para i entre 0 e $l-1$.

Seja agora uma palavra ν não trivial pertencente a $\mathcal{F}_l$, o grupo livre de posto l. Temos

$$\nu(v_0, v_1, \ldots, v_{l-1}) = v_{i_1}^{s_1} \cdots v_{i_k}^{s_k},$$

com $i_j \neq i_{j+1}$ e $s_j \neq 0$.

Assim

$$\nu(v_0, v_1, \ldots, v_{l-1}) = x^{i_1} v^{rs_1} x^{-i_1} x^{i_2} v^{rs_2} \cdots x^{i_k} v^{rs_k} x^{-i_k} =$$

$$x^{i_1} v^{rs_1} x^{i_2 - i_1} v^{rs_2} \cdots x^{i_k - i_{k-1}} v^{rs_k} x^{-i_k}.$$

Em vista de 2.12 temos que um elemento $\omega = x^{i_1} v^{rs_1} \cdots x^{i_k} v^{rs_k} x^{i_{k+1}}$, pertencente a $\langle x, v^r \rangle$, é diferente de 1 sempre que $k \geq 1$, $s_1, \ldots, s_k \neq 0$, e l não dividir $i_2, i_3, \ldots, i_k$. Por hipótese temos que os s_j são não nulos. Basta mostrar que l não divide $i_j - i_{j-1}$, para j entre 2 e k.

Por hipótese temos $i_j - i_{j-1} \neq 0$. Além disto temos $0 \leq i_j \leq l-1 < l$. Logo temos a desigualdade

$$-l < i_j - i_{j-1} < l,$$

que nos faz concluir que l não divide $i_j - i_{j-1}$. Portanto temos que $\nu(v_0, \ldots, v_{l-1}) \neq 1$, concluindo assim a demonstração. □

5. Estimando r

Durante a demonstração dos teoremas das duas últimas seções mostramos que era possível gerar grupos livres a partir de uma potência de v que chamamos de r. Nesta seção faremos algumas estimativas para o tal r. Isto é calcularemos os números $|\alpha c|^{-1}$ (usado no caso ímpar) e $|\alpha_2 c|^{-1}$ (usado no caso par).

Começaremos calculando $|c|$

$$c = \zeta_n - \zeta_n^{-1} = \cos(\frac{2\pi}{n}) + \operatorname{sen}(\frac{2\pi}{n})\mathbf{i} - \cos(\frac{2\pi}{n}) + \operatorname{sen}(\frac{2\pi}{n})\mathbf{i} =$$

$$= 2\operatorname{sen}(\frac{2\pi}{n})\mathbf{i}.$$

e temos $|c| = 2\operatorname{sen}(\frac{2\pi}{n})$, para todo $n \geq 3$.

Com a finalidade calcular o módulo de α, começaremos estudando o módulo de números do tipo

$$\frac{\beta+1}{\beta-1},$$

onde $|\beta| = 1$. Podemos assumir $\beta = e^{\mathbf{i}\theta} = \cos\theta + \mathbf{i}\operatorname{sen}\theta$. Assim teremos $\beta + \overline{\beta} = 2\cos\theta$. Mostraremos que $\left|\frac{\beta+1}{\beta-1}\right| = \frac{1}{|\tan\frac{\theta}{2}|}$:

$$\left|\frac{\beta+1}{\beta-1}\right| = \sqrt{\left(\frac{\beta+1}{\beta-1}\right)\left(\frac{\overline{\beta}+1}{\overline{\beta}-1}\right)} = \sqrt{\frac{1+|\beta|^2+\beta+\overline{\beta}}{1+|\beta|^2-\beta-\overline{\beta}}} =$$

$$= \sqrt{\frac{1+\cos\theta}{1-\cos\theta}} = \sqrt{\frac{1+\cos^2\frac{\theta}{2}-\operatorname{sen}^2\frac{\theta}{2}}{1-\cos^2\frac{\theta}{2}+\operatorname{sen}^2\frac{\theta}{2}}} = \sqrt{\frac{2\cos^2\frac{\theta}{2}}{2\operatorname{sen}^2\frac{\theta}{2}}} = \frac{1}{|\tan\frac{\theta}{2}|}$$

Com este resultado calcularemos α, quando n é ímpar, e α_2 quando n é par. Quando n é ímpar temos $\alpha = \frac{\beta+1}{\beta-1}$, com $\beta = \zeta_n^{\frac{n-1}{2}} = e^{\mathbf{i}\frac{\pi(n-1)}{n}}$ pelo resultado anterior temos

$$|\alpha| = \frac{1}{|\tan\frac{\pi(n-1)}{2n}|} = \frac{1}{|\tan(\frac{\pi}{2}-\frac{\pi}{2n})|}$$

E para todo ω temos $\cos(\frac{\pi}{2}-\omega) = \operatorname{sen}\omega$. Assim se $\cos\omega$, $\operatorname{sen}\omega \neq 0$, temos

$$\tan\omega = \frac{1}{\tan(\frac{\pi}{2}-\omega)}.$$

Com esta observação temos

$$|\alpha| = \left|\tan\frac{\pi}{2n}\right| = \tan\frac{\pi}{2n}.$$

No caso n par, temos $\alpha_2 = \frac{\beta+1}{\beta-1}$, com $\beta = \zeta_n^{\frac{n-2}{2}} = e^{\mathbf{i}\frac{\pi(n-2)}{n}}$. Como no caso ímpar temos

$$|\alpha| = \frac{1}{|\tan\frac{\pi(n-2)}{2n}|} = \frac{1}{|\tan(\frac{\pi}{2}-\frac{\pi}{n})|} = \tan\frac{\pi}{n}.$$

Temos assim, as seguintes estimativas para r: Se n é ímpar tomamos

$$r \geq \frac{1}{2 \operatorname{sen} \frac{2\pi}{n} \tan \frac{\pi}{2n}},$$

e se n é par tomamos

$$r \geq \frac{1}{2 \operatorname{sen} \frac{2\pi}{n} \tan \frac{\pi}{n}}.$$

CAPíTULO 3

Unidades centrais em $\mathbb{Z}[D_n]$ e $\mathbb{Z}[DC_n]$

Neste capítulo estudaremos as unidades centrais de $\mathbb{Z}[D_n]$, onde D_n denota o grupo diedral de ordem $2n$, e as unidades centrais de $\mathbb{Z}[DC_n]$, onde DC_n. denota o grupo dicíclico de ordem $4n$

$$DC_n = \langle x, y | x^{2n} = 1, y^2 = x^n, yxy^{-1} = x^{-1} \rangle .$$

1. Introdução

Seja G um grupo, temos $U(\mathbb{Z}[G]) = U(\mathbb{Z}) \times U_1(\mathbb{Z}[G])$, onde $U_1(\mathbb{Z}[G])$ denota o grupo das unidades normalizadas de $\mathbb{Z}[G]$. Caracterizaremos as unidades centrais de $U_1(\mathbb{Z}[G])$ e teremos por conseqüência uma caracterização do grupo das unidades centrais de $U(\mathbb{Z}[G])$.

