Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

O Problema de Isomorfismos em Anéis de Grupos sobre os Inteiros

por

Dércio Braga Santos

sob orientação do

Prof. Dr. Orlando Stanley Juriaans

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Dezembro/2003

João Pessoa - Pb

O Problema de Isomorfismos em Anéis de Grupos sobre os Inteiros

por

Dércio Braga Santos

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

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

Prof. Dr. Antônio de Andrade e Silva - UFPB (Co-Orientador)

Prof. Dr. Hélio Pires de Almeida - UFPB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Dezembro/2003

Agradecimentos

- A Deus, por todo o apoio espiritual e pela forte presença em minha vida.

- Aos Professores *Dr. Antônio de Andrade e Silva* e *Dr. Orlando Stanley Juriaans*, que compreendem o verdadeiro sentido da palavra *orientação*.

- Ao amigo Andrade, pela paciência, dedicação, compreensão e amizade.

- Aos Professores Hélio Pires de Almeida e João Bosco Nogueira pelas gratas contribuições nesta dissertação.

- Aos professores do programa de mestrado, em especial ao Professores Antônio de Andrade e Silva, Orlando Stanley Juriaans, Hélio Pires de Almeida que muito contribuiram para a minha formação.

- Aos meus pais, Isaias e Onília e irmãos, Marcelo e Maria Felícia, que não mediram esforços para que este grande sonho se tornasse realidade.

- À minha esposa Fernanda e a Juliana, pelo carinho e companheirismo em todos os momentos.

- Ao meu sogro Manoel e minha sogra Terezinha, pelo apoio e incentivos.

- Aos colegas do curso de mestrado, em especial aos amigos Aroldo, Joelma e João.

- À Sônia, pela competência e presteza no atendimento na secretaria.

- Aos meus professores da graduação do Departamento de Matemática - UFMT - Campus de Rondonópolis.

- Aos amigos de sempre: Isaias, Onília, Marcelo, Maria Felícia e Edézio pelo carinho e incentivo.

- À CAPES, ao meu pai, ao meu irmão e ao meu primo (Edézio), pelo suporte financeiro para a realização do curso de mestrado.

Dedicatória

Aos meus pais Isaias e Onília
Aos meus irmãos Marcelo e Maria Felícia
À minha esposa Fernanda e aos demais de minha família, em especial àqueles que estiveram presentes nos momentos mais marcantes de minha trajetória.

Resumo

Respondemos à questão de Mazur, dando assim condições para que o problema do isomorfismo seja válido para anéis de grupos sobre os inteiros de grupos da forma $G = N \times A$, onde N é finito e A é um abeliano livre finitamente gerado. Mostramos também que o problema do isomorfismo para grupos infinitos é bastante relacionado com a conjectura do normalizador. Além disso, mostramos que a conjectura do automorfismo vale para grupos abelianos infinitos finitamente gerados se, e somente se, $\mathbb{Z}G$ tem somente unidades triviais. Respondemos parcialmente o problema de Sehgal, isto é, mostramos que a classe de um grupo nilpotente finitamente gerado G é determinado por seu anel de grupo sobre os inteiros, contanto que G tenha somente torção ímpar. Quando G tem classe de nilpotência 2, não é necessária a restrição de ser finitamente gerado. Assim, junto com um resultado de Ritter e Sehgal solucionamos o problema do isomorfismo para grupos nilpotente finitamente gerado de classe 2. Além disso, ressaltamos uma ligação entre este problema e o do subgrupo de dimensão.

Abstract

We answer a question of Mazur by giving conditions for the isomorphism problem to be true for integral group rings of groups that are a direct product of a finite group and a finitely generated free abelian group. It is also shown that the isomorphism problem for infinite groups is strongly related to the normalizer conjecture. We show that the automorphism conjecture holds for infinite finitely generated abelian groups G if and only if $\mathbb{Z}G$ has only trivial units. We partially answer a problem of Sehgal: We show that the class of a finitely generated nilpotent group G is determined by its integral group ring provided G has only odd torsion. When G has nilpotency class two then the finitely generated restriction is not needed. This, together with a result of Ritter and Sehgal, settles the isomorphism problem for finitely generated nilpotency class two groups. A link is pointed out between this problem and the dimension subgroup problem.

