# A IMPORTÂNCIA

# DAS UNIDADES CENTRAIS

# EM ANÉIS DE GRUPO

ANTÔNIO CALIXTO DE SOUZA FILHO

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

Área de Concentração: **Álgebra**
Orientador: **Prof. Dr. Orlando Stanley Juriaans**

-São Paulo, 14 de dezembro de 2000-

**A IMPORTÂNCIA DAS UNIDADES CENTRAIS EM ANÉIS DE GRUPO**

Este exemplar corresponde à redação final
da dissertação devidamente corrigida e
defendida por
ANTÔNIO CALIXTO DE SOUZA FILHO
e aprovada pela comissão julgadora

–São Paulo, 16 de janeiro de 2001–

BANCA EXAMINADORA

-Prof. Dr. Orlando Stanley Juriaans (IME-USP)-

-Prof. Dr. Noraí Romeu Rocco(UnB)-

-Prof. Dr. Michael Dokuchaev(IME-USP)-

## agradecimentos

Acima de tudo, agradeço a Deus.

Agradeço a meus pais, Terezinha Costa de Souza e Antônio Calixto de Souza pela educação e conduta que me ajudam a construir, as minhas irmãs, Liliane Cristina de Souza e Sônia Regina Vieira pela compreensão por minha ausência e a minha sobrinha, Patrícia Regina Vieira por sua confiança e estima.

Agradeço a minhas tias, tios, primas e primos que participaram comigo dessa etapa.

Agradeço a meu amigo Antônio Sérgio Munhoz, por sugerir o verão IME-97, que me ligou ao instituto de matemática. Aos meus amigos e colegas do instituto: Édson Iwaki, Wálter Martins, Ronaldo Garcia, Clézio, Emivan, Noel, Raul, Célia, Sônia, Nestor, Jorge, Jose Domingo, Sandra, Luciano, entre outros, cuja diversidade de relação é grande, são pessoas de valorosa participação nestes anos. Agradeço à Ângela por seu fenômeno recente e à Regina e sua irmã Cida, pela paciência, zelo e energia nas correções do texto.

Agradeço à professora Iracema Bund por sua orientação inicial, a minha orientadora da especialização, professora Elza Gomide, ao professor Héctor Mérklen, presidente da CPG, e aos professores —dedicados professores!— desse instituto. Agradeço aos meus professores das graduações em Engenharia e Filosofia. Particularmente agradeço à professora Maria Helena Nunes, por sua presença e força em meus primeiros anos escolares.

Agradeço aos funcionários, alunos, e professores, do Instituto de Matemática e Estatística e da Universidade de São Paulo, pelo apoio e à estrutura, possíveis pelo trabalho destes.

Agradeço aos professores integrantes das bancas de qualificação e defesa pela valiosa contribuição para este trabalho.

Agradeço a meu orientador, professor Stanley. Síntese de todo um processo, de anos de busca e tentativas.

Antônio Calixto de Souza Filho

# Dedicatória

*"A inocência é uma coisa admirável; mas é, por outro lado, muito triste que ela se possa preservar tão mal e deixe-se tão facilmente seduzir. E é por isso que a própria sageza —que de resto consiste mais em fazer ou não fazer, do que em saber— precisa também da ciência, não para aprender dela, mas assegurar às suas prescrições entrada nas almas e para lhes dar estabilidade."* (I. Kant)

*"Pois eu sou e sempre tenho sido uma daquelas naturezas que deve ser guiada pela razão; não importa o que a razão possa ser, sobre a reflexão ela surge como a melhor."* (Platão)

Dedico este trabalho a minha família, exemplo constante e referência de vida.

## 0.1 Resumo

Na presente dissertação, discutimos o Problema do Isomorfismo em anéis de grupo para grupos infinitos da forma $G \times C_\infty$, apresentado no artigo de Mazur [14], que enuncia um teorema mostrando a equivalência para o Problema do Isomorfismo entre essa classe de grupos infinitos e grupos finitos que satisfaçam a Conjectura do Normalizador. Nossa ênfase concentra-se na relação entre a Conjectura do Isomorfismo e a Conjectura do Normalizador, primeiramente, observada nesse artigo. Em seguida, consideramos um teorema de estrutura para as unidades centrais em anéis de grupo comunicado, pela primeira vez, no artigo de Jespers-Parmenter-Sehgal [9], e generalizado por Polcino Milies-Sehgal em [17], e Jespers-Juriaans em [7]. Evidenciamos a importância desse teorema para a Teoria de Anéis de Grupo e apresentamos uma nova demonstração para o teorema de equivalência de Mazur, considerando, para tanto, uma apropriada unidade central e sua estrutura, caracterizada pelo teorema comunicado para as unidades centrais. Concluímos a dissertação, descrevendo a construção do grupo das unidades centrais para o anel de grupo $\mathbb{Z}A_5$, um grupo livre finitamente gerado de posto 1, utilizando a construção dada no artigo de Aleev [1].

## (Abstract)

In this dissertation, we discuss the Problem of the Isomorphism in group rings for infinite groups as $G \times C_\infty$. This is presented in [14]. Such article states a theorem which shows an equivalence to the isomorphism problem between that infinite class group and finite groups verifing the Normalizer Conjecture. Our main purpose is the Normalizer Conjecture and the Isomorphism Conjecture relationship remarked in the cited article to the groups above. Following, we consider a group ring theorem to the central units subgroup firstly communicated in [9] and generalized in [17] and [7]. We point up the importance of such theorem to the Group Ring Theory and we give a short and a new demonstration to Mazur's equivalence theorem from using a suitable central unit altogether with its structure lightly by the Central Unit Theorem on focus. We conclude this work sketching the $\mathbb{Z}A_5$ central units subgroup on showing it is a free finitely generated group of rank 1 from the presenting construction in Aleev's article [1].

# Sumário

## 0.2 Introdução

Seja $G$ um grupo, e $R$ um anel associativo com unidade. O anel de grupo $RG$ é um $R$-módulo livre com base $G$, cuja multiplicação é induzida pela multiplicação de $G$.

Os anéis de grupo relacionam-se com a Teoria dos Anéis, Teoria dos Grupos, Teoria dos Números, Teoria dos Anéis de Matrizes sobre Anéis de Divisão, entre outras, o que torna a teoria interessante em si mesma. Além de que, a teoria alcança várias áreas da matemática como, por exemplo, Cohomologia de Grupos Finitos ou Topologia Algébrica, implicando, portanto, preparo e conhecimento matemático em importantes áreas de pesquisa. Grandes matemáticos, como Hans J. Zassenhaus, A. Amitsur têm contribuído nessa área. D. S. Passman também tem colaborado, significativamente, com problemas como a Semi-Simplicidade de uma Álgebra de Grupo e Os Divisores de Zero ([16]), isto é, para grupos livres de torção é perguntado se o anel $KG$, para $K$ um corpo, tem divisores de zero.

A seguir citaremos algumas das conjecturas e problemas relevantes da área ([22]):

- (**NC**) Seja $\alpha$ uma unidade de $\mathcal{U}_1(\mathbb{Z}G)$ que normaliza o grupo $G$. Então existe $g \in G$, e uma unidade central $w$, tal que $\alpha = gw$. Ou seja, a conjugação de $\alpha$ sobre $G$ é induzida por um elemento de $G$.
- (**ISO**) Seja $\mathbb{Z}G$ um anel de grupo. Pode-se afirmar que a classe de isomorfismo de $G$ é determinada por $\mathbb{Z}G$?
- (**ZC1**) Seja $\alpha$ uma unidade de torção. Então, existe uma unidade $u \in QG$, tal que $u^{-1}\alpha u \in \pm G$.
- (**ZC3**) Seja $H$ um subgrupo finito de $\mathbb{Z}G$, tal que $\epsilon(H) = 1$, onde $\epsilon$ é o homomorfismo de aumento. Então, $H$ é conjugado em $\mathbb{Q}G$ a um subgrupo de $G$.

Os problemas e conjecturas acima são de fácil enunciado, mas como a maioria dos problemas, nessa área, são de difícil verificação. Muitos deles estão em aberto há mais de meio século. Vale observar que as conjecturas (**ZC**) foram formuladas pelo famoso matemático alemão Hans J. Zassenhaus. Berman e Higman, de certa forma, foram os primeiros a verificarem as conjecturas de Zassenhaus para determinada classe de grupos finitos. De fato, como conseqüência de seus trabalhos, temos o seguinte resultado:

**Teorema 0.2.1.** *Seja $G$ um grupo abeliano finito. Então, as unidades de torção de $\mathbb{Z}G$ são triviais.*

Esse resultado, recentemente, foi estendido por Bovdi-Marciniak-Sehgal ([2]) para grupos abelianos em geral (veja também [17]).

**Teorema 0.2.2.** *Seja $G$ um grupo, e $u \in \mathbb{Z}G$ uma unidade central normalizada. Se $u$ é elemento de torção, então $u \in G$.*

Neste trabalho oferecemos uma nova demonstração para esse resultado.

Em 1995, M. Mazur mostrou [14] uma íntima ligação entre a conjectura do isomorfismo e a conjectura do normalizador. Roggenkamp e Marcianiak [12] valeram-se dessa descoberta para produzir um contra-exemplo à conjectura do isomorfismo para certa extensão de $\mathbb{Z}$, demonstrando que a conjectura do normalizador é falsa, se o anel de coeficientes não for $\mathbb{Z}$.

No artigo *Sobre o Problema do Isomorfismo para anéis de grupo de grupos Infinitos*, Marcin Mazur apresenta um teorema para anéis de grupo sobre a família dos grupos infinitos do tipo $K = G\times < t >$, sendo $G$ um grupo finito, e $t$ um elemento de ordem infinita. Esse teorema mostra que o problema do isomorfismo para os grupos infinitos, do tipo acima, equivale ao problema do isomorfismo para grupos finitos, que verifiquem a conjectura do normalizador.

Uma conseqüência desse teorema é a relação, para essa família de grupos, entre o Problema do Isomorfismo e a Conjectura do Normalizador. Portanto, como corolário desse teorema, para os grupos da forma $K$, demonstramos neste trabalho que $K$ satisfaz o Problema do Isomorfismo, se e somente se, $G$ satisfaz o Problema do Isomorfismo e a Conjectura do Normalizador.

Tal propriedade, que relaciona essas duas conjecturas, até então, não era conhecida. De modo que, a partir desse teorema de Mazur a tentativa de produzir um contra-exemplo para o Problema do Isomorfismo passou a considerar, para isso, também, a Conjectura do Normalizador.

Em 1996, Hertweck, usando essas idéias, anunciou um contra-exemplo para a conjectura do isomorfismo sobre os inteiros. Isto colocaria fim a uma conjectura que está em aberto há mais de meio século! Porém, a prova final, até o momento, ainda não foi publicada em artigo.

Jespers, Parmenter e Sehgal, em [9], provaram o seguinte resultado:

**Teorema 0.2.3.** *Seja $G$ um grupo nilpotente finitamente gerado, $T(G)$ o subgrupo de torção de $G$, e $u \in \mathbb{Z}G$ uma unidade central. Então, existe $g \in G$, e $w \in \mathbb{Z}T(G)$, tal que $u = gw$.*

Esse é um dos resultados mais importantes de estrutura de unidades centrais, em anéis de grupo, que se conhece. E. Jespers e O. S. Juriaans, usando esse teorema, generalizaram os resultados de Mazur em [14], e provaram que para grupos nilpotentes finitamente gerados existe uma forte ligação com várias outras conjecturas.

Um contra-exemplo para uma determinada conjectura para grupos nilpotentes finitamente gerados implicaria uma outra para os grupos finitos. Por exemplo, em [7] é provado que se a classe de nilpotência de $G$ não for um invariante do anel de grupo, então existe uma imagem homomórfica finita de G, que é um contra-exemplo à famosa conjectura sobre os grupos de dimensão. Isso mostrou que as unidades centrais desempenham papel fundamental em anéis

de grupo, porém só recentemente esse papel está tornando-se claro. Em [8] é demonstrado um teorema de caracterização para $\mathcal{N}_{\mathcal{U}_1}G$, o subgrupo normalizador de um grupo $G$ no grupo das unidades normalizadas de $\mathbb{Z}G$ (teorema 1), permitindo novos resultados em anéis de grupo.

O teorema de estrutura para as unidades centrais foi também empregado em [9] e [7],[17], [8] para calcular subgrupos de índice finito no subgrupo de unidades centrais do grupo de unidades para grupos nilpotentes finitamente gerados, e para grupos em geral, respectivamente. No entanto, somente em alguns casos, tem-se uma descrição completa de subgrupos de unidades centrais do anel. [1] foi o primeiro a exibir o subgrupo do centro do anel de grupo sobre os inteiros para os grupos alternados $A_5$, $A_6$ e $A_7$. Para esses grupos o subgrupo de unidades centrais é cíclico. É importante lembrar que Ritter e Sehgal provaram em [18] que a trivialidade do grupo de unidades centrais depende apenas do grupo $G$ em questão.

Os fatos acima evidenciam que as unidades centrais têm papel fundamental na verificação de importantes conjecturas da área e na descrição do grupo de unidades centrais de um anel de grupo. Por isso elas serão objeto de estudo sistemático desta dissertação.

Em linhas gerais temos o seguinte cenário: Mazur anuncia um teorema para o problema do isomorfismo para anéis de grupo, cujo grupo base é um grupo infinito. Concomitantemente, Jespers, Parmenter e Sehgal publicam um teorema de estruturas para as unidades centrais de um grupo nilpotente finitamente gerado, o qual caracteriza a unidade central de um anel de grupo $RG$, para um anel $R$ que é $G$-adaptado. A família de grupos, apresentada por Mazur, satisfaz as condições do teorema para as unidades centrais, de modo que, utilizando-se adequadamente essa representação para a unidade central, é possível simplificar a demonstração dada por Mazur, bem como exibir a unidade a qual seu teorema refere-se.

Este trabalho constitui-se de três partes: inicialmente discutimos o teorema de Mazur para o problema do isomorfismo em anéis de grupo, cujo grupo base seja da forma $H \times C_\infty$, apresentando a relação existente entre o Problema do Isomorfismo, daqui em diante tratado por (ISO) e a Conjectura do Normalizador, referida por (NC). Apontamos para um corolário que indica exatamente uma família de grupos que refute a (ISO), para o caso infinito, e observamos a possibilidade de uma nova demonstração a partir da consideração de uma unidade central no anel de grupo. Em seguida, passamos à consideração do centro das unidades de um anel de grupos e demonstramos um teorema de estrutura para esse subgrupo. Apresentamos uma outra demonstração para o teorema discutido anteriormente sobre (ISO) para anéis de grupo cujo grupo base é infinito. Obtemos como resultado do teorema, anteriormente mencionado, de estrutura para as unidades centrais de um anel de grupo, que o subgrupo das unidades centrais é finitamente gerado. Ademais, é ainda possível construir subgrupos do grupo das unidades centrais, de índice finito sobre esse grupo, a partir de um número finito de geradores. Concluímos a dissertação construindo o grupo das unidades centrais para um grupo tipo Mazur, cujo centro das unidades é obtido pelo centro das unidades do anel $\mathbb{Z}A_5$. Nossa escolha para tal exemplo

justifica-se porque Aleev, [1], determinou completamente esse subgrupo e não um subgrupo deste de índice finito.

# Capítulo 1

# PRELIMINARES

Admitimos conhecidas as definições de grupos, módulos e anéis. Utilizamos, ao longo do texto, as letras $G, H, K, L$ para os grupos, $M$ para os módulos, e $R, S$, ou $\mathbb{Z}$ para os anéis, esse último o anel dos inteiros. Para o subgrupo das unidades de um anel usamos a letra $\mathcal{U}$; o conjunto dos elementos de torção de um anel de grupo está denotado por $\mathcal{T}$; $Ker(\varphi)$ é o núcleo de um dado morfismo $\varphi$, e $\mathcal{A}ut(G)$, ou $\mathcal{A}ut(K)$ são os grupos dos automorfismos, respectivamente, de um grupo $G$ ou um corpo $K$. Salvo referência indicada, os anéis considerados são associativos com unidade. Para a ordem de um elemento $g$ de um grupo, utilizamos $o(g)$, enquanto que para a ordem de um grupo, ou para a cardinalidade de um conjunto, por exemplo $C$, denotamos por $|C|$. As principais fontes utilizadas, para a teoria de Grupos e Anéis, são as referências [19] e [6], respectivamente.

## 1.1 Grupos e Anéis

A seguir apresentamos alguns resultados conhecidos na teoria de grupos, que serão utilizados nas discussões procedentes.

### 1.1.1 Noções Básicas da Teoria dos Grupos

Seja $G$ um grupo. Podemos, para um subgrupo $H$ de $G$, considerar os conjuntos formados pela operação de cada elemento $g \in G$ com o subgrupo $H$, por exemplo, à esquerda, isto é, $G \cdot H = \{g \cdot H, \text{ com } g \in G\}$. Os elementos desse conjunto são as classes laterais do subgrupo $H$ em $G$. A cardinalidade deste é definida como o índice de $H$ em $G$ e denotada por $[G : H]$, ou seja, o número de classes laterais de $H$ em $G$. Podemos obter o grupo $G$ a partir do conjunto das classes laterais, isto é, definindo-se um transversal de $H$ em $G$, denotado por $T$, como um

conjunto formado a partir das classes laterais de $H$ em $G$, ou seja, $T = \{t\colon\ t \in gH$, para cada $g \in G$, e $t$ um único elemento de $gH\}$. Nesse caso

$$G = \dot{\bigcup_{t\in T}} tH.$$

**Teorema 1.1.1.** *([19], 1.3.11) Seja $G$ um grupo, e $H, K$ dois subgrupos de $G$. Então $[G : H \cap K] \leq [G : H][G : K]$ com a igualdade válida para $[G : K]$ e $[G : H]$ inteiros co-primos.*

**Corolário 1.1.2.** ***(Teorema de Poincaré)***([19], 1.3.12) *A intersecção de um conjunto finito de subgrupos, cada qual de índice finito, é também de índice finito.*

**Definição 1.1.3.** *Seja $G$ um grupo. Dizemos que $g \in G$ é um elemento de torção se existe um inteiro $n$ tal que $g^n = 1$. Denotamos por $T(G)$ o conjunto de todos os elementos de torção do grupo $G$. Dizemos que $G$ é de torção se $G = T(G)$ e que $G$ é livre de torção se $T(G) = \{1\}$. Se existir um inteiro $m$, tal que $g^m = 1$, para todo $g \in G$, o menor número inteiro com essa propriedade é denominado expoente de $G$ e denotado por $exp(G)$.*

Para um grupo $G$, não é sempre verdadeiro que o conjunto $T(G)$ seja um subgrupo de $G$, embora isso ocorra para os grupos abelianos, [19].

**Proposição 1.1.4.** *([19], 4.2.9) Um grupo abeliano finitamente gerado que é de torção é um grupo finito.*

**Teorema 1.1.5.** *Seja $G$ um grupo, e $N$ um subgrupo normal finito de $G$. Se $G/N$ é livre de torção, então $N = T(G)$, com $T(G)$ a torção de $G$. Ademais, se $\overline{g} \neq \overline{1} \in G/T(G)$, então $o(g) = \infty$.*

**Teorema 1.1.6.** ***(Teorema da Correspondência para Grupos)*** *Seja $\sigma : G \twoheadrightarrow H$ um epimorfismo. Então há uma correspondência biunívoca entre os subgrupos normais de $H$ e os subgrupos normais de $G$ que contêm o subgrupo $Ker(\sigma)$.*

**Definição 1.1.7.** *Seja $G$ um grupo. O comutador, ou grupo derivado de $G$ é definido como $G' =< [a, b] = aba^{-1}b^{-1}$, $a, b \in G >$. Dizemos, também, que $G'$ é o subgrupo comutador de $G$. Seja $X_1$ e $X_2$ subgrupos de $G$. Podemos definir o subgrupo comutador de $X_1$ e $X_2$ como*

$$[X_1, X_2] =< [a, b] = aba^{-1}b^{-1}, \text{ tal que } a \in X_1, b \in X_2 > .$$

A partir daqui, se $a, b$ são elementos de um grupo $G$, denotamos

$$aba^{-1} := b^a.$$

**Proposição 1.1.8.** *Sejam $x, y, z$ elementos de um grupo. Então*

$$[xy, z] = [y, z]^x[x, z].$$

Pela proposição anterior, tem-se que $[x^2, y] = [xx, y] = [x, y]^x[x, y]$.

**Proposição 1.1.9.** *Seja $G$ um grupo, e $N$ um subgrupo de $G$, tal que $N$ contém $G'$. Então $N$ é um subgrupo normal em $G$.*

**Proposição 1.1.10.** *Seja $G$ um grupo, e $N$ um subgrupo normal de $G$. Então*

$$G/N \text{ é abeliano } \iff N \supset G'.$$

**Teorema 1.1.11.** *(**Teorema de Schur**) Seja $G$ um grupo, tal que $[G : \mathcal{Z}(G)] = n < \infty$. Então*

**i.** $|G'| < \infty$;

**ii.** $g^n = 1 \ \forall \ g \in G'$, *ou seja,* $exp(G') < n$.

**Definição 1.1.12.** *Um grupo $G$ é denominado nilpotente se ele tem uma série central finita, ou seja, uma série normal —cada elemento da série é um subgrupo normal em $G$, isto é,*

$$\{1\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G, \ G_i \lhd G, \quad 1 \leq i \leq n,$$

*tal que $G_{i+1}/G_i \subset \mathcal{Z}(G/G_i) \ \forall \ i$. O comprimento da série é o número de fatores desta, e o comprimento da menor série central de $G$ é a classe de nilpotência de $G$.*

**Definição 1.1.13.** *Sejam $\mathcal{P}$ e $\mathcal{Q}$ duas propriedades de grupos. Um grupo $G$ é poli$\mathcal{Q}$-por-$\mathcal{P}$ se $G$ possui um subgrupo normal $N$, tal que o grupo quociente $G/N$ satisfaz $\mathcal{P}$, e o subgrupo $N$ tem uma série subnormal*

$$N = N_0 \rhd N_1 \rhd \cdots \rhd N_s = \{1\},$$

*a qual cada fator $N_i/N_{i+1}$ possui a propriedade $\mathcal{Q}$.*

Por exemplo, $G$ será policíclico por finito se $G$ possuir um subgrupo normal $N$, tal que o grupo quociente $G/N$ seja finito, e $N$ tenha uma série subnormal, a qual cada fator seja cíclico. Portanto, se $G = T \times < t >$, sendo $|T| < \infty$, e $o(t) = \infty$, então $G$ é um grupo policíclico por finito. Tome $N =< t >$, subgrupo normal de $G$, de modo que $G/N$ é um grupo finito e $N$ tem uma série subnormal

$$< t >= N_0 \rhd N_1 =< 1 >$$

cujos fatores são cíclicos.

**Definição 1.1.14.** *Um grupo $G$ é noetheriano se $G$ satisfaz a condição de cadeia ascendente sobre seus subgrupos, isto é, se qualquer seqüência*

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n \subseteq \cdots,$$

*de subgrupos de $G$ estaciona, ou seja, existe $k$, natural, tal que $G_{k+i} = G_k$, para todo $i$ inteiro não negativo.*

Os únicos exemplos conhecidos de grupos noetherianos são os grupos policíclicos-por-finito, veja [21].

**Definição 1.1.15.** *Definimos um grupo $G$ ordenado se os elementos de $G$ podem ser linearmente ordenados de um modo compatível com a operação do grupo. Ou seja, os elementos de $G$ estão linearmente ordenados pela relação de ordem $\succ$, e para todo $a, b, c \in G$, $a \succ b$ implica $ac \succ bc$ e $ca \succ cb$.*

Inferimos dessa definição que todo grupo ordenado é livre de torção.

**Teorema 1.1.16.** *([22], corolário 6.45.4) Seja $G$ um grupo nilpotente livre de torção. Então $G$ é um grupo ordenado.*

**Teorema 1.1.17.** *([19], 5.2.6) Seja $\mathcal{P}$ uma propriedade grupo-teórica herdada por imagens de produtos tensoriais e por extensões. Se $G$ é um grupo nilpotente, tal que $G/G'$ possui essa propriedade $\mathcal{P}$, então também, o grupo $G$ satisfaz $\mathcal{P}$.*

**Teorema 1.1.18.** *Seja $G$ um grupo nilpotente. Então o conjunto dos elementos de torção de $G$ forma um subgrupo normal de $G$. Ademais, se $G$ é um grupo finitamente gerado, então $T(G)$ tem ordem finita, e o grupo $G/T(G)$, que é livre de torção e finitamente gerado, é ordenado.*

**Demonstração.** Pelo teorema 1.1.17, $T(G)$ é um subgrupo normal de $G$. Considerando o grupo $G$ finitamente gerado, seja $T'$ o comutador de $T(G)$, $T(G)/T'$ é um grupo abeliano finitamente gerado, logo pela proposição 1.1.4, esse grupo quociente é finito. Considere para a propriedade grupo-teórica do teorema 1.1.17 $\mathcal{P}$ =finita. Assim, por esse teorema, se $|T(G)/T'|$ é finita, então $|T(G)|$ é finita. Finalmente, $G/T(G)$ é um grupo nilpotente livre de torção. Portanto, pelo teorema 1.1.16, este é ordenado. □

**Definição 1.1.19.** *Seja $G$ um grupo, dizemos que dois subconjuntos de $G$, $S$ e $S'$, são conjugados se existe um elemento $g$ de $G$, tal que $S' = gSg^{-1}$. A classe de conjugação de $S$ é o conjunto dos subconjuntos de $G$ que são conjugados a $S$. Denotamos $cl(S) = \{S' \subset G\colon \exists\ g \in G$ com $gS'g^{-1} = S\}$. No caso de $S = \{g\}$, $cl(\{g\}) \doteq cl(g) = \{h \in G\colon \exists\ x \in G$ com $xhx^{-1} = g\}$, essa é a classe de conjugação de $g$ em $G$. Desse modo, dizemos que $h \sim g$ se $h \in cl(g)$.*

**Definição 1.1.20.** *Seja $G$ um grupo, e $S$ um subconjunto deste. Definimos o centralizador de $S$ em $G$, notado por $C_G(S)$, por*

$$C_G(S) = \{g \in G : \forall s \in S, gs = sg\};$$

*$C_G(g) = \{h \in G\colon gh = hg\}$ é o centralizador de $g$ em $G$.*

**Definição 1.1.21.** *Seja $G$ um grupo, e $S$ um subconjunto de $G$. Definimos o normalizador de $S$ em $G$ por*

$$\mathcal{N}_G(S) = \{g \in G : gSg^{-1} \subset S\}.$$

**Proposição 1.1.22.** *Seja $G$ um grupo. Se $S$ é um subconjunto de $G$, então $[G : \mathcal{N}_G(S)] = |cl(S)|$.*

**Corolário 1.1.23.** *Seja $G$ um grupo e $x \in G$. Então $[G : C_G(x)] = |cl(x)|$.*

**Definição 1.1.24.** *Seja $G$ um grupo. Definimos o FC-centro de $G$, que denotamos por $\Delta(G)$, por*

$$\Delta(G) = \{g \in G : |cl(g)| < \infty\}.$$

**Proposição 1.1.25.** *Seja $G$ um grupo. O FC-centro de $G$ é um subgrupo de $G$.*

**Definição 1.1.26.** *Seja $G$ um grupo. Dizemos que $G$ é um FC-grupo se $G$ é igual a seu FC-centro.*

**Teorema 1.1.27.** *Seja $G$ um grupo finitamente gerado. Então valem as seguintes equivalências:*

$$G \text{ é } FC \Longleftrightarrow [G : \mathcal{Z}(G)] < \infty \Longleftrightarrow |G'| < \infty.$$

**Demonstração.** Inicialmente, mostremos que se $|G'| < \infty$, então $G$ é um grupo FC. Seja $|G'| < \infty$; para todo $g \in G$ o conjunto $cl(g) \subset gG'$. Com efeito, $x \in cl(g); [g^{-1}, x] = g^{-1}g^x$, logo $g[g^{-1}, x] = g^x \in g^{-1}G'$. Portanto, $cl(g) \subset gG'$, $|cl(g)| < |G'| < \infty$. Suponha que $G$ é um $FC$-grupo finitamente gerado; seja $G =< f_1, \cdots, f_n >$, definimos $H_i = C_G(f_i)$, o centralizador de $f_i$ em $G$, um subgrupo de $G$. Pelo corolário 1.1.23, $[G : C_G(f_i)] = |cl(f_i)| < \infty$; $G$ é, pois, um grupo FC. Então pelo lema 1.1.2, $H = \bigcap_i H_i$, $[G : H] < \infty$. Se $h \in H$, então $hf_i = f_ih$, $1 \leq i \leq n$. Portanto, $h \in \mathcal{Z}(G)$, logo $[G : \mathcal{Z}(G)] \leq [G : H] \leq \infty$. Pelo teorema de Schur 1.1.11, $[G : \mathcal{Z}(G)]$ finito implica $G'$ finito. □

**Definição 1.1.28.** *Um grupo $G$ é residualmente finito se para todo $1 \neq x \in G$, existe um $N_x \lhd G$, tal que $x \notin N_x$, e $[G : N_x] < \infty$.*

**Observação 1.1.29.** *Se $G$ é um grupo nilpotente e finitamente gerado, então, pela demonstração do teorema 1.1.18, $G$ é um grupo policíclico, pois $G$ tem uma série central, cujos fatores são cíclicos de ordem prima, ou ordem infinita. Pelo teorema ([19] [5.4.17](Hirsch)), i.e., um grupo policíclico é residualmente finito, $G$ é residualmente finito.*

**Lema 1.1.30.** *Seja $G$ um grupo residualmente finito, e $X$ um subconjunto finito de $G$. Então existe $N$, um subgrupo normal de $G$, tal que a projeção canônica $\pi : G \longrightarrow G/N$ é injetiva, quando restrita a $X$.*

**Demonstração.** Para $|G| < \infty$ o resultado é trivial; seja $|G| = \infty$. Sendo $G$ residualmente finito, para $X$ um subconjunto qualquer finito de $G$, considere $Y = XX^{-1} = \{xy^{-1}$, tal que $x, y \in X\}$ um subconjunto finito de $G$. Para todo $z \in Y$, $\exists\ N_z \lhd G$ com $z \notin N_z$, e $[G : N_z] < \infty$.