Seja R um anel comutativo unitário e G um grupo que a princípio suporemos finito. Tomemos para cada elemento g de G, o conjunto $C\ell(g) = \{hgh^{-1} | h \in G\}$, que chamaremos de **classe de conjugação de** g , e seja λ_g o elemento de $R[G]$,

$$\lambda_g = \sum_{h \in C\ell(g)} h.$$

O elemento λ_g é denominado **soma da classe de conjugação de** g .É um fato bastante conhecido que o centro do anel $R[G]$, $\mathcal{Z}(R[G])$ é gerado livremente sobre R pelos elementos λ_g, isto é um elemento central de $R[G]$ será da forma $\alpha_1 \lambda_{g_1} + \cdots + \alpha_s \lambda g_s$, com os α_i´s pertencentes a R. Portanto para começarmos o estudo de elementos centrais em $U_1(\mathbb{Z}[G])$ faz-se necessário conhecer as classes de conjugação de G.

2. Unidades centrais em $U_1(\mathbb{Z}[D_n])$

Relembraremos quais são as classes de conjugação de D_n

$$D_n = \langle x, y | x^n = y^2 = 1, yxy^{-1} = x^{-1} \rangle .$$

Eis as classes de conjugação de D_n.

- Se n é ímpar temos :

$$\{1\}, \{x, x^{-1}\} \ldots \{x^{(n-1)/2}, x^{(n+1)/2}\}, \{y, xy, \ldots x^{n-1}y\}.$$

- Se n é par com $n = 2l$, temos :

$$\{1\}, \{x^l\}\{x, x^{-1}\} \ldots \{x^{l-1}, x^{l+1}\}, \{xy, x^3y, \ldots, x^{n-1}y\}, \{y, x^2y, \ldots, x^{n-2}y\}.$$

Se $n = 2$, temos $D_2 = V_4$, o grupo de Klein, e sabemos que V_4 é um grupo abeliano, logo toda unidade é central. Vamos agora a um teorema que nos esclarece melhor o que acontece quando $n \neq 2$.

TEOREMA 3.1. *Seja D_n, com $n \geq 3$ o grupo diedral de $2n$ elementos,*

$$D_n = \left\langle x, y | x^n = y^2 = 1, yxy^{-1} = x^{-1} \right\rangle.$$

O centro de $U_1(\mathbb{Z}[D_n])$ está contido em $U_1(\mathbb{Z}[\langle x \rangle])$.

DEMONSTRAÇÃO:

Vamos dividir em 2 casos:

n ímpar:

Sejam $X_i = x^i + x^{-i}$, com $1 \leq i \leq (n-1)/2$, e $Y = y + xy + \cdots + x^{n-1}y$, elementos de $\mathbb{Z}[D_n]$. Como vimos os X_i's e Y são soma das classes de conjugação de D_n e portanto formam junto com 1 uma base para o centro de $\mathbb{Z}[D_n]$, logo uma unidade u_1 central em $U_1(\mathbb{Z}[D_n])$ deve ser da forma:

$$u_1 = a_0 + a_1X_1 + \cdots + a_{(n-1)/2}X_{(n-1)/2} + bY$$

com os a_i's e b, números inteiros. Tendo em vista que $u_1 \in U_1(\mathbb{Z}[D_n])$, temos, usando a função aumento

$$1 = a_0 + 2a_1 + \cdots + 2a_{(n-1)/2} + nb.$$

Em contra partida temos o morfismo μ de $\mathbb{Z}[D_n]$ em $\mathbb{Z}$ extensão linear do morfismo de grupos, que leva x em 1 e y em -1. Como u_1 é unidade $\mu(u_1) = \pm 1$ e portanto temos a equação:

$$\pm 1 = a_0 + 2a_1 + \cdots + 2a_{(n-1)/2} - nb.$$

Subtraindo da primeira equação a segunda temos:

$$1 \mp 1 = 2nb.$$

Ou seja ou $b = 0$ ou $b = 1/n$. Como b pertence a $\mathbb{Z}$, não podemos ter a segunda opção. Logo temos que $b = 0$ e portanto $u_1 \in \mathbb{Z}[\langle x \rangle]$.

n par:

Temos que o centro de $\mathbb{Z}[D_n]$ tem como base os elementos 1, $x^{\frac{n}{2}}$,$X_i = x^i + x^{-i}$, com $1 \leq i \leq \frac{n}{2} - 1$, $Y_0 = y + x^2y + \cdots + x^{n-2}y$, e $Y_1 = xy + x^3y + \cdots + x^{n-1}y$. Assim todo elemento do centro de $U_1(\mathbb{Z}[D_n])$ é da forma

$$a_0 + a_1X_1 + \cdots + a_{\frac{n}{2}-1}X_{\frac{n}{2}-1} + a_{\frac{n}{2}}x^{\frac{n}{2}} + b_0Y_0 + b_1Y_1.$$

De forma análoga a anterior temos via aumento e via o morfismo μ, as equações:

$$1 = a_0 + 2a_1 + \cdots + 2a_{\frac{n}{2}-1} + a_{\frac{n}{2}} + \frac{n}{2}b_0 + \frac{n}{2}b_1,$$

e

$$i_2 = \pm 1 = a_0 + 2a_1 + \cdots + 2a_{\frac{n}{2}-1} + a_{\frac{n}{2}} - \frac{n}{2}b_0 - \frac{n}{2}b_1.$$

Como a ordem de $\langle x \rangle$ é par temos dois novos morfismos de grupos entre D_n e $\{1, -1\}$: η_1 e η_2.

O morfismo η_1 leva x em -1 e y em 1. Já η_2 leva x em -1 e y em -1. Podemos estendê-los a um morfismo de anéis entre $\mathbb{Z}[D_n]$ e $\mathbb{Z}$, e assim calculados na unidade central de $U_1(\mathbb{Z}[D_n])$, teremos por η_1,

$$i_3 = a_0 - 2a_1 + \cdots + (-1)^{\frac{n}{2}}a_{\frac{n}{2}} + \frac{n}{2}b_0 - \frac{n}{2}b_1,$$

onde $i_3 \in \{-1, 1\}$, e via η_2

$$i_4 = a_0 - 2a_1 + \cdots + (-1)^{\frac{n}{2}}a_{\frac{n}{2}} - \frac{n}{2}b_0 + \frac{n}{2}b_1.$$

onde $i_4 \in \{-1, 1\}$. Subtraindo da primeira equação a segunda, obtemos :

$$1 - i_2 = 2\frac{n}{2}(b_0 + b_1) = n(b_0 + b_1),$$

e subtraindo da terceira equação a quarta obtemos:

$$i_3 - i_4 = 2\frac{n}{2}(b_0 - b_1) = n(b_0 - b_1).$$

Verificando que $|1 - i_2 + i_3 - i_4| \leq 4$ e que $|1 - i_2 - i_3 + i_4| \leq 4$, obtemos facilmente

$$|2nb_0| \leq 4, \quad e \quad |2nb_1| \leq 4.$$

Como n é um inteiro maior ou igual a 4 temos que a única possibilidade inteira de b_0 e b_1 é $b_0 = b_1 = 0$, e portanto $u \in \mathbb{Z}[\langle x \rangle]$. □

Tendo em vista a observação 2.3, temos que um elemento h de $\mathbb{Z}[\langle x \rangle]$ será central em $\mathbb{Z}[D_n]$ se e só $h = h^*$, onde $*$ denota a involução que estende o anti-morfismo, $x \mapsto x^{-1}$. Assim um elemento de $\mathbb{Z}[\langle x \rangle]$ será central em $\mathbb{Z}[D_n]$ se for $*$-simétrico, ou como chamado na literatura da área, se for simétrico. Com esta observação e o teorema anterior temos o seguinte.