Notação

G - Grupo

aH - Classe lateral à esqueda de H em G

$\frac{G}{H}$ - Grupo quociente de G por H

$\langle g \rangle$ - Subgrupo cíclico de G gerado por g

$\mathbb{N}$ - Conjunto dos números naturais

$\mathbb{Z}$ - Conjunto dos números inteiros

$\equiv$ - Congruente

RG - Anel de grupo sobre o anel R.

$\text{supp}\,(\lambda)$ - Suporte de λ

$\epsilon\,(\lambda)$ - Função aumento

$\Delta_R\,(G)$ ou $\Delta\,(G)$ - Ideal de aumento de RG

$\Delta_R\,(G,N)$ ou $\Delta\,(G,N)$ - Núcleo da aplicação $RG \longrightarrow R\left(\frac{G}{N}\right)$

$\mathcal{U}\,(R)$ - Grupos das unidades de R

$\mathcal{U}_1\,(\mathbb{Z}G)$ - Grupo das unidades de aumento 1

$\mathcal{N}_G\,(H)$ - Normalizador de H de G

$[x,y]$ - Comutador de x e y

$(x,y) = xy - yx$ - Produto de Lie de x e y

(R,R) - Grupo aditivo gerado por todos os produtos de Lie

$D_n\,(G)$ - n-ésimo subgrupo de dimensão de G

$\text{Aut}\,(G)$ - Grupo de Automorfismos de G

$\sim$ - relação de conjugação num grupo

$[G:A]$ - Índice de um subgrupo aditivo A em G

$\simeq$ - Isomorfo

$\forall$ - Para todo

$\sum$ - Soma

$\mathcal{Z}(G)$ - Centro do grupo G

$\gamma(G)$ - Índice de nilpotência do grupo G

$\gamma_n(G)$ - n-ésimo termo da série central inferior

$\gamma_2(G) = G'$ - Grupo dos comutadores de G

$\mathcal{Z}_n(G)$ - n-ésimo termo da série central superior

$\mathcal{Z}_1(G)$ - Centro do grupo G

Sumário

Introdução

A presente dissertação é baseada no artigo "Isomorphisms of Integral Group Rings of Infinite Groups."

O *Problema de Isomorfismo* foi formulado explicitamente por R. M. Thrall que, na Conferência de Álgebra de Michigan de 1947, o apresentou da seguinte forma: Dados um grupo G e um corpo K, determinar todos o grupos H, tais que

$$KG \simeq KH.$$

A primeira resposta parcial foi dada por S. Perlis e G. Walker em 1950, que colocaram o problema nos seguintes termos: Dados dois grupos G e H de mesma ordem n, determinar todos os corpos K para os quais

$$KG \simeq KH.$$

Nesse trabalho eles responderam completamente a questão em que G e H são grupos abelianos e a característica de K não divide n.

Mazur aborda o problema do isomorfismo da seguinte maneira: A existência de um isomorfismo de uma "R-álgebra" do anel de grupo RG e RH implica na existência de um isomorfismo dos grupos G e H? Sehgal atenta para o seguinte problema: Se G é um grupo nilpotente infinito, então

$$\mathbb{Z}G \simeq \mathbb{Z}H \Longrightarrow G \simeq H? \tag{1}$$

Embora recentemente Hertweck (veja [6]) tenha dado um contra-exemplo para o problema do isomorfismo para anéis de grupos sobre os inteiros de grupos finitos, ainda resta o desafio de determinar quais grupos satisfazem à conjectura. Uma solução positiva para esta conjectura foi dada por Roggenkamp e Scott para grupos nilpotentes finitos e por Whitcomb para grupos metabelianos finitos. Para os grupos infinitos pouco se sabe. Não se sabe nem mesmo se a classe de nilpotência do grupo é preservada para anéis de

grupos sobre os inteiros de grupos nilpotentes infinitos. Existe atualmente uma resposta satisfatória para a conjectura somente para uma classe especial de grupos policíclicos-por-finito, a saber, para grupos da forma $N \times A$, um produto direto de um grupo finito N com um grupo cíclico infinito A. Mazur prova que, se H é outro grupo tal que $\mathbb{Z}(N \times A) \simeq \mathbb{Z}H$, então $H = N \rtimes A$, um produto semidireto, onde a ação de $\mathbb{Z}$ sobre o grupo finito N é induzida por uma unidade de $\mathbb{Z}N$. Assim, a conjectura do isomorfismo vale para $N \times A$ se, e somente se, ambas as conjecturas do isomorfismo e do normalizador valem para N.