Seja $N := \bigcap_{1 \neq x \in Y} N_x$, pelo teorema 1.1.2, $[G : N] < \infty$. Sendo $|G| = \infty$. Então $N \neq < 1 >$. Seja $\pi : G \longrightarrow G/N$. Suponha $x \neq y \in Y$, tais que $\pi(x) = \pi(y)$; $\pi(xy^{-1}) = \overline{1} \Longrightarrow xy^{-1} \in Ker(\pi) = N$. Então $z = xy^{-1} \in N \subset N_z \Longrightarrow z \in N_z$. Contradição. Portanto, $x = y$. □

Considere $\mathcal{F}$ e $\Lambda$ uma família de grupos e de índices, respectivamente. Seja $\mathcal{F} = \{G_\lambda, \lambda \in \Lambda\}$. Definimos

$$C = \prod_{\lambda \in \Lambda} G_\lambda$$

o produto cartesiano dos membros da família de grupos, ou seja, $C$ é o conjunto de vetores $(g_\lambda)_{\lambda \in \Lambda}$, no qual $g_\lambda \in G_\lambda$, para cada $\lambda \in \Lambda$.

**Definição 1.1.31.** *O produto direto externo dos grupos da família $\mathcal{F}$ é o conjunto dos elementos de $C$, isto é, $(g_\lambda)_{\lambda \in \Lambda} \in C$, cujos termos $g_\lambda$ são os elementos neutros de $G_\lambda$, a menos de um número finito desses elementos. Denotamos o produto direto externo por*

$$D = Dr_{\lambda \in \Lambda} G_\lambda.$$

O produto direto externo $D$ é um subgrupo normal de $C$. Considerando-se para cada índice $\lambda_0 \in \Lambda$ o homomorfismo de inclusão $i_{\lambda_0} : G_{\lambda_0} \hookrightarrow C$, que associa a cada elemento de $G_{\lambda_0}$ a identidade de $G_\lambda$ na posição $\lambda \neq \lambda_0$, e os elementos de $G_{\lambda_0}$ na posição $\lambda_0$, temos assim, as seguintes relações:

**i.** $D =< i_\lambda(G_\lambda) : \lambda \in \Lambda >$;

**ii.** $< i_\lambda(G_\lambda) : \lambda \in \Lambda > \bigcap_{\mu \neq \lambda} < i_\mu(G_\mu) : \mu \in \Lambda >= 1_C, \forall\ \lambda, \mu \in \Lambda.$

**Definição 1.1.32.** *Seja $H$ um grupo, e $\mathcal{F} = \{H_\lambda : \lambda \in \Lambda\}$ uma família de subgrupos normais em $H$, tais que:*

**i.** $H =< H_\lambda : \lambda \in \Lambda >$;

**ii.** $H_\lambda \cap < H_\mu : \mu \in \Lambda,\ \mu \neq \lambda >= 1_H, \forall\ \lambda \in \Lambda.$

*Então, dizemos que $H$ é o produto direto interno de $H_\lambda$, denotado por:*

$$H = Dr^i_{\lambda \in \Lambda} H_\lambda.$$

Consideremos $\pi_\lambda : D \longrightarrow G_\lambda$ a projeção canônica. Se definirmos $\varphi : Dr_{\lambda \in \Lambda} G_\lambda \longrightarrow Dr^i_{\lambda \in \Lambda} H_\lambda$, tal que $\varphi((g_\lambda)) = \prod \pi_\lambda(g_\lambda)$. Então $\varphi$ é um isomorfismo; $\varphi$ é um homomorfismo: $\varphi((g^1_\lambda)(g^2_\lambda)) = \prod \pi_\lambda(g^1_\lambda g^2_\lambda)$, pela propriedade 2 do produto direto interno, $\prod \pi_\lambda(g^1_\lambda)\pi_\lambda(g^2_\lambda) = \prod \pi_\lambda(g^1_\lambda) \prod \pi_\lambda(g^2_\lambda) =$

$\varphi(g_\lambda^1)\varphi(g_\lambda^2)$; $\varphi$ é sobrejetora, pois para todo $g = g_1.\cdots.g_n \in H$, este é o produto de um número finito de elementos $g_\lambda \in H_\lambda$, não idênticos à unidade, e, portanto, existe $D \ni x = i_{\lambda_1}(g).\cdots.i_{\lambda_n}(g)$, tal que $\varphi(x) = g$; pela propriedade 2, $Ker(\varphi) = 1$, logo $\varphi$ é um isomorfismo.

**Definição 1.1.33.** *Seja $G$ um grupo, e $H$ e $N$ subgrupos de $G$, tal que $N$ seja normal em $G$, $G = HN$, e $H \cap N = \{1\}$. Então dizemos que $G$ é o produto semidireto interno de $H$ e $N$, e denotamos isso por $G = N \rtimes H$, ou $H \ltimes N$. Nesse caso, podemos definir um homomorfismo de grupos*

$$\begin{gathered}\alpha : H \longrightarrow \mathcal{A}ut(N), \text{ por} \\ h \mapsto \alpha_h : N \longrightarrow N \\ n \mapsto hnh^{-1}.\end{gathered}$$

**Definição 1.1.34.** *Sejam $H$ e $N$ dois grupos, e $\alpha : H \longrightarrow \mathcal{A}ut(N)$ um homomorfismo de grupos. Introduzimos a seguinte notação: $\alpha(h) : N \longrightarrow N$, com $\alpha(h) \doteq h^\alpha$ e $h^\alpha(n) \doteq n^{h^\alpha}$. O produto semidireto externo entre $H$ e $N$, dado o homomorfismo $\alpha$, denotando-o por $H \ltimes_\alpha N$ ou $N_\alpha \rtimes H$, é o conjunto de todos os pares $(n, h)$, $n \in N$ e $h \in H$, com a seguinte operação:*

$$(n, h)(n_1, h_1) = (nn_1^{h^\alpha}, hh_1).$$

**Observação 1.1.35.** *Assim como fizemos para o produto direto externo, consideramos as inclusões:*

$$\begin{array}{ll} i_H : H \hookrightarrow G & i_N : N \hookrightarrow G \\ h \mapsto (1_N, h) & n \mapsto (n, 1_H), \end{array}$$

*definindo $H^* = i_H(H)$ e $N^* = i_N(N)$. Então $H^* \cong H$ e $N^* \cong N$, $H^*$ e $N^*$ são subgrupos de $G$, tais que são verificadas as seguintes condições:*

**i.** $G = N^*H^*$;

**ii.** $N^* \cap H^* = \{1\}$, *sendo $N^*$ subgrupo normal de $G$, isto é, para o par $(x, y)$, com $x \in N$, e $y \in H$,*

$$(x, y)(n, 1_H)(x, y)^{-1} = (xn^{y^\alpha}, y)(x^{-1}, y^{-1}) = (xn^{h^\alpha}(x^{-1})^{y^\alpha}, 1_H) \in N^*.$$

*Então $G = N^* \rtimes H^* = N \rtimes_\alpha H$. Sendo $N$ isomorfo a $N^*$, podemos identificá-los indistintamente no produto semidireto interno, ou no produto semidireto externo.*

**Proposição 1.1.36.** *Seja $G$ um grupo, $H$ e $N$ subgrupos de $G$, sendo o subgrupo $N$ normal em $G$, e $\alpha : H \longrightarrow \mathcal{A}ut(N)$, um homomorfismo. Então podemos identificar o produto semidireto interno com o produto semidireto externo*

$$H \ltimes_\alpha N = H \ltimes N.$$

### 1.1.2 Anéis Semi-Simples

**Definição 1.1.37.** *Seja $M$ um $R$-módulo; $M$ é denominado simples se os seus únicos $R$-submódulos são os triviais, ou seja, $0$ e $M$ são os únicos $R$-submódulos de $M$.*

**Definição 1.1.38.** *Seja $M$ um $R$-módulo. Seja $\{N_i\}_{i\in I}$ uma família de $R$-submódulos do módulo $M$, para o qual $I$ é uma família de índices. Dizemos que $M$ é soma direta dos $R$-submódulos $N_i$ se todo elemento $m \in M$ pode-se escrever, de modo único, na forma*

$$m = \sum_{i\in I} n_i, \quad n_i \in N_i,$$

*ou equivalentemente, satisfazendo as seguintes condições:*

**i.** $M = \sum_{i\in I} N_i$;

**ii.** $N_j \cap (\sum_{I\ni i\neq j} N_i) = 0, \forall\ j \in I.$

*Nesse caso, denotamos*

$$M \cong \bigoplus_{i\in I} N_i,$$

*e cada $N_i$ é um somando direto de $M$.*

**Definição 1.1.39.** *Seja $M$ um $R$-módulo; $M$ é um módulo semi-simples se todo $R$-submódulo de $M$ é um somando direto de $M$.*

**Proposição 1.1.40.** *Seja $M$ um $R$-módulo semi-simples. Se $N$ é um $R$-submódulo de $M$, então $N$ é um módulo semi-simples e contém um módulo simples.*

Podemos considerar um anel $R$ como um $R$-módulo, sobre si mesmo, à esquerda. Denotamos isso por ${}_RR$; note que os $R$-submódulos do ${}_RR$ são os ideais à esquerda do anel $R$.

**Definição 1.1.41.** *Seja $R$ um anel. Dizemos que $R$ é semi-simples se o $R$-módulo ${}_RR$ for semi-simples.*

Com o seguinte teorema, estaremos em condições de caracterizar um anel semi-simples a partir de seus ideais minimais laterais.

**Teorema 1.1.42.** *Seja $M$ um $R$-módulo; $M$ é semi-simples, se e somente se, $M$ é soma direta de $R$-submódulos simples.*

Dizemos que o comprimento de um $R$-módulo semi-simples é o número de componentes simples na decomposição do módulo em soma direta de $R$-módulos simples.

**Definição 1.1.43.** *Um anel $R$ é artiniano(noetheriano) se toda cadeia descendente(ascendente) de ideais estabiliza-se, ou equivalentemente, se toda família de ideais de $R$ admite um elemento minimal(maximal).*

**Proposição 1.1.44.** *Se o anel $R$ é semi-simples, então o $R$-módulo à esquerda ${}_RR$ é um módulo de comprimento finito, isto é, ${}_RR$ é um $R$-módulo artiniano e noetheriano.*

**Teorema 1.1.45.** *Seja $R$ um anel. São equivalentes:*

**i.** *Todo $R$-módulo é semi-simples;*

**ii.** *$R$ é semi-simples;*

**iii.** *$R$ é soma direta finita de ideais à esquerda minimais.*

**Teorema 1.1.46.** *Seja $R$ um anel semi-simples com unidade. Então existe uma família $\mathcal{F} = \{e_1, ..., e_n\}$ de elementos de $R$, tal que:*

**i.** $e_i^2 = e_i$, $1 \leq i \leq n$ *(idempotentes);*

**ii.** $e_i e_j = \delta_{ij}$ *(ortogonais);*

**iii.** $1 = \sum_{i=1}^{n} e_i$ *($\mathcal{F}$ é uma família completa de idempotentes ortogonais);*

**iv.** *Se $e_i = e_i' + e_i''$, com $e_i'$ e $e_{ii}'$ idempotentes ortogonais distintos, então $e_i', e_i'' \in \{0, e_i\}$ (primitivos).*

*Reciprocamente, se $\mathcal{F} = \{e_1, ..., e_n\}$ satisfaz as condições acima, então $L_i = Re_i$ é um ideal à esquerda minimal, e*

$$R \cong \bigoplus_{i=1}^{n} L_i.$$

**Lema 1.1.47.** *Seja $R$ um anel semi-simples, $M$ um $R$-módulo simples, e $L$ um ideal à esquerda minimal de $R$. Então $LM \neq 0 \iff L \cong M$. E, nesse caso, $LM = M$.*

**Proposição 1.1.48.** *Seja $R \cong \bigoplus_{i=1}^{n} L_i$, um anel que é isomorfo à soma direta de ideais à esquerda minimais, e seja $M$ um $R$-módulo simples. Então $M \cong L_i$ para algum índice $i$.*

**Lema 1.1.49.** *Seja $L$ um ideal à esquerda minimal de um anel $R$ semi-simples, e seja $B$ a soma de todos os ideais à esquerda de $R$ isomorfos ao ideal $L$. Então $B$ é um ideal bilateral de $R$.*

**Lema 1.1.50.** *Seja $I$ um ideal bilateral de um anel $R$ semi-simples. Se $I$ contém um ideal à esquerda minimal de $L$, então $I$ contém todo ideal à esquerda minimal de $R$ que é isomorfo ao ideal $L$.*

**Teorema 1.1.51.** *Nas condições do lema 1.1.49, o ideal bilateral $B$ é um ideal bilateral minimal. Logo, considerado como anel, ele é simples.*

Se consideramos $R$ um anel semi-simples, cujos ideais à esquerda minimais são $L_i$, sabemos que $R \cong \bigoplus_{i=1}^{n} L_i$. Tomando-se $\mathcal{S} = \{L_{i_1}, \cdots, L_{i_j}\}$, $1 \leq i_j \leq n$, um conjunto com todos, a menos de isomorfismos, os tais ideais não isomorfos entre si. Então $A_i = \sum_{S \ni L_{j_i} \cong L_k} L_k$ é um ideal bilateral de $R$, com $1 \leq k \leq n$ e $1 \leq i \leq |S| = m$.

**Teorema 1.1.52.** *Com a notação acima, se $A$ é um anel semi-simples, então o anel $A$ é isomorfo à soma direta de um número finito de anéis simples, isto é, $R \cong \bigoplus_{i}^{m} A_i$, com $A_i A_j = 0$, se $i \neq j$.*

**Teorema 1.1.53.** *(**Teorema de Artin-Wedderburn**) Um anel $R$ é semi-simples, se e somente se,*

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s),$$

*no qual $D_i$ é um anel de divisão, e $M_{n_i}(D_i)$ é uma matriz $n_i \times n_i$ sobre $D_i$ com $1 \leq i \leq s$.*

## 1.2 anéis de grupo

**Definição 1.2.1.** *Seja $G$ um grupo, e $R$ um anel. O anel de grupo $RG$ é o conjunto formado pelas somas formais $\sum_{g \in G} \alpha_g g$, sendo $\alpha_g = 0$, a exceção de um número finito de termos em cada soma, e $\alpha_g \in R$, $g \in G$, com as seguintes operações:*

$$\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g,$$

$$(\sum_{g \in G} \alpha_g g)(\sum_{h \in G} \beta_h h) = \sum_{g,h \in G} (\alpha_g \beta_h) gh,$$

$$rg = gr, \ \forall g \in G, \ e \ r \in R.$$

*Definimos o suporte de $\alpha \in RG$ como o conjunto dos elementos $g \in G$, cujo escalar $\alpha_g \in R$ seja não nulo, isto é, se $\alpha = \sum_{g \in G} \alpha_g g$. Então*

$$Supp(\alpha) = \{g \in G \text{ tal que } \alpha_g \neq 0\}.$$

*Pela definição de $RG$, temos que a cardinalidade de $Supp(\alpha)$ é finita.*

**Definição 1.2.2.** *Seja $R$ um anel comutativo. Uma $R$-álgebra é um anel $A$, com estrutura de $R$-módulo, tal que a multiplicação de $A$, como anel, e a multiplicação, com relação à estrutura de $R$-módulo, são compatíveis no seguinte sentido*

$$x(ab) = (xa)b = a(xb) \forall x \in R; a, b \in A.$$

*Quando $R$ é um corpo, uma base para a $R$-álgebra $A$ é uma base para $A$ vista como $R$-espaço vetorial. Nesse caso, a $R$-álgebra $A$ é dita de dimensão finita sobre $R$ se admite uma $R$-base finita.*

**Proposição 1.2.3.** *Seja $R$ um anel comutativo, e $G$ um grupo. O anel de grupo $RG$ é uma $R$-álgebra.*

**Definição 1.2.4.** *Seja dada uma seqüência de $R$-módulos e $R$-homomorfismos*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \longrightarrow \cdots .$$

*Essa seqüência é dita exata em $M_i$, quando $Im(\varphi_i) = Ker(\varphi_{i+1})$. Uma seqüência é exata quando é exata em cada componente $M_i$.*

**Definição 1.2.5.** *Dizemos que um $R$-módulo $N$ é plano se dada uma seqüência exata à esquerda*

$$0 \xrightarrow{\varphi_1} \cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \longrightarrow \cdots .$$

*Então, a seqüência*

$$0 \xrightarrow{\varphi_1 \otimes 1} \cdots \longrightarrow M_{i-1} \bigotimes_R N \xrightarrow{\varphi_i \otimes 1} M_i \bigotimes_R N \xrightarrow{\varphi_{i+1} \otimes 1} M_{i+1} \bigoplus_R N \longrightarrow \cdots$$

*é exata à esquerda.*

**Teorema 1.2.6.** *Seja $R$ um anel, e sejam os grupos $A, G, H$. Se $RG \cong RH$, então $R[G \times A] \cong R[H \times A]$.*

**Demonstração.** Seja $\theta : RG \longrightarrow RH$ um isomorfismo. Então a seqüência

$$0 \longrightarrow RG \xrightarrow{\theta} RH \longrightarrow 0$$

é exata. O anel de grupo $RA$ é uma álgebra livre, portanto, um módulo plano. Dessa forma, a seqüência

$$0 \longrightarrow RG \bigotimes_R RA \xrightarrow{\theta \otimes 1} RH \bigotimes_R RA \longrightarrow 0$$

é exata. Logo $RG \bigotimes_R RA \cong RH \bigotimes_R RA$ $(*)$. Portanto, é suficiente mostrar que $R[G \times A] \cong RG \bigotimes_R RA$. Para isso, definimos

$$\begin{aligned} \nu : RG \times RA &\longrightarrow R[G \times A] \\ (\sum_{g \in G} r_g g, \sum_{a \in G} s_a a) &\mapsto \sum_{g,a \in G} r_g s_a (g,a), \quad \text{que é uma função balanceada.} \end{aligned}$$

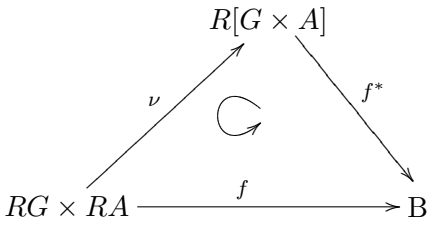
Seja

$$f : RG \times RA \longrightarrow \mathrm{B} \quad \text{uma aplicação balanceada.}$$

Definimos

$$\begin{aligned} f^* : R[G \times A] &\longrightarrow \mathrm{B} \\ \sum_{g,a \in G} r_{ga}(g,a) &\mapsto \sum_{g,a \in G} r_{ga} f(g,a). \end{aligned}$$

Então, temos que $f^* \circ \nu = f$, isto é, o diagrama




comuta. Pela propriedade universal do produto tensorial, temos que $R[G \times A] \cong RG \bigotimes_R RA$. Logo, obtemos que

$$R[G \times A] \cong RG \bigotimes_R RA \cong RH \bigotimes_R RA \cong R[H \times A].$$

□

**Corolário 1.2.7.** *Seja $C_\infty$ um grupo cíclico infinito. Se $\mathbb{Z}G \cong \mathbb{Z}H$, então $\mathbb{Z}[G \times C_\infty] \cong \mathbb{Z}[H \times C_\infty]$.*

**Teorema 1.2.8.** ***(Teorema de Mashke)*** *Suponha $|G| < \infty$ e $MDC(char(K), |G|) = 1$. Então $KG$ será semi-simples.*

**Demonstração.** Seja $M \subset KG$, um $KG$-submódulo. Mostremos que $\exists\ N \subset KG$, submódulo, tal que $KG \cong M \oplus N$. De fato, $|G| < \infty \Longrightarrow dim_K KG = |G|$. Como espaço vetorial, então, $dim_K M$ é finita. Vamos construir $N$, tal que seja um $KG$-módulo. Seja $\pi$ a projeção de $KG$ em M

$$\begin{aligned} \pi : KG &\longrightarrow M \\ m + n &\mapsto m. \end{aligned}$$

Defina

$$\begin{aligned}\hat{\pi} : KG &\longrightarrow KG \\ \alpha &\mapsto \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(\alpha g).\end{aligned}$$

Ocorre que $g^{-1}\pi(\alpha g) \in M$, pois $M$ é $KG$-submódulo; de fato, $\pi(KG) \subset M$, $\hat{\pi}(\alpha) \in M$, portanto, $\mathcal{I}m(\hat{\pi}) \subset M$. Tome $m \in KG$, $\hat{\pi}(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(mg)$, mas $\pi(mg) \in M \implies \pi(mg) = \pi(m)g = g\pi(m)$, então, $\hat{\pi}(m) = \pi(m)$, para todo $m \in KG$. Portanto, $\hat{\pi} = \hat{\pi}^2$. Logo $\hat{\pi}$ é uma projeção; $\hat{\pi}$ é $KG$-linear, pois sabemos que $\hat{\pi}$ é $K$-linear. De fato, $\pi$ é $K$-linear, seja $h \in G$, $x \in KG$, então $\hat{\pi}(hx) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(ghx) = \frac{1}{|G|}\sum_{g\in G} h(h^{-1}g^{-1})\pi(ghx) = \frac{h}{|G|}\sum_{g\in G}(gh)^{-1}\pi(ghx) = \frac{h}{|G|}\sum_{y\in G} y^{-1}\pi(yx) = h\hat{\pi}(x)$. Portanto, $\hat{\pi}$ é $KG$-linear. Então para a seqüência exata

$$1 \longrightarrow Ker(\hat{\pi}) \longrightarrow KG \underset{i}{\overset{\hat{\pi}}{\rightleftarrows}} M,$$

$\hat{\pi} \circ i = i$. Portanto, a seqüência cinde, e $KG \cong M \oplus Ker(\hat{\pi})$. □

**Corolário 1.2.9.** *Para todo $K \supset \mathbb{Q}$ e $|G| < \infty$, $KG$ é semi-simples. Ou seja, $KG \cong \sum_{i=1}^{n} M_{n_i}(D_i)$.*

**Lema 1.2.10.** *Nas condições do corolário 1.2.9, se $K$ é um corpo algebricamente fechado, então as seguintes afirmações são verdadeiras:*

**i.** *$D_i = K$, para todo $i$;*

**ii.** $|G| = \sum_{i=1}^{n} n_i^2$;

**iii.** *$dim_K(\mathcal{Z}(KG)) = n$, o número de componentes simples de $KG$;*

**iv.** $\mathcal{Z}(KG) \cong \bigoplus_{i=1}^{n} K$.

**Demonstração.** Sendo $G$ um grupo finito. Então $[KG : K] < \infty$. O anel $KG$ é semi-simples e, portanto, pelo Teorema de Artin-Wedderburn $KG \cong \bigoplus_{i}^{s} M_{n_i}(D_i)$. Então $dim_K(KG) = k = \sum_{i=1}^{s} dim_K(M_{n_i}(D_i)) = \sum n_i^2[D_i : K] < \infty$ $(*)$. Logo $dim_K(M_{n_i}(D_i)) < \infty \implies [D_i : K] < \infty$. Daí, $D_i$ é algébrico sobre $K$ para todo $1 \leq i \leq s$. Seja $\alpha \in D_i$, e $Irr(\alpha, K)(X) = F_\alpha(X) \in K[X]$ o polinômio irredutível de $\alpha$. Esse polinômio é não nulo, pois sendo $D_i$ algébrico,

podemos supor que $[K(\alpha) : K] = m_i$, logo o conjunto $B = \{\alpha, \cdots, \alpha^{m_i}\}$ é linearmente dependente sobre $K$. Ora, sendo $K$ um corpo algebricamente fechado, $\alpha \in K$. Logo $D_i = K$. De $(*)$ e $[D_i : K] = 1$, concluímos que $|G| = \sum_{i=1}^{s} n_i^2$. Para o item *iii.*, basta observar que $\mathcal{Z}(M_{n_i}(D_i)) \cong \mathcal{Z}(D_i)I_{id} = \{diag(\lambda \cdots \lambda) : \lambda \in \mathcal{Z}(D_i)\}$, logo $dim_K(\mathcal{Z}(M_{n_i}(D_i))) = [\mathcal{Z}(D_i) : K]$. Portanto, $dim_K(\mathcal{Z}(KG)) = \sum_{i=1}^{s}[K : K] = s$, o número de componentes simples de $KG$, pois $K$ é algebricamente fechado. □

**Corolário 1.2.11.** *Se $K$ é algebricamente fechado, e $|G|$ é finito, então $dim_K(\mathcal{Z}(KG))$ é o número de classes de conjugação de $G$.*

**Definição 1.2.12.** *Seja $G$ um grupo, e $R$ um anel. A aplicação*

$$\begin{aligned} \epsilon : RG &\longrightarrow R \\ \sum_{g\in G} \alpha_g g &\mapsto \sum_{g\in G} \alpha_g, \end{aligned}$$

*denomina-se homomorfismo de aumento.*

O homomorfismo de aumento é um homomorfismo do anel $RG$. Portanto, $Ker(\epsilon)$, o núcleo do homomorfismo, é um ideal de $RG$.

**Teorema 1.2.13.** *Seja $G$ um grupo, e $N$ um subgrupo normal em $G$. Então $\Delta(G, N) \doteq < 1 - h, h \in N >$ é ideal de $RG$.*

**Corolário 1.2.14.** *Nas condições do teorema 1.2.13, $RG/\Delta(G, N) \cong R(G/N)$.*

**Definição 1.2.15.** *Dizemos que um homomorfismo de anéis*

$$\varphi : RG \longrightarrow RH$$

*preserva aumento se dados $\epsilon_G$ e $\epsilon_H$, os homomorfismos de aumento dos anéis $RG$ e $RH$, respectivamente, e $\alpha \in RG$. Então*

$$\epsilon_G(\alpha) = \epsilon_H(\varphi(\alpha)).$$

*Isto é, o diagrama*

$$\begin{array}{ccc} RG & \xrightarrow{\varphi} & RH \\ & \searrow^{\epsilon_G} & \downarrow{\scriptstyle \epsilon_H} \\ & & R \end{array}$$

*comuta. Nesse caso, se $\varphi$ é um isomorfismo que preserva aumento, dizemos que este é um isomorfismo normalizado.*

**Definição 1.2.16.** *Seja $G$ um grupo, e $R$ um anel. Dado $\alpha \in RG$, $\alpha = \sum_{g\in G} \alpha_g g$, definimos o traço de $\alpha$ por $tr(\alpha) = \alpha_1$. Sendo $1 \in G$ o elemento neutro do grupo $G$.*

**Teorema 1.2.17.** *Seja $\phi$ um isomorfismo de anéis de grupo sobre o anel dos inteiros. Então existe um isomorfismo, definido a partir de $\phi$, que preserva aumento e traço.*

**Demonstração.** Seja $\phi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ um isomorfismo. Definimos

$$\hat{\phi} : \mathbb{Z}G \longrightarrow \phi(\mathbb{Z}G) = \mathbb{Z}H$$
$$\sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \frac{\alpha_g}{\epsilon_H(\phi(g))}\phi(g).$$

Mostremos que $\hat{\phi}$ é um isomorfismo de anéis que preserva aumento e traço. A aplicação está bem definida, pois, $\epsilon_H(\phi(g)) = \pm 1$. Verificamos que $\hat{\phi}(1) = 1$; $\hat{\phi}$ é um homorfismo de anéis. Tomemos $a, b \in \mathbb{Z}G$, com $a = \sum a_g g$, $b = \sum b_g g$. Então $\hat{\phi}(ab) = \hat{\phi}(\sum_{g\in G} a_g g \sum_{h\in G} b_h h) = \hat{\phi} \sum_{g,h\in G} (a_g b_h gh) = \sum_{g,h\in G} \frac{a_g b_h}{\epsilon_H(\phi(gh))}\phi(gh) = \sum_{g\in G} \frac{a_g}{\epsilon_H(\phi(g))}\phi(g) \sum_{h\in G} \frac{b_h}{\epsilon_H(\phi(h))}\phi(h) = \hat{\phi}(a)\hat{\phi}(b)$, também, para $\hat{\phi}(a+b) = \hat{\phi}(\sum_{g\in G}(a_g + b_g)g) = \sum_{g\in G} \frac{a_g + b_g}{\epsilon_H(\phi(g))} g = \hat{\phi}(a) + \hat{\phi}(b)$; a aplicação é injetiva, pois se tomamos $a \in \mathrm{Ker}(\hat{\phi}) \Longrightarrow \sum_{g\in G} \frac{a_g}{\epsilon_H(\phi(g))}\phi(g) = 0$ e $\phi(g) \neq 0 \Longrightarrow \alpha_g = 0$, porque $G$ é uma $\mathbb{Z}$-base. Logo $a = 0$; $\hat{\phi}$ é sobrejetiva. Com efeito, dado $a \in \mathbb{Z}H$, $a = \sum_{g'\in H} a_{g'} g' = \sum_{g=\phi^{-1}(g')\in G} a_g \phi(g) = \sum_{g\in G} \frac{a_g \epsilon_H(\phi(g))}{\epsilon_H(\phi(g))}\phi(g) = \sum_{g\in G} \frac{a'_g}{\epsilon_H(\phi(g))}\phi(g) = \hat{\phi}(a')$, para $a' = \sum_{g\in G} a_g \epsilon_H(\phi(g))g \in \mathbb{Z}G$. Com isso, podemos mostrar que $\hat{\phi}$ preserva aumento e traço. Seja $\alpha = \sum_{g\in G} \alpha_g g$ um elemento de $\mathbb{Z}G$. Temos que $\epsilon_H(\hat{\phi}(\alpha)) = \epsilon_H(\sum_{g\in G} \hat{\phi}(\alpha_g g)) = \epsilon_H(\sum_{g\in G} \alpha_g \hat{\phi}(g)) = \epsilon_H(\sum_{g\in G} \alpha_g \frac{\phi(g)}{\epsilon_H(\phi(g))}) = \sum_{g\in G} \frac{\alpha_g}{\epsilon_H(\phi(g))}\epsilon_H(\phi(g)) = \sum_{g\in G} \alpha_g = \epsilon_G(\alpha)$. Portanto, $\hat{\phi}$ preserva aumento. Pela definição de traço, $tr(\alpha) = \alpha(1)$; $tr(\hat{\phi}(\alpha)) = \frac{\alpha_1}{\epsilon_H(\phi(1))}\phi(1)$, sendo $\phi(1) = 1_h$, e $\epsilon_H(\phi(1)) = 1$. Então $\hat{\phi}$ preserva traço. □

**Definição 1.2.18.** *Seja $RG$ um anel de grupo. Denotamos por $\mathcal{U}(RG)$ o conjunto das unidades de $RG$, isto é, $\mathcal{U}(RG) = \{\alpha \in RG$: $\exists\ \beta \in RG$, tal que $\alpha\beta = \beta\alpha = 1\}$. As unidades $u = vg$, tais que $v \in \mathcal{U}(R)$ e $g \in G$ são chamadas Unidades Triviais. Se $u \in \mathcal{U}(RG)$ é um elemento de torção, então $u$ é chamada unidade de torção de $RG$. As unidades, $u \in \mathcal{U}(RG)$, de aumento um, $\epsilon(u) = 1$, são chamadas unidades normalizadas. Denotamos por $\mathcal{U}_1(RG)$ o conjunto das unidades normalizadas de $RG$, isto é, $\mathcal{U}_1(RG) = \{u \in \mathcal{U}(RG)$: $\epsilon(u) = 1\}$, que é um subgrupo do grupo das unidades do anel de grupo.*

Se $|G| < \infty$, então toda unidade trivial é de torção. As propriedades "de torção" e "trivial" estão intrinsecamente, em alguns casos excepcionais, relacionadas, como mostra o teorema de Berman-Higman.