TEOREMA 3.2. *Sejam D_n, com $n \geq 3$ o grupo diedral de $2n$ elementos, $\mathcal{Z}(U_1(\mathbb{Z}[D_n]))$, o centro de $(U_1(\mathbb{Z}[D_n])$, e $U_s(\mathbb{Z}[C_n])$ as unidades simétricas de $(U_1(\mathbb{Z}[C_n])$. Temos $\mathcal{Z}((U_1(\mathbb{Z}[D_n])) = U_s(\mathbb{Z}[C_n])$*

Vamos então estudar os elementos simétricos do grupo $U_1(\mathbb{Z}[C_n])$.

Se $n = 3, 4$ ou 6 temos que o grupo de unidades, $U_1(\mathbb{Z}[C_n])$ será o próprio C_n. Neste caso teremos que o centro de $U_1(\mathbb{Z}[D_3])$ será $\{1\}$, o de $U_1(\mathbb{Z}[D_4])$ será $\{1, x^2\}$, e o de $U_1(\mathbb{Z}[D_6])$ será $\{1, x^3\}$.

Quando $n = 5$, ou $n > 6$, temos que o grupo de unidades de C_n contém grupos abelianos livres. Enunciaremos agora uma proposição que no ajudará a identificar os elementos simétricos de $U_1(\mathbb{Z}[C_n])$. Vamos antes a algumas notações.

Seja G um grupo finito e seja ε a função aumento de $\mathbb{Z}[G]$ em $\mathbb{Z}$, denotaremos por $\Delta(G)$ o núcleo de ε, e por $\Delta^2(G)$, o ideal $\Delta(G) \cdot \Delta(G)$. Seja $1 + \Delta^2(G)$ o conjunto formado pelos elementos da forma $1 + \gamma$ com $\gamma \in \Delta^2(G)$, e seja $U(1 + \Delta^2(G)) = U_1(\mathbb{Z}[G]) \cap (1 + \Delta^2(G))$.

Vale notar que $U(1 + \Delta^2(G))$ é de fato um grupo visto que $\Delta^2(G)$ é um ideal. Com estas definições enunciaremos a proposição.

PROPOSIÇÃO 3.3. *[Cliff,Sehgal, Weiss,* **[CSW81]***] Seja A um grupo abeliano finito.*

(1) $U_1(\mathbb{Z}[A]) = A \times U(1 + \Delta^2(A))$.
(2) $U_1(\mathbb{Z}[A])$ *é finitamente gerado.*
(3) $U(1 + \Delta^2(A))$ *é um grupo abeliano livre.*
(4) *Se $u \in U(1 + \Delta^2(A))$, então $u^* = u$.*

Uma demonstração detalhada desta proposição pode ser encontrada em **[Karp]** ou **[CSW81]**.

Segue do resultado acima que toda unidade u pertencente a $U_1\mathbb{Z}[C_n]$, com n nas condições acima é da forma $x^i v$, onde $v \in U(1 + \Delta^2(C_n))$, e em particular v é uma unidade simétrica de $U\mathbb{Z}[C_n]$, isto é $v = v^*$. Concluimos assim que $u = u^*$ se e só se $x^i = x^{i*}$.

Assim utilizando o teorema 3.2 temos o seguinte.

TEOREMA 3.4. *Seja n um inteiro diferente de $1, 2, 3, 4$ e 6, e $U(1+\Delta^2(C_n)$ como definido acima. Então o centro do grupo $U_1(\mathbb{Z}[D_n])$ é dado por $U(1+\Delta^2(C_n))$, se n for ímpar e por $\langle x^{\frac{n}{2}}\rangle \times U(1+\Delta^2(C_n))$, se n for par.*

DEMONSTRAÇÃO:

Se n é ímpar temos que as unidades $*$-simétricas de $U_1(\mathbb{Z}[C_n])$ são precisamente os elementos de $U(1+\Delta^2(C_n))$, visto que para todo elemento g de C_n, não trivial, teremos $g^* = g^{-1} \neq g$. Logo pelo teorema 3.2, teremos

$$\mathcal{Z}(U_1(\mathbb{Z}[D_n]) = U(1+\Delta^2(C_n)).$$

Se n for par digamos $n = 2l$, temos que o grupo das unidades simétricas será o subgrupo $\langle x^l\rangle \times U(1+\Delta^2(C_n))$, visto que como x^l tem ordem 2, $x^{-l} = x^{l*} = x^l$. Assim

$$\mathcal{Z}(U_1(\mathbb{Z}[D_n]) = \langle x^{\frac{n}{2}}\rangle \times U(1+\Delta^2(C_n)).\square$$

3. Unidades Centrais em $\mathbb{Z}[DC_n]$

Vamos estudar agora as unidades centrais de uma família de grupos que são semelhantes de uma certa forma com a família dos grupos diedrais. Se trata da família dos grupos dicíclicos definidos na forma de geradores e relações por

$$DC_n = \langle x, y | x^{2n} = 1, y^2 = x^n, yxy^{-1} = x^{-1}\rangle,$$

onde $n \geq 2$. Se $n = 2$ temos o grupo K_8 dos quatérnios. Se n for uma potência de 2 este grupo é também conhecido por **quatérnio generalizado** , e costumeiramente denotado por Q_k onde temos que k é tal que $n = 2^k$. Temos facilmente que a ordem de $DC_n = 4n$, e além disso podemos notar que todo elemento de DC_n pode ser escrito de forma única como $x^r y^s$, com $0 \leq r \leq 2n-1$ e r entre 0 e 1. Vamos agora estudar as classes de conjugação de DC_n.

Claramente temos que 1 e x^n são os únicos elementos centrais de DC_n. Como $\langle x\rangle$ centraliza x^i, temos que a classe de conjugação de x^i, para i diferente de 0 e n tem ordem $\frac{|DC_n|}{|\langle x\rangle|} = \frac{4n}{2n} = 2$, logo como $x^{-1} = yxy^{-1}$, temos que a classe de conjugação de x^i será $\{x^i, x^{-i}\}$.

Já os elementos da forma $x^i y$ tem como centralizador o grupo $\langle x^i y\rangle$, e portanto sua classe de conjugação terá cardinalidade n, visto que a cardinalidade de $\langle x^i y\rangle$ é igual a 4. Vamos ver agora quem são os elementos da classe de conjugação de $x^i y$. Temos

$$x^j x^i y x^{-j} = x^j x^i x^j y = x^{i+2j}$$

Daí concluimos facilmente que os x^iy se dividem em duas classes de conjugação de cardinalidade n:

$$C_1 = \{y, x^2y, \ldots, x^{2n-2}y\}$$

e

$$C_2 = \{xy, x^3y, \ldots, x^{2n-1}y\}.$$

Chamaremos de X_i o elemento $x^i + x^{-i}$, com $0 < i < n$, e de Y_j a soma de classe da classe de conjugação C_1, isto é, o elemento $\sum_{g \in C_j} g$. Sabemos que tais elementos formam juntamente com 1 e x^n uma base para o centro de $\mathbb{Z}[DC_n]$.