Mazur questionou se este resultado podesse ser estendido para o produto direto de um grupo finito N com um grupo A abeliano livre finitamente gerado.

Após alguns trabalhos preliminares nos capítulos 1 e 2, sobre resultados clássicos da teoria de grupos, anéis de grupos e sobre unidades centrais de alguns anéis de grupos sobre os inteiros, respondemos no capítulo 3 a questão de Mazur. A técnica usada nas provas permite que se construam grupos não isomorfos a $N \times A$ e que se obtenha, assim, um contra-exemplo infinito para o problema do isomorfismo.

No capítulo 3 damos condições necessárias e suficientes para que a conjectura do automorfismo seja válida para $\mathbb{Z}(N \times A)$. Segue que esta conjectura é válida para anéis de grupos sobre os inteiros de um grupo G abeliano finitamente gerado se, e somente se, G é finito ou as unidades de $\mathbb{Z}G$ são triviais.

O restante do capítulo 3 refere-se ao problema de Sehgal (cf. equação 1). Primeiro provamos que o problema de isomorfismo vale para grupos nilpotentes finitamente gerados de classe 2. Note que Ritter e Sehgal provaram o seguinte resultado: Se G e H são ambos nilpotentes finitamente gerados de classe 2, tais que $\mathbb{Z}G \simeq \mathbb{Z}H$, então $G \simeq H$. A seguir, mostramos que a classe de nilpotência de um grupo G nilpotente, finitamente gerado, é determinada por seu anel de grupo sobre os inteiros contanto, que G tenha somente torção ímpar. Além disso, ressaltamos uma ligação entre este problema e o do subgrupo de dimensão.

Capítulo 1

Resultados Básicos

Apresentaremos aqui alguns resultados básicos da teoria dos grupos, que serão necessários para que haja uma melhor compreensão dos capítulos seguintes.

1.1 Grupos

Os resultados clássicos da teoria dos grupos inseridos nesta seção serão úteis para que se possa compreender o desenvolvimento deste trabalho. Lançaremo-los aqui sugerindo ao leitor interessado em mais detalhes que consulte [2].

Um conjunto não vazio G equipado com uma operação binária

$$\begin{aligned} * : \quad & G \times G \longrightarrow G \\ & (a, b) \longmapsto a * b \end{aligned}$$

é um *grupo* se as seguintes condições são satisfeitas:

1. $a * (b * c) = (a * b) * c$, para todo a, b, $c \in G$.

2. Existe $1 \in G$ tal que $1 * a = a * 1 = a$, para todo $a \in G$.

3. Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = 1$.

O grupo é *abeliano* ou *comutativo* se também vale a condição

4. $a * b = b * a$, para todo a, $b \in G$.

Com o objetivo de simplificar a notação usaremos ab em vez $a * b$. A *ordem* ou *cardinalidade* de um grupo G é o número de elementos de G que denotaremos por $|G|$.

Sejam G um grupo e H um subconjunto de G. Dizemos que H é um *subgrupo* de G, em símbolos $H \leq G$, se as seguintes condições são satisfeitas:

1. $H \neq \emptyset$;

2. $ab^{-1} \in H$, para todo a, $b \in H$.

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, o conjunto

$$aH = \{ah : \forall h \in H\}$$

é chamado a *classe lateral à esquerda* de H em G determinada por a. De modo semelhante, podemos definir a classe lateral à direita Ha de H em G. O conjunto de todas as classes laterais à esquerda de H em G forma uma partição de G, que denotamos por $\frac{G}{H}$.