**Teorema 1.2.19.** *(**Berman-Higman-Passman**)([21], 6.45.8) Sejam $G$ um grupo qualquer, $\gamma = \sum_{g\in G} \gamma_g g$, uma unidade de torção de $\mathbb{Z}G$ e $\gamma_1 \neq 0$. Então $\gamma = \pm 1$.*

**Corolário 1.2.20.** *(**Bovdi-Marciniak-Sehgal**) Se $u$ é uma unidade central de torção de um anel de grupo $\mathbb{Z}G$, então $u$ é trivial.*

**Observação 1.2.21.** *Neste trabalho, não apresentamos a demonstração do teorema 1.2.19, pois esta é uma demonstração clássica, encontrada na bibliografia. Para o corolário 1.2.20, que trata de unidades centrais, julgamos conveniente dar duas demonstrações para esse corolário: a primeira, no final deste capítulo e a segunda, no terceiro capítulo. Ao longo de algumas demonstrações neste trabalho, referimo-nos ao corolário 1.2.20, "para o caso finito", ou seja, em condições onde é suficiente supor que o referido grupo $G$, desse corolário, seja um grupo finito. Isso ocorre, mais exatamente, na demonstração do teorema 3.2.2, que é o mesmo corolário 1.2.20, e do corolário 3.1.10. Vale mencionar que essa primeira demonstração é inédita.*

**Teorema 1.2.22.** *Sejam $G$ e $H$ dois grupos. Se $\mathbb{Z}G \cong \mathbb{Z}H$, então $\mathcal{U}_1(\mathbb{Z}G) \cong \mathcal{U}_1(\mathbb{Z}H)$.*

**Demonstração.** Pelo teorema 1.2.17, existe $\hat{\phi} : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ um isomorfismo que preserva aumento. Então $\hat{\phi}(\mathcal{U}_1(\mathbb{Z}G)) \subseteq \mathcal{U}_1(\mathbb{Z}H)$, analogamente para $\hat{\phi}^{-1}$, obtemos que $\mathcal{U}_1(\mathbb{Z}G) \cong \mathcal{U}_1(\mathbb{Z}H)$. □

Uma conseqüência imediata, que simplifica muito a condição de isomorfismo entre anéis de grupo de um isomorfismo normalizado, é que podemos, quando $RG \cong RH$, considerar $RG = RH$. Essa identificação é elucidada a partir do seguinte teorema:

**Teorema 1.2.23.** *Seja $RG \cong RH$, tal que $\theta : RG \longrightarrow RH$ seja um isomorfismo normalizado. Então $RG^\theta = RH$, isto é, $RG = RH$, onde $\theta(G) = G^\theta$.*

**Demonstração.** Mostremos que $G^\theta$ é uma $R$-base de $RH$. De fato, seja $h \in \theta(G)$, existe um único $g \in G$, $\theta(g) = h$; $\sum_{h\in G^\theta} r_h h = 0 \Longrightarrow \sum_{h\in G^\theta} r_h \theta^{-1}(h) = \sum_{h\in G^\theta} r_h g = 0$. Portanto, $r_h = 0$. Seja $x \in RH$, então $\theta^{-1}(x) \in RG$. Portanto, $\theta^{-1}(x) = \sum_{g\in G} x_g g \Longrightarrow x = \theta(\theta^{-1}(x)) = \sum_{g\in G} x_g \theta(g)$ $\in R\theta(G)$. Daí, $RG^\theta = RH$. Sendo $G \cong G^\theta$, podemos identificar $G$ com $G^\theta$ e, portanto, $RG = RH$. □

**Definição 1.2.24.** *Seja $G$ um grupo, e $R$ um domínio de integridade de característica zero, que satisfaz $\mathcal{U}(R) \cap \{o(g)$, tal que $g \in G$, $o(g)$ um número primo $\} = \{1\}$, isto é, os elementos de ordem prima do grupo $G$ não são invertíveis em $R$. Nesse caso, $R$ é chamado um anel $G$-adaptado.*

**Lema 1.2.25.** *([22], 5.37.1) Qualquer grupo finito de unidades normalizadas de $\mathbb{Z}G$ é um conjunto de elementos linearmente independentes em $\mathbb{Z}G$.*

**Lema 1.2.26.** *([22], 5.37.3) A ordem de qualquer $H \subset \mathcal{U}_1(\mathbb{Z}G)$ divide a ordem de $G$.*

**Corolário 1.2.27.** *([22], 5.37.2) Qualquer subgrupo finito de $\mathcal{U}_1(\mathbb{Z}G)$ tem ordem no máximo igual a $|G|$.*

**Lema 1.2.28.** *([22], 5.37.4) Se $H$ é subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$, com $|H| = |G|$, então $\mathbb{Z}H = \mathbb{Z}G$.*

O lema seguinte é uma generalização desses resultados ([21], 5.37.1 a 5.37.4) para um anel $R$-adaptado e $G$ um grupo finito.

**Lema 1.2.29.** *Seja $G$ um grupo finito. Se $R$ é $G$-adaptado, e $G_1$ é um subgrupo finito das unidades normalizadas de $RG$, então*

**i.** *$|G_1|$ divide $|G|$;*

**ii.** *se $|G_1| = |G|$, então $RG = RG_1$.*

**Demonstração.** A primeira parte é conseqüência imediata do lema 1.2.26 para anéis $R$-adaptados. Para a segunda afirmação, é suficiente verificar que se $|G| = |G_1|$, então $G_1$ é uma $R$-base de $RG$. Seja $\sum_{g\in G_1} a_g g = 0$, calculamos $tr(\sum_{g\in G_1} a_g g h^{-1}) = a_1$ para cada $h \in G_1$. Logo $a_h = 0$. Afirmamos que $G_1$ gera $RG$: $\forall\ h \in G\ \exists\ x_g \in R$, tal que $h = \sum_{g\in G_1} x_g g \in RG_1$. Para isso, inicialmente, mostremos que existe $a \in R$, $ah = \sum_{g\in G_1} a_g g$. De fato, seja $K$ o corpo de frações de $R$. Então $dim_K KG = dim_K KG_1$, pois $|G| = |G_1|$. Logo como $h \in G$, $h = \sum_{g\in G_1} k_g g$, sendo $k_g = \frac{a_g}{b_g}$, $a_g$ e $0 \neq b_g \in R$. Seja $a = \prod_{g\in G_1} b_g$ nesse caso, $ah \in RG_1$. Então para todo $b \in G_1$, considere o traço de $ahb^{-1} = \sum_{g\in G_1} a_g g b^{-1}$, $tr(ahb^{-1}) = ahb_1^{-1} = a_b$. Daí $a|a_b$. Logo $h = \sum_{g\in G_1} \frac{a_g}{a} g = \sum x_g g \in RG_1$, com $x_g = \frac{a_g}{a}$. □

Para $RG \cong RH$, existem casos onde é importante determinar em que condições os subgrupos normais em $G$ estão em correspondência com os subgrupos normais do grupo $H$. Para os subgrupos normais finitos de $G$, o seguinte teorema mostra que há uma correspondência biunívoca entre esses subgrupos e os subgrupos normais finitos do grupo $H$.

**Teorema 1.2.30.** ***(Teorema da Correspondência para Subgrupos Normais Finitos)*** *Seja $G$ um grupo, e $R$ um anel $G$-adaptado. Suponha que $RG \cong RH$. Sendo $L_{FN}G$ o reticulado*

*de subgrupos normais finitos em $G$, e $L_{FN}H$ o reticulado de subgrupos normais finitos em $H$, as seguintes afirmações são verdadeiras:*

**i.** *Existe uma bijeção $\phi$ entre $L_{FN}G$ e $L_{FN}H$, isto é*

$$\begin{aligned} \phi : L_{FN}G &\longrightarrow L_{FN}H \\ G \rhd M &\longleftrightarrow N \lhd H; \end{aligned}$$

**ii.** *Se $\phi(M) = N$, então $\Delta(G, M) = \Delta(H, N)$.*

A demonstração desse teorema encontra-se em ([21], III.4.17, III.4.18 e III.4.19).

**Definição 1.2.31.** *Seja $RG$ um anel de grupo. Denotando-se $\sim$ a relação de conjugação em um grupo $G$, definida em 1.1.19, para $\alpha \in RG$, $\alpha = \sum_{g\in G} \alpha_g g$, definimos*

$$\tilde{\alpha}_g := \sum_{h\sim g} \alpha_g =: t_{cl(g)}(\alpha).$$

**Teorema 1.2.32.** *([10], Teorema 2.1) Seja $G$ um grupo que contém um subgrupo normal $H$ localmente noetheriano, tal que $G/H$ é um grupo de torção. Se $\alpha \in \mathcal{U}_1\mathbb{Z}G$ é uma unidade de torção, e $g \in G$ é um elemento de ordem infinita, então $\tilde{\alpha}(g) = 0$.*

Esse resultado, originalmente, foi apresentado em [22], proposição 47.5, por Bovdi-Marciniak-Sehgal para grupos noetherianos.

**Teorema 1.2.33.** *([10], Corolário 2.3) Seja $K$ um grupo, e $H$ um subgrupo localmente noetheriano, livre de torção e normal em $K$, tal que $K/H$ seja um grupo de torção. Então o homomorfismo canônico $\psi : \mathbb{Z}K \longrightarrow \mathbb{Z}(K/H)$ é injetivo sobre os subgrupos de torção de $\mathbb{Z}K$. Em particular, todo subgrupo de torção de $\mathcal{U}_1(\mathbb{Z}K)$ é finito, se o índice de $H$ em $K$ for finito.*

**Demonstração.** Seja $N < \mathcal{U}_1(\mathbb{Z}K)$, subgrupo finito, e $\alpha \in N$, tal que $\psi(\alpha) = 1$. Queremos provar que $\alpha = 1$. De fato, seja $T$ um transversal de $H$ em $G$, $T = \{t_\lambda\}$, $\lambda \in \Lambda$, sendo $\Lambda$ um conjunto de índices. Então podemos escrever $\alpha = \sum_{\lambda\in\Lambda} \alpha_\lambda t_\lambda$, $t_\lambda \in T$, e $\alpha_\lambda \in \mathbb{Z}H$. Logo $1 = \psi(\alpha) = \psi(\alpha_1) = \epsilon(\alpha_1)$. Portanto, $\sum_{h\in H} \alpha_h = 1$, e existe $h_0 \in H$, tal que $\tilde{\alpha}(h_0) \neq 0$, por 1.2.31, $h_0 = 1$. Assim, por 1.2.19, $\alpha = 1$. Portanto, $\psi|_N$ é injetiva. □

**Proposição 1.2.34.** *Nas condições do teorema anterior, seja $K$ um grupo com $G$ e $H$ subgrupos de $K$, tais que $G$ seja um subgrupo finito, $H$ um subgrupo normal em $K$, e $W$ um grupo, tal que $\mathbb{Z}K \cong \mathbb{Z}W$. Se $T$ é um subgrupo de $W$, tal que $|G| = |T|$, e $\mathbb{Z}(K/H) \cong \mathbb{Z}G$, então $\mathbb{Z}T \cong \mathbb{Z}G$.*

**Demonstração.** Seja o isomorfismo $\Psi : \mathbb{Z}W \longrightarrow \mathbb{Z}K$. Pelo teorema anterior o homomorfismo canônico $\psi : \mathbb{Z}K \longrightarrow \mathbb{Z}(K/H)$ é injetivo, quando restrito a $F$, um subgrupo de torção de $\mathbb{Z}K$. Sendo $\Psi$ um isomorfismo, $T \cong \Psi(T) \subset \mathbb{Z}K$. Portanto, $|T| = |\Psi(T)|$. Considere $F = \Psi(T)$, então $\psi|_F$ é injetiva. Sendo $\psi(\Psi(T)) \cong \Psi(T) \cong T$, esses subgrupos têm a mesma ordem. Pelo lema 1.2.29, com $\mathbb{Z}$ um anel $G$-adaptado, sendo $\psi(\Psi(T)) \subset \mathbb{Z}K/H = \mathbb{Z}G$, e $G \subset \mathcal{U}_1\mathbb{Z}(K/H)$, então $\mathbb{Z}\psi(\Psi(T)) = \mathbb{Z}G$. Logo $\mathbb{Z}T \cong \mathbb{Z}G$. □

### 1.2.1 Unidades Centrais em anéis de grupo

**Lema 1.2.35.** *Seja $G$ um grupo finito, e $k_1, \cdots, k_s$ as classes de conjugação de $G$. Seja $\mathcal{K}_i = \sum_{x \in k_i} x \in \mathbb{Z}G$, $1 \leq i \leq s$. Então $\{\mathcal{K}_1, \cdots, \mathcal{K}_s\}$ forma uma base do $\mathcal{Z}(\mathbb{Z}G)$.*

**Demonstração.** Inicialmente, mostramos que $\mathcal{K}_i \in \mathcal{Z}(\mathbb{Z}G)$. De fato, $g\mathcal{K}_i g^{-1} = g \sum_{x \in k_i} xg^{-1} = \sum_{x \in k_i} gxg^{-1} = \sum_{x \in k_i} x = \mathcal{K}_i$. Se $\sum_{j=1}^{s} \alpha_j \mathcal{K}_j = 0 = \sum_{j=1}^{s} \alpha_i (\sum_{x \in k_j} x) = \sum_{j=1}^{s} \sum_{x \in k_j} \alpha_j x \Longrightarrow \alpha_j = 0$, pois $Supp(\mathcal{K}_i)$ são disjuntos. Finalmente, se $\sum_{g \in G} \alpha_g g = \alpha \in \mathcal{Z}(\mathbb{Z}G)$, e $h \in G$, então $h\alpha h^{-1} = \alpha = \sum_{g \in G} \alpha_g g^h = \sum_{g \in G} \alpha_g g$. Portanto, $\alpha_{g^h} = \alpha_g$, para todo $h \in G$. Logo $\alpha$ é combinação linear dos $\mathcal{K}_i$. □

**Teorema 1.2.36.** *Seja $G$ um grupo, e $\Delta(G)$ o $FC$-subgrupo de $G$. Então $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) \subset \mathbb{Z}\Delta(G)$.*

**Demonstração.** Seja $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$. Vamos provar que $Supp(u) \subset \Delta(G)$. Supomos o contrário, isto é, que $Supp(u) \not\subset \Delta(G)$. Seja $g_0 \in Supp(u)$ e $g_0 \notin \Delta(G)$; $g_i \in cl(g_0) \Longrightarrow \exists x \in G$, tal que $g_i = g_0^x$. Sendo $u$ um elemento central, $u = u^x = (\sum_{g \in G} \alpha_g g)^x = \alpha_{g_0} g_0^x + \sum_{g_0 \neq g \in G} \alpha_g g^x = \alpha_{g_0} g_i + \sum_{g_0 \neq g \in G} \alpha_g g^x$, com $g_i \notin \{g^x, g_0 \neq g \in G\}$, portanto, $g_i \in Supp(u)$, então $cl(g_0) \subset Supp(u)$. Contradição. Pois $g_0$ foi tomado de modo que $|cl(g_0| = \infty$ e $|Supp(u)| < \infty$. Logo $Supp(u) \subset \Delta(G)$. Portanto, $u \in \mathbb{Z}\Delta(G)$. □

**Corolário 1.2.37.** *Seja $u$ uma unidade central normalizada de um anel de grupo sobre os inteiros. Então o grupo gerado pelo suporte da unidade é um $FC$-grupo finitamente gerado.*

**Demonstração.** Pelo teorema, $u \in \mathbb{Z}\Delta(G)$, logo $G_0 =< g : g \in Supp(u) > \subset \Delta(G)$ é um $FC$-grupo finitamente gerado. □

### 1.2.2 Produto Cruzado

**Definição 1.2.38.** ***Produto Cruzado*** *([21], VI.1) Seja $G$ um grupo, e $R$ um anel. Suponhamos conhecida uma função $\rho : G \times G \longrightarrow \mathcal{U}(R)$, chamada fator de sistema, e automorfismos $\sigma_g \in \mathcal{A}ut(R)$ de conjugação para cada $g \in G$. Supondo que $\rho$ e $\sigma$ satisfaçam, para cada $g, h, l \in G$, e $a \in R$, as seguintes propriedades:*

$$\rho(g,h)\rho(gh,l) = \sigma_g(\rho(h,l))\rho(g,hl); \tag{1.1}$$

$$\rho(h,g)\sigma_{hg}(a) = \sigma_h(\sigma_g(a))\rho(h,g). \tag{1.2}$$

*Então, pelo produto cruzado $R(G,\rho,\sigma)$ de $G$ sobre $R$ com fator de sistema $\rho$ e automorfismos $\sigma$, que denotaremos por $R * G$, entendemos o conjunto das somas finitas*

$$\{\sum a_i\overline{g}_i : a_i \in R, g_i \in G\},$$

*o qual $\overline{g}_i$ é um símbolo correspondente a $g_i$. Igualdade e adição estão definidas componente a componente, e para $g, h \in G$, e $a \in R$, temos*

$$\overline{g}\,\overline{h} = \rho(g,h)\overline{gh}; \tag{1.3}$$

$$\overline{g}a = \sigma_g(a)\overline{g}. \tag{1.4}$$

**Proposição 1.2.39.** *Seja $G$ um grupo, e $R$ um anel. O produto cruzado $R * G$ é um anel associativo.*

**Demonstração.** Estendendo-se as aplicações 1.3 e 1.4, distributivamente, não há problemas em verificar que $R*G$ é um grupo abeliano com a propriedade de soma. Para o produto, verificamos que se $a, b \in R * G$

$$ab = \sum_{g\in G} a_g\overline{g}\sum_{h\in G} b_h\overline{h} = \sum_{g,h\in G} a_g\overline{g}b_h\overline{h} = \sum_{g,h\in G} a_g\sigma_g(b_h)\overline{g}\,\overline{h} = \sum_{g,h\in G} a_g\sigma_g(b_h)\rho(g,h)\overline{gh} = \sum_{l=gh} c_l\overline{l}.$$

com $c_l = a_g\sigma_g(b_h)\rho(g,h) \in R$, portanto, $ab \in R * G$. A propriedade associativa decorre da definição da ação 1.3 e da torção 1.4. Com efeito, inicialmente verificamos que a associatividade é garantida para os escalares com os elementos da base

$$(\overline{g}\,\overline{h})a = (\rho(g,h)\overline{gh})a = \rho(g,h)\sigma_{gh}(a)\overline{gh};$$
$$\overline{g}(\overline{h}a) = \overline{g}\sigma_h(a)\overline{h} = \sigma_g(\sigma_h(a))\overline{g}\,\overline{h} = \sigma_g(\sigma_h(a))\rho(g,h)\overline{gh}.$$

Pela propriedade 1.1, bem como para os elementos da base, temos que se $g, h, l \in G$, então

$$\overline{g}(\overline{h}\,\overline{x}) = \overline{g}(\rho(h,x))\overline{hx} = \sigma_g(\rho(h,x))\overline{g}\,\overline{hx} = \sigma_g(\rho(h,x))\rho(g,hx)\overline{ghx};$$
$$(\overline{g}\,\overline{h})\overline{x} = \rho(g,h)\overline{gh}\,\overline{x} = \rho(g,h)\rho(gh,x)\overline{ghx}.$$

Com isso verificamos a associatividade de $R*G$. De fato $a, b, c \in R*G$, ocorre que $abc = a(bc) = (ab)c$. Com efeito,

$$a(bc) = \sum_{g\in G} a_g\overline{g}(\sum_{h\in G} b_h\overline{h}\sum_{l\in G} c_l\overline{x}) = \sum a_g\overline{g}(\sum\sum b_h\overline{h}c_x\overline{x}) = \sum a_g\overline{g}(\sum\sum b_h\sigma_h(c_x)\overline{h}\overline{x}) =$$
$$= \sum a_g\overline{g}(b_h\sigma h(c_x))(\overline{h}\overline{x}) = \sum a_g\sigma_g(b_h\sigma_h(c_x))\overline{g}(\overline{h}\overline{x});$$
$$(ab)c = (\sum_{g,h\in G} a_g\overline{g}b_h\overline{h})\sum_{x\in G} c_x\overline{x} = \sum_{g,h,x\in G} (a_g\sigma_g(b_h)\overline{g}\overline{h})(c_x)\overline{x} = \sum a_g\sigma_g(b_h)\sigma_{gh}(c_x)(\overline{g}\overline{h})\overline{x}.$$

Ora, sendo a condição $\overline{g}(\overline{h}\overline{x}) = (\overline{g}\overline{h})\overline{x}$ satisfeita, então segue a associatividade do produto cruzado $(R * G)$. □

**Proposição 1.2.40.** *Seja $G$ um grupo, e $N$ subgrupo normal em $G$. Então $\mathbb{Z}G \cong (\mathbb{Z}N) * G/N$.*

**Demonstração.** Devemos mostrar que $\overline{G} = G/N$ é uma $\mathbb{Z}N$-base, e as funções $\rho$ e $\sigma$ estão definidas. Seja $\{\overline{g}\}$ o conjunto de representantes de $\overline{G}$ e $T$ o transversal de $N$ em $G$, obtido a partir deste conjunto. Temos que $G = \dot{\bigcup_{t\in T}} Nt$ e, portanto,

$$\mathbb{Z}G = \bigoplus((\mathbb{Z}N)\bar{t}), \text{ sendo } \bar{t} = Nt \in \overline{G},$$

Logo $\overline{G}$ é uma $\mathbb{Z}N$-base. Sendo $N \lhd G$, temos que $g\mathbb{Z}Ng^{-1} = \mathbb{Z}N$. Portanto ,

$$\sigma_g : \mathbb{Z}N \longrightarrow \mathbb{Z}N$$
$$\alpha \mapsto g\alpha g^{-1},$$

está bem definida e é um automorfismo do anel $\mathbb{Z}N$. Além disso, definimos a aplicação

$$\rho : \overline{G} \times \overline{G} \longrightarrow \mathcal{U}(\mathbb{Z}N)$$
$$(\overline{g}, \overline{h}) \mapsto n, \text{ tal que, } gh = nt, n \in N \subset \mathcal{U}(\mathbb{Z}N).$$

Dados $\overline{g}, \overline{h} \in \overline{G}$, existem únicos $t \in T, n \in N$, tal que $gh = nt$, portanto $\overline{g}\overline{h} = n\overline{gh}$ e definimos $\rho(\overline{g}, \overline{h}) := n$, portanto, $\rho$ está bem definida. □

Assim, por essa, proposição,

$$\mathbb{Z}[G \times C_\infty] \cong \mathbb{Z}G * \overline{C}_\infty, \quad com \quad \overline{C}_\infty = [G \times C_\infty]/G \cong C_\infty.$$

**Teorema 1.2.41.** *Seja $G$ um grupo ordenado, e $R$ um domínio. Então*

$$\mathcal{U}_1(R*G) = \{u * \overline{w} : u \in \mathcal{U}(R), w \in G\}.$$

**Demonstração.** Seja $u \in \mathcal{U}_1(R*G)$. Admita que $u$ seja não trivial

$$u = \sum_{g\in G} r_g\overline{g} \text{ e } u^{-1} = \sum_{g\in G} s_g\overline{g};$$
$$uu^{-1} = \sum_{g\in G} r_g\overline{g}\sum_{h\in G} s_h\overline{h} = \sum_{g,h\in G} r_g\overline{g}s_h\overline{h} = \underbrace{\sum_{g,h\in G} r_g\sigma_g(s_h)\overline{g}\overline{h} = \sum_{g,h\in G} r_g\sigma_g(s_h)\rho(g,h)\overline{gh}}_{\text{equações 1.3,1.4}} = 1.$$

Sendo $R$ um domínio, então $r_g\sigma_g(s_h)\rho(g,h)$ são não nulos para $g,h \in G$. Tomando-se os termos $g_1,h_1$ e $g_2,h_2$, respectivamente, os elementos mínimos e máximos de seus respectivos suportes em $G$, então

$$g_1 < g_2 \Longrightarrow g_1h_1 < g_2h_1;$$
$$h_1 < h_2 \Longrightarrow g_2h_1 < g_2h_2.$$

Se $g_1 \neq g_2$ ou $h_1 \neq h_2$, então $g_1h_1 < g_2h_2$. Portanto, $|Supp(uu^{-1})| \geq 2$. Absurdo. □

**Proposição 1.2.42.** *Se $G$ é um grupo abeliano finitamente gerado livre de torção, e $R$ é um domínio de integridade de característica 0, então o grupo das unidades do anel $RG$ é trivial.*

**Demonstração.** Sendo $G$ um grupo nilpotente e livre de torção, então pelo teorema 1.1.16, $G$ é um grupo ordenado. Pelo teorema anterior as unidades de $RG$ são triviais. □

**Corolário 1.2.43.** *Seja $C$ um grupo cíclico infinito. Então $\mathcal{U}_1(\mathbb{Z}C) = C$.*

**Proposição 1.2.44.** *(Krempa) Seja $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}G$. Então o automorfismo de $G$ induzido pela unidade $u^2$, isto é, $\varphi^2$, é um automorfismo interno, ou seja, $u^2 \in (G)\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.*

Na demonstração que apresentamos a seguir para o próximo teorema, temos uma aplicação do teorema 1.1.30. Obviamente, esse é um caso particular do teorema 1.2.19, porém de demonstração mais simplificada. Como veremos na demonstração do teorema, recaímos no caso de um grupo residualmente finito.

**Teorema 1.2.45.** *Seja $G$ um grupo. Se $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é de torção, então $u$ é trivial.*

**Demonstração.** Seja $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ de torção, seja $X = Supp(u)$. Consideramos $G_1 =< x : x \in X >$. Pelo corolário 1.2.37, $G_1$ é um $FC$-grupo finitamente gerado, portanto, é policíclico-por-finito. Daí inferimos 1.1.29, que este é residualmente finito. Pelo lema 1.1.30, $\exists\ N \lhd G$, cujo $[G:N] < \infty$, e $\pi : G \longrightarrow G/N$, sobre $X = Supp(u)$, é injetora. Estendemos $\pi : \mathbb{Z}G \longrightarrow \mathbb{Z}(G/N)$, então $\pi(u) = \overline{u}$ é central, de torção e $|G/N| < \infty$. Pelo teorema 1.2.19, temos que $|Supp(\pi(X))| = 1$, logo $|Supp(u)| = 1$. Portanto, $u \in G$. □

A seguir, ressaltamos a propriedade, para grupos infinitos da forma $G \times C_\infty$, sendo $G$ um grupo finito, e $C_\infty$ um grupo cíclico infinito, de que há uma relação entre (ISO) e (NC), definidas abaixo.

- **(ISO)** Seja $\mathbb{Z}G$ um anel de grupo. Podemos afirmar que a classe de isomorfismo de G é determinada por $\mathbb{Z}G$?
- **(NC)** Seja $\alpha$ uma unidade de $\mathcal{U}_1(\mathbb{Z}G)$ que normaliza o grupo $G$. Então existe $g \in G$, e uma unidade central $w$, tal que $\alpha = gw$. Ou seja, a conjugação de $\alpha$ sobre $G$ é induzida por um elemento de $G$.

No capítulos II, destacamos a relação entre essas duas conjecturas para grupos do tipo $G \times C_\infty$, sendo $G$ um grupo finito e $C_\infty$ um grupo cíclico infinito, ressaltando que no isomorfismo entre os anéis de grupos sobre anel dos inteiros para esses grupos é suficiente estudar a parte finita desses grupos, ou seja, o grupo $G$. No capítulo III demonstramos que existe uma estrutura para as unidades centrais. Uma Característica que permite maior abrangência em problemas que envolvam essas unidades, assim como, simplifica certas demonstrações. No presente trabalho, desejamos explorar esse último fato, apresentando alternativas para demonstrações de alguns teoremas, quando se considera para a unidade central uma estrutura.

# Capítulo 2

# ANÉIS DE GRUPO ISOMORFOS DE GRUPOS INFINITOS

Se $\mathbb{Z}G \cong \mathbb{Z}H$, quais propriedades do grupo $G$ são preservadas em $H$? Por exemplo, se $G$ é um grupo finito, ou abeliano ([21], III.2.10), ou nilpotente infinito ([22], Röhl), ou meta-abeliano finito [Withcomb], ou residualmente finito, ou FC e finitamente gerado ([14], lema 2), então $H$ tem a respectiva propriedade. Não sabemos, porém, caso $G$ seja nilpotente infinito, se $H$ tem o mesmo comprimento de nilpotência de $G$. Porém, quando a classe de nilpotência de $G$ é 2, sabemos que $H \cong G$, veja [7].

Vamos concentrar nosso estudo no anel dos inteiros. Para outras classes de anéis existem contra-exemplos para o Problema do Isomorfismo [20].