Vale notar que $\langle x^2 \rangle$ é subgrupo normal de índice 4 em DC_n. Vamos notar tal grupo por N. Vamos agora a

PROPOSIÇÃO 3.5. *Seja u_c uma unidade central de $U_1(\mathbb{Z}[DC_n])$. Então u_c pertence a $U_1(\mathbb{Z}[\langle x \rangle])$.*

DEMONSTRAÇÃO: Seja $K = \frac{DC_n}{N}$. Seja o morfismo de grupos π definido por

$$\begin{array}{rccc} \pi: & DC_n & \to & K \\ & g & \mapsto & gN \end{array}$$

e estendido por linearidade ao morfismo π de anéis entre $\mathbb{Z}[DC_n]$ e $\mathbb{Z}[K]$. E seja u_c uma unidade central de $U_1(\mathbb{Z}[DC_n])$, teremos

$$u_c = \alpha_0 + \alpha X_1 + \cdots + \alpha_n x^n + \beta_1 Y_1 + \beta_2 Y_2.$$

$$\pi(u_c) = a_0 + a_1\pi(x) + n\beta_1\pi(y) + n\beta_2\pi(xy),$$

Onde $a_0 = \alpha_0 + 2\alpha_2 + \cdots + 2\alpha_{n-2} + \alpha_n$, e $a_1 = 2(\alpha_1 + \cdots + \alpha_{n-1})$ se n é par e $a_0 = \alpha_0 + 2\alpha_2 + \cdots + 2\alpha_{n-1}$ e $a_1 = 2\alpha_1 + \cdots + 2\alpha_{n-2} + \alpha_n$ se n é ímpar. Claramente $\pi(u_c)$ é unidade central de $U(\mathbb{Z}[K])$, e como K tem ordem 4 temos que toda unidade é trivial, logo temos que exatamente um dentre os números a_0, a_1, $n\beta_1$, e $n\beta_2$ é igual a 1, e os outros são iguais a 0. Como n é maior que 1 teremos $n\beta_1 = n\beta_2 = 0$, e assim $\beta_1 = \beta_2 = 0$, donde concluimos que

$$u_c = \alpha_0 + \alpha X_1 + \cdots + \alpha_n x^n. \square$$

Usando agora do mesmo raciocínio do caso diedral temos o seguinte.

TEOREMA 3.6. *Seja DC_n o grupo dicíclico de ordem $4n$, com $n > 1$. Temos $\mathcal{Z}(U_1(\mathbb{Z}[DC_n])) = \langle x^n \rangle \times U(1 + \Delta(\langle x \rangle)^2$.*

DEMONSTRAÇÃO:

Como no caso diedral temos $yxy^{-1} = x^{-1}$, e portanto temos que os elementos centrais contidos em $\mathbb{Z}[\langle x \rangle]$ são os elementos simétricos. Logo concluimos que as unidades centrais contidas em $U_1(\mathbb{Z}[\langle x \rangle])$ são as unidades simétricas de $U_1(\mathbb{Z}[\langle x \rangle])$, e como $\langle x \rangle$ é um grupo cíclico de ordem par, utilizando 3.3, e seguindo o mesmo raciocínio de 3.4 temos que

$$\mathcal{Z}(U_1(\mathbb{Z}[DC_n]) = \langle x^n \rangle \times U(1 + \Delta(\langle x \rangle))^2. \square$$

4. Unidades centrais em $\mathbb{Z}[D_\infty]$

Vamos agora determinar o grupo das unidades centrais do anel $\mathbb{Z}[D_\infty]$, onde D_∞ denota o grupo diedral infinito que tem a seguinte apresentação:

$$D_\infty = \left\langle x, y | y^2 = 1, yxy^{-1} = x^{-1} \right\rangle.$$

Usaremos fortemente que existem 2 classes de conjugação infinitas em D_∞.

A saber as classes

$$\{\ldots, x^{-2}y, y, x^2y, x^4y, \ldots\} \quad e\{\ldots x^{-1}y, xy, x^3y, \ldots\}$$

Com isto podemos demonstrar o teorema

TEOREMA 3.7. *O centro do grupo $U_1(\mathbb{Z}[D_\infty])$ está contido em $U_1(\mathbb{Z}[\langle x \rangle])$.*

DEMONSTRAÇÃO:

Seja u um elemento central em $U_1(\mathbb{Z}[D_\infty])$, e digamos que exista no suporte de u um elemento da forma $x^r y$, com $r \in \mathbb{Z}$.

Como o suporte de u é finito existe um s tal que $x^{r+2s}y$ não pertence ao suporte de u. Como u é central teremos a igualdade

$$x^s u x^{-s} = u$$

Sabemos porém que $x^s x^r y x^{-s} = x^{2s+r}y$, e que portanto $x^{2s+r}y$ pertence ao suporte de $x^s u x^{-s}$. Absurdo visto que $x^{2s+r}y$ não pertence ao suporte de u. Logo no suporte de u não há elementos da forma $x^r y$, e conseqüentemente o centro de $U_1(\mathbb{Z}[D_\infty])$ está contido em $U_1(\mathbb{Z}[\langle x \rangle])$ $\square$

Se notarmos que $\langle x \rangle \simeq C_\infty$, e usarmos o fato que $U_1(\mathbb{Z}[C_\infty]) \simeq C_\infty$. Teremos o

TEOREMA 3.8. *O centro de $U_1(\mathbb{Z}[D_\infty])$ é trivial, isto é, igual a $\{1\}$*

DEMONSTRAÇÃO:

A luz do teorema anterior e da observação acima, nos resta apenas analisar quais elementos de C_∞ são centrais. E claramente temos que $x^r y \neq yx^r = x^{-r}y$, sempre que $r \neq 0$, concluindo assim a demonstração. □

CAPíTULO 4

Subgrupos livres em $U(\mathbb{Z}[K_8 \times C_p])$

Nesta seção construiremos subgrupos livres no grupo de unidades do anel $\mathbb{Z}[G]$, onde G é um grupo Hamiltoniano, mas não 2-Hamiltoniano, a partir de unidades cíclicas de Bass. Para tanto construiremos subgrupos livres nas unidades do sub anel $\mathbb{Z}[K_8 \times C_p]$. Como ferramenta usaremos a construção do anel dos quatérnions sobre um anel R para alguns anéis específicos.

1. O Anel $\mathbb{H}(R)$

Seja R um anel comutativo com unidade. Nesta seção construiremos o anel dos quaternions sobre R, e estudaremos algumas de suas propriedades. Denotaremos tal anel por $\mathbb{H}(R)$.

DEFINIÇÃO 4.1. *Seja R um anel comutativo com unidade, definimos* **o anel de quatérnions sobre** R, como o anel

$$\mathbb{H}(R) = R \oplus Ri \oplus Rj \oplus Rk,$$

com o produto dado pelas relações

$$i^2 = j^2 = -1, \quad ij = k = -ji.$$

Em $\mathbb{H}(R)$ temos o subanel $R_2 = R \oplus Ri$. Com este anel podemos construir um morfismo injetivo F_R entre $\mathbb{H}(R)$ e $M_2(R_2)$, usando a seguinte.