Dados a, $b \in G$, dizemos que a é *congruente* a b *módulo* H se $a^{-1}b \in H$, que denotamos por $a \equiv b \pmod{H}$. É fácil verificar que $\equiv$ é uma relação de equivalência em G e que a classe de equivalência determinada por a é igual à classe lateral à esquerda aH. O elemento a é chamado um *representante* da classe de equivalência. É também fácil verificar que existe uma correspondência biunívoca entre o conjunto das classes laterais à esquerda de H em G e o conjunto das classes laterais à direita de H em G. A cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de H em G é chamado o *índice* de H em G, que denotaremos por $[G : H]$.

Sejam G um grupo e H um subgrupo de G. Dizemos que H é um *subgrupo normal* de G, em símbolos $H \trianglelefteq G$, se

$$Ha = aH, \forall a \in G,$$

isto é,

$$aHa^{-1} = H, \forall a \in G.$$

Sejam G um grupo e H um subgrupo de G. Então $\frac{G}{H}$ é um grupo com a operação $aHbH = abH$, para $a, b \in G$ se, e somente se, H é um subgrupo normal de G. Neste caso, $\frac{G}{H}$ é chamado o *grupo quociente* de G por H.

Seja G um grupo. G é dito *residualmente finito* se para todo $g \in G$ existir um subgrupo normal H_g, tal que $g \notin H_g$ e $[G : H_g]$ é finito.

Sejam G e H grupos. O produto cartesiano $G \times H$ equipado com a operação binária componente a componente

$$(a, b) * (g, h) = (ag, bh)$$

é um grupo com elemento neutro $(1,1)$ e (g^{-1},h^{-1}) o inverso de (g,h). O grupo $G\times H$ é chamado *produto direto* (*externo*). De modo indutivo, segue-se que

$$G_1\times\cdots\times G_n$$

é um grupo. Em particular,

$$G^n=\underbrace{G\times\cdots\times G}_{n-\text{vezes}}$$

é um grupo.

Teorema 1.1 (Lagrange) *Sejam G um grupo finito e H um subgrupo de G. Então $|H|$ divide $|G|$.* ■

Sejam X um subconjunto não vazio de G e

$$\mathcal{F}=\{H : H\leq G \text{ e } X\subseteq H\}.$$

Então

$$\langle X\rangle=\bigcap_{H\in\mathcal{F}} H$$

é o menor subgrupo de G contendo X e chamado o *subgrupo gerado* por X. Se X é um conjunto finito, digamos

$$X=\{x_1,\ldots,x_n\},$$

denotaremos $\langle X\rangle$ por

$$\langle X\rangle=\langle x_1,\ldots,x_n\rangle.$$

Proposição 1.1 *Sejam G um grupo e X um subconjunto não vazio de G. Então*

$$\langle X\rangle=\left\{x_1^{\varepsilon_1}\cdots x_k^{\varepsilon_k} : x_i\in X,\varepsilon_i=\pm 1,k\in\mathbb{N}\right\}.$$

■

Dizemos que G é *finitamente gerado* se existir um subconjunto finito X de G tal que $G=\langle X\rangle$. Em particular, se $X=\{a\}$, então

$$G=\langle a\rangle=\{a^n : n\in\mathbb{Z}\}$$

é chamado o *grupo cíclico* gerado por a.

Sejam G um grupo e H um subgrupo de G. Os conjuntos

$$\mathcal{N}_G(H) = \{g \in G : g^{-1}Hg = H\}$$

e

$$\mathcal{C}_G(H) = \{g \in G : gh = hg, \forall h \in H\}$$

chamados *normalizador* e *centralizador* de H em G, respectivamente, são subgrupos de G. Dizemos que um subgrupo K normaliza H se $K \leq \mathcal{N}_G(H)$. O conjunto

$$\mathcal{Z}(G) = \{g \in G : gx = xg, \forall x \in G\}$$

é chamado o *centro* de G e é um subgrupo normal de G.