Ainda em [14], é feita uma relação entre (NC) e (ISO), até então não observada (teorema 2.2.1). Esse teorema permitirá um novo caminho para o Problema do Isomorfismo para grupos infinitos. Com efeito, a partir do trabalho de Mazur, [14], Hertweck anunciou a construção de um contra-exemplo para o Problema do Isomorfismo para anéis de grupo sobre o anel dos inteiros para grupos finitos, o qual não iremos tratar neste trabalho. Em [12], Roggenkamp e Marciniak discutem as principais idéias envolvidas nessa construção.

Iniciamos nossa apresentação do Problema do Isomorfismo com a classe de grupos abelianos, para a qual esse problema tem resposta positiva.

## 2.1 O Problema do Isomorfismo e a Conjectura do Normalizador

**Teorema 2.1.1.** *Seja $G$ um grupo abeliano finito, e $H$ um grupo, tal que $\mathbb{Z}G \cong \mathbb{Z}H$. Então $G \cong H$.*

**Demonstração.** Podemos considerar $\mathbb{Z}G = \mathbb{Z}H$. Pelo corolário 1.2.20, as unidades de torção de $\mathbb{Z}G$ e $\mathbb{Z}H$ são triviais. Como para qualquer $h \in H$, $o(h) < \infty$, então $h \in G$. Portanto $G = H$. □

**Observação 2.1.2.** *Esse teorema é verdadeiro para $|G| = \infty$, ver [13] e ([21],III.2.10).*

**Proposição 2.1.3.** *Sejam $C$ e $S$ dois grupos, sendo $C$ cíclico infinito, tal que $\mathbb{Z}C \cong \mathbb{Z}S$. Então $C$ e $S$ são isomorfos.*

**Demonstração.** Seja $\phi : \mathbb{Z}C \longrightarrow \mathbb{Z}S$ um isomorfismo normalizado. Sendo $C$ um grupo cíclico infinito, $C$ é ordenado. Logo pela proposição 1.2.43, $\mathcal{U}_1(\mathbb{Z}C) = C$. Sendo $\phi$ um isomorfismo, $\mathbb{Z}S$ tem somente unidades triviais, então $\mathcal{U}_1(\mathbb{Z}S) = S$, como $\phi$ é normalizado, temos que $C = \mathcal{U}_1(\mathbb{Z}C) \cong \mathcal{U}_1(\mathbb{Z}S) = S$. □

Se os anéis de grupo $\mathbb{Z}G$ e $\mathbb{Z}H$ são isomorfos, observamos no início deste capítulo, que a menos que (ISO) verifique-se para o grupo $G$, não são todas as propriedades do grupo $G$ que se estendem ao grupo $H$. A seguinte proposição evidencia, também, que a conjectura do normalizador estende-se para o anel $\mathbb{Z}H$, quando (ISO) ocorre.

**Proposição 2.1.4.** *Se $\mathbb{Z}G \cong \mathbb{Z}H$, e $G$ satisfaz (ISO) e (NC), então $H$ satisfaz NC.*

**Demonstração.** Como $G$ satisfaz (ISO), então $G \cong H$. Consideremos o isomorfismo $\varphi : H \longrightarrow G$ estendendo-o para o anel de grupos, isto é, $\varphi : \mathbb{Z}H \longrightarrow \mathbb{Z}G$. Seja $w \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}H)}H$, então $wHw^{-1} = H$. Daí $\varphi(w)G\varphi(w^{-1}) = \varphi(w)\varphi(H)\varphi(w^{-1}) = \varphi(wHw^{-1}) = \varphi(H) = G$. Portanto, $\varphi(w) \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}G$, logo da hipótese que $G$ satisfaz (NC) temos que $\varphi(w) = gv$, $g \in G$, $v \in \mathcal{Z}(\mathbb{Z}G)$. Portanto, $w = \varphi^{-1}(gv) = \varphi^{-1}(g)\varphi^{-1}(v)$, para $\varphi^{-1}(g) \in H$ e $\varphi^{-1}(v) \in \mathcal{Z}(\mathbb{Z}H)$. □

A seguir, apresentamos um dos resultados centrais deste trabalho. Nosso objetivo é apontar algumas questões que o seguinte teorema permite formular, procurando ressaltar a relação desse teorema com as conjecturas (ISO) e (NC).

A partir da próxima seção, denotaremos:

- $\mathcal{A}ut_R(G)$ o conjunto dos automorfismos de $G$ que são a conjugação de alguma unidade $u \in \mathcal{U}_1(RG)$ que normaliza $G$, isto é, $u \in \mathcal{N}_{\mathcal{U}_1(RG)}G$, e $\eta_u \in \mathcal{A}ut_RG$ seja tal que $\eta_u(g) = ugu^{-1}$.

## 2.2 O Problema do Isomorfimo para Grupos Infinitos

Seja $H$ um grupo finito, e $C_\infty$ um grupo cíclico infinito. Consideramos grupos da forma

$$K = H \rtimes_\varphi C_\infty.$$

Lembrando que se $h \in H$ e $C_\infty =< t >$, então

$$tht^{-1} := \varphi(h), \text{ e } (g, t^m)(h, t^n) = (g\varphi^m(h), t^{m+n}).$$

**Teorema 2.2.1.** *Seja $G$ um grupo finito, $R$ um anel $G$-adaptado, e $W$ um grupo qualquer. Então as $R$-álgebras $R[G \times C_\infty]$ e $RW$ são isomorfas, se e somente se, $W = H \rtimes_\varphi C_\infty$, de modo que*

**i.** *O grupo $H \subseteq W$ é um subgrupo finito, tal que as $R$-álgebras $RG$ e $RH$ são isomorfas;*

**ii.** *O automorfismo $\varphi$, do grupo $H$, é induzido pela conjugação com uma unidade $x \in RH$, que normaliza $H$.*

**Observação 2.2.2.** *(1) Embora o teorema esteja enunciado para um anel $R$ que é $G$-adaptado, demonstramos o teorema para o anel $\mathbb{Z}$.*

*(2) Partindo-se do fato $G \times C_\infty \cong G \rtimes_\varphi C_\infty \Leftrightarrow \varphi \in \mathcal{I}nn\ (G)$, corolário 2.2.7, então se $\mathbb{Z}[G \times C_\infty] \cong \mathbb{Z}[G \rtimes_\varphi C_\infty]$ satisfaz (ISO), obtemos a importante relação entre (ISO) e (NC). Veja proposição 2.2.8 , a partir desse teorema.*

*(3) No capítulo 3 demonstramos essa mesma relação anterior sem o uso dos lemas 4,5 de [14].*

*(4) A afirmação (ii) do teorema é outra forma de dizer que $\varphi \in \mathcal{A}ut_R(H)$.*

Antes de prosseguirmos com a demonstração do teorema 2.2.1, vamos inicialmente provar alguns resultados que permitam uma melhor compreensão das idéias envolvidas nesse teorema. A seguir, demonstramos algumas afirmações, concluímos a demonstração do teorema e enunciamos uma proposição que relaciona (ISO) e (NC) a partir desse teorema.

**Teorema 2.2.3.** *Seja $G$ um grupo finito. Se as $\mathbb{Z}$ álgebras $\mathbb{Z}[G \rtimes_\chi C_\infty]$ e $\mathbb{Z}W$ são isomorfas, então existe um grupo finito $H$ de mesma ordem de $G$, tal que $W = H \rtimes_\eta C_\infty, \eta \in \mathcal{A}ut(H)$.*

**Demonstração.** Seja $\phi : \mathbb{Z}[G \rtimes_\chi C_\infty] \longrightarrow \mathbb{Z}W$ um isomorfismo, e denotemos $G \rtimes_\chi C_\infty = K$. Sendo $G$ um grupo finito, e $\mathbb{Z}$ um domínio de integridade, tal que $\mathcal{U}(\mathbb{Z}) \cap \{o(g), g \in G\} = \{1\}$, podemos afirmar, pelo teorema 1.2.30, que há uma correspondência biunívoca entre os subgrupos finitos normais em $K$ e $W$. Logo $\exists\ H \leq W$, tal que $K \rhd G \leftrightarrow H \lhd W$ e $|G| = |H|$. Além disso, pelo teorema 1.2.30, item $[ii.]$ $\Delta(K, G) = \Delta(W, H)$. Segue, então que

$$\frac{\mathbb{Z}K}{\Delta(K, G)} \cong \frac{\mathbb{Z}W}{\Delta(W, H)} \Longrightarrow \mathbb{Z}(K/G) \cong \mathbb{Z}(W/H).$$

Como $\mathbb{Z}(K/G) \cong \mathbb{Z}C_\infty$, decorre da proposição 2.1.3 que $W/H \cong C_\infty$. Sendo $|H| < |\infty|$, segue por 1.1.5 que $H = T(W)$, o subgrupo de torção de $W$. Pela proposição 1.1.10, $W/T(W)$ é abeliano, então $T(W) \supseteq W'$, sendo este o subgrupo comutador de $W$. Seja $\theta : W \twoheadrightarrow W/T(W)$

a projeção de $W$ em $W/T(W)$; $W/T(W) =< \overline{w} >, o(\overline{w}) = \infty \Rightarrow \exists w \in W$, tal que $\theta(w) = \overline{w}$, então por 1.1.5, $o(w) = \infty$. Logo $< w > \subseteq W$. Além disso, $< w > \cap T(W) = 1$, pois $< w >$ é livre de torção. Considerando-se a proposição 1.1.9 na cadeia de inclusões abaixo, então

$$W' \subseteq T(W) \subseteq T(W) < w > \Rightarrow T(W) < w > \lhd W.$$

Por 1.1.6, existe N, subgrupo normal de $W/T(W)$, tal que $N = \theta(T(W) < w >) =< \overline{w} >$. Portanto, $T(W) < w >= W$, pois $\theta$ é um epimorfismo, e

$$W = T(W) \rtimes < w > .$$

Estando definido um homomorfismo $\eta$ da seguinte forma:

$$\eta :< w > \longrightarrow \mathcal{A}ut(T(W)).$$

Para

$$\begin{array}{c} \eta_w \in \mathcal{A}ut(T(W)) \\ \eta_w : T(W) \longrightarrow T(W) \\ t \mapsto wtw^{-1} \end{array},$$

identificando-se $\eta_w$ com $\eta$, temos que, pela proposição 1.1.34,

$$W = T(W) \rtimes_\eta < w > .$$

□

**Definição 2.2.4.** *Seja $G$ um grupo, e $H$ um subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$. Dizemos que $H$ é uma base de grupo de $\mathbb{Z}G$ se*

$$\begin{cases} \mathbb{Z}G = \mathbb{Z}H \\ H \text{ é linearmente independente sobre o anel } \mathbb{Z}. \end{cases}$$

A proposição 1.1.36 mostra que o produto semidireto externo pode ser identificado com um produto direto interno, de modo que as operações podem ser feitas como se estivéssemos tratando do produto semidireto interno.

**Lema 2.2.5.** *Seja $G$ um grupo finito $\phi$, $\theta \in \mathcal{A}ut(G)$, tais que $\eta = \phi\theta^{-1} \in \mathcal{A}ut_{\mathbb{Z}}G$. Então as $\mathbb{Z}$ álgebras $\mathbb{Z}[G \rtimes_\phi C_\infty]$ e $\mathbb{Z}[G \rtimes_\theta C_\infty]$ são isomorfas.*

**Demonstração.** Sejam $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}G$, tal que $\eta_u \in \mathcal{A}ut_{\mathbb{Z}}G$, e $C_\infty =< v >$ em $G \rtimes_\theta C_\infty$. Seja $\varphi$ a aplicação definida por

$$\begin{array}{c} \varphi : G \rtimes_\phi C_\infty \longrightarrow \mathbb{Z}[G \rtimes_\theta C_\infty], \text{ de modo que } G \rtimes_\theta C_\infty = G \rtimes_\theta < v > \\ gu^n \mapsto g(uv)^n, \end{array}$$

que é estendida a $\mathbb{Z}[G \rtimes_\phi C_\infty]$ por

$$\varphi : \mathbb{Z}[G \rtimes_\phi C_\infty] \longrightarrow \mathbb{Z}[G \rtimes_\theta C_\infty],$$
$$\sum_{g\in G, n\in\mathbb{Z}} a_{n,g} g u^n \mapsto \sum_{g\in G, n\in\mathbb{Z}} a_{n,g} g (uv)^n,$$

Vamos demonstrar que $\varphi$ é um isomorfismo. De fato, temos que:

$$\varphi((gv^m)(hv^n)) = \varphi(g\phi^m(h)v^{m+n}) = (g\phi^m(h)(uv)^{m+n});$$
$$\varphi(gv^m)\varphi(hv^n) = (g(uv)^m)(h(uv)^n). \quad (*)$$

Afirmamos que $(uv)^m h = \phi^m(h)(uv)^m$. Pois por indução no expoente $n$ temos: $(uv)h = uvhv^{-1}u^{-1}uv = u\theta(h)u^{-1}uv = \eta(\theta(h))uv = \phi(h)uv$; supomos por indução que $(uv)^{m-1}h = \phi^{m-1}(h)(uv)^{m-1}$. Então da hipótese de indução,
$(uv)^m h = (uv)(uv)^{m-1}h = uv\phi^{m-1}(h)v^{-1}u^{-1}uv(uv)^{m-1} = \phi^m(h)(uv)^m$. Portanto, $\varphi$ é um homomorfismo. Sejam $(g_1, v^m), (g_2, v^n)$, tais que $\varphi(g_1v^m) = \varphi(g_2v^n) \Longrightarrow g_1(uv)^m = g_2(uv)^n$, portanto, $g_1 = g_2$ e $m = n$. Logo $\varphi$ é homomorfismo injetor. Para provar a sobrejetividade, de $\varphi$ vamos considerar o grupo $H = \varphi(G \rtimes_\phi < u >)$ e provar que $H$ é uma base de grupo para o anel de grupo $\mathbb{Z}[G \rtimes_\theta < v >]$. Sendo $\varphi$ um homomorfismo, nesse caso $\epsilon(\varphi(gv^n)) = \epsilon(g(uv)^n) = 1$, para $g \in G$, e $n \in \mathbb{Z}$, portanto, $H \subset \mathcal{U}_1(G \rtimes_\theta < v >)$. Observamos que $uv \in H$, e afirmamos que $v \in \mathbb{Z}H$. Com efeito, definimos $z := uv$, daí, $v = u^{-1}z$. Ora $u^{-1} \in \mathbb{Z}G \Longrightarrow u^{-1} = \sum_{g\in G} u_g g$. Portanto, $v = (\sum_{g\in G} u_g g)z = \sum_{g\in G} u_g(gz)$, com $gz = h \in H$. Logo $v = \sum_{h\in H} u_{hz^{-1}}h \in \mathbb{Z}H$. De forma que, se $k \in K = G \rtimes_\theta < v >$, então $k = gv^n$ $n \in \mathbb{Z}$, $g \in G$, assim, $k = g(\sum_{h\in H} u_{hz^{-1}}h)^n \in \mathbb{Z}H$. Desse modo, $\alpha \in \mathbb{Z}K \Longrightarrow \alpha = \sum_{k\in K} \alpha_k k \in \mathbb{Z}H$. Logo $\mathbb{Z}K \subseteq \mathbb{Z}H \subseteq \mathbb{Z}K \Longrightarrow \mathbb{Z}H = \mathbb{Z}K$. Também, $H$ é $\mathbb{Z}$-linearmente independente. De fato suponha $\sum_{h\in H} \alpha_h h = 0$, com $\alpha_h$ inteiro, para cada $h$ existem $g_h \in G$, e $n_h \in \mathbb{Z}$, tal que $h = g(uv)^{n_h}$. Por indução no expoente de $(uv)^n$, vemos que $(uv)^n = u_1v^n$, com $u_1 \in \mathcal{U}(\mathbb{Z}G)$, de modo que $h = g(uv)^{n_h} = gu_hv^{n_h}$. Portanto, $0 = \sum_{h\in H} \alpha_h h = \sum_h \alpha_h g u_h v^{n_h}$, e $\{v^n, n \in \mathbb{Z}\}$ é $(\mathbb{Z}G)$-LI. Logo $\alpha_h g u_h = 0$, para todo $h \in H$, implicando que $\alpha_h = 0$, pois $gu_h \in \mathcal{U}(\mathbb{Z}H)$. Usando isso, segue que $\varphi$ é injetora. □

Com os resultados acima, estamos em condições de provar o teorema 2.2.1

**Demonstração.** Seja $K = G \times C_\infty$. Inicialmente observamos que

$$\mathbb{Z}K = \mathbb{Z}[G \rtimes_{I_d} C_\infty] \cong \mathbb{Z}W.$$

Pelo lema 2.2.3

$$W = T(W) \rtimes_\phi C_\infty, \text{ com } |T(W)| = |G|, \phi \in \mathcal{A}ut(T(W)).$$

Consideremos

$$\psi : \mathbb{Z}K \longrightarrow \mathbb{Z}[T(W) \rtimes_\phi C_\infty]$$

um isomorfismo normalizado, possível pelo teorema 1.2.17, de modo que podemos considerar $\mathbb{Z}K = \mathbb{Z}[T(W) \rtimes_\phi C_\infty]$. Sejam $H = \psi^{-1}(T(W))$, e $v$ o gerador da parte livre de torção do grupo $K$, ou seja, $C_\infty =< v >$. Definindo-se $R = \mathbb{Z}[v^{-1}, v]$, o anel de polinômios nas indeterminadas $v$ e $v^{-1}$, então $R$ é um anel $G$-adaptado, $H \subset \mathbb{Z}[G\times < v >] = RG$, e $|G| = |H|$. Logo pelo lema 1.2.29, $RG = RH$. Definindo-se $I \doteq \Delta(K, C_\infty)$ segue, pelo corolário 1.2.14, que

$$RG/I \cong \mathbb{Z}[G \times C_\infty]/I \cong \mathbb{Z}[G \times C_\infty/I] \cong \mathbb{Z}G,$$
$$\text{como } RG = RH \text{ temos que } \mathbb{Z}G \cong \mathbb{Z}H.$$

Vamos mostrar que existe $\phi \in \mathcal{A}ut_{\mathbb{Z}H}H$, que é induzida pela conjugação de uma $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}H)}H$. Consideramos a projeção de $\mathbb{Z}[G\times < v >]$ sobre $\mathbb{Z}[G\times < v >]/ < v >$. Do isomorfismo $\mathbb{Z}G \cong \mathbb{Z}H$ obtemos,

$$\begin{array}{ccc} \mathbb{Z}[G\times < v >] & \xrightarrow{\psi} & \mathbb{Z}[T(W)\rtimes_\phi < w >] \\ \pi \big\downarrow & & \\ \mathbb{Z}G. & & \end{array}$$

Seja $t := \psi^{-1}(w)$, então $\pi(t)$, é uma unidade que normaliza o subgrupo $H$, logo induz um automorfismo $\varphi \in \mathcal{A}ut(H)$. Com efeito,

$$\pi(\psi^{-1}(w))H(\pi(\psi^{-1}(w)))^{-1} = \pi(\psi^{-1}(w)\psi^{-1}(T(W))\psi^{-1}(w^{-1})) = \pi(\psi^{-1}(wT(W)w^{-1})) =$$
$$\pi(\psi^{-1}(\phi(T(W)))) = \pi \circ \psi^{-1} \circ \phi \circ \psi(H).$$

Sendo $K$ um grupo noetheriano, $< v >$ um grupo livre de torção, e o quociente $K/ < v >$ um grupo de torção, pelo teorema 1.2.33, a restrição de $\pi$ sobre $H$, é injetiva. Portanto, $\varphi = \psi^{-1} \circ \phi \circ \psi$, é um automorfismo de $H$. Isto é, $\varphi \in \mathcal{A}ut(H)$ é induzida pela unidade $\pi(t) \in \mathcal{U}(\mathbb{Z}H)$, que conjuga o grupo $H$. Da proposição 1.1.36, $H \rtimes_\varphi < v >\cong H \rtimes < v >$, e este último é isomorfo a $T(W)\rtimes_\phi < w >= W$. Portanto, $H \rtimes_\varphi < v >\cong W$. Reciprocamente $\mathbb{Z}G \cong \mathbb{Z}H$, então pelo corolário 1.2.7, $\mathbb{Z}[G \times C_\infty] \cong \mathbb{Z}[H \times C_\infty]$. Sendo $x$ uma unidade que induz $\varphi \in \mathcal{A}ut_{\mathbb{Z}}H$, pelo lema 2.2.5, $\mathbb{Z}[G \times C_\infty] \cong \mathbb{Z}[H \times C_\infty] \cong \mathbb{Z}[H \rtimes_\varphi C_\infty]$. □

Denotamos por $\mathcal{O}ut(G)$ o quociente

$$\mathcal{O}ut(G) = \mathcal{A}ut(G)/\mathcal{I}nn(G).$$

Retomemos o item 3 da observação 2.2.2 do teorema 2.2.1. Com o seguinte lema, temos uma compreensão melhor daquela observação:

**Lema 2.2.6.** *Seja $G$ um grupo que não admite epimorfismos sobre o grupo cíclico infinito. Então os grupos $G \rtimes_\phi C_\infty$ e $G \rtimes_\theta C_\infty$ são isomorfos, se e somente se, $\phi$ e $\theta^\epsilon$ são conjugados em $\mathcal{O}ut(G)$, e $\epsilon = \pm 1$.*

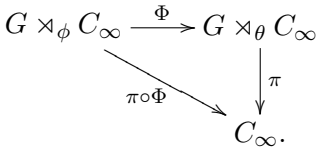
**Demonstração.** Seja

$$\Phi : G \rtimes_\phi C_\infty \longrightarrow G \rtimes_\theta C_\infty;$$

um isomorfismo de grupos, e

$$\pi : G \rtimes_\theta C_\infty \longrightarrow C_\infty,$$

a projeção de $G \rtimes_\theta C_\infty$ sobre $C_\infty$. Consideremos o diagrama abaixo




Afirmação: $\Phi(G) \subset Ker(\pi) = G$. De fato, considere a restrição $f = \pi \circ \Phi|_G : G \longrightarrow C_\infty$. Mostremos que $f(G) = 1$. Suponha que $\exists\, g \in G$, $t = f(g) \neq 1$. Então $0 \neq n \in \mathbb{Z}$, $f(G) =< t^n >$. Portanto, $|f(G)| = \infty$. Nesse caso a restrição de $f : G \longrightarrow \mathcal{I}m(f)$ é um epimorfismo de G sobre um grupo cíclico infinito. Absurdo, pois o lema afirma o contrário para o grupo $G$. Então $\pi(\Phi(g)) = 1$, $\forall g \in G$, portanto, $\Phi(G) \subset Ker(\pi)$. Analogamente, repetimos o argumento para $\Phi^{-1}$ e, portanto, $\Phi(G) = Ker(\pi) = G$, logo $\Phi|_G \in \mathcal{A}ut(G)$ para todo isomorfismo $\Phi$. Mostremos a partir daí que, $G \rtimes_\phi C_\infty \cong G \rtimes_\theta C_\infty \Longrightarrow \phi$, $\theta^\epsilon$ são conjugados em $\mathcal{O}ut(G)$, sendo $\epsilon = \pm 1$. Seja $\Phi$ um isomorfismo, tal que definamos $\Phi(1, t) = (g, t^\epsilon)$, fixado $g \in G$, e identificado no produto semidireto interno por $\Phi(t) = gt^\epsilon$. Em particular, para $g = 1$, $\Phi(t) = (1, t^\epsilon) \cong C_\infty \Longrightarrow \epsilon = \pm 1$. Pelo argumento acima, $\Phi(h, 1) = (\Phi(h), 1)$ está bem definida, cuja identificação no produto semidireto interno é $(\Phi(h), 1) = \Phi(h)1 = \Phi(h)$. Para checar a conjugação de $\phi$, $\theta^\epsilon$ em $\mathcal{O}ut(G)$, basta utilizar que $\Phi$ é homomorfismo

$$\Phi((1, t)(h, 1)) = \Phi(1, t)\Phi(h, 1) = (g, t^\epsilon)(\Phi(h), 1) = (g\theta^\epsilon \circ \Phi(h), t^\epsilon); \quad (*)$$
$$\Phi((1, t)(h, 1)) = \Phi(1\phi \circ (h), t) = \Phi(\phi(h), t),$$

identificando-se essa operação no produto semidireto interno, temos:

$$\Phi(\phi(h)t) = \Phi(\phi(h))\Phi(t) = (\Phi \circ \phi(h))(gt^\epsilon) = (\Phi \circ \phi(h)g)t^\epsilon,$$

que tem como representação no produto semidireto externo

$$(\Phi \circ \phi(h)g, t^\epsilon).$$

Portanto,

$$\Phi((1, t)(h, 1)) = \Phi(\phi(h), t) = (\Phi \circ \phi(h)g, t^\epsilon), \quad (**)$$

logo igualando-se as expressões em $(*)$ e $(**)$, temos:

$$(g\theta^\epsilon \circ \Phi(h), t^\epsilon) = (\Phi \circ \phi(h)g, t^\epsilon) \quad \forall h \in G \Longrightarrow$$
$$g\theta^\epsilon \circ \Phi = \Phi \circ \phi g \Longrightarrow \theta^\epsilon = g^{-1}\Phi \circ \phi g \circ \Phi^{-1}.$$

Logo $\theta^\epsilon = g^{-1}\Phi \circ \phi \circ (g^{-1}\Phi)^{-1}$. Então $\phi, \theta^\epsilon$ são conjugados em $\mathcal{O}ut(G)$. Reciprocamente, suponha que $\phi$ e $\theta^\epsilon$ são conjugados em $\mathcal{O}ut(G)$, e $\epsilon = \pm 1$. Queremos provar que os grupos são isomorfos. De fato, definindo-se a conjugação externa

$$(\bigstar) \quad \phi(h) = q\Phi^{-1} \circ \theta^\epsilon \circ \Phi(h)q^{-1}, \text{ para algum } q \in G, \Phi \in \mathcal{A}ut(G), \text{ e } \forall \quad h \in G.$$

A aplicação

$$\begin{aligned} \varphi : G \rtimes_\phi C_\infty &\longrightarrow G \rtimes_\theta C_\infty \\ (h, t^m) &\mapsto (\Phi(qhq^{-1}), t^{\epsilon m}) \end{aligned}$$

é um isomorfismo. Supondo $\phi$ e $\theta^\epsilon$ conjugados em $\mathcal{O}ut(G)$, verificamos que $\varphi$ é homomorfismo

$$\varphi((g,t^m)(h,t^n)) = \varphi(g\phi^m(h), t^{m+n}) = (\Phi(qg\phi^m(h)q^{-1}), t^{\epsilon(m+n)}) =$$
$$(\Phi(qgq^{-1})\Phi(q\phi^m(h)q^{-1}), t^{\epsilon(m+n)});$$
$$\varphi(g,t^m)\varphi(h,t^n) = (\Phi(qgq^{-1}), t^{\epsilon m})(\Phi(qhq^{-1}), t^{\epsilon n}) = (\Phi(qgq^{-1})\theta^{\epsilon m} \circ \Phi(qhq^{-1}), t^{\epsilon(m+n)});$$
$$\text{então das igualdades das condições acima}$$
$$\Phi(qgq^{-1})\Phi(q\phi^m(h)q^{-1}) = \Phi(qgq^{-1})\theta^{\epsilon m} \circ \Phi(qhq^{-1}) \Longrightarrow \Phi \circ \alpha_q \circ \phi^m = \theta^{\epsilon m} \circ \Phi \circ \alpha_q;$$
$$\text{tomando-se o quociente em } \mathcal{I}nn(g) \text{ obtemos}$$
$$\Phi \circ \phi^m = \theta^{\epsilon m} \circ \Phi, \text{ de acordo com } (\bigstar)$$

$\varphi$ é monomorfismo

$$\varphi(h_1, t^m) = \varphi(h_2, t^n) = (\Phi(h_1)\Phi(q), t^{\epsilon m}) = (\Phi(h_2)\Phi(q), t^{\epsilon n}) \text{ portanto } h_1 = h_2,\ m = n,$$

$\varphi$ é epimorfismo.

$$\forall (h, t^i) \in G \rtimes_\theta C_\infty \quad \exists (g, t^j) \in G \rtimes_\phi C_\infty \text{ tal que } \varphi(g, t^j) = (\Phi(gq), t^{\epsilon j}) = (h, t^i). \text{ Sendo}$$
$$\epsilon = \pm 1 \longrightarrow j = \pm i \text{ e sendo } \Phi \text{ isomorfismo de G, } \exists g \in G, \Phi(g) = h\Phi(q^{-1}).$$

□

**Corolário 2.2.7.** *Se $G$ é um grupo finito, então $G \times C_\infty \cong G \rtimes_\theta C_\infty$, se e somente se, $\theta$ é um automorfismo interno de $G$.*

**Demonstração.** Basta verificar que estamos nas condições do lema anterior. Sendo $|G| < \infty$, os elementos de $G$ são de torção e, portanto, a imagem $\Phi(G)$, do isomorfismo do lema anterior, está contida em $Ker(\pi)$, logo $\Phi|_G \in \mathcal{A}ut(G)$. Dessa forma, $G$ finito satisfaz às condições do lema anterior. Seja $G \times C_\infty \cong G \rtimes_\theta C_\infty$, pelo lema anterior $Id$, identidade, e $\theta^\epsilon$ são conjugados em $\mathcal{O}ut(G)$. Portanto, $Id = \Phi \circ \theta^\epsilon \circ \Phi^{-1} \Longrightarrow \theta^\epsilon \in \mathcal{I}nn(G)$. Analogamente $\theta \in \mathcal{I}nn(G) \Longrightarrow$, em $\mathcal{O}ut(G) = \mathcal{A}ut(G)/\mathcal{I}nn(G)$, $\overline{\theta} = \overline{Id}$, portanto, $\overline{\theta}^\epsilon = \overline{Id}$ e $\overline{Id}$ são trivialmente conjugados em $\mathcal{O}ut(G)$, logo Pelo lema anterior, os grupos são isomorfos. □

Se ocorre o isomorfismo $\mathbb{Z}[G\times C_\infty] \cong \mathbb{Z}[G\rtimes_\varphi C_\infty]$, então pelo teorema 2.2.1, $\varphi \in \mathcal{A}ut_{\mathbb{Z}}G$. Pelo corolário 2.2.7, sabemos que $G \times C_\infty \cong G \rtimes_\varphi C_\infty$, se e somente se, $\varphi \in \mathcal{I}nn(G)$. Isso permite, para grupos onde $\mathcal{A}ut_R G \neq \mathcal{I}nn(G)$, exibir contra-exemplos para o problema da (ISO) para grupos infinitos. Além disso, $\mathcal{A}ut_R G = \mathcal{I}nn(G) \Longrightarrow G$ satisfaz (NC), com efeito $x \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}G$, $x^{-1}gx \in G \ \forall\ g$, $\varphi_{x^{-1}}(g) := x^{-1}gx \Longrightarrow \varphi_{x^{-1}} \in \mathcal{A}ut_{\mathbb{Z}}G$. Como $\mathcal{A}ut_{\mathbb{Z}}G = \mathcal{I}nn(G) \Longrightarrow \exists\ h \in G$, tal que $\varphi_{x^{-1}} = \varphi_h$. Portanto, $x^{-1}gx = hgh^{-1} \Longrightarrow g = xhg(xh)^{-1} \Longleftrightarrow xh \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. Assim, $\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}G =< G, \mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) >$.