PROPOSIÇÃO 4.2. *A função F_R definida de $\mathbb{H}(R)$ em $M_2(R_2)$ por*

$$F_R(a_1 + a_2 i + a_3 j + a_4 k) = \begin{pmatrix} a_1 + a_2 i & a_4 i + a_3 \\ a_4 i - a_3 & a_1 - a_2 i \end{pmatrix},$$

com a_1, a_2, a_3 e a_4 pertencentes a R, é um monomorfismo de anéis.

DEMONSTRAÇÃO :

Temos que $\mathbb{H}(R)$ é um R_2 módulo livre à esquerda, com base $\{1, j\}$.

Associaremos agora a cada $a \in \mathbb{H}(R)$ o endomorfismo (à direita) T_a de R_2-módulos em $H(R)$ ($T_a \in End^{op}_{R_2}\mathbb{H}(R)$):

$$\begin{array}{rccc} (.)T_a: & \mathbb{H}(R) & \to & \mathbb{H}(R) \\ & x & \mapsto & xa \end{array}$$

Temos assim o morfismo de anéis T:

$$\begin{array}{rccc} T & \mathbb{H}(R) & \to & End^{op}_{R_2}\mathbb{H}(R) \\ & a & \mapsto & T_a \end{array}$$

Claramente T é injetor pois $T_a = T_b$ implicaria $(1)T_a = (1)T_b$ e portanto $a = b$

Fazendo uso do isomorfismo canônico entre $End^{op}_{R_2}\mathbb{H}(R)$ e $M_2(R_2)$ construiremos

$$F_R: \quad \mathbb{H}(R) \quad \to \quad M_2(R_2)$$

Aqui ressaltamos que como a composição de funções é tomada da direita para esquerda, os vetores $(1)T_a$ e $(j)T_a$ serão as linhas da matriz $F_R(a)$. (e não as colunas.)

Assim se $a = a_1 + a_2 i + a_3 j + a_4 k$, temos

$$(1)T_a = 1(a_1 + a_2 i + a_3 j + a_4 k) =$$
$$a_1 + a_2 i + a_3 j + a_4 k = (a_1 + a_2 i)1 + (a_3 + a_4 i)j$$

e

$$(j)T_a = j(a_1 + a_2 i + a_3 j + a_4 k) =$$
$$a_1 j - a_2 k - a_3 + a_4 i = (-a_3 + a_4 i)1 + (a_1 - a_2 i)j.$$

Assim obtemos

$$F_R(a) = \begin{pmatrix} a_1 + a_2 i & a_4 i + a_3 \\ a_4 i - a_3 & a_1 - a_2 i \end{pmatrix},$$

e concluimos a demonstração. □

Vamos agora estudar o caso em que R é uma extensão algébrica de $\mathbb{Q}$, o corpo dos racionais, ou um anel de inteiros algébricos. Vamos supor primeiramente que R é um corpo. Temos a seguinte.

PROPOSIÇÃO 4.3. *Seja R uma extensão algébrica de $\mathbb{Q}$, e seja $\mathbf{i}$ a quantidade imaginária de $\mathbb{C}$. Suponha que $\mathbf{i} \notin R$. Então R_2 como construído acima é isomorfo a $R[\mathbf{i}]$, e portanto pode ser imerso em $\mathbb{C}$, via o morfismo ι*

$$\iota(a_1 + a_2 i) = a_1 + a_2 \mathbf{i},$$

com $a_1, a_2 \in R$.

DEMONSTRAÇÃO:

Claramente ι é morfismo de anéis. Vamos mostrar que a imagem de ι é $R[\mathbf{i}]$. Seja $a_1 + a_2\mathbf{i}$ pertencente a $R[\mathbf{i}]$. Basta tomar $a_1 + a_2 i$ em R_2 e temos $\iota(a_1 + a_2 i) = a_1 + a_2\mathbf{i}$.

Vamos mostrar que ι é injetora. Suponha que exista $c + di$ tal que $\iota(c + di) = 0$. Então temos $c + d\mathbf{i} = 0$. Então ou $d = 0$ o que implicaria $c = 0$, ou $d \neq 0$ e teríamos $\mathbf{i} = -cd^{-1} \in R$, absurdo. Logo concluimos que ι é injetor e portanto isomorfismo de anéis entre R_2 e $R[\mathbf{i}]$. □

Podemos ver ι como um monomorfismo de R_2 em $\mathbb{C}$, e estender a um monomorfismo entre $M_2(R_2)$ e $M_2(\mathbb{C})$, da forma natural isto é coordenada a coordenada. Sendo assim temos o morfismo injetor $\iota \circ F_R$ entre $\mathbb{H}(R)$ e $M_2(\mathbb{C})$, sempre que R for uma extensão algébrica de $\mathbb{Q}$ e $\mathbf{i} \notin R$, ou quando R for um sub anel com unidade de um corpo satisfazendo as condições acima.

Daqui em diante p denotará sempre um primo ímpar, e ζ_p a raiz p-ésima da unidade $e^{\frac{2\pi\mathbf{i}}{p}}$. Nossos objetos de estudo serão corpos algébricos da forma $\mathbb{Q}[\zeta_p]$, e seus anéis de inteiros algébricos $\mathbb{Z}[\zeta_p]$. É sabido que $\mathbf{i} \notin \mathbb{Q}[\zeta_p]$, e portanto temos a inclusão de $\mathbb{H}(\mathbb{Q}[\zeta_p])$ e $\mathbb{H}(\mathbb{Z}[\zeta_p])$ em $M_2(\mathbb{C})$ via o morfismo $\iota \circ F_{\mathbb{Q}[\zeta_p]}$, que a propósito chamaremos nas próximas seções de F_H.

2. Subgrupos livres em $U(\mathbb{H}(\mathbb{Z}[\zeta_p]))$

Construiremos aqui grupos livres em $\mathbb{H}(\mathbb{Z}[\zeta_p])$, com unidades da forma $(a_1 + a_2 i)^m$ e $(a_1 + a_2 j)^m$ com a_1 e a_2 pertencentes a $\mathbb{Z}[\zeta_p]$ e m um número inteiro.

A primeira observação a ser feita consiste no fato de que $(a_1 + a_2 i)$ e $(a_1 + a_2 j)$ são conjugadas em $\mathbb{Q}[\zeta_p]$, isto é

$$a_1 + a_2 j = \sigma^{-1}(a_1 + a_2 i)\sigma,$$

onde $\sigma = i + j$ é uma unidade de $\mathbb{Q}[\zeta_p]$, com inverso $-\frac{i+j}{2}$.