Enunciamos aqui a proposição que explicita a relação entre as conjecturas (ISO) e (NC).

**Proposição 2.2.8.** *Seja $G$ um grupo finito, e $K = G\times C_\infty$. Então são equivalentes as seguintes afirmações:*

**i.** *$K$ satisfaz (ISO);*

**ii.** *$G$ satisfaz (ISO) e (NC).*

**Demonstração.** Mostremos que $i \Rightarrow ii$.

(1) Seja $G$ um grupo que satisfaz (ISO). Tal como procedemos na demonstração do teorema. Consideremos $K = G \times \mathbb{C}_\infty$; $\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow \mathbb{Z}K \cong \mathbb{Z}G \bigotimes_{\mathbb{Z}} C_\infty \cong \mathbb{Z}H \bigotimes_{\mathbb{Z}} C_\infty \cong \mathbb{Z}[H \times \mathbb{C}_\infty]$. Como $K$ satisfaz (ISO), então $K \cong H \times C_\infty$. Logo $G = T(G \times C_\infty) \cong T(H \times C_\infty) = H$.

(2) $G$ satisfaz (NC). Vamos provar que dado $u \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G) \Rightarrow \theta_u \in \mathcal{I}nn(G)$. Consideremos $< t >:= C_\infty$. Nesse caso $t$ é central em $\mathbb{Z}K$, e $o(t) = \infty$; tomemos $v := ut = tu \in \mathbb{Z}K$. Assim, $G^v = vGv^{-1} = (ut)G(ut)^{-1} = utGt^{-1}u^{-1} = uGu^{-1} = G$, portanto, $v \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G)$. Definimos $W :=< G, v >$ com $< v > \cap G = 1$, de modo que pela definição 1.1.33, $W = G\rtimes < v >$. Nessas condições, $W$ é uma $\mathbb{Z}$-base de $\mathbb{Z}K$ (veja a demonstração do lema 2.2.6, considerando a aplicação $\varphi : \mathbb{Z}[G\times < t >] \longrightarrow \mathbb{Z}[G\rtimes < v >)$. Logo $W$ é $\mathbb{Z}$-LI sobre $\mathbb{Z}K$. Portanto, $\mathbb{Z}K = \mathbb{Z}W$, e pela hipótese $K = G\times < t > \cong G\rtimes < v >$. Podemos definir,

$$\begin{aligned} \alpha :< t > &\longrightarrow \mathcal{A}ut(G) \\ t &\mapsto \theta_v. \end{aligned}$$

portanto $G\rtimes < v > \cong G\rtimes_\alpha < t > \Longrightarrow G\rtimes < v > \cong G\times < t > \cong G\rtimes_\alpha < t >$, sendo $\alpha = \theta_v$ e, pelo corolário 2.2.7, $\theta_v \in \mathcal{I}nn(G)$ portanto $\theta_v = \theta_{ut} = \theta_u$ é um automorfismo interno de $G$. Logo $G$ satisfaz (NC)

Reciprocamente, seja $\mathbb{Z}[G \times C_\infty] \cong \mathbb{Z}W$. Pelo teorema 2.2.1, $W = H \rtimes_\varphi C_\infty$, e $\mathbb{Z}G \cong \mathbb{Z}H$. Por hipótese, $G$ satisfaz (ISO), e $\mathbb{Z}G$ satisfaz (NC). Então do isomorfismo $\mathbb{Z}G \cong \mathbb{Z}H$, pela proposição 2.1.4, $H$ satisfaz (NC). Logo $\varphi \in \mathcal{I}nn(G) \Rightarrow H \rtimes_\varphi C_\infty \cong H \times C_\infty$, que é um resultado do corolário

2.2.7. Retomando a condição $\mathbb{Z}G \cong \mathbb{Z}H \underbrace{\Rightarrow}_{Gsatisfaz(ISO)} G \cong H \Rightarrow K = G \times C_\infty \cong H \times C_\infty \cong H \rtimes_\varphi C_\infty = W$. Portanto, $K$ satisfaz (ISO). □

Observamos que na recíproca dessa demonstração é essencial o teorema 2.2.1, bem como o fato da proposição 2.1.4.

Quando afirmamos que uma demonstração do teorema 2.2.1 pode ser feita de forma mais direta, estamos chamando a atenção para o fato de que a demonstração dada não explicita diretamente a unidade $u$, segundo o teorema 2.2.1, que induz um automorfismo $\varphi \in \mathcal{A}ut_{\mathbb{Z}}H$, para $H$ um grupo finito. Ou seja, após mostrar pelo teorema 2.2.3 que $W = T(W) \rtimes_\phi C_\infty$, ainda temos que construir um outro produto semidireto $H \rtimes_\varphi C_\infty$, bem como determinar a unidade $u$ em uma adequada projeção no anel $\mathbb{Z}H$. Afirmamos, no entanto, que essa unidade $u$ pode ser construída no anel $\mathbb{Z}(T(W) \rtimes_\phi C_\infty)$, sem a necessidade daquela passagem adicional.

No capítulo III apresentamos um importante teorema de estrutura para as unidades centrais do anel de grupo inteiro para grupos nilpotentes finitamente gerados, que é estendido em [17] para grupos quaisquer, veja também [7]. Com esse teorema, um resultado de [10] e a proposição 1.2.34, conduzimo-nos à nova demonstração proposta.

# Capítulo 3

# AS UNIDADES CENTRAIS NO PROBLEMA DO ISOMORFISMO

Neste capítulo, apresentamos um teorema de estrutura para as unidades centrais em um anel de grupo $RG$, sendo $R$ um anel $G-adaptado$, e $G$ um grupo nilpotente finitamente gerado. O teorema é demonstrado em [9] para o anel $\mathbb{Z}$, e posteriormente generalizado em [17] e [7], para grupos quaisquer.

O teorema, que denominaremos por Teorema de Estrutura para as Unidades Centrais (TEUC), mostra que toda unidade central de um anel de grupo é igual ao produto de um elemento do grupo $G$ por um elemento do anel de grupo $RT$, sendo $T$ a torção de $G$. Na demonstração do teorema 2.2.1, podemos considerar uma unidade central do anel de grupo e aplicar o (TEUC), simplificando a demonstração dada no capítulo II.

Em [9] essa característica de estrutura para uma unidade central, e conseqüentemente uma idéia mais precisa desse elemento, é essencial para determinar geradores para subgrupos de índice finito no grupo das unidades centrais para os anéis de grupo que verifiquem a condição desse teorema. Neste capítulo, também, desenvolvemos uma demonstração simplificada para corolário 1.2.20 do teorema 1.2.19.

A demonstração utiliza amplamente propriedades do produto cruzado visto anteriormente. Essa abordagem, permite-nos utilizar teoremas da Teoria de Grupos e da Teoria de Anéis de um modo sistemático.

## 3.1 Um Teorema de Estrutura das Unidades Centrais em anéis de grupo

Nesta seção vamos supor que $R$ é um anel com unidade e um domínio de integridade, $K$ o corpo de frações do anel $R$, $G$ um grupo, tal que o subgrupo de torção de $G$, denominado por $T$, seja finito, e $F := G/T$; $\mathcal{I} = \{e_1, \cdots, e_n\}$ uma é família completa de idempotentes primitivos centrais e ortogonais em $KT$.

**Lema 3.1.1.** *(Maschke, 1.2.9) Seja $T$ um grupo finito, e $K$ um corpo de característica zero. Então o anel $KT$ é semi-simples, isto é,*

$$KT \cong \bigoplus_{i=1}^{n} A_i = \bigoplus_{i=1}^{n} (KT)e_i,$$

*sendo os anéis $A_i = (KT)e_i$ anéis simples e $e_i \in \mathcal{I}$.*

**Lema 3.1.2.** *Seja $\mathcal{I}$ a família de idempotentes primitivos, centrais e ortogonais em $KT$. A aplicação*

$$\begin{aligned} \varphi : F \times \mathcal{I} &\longrightarrow \mathcal{I} \\ (\overline{f}, e) &\mapsto \overline{f}e\overline{f}^{-1}, \text{ onde } \overline{f}e\overline{f}^{-1} := fef^{-1} \text{ e } \varphi(\overline{f}, e) := \varphi_{\overline{f}}(e) \end{aligned}$$

*é uma ação do grupo $F$ sobre o conjunto $\mathcal{I}$.*

**Demonstração.** Com efeito, $\varphi$ é uma ação de grupo. Pois seja $e \in \mathcal{I}$,
$\varphi_{\overline{gh}}(e) = \overline{gh}e\overline{h}^{-1}\overline{g}^{-1} = \overline{g}\varphi_{\overline{h}}(e)\overline{g}^{-1} = \varphi_{\overline{g}}\varphi_{\overline{h}}(e) = \varphi_{\overline{g}} \circ \varphi_{\overline{h}}(e) \Longrightarrow \varphi_{\overline{gh}} = \varphi_{\overline{g}} \circ \varphi_{\overline{h}}$
$(\varphi_{\overline{g}}(e))^2 = (\overline{g}e\overline{g}^{-1})^2 = \overline{g}e^2\overline{g}^{-1} = \overline{g}e\overline{g}^{-1} = \varphi_{\overline{g}}e$, um idempotente. Além disso, para $e \in \mathcal{I} \subset \mathcal{Z}(KT)$, escrevemos $e = \sum_{n\in T} e_n n$. Logo $\varphi_{\overline{g}}(e) = \overline{g}(\sum_{n\in T} e_n n)\overline{g}^{-1} = \sum_{n\in T} e_n \overline{g}n\overline{g}^{-1} = \sum_{w\in T} e_{\overline{g}^{-1}w\overline{g}}w \in KT$. Portanto, $\varphi_{\overline{g}}(e_i) \in \mathcal{I}$, e $\varphi$ está bem definida. Então $\varphi_{\overline{g}}(\mathcal{I}) \subset \mathcal{I}$, $\forall\ \overline{g} \in F$, logo $\varphi$ é uma ação de grupos. □

**Corolário 3.1.3.** *Nas condições do lema anterior, se $\mathcal{O}_i$ define a órbita de $e_i$, $O_i = |\mathcal{O}_i|$, e $O$ é o número de órbitas. Então os elementos*

$$E_i = \sum_{e_j \in \mathcal{O}_i} e_j,$$

*formam uma família completa de idempotentes ortogonais e centrais em $KG$. Nessas condições,*

$$KT \cong \bigoplus_{i=1}^{O} R_i, \text{ sendo } R_i = (KT)E_i \cong \bigoplus_{e_i \sim e_j} (KT)e_j \text{ com } e_i, e_j \in \mathcal{I}.$$

**Demonstração.** Seja $\mathcal{O}_i = \{e_j : e_i \sim e_j\}$ a órbita de $e_i$. Então $E_i = \sum_{e_j \in \mathcal{O}_i} e_j \ 1, \leq i \leq O$, formam uma família completa de idempotentes ortogonais e centrais em $KG$, ou seja, para cada $i$, $E_i$ é um idempotente. De fato, sendo $e_j$ é um idempotente ortogonal, $E_i^2 = \sum_{e_j \in \mathcal{O}_i} e_j \sum_{e_j \in \mathcal{O}_i} e_j = \sum_{e_j, e_h \in \mathcal{O}_i} e_j e_h = \sum_{e_j \in \mathcal{O}_i} e_j^2 = E_i$

$E_i E_j = \sum_{e_h \in \mathcal{O}_i} e_h \sum_{e_l \in \mathcal{O}_j} e_l = \sum_{e_h \in \mathcal{O}_i, e_l \in \mathcal{O}_j} e_h e_l = \sum_{e_h \in \mathcal{O}_i, e_l \in \mathcal{O}_j} e_h \delta_{h,l} = E_i \delta_{i,j}$, sendo $\delta_{i,j}$ o delta de Kronnecker. Seja $o = |\mathcal{I}|$, sendo $\mathcal{I} = \dot{\bigcup}_{i=1,O} \mathcal{O}_i$. Segundo a definição de $E_i$, $\sum_i^O E_i = \sum_{i=1}^O \sum_{e_j \in \mathcal{O}_i} e_j = \sum_{j=1}^o e_j = 1$, pois a família dos $e_j$ é completa. Logo os $E_i$ formam uma família completa. □

**Lema 3.1.4.** *Se $R$ é um anel comutativo, e $F = G/T$ é um grupo ordenado, tal que*

$$KG = \bigoplus_i^O R_i * F, \qquad (\star)$$

*sendo, para cada $i$, $R_i = (KT)E_i$ um anel semi-simples, e os $E_i$, $i = 1, \cdots, O$, são idempotentes ortogonais e centrais em $KG$. Então se $u \in \mathcal{Z}(\mathcal{U}(RG)) \subset \mathcal{Z}(\mathcal{U}(KG))$, e $S$ for um transversal de $T$ em $G$, como definido em* **??**, *temos que*

$$u = \bigoplus_i^O \alpha_i \overline{f_i};$$

*$f_i \in G$, e os escalares $\alpha_i \in R_i$, sendo os $R_i$ anéis artinianos, $i = 1, \cdots, O$.*

**Demonstração.** Pela condição $(\star)$, $u = \bigoplus_{i=1}^O u_i$, $0 \neq u_i \in R_i * F$, portanto, $u_i = \sum_{f \in S} u_f \overline{f}$, $u_f \in R_i$. Devemos provar que para cada componente $u_i = \sum u_f \overline{f}$, seu suporte, $Supp(u_i) = \{\overline{f_i}\}$, é um conjunto unitário, ou seja, $|Supp(u_i)| = 1$. Afirmamos que cada $u_f$ é uma unidade em $R_i$. Com efeito, considere

$$\pi_i : KG \longrightarrow R_i * F$$
$$\alpha \mapsto \alpha_i;$$

$\pi_i(u) = u_i$; $\pi_i(KT) = (KT)E_i = R_i$. Sendo $u$ um elemento central $\pi_i(u(KT)) = \pi_i((KT)u)$ , portanto,

$$u_i R_i = R_i u_i, \ (\sum_{f \in S} u_f \overline{f}) R_i = R_i (\sum_{f \in S} u_f \overline{f}) = \sum_{f \in S} (u_f \overline{f}) R_i = \sum u_f (\overline{f} R_i \overline{f}^{-1}) \overline{f} = \sum u_f R_i^{\overline{f}} \overline{f},$$

então

$$\sum_{f \in S} (u_f R_i^{\overline{f}}) \overline{f} = \sum_{f \in S} (R_i u_f) \overline{f}.$$

Sendo $\overline{f} \in F$, uma $K$-base. Então $u_f R_i^{\overline{f}} = R_i u_f$. Por construção, temos que $R_i = \bigoplus_{e_i \sim e_j} (KT)e_j$, logo $R_i^{\overline{f}} = R_i$. Portanto,

$$u_f R_i = R_i u_f, f \in S.$$

Da expressão $R_i = \bigoplus_{e_i \sim e_j} (KT)e_j = (KT)E_i := \bigoplus_{j=1}^{O_i} (KT)e_{i_j}$, $A_{i_j} = (KT)e_{i_j}$. Multiplicando-se por $e_{i_j}$, que é um idempotente ortogonal e central, temos $e_{i_j}u_f(KT)(e_{i_1} + \cdots + e_{i_{O_i}}) = e_{i_j}(KT)(e_{i_1} + \cdots + e_{i_{O_i}})u_f$, logo

$$A_{i_j}u_f = u_f A_{i_j}, \text{ para todo } j.$$

Ora, $A_{i_j}$ é um anel simples, então $u_f e_{i_j}$ é uma unidade em $A_{i_j}$, daí, $0 \neq u_f e_{i_j}$ não é divisor de zero em cada $A_{i_j}$. Como $R_i$ é determinado pela órbita $O_i$, segue que $u_f \in \mathcal{U}(R_i)$. Desse modo, $u_i = \sum_{f \in S} u_f \overline{f}$ e $u_f \in \mathcal{U}(R_i)$, $u_i \in R_i * F$, $F$ é um grupo ordenado e cada componente $u_f$ não é um divisor de zero. Portanto, pelo teorema 1.2.41, $u_i$ é uma unidade trivial, ou seja $|Supp(u_i)| = 1$. Daí o resultado

$$u = \bigoplus_{i}^{O} \alpha_i \overline{f}_i, \ \alpha_i \in R_i, f \in G.$$

□

**Lema 3.1.5.** *Nas condições do lema anterior, se $u$ é uma unidade central do anel de grupo $RG$, existe um anel de grupo comutativo, que denotaremos por $AX$, que contém uma conveniente potência da unidade $u$, isto é:*

$$u^k \in AX, \text{ sendo } k \text{ um número inteiro positivo.}$$

*Além disso, o grupo $X$ é livre do torção, e $A$ é um anel artiniano, finitamente gerado e um domínio de integridade de característica nula.*

**Demonstração.** Vamos construir um anel de grupo comutativo $AX$ e mostrar que $u^k \in AX$ para um inteiro positivo $k$. Pelo lema anterior, $u = \bigoplus_{i}^{(O)} \alpha_i \overline{f}_i$, com $\alpha_i \in R_i = (KT)E_i$. Seja

$$X_0 =< \overline{f}_i \in Supp(u) >,$$

pelo corolário 1.2.37 e sendo $u$ uma unidade central, então $X_0$ é um $FC$-grupo finitamente gerado, logo pelo teorema 1.1.27, o índice de $\mathcal{Z}(X_0)$ em $X_0$ é finito, digamos $[X_0 : \mathcal{Z}(X_0)] = m < \infty$. Sendo $T$ um subgrupo finito, então $l = |\mathcal{A}ut(T)| < \infty$. Consideremos $k = lm$, logo $u^k$ é elemento de um anel comutativo. De fato, seja $\varphi_g \in \mathcal{A}ut(T)$ a conjugação com os elementos de $g \in G$. Então $\varphi_g^l = I_d \Longrightarrow t = \varphi_f^l(t) = f^l t f^{-l}$, mostrando que $f^l$ comuta com $T$ para todo elemento de

$G$. Naturalmente, essa mesma propriedade é válida para o grupo $F$ e qualquer múltiplo de $l$, em particular para $k$, logo

$$\overline{f}^k t \quad = \quad t\overline{f}^k, \forall t \in T. \tag{3.1}$$

Prosseguimos explicitando melhor a potência $u^k = (\oplus u_i)^k = \oplus u_i^k = \oplus(\alpha_i \overline{f}_i)^k$, sendo, portanto, suficiente efetuar o cálculo em alguma parcela da soma direta. Seja $\alpha\overline{f} = \alpha_i\overline{f}_i =$ esse termo, temos:
$(\alpha\overline{f})^k = \alpha\overline{f}\alpha\overline{f}\cdots\alpha\overline{f} = \alpha\overline{f}\alpha\overline{f}^{-1}\overline{f}^2\cdots\alpha\overline{f} = \alpha\alpha^{\overline{f}}\overline{f}^2\alpha\overline{f}\cdots\alpha\overline{f} = \cdots$
$\alpha\alpha^{\overline{f}}\alpha^{\overline{f}^2}\cdots\alpha^{\overline{f}^{n-1}}\overline{f}^n\alpha\overline{f}\cdots\alpha\overline{f} = \cdots$
$\alpha\alpha^{\overline{f}}\alpha^{\overline{f}^2}\cdots\alpha^{\overline{f}^{k-1}}\overline{f}^k.$
Sendo $\alpha^{\overline{f}^n} \in R_i$, para todo $n$. Então $\beta = \alpha\alpha^{\overline{f}}\alpha^{\overline{f}^2}\cdots\alpha^{\overline{f}^{k-1}} \in R_i$, para $1 \leq i \leq O$, logo

$$u^k = \bigoplus_{i=1}^{O} \beta_i \overline{f}_i^k \quad \beta_i \in R_i \quad f \in S \subset G.$$

E não mais garantimos que cada $f_i^k \neq f_j^k$ implica que $\overline{f_i}^k \neq \overline{f_j}^k$. Colecionando-se os escalares $\beta_i$ que têm os $\overline{f}_i^k$ equivalentes, ou seja, que estejam na mesma classe de $T(G)$ obtemos para

$$u^k = \oplus_i \beta_i' \overline{f}_i^k, \beta_i' \in A_i' = \bigoplus_{\overline{f}_i^k \sim \overline{f}_j^k} A_j;$$

$$\beta_i' = \sum_{\overline{f}_i^k \sim \overline{f}_j^k} \beta_j, \text{ também satisfazendo, } \beta_i'^t = \beta_i'.$$

Sendo $\beta_i'$ invariante por conjugação com os elementos de $T(G)$. Definindo-se o anel $A =< \beta_i' :$ $\beta_i'$ são os coeficientes de $u^k >$ finitamente gerado, pela proposição 1.1.44, o anel $A$ é artiniano, pois cada $\beta_i' \in \bigoplus A_j$, sendo $A_j$ componentes artinianas. Além disso, $A$ é um anel comutativo, pois para cada gerador $\beta_i', \beta_j'$ de $A$, com $i \neq j$, $\beta_i'\beta_j' = \sum \beta_k\beta_l = 0$, pelo fato que $\beta_i \in R_i$;

$$\beta_i'\beta_j' = \beta_i' \sum_{t\in T(G)} \beta_j'(t)t = \underbrace{\sum_{t\in T(G)} \beta_j'(t)\beta_i' t = \sum_{t\in T(G)} \beta_j'(t)t\beta_i'}_{\text{pois } R \text{ é comutativo e } \beta_i'^t = \beta_i'} = \beta_j'\beta_i',$$

e $A$ é um anel finitamente gerado. Ademais, sendo os geradores de $A$, obtidos através dos coeficientes da unidade $u$, que pelo lema 3.1.4 não são divisores de zero. Então $A$ é um domínio de integridade, cuja característica $char(A) = char(R) = 0$. Reconstruímos o grupo $X$: gerado pelos elementos do suporte de $u^k$, isto é $X =< \overline{f_1}^k, \cdots, \overline{f_p}^k >$ é um grupo abeliano, finitamente gerado e livre de torção. Assim $u^k \in AX$, que é um anel de grupo comutativo. □

**Lema 3.1.6.** *Nas condições do lema anterior, sendo $u^k$ uma unidade de um anel de grupo $AX$, na qual $X$ é um grupo abeliano, finitamente gerado e livre de torção, e $A$ um anel comutativo, finitamente gerado que é um domínio de integridade de característica 0, então $u^k$ é uma unidade trivial.*

**Demonstração.** Sendo $X$ um grupo abeliano, $X$ é um grupo nilpotente, e nas condições do lema, finitamente gerado e livre de torção, e $A$ um domínio de característica $O$, pela proposição 1.2.42 as unidades de $AX$ são triviais. Logo $u^k$ é uma unidade trivial. □

**Teorema 3.1.7.** *(**Teorema de Estrutura das Unidades Centrais**) [9] Seja $G$ um grupo, e $T(G)$ o conjunto dos elementos de torção de $G$, tal que $T(G)$ forme um subgrupo. Suponha que $G/T(G)$ seja um grupo ordenado. Então dada $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, existe $r \in \mathbb{Z}T(G)$, e $g \in G$, tal que $u = rg$.*

**Observação 3.1.8.** *A notação que segue está de acordo com aquela da definição 1.2.38, mais especificamente, utilizamos a mesma expressão para os elementos do produto cruzado que aquela utilizada na proposição 1.2.40, ou se seja, para $a \in \mathbb{Z}T(G) * F$ com $F = G/T(G)$, $a = \sum_{g\in G} a_g\overline{g}$, $a_g \in \mathbb{Z}T(G)$, $g \in G$. Estamos considerando que $g$ é um elemento de um transversal $S$ de $T(G)$ em $G$. Essa notação tem motivos técnicos que serão úteis ao longo do texto. Lembramos que se $S \ni f \neq g \in S$. Então $\overline{f} = fT(G) \neq gT(G) = \overline{g}$.*

**Demonstração.** Para o anel de grupo $\mathbb{Q}G$, sendo $T(G) \lhd G$, pela proposição 1.2.40, temos que

$$\mathbb{Q}G \cong (\mathbb{Q}T(G)) * G/T(G).$$

Pelo lema 3.1.1

$$\mathbb{Q}T(G) \cong \bigoplus_{i}^{n} A_i,$$

sendo $A_i \cong (\mathbb{Q}T(G))e_i$ anéis simples, e o conjunto $\mathcal{I} = \{e_1, \cdots, e_n\}$ forma uma família completa de idempotentes centrais ortogonais primitivos em $\mathbb{Q}T(G)$. É conveniente que determinemos idempotentes $E_i$ ortogonais e centrais em $\mathbb{Q}G$, que formem uma família completa de idempotentes em $\mathbb{Q}G$. O corolário 3.1.3 mostra que esses idempotentes são expressos por uma soma adequada dos idempotentes $e_i \in \mathcal{I}$ do lema 3.1.1, isto é,

$$E_i = \sum_{e_i \cong e_j} e_j$$

Portanto, pelo corolário 3.1.3. podemos obter uma decomposição, em soma direta, para $\mathbb{Q}T(G)$ em idempotentes centrais e ortogonais em $\mathbb{Q}G$, ou seja

$$\mathbb{Q}T(G) = \bigoplus_{i=1}^{O} R_i; \tag{3.2}$$

$$R_i = \bigoplus_{e_i \sim e_j} (\mathbb{Q}T(G))e_j = (\mathbb{Q}T(G))E_i, \tag{3.3}$$

para cada $1 \leq i \leq O$, sendo $O$ o número de órbitas da ação do lema 3.1.2. Com isso, o anel de grupo $\mathbb{Q}G$ pode ser expresso por:

$$\mathbb{Q}G \cong (\bigoplus_{i=1}^{O} R_i) * F.$$

Os anéis $R_i$ são anéis artinianos semisimples, ou seja $R_i = \bigoplus_{e_i \sim e_j} A_{i_j}$, com $A_{i_J} = (\mathbb{Q}T)e_j$, componentes simples. Temos, portanto, um modo natural de apresentarmos $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) \subset \mathcal{Z}(\mathcal{U}(\mathbb{Q}G))$, ou seja, se $S$ é um transversal de $T(G)$ em $G$, como definido em **??**, $u = \bigoplus_{i=1}^{O} u_i$, com $u_i \in R_i * F$ e, portanto, pela definição de produto cruzado, $u_i = \sum_{f \in S} u_f \overline{f}$, $u_f \in R_i$. Pelo lema 3.1.4, $|Supp(u_i)| = 1$, logo na expressão de $u_i = \sum_{f \in S} u_f \overline{f}$, existe um único termo não nulo no somatório, isto é,

$$u_i = \alpha_f \overline{f}, \alpha_f \in R_i, \quad f \in S.$$

Por conveniência denotamos por $u_i \doteq \alpha_i \overline{f}_i$. Concluímos a demonstração provando que todos os elementos $\overline{f_i} \in F$ estão na mesma classe. Com efeito, pelo lema 3.1.5, existe um anel comutativo, $RX$, que contém uma conveniente potência da unidade central $u$, ou seja

$$\exists k \in \mathbb{N}, u^k \in RX \text{anel comutativo. sendo } X \text{ um grupo abeliano livre}$$

Além disso, pelo lema 3.1.6, $u^k$ é uma unidade trivial em $RX$, ou seja

$$u^k = \beta \overline{f}^k, \beta \in \bigoplus_{i}^{O} R_i, f \in G,$$

isso implica que para a unidade central $u = \bigoplus u_i = \bigoplus \alpha_i \overline{f}_i$, todos os $f$ devem estar na mesma classe. Pois sendo $u^k$ uma unidade trivial de $RX$, $\overline{f}_i^k = \overline{f}_j^k \Longrightarrow (\overline{f_i f_j^{-1}})^k = 1$, e $\overline{f_i f_j^{-1}} \in F$, grupo livre de torção. Portanto, $\overline{f_i} = \overline{f_j}$. Então $u = \alpha \overline{f}$, sendo $\alpha \in \mathbb{Z}T(G)$, e $\overline{f} \in F$, de modo que $f = hg$, com $h \in T(G)$, e $g \in G$. Logo $u = \alpha hg = rg$, $\alpha h = r \in \mathbb{Z}T(G)$. □

**Corolário 3.1.9.** *[7] Nas condições do teorema 3.1.7, se $u$ é uma unidade central de $\mathbb{Z}G$, tal que $u = rg$, $r \in \mathbb{Z}T(G)$, e $g \in G$. Então existe um inteiro positivo $n$, tal que $g^n$, $r^n$ sejam centrais.*

**Demonstração.** Seja $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, então $u = rg$ com $g \in G$, e $r \in \mathbb{Z}T(G)$. Consideremos o homomorfismo $\pi : \mathbb{Z}G \longrightarrow \mathbb{Z}(G/T(G))$, $\pi(u) \in \mathcal{Z}(\mathbb{Z}(G/T(G)))$, sendo $G/T(G)$ um grupo ordenado, pelo teorema 1.2.41, $\mathcal{U}_1(\mathbb{Z}(G/T(G))) = G/T(G)$. Portanto, $\pi(u) \in \mathcal{Z}(G/T(G))$, $\pi(u) = \pi(r)\pi(g)$, e $\mathbb{Z}T(G) \ni \pi(r) = \epsilon(r) = \overline{1}$, o aumento de $r$, implica que $\pi(u) = \pi(g) = g\overline{1} = gT(G) \in \mathcal{Z}(G/T(G))$. Para todo $h, a \in G$, $[h, a] \in T(G)$, uma vez que $\pi([h, a]) = \overline{1}$. Sendo $u$ uma unidade central, então $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}G \Longrightarrow r^2 g^2 = u^2 \in G\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$, teorema 1.2.44, logo $r^2 \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}T))$. Com isso, para $h \in G$, da propriedade 1.1.8 do comutador, $[g^2, h] = [g, h]^g[g, h] = [g, h]^2$, pois $g$ comuta com os elementos de $T(G)$. Assim, considerando $|T| = |T(G)|$, pela propriedade anterior, $[g^{2|T|}, h] = [g, h]^{2|T|} = 1$. Logo $g^{2|T|} \in \mathcal{Z}(G)$, e sendo $u$ e $g^{2|T|}$ centrais, então $u^{2|T|} = r^{2|T|} g^{2|T|} \Longrightarrow r^{2|T|}$ é central, daí, $n = 2|T|$ é o inteiro asserido. □

O teorema 3.1.7 foi primeiramente enunciado em [9], para um grupo $G$ nilpotente finitamente gerado. Posteriormente, em [17] o teorema foi generalizado para um grupo $G$ qualquer, considerando-se o $FC$-centro de $G$, ou seja, se $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, então $Supp(u) \subset \Delta(G)$, logo $G_0 :=< Supp(u) >$ é um FC-grupo, finitamente gerado. Em particular $T(G_0) < \infty$, e $G_0/T(G_0)$ é um grupo abeliano livre de torção, pois $T(G_0) \supset G_0'$, logo por 1.1.16, $G_0/T(G_0)$ é um grupo ordenado. A forma que utilizamos para enunciar o TEUC encontra-se em [7].