E de fato:

$$\frac{i+j}{-2}(a_1 + a_2 i)(i + j) = \frac{i+j}{-2}(a_1 i + a_1 j - a_2 + a_2 k) =$$

$$\frac{-a_1 + a_1 k - a_2 i - a_2 j - a_1 k - a_1 - a_2 j + a_2 i}{-2} = \frac{-2a_1 - 2a_2 j}{-2} = a_1 + a_2 j.$$

Usando a função F_H construída na seção anterior definida de $\mathbb{H}(\mathbb{Q}[\zeta_p])$ em $M_2(\mathbb{C})$. Teremos

$$F_H(a_1 + a_2 i) = \begin{pmatrix} a_1 + a_2\mathbf{i} & 0 \\ 0 & a_1 - a_2\mathbf{i} \end{pmatrix}$$

e

$$F_H(i + j) = \begin{pmatrix} \mathbf{i} & 1 \\ -1 & -\mathbf{i} \end{pmatrix}.$$

Seja $U_{\mathbb{H}} = U(\mathbb{H}(\mathbb{Q}[\zeta_p]))$ o grupo de unidades de $\mathbb{H}(\mathbb{Q}[\zeta_p])$. Temos que F_H restrito a $U_{\mathbb{H}}$ é um morfismo de grupos entre $U_{\mathbb{H}}$ e $GL_2(\mathbb{C})$. Assim se tomarmos Υ como definida no capítulo 2 teremos uma função $\Gamma = \Upsilon \circ F_H$ definida de $U_{\mathbb{H}}$ em $\mathcal{M}$, o grupo de Möbius.

Teremos

$$\Gamma(a_1 + a_2 i)(z) = \frac{(a_1 + a_2\mathbf{i})z}{a_1 - a_2\mathbf{i}} = \frac{a_1 + a_2\mathbf{i}}{a_1 - a_2\mathbf{i}} z$$

e

$$\Gamma(i + j)(z) = \frac{\mathbf{i}z + 1}{-z - \mathbf{i}} = \frac{z - \mathbf{i}}{\mathbf{i}z - 1}.$$

Vale notar que como $-\frac{1}{2}$ é central temos que $\Gamma(-\frac{1}{2}) = 1$, e portanto

$$\Gamma\left(-\frac{i + j}{2}\right)(z) = \Gamma(i + j)(z) = \frac{z - \mathbf{i}}{\mathbf{i}z - 1}.$$

Logo $\Gamma(a_1 + a_2 j) = \Gamma(i + j)\Gamma(a_1 + a_2 i)\Gamma(i + j)$.

O teorema abaixo, nos dá uma condição suficiente para que duas unidades gerem um produto livre da forma $C_2 * C_\infty$ em $\mathcal{M}$

TEOREMA 4.4. *Seja λ pertencente a $\mathbb{C}$, tal que $0 < |\lambda| < 3 - 2\sqrt{2}$. As transformações de Möbius $g_1(z) = \lambda z$ e $g_2(z) = \frac{z-\mathbf{i}}{\mathbf{i}z-1}$, de ordem respectivamente ∞ e 2 geram um grupo $\langle g_1, g_2 \rangle$ que é isomorfo a $\langle g_1 \rangle * \langle g_2 \rangle$. Como conseqüência temos que g_1 e $g_2 g_1 g_2^{-1} = g_2 g_1 g_2$ geram um grupo livre em $\mathcal{M}$.*

DEMONSTRAÇÃO: Veja [**GMS1**] □

Com este teorema e com as observações feitas acima demonstraremos o seguinte.

TEOREMA 4.5. *Sejam $a_1 + a_2 i$ e $a_1 + a_2 j$ duas unidades em $U(\mathbb{H}(\mathbb{Z}[\zeta_p]))$, com a_1 e a_2 pertencentes a $\mathbb{Z}[\zeta_p]$. Suponha que para algum m tenhamos*

$$0 < \left| \frac{a_1 + a_2\mathbf{i}}{a_1 - a_2\mathbf{i}} \right|^m < 3 - 2\sqrt{2}.$$

Então $(a_1 + a_2 i)^m$ e $(a_1 + a_2 j)^m$ gerarão um grupo livre em $\mathbb{H}(\mathbb{Z}[\zeta_p])$.

DEMONSTRAÇÃO:

É suficiente mostrar que $\Gamma((a_1 + a_2 i)^m)$ e $\Gamma((a_1 + a_2 j)^m)$ geram um grupo livre. Como vimos

$$\Gamma((a_1 + a_2 i)^m)(z) = \left(\frac{a_1 + a_2\mathbf{i}}{a_1 - a_2\mathbf{i}}\right)^m z$$

Por hipótese temos $\Gamma((a_1 + a_2 i)^m)(z) = \lambda z$, com $|\lambda|$ entre 0 e $3 - 2\sqrt{2}$.

Por outro lado

$$\Gamma((a_1 + a_2 j)^m) = \Gamma(i + j)\Gamma((a_1 + a_2 i)^m)\Gamma(i + j).$$

$\Gamma(i + j)$ é exatamente o g_2 do teorema anterior. Portanto pelo teorema 4.4 temos que $\Gamma((a_1 + a_2 i)^m)$ e $\Gamma((a_1 + a_2 j)^m)$ geram um grupo livre, e assim concluimos que $(a_1 + a_2 i)^m$ e $(a_1 + a_2 j)^m$ geram um grupo livre. □

Sejam $K_8 = \langle a, b | a^4 = 1, b^2 = a^2, aba^{-1} = b^{-1}\rangle$ e $C_p = \langle c | c^p = 1\rangle$. Usaremos os resultados obtidos nesta seção para mostrar que determinadas unidades cíclicas de Bass geram grupos livres em $U(\mathbb{Z}[K_8 \times C_p])$. Tais unidades são obtidas a partir de dois subgrupos cíclicos de ordem $4p$ de $K_8 \times C_p$, a saber os subgrupos $H_a = \langle ac\rangle$ e $H_b = \langle bc\rangle$.

3. O caso $p = 3$

Estudaremos nesta seção o subgrupo gerado pelas unidades cíclicas de Bass,

$$u_a = (1 + ac + a^2c^2 + a^3 + c)^4 - 52(\widehat{ac}),$$

onde $\widehat{ac} = 1 + ac + \cdots + (ac)^{11}$ e

$$u_b = (1 + bc + b^2c^2 + b^3 + c)^4 - 52(\widehat{bc}),$$

pertencentes a $\mathbb{Z}[K_8 \times C_3]$. Note que $\phi(12) = 4$ e que $\frac{5^4-1}{12} = 52$.

Seja o subgrupo $G_1 = \langle i, j, \zeta_p\rangle$ das unidades de $\mathbb{H}(\mathbb{Z}[\zeta_p])$. Definiremos o isomorfismo de grupos Ψ de $K_8 \times C_p$ em G_1, tomando $\Psi(a) = i$, $\Psi(b) = j$, $\Psi(c) = \zeta_p$. Podemos estender este morfismo a um morfismo de anéis Ψ de $\mathbb{Z}[K_8 \times C_p]$ em $\mathbb{H}(\mathbb{Z}[\zeta_p])$ por linearidade. Através deste morfismo obtemos o seguinte.