Pelo teorema 1.1.18, se $G$ é um grupo finitamente gerado nilpotente, $T(G) \lhd G$, e $|T(G)| < \infty$. Note que $F = G/T(G)$ é um grupo livre de torção finitamente gerado, e, portanto, pelo teorema 1.1.16, $F$ é um grupo ordenado. Os corolários apresentados abaixo, portanto, estão nas condições do teorema 3.1.7.

**Corolário 3.1.10.** *Seja $G$ um grupo finitamente gerado e nilpotente. Se $\mathcal{Z}(\mathcal{U}(\mathbb{Z}T(G)))$ é trivial, então $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é trivial.*

**Demonstração.** Consideremos que $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ seja não trivial, então $|Supp(u)| > 1$. Pelo teorema 1.1.30, $\exists\ N \lhd G$, cujo $[G : N] < \infty$, e $\Pi : G \longrightarrow G/N$, o homomorfismo canônico restrito a $X = Supp(u)$, que é um conjunto finito, é um homomorfismo injetor. Estendemos $\Pi$ para o anel $\mathbb{Z}G$, $\Pi : \mathbb{Z}G \longrightarrow \mathbb{Z}(G/N)$, $\Pi(u) = \overline{u}$, $|\Pi(u)| = |X| > 1$, então $\overline{u}$ não é de torção, teorema 1.2.20 para grupos finitos. Sendo $u$ uma unidade central, logo $u = rg$, $r \in \mathbb{Z}T(G)$, e $g \in G$, teorema 3.1.7. Tomando-se a projeção $\Pi(u) = \overline{u} = \overline{rg}$, $\overline{u}$ é central, daí, $\overline{u}^n = \overline{r}^n\overline{g}^n$, logo $\overline{r}$ não é de torção— pois senão existiria $n = MMC(o(\overline{r}), [G : N])$, tal que $o(\overline{u}) = n$, e $\overline{u}$ seria de torção. Absurdo! Ocorre que, pelo corolário 3.1.9, $\exists\ n = 2|T(G)|$, tal que $[g^n, T] = 1$, $r^n \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}T(G)))$. Mas $r^n$ não tem ordem finita e é uma unidade central de $\mathbb{Z}T(G)$, então pelo corolário 1.2.20 para grupos finitos, $r^n$ é não trivial. □

**Lema 3.1.11.** *Seja $G$ um grupo finito. Então $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é um grupo finitamente gerado.*

**Demonstração.** Considere

$$\psi : \mathbb{Z}G \hookrightarrow \mathbb{Q}G = \bigoplus_i M_{n_i}(D_i);$$

$\mathcal{Z}(\mathbb{Q}G) = \mathcal{Z}(\bigoplus_i M_{n_i}(D_i)) = \bigoplus_i \mathcal{Z}(D_i)I_{n_i \times n_i}$, o qual $I_{n_i \times n_i} = \bigoplus_i(\mathcal{Z}(D_i)$ denota a matriz identidade de ordem $n_i$. Seja $\mathcal{Z}(D_i) = K_i$. Como $\mathbb{Z}G \subset \mathbb{Q}G$, temos que

$$\psi : \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G) \hookrightarrow \bigoplus_i K_i.$$

Consideremos $\alpha \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, então $\alpha$ é um elemento algébrico sobre $\mathbb{Q}$, pois $dim_{\mathbb{Q}}(\mathbb{Q}G) = |G| < \infty$; em particular $\psi(\alpha)$ é algébrica, portanto, $\psi(\alpha) = \oplus\alpha_i$, $\alpha_i \in K_i \Longrightarrow \alpha_i \in I_{K_i|\mathbb{Q}}$, o anel dos inteiros de $K_i$ sobre $\mathbb{Q}$. Logo

$$\psi(\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))) \subseteq \bigoplus(\mathcal{U}(I_{K_i|\mathbb{Q}})).$$

Pelo Teorema das Unidades de Dirichlet 4.1.36, $F_i := \mathcal{U}(I_{K_i|\mathbb{Q}})$ é finitamente gerado e, portanto, $\psi(\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)))$ é subconjunto de $\bigoplus_i F_i$, um grupo abeliano finitamente gerado, e é, portanto, finitamente gerado. □

**Corolário 3.1.12.** *Seja $G$ como no corolário 3.1.10. Então $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é finitamente gerado. Além disso, $(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) \cap \mathcal{Z}(\mathcal{U}(\mathbb{Z}T(G)))\mathcal{Z}(G))$ é de índice finito em $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.*

**Demonstração.** Inicialmente provamos que se $S = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) \cap \mathcal{Z}(\mathcal{U}(\mathbb{Z}T(G)))$ então $[\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) : S\mathcal{Z}(G)]$ tem índice finito. De fato, seja $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$, e a projeção $\pi : \mathbb{Z}G \longrightarrow \mathbb{Z}(G/T(G))$. O grupo $G/T(G)$ é um grupo ordenado, então pelo teorema 1.2.41, as unidades do anel de grupo $\mathbb{Z}(G/T(G))$ são as unidades triviais, portanto, $\pi(u) \in \mathcal{U}(Z(G/T(G)))$ é uma unidade trivial. Sendo $u$ uma unidade central, pelo Teorema de Estrutura das Unidades Centrais 3.1.7, $u = rg \Longrightarrow \pi(rg) \in G/T$, com $r \in \mathcal{U}(\mathbb{Z}T(G))$, ora sendo a projeção de $u$ uma unidade trivial, obtemos que $gT(G) \in \mathcal{Z}(G/T(G))$. Seja $n = 2|T(G)|$, pelo teorema 3.1.9, então $[g^n, T(G)] = 1$. Isso implica que $u^n = r^n g^n$, e como $r^n \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}(T(G))))$ e $r^n = u^n g^{-n} \in \mathcal{Z}(\mathbb{Z}G)$, então $r^n \in S$, portanto, $u^n \in S\mathcal{Z}(G)$, isto é, $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))/S\mathcal{Z}(G)$ é um grupo de torção de expoente limitado. Pelo lema 3.1.11, sendo $\mathcal{Z}(\mathcal{U}(\mathbb{Z}(T(G)))) \supset S$ um grupo finitamente gerado, então $S$ é finitamente gerado, daí, segue que $S\mathcal{Z}(G)$ é finitamente gerado, pois $S$ e $\mathcal{Z}(G)$ são finitamente gerados. Assim, $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))/S\mathcal{Z}(G)$ é um grupo de expoente limitado, portanto, posto($\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$=posto($S\mathcal{Z}(G)$), além disso $T(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))) \in T(G)$, portanto, o subgrupo de torção $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é finito. Sendo $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ um grupo abeliano, este é finitamente gerado. □

## 3.2 As Unidades Centrais em anéis de grupo

Estamos então em condições de apresentar uma outra demonstração do teorema 2.2.1 para condição necessária da implicação, ou seja, mostramos que dado o isomorfismo entre os anéis de grupo $\mathbb{Z}[G \times C_\infty]$ e $\mathbb{Z}W$, com $|G| < \infty$, então verificamos o isomorfismo para os anéis de grupos $\mathbb{Z}G \cong \mathbb{Z}T(W)$ e explicitamos uma unidade $x$ que conjuga o grupo $H$, tal que $\varphi \in \mathcal{A}ut_{\mathbb{Z}}H$, $\varphi(h) = xhx^{-1}$, $h \in H$.

**Teorema 3.2.1.** *Seja $G$ um grupo finito, $\mathbb{Z}$ um anel $G$-adaptado, e $W$ um grupo qualquer. Então as $\mathbb{Z}$-álgebras $\mathbb{Z}[G \times C_\infty]$ e $\mathbb{Z}W$ são isomorfas, se e somente se, $W = H \rtimes_\varphi C_\infty$, de modo que*

**i.** *O grupo $H \subseteq W$ é um subgrupo finito, tal que as $\mathbb{Z}$-álgebras $\mathbb{Z}G$ e $ZH$ são isomorfas;*

**ii.** *O automorfismo $\varphi$ de $H$ é induzido pela conjugação com uma unidade $x \in \mathbb{Z}H$ que normaliza $H$.*

**Demonstração.** Seja $K = G \times C_\infty$. Então pelo corolário 2.2.3, $W = T(W) \rtimes_\varphi C_\infty$, com $|T(W)| = |G|$ e pelo corolário 1.2.34, $\mathbb{Z}G \cong \mathbb{Z}T(W)$. Podemos tomar $\psi$ um isomorfismo normalizado entre os anéis $\mathbb{Z}K$ e $\mathbb{Z}W$, supondo $\mathbb{Z}K = \mathbb{Z}W$. Seja $z \in K$, tal que $< z >= C_\infty$, e $w \in W$, tal que $< w >= C_\infty$. Sendo $z$ central em $\mathbb{Z}K = \mathbb{Z}W$, então $z \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}W))$. Pelo teorema 3.1.7, temos que $z = rg$, $r \in \mathbb{Z}T(W)$, e $g \in W$. Escrevendo $g = sw^n$, $n \in \mathbb{Z}$, $s \in T(W)$, temos que $z = rsw^n = x^{-1}w^n$, $rs = x^{-1} \in \mathbb{Z}T(W)$. Tomando-se o quociente de $ZK = \mathbb{Z}W$ por $\Delta(K, G) = \Delta(W, T(W))$, obtemos $\mathbb{Z}C_\infty = \mathbb{Z}< w >$. Consideramos, por um lado, a projeção de $z = x^{-1}w^n$ em $\mathbb{Z}C_\infty = \mathbb{Z}< w >$, ou seja $\overline{z} = \overline{w}^n$, por outro lado, pelo corolário 1.2.43, $\mathcal{U}_1(\mathbb{Z}C_\infty) = C_\infty =< \overline{z} >=< \overline{w} >= \mathcal{U}_1(\mathbb{Z} < w >)$, portanto $< \overline{w} >=< \overline{w}^n > \Longrightarrow n = \pm 1$. Logo a projeção de $z$ em $\mathbb{Z}C_\infty$ e em $\mathbb{Z}< w >$ é a mesma. Portanto, $n = \pm 1$, e $z = x^{-1}w$. Tomemos $h \in T(W)$, $h = z^{-1}hz$, pois $z$ é central. Então $h = w^{-1}xhx^{-1}w \Longrightarrow \varphi(h) = whw^{-1} = xhx^{-1} = h^x \in T(W)$, logo $x$ é a unidade que normaliza $H = T(W)$. □

Finalizamos este capítulo com uma demonstração do corolário 1.2.20 para unidades centrais de torção em anéis de grupo, usando o teorema de estrutura das unidades centrais discutido.

**Teorema 3.2.2.** *Seja $G$ um grupo. As unidades centrais de torção de $\mathbb{Z}G$ são triviais.*

**Demonstração.** Seja $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ uma unidade de torção, $o(u) = n$. Pelo teorema 3.1.7, $u = rg$, $r \in \mathbb{Z}T(G)$, $g \in G$; $u^n = r^n g^n = 1$, portanto, $r^n = g^{-n} \in \mathbb{Z}T(G)$; $g^n \in \mathbb{Z}T(G) \cap G$, sendo $T(G) \subset G$, então $g^n = h \in T$. De fato, podemos considerar o homomorfismo $i : \mathbb{Z}T(G) \hookrightarrow \mathbb{Z}G$, então $h = \sum_{t \in T(G)} \alpha_t t \in \mathbb{Z}G$, pela independência dos elementos da base $T(G)$, $h \in T(G)$. Então $g \in T(G)$. Portanto, $u \in \mathbb{Z}T(G)$, e pelo corolário 1.2.20, para grupos finitos, $u$ é trivial. □

## 3.3 Reflexão sobre Alguns Resultados Obtidos

Encerramos este capítulo considerando o grupo das unidades centrais de anéis de grupo infinitos do tipo estudado no segundo capítulo, isto é, $\mathbb{Z}[G \times C_\infty]$, para alguns grupos finitos, representados por $G$. Consideremos daqui em diante $C_\infty =< v >$.

O artigo [9] apresenta a contrução de geradores para o centro das unidades de grupos nilpotentes finitamente gerados, ou seja, de geradores para subgrupos do grupo $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. No caso de nosso exemplo, uma vez conhecida a estrutura de uma unidade central qualquer, podemos obter resultados mais gerais para o anel de grupo dessa classe de grupos. Com efeito, seja $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}[G\times < v >]))$, então $u = rg$, $r \in \mathbb{Z}G$ e $g \in [G\times < v >]$, logo $g = g_1 v^n$ com $g_1 \in G$ e $n \in \mathbb{Z}$; $u = rg_1 v^n = r_1 v^n$, com $r_1 \in \mathbb{Z}G$. Ora, $r_1 = uv^{-n}$ e sendo $v$ um elemento central em $G\times < v >$, então $r_1$ é central, portanto, o centro de $\mathcal{U}(\mathbb{Z}[G\times < v >])$ fica determinado a partir de $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.

Apresentamos alguns resultados para o centro de $\mathcal{U}(\mathbb{Z}G)$ quando $G$ é finito:

(1) Se $G$ é abeliano de expoente $2, 3, 4, 6$ ou G é um 2-grupo hamiltoniano, então $\mathcal{U}(\mathbb{Z}G) = \pm G$. (Higman). Portanto,

$$\mathcal{Z}(\mathcal{U}(\mathbb{Z}[G\times < v >])) = \pm[\mathcal{Z}(G)\times < v >]$$

(2) Se $G = S_n$, o grupo de permutações de n elementos, então

$$\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) = \begin{cases} \pm S_2 & \text{se } n = 2 \\ \pm 1 & \text{se n} > 2 \end{cases} \text{ (Ritter-Sehgal)}$$

E, portanto, o centro das unidades do anel de grupo é

$$\mathcal{Z}(\mathcal{U}(\mathbb{Z}[G\times < v >])) = \begin{cases} \pm[S_2\times < v >] & \text{se } n = 2 \\ \pm < v > & \text{se } n > 2 \end{cases}$$

(3) Se $G = A_n$, o grupo alternado, subgrupo de $S_n$, então se $n < 4$, o centro das unidades de $\mathbb{Z}G$ é trivial (Higman), e se $n \geq 4$, podemos garantir, pelo corolário 3.1.11, que $\mathcal{U}(\mathbb{Z}G)$ é um grupo finitamente gerado.

Finalizamos a dissertação com a construção do grupo das unidades centrais do anel $\mathbb{Z}A_5$, que é um grupo finitamente gerado (lema 3.1.11). Provamos que para $\mathbb{Z}A_5$, o grupo de unidades centrais é um grupo livre de posto 1.

Para apresentação dos resultados, discutimos alguns tópicos básicos da teoria de caracteres e alguns teoremas sobre representação do grupo de unidades centrais do anel de grupo sobre os racionais desse grupo.

Observamos, novamente, que em [9] é mostrado um método para construção de geradores para subgrupos do grupo de unidades centrais. Aqui, no entanto, exibimos explicitamente o grupo de unidades centrais do anel de grupo estudado.

# Capítulo 4

# O GRUPO DAS UNIDADES CENTRAIS DE $\mathbb{Z}A_5$

Neste capítulo, descrevemos o grupo das unidades centrais do anel de grupo $\mathbb{Z}A_5$, sendo $A_5$ o subgrupo alternado de $S_5$ o grupo das permutações de 5 elementos.

Nosso objetivo é determinar o centro das unidades para anéis de grupo da forma $\mathbb{Z}(G \times C_\infty)$, que com o auxílio do teorema 3.1.7, reduz-se à determinação do centro de $\mathbb{Z}G$, para $G$ um grupo de ordem finita.

O artigo [9], como mencionamos, apresenta um procedimento para construir geradores para um subgrupo de índice finito no grupo das unidades centrais de grupos nilpotentes finitamente gerados. Apresentamos neste capítulo uma construção mais abrangente, isto é, explicitamos os geradores do centro das unidades do anel de grupo $\mathbb{Z}A_5$.

Iniciamos com alguns fatos básicos de teoria de caracteres e teoria de números.

## 4.1 Preliminares

### 4.1.1 Teoria de Caracteres

**Definição 4.1.1.** *Seja $G$ um grupo, e $V$ um espaço vetorial sobre um corpo $K$. Uma $K$-representação de um grupo $G$ é um homomorfismo:*

$$\begin{aligned} \Psi : G &\longrightarrow GL(V) \quad GL(V) = \{T : V \longrightarrow V, \textit{transformação linear invertível}\} \\ g &\mapsto T_g. \end{aligned}$$

*Se supusermos $n = dim_K V$ e $B$ uma base de $V$, a cada $g \in G$, associamos $\mathcal{I}m(\Psi_g) \in GL(V)$ com $T_g := [\Psi_g]_B$.*

Nessa discussão, consideramos $V$ um espaço vetorial de dimensão finita e $G$ um grupo de ordem finita.

**Proposição 4.1.2.** *Nas condições acima,*

$$\begin{aligned}\hat{\Psi} : G &\longrightarrow M_n(K) \in GL(n,K)\\ g &\mapsto T_g = [\Psi_g]_B\end{aligned}$$

*é uma representação de $G$.*

**Demonstração.** De fato, $\hat{\Psi}(gh) = [\Psi_{gh}]_B = [\Psi_g \circ \Psi_h]_B = [\Psi_g]_B[\Psi_h]_B = \hat{\Psi}_g\hat{\Psi}_h$. Logo $\hat{\Psi}$ é homomorfismo. Além disso, $\mathcal{I}m(\Psi) \subseteq GL(n,K) = \{A \in M_n(K) : det(A) \neq 0\}$, pois $\Psi_g\Psi_{g^{-1}} = Id_V$. □

**Lema 4.1.3.** *Podemos considerar uma $K$-representação de $G$ como um $KG$-módulo.*

**Demonstração.** Seja $V$ um $KG$-módulo. Estendemos $\Psi$, definida em 4.1.1, de $KG$ em $V$, da seguinte forma:

$$\begin{aligned}\hat{\Psi}_g : KG \times V &\longrightarrow V\\ (\textstyle\sum \alpha_g g, v) &\mapsto \textstyle\sum \alpha_g \Psi_g(v).\end{aligned}$$

□

**Definição 4.1.4.** *Suponha $\Psi$ como na definição 4.1.1. O caractere associado a $\Psi$ é definido por:*

$$\begin{aligned}\chi : G &\longrightarrow K\\ g &\mapsto tr[(\Psi_g)]_B,\end{aligned}$$

*a qual $tr$ é a função traço que associa à matriz $M = (a_{ij})$ seu traço $tr(M) = \sum_{i=1}^{n} a_{ii}$, sendo $n$ a dimensão de $V$.*

Observe que $\chi$ está bem definida, pois se $B$ e $B_1$ são duas bases de $V$, então $A = [\Psi g]_B \sim [\Psi g]_{B_1} = B \Longrightarrow tr(A) = tr(B)$.

**Definição 4.1.5.** *Uma função $f : G \longrightarrow K$ é dita uma função de classe se $g \sim h \Longrightarrow f(g) = f(h)$, isto é, $f$ é constante sobre classes de conjugação.*

**Lema 4.1.6.** *Seja $\chi : G \longrightarrow K$ o caractere associado a $\Psi$. Então $\chi$ é uma função de classe.*

**Demonstração.** $\chi(ghg^{-1}) = tr([\Psi(ghg^{-1})]_B) = tr([\Psi(g)\Psi(h)\Psi(g^{-1})]_B) =$
$tr([\Psi(g)]_B[\Psi(h)]_B[\Psi(g^{-1})]_B) = tr([\Psi(h)]_B) = tr(h)$. □

Para os $K$ espaços vetoriais $V, W$, dadas as representacões

$$\Psi_1 : G \longrightarrow GL(V)$$
$$\Psi_2 : G \longrightarrow GL(W),$$

$V, W$ podem ser tomados como $KG$-módulos.

**Definição 4.1.7.** *Dizemos que $\Psi_1$ e $\Psi_2$ são equivalentes, se $\exists\ \alpha : V \longrightarrow W$, um $KG$-isomorfismo, tal que o diagrama*

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & W \\ {\scriptstyle \Psi_{1g}}\downarrow & & \downarrow{\scriptstyle \Psi_{2g}} \\ V & \xrightarrow{\alpha} & W \end{array}$$

*comuta, $\forall\ g \in G$.*

Isto é, se para $v \in V$ $gv := \Psi_{1g}(v)$ e para $w \in W$, $gw := \Psi_{2g}(w)$, então para $v \in V$ temos que $\alpha(\Psi_{1g}v) = \Psi_{2g}(\alpha(v))$, ou seja $\alpha(gv) = g\alpha(v)$.

**Lema 4.1.8.** *Se $\Psi_1, \Psi_2$ são representações equivalentes de $G$, então elas induzem o mesmo caractere.*

**Definição 4.1.9.** *Seja $\Psi : G \longrightarrow V$ uma $K$-representação. Considerando-se $V$ como $KG$-módulo, dizemos que $\Psi$ é redutível se $V$ for decomponível como $KG$-módulo, isto é, $V = V_1 \oplus V_2$, com $V_1$ e $V_2$ $KG$-submódulos próprios de $V$.*

**Proposição 4.1.10.** *Suponha que $V = V_1 \oplus V_2$ como $KG$-módulos, e $\Psi_i : G \longrightarrow GL(V_i)$, para $i = 1, 2$. Se $B_1, B_2$ são as bases de $V_1$ e $V_2$, respectivamente bases. Então $B = B_1 \cup B_2$ é uma base de $V$, ou seja,*

$$[\Psi_g]_B = \begin{pmatrix} [\Psi_g]_{B1} & 0 \\ 0 & [\Psi_g]_{B2} \end{pmatrix}_B .$$

**Teorema 4.1.11.** *Seja $G$ um grupo finito, $k_1, \cdots, k_s$ as classes de conjugação de $G$, e $\mathcal{K}_i = \sum_{x \in k_i} x$ $\in \mathbb{C}G$, $1 \leq i \leq s$ as somas das classes de conjugação $k_i$. Então $\{\mathcal{K}_1, \cdots, \mathcal{K}_s\}$ forma uma base do $\mathcal{Z}(\mathbb{C}G)$.*

**Demonstração.** A demonstração é idêntica a do lema 1.2.35 para o corpo $\mathbb{C}$, em lugar do anel $\mathbb{Z}$. □

Para a discussão procedente, é suficiente tomarmos $K = \mathbb{C}$, ou seja, consideramos o anel $\mathbb{C}G$ com $G$ um grupo finito. Nessas condições, pelo teorema 1.2.9, $\mathbb{C}G = \bigoplus_{i=1}^{n} M_{n_i}(\mathbb{C})$, $M_{n_i}(\mathbb{C}) \cong$

$(\mathbb{C}G)e_i$ e do corolário 1.2.11, $n = s$ o número de classes de conjugação do grupo $G$. Sendo $1 = \sum_{i=1}^{n} e_i$, $e_i$ os idempotentes ortogonais, primitivos e centrais em $\mathbb{C}G$. Para cada $i$ definimos

$$\begin{aligned} \Phi_i : G &\longrightarrow M_{n_i}(\mathbb{C}) \\ g &\mapsto ge_i. \end{aligned}$$

Então $\Phi_i(gh) = (gh)e_i = (gh)e_i^2 = (ge_ihe_i) = \Phi_i(g)\Phi_i(h)$ e, portanto, $\Phi_i$ é um homomorfismo.

**Proposição 4.1.12.** *A cada $\Phi_i$ definido acima está associado $V_i = \mathbb{C}^{n_i}$ como $\mathbb{C}G$-módulo. Nessas condições, $F = \{\Phi_1, \cdots, \Phi_n\}$ é o conjunto de todas as $\mathbb{C}$-representações irredutíveis de $\mathbb{C}G$.*

**Definição 4.1.13.** *Seja $F = \{\Phi_1, \cdots, \Phi_s\}$ o conjunto de todas as $\mathbb{C}$-representações irredutíveis de um $\mathbb{C}G$-módulo com $s$ o número de classes de conjugação de $G$, associamos a cada $\Phi_i$ o caractere $\chi_i$ com $1 \leq i \leq s$, isto é,*

$$\begin{aligned} \Phi_i \longmapsto \chi_i : G &\longrightarrow \mathbb{C} \\ g &\mapsto tr[\Phi_i(g)]. \end{aligned}$$

*Definimos $\mathcal{I}rr(G) = \{\chi_i : 1 \leq i \leq s\}$ o conjunto dos caracteres irredutíveis de $G$.*

**Teorema 4.1.14.** *Seja $G$ um grupo finito. Os caracteres do conjunto $\mathcal{I}rr(G) = \{\chi_i : 1 \leq i \leq s\}$, são todos distintos.*

**Demonstração.** Com efeito, sendo $\mathbb{C}G = \sum M_i$, o qual $\{M_1, \cdots, M_s\}$ é um conjunto representativo de $CG$-módulos irredutíveis, então se $1 \in \mathbb{C}G$, $1 = \sum_{i=1}^{s} e_i$. Fixado algum $M_i$, com $i \neq j$, $M_j$ é o anulador de $M_i$, portanto, $\Psi_i(1) = I_{id} = \Psi_i(e_i)$, e $\Psi_i(e_j) = 0$, se $i \neq j$. Portanto, $\chi_i(1) = \chi_i(e_i) \neq 0$, logo os $\chi_i$ são distintos. □

**Corolário 4.1.15.** *Se $\mathbb{C}G = \bigoplus(\mathbb{C}G)e_i$, então $\chi_i(e_j) = \chi_i(1)\delta_{ij}$.*

Definimos $\Phi_i$ a representação associada ao módulo irredutível $M_i$ e $\chi_i$ o caractere oferecido por esta. Nesse caso, $\chi_i(1) = dim_K(M_i)$, pois, $\Phi_i(1) = I_{id}$, restrita a $M_i$. Podemos, então enunciar a seguinte proposição:

**Proposição 4.1.16.** *Seja $K$ um corpo algebricamente fechado, e $G$ um grupo finito. Então a cardinalidade de $\mathcal{I}rr(G)$ é o número de classes de conjugação de $G$, e $|G| = \sum_{\chi \in \mathcal{I}irr(G)} \chi(1)^2$.*

**Teorema 4.1.17.** *Toda função de classe $\varphi$ de $G$ pode ser unicamente expressa na forma $\varphi = \sum_{\chi \in \mathcal{I}rr(G)} a_\chi \chi$, com $a_\chi \in \mathbb{C}$. Além disso, $\varphi$ é um caractere, se e somente se, todos os $a_\chi$ são inteiros não negativos, e $\varphi \neq 0$.*

**Observação 4.1.18.** *Em 4.2.4, recaímos naturalmente no exemplo de um sub-anel $KG \subset \mathbb{C}G$ o qual $K$, não é um corpo algebricamente fechado, de modo que o número de componentes simples do centro das unidades do anel $KG$ não é o mesmo das componentes simples de seu anel.*

A todo $K$-módulo podemos associar um $K$-espaço vetorial $V$. Considerando $KG$ um $KG$-módulo sobre si mesmo, podemos considerar a $K$-representação de $G$ associada a esse módulo.

**Definição 4.1.19.** *Seja $V$ o espaço vetorial associado ao $KG$-módulo $KG$, cuja $K$-base é constituída pelos elementos de um grupo finito $G$. Definimos a $K$-representação regular de $G$ como sendo*

$$\begin{aligned} \hat{\varrho} : G &\longrightarrow GL(KG) \\ g &\mapsto [\varrho_g]_B : V \longrightarrow V \\ & \qquad\quad v \mapsto [\varrho_g]_B v. \end{aligned}$$

*o qual $B = G$, sendo $[\varrho_g]_B$. Denote $\rho$ o caractere oferecido por essa representação.*

**Proposição 4.1.20.** *Seja $g \in G$. Então*

$$\rho(g) = \begin{cases} |G| & \text{se } g\text{=}1, \\ 0 & \text{se } g \neq 1 \end{cases}$$

**Lema 4.1.21.** *Sendo $\rho$ um caractere de $G$, este pode ser expresso como uma combinação linear inteira de $\chi_i$, temos*

$$\rho = \sum_{i=1}^{s} \chi_i(1)\chi_i.$$

**Demonstração.** Sendo $KG$ semisimples, temos que $KG = \bigoplus_{i=1}^{n} M_i$. Sejam $B_i$ bases de $V_i$, espaços vetoriais associados aos $KG$-módulos $M_i$; $B = \dot{\bigcup}_{i=1,n} B_i$, logo

$$[\varrho(g)]_B = \begin{pmatrix} [M_1]_{B_1} & & & & 0 \\ & \ddots & & & \\ & & [M_i]_{B_i} & & \\ & & & \ddots & \\ 0 & & & & [M_n]_{B_n} \end{pmatrix}.$$

Como o traço independe da base, o caractere oferecido por essa representação é $\rho(g) = \sum_{i=1}^{s} n_{M_i}(V)\chi_i$, sendo $n_{M_i}(V) = dim_K(M_i) = \chi_i(1)$. Daí segue o resultado. □

**Teorema 4.1.22.** *Seja $G$ um grupo de ordem finita, e $e_i$ os idempotentes da decomposição de $\mathbb{C}G = \bigoplus_{i=1}^{s}(\mathbb{C}G)e_i$, sendo $s$ o número de classes de conjugação de $G$. Então os idempotentes $e_i$, $1 \leq i \leq s$, podem ser escritos da seguinte forma:*

$$e_i = \frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g.$$

**Demonstração.** Seja $e_i = \sum_{g\in G}\alpha_i(g)g$. Pela proposição (4.1.20), $\rho(e_ig^{-1}) = \alpha_i(g)|G| \Longrightarrow e_i = \frac{1}{|G|}\sum_{g\in G}\rho(e_ig^{-1})g$, pelo lema (4.1.21), $\rho = \sum_i \chi_i(1)\chi_i \Longrightarrow e_i = \frac{1}{|G|}\sum_{g\in G}\sum_{j=1}^{s}\chi_j(1)\chi_j(e_ig^{-1})g$, do resultado do corolário 4.1.15, $e_i = \frac{1}{|G|}\sum_{g\in G}\sum_{j=1}^{s}\chi_j(1)\chi_j(g^{-1})g\delta_{ij}$, daí o resultado do teorema. □

**Teorema 4.1.23** (Relação geral de ortogonalidade)**.** *Seja $G$ um grupo finito. Para todo $h \in G$, temos*

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(gh)\chi_j(g^{-1}) = \delta_{ij}\frac{\chi_i(h)}{\chi_i(1)}.$$

**Demonstração.** Basta calcular o produto $e_ie_j = \delta_{ij}e_i$, utilizando a expressão do teorema anterior para cada idempotente. □

**Corolário 4.1.24** (Primeira Relação de Ortogonalidade)**.** *Tomando $h = 1$ no teorema (4.1.23), obtemos*

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = \delta_{ij}.$$

**Lema 4.1.25.** *Seja $\Psi$ uma $\mathbb{C}$-representação de $G$, um grupo finito, provindo o caractere $\chi$, e seja $g \in G$, cuja $o(g) = n$. Então*

**i.** *$\Psi(g)$ é semelhante a uma matriz diagonal*

$$\Psi(g) \cong \begin{pmatrix} \epsilon_1 & & \\ & \ddots & \\ & & \epsilon_n \end{pmatrix},$$

*com $\epsilon_i$ raiz $n$-ésima da unidade;*

**ii.** $\chi(g) = \sum_{i=1}^{s}\epsilon_i$ *e* $|\chi(g)| \leq \chi(1)$*;*

**iii.** $\chi_i(g^{-1}) = \overline{\chi_i(g)}$.

**Demonstração.** Considerando-se $V$ como um $\mathbb{C}G$-módulo, definimos

$$\Psi_g : V \longrightarrow V \text{ uma } \mathbb{C}\text{-representação de V.}$$

Sendo $o(g) = n$, ocorre que $\Psi_{g^n} = (\Psi_g)^n = I_d$, a matriz identidade, $(\Psi_g)^n - I_d = 0$. Logo o polinômio $p(x) = x^n - 1$, múltiplo do polinômio minimal de $\Psi_g$, é um polinômio separável em $\mathbb{C}[x]$. Portanto $p(x)$ tem $n$ raízes distintas, assim se $B$ é uma base de $V$, a matriz $[\Psi]_B$ é diagonalizável, logo

$$\Psi(g) \cong \begin{pmatrix} \epsilon_1 & & \\ & \ddots & \\ & & \epsilon_n \end{pmatrix},$$

e $\chi(g) = tr(\Psi_g) = \sum_{i=1}^{s} \epsilon_i$, sendo cada $\epsilon_i$ raiz do polinômio $p(x)$, portanto, uma raiz $n$-ésima da unidade. Os caracteres irredutíveis de $\Psi_g$ são cada $\chi_i(g) = \epsilon_i$. Considerando $\Psi_{g^{-1}} = (\Psi_g)^{-1}$ e temos

$$(\Psi(g))^{-1} \cong \begin{pmatrix} \frac{1}{\epsilon_1} & & \\ & \ddots & \\ & & \frac{1}{\epsilon_n} \end{pmatrix} = \begin{pmatrix} \overline{\epsilon_1} & & \\ & \ddots & \\ & & \overline{\epsilon_n} \end{pmatrix}.$$

Logo $\chi(g^{-1}) = \overline{\chi(g)}$. □

**Corolário 4.1.26.** *Seja $G$ um grupo finito. Seja $\chi \in \mathcal{I}rr(G)$. Então $\chi(g)$ é um inteiro algébrico.*

A partir do resultado do lema anterior $\chi(g^{-1}) = \overline{\chi(g)}$, e pelo corolário 4.1.24, obtemos a relação:

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}.$$

**Definição 4.1.27.** *Seja $G$ um grupo finito. Se $s$ é o número de classes de conjugação distintas de $G$, $g_i$ são representantes de cada classe de conjugação, e $\chi_i \in \mathcal{I}rr(G)$, para $1 \leq i \leq s$. Definimos a tábua de caracteres de $G$ como sendo a matriz $\mathcal{X} = (\chi_i(g_j))$, $1 \leq i, j \leq s$.*

**Teorema 4.1.28** (Segunda Relação de Ortogonalidade)**.** *Sejam $g, h \in G$. Então*

$$\sum_{\chi \in \mathcal{I}rr(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |C(g)|, \text{ se } g \sim h \\ 0, \text{ se } g \not\sim h. \end{cases}$$

**Demonstração.** Do corolário anterior, $|G|\delta_{ij} = \sum_{g \in G} \chi_i(g)\overline{\chi}_j(g) = \sum_{\nu=1}^{s} |k_\nu|\chi_i(g_\nu)\overline{\chi}_j(g_\nu)$, sendo $|k_i|$ a ordem de $|cl(g_i)|$, a classe de conjugação de $g_i \in G$. Tomando-se $\mathcal{X}$, a tábua de caracteres

de $G$ e definindo-se

$$D \doteq \begin{pmatrix} k_1 & & \\ & \ddots & \\ & & k_s \end{pmatrix}.$$

Então $|G|\delta_{ij} = \mathcal{X}D\overline{\mathcal{X}}$. Ora, $\mathcal{X} = \chi_{ij}E_{ij}$, e $\overline{\mathcal{X}} = \overline{\chi}_{ij}E_{ij} \Longrightarrow \mathcal{X}\overline{\mathcal{X}}^T = \chi_{ij}E_{ij}\overline{\chi}_{lm}E_{lm}$, com $E_{ij}$ as matrizes fundamentais. Sendo $D$ matriz diagonal, $D\mathcal{X}\overline{\mathcal{X}}^T = \sum_i k_\nu \chi_{\nu i}\overline{\chi}_{\nu i}E_{\nu\nu} = \sum_i k_\nu \overline{\chi}_{\nu i}\chi_{\nu i}E_{\nu\nu} = D\overline{\mathcal{X}}^T\mathcal{X}$. Portanto, $|G|\delta_{ij} = \sum_\nu |k_i|\overline{\chi}_\nu(g_i)\chi_\nu(g_j)$, sendo $\frac{|G|}{k_i} = |C_G(g_i)|$, a ordem do centralizador. Então temos o resultado do teorema. □

**Definição 4.1.29.** *Para o conjunto das classes de conjugação distintas, de um grupo $G$, $cl(g_i)$, definimos $\mathcal{K}_i$, pela soma dos elementos da classe $cl(g_i)$, sendo $1 \leq i \leq s$, e $s$ o número de classes de conjugação do grupo $G$.*

As propriedades até aqui discutidas permitem obter dois importantes resultados para a apresentação do exemplo proposto neste capítulo. Temos, então o seguinte lema:

**Lema 4.1.30.** *Seja $G$ um grupo finito. Considere $\mathbb{C}G = \bigoplus_{i=1}^{s}(\mathbb{C}G)e_i$, sendo $s$ o número de classes distintas de conjugação de $G$. Podemos exprimir os idempotentes $e_i$ na base $B = \{\mathcal{K}_1, \cdots, \mathcal{K}_s\}$, bem como para cada $\mathcal{K}_i \in B$, escrevê-los na base $E = \{e_1, \cdots, e_s\}$. Então temos*

$$e_i = \frac{\chi_i(1)}{|G|}\sum_{j=1}^{s}\overline{\chi}_i(g)\mathcal{K}_j; \tag{4.1}$$

$$\mathcal{K}_i = |k_i|\sum_{j=1}^{s}\frac{\chi_j(g_i)}{\chi_j(1)}e_j. \tag{4.2}$$

**Demonstração.** Cada $e_i$ é combinação linear sobre $\mathbb{C}G$ dos elementos da base $B$. Pelo teorema teorema 4.1.22,

$e_i = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\overline{\chi}_i(g)g$, sendo $G = \dot{\bigcup}_{i=1,s} Supp(\mathcal{K}_i)$, então $\sum_{g\in G}\overline{\chi}_i(g)g = \sum_{j=1}^{s}\sum_{l=1}^{|k_j|}\overline{\chi}_i(g_{j_l})g_{j_l} = \sum_{j=1}^{s}\overline{\chi}_i(g_j)\mathcal{K}_j$.
Seja $\mathcal{K}_i \in B$, cada $\mathcal{K}_i$ pode ser escrito como combinação linear, sobre $\mathbb{C}G$, dos idempotentes $e_i$, isto é, se $\mathcal{K}_i = \sum_j x_j e_j \Longrightarrow \chi_j(\mathcal{K}_i) = \sum_k x_k\chi_j(e_k) = x_j\chi_j(1)$, também sabemos que, $\chi_j(\mathcal{K}_i) = \chi_j(\sum_{g\cong g_i} g_i) = \mathcal{K}_i\chi_j(g_i)$. Portanto, $x_j = \frac{\mathcal{K}_i\chi_j(g_i)}{\chi_j(1)}$. □

**Proposição 4.1.31.** *Seja $u$ uma unidade central arbitrária do anel de grupo $\mathbb{C}G$. Então*

**i.** $u = \sum_{i=1}^{s}\gamma_i\mathcal{K}_i = \sum_{i=1}^{s}\beta_i e_i$;

**ii.** *Se denotamos* $\beta = (\beta_1, \cdots, \beta_s)$, *e* $\gamma = (\gamma_1, \cdots, \gamma_s)$, *temos que*

$$\begin{aligned} \beta &= S\gamma; && (4.3)\\ \gamma &= T\beta; && (4.4)\\ S &= diag(\frac{1}{\chi_1(1)}, \cdots, \frac{1}{\chi_s(1)})\mathcal{X}diag(|k_1|, \cdots, |k_s|); && (4.5)\\ T &= \frac{1}{|G|}\mathcal{X}^* diag(\frac{1}{\chi_1(1)}, \cdots, \frac{1}{\chi_s(1)}); && (4.6)\\ \mathcal{X} &= (\chi_i(g_j)), 1 \leq i, j \leq s. && (4.7) \end{aligned}$$

### 4.1.2 Teoria dos Números

#### 4.1.2.1 O Teorema dos Invertíveis de Dirichlet

**Definição 4.1.32.** *Seja* $L$ *um corpo, e seja* $S$ *um subanel de* $L$. *Definimos* $\mathcal{Q}(S) = \{ab^{-1} | a, b \in S \text{ e } b \neq 0\}$, *o menor subcorpo de* $L$ *que contém* $S$, *como o corpo de quocientes de* $S$ *em* $L$.

**Definição 4.1.33.** *Dada uma extensão* $L$ *de* $\mathbb{Q}$, *cujo grau é* $n$, *existem exatamente* $n$ *isomorfismos* $\sigma$ *de* $L$ *em* $\mathbb{C}$. *Dizemos que* $\sigma$ *é uma imersão real (respectivamente complexa) de* $L$, *quando* $\sigma(L) \subset \mathbb{R}$ *(respectivamente* $\not\subset \mathbb{R}$*). No caso de* $\sigma$ *ser uma extensão complexa, então a aplicação* $\overline{\sigma} : L \longrightarrow \mathbb{C}$, *que associa a cada* $\alpha \in L$ *o complexo conjugado de* $\sigma(\alpha)$, *também é uma imersão complexa e o par* $\sigma, \overline{\sigma}$ *são imersões complexo-conjugadas.*

**Definição 4.1.34.** *O anel* $I_S(R)$ *é chamado o fecho inteiro de* $R$ *em* $S$. *Este é o conjunto dos elementos de* $S$ *que são inteiros sobre* $R$, *ou seja,* $\alpha \in I_S(R)$, *se e somente se, existe* $f(x) \in R[x]$, *tal que* $f(\alpha) = 0$. *No caso em que* $S = L$, *o corpo de números algébricos, o anel* $I_L(\mathbb{Z})$ *é chamado o anel dos inteiros algébricos de* $L$, *e denotado por* $I_L$.

**Definição 4.1.35.** *Definimos W(L) o grupo das raízes da unidade em* $L$, *ou seja o subgrupo de torção do grupo multiplicativo* $L^*$ *de* $L$.

**Teorema 4.1.36.** *[Teorema das Unidades de Dirichlet] Seja* $L$ *uma extensão de* $\mathbb{Q}$ *de grau* $n$ *que possua* $s$ *imersões reais, e* $t$ *pares de imersões complexo-conjugadas, e seja* $S$ *um subanel de* $I_L$, *tal que* $\mathcal{Q}(S) = L$. *Então existem* $\epsilon_1, \cdots, \epsilon_{s+t-1} \in U(S)$, *tal que*

$$U(S) = T(S) \odot < (\epsilon_1) > \cdots \odot < (\epsilon_{s+t-1}) > .$$

*O produto direto do grupo cíclico finito* $T(S) = T(L) \cap U(S)$ *e dos grupos cíclicos infinitos gerados por* $\epsilon_1, \cdots, \epsilon_{s+t-1}$.

#### 4.1.2.2 Invertíveis em Corpos Quadráticos

Nesta seção, apresentamos as soluções da equação

$$x^2 - ky^2 \text{ Equação de Pell.}$$

Denominamos $L$ um corpo quadrático um subcorpo do corpo dos números complexos de índice 2 sobre $\mathbb{Q}$, isto é, $[L:\mathbb{Q}] = 2$. Vamos utilizar $\mathcal{D}$ para representar o conjunto de números inteiros livres de quadrado, ou seja, $\mathcal{D} = \{d \in \mathbb{Z} : n^2 \text{ não divide } d \text{ para todo } n \in \mathbb{Z} \setminus \{\pm 1\}\}$.

**Teorema 4.1.37.** *Seja $L = \mathbb{Q}(\sqrt{d})$, o qual $d \in \mathcal{D}$, e seja $\delta = \sqrt{d}$ (respectivamente $\delta = \frac{1+\sqrt{d}}{2}$), se $d \equiv 2$, ou 3 (respectivamente $d \equiv 1$) mod4, então $\{1, \delta\}$ forma uma base do $\mathbb{Z}$-módulo $I_L$.*

**Definição 4.1.38.** *Se $L$ é uma extensão finita de $\mathbb{Q}$, definimos ordem de $L$ um subanel $S \subseteq I_L$, tal que $S$ seja um $\mathbb{Z}$-módulo livre de posto $n$.*

Sendo $d \in \mathcal{D}$, e $L_d = \mathbb{Q}(\sqrt{d})$, definimos $S_{n,d}$ o subanel $\mathbb{Z}[n\delta]$ de $I_d$, para o qual $\{1, n\delta\}$ forma uma $\mathbb{Z}$-base sendo $\delta = \sqrt{d}$ (respectivamente $\delta = \frac{1+\sqrt{d}}{2}$) se $d \equiv 2$, ou 3 (respectivamente $d \equiv 1$) $mod4$.

**Definição 4.1.39.** *Seja $S \subset I_d$, tal que $S \neq \mathbb{Z}$, uma ordem de $L_d$. Definimos o conjunto $U(S) = \{\eta \in S : |\mathcal{N}(\eta)| = 1\} = U(I_d) \cap S$, sendo $\mathcal{N} = \mathcal{N}_{L_d}|\mathbb{Q}$ a norma em relação à extensão $L_d|\mathbb{Q}$. Pelo fato da norma poder assumir os valores $\pm 1$, é conveniente definir $U_e(S) = \{\eta \in S : \mathcal{N}(\eta) = (-1)^e\}$, $e \in \{0, 1\}$.*

Pela definição acima $U(S) = U_0(S) \dot{\cup} U_1(S)$. Sendo $\mathcal{N}(\eta)$, $\eta \in S$ dada pelas expressões:

$$\mathcal{N}(x + yn\sqrt{d}) = x^2 - n^2 dy^2; \tag{4.8}$$

$$\mathcal{N}(x + yn\frac{1+\sqrt{d}}{2}) = x^2 + xyn + (yn)^2\frac{1-d}{4}. \tag{4.9}$$

**Proposição 4.1.40.** *Para $a, b \in \mathbb{Z}$, temos:*

**i.** *$a + bn\sqrt{d} \in U_e(\mathbb{Z}[n\sqrt{d}])$, se e somente se, (a,b) for solução da equação 4.8.*

**ii.** *Se $d \equiv 1 mod 4$, então $a + bn\delta \in U_e(S_{d,n})$, se e somente se, (a,b) for solução da equação 4.9.*

Consideramos, para os resultados seguintes, que o corpo $L_d$ é um corpo real, isto é, $d > 0$. Nesse caso, temos que $W = \{-1, 1\}$ e, pelo teorema 4.1.36, $\mathcal{U}(S) = \{-1, 1\} \odot (\epsilon)$, a qual $\epsilon$ tem ordem infinita.

**Definição 4.1.41.** *Seja $L_d$ um corpo real, e $S \subset L_d$. Definimos o invertível fundamental de $S$ como sendo o elemento do conjunto $\{\epsilon, -\epsilon, \epsilon^{-1}, -\epsilon^{-1}\}$ que é maior que 1.*

Definindo-se

$$V(S) = \{\eta \in U(S) : \eta > 1\},$$

então $V(S) = \{\epsilon^j : j \in \mathbb{N} \setminus \{0\}\}$. Portanto $\epsilon = minV(S)$.

**Proposição 4.1.42.** *Para todo $d$ livre de quadrados, e $n \in \mathbb{N} \setminus \{0\}$, temos que $V(S_{d,n}) \subseteq \{a + bn\delta : a, b \in \mathbb{Z},\ a > 0,\ e\ b > 0\}$, exceto quando $(d, n) = (5, 1)$ e nesse caso $a \geq 0$.*

Considerando para o conjunto $V(S)$ as mesmas condições de $U(S)$ sobre a norma, temos que $V(S) = V_0(S)\dot{\cup}V_1(S)$, sendo $V_e(S) = V(S) \cap U_e(S) = \{\eta \in S,\ \eta > 1,\ \text{e}\ \mathcal{N}(\eta) = (-1)^e\}$, $e \in \{0, 1\}$. O próximo teorema caracteriza esses conjuntos:

**Teorema 4.1.43.** *As seguintes afirmações são verdadeiras*

**i.** *Se $d \equiv 2$, ou $3 mod 4$, então $V_e(S_{d,n}) = \{a + bn\sqrt{d} : a, b \in \mathbb{N} \setminus \{0\},\ a^2 - n^2db^2 = (-1)^e\}$, $e \in \{0, 1\}$;*

**ii.** *Se $d \equiv 1 mod 4$, então $V_e(S_{d,n}) = \{a+bn\delta : a \in \mathbb{N},\ e\ b \in \mathbb{N}\setminus\{0\},\ a^2+nab-n^2\dfrac{d-1}{4}b^2 = (-1)^e\}$, $e \in \{0, 1\}$.*

**Corolário 4.1.44.** *Sejam $\eta_1, \eta_2 \in V(S_{d,n})$, com:*

$$\eta_j = \begin{cases} a_j + b_j n\sqrt{d} & caso\ d \equiv 2, ou 3 mod 4; \\ \dfrac{a_j}{2} + \dfrac{b_j}{2} n\sqrt{d} & caso\ d \equiv 1 mod 4. \end{cases}$$

*o qual $a_j, b_j \in \mathbb{N} \setminus \{0\}$, $(j = 1, 2)$. Então $\eta_1 \leq \eta_2$, implica $b_1 \leq b_2$.*

**Observação 4.1.45.** *Esse corolário permite calcular o invertível fundamental $\epsilon$, bastando para isso calcular o menor inteiro $b \in \mathbb{N} \setminus \{0\}$, tal que $a^2 - n^2db^2 \in \{-q, q\}$, sendo $q = 1$ (respectivamente $q = 4$) se $d \equiv 2, 3$ (respectivamente $d \equiv 1$) $mod 4$. Ou seja, o menor inteiro $b$, de modo que um dos inteiros $\{n^2db^2 - q, n^2db^2 + q\}$ seja um quadrado em $\mathbb{N} \setminus \{0\}$. Com isso, o invetível fundamental é*

$$\epsilon_{d,n} = \begin{cases} \dfrac{a}{2} + \dfrac{b}{2} n\sqrt{d} & se\ d \equiv 1 mod 4; \\ a + bn\sqrt{d} & caso\ contrário. \end{cases}$$

*e sua norma será, respectivamente, $-1$ ou $1$.*

**Proposição 4.1.46.** *Com a notação acima, são verdadeiras as afirmações*

**i.** *Se o invertível fundamental $\epsilon$ de $S$ tiver norma $1$, então*
$V_0(S) = \{\epsilon^j : j \in \mathbb{N} \setminus \{0\}\} = V(S)$, $V_1(S) = \varnothing$,
$U_0(S) = \{\pm\epsilon^j : j \in \mathbb{Z}\} = U(S)$, $U_1(S) = \varnothing$.

**ii.** *Se o invertível fundamental $\epsilon$ de $S$ tiver norma $-1$, então*
$V_0(S) = \{\epsilon^{2j} : j \in \mathbb{N} \setminus \{0\}\}$, $V_1(S) = \{\epsilon^{2j+1} : j \in \mathbb{N}\}$,
$U_0(S) = \{\pm\epsilon^{2j} : j \in \mathbb{Z}\}$, $U_1(S) = \{\pm\epsilon^{2j+1} : j \in \mathbb{Z}\}$.

Podemos, com esses resultados, apresentar o conjunto solução da equação de Pell

$$X^2 - kY^2 = 1,$$

sendo $k$ um inteiro positivo, livre de quadrado em $\mathbb{Z}$. Observamos que $k = n^2d$, com $d$ livre de quadrados, e $n \in \mathbb{N} \setminus \{0\}$ únicos. Temos, então a seguinte proposição:

**Proposição 4.1.47.** *Seja $k = n^2d$, onde $d$ é um inteiro positivo livre de quadrados. Então $\mathbb{Z}[\sqrt{k}] = \mathbb{Z}[n\sqrt{d}] = S_{d,n}$ (respectivamente $S_{d,2n}$) se $d \equiv 2$, ou $3$ (respectivamente $1$) mod$4$.*

**Definição 4.1.48.** *Definimos em $\mathbb{Z} \times \mathbb{Z}$, a multiplicação $\cdot_k$ dada por*

$$(a, b) \cdot_k (a', b') = (aa' + bb'k, ab' + a'b),\ (a, b), (a', b') \in \mathbb{Z} \times \mathbb{Z}$$

.

**Lema 4.1.49.** *Munido da definição da multiplicação $\cdot_k$, o anel $\mathbb{Z} \times \mathbb{Z}$ torna-se um anel $\mathcal{R}$, isomorfo a $\mathbb{Z}[k] = S_{d,n}$, ou seja a aplicação*

$$\begin{aligned} \varphi : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}[n\sqrt{d}] \\ (a, b) &\mapsto a + bn\sqrt{d} \end{aligned}$$

*é um isomorfismo.*

**Definição 4.1.50.** *Definimos $\mathcal{U}_k$ (respectivamente $\mathcal{U}_{e,K}$), a imagem inversa de $U(\mathbb{Z}[\sqrt{k}])$ (respectivamente $U_e(\mathbb{Z}[\sqrt{k}])$), o qual $e \in \{0, 1\}$ pelo isomorfismo $\varphi$.*

*Temos, então os seguinte resultado:*

**Teorema 4.1.51.** *O conjunto solução da equação $X^2 - kY^2 = (-1)^e$ é $\mathcal{U}_{e,k}$, sendo $e \in \{0, 1\}$.*

O corolário abaixo mostra que as soluções inteiras da equação de Pell $X^2 - kY^2 = 1$ correspondem, biunivocamente, aos elementos invertíveis de $\mathbb{Z}[\sqrt{k}]$ de norma 1. Se consideramos $e_k = (v_k, w_k)$ a imagem inversa sobre o isomorfismo $\varphi$, acima, do invertível fundamental de $\mathbb{Z}[\sqrt{k}]$, então

**Corolário 4.1.52.** *Sob as mesmas notações acima, as afirmações abaixo são verdadeiras.*

**i.** *Se o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tem norma $-1$, então $\mathcal{U}_{0,k} = \{\pm e^{2j} : j \in \mathbb{Z}\}$ e $\mathcal{U}_{1,k} = \{\pm e^{2j+1} : j \in \mathbb{Z}\}$.*

**ii.** *Se o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tem norma $1$, então $\mathcal{U}_{0,k} = \mathcal{U}_k = \{\pm e^j : j \in \mathbb{Z}\}$ e $\mathcal{U}_{1,k} = \varnothing$. Isso ocorrerá, em particular, quando $\mathcal{N}(\epsilon_d) = 1$.*

## 4.2 O Grupo das Unidades Centrais em $RG$ com $G$ Finito

**Definição 4.2.1.** *Seja $K$ um sub-corpo de $\mathbb{C}$, o corpo dos números complexos, e $G$ um grupo finito. Dizemos que um $KG$-módulo $V$ é absolutamente irredutível se o módulo $K \bigotimes_{\mathbb{C}} V$ é um $\mathbb{C}G$-módulo irredutível. Definimos $K$ um corpo de decomposição de $G$ se todo $KG$-módulo for absolutamente irredutível.*

**Teorema 4.2.2.** *(Brauer) Seja $G$ um grupo finito de expoente $n$. A extensão $\mathbb{Q}(\sqrt[n]{1})$ é corpo de decomposição para o grupo $G$.*

**Definição 4.2.3.** *Seja $G$ um grupo de expoente $n$, e $A$ o grupo de Galois da extensão $\mathbb{Q}(\sqrt[n]{1})$ sobre o corpo $\mathbb{Q}$. Para $\sigma \in A$, podemos definir para $\chi_i \in \mathcal{I}rr(G)$, $1 \leq i \leq s$, a aplicação*

$$\begin{gathered}\chi_i^\sigma : G \longrightarrow \mathbb{C} \\ g \mapsto \sigma(\chi_i(g)), \chi_i^\sigma \in \mathcal{I}rr(G).\end{gathered}$$

*Nesse caso, dizemos que os caracteres $\chi_i$ e $\chi_i^\sigma$ são caracteres algebricamente conjugados.*

Seja $\chi_i$ um caractere irredutível do grupo finito $G$, definimos $\mathbb{Q}(\chi_i)$ como a extensão finita de $\mathbb{Q}$ gerada pelos elementos $\chi_i(g)$, para $g \in G$, que segundo lema 4.1.25 são inteiros algébricos.

**Teorema 4.2.4.** *Seja $Irr(G) = \{\chi_1 = 1_G, \chi_2, \cdots, \chi_p\}$ o conjunto dos caracteres irredutíveis, não conjugados, provindos da $\mathbb{C}$-representação de $G$, $\Psi_i$. Para cada $1 \leq i \leq p$, denotamos por $\mathbb{Q}(\chi_i)$ a menor extensão do corpo $\mathbb{Q}$, que contém a imagem do caractere $\chi$. Então o centro da álgebra de grupo $\mathbb{Q}G$ será*

$$\mathcal{Z}(\mathbb{Q}G) \cong \mathbb{Q}(\chi_1) \oplus \cdots \oplus \mathbb{Q}(\chi_p).$$

**Demonstração.** Consideremos a aplicação:

$$\begin{gathered}\psi : \mathcal{Z}(\mathbb{Q}G) \longrightarrow \mathbb{Q}(\chi_1) \oplus \cdots \oplus \mathbb{Q}(\chi_p) \text{ definida por:} \\ u = \sum_{i=1}^{s} \gamma_i \mathcal{K}_i = \sum_{i=1}^{s} \beta_i e_i \mapsto (\beta_1, \cdots, \beta_p).\end{gathered}$$

Pelo teorema 4.1.22, $\beta_i \in \mathbb{Q}(\chi_i)$, logo a aplicação $\psi$ está bem definida. Para todo $(\beta_1, \cdots, \beta_p) \in \bigoplus_{i=1}^{p} \mathbb{Q}(\chi_i)$, $\beta_i \in \mathbb{Q}(\chi_i) \Longrightarrow \beta_i = \sum_{g \in G} q_g \chi_i(g) \in \mathbb{Q}G$. Portanto $\psi$ é sobrejetora. Considerando-se que os $e_i$ são ortogonais, de modo que $(\alpha_1, \cdots, \alpha_s)(\beta_1, \cdots, \beta_s) = (\alpha_1\beta_1, \cdots, \alpha_s\beta_s)$, verificamos que $\psi$ é um epimorfismo. Calculando-se o núcleo de $\psi$, concluímos que $\psi$ é um isomorfismo. De fato, seja $u = \sum_{i=1}^{s} \gamma_i \mathcal{K}_i = \sum_{i=1}^{s} \beta_i e_i \in Ker(\psi)$, então $\beta_1 = \beta_2 = \cdots = \beta_p = 0$. Suponhamos, por contradição, que $\beta_k$ seja não nulo, para algum $p+1 \leq k \leq s$. Nesse caso, existe algum $\sigma \in A$, o grupo de Galois da extensão $\mathbb{Q}(\sqrt[n]{1})$ sobre o corpo $\mathbb{Q}$, tal que $\chi_k = \chi_i^\sigma$, para algum $1 \leq i \leq s$. Então da expressão 4.1.30, temos

$$\beta_k e_k = \sum_i \gamma_i \mathcal{K}_i = \sum_i \gamma_i |k_i| \sum_{j=1}^{s} \frac{\chi_j(g_i)}{\chi_j(1)} e_j. \text{ Logo}$$

$$\beta_k = \sum_i |k_i|\gamma_i \frac{\chi_k(g_i)}{\chi_k(1)} = \sum_i |k_i|\gamma_i \frac{\chi_i^{\sigma}(g_i)}{\chi_k(1)} = \sigma(\sum_i |k_i|\gamma_i \frac{\chi_i(g_i)}{\chi_i(1)}) = \sigma(\beta_i) = 0, \text{ pois } \chi_i(1) = \chi_k(1).$$

Contradição com a hipótese inicial. Portanto $Ker(\psi) = \{0\}$, logo $\psi$ é um isomorfismo. □

Pela proposição 4.1.31, para toda unidade central $u$ de $\mathbb{Z}G \subset \mathbb{C}G$, $u = \sum_{i=1}^{s} \gamma_i \mathcal{K}_i = \sum_{i=1}^{s} \beta_i e_i$.