TEOREMA 4.6. *As unidades u_a e u_b construídas acima geram um grupo livre em $\mathbb{Z}[K_8 \times C_3]$.*

DEMONSTRAÇÃO

Aplicando Ψ a u_a e u_b teremos:

$$\Psi(u_a) = \Psi((1 + ac + a^2c^2 + a^3 + c)^4 - 52(\widehat{ac})) =$$
$$(\Psi(1) + \Psi(ac) + \Psi(a^2c^2) + \Psi(a^3) + \Psi(c))^4 - 52\Psi(\widehat{ac}) =$$
$$(1 + \zeta_3 i - \zeta_3^2 - i + \zeta_3)^4 = (-2\zeta_3^2 + (\zeta_3 - 1)i)^4$$

e de forma análoga

$$\Psi(u_b) = (-2\zeta_3^2 + (\zeta_3 - 1)j)^4,$$

Usamos acima o fato que $\Psi(\widehat{ac}) = (1 + \zeta_3 + \zeta_3^2)(1 + i - 1 - i) = 0$ e $\Psi(\widehat{bc}) = 0$. Se observarmos que

$$(1 - \zeta_3^2 i)^2 = (1 - \zeta_3 - 2i\zeta_3^2) = i(-2\zeta_3^2 + (\zeta_3 - 1)i),$$

teremos

$$(1 - \zeta_3^2 i)^8 = i^4(-2\zeta_3^2 + (\zeta_3 - 1)i)^4 = (-2\zeta_3^2 + (\zeta_3 - 1)i)^4 = \Psi(u_a).$$

Analogamente

$$(1 - \zeta_3^2 j)^8 = \Psi(u_b).$$

Logo se mostrarmos que $(1 - \zeta_3^2 i)^2$ e $(1 - \zeta_3^2 j)^2$, geram um grupo livre em $\mathbb{H}(\mathbb{Z}[\zeta_3])$, teremos em particular que u_a e u_b geram um grupo livre em $\mathbb{Z}[K_8 \times C_3]$.

Pelo teorema 4.5 basta demonstrar que

$$\left|\frac{1 - \zeta_3^2 \mathbf{i}}{1 + \zeta_3^2 \mathbf{i}}\right|^2 < 3 - 2\sqrt{2}.$$

De fato

$$\left|\frac{1 - \zeta_3^2 \mathbf{i}}{1 + \zeta_3^2 \mathbf{i}}\right|^2 = \left(\frac{(1 - \zeta_3^2 \mathbf{i})(1 + \overline{\zeta_3^2} \mathbf{i})}{(1 + \zeta_3^2 \mathbf{i})(1 - \overline{\zeta_3^2} \mathbf{i})}\right) = \frac{(1 - \zeta_3^2 \mathbf{i})(1 + \zeta_3 \mathbf{i})}{(1 + \zeta_3^2 \mathbf{i})(1 - \zeta_3 \mathbf{i})} =$$

$$\frac{2 + (\zeta_3 - \zeta_3^2)\mathbf{i}}{2 + (\zeta_3^2 - \zeta_3)\mathbf{i}} = \frac{2 + (2\,\mathrm{sen}\,\frac{2\pi}{3}\mathbf{i})\mathbf{i}}{2 - (2\,\mathrm{sen}\,\frac{2\pi}{3}\mathbf{i})\mathbf{i}} = \frac{1 - \frac{\sqrt{3}}{2}}{1 + \frac{\sqrt{3}}{2}} = \frac{2 - \sqrt{3}}{2 + \sqrt{3}} = (7 + 4\sqrt{3})^{-1}.$$

Como $7 + 4\sqrt{3} > 3 + 2\sqrt{2} = (3 - 2\sqrt{2})^{-1}$, temos que $(7 + 4\sqrt{3})^{-1} < 3 - 2\sqrt{2}$, e portanto concluimos que u_a e u_b geram um grupo livre em $\mathbb{Z}[K_8 \times C_3]$. □

4. O caso $p \neq 3$

Neste caso usaremos as unidades

$$u_a = (1 + ac + a^2c^2)^{\phi(4p)} - k\widehat{ac}$$

e

$$u_b = (1 + bc + b^2c^2)^{\phi(4p)} - k\widehat{bc},$$

onde $k = \frac{3^{\phi(4p)}-1}{4p}$.

Analogamente ao caso $p = 3$, temos o seguinte.

TEOREMA 4.7. *As unidades u_a e u_b construídas acima geram um grupo livre em $\mathbb{Z}[K_8 \times C_p]$.*

DEMONSTRAÇÃO:

Denotaremos ζ_p por ζ. Vamos calcular $\Psi(u_a)$ e $\Psi(u_b)$. Vale lembrar que $\Psi(\widehat{ac}) = \Psi(\widehat{bc}) = 0$.

$$\Psi(u_a) = \Psi((1 + ac + a^2c^2)^{\phi(4p)} - k\widehat{ac}) = (1 + \zeta i - \zeta^2)^{\phi(4p)}.$$

De forma análoga temos

$$\Psi(u_b) = (1 + \zeta j - \zeta^2)^{\phi(4p)}.$$

Vamos mostrar que $\Psi(u_a)$ e $\Psi(u_b)$, geram um grupo livre em $U(\mathbb{H}(\mathbb{Z}[\zeta]))$. Em vista do teorema 4.5 basta mostrar que

$$\left|\frac{(1 - \zeta^2 + \zeta\mathbf{i})}{(1 - \zeta^2 - \zeta\mathbf{i})}\right|^{\phi(4p)} < 3 - 2\sqrt{2}.$$

Vamos então calcular $\left|\frac{(1-\zeta^2+\zeta\mathbf{i})}{(1-\zeta^2-\zeta\mathbf{i})}\right|$.

$$\left|\frac{(1 - \zeta^2 + \zeta\mathbf{i})}{(1 - \zeta^2 - \zeta\mathbf{i})}\right| = \left|\frac{\zeta^{-1} - \zeta + \mathbf{i}}{\zeta^{-1} - \zeta - \mathbf{i}}\right| = \left|\frac{-2\,\mathrm{sen}(\omega)\mathbf{i} + \mathbf{i}}{-2\,\mathrm{sen}(\omega)\mathbf{i} - \mathbf{i}}\right| =$$
$$\left|\frac{-2\,\mathrm{sen}(\omega) + 1}{-2\,\mathrm{sen}(\omega) - 1}\right| = \left|\frac{1 - 2\,\mathrm{sen}(\omega)}{1 + 2\,\mathrm{sen}(\omega)}\right|,$$

onde $\omega = \frac{2\pi}{p}$.

Afim de retirarmos o módulo, iremos estudar os dois casos possíveis: $2\,\mathrm{sen}(\omega) > 1$ e $2\,\mathrm{sen}(\omega) < 1$. Vale notar que $0 < \omega < \pi$ e portanto $\mathrm{sen}(\omega) > 0$, e que não teremos $2\,\mathrm{sen}(\omega) = 1$, visto que para tanto teríamos $\omega = \frac{2\pi}{12}$ e 12 não é primo.

Primeiro caso: $2\,\mathrm{sen}(\omega) > 1$ (isto é $p \leq 11$).

Neste caso teremos

$$\left|\frac{1-2\,\mathrm{sen}(\omega)}{1+2\,\mathrm{sen}(\omega)}\right| = \frac{2\,\mathrm{sen}(\omega)-1}{1+2\,\mathrm{sen}(\omega)} = 1 - \frac{2}{2\,\mathrm{sen}(\omega)+1} \leq 1 - \frac{2}{3} = \frac{1}{3}.$$

Visto que $\mathrm{sen}(\omega) \leq 1$ e portanto $2\,\mathrm{sen}(\omega)+1 \leq 3$.