**Proposição 4.2.5.** *Se $u$ é uma unidade central de $\mathbb{Z}G$, então $\epsilon(u) = \beta_1 = \sum_{i=1}^{s} \gamma_i |k_i|$.*

**Demonstração.** Pelo teorema anterior, $\mathcal{Z}(\mathbb{Q}G) \cong \mathbb{Q}(\chi_1) \oplus \cdots \oplus \mathbb{Q}(\chi_p)$. Consideremos a projeção

$$\psi : \mathcal{Z}(\mathbb{Q}G) \longrightarrow \mathbb{Q}(\chi_i),$$

a unidade $u \in \mathcal{Z}(\mathbb{Z}G) \subset \mathcal{Z}(\mathbb{Q}G)$, $u = \sum_{i=1}^{s} \gamma_i \mathcal{K}_i = \sum_{i=1}^{s} \beta_i e_i$. Considerando-se para essa última igualdade o teorema 4.1.22, temos que $\psi_i(u) = \beta_i$. Portanto $\psi_1 = \beta_1$. Sendo $\beta_1 = \sum_i |k_i|\gamma_i \frac{\chi_1(g_1)}{\chi_1(1)} = \sum_i |k_i|\gamma_i = \epsilon(\sum_i \gamma_i \mathcal{K}_i)$, que é o aumento de $u$. □

**Observação 4.2.6.** *Nas condições da proposição anterior, sendo $\mathbb{C}G = \bigoplus_{n}^{s} \mathbb{C}Ge_i$ se $u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$, $u = \sum_i \beta_i e_i \implies \beta_i \in \mathcal{U}(\mathbb{C}G)$. Ora, nesse caso, $\beta_i = \sum_i k_i\gamma_i$ $\mathbb{Z}$ é uma unidade em $\mathbb{Z}$, portanto $\beta_1 = \pm 1$.*

Seja $I_{\mathcal{Z}}$ o anel de inteiros de $\mathcal{Z}(\mathbb{Q}G)$, segundo a definição 4.1.34.

**Teorema 4.2.7.** *O grupo de unidades de $I_{\mathcal{Z}}$ é isomorfo ao produto direto do anel de inteiros dos grupos de unidades dos anéis $\mathbb{Q}(\chi_1), \cdots, \mathbb{Q}(\chi_p)$.*

**Teorema 4.2.8.** *(Ritter-Sehgal)([22], 6.1) Seja $G$ um grupo finito. O anel de grupo $\mathbb{Z}G$ tem um número finito de unidades centrais, se e somente se, o corpo $\mathbb{Q}(\chi)$, de cada caractere irredutível $\chi$ de $G$, é o corpo $\mathbb{Q}$ ou um corpo quadrático complexo.*

**Observação 4.2.9.** *Esse teorema é equivalente à seguinte condição: seja $G$ um grupo finito. Todas as unidades centrais de $\mathbb{Z}G$ são triviais, se e somente se, para cada $g \in G$, e cada natural $j$, relativamente primo com $|G|$, $g^j \sim g$ ou $g^j \sim g^{-1}$.*

Podemos prosseguir com a apresentação do exemplo proposto no final do capítulo III.

### 4.2.1 O Grupo das Unidades Centrais $\mathcal{U}(\mathbb{Z}A_5)$

Seja $G$ um grupo finito. O teorema 4.2.4 permite decompor o centro das unidades do anel $\mathbb{Q}G$, e, portanto, de $\mathbb{Z}G$ a partir da tábua de caracteres de $G$.

Para o grupo alternado $A_n$, temos os seguintes resultados:

(1) se $n < 3$, $A_n = 1$, portanto $\mathcal{U}(\mathbb{Z}A_n) =< \pm 1 >$.

(2) se $n = 3$ pelo teorema de Higman, $\mathcal{U}(\mathbb{Z}A_3) =< \pm 1 > \times A_3$.

(3) se $n = 4$, consideramos a tábua de caracteres desse grupo,

$$\mathcal{X} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \lambda & \lambda^2 \\ 1 & 1 & \lambda^2 & \lambda \\ 3 & -1 & 0 & 0 \end{pmatrix}, \quad \text{onde } \lambda = \tfrac{-1}{2} + \tfrac{\sqrt{-3}}{2}.$$

Seja $A$ o grupo de Galois do corpo $K$ de decomposição do grupo $A_4$. O automorfismo $\sigma : K \longrightarrow K$, definido por $\sigma(a + b\sqrt{-3}) = a - b\sqrt{-3}$, é, tal que $\sigma \in A$. Ocorre que $\lambda^2 = \dfrac{-1}{2} - \dfrac{\sqrt{-3}}{2}$, logo $\sigma(\lambda) = \lambda^2$ e, portanto, se identificarmos $\chi_i$ com a linha $i$ da tábua de caracteres de $\chi$, então $\chi_2$ e $\sigma(\chi_2) = \chi_3$ são algebricamente conjugados e os únicos caracteres com essa propriedade, pois os demais têm, pelo menos, um elemento racional não comum, que fixos pelos elementos de $A$ são distintos. Portanto o número de somandos diretos do teorema 4.2.4 é 3, logo

$$\mathcal{Z}(\mathbb{Q}A_4) = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\lambda).$$

Sendo $\mathbb{Q}(\lambda) = \mathbb{Q}\sqrt{-3}$, portanto, pelo teorema de Ritter-Sehgal, $\mathcal{Z}(\mathbb{Q}A_4)$ é trivial, ou seja, $\mathcal{Z}(\mathbb{Q}A_4) =< \pm 1 > \mathcal{Z}(A_4) =< \pm 1 >$.

Para o anel $\mathbb{Z}A_5$, inicialmente, prosseguimos como no caso anterior, analisando a tábua de caracteres do grupo $A_5$. Nesse caso, existe uma componente dessa tábua, que é uma raiz real e, portanto, existem unidades centrais não triviais. Prosseguimos então à determinação de $\mathcal{Z}(\mathbb{Q}A_5)$.

Abaixo, a tábua de caracteres do grupo alternado $A_5$

$$\mathcal{X} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 0 & w & -\frac{1}{w} \\ 3 & -1 & 0 & -\frac{1}{w} & w \\ 4 & 0 & 1 & -1 & -1 \\ 5 & 1 & -1 & 0 & 0 \end{pmatrix}, \quad \text{onde } w = \tfrac{1}{2} + \tfrac{\sqrt{5}}{2}.$$

O mesmo argumento dado à tabua do $A_4$ mostra que $\chi_2$ e $\chi_3$ são os únicos caracteres algebricamente conjugados. Portanto o número de somandos diretos é 4. Pelo teorema 4.2.4:

$$\mathcal{Z}(\mathbb{Q}A_5) = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(w),$$

sendo $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{5})$.

**Teorema 4.2.10.** *Seja $U = \mathcal{U}(\mathcal{Z}(\mathbb{Z}A_5))$ o grupo das unidades centrais de $\mathbb{Z}A_5$. Então $U$ é um grupo cíclico infinito.*

**Demonstração.** Pelo teorema 4.2.4 $\mathcal{Z}(\mathcal{U}(\mathbb{Z}A_5)) \subset \mathcal{Z}(\mathcal{U}(\mathbb{Q}A_5)) \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\sqrt{5})$. Na realidade $\mathcal{Z}(\mathbb{Z}G)$ e $I_{\mathcal{Z}}$ são $\mathbb{Z}$-ordens em $\mathcal{Z}(\mathbb{Q}G)$. Logo $[\mathcal{U}(I_{\mathcal{Z}}) : \mathcal{U}(\mathcal{Z}(\mathbb{Z}G))] < \infty$, pois $I_{\mathbb{Z}} \supseteq \mathcal{Z}(\mathbb{Z}G)$. Então $posto(\mathcal{Z}(\mathcal{U}(\mathbb{Z}A_5))) = posto(\mathcal{U}(\mathcal{Z}(\mathbb{Z}(\sqrt{5}))))$. Sendo $\mathbb{Z}(\sqrt{5})$ o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{5})$, uma extensão quadrática de $\mathbb{Q}$, portanto com exatamente 2 imersões reais, pelo Teorema das Unidades de Dirichlet, $posto(\mathbb{Z}(\sqrt{5})) = 2 - 1 = 1$, portanto, $U$ é um grupo cíclico infinito. □

Pela proposição 4.1.31, obtemos as seguintes matrizes:

$$T = \frac{1}{60}\begin{pmatrix} 1 & 9 & 9 & 16 & 25 \\ 1 & -3 & -3 & 0 & 5 \\ 1 & 0 & 0 & 4 & -5 \\ 1 & 3w & -\frac{3}{w} & -4 & 0 \\ 1 & -\frac{3}{w} & 3w & -4 & 0 \end{pmatrix} \quad \text{e } S = \begin{pmatrix} 1 & 15 & 20 & 12 & 12 \\ 1 & -5 & 0 & 4w & -\frac{4}{w} \\ 1 & -5 & 0 & -\frac{4}{w} & 4w \\ 1 & 0 & 5 & -3 & -3 \\ 1 & 3 & -4 & 0 & 0 \end{pmatrix}.$$

Assim, segundo a proposição 4.1.31, temos definidas relações entre os coeficientes de uma unidade central do anel. Uma expressa nas bases dos idempotentes ortogonais centrais primitivos, e outra nas somas formais das classes de conjugação. Essas relações, bem como propriedades sobre os coeficientes inteiros de uma unidade central, conduzem ao seguinte resultado:

**Lema 4.2.11.** *Seja $u$ uma unidade central normalizada de $\mathbb{Z}A_5$. Para $u = \sum_{i=1}^{5} \gamma_i \mathcal{K}_i = \sum_{i=1}^{5} \beta_i e_i$. As seguintes afirmações são verdadeiras:*

$$\beta_1 = 1; \tag{4.10}$$

$$\beta_4 = \beta_5 = 1; \tag{4.11}$$

$$x = \frac{\beta_2 + \beta_3}{2} = 1 + 10(\gamma_4 + \gamma_5); \tag{4.12}$$

$$y = \frac{\beta_2 - \beta_3}{4\sqrt{5}} = \gamma_4 - \gamma_5. \tag{4.13}$$

**Demonstração.** Pela proposição 4.2.5 $\beta_1 = \epsilon(u) = 1$. Para o grupo $A_5$, obtemos

$$k_1 = 1; k_2 = 15; k_3 = 20; k_4 = k_5 = 12,$$

então

$$\gamma_1 + 15\gamma_2 + 20\gamma_3 + 12\gamma_4 + 12\gamma_5 = 1.$$

pela proposição 4.1.31, expressões 4.3 e 4.4, temos conseqüentemente que

$$\begin{cases} \beta_1 = \gamma_1 + 15\gamma_2 + 20\gamma_3 + 12\gamma_4 + 12\gamma_5 = 1; \\ \beta_2 = \gamma_1 - 5\gamma_2 + 4w\gamma_4 - \frac{4}{w}\gamma_5; \\ \beta_3 = \gamma_1 - 5\gamma_2 - \frac{4}{w}\gamma_4 + 4w\gamma_5; \\ \beta_4 = \gamma_1 + 5\gamma_3 - 3\gamma_4 - 3\gamma_5; \\ \beta_5 = \gamma_1 + 3\gamma_3 - 4\gamma_4 \end{cases} \quad \text{e} \quad \begin{cases} \gamma_1 = (\beta_1 + 9\beta_2 + 9\beta_3 + 16\beta_4 + 25\beta_5)/60; \\ \gamma_2 = (\beta_1 - 3\beta_2 - 3\beta_3 + 5\beta_5)/60; \\ \gamma_3 = (\beta_1 + 4\beta_4 - 5\beta_5)/60; \\ \gamma_4 = (\beta_1 + 3w\beta_2 - \frac{3}{w}\beta_3 - 4\beta_4)/60; \\ \gamma_5 = (\beta_1 - \frac{3}{w}\beta_2 + 3w\beta_3 - 4\beta_4)/60 \end{cases}$$

Pela expressão acima, $\beta_4 + \beta_5$ são inteiros, pois são combinações lineares de $\gamma_i \in \mathbb{Z}$, com coeficientes inteiros. Ora, da observação 4.2.6 resulta que $\beta_4 = \pm 1$ e $\beta_5 = \pm 1$. Somando-se, convenientemente, os coeficientes $\gamma_i$, das equações acima, sendo $w - \frac{1}{w} = 1$ e $\beta_1 = 1$, obtemos:

$$\gamma_2 + \gamma_3 + \gamma_4 + \gamma_5 = \frac{4\beta_1 + 3(\beta_2 + \beta_3)(-1 + w - \frac{1}{w}) - 4\beta_4}{60} = \frac{1 - \beta_4}{15}. \tag{4.14}$$

Portanto, sendo essa expressão um número inteiro, concluímos que $\beta_4 = 1$. Analogamente, após determinarmos $\beta_4$, obtemos a expressão

$$\gamma_2 + \gamma_4 + \gamma_5 = \frac{\beta_5 - 1}{12}. \tag{4.15}$$

Portanto $\beta_5 = 1$. Com isso, restam $\beta_2$ e $\beta_3$ a serem determinados. De modo análogo, as demais igualdades são obtidas, resultando em

$$\gamma_4 + \gamma_5 = \frac{-2 + \beta_2 + \beta_3}{20}; \tag{4.16}$$

$$\gamma_4 - \gamma_5 = \frac{\beta_2 - \beta_3}{4\sqrt{5}} = y. \tag{4.17}$$

Daí verificamos que $x = \dfrac{\beta_2 + \beta_3}{2} = 1 + 10(\gamma_4 + \gamma_5)$. □

Podemos, ainda, determinar o produto $\beta_2\beta_3$ e demonstrar que o par $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, para $x$ e $y$ como acima, satisfaz a uma determinada expressão. Enunciamos essa afirmação com seguinte lema:

**Lema 4.2.12.** *O produto $\beta_2\beta_3 = 1$. Ademais, as expressões determinadas, para $x$ e $y$, resultam em números inteiros que satisfazem à seguinte equação de Pell*

$$X^2 - 20Y^2 = 1.$$

**Demonstração.** Consideremos $u^{-1} = \displaystyle\sum_{i=1}^{5} \frac{1}{\beta_i} e_i = \sum_{i=1}^{5} \delta_i \mathcal{K}_i$, sendo $\delta_i \in \mathbb{Z}$. A expressão de $u^{-1}$, na base dos idempotentes $e_i$, é $\displaystyle\sum_{i=1}^{5} \beta_i^{-1} e_i$. Do lema anterior, conhecemos $\beta_1 = \beta_4 = \beta_5 = 1$. Seja

$u^{-1} = \sum_{i=1}^{5} \delta_i \mathcal{K}_i$, com $\delta_i \in \mathbb{Z}$, então pela proposição 4.1.31, expressão 4.4, obtemos:

$$\begin{cases} \delta_1 = (14 + 3(\frac{1}{\beta_2} + \frac{1}{\beta_3}))/20; \\ \delta_2 = (2 - (\frac{1}{\beta_2} + \frac{1}{\beta_3}))/20; \\ \delta_3 = 0; \\ \delta_4 = (-1 + \frac{w}{\beta_2} - \frac{1}{w\beta_3})/20; \\ \delta_5 = (-1 - \frac{1}{w\beta_2} + \frac{w}{\beta_3})/20. \end{cases} \tag{4.18}$$

Utilizamos o mesmo procedimento anterior e calculamos

$$\delta_1 - 7\delta_2 = \frac{1}{2}(\frac{1}{\beta_2} + \frac{1}{\beta_3}) = \frac{x}{\beta_2\beta_3} = \delta,$$
$$\delta_4 - \delta_5 = \frac{y}{\beta_2\beta_3} = \Delta.$$

Daí, as seguintes relações:

$$x = \beta_2\beta_3\delta; \tag{4.19}$$
$$y = \beta_2\beta_3\Delta. \tag{4.20}$$

Logo $\beta_2\beta_3 = \frac{1}{4}((\beta_2+\beta_3)^2 - (\beta_2-\beta_3)^2) = (\frac{\beta_2+\beta_3}{2})^2 - 20(\frac{\beta_2-\beta_3}{4\sqrt{5}})^2 = x^2 - 20y^2$, onde $x$ e $y$ estão definidos no lema 4.2.11. Da expressão 4.19 e 4.20 obtemos: $\beta_2\beta_3 = (\beta_2\beta_3)^2(\delta^2 + \Delta^2)$. Portanto, sendo $\delta$ e $\Delta$ inteiros, então $\beta_2\beta_3$ é uma unidade em $\mathbb{Z}$. Calculando-se $\beta_2\beta_3 = x^2 + y^2 = (1 + 10(\gamma_4 + \gamma_5))^2 - 20(\gamma_4 - \gamma_5)^2$, obtemos $\beta_2\beta_3 = 1 + 20(\gamma_4 + \gamma_5 + 5(\gamma_4 + \gamma_5)^2 - (\gamma_4 - \gamma_5)^2) \equiv 1(mod 20)$. Portanto $\beta_2\beta_3 = 1$ implica que $(x, y)$ é solução da equação de *Pell* acima. □

**Teorema 4.2.13.** *O conjunto solução da equação de Pell*

$$x^2 - 20y^2 = 1 \text{ é}$$
$$\mathcal{U}_{0,5} = \{(\pm x_n, \pm y_n) : x_n + 2\sqrt{5}y_n = (9 + 4\sqrt{5})^n\}.$$

**Demonstração.** Pelo corolário 4.1.44, o invertível fundamental $(\epsilon_{5,2})$ é obtido a partir de $a^2 - 2^2.5.b^2 \in \{-4, 4\}$. O menor $b$, tal que ocorre $a^2 = \pm 4 + 4.5.b^2$, é $b = 1$. Logo $a^2 = 16$ e $a \in \mathbb{N}$, portanto $a = 4$. Pela observação 4.1.45, $\epsilon_{5,2} = 2 - \sqrt{5}$. Pelo corolário 4.1.52, o conjunto $\mathcal{U}_{0,5}$ é o conjunto solução da equação, cuja expressão $\epsilon_{5,2}^{2n} = (2 - \sqrt{5})^{2n} = (9 - 4\sqrt{5})^n$. □

**Teorema 4.2.14.** *São satisfeitas as seguintes relações para os coeficientes de u:*

$$\frac{\beta_2 + \beta_3}{2} = \frac{(9 + 4\sqrt{5})^{2n} + (9 - 4\sqrt{5})^{2n}}{2}; \tag{4.21}$$
$$\frac{\beta_2 - \beta_3}{4\sqrt{5}} = \pm\frac{(9 + 4\sqrt{5})^{2n} - (9 - 4\sqrt{5})^{2n}}{4\sqrt{5}}, \tag{4.22}$$

*onde n é um inteiro.*

**Demonstração.** Pelo teorema anterior, sabemos que se o par $(x, y)$ satisfaz a equação $x^2 - 20y^2 = 1$, então $x + 2\sqrt{5}y = (9 + 4\sqrt{5})^n$, para algum $n$ inteiro não negativo. Ora, para explicitar o valor de $x$, podemos expandir esse binômio e exprimi-lo na base $B = \{1, 2\sqrt{5}\}$. Isso pode ser calculado mais facilmente se considerarmos a expressão abaixo, a qual dessa expansão, resulta diretamente em $x$, o coeficiente do termo 1, da base $B$. Analogamente, encontramos $y$. Temos as seguintes igualdades:

$$x = \frac{\beta_2 + \beta_3}{2} = 1 + 10(\gamma_4 + \gamma_5) = \mu\frac{(9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n}{2};$$
$$y = \frac{\beta_2 - \beta_3}{4\sqrt{5}} = \gamma_4 - \gamma_5 = \pm\mu\frac{(9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n}{4\sqrt{5}}.$$

Nosso objetivo é provar que $\mu = 1$ e $n$ é um número par. Expandindo-se o binômio de $y$: $y = \frac{\pm 1}{4\sqrt{5}}\sum_{i=1}^{n}\binom{n}{i}(9^{n-i}(4\sqrt{5})^i - 9^{n-i}(-4\sqrt{5})^i) = \frac{\pm 1}{4\sqrt{5}}\sum_{i=1}^{n}\binom{n}{i}(1 - (-1)^i) =$
$\frac{\pm 2}{4\sqrt{5}}\sum_{i\leq n/2}\binom{n}{2i-1}9^{n-2i+1}(4\sqrt{5})^{2i-2}$, temos que:

$$y = \pm 2\sum_{1\leq i\leq (n+1)/2}\binom{n}{2i-1}9^{n-2i+1}80^{i-1},$$

portanto, $y = \gamma_4 - \gamma_5$ é par. Logo $\gamma_4 + \gamma_5 = m$ é par. Analogamente para $x = 1 + 10m = \frac{\mu}{2}\sum_{i=0}^{n}\binom{n}{i}9^{n-i}(4\sqrt{5})^i(1 + (-1)^i)$, obtemos:

$$x = 1 + 10m = \mu\sum_{0\leq n/2}\binom{n}{2i}9^{n-2i}80^i = \mu 9^n + 80\sum_{i\leq n/2}\binom{n}{2i}9^{n-2i}80^{i-1},$$

assim, $m = \frac{x-1}{10} = \frac{\mu 9^n - 1}{10} + 8\mu\sum_i\binom{n}{2i}9^{n-2i}80^{i-1}$ é par, se e somente se, $\frac{\mu 9^n - 1}{10}$ é par. Calculando-se essa parcela, que é um inteiro par,

$$\frac{\mu 9^n - 1}{10} = \frac{\mu(10-1)^n - 1}{10} = \frac{-1 + \mu(-1)^n + 10\mu n(-1)^{n-1} + 100\mu\sum_{i\leq n}\binom{n}{i}10^{n-i-2}(-1)^i}{10},$$

então devem ser verificadadas as condições abaixo:

$$\begin{cases} (-1 + \mu(-1)^n) \equiv mod 10; \quad (a) \\ \dfrac{-1 + \mu(-1)^n - 10\mu n(-1)^n}{10} \text{ é par .} \quad (b) \end{cases} \tag{4.23}$$

Da condição 4.23(a), temos que $\mu(-1)^n - 1 = 0$ cuja solução é $n$ um número par e $\mu = 1$ ou $n$ um número ímpar e $\mu = -1$. A condição 4.23(b) implica que $n$ é par e $\mu = 1$. □

**Corolário 4.2.15.** *Nas condiçoes do lema anterior*

$$\begin{cases} \beta_2 = (9 + 4\sqrt{5})^{2n} \\ \beta_3 = (9 - 4\sqrt{5})^{2n} \ ou \end{cases} \quad \begin{cases} \beta_2 = (9 - 4\sqrt{5})^{2n} \\ \beta_3 = (9 + 4\sqrt{5})^{2n}. \end{cases}$$

**Teorema 4.2.16.** *Os geradores do grupo das unidades centrais de $\mathbb{Z}A_5$ são:*

$$\begin{aligned} u &= 49\mathcal{K}_1 - 16\mathcal{K}_2 + 26\mathcal{K}_4 - 10\mathcal{K}_5 && (4.24)\\ &= e_1 + (161 + 72\sqrt{5})e_2 + (161 - 72\sqrt{5})e_3 + e_4 + e_5; && (4.25)\\ u^{-1} &= 49\mathcal{K}_1 - 16\mathcal{K}_2 - 10\mathcal{K}_4 + 26\mathcal{K}_5 && (4.26)\\ &= e_1 + (161 - 72\sqrt{5})e_2 + (161 + 72\sqrt{5})e_3 + e_4 + e_5. && (4.27) \end{aligned}$$

*Portanto,*

$$U =< \epsilon >< u^{\epsilon} > \text{, } com\ \epsilon = \pm 1.$$

**Demonstração.** Do corolário anterior, $\beta_2 = (9 + 4\sqrt{5})^{2n}$ e $\beta_3 = (9 - 4\sqrt{5})^{2n}$. Tomemos n=1, então $\beta_2 = 161 + 72\sqrt{5}, \beta_3 = 161 - 72\sqrt{5}$. Portanto, podemos calcular os coeficientes de $u = \sum \gamma_i \mathcal{K}_i$. Retomando as equações 4.16,4.17, obtemos $\mathcal{K}_4 = -10$ e $\mathcal{K}_5 = 26$, pelas expressões 4.15 e 4.14 os coeficientes $\mathcal{K}_3 = 0$ e $\mathcal{K}_2 = -16$ respectivamente. Assim obtemos $\mathcal{K}_1 = 49$. Desse modo,

$$u = e_1 + (161 + 72\sqrt{72})e_2 + (161 - 72\sqrt{72})e_3 + e_4 + e_5 = 49\mathcal{K}_1 - 16\mathcal{K}_2 + 26\mathcal{K}_4 - 10\mathcal{K}_5.$$

Pela expressão 4.18, de posse dos coeficientes $\beta_i$, obtemos os coeficientes $\delta_i$, $1 \leq i \leq 5$. Pelo lema 4.2.11, obtemos os coeficientes de $\mathcal{K}_i$ para $u^{-1}$. □

Em [11], Li obtém esse mesmo resultado, porém de outro modo. Nesse artigo Li utiliza as propriedades da $\mathbb{Z}$-base definida pelas somas das classes de conjugação do grupo $A_5$. De modo que, sendo possível determinar a tábua de multiplicação da $\mathbb{Z}$-base considerada, em seu trabalho, Li representa os elementos do centro de $\mathcal{U}(\mathbb{Z}A_5)$ nessa base. Ocorre que Li não considera em seu cálculos, a inclusão de $\mathcal{Z}(\mathcal{U}(\mathbb{Z}A_5)) \hookrightarrow \mathcal{Z}(\mathcal{U}(\mathbb{Q}A_5))$, bem como a tábua de caracteres do grupo $A_5$. Consideramos, no entanto, a teoria desenvolvida por Aleev, porque esta, inicialmente, demonstra que $\mathcal{Z}(\mathcal{U}(\mathbb{Z}A_5))$ é finitamente gerado de posto 1, e a partir daí inicia a determinação do gerador desse grupo.

# Referências Bibliográficas


[1] R. Ž. Aleev, *Higman's Central Unit Theory, Units of Integral Group Rings of Finite Cyclic Groups and Fibonacci Numbers*, International Journal of Algebra and Computation vol. 4(3)(1994) 309-358, World, Singapura.

[2] A. A. Bovdi, Z. Marcianik, S. K. Sehgal, *Torsion Units in Infinite Group Rings*, Journal of Number Theory 47(1994), 284-299.

[3] C. W. Curtis, I. Reiner, *Methods of Representation Theory*,vol 1, Wiley & Sons, New York, 1981.

[4] O. Endler, *Números Algébricos*, sexta edição, IMPA, Rio de Janeiro,

[5] I. M. Isaacs, *Character Theory of Finite Groups*, Mathematics 69, Academic Press, New York, 1976.

[6] N. Jacobson, *Basic Algebra*, vol. 1, second edition, W. H. Freeman and Company, New York, 1985.

[7] E. Jespers, O. S. Juriaans, *Isomorphisms of Integral Group Rings of Infinite Groups*, Journal of Algebra, vol. 1(223)(2000) 171-189.

[8] E. Jespers, O. S. Juriaans, J. R. Rogério, J. M. de Miranda, *On the Normalizer Conjecture*, to appear.

[9] E. Jespers, M. M. Parmenter. S. K. Sehgal, *Central Units of Integral Group Rings of Nilpotent Groups*, Proc. Amer. Math. Soc. 124(april, 1996) 1007-1012, USA.

[10] O. S. Juriaans, *Trace Properties of Torsion Units in Group Rings II*, RT-MAT96-07, IME-USP.

[11] Y. Li, M. M. Parmenter, *Central Units of the Group Ring* $\mathbb{Z}A_5$, Proc. Amer. Math. Soc. 125(january 1997), 61,65, USA.

[12] Z. S. Marciniak, K. W. Roggenkamp, *The Normalizer of a Finite Group in its Integral Group Ring and Čech Cohomology*, to appear.

[13] W. May, *Isomorphism of Group Algebra*, Journal of Algebra vol. 1(40)(1976) 10-18.

[14] M. Mazur, *On the Isomorphism Problem for Infinite Group Rings*, Expositiones Mathematicae 13(1995), 433-445, Spektrum, Heidelberg 1995.

[15] D. Passman, *Group Rings, Crossed Products and Galois Theory*, AMS $n^o$ 64, Expository Lectures, 1985.

[16] D. Passman, *The Algebraic Structure of Group Rings*, Wiley & Sons, New York, 1977.

[17] F. C. Polcino Milies, S. K. Sehgal, *Central Units of Integral Group Rings*, preprint.

[18] J. Ritter, S. K. Sehgal, *Integral Group Rings with Trivial Central Units*, Proc. Amer. Math. Soc. 108(1990),327-329.

[19] Robinson, J. S. Derek, *A course in the theory of groups*,second edition, Springer Verlag, 1995.

[20] K. W. Roggenkamp, A. Zimmermann, *Outer Group Automorphims May Become Inner in the Integral Group Ring*, J. Pure and Applied Mathmatics Algebra, 103(1995), 91-99.

[21] S. K. Sehgal, *Topics in Group Rings*, Marcel Dekker, New York and Basel, 1978.

[22] S. K. Sehgal, *Units in Integral Group Rings*, Longman, Harlon, 1994.