Como $9 = 3^2 > 3 + 2\sqrt{2} = (3-2\sqrt{2})^{-1}$, temos que $\frac{1}{9}$ é menor que $3-2\sqrt{2}$, e portanto para todo $m \geq 2$ temos

$$\left|\frac{(1-\zeta^2+\zeta\mathbf{i})}{(1-\zeta^2-\zeta\mathbf{i})}\right|^m \leq \frac{1}{9} < 3-2\sqrt{2}.$$

Como $\phi(4p) = 2(p-1) > 2$, temos que este caso está resolvido.

Segundo caso: $2\,\mathrm{sen}(\omega) < 1$ (isto é $p \geq 13$).

Teremos neste caso

$$\left|\frac{1-2\,\mathrm{sen}(\omega)}{1+2\,\mathrm{sen}(\omega)}\right| = \frac{1-2\,\mathrm{sen}(\omega)}{1+2\,\mathrm{sen}(\omega)} = \frac{2}{2\,\mathrm{sen}(\omega)+1} - 1.$$

Como $\omega \leq \frac{2\pi}{13} < \frac{\pi}{3}$, temos que $\cos(\omega) > \frac{1}{2}$ e assim

$$\mathrm{sen}(\omega) = \cos(\omega)\tan(\omega) > \frac{1}{2}\cdot\omega = \frac{\omega}{2}.$$

Logo temos

$$\frac{2}{2\,\mathrm{sen}(\omega)+1} - 1 < \frac{2}{\omega+1} - 1 = \frac{2}{\frac{2\pi}{p}+1} - 1 =$$

$$\frac{2p}{p+2\pi} - 1 = \frac{p-2\pi}{p+2\pi}.$$

Faremos agora uma estimativa para m tal que

$$\left(\frac{p-2\pi}{p+2\pi}\right)^m < 3-2\sqrt{2}.$$

Para tal estimativa inverteremos a desigualdade, isto é, procuraremos m tal que

$$\left(\frac{p+2\pi}{p-2\pi}\right)^m > 3+2\sqrt{2}.$$

Podemos minorar o lado esquerdo,

$$\left(\frac{p+2\pi}{p-2\pi}\right)^m = \left(1+\frac{4\pi}{p-2\pi}\right)^m > 1 + m\frac{4\pi}{p-2\pi} > 1 + \frac{4m\pi}{p}$$

e estudar a desigualdade

$$1 + \frac{4m\pi}{p} > 3 + 2\sqrt{2},$$

que tem como solução

$$m > \left(\frac{1+\sqrt{2}}{2\pi}\right) p.$$

Assim para $m > (\frac{1+\sqrt{2}}{2\pi})p$ vale

$$\left|\frac{(1-\zeta^2+\zeta\mathbf{i})}{(1-\zeta^2-\zeta\mathbf{i})}\right|^m < 3 - 2\sqrt{2}.$$

Como $\phi(4p) = 2(p-1) > \frac{p}{2} > (\frac{1+\sqrt{2}}{2\pi})p$, concluimos este segundo caso e a demonstração. □

Como conseqüência obtemos o seguinte.

COROLÁRIO 4.8. *Seja G um grupo Hamiltoniano, não 2-Hamiltoniano. Existem unidades cíclicas de Bass em $U_1(\mathbb{Z}[G])$, u_a e u_b que geram um subgrupo livre em $U_1(\mathbb{Z}[G])$.*

Referências Bibliográficas

[Ahl] L.V.Ahlfors *Complex analysis, International student edition,* Mac-Graw-Hill, Kogakusha, Tokyo, 1966.

[Bass] H.Bass, *The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups,* Topology, **4** (1966), 391-410.

[CSW81] G.Cliff, S.K.Sehgal, A.Weiss, *Units of integral group rings of metabelian groups,* Journal of Algebra, **73** (1981), 167-185.

[DG1] M.A.Dokuchaev, J.Z.Gonçalves, *Semigroup identities on units of integral group rings,* Glasgow Math. Journal, **39** (1997), 1-6.

[Fer] N.A.Fernandes, *A caracterization of units in* $\mathbb{Z}[D_m]$, J.Indian Math. Soc, **55** (1987), 89-110.

[G1] J.Z.Gonçalves, *Free subgroups of units in group rings,* Canad. Math. Bull., **27**, 3 (1984), 309-312.

[G2] J.Z.Gonçalves, *Free groups in subnormal subgroups and the residual nilpotence of the groups of units of group rings,* Canad. Math. Bull., **27**, 3 (1984), 365-370.

[G3] J.Z.Gonçalves, *Free subgroups in the group of units of group rings II,* Journal of number theory, **21**, 2 (1985) , 121-127.

[G4] J.Z.Gonçalves, *Free subgroups and the residual nilpotence of the group of units of modular and p-adic group rings,* Canad. Math. Bull., **29**, 3 (1986), 321-328.

[GMS1] J.Z.Gonçalves, A. Mandel, M. Shirvani, *Free products of units in algebras I. Quaternion algebras,* Journal of Algebra, **214** (1999), 301-316.

[GMS2] J.Z.Gonçalves, A. Mandel, M. Shirvani, *Free products of units in algebras II. Crossed products,* Journal of Algebra, **233** (2000), 567-593.

[HP] B.Hartley, P.F.Pickel, *Free subgroups in the unit groups of integral group rings,* Canad. J. Math., **32**, 6 (1980), 1342-1352.

[HP2] I.Hughes, K.R.Peason, *The group of units of the integral group ring* $\mathbb{Z}S_3$, Canad. Math. Bull., **15**, 4 (1972), 529-534.

[JSP] E.Jespers, M.M.Parmenter, S.K.Sehgal, *Central units of integral group rings of nilpotent groups,* Proc. Amer. Math. Soc., **124**, 3 (1996), 1007-1012.

[Karp] G.Karpilovsky, *Unit groups of classical rings,* Claredon Press, Oxford, 1988.

[Harpe] P.LaHarpe, *Free groups in linear groups,* Le Enseigment Matematique, **t.29** (1983), 129-144.

[MS] Z.Marciniak, S.K.Sehgal, *Constructing free subgroups of integral group ring units,* Proc. Amer. Math. Soc., **125** , 4 (1997), 1005-1009.

[Mask] B.Maskit, *Kleinian groups,* Springer Verlag, Berlin, 1980.

[PasSmi] D.S Passman, P.F.Smith, *Units in integral group rings,* Journal of Algebra, **69** (1981), 213-239.

[Polc] F.C.Polcino Milies, *The group of units of the integral group ring* $\mathbb{Z}D_4$, Bol. da Soc. Bras. de Mat. **4**, 2 (1973), 85-92.

[PS] F.C.Polcino Milies, S.K.Sehgal, *An introduction to group rings,* Kluwer, Dodrecht, 2001.

[Rob] D.J.S. Robinson, *A course in the theory of groups,* Springer Verlag, Berlin, 1991.
[Sco] W.R.Scott, *Group theory,* Dover, New York, 1987.
[Seh1] S.K.Sehgal, *Topics in group rings,* Marcel Dekker, New York, 1978.
[Seh2] S.K.Sehgal, *Units in integral group rings,* Longman, Essex, 1993.