Proposição 1.2 *Sejam G um grupo e H um subgrupo de G. Então*:

1. *$\mathcal{N}_G(H)$ é um subgrupo de G que contém H;*
2. *H é um subgrupo normal de $\mathcal{N}_G(H)$;*
3. *Se K é um subgrupo de G tal que H é normal em K, então $K \subseteq \mathcal{N}_G(H)$, isto é, $\mathcal{N}_G(H)$ é o maior subgrupo de G no qual H é normal;*
4. *H é um subgrupo normal G se, e somente se, $\mathcal{N}_G(H) = G$.* ■

Observação 1.1 *Seja $G = N \times H$. Então*

$$\mathcal{Z}(G) = \mathcal{Z}(N) \times \mathcal{Z}(H).$$

Sejam G e H conjuntos não vazios equipados com as operções binárias $*$ e $\circ$, respectivamente. Uma função φ de G em H é um *morfismo* se

$$\varphi(a * b) = \varphi(a) \circ \varphi(b), \forall a, b \in G.$$

Em particular, se G e H são grupos, dizemos que φ é *homomorfismo de grupos*. Neste caso, a *imagem* de φ, $\operatorname{Im}\varphi$, é um subgrupo de H. O *núcleo* de φ é o conjunto $\ker\varphi = \{g \in G : \varphi(g) = 1\}$ que é um subgrupo normal de G.

Um homomorfismo de grupos $\varphi : G \longrightarrow H$ é um *isomorfismo* se φ é bijetora. Quando existir um isomorfismo entre G e H dizemos que G e H são *isomorfos* e denotamos isto

por $G \simeq H$. Um *endomorfismo* de um grupo G é um homomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\mathrm{End}\,(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um homomorfismo}\}.$$

Um *automorfismo* de um grupo G é um isomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\mathrm{Aut}\,(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um isomorfismo}\}.$$

É fácil verificar que $\mathrm{End}\,(G)$ e $\mathrm{Aut}\,(G)$ são grupos com a operação composição.

Seja $a \in G$. A função

$$\begin{array}{rccc} \sigma_a : & G & \longrightarrow & G \\ & x & \longmapsto & axa^{-1} \end{array}$$

é um automorfismo de G chamado de *automorfismo interno* de G induzido por a. Denotamos por

$$\mathrm{Inn}(G) = \{\sigma_a \in \mathrm{Aut}\,(G) : a \in G\}.$$

Um subgrupo H de um grupo G é *característico* se

$$\varphi(H) \subseteq H, \forall \varphi \in \mathrm{Aut}\,(G)\,.$$

Em particular, todo subgrupo característico é normal.

Teorema 1.2 (1º Teorema de Isomorfismo) *Seja $\varphi : G \longrightarrow H$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker \varphi} \simeq \mathrm{Im}\,\varphi.$$

■

Teorema 1.3 (N/C Lema) *Sejam G um grupo e H um subgrupo de G. Então*:

1. *$\mathcal{C}_G(H)$ é um subgrupo normal de $\mathcal{N}_G(H)$ e $\frac{\mathcal{N}_G(H)}{\mathcal{C}_G(H)}$ é isomorfo a um subgrupo de* $\mathrm{Aut}\,(H)$;

2. *$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}\,(G)$ e $\frac{G}{\mathcal{Z}(G)} \simeq \mathrm{Inn}(G)$.* ■

Teorema 1.4 (2º Teorema de Isomorfismo) *Sejam H e K subgrupos de um grupo G e $K \trianglelefteq G$. Então*

$$\frac{H}{H \cap K} \simeq \frac{HK}{K}.$$

■

Teorema 1.5 (3º Teorema de Isomorfismo) *Sejam H e K subgrupos normais de um grupo G e $K \subset H$. Então*

$$\frac{G}{K}\Big/\frac{H}{K} \simeq \frac{G}{H}.$$

■

Lema 1.1 (Lema de Zassenhaus) *Sejam G um grupo, H, K subgrupos de G e M, N subgrupos normais de H e K, respectivamente. Então*

$$M\left(H \cap N\right) \trianglelefteq M\left(H \cap K\right) \;\; e \;\; N\left(M \cap K\right) \trianglelefteq N\left(H \cap K\right)$$

Além disso,

$$\frac{M\left(H \cap K\right)}{M\left(H \cap N\right)} \simeq \frac{N\left(H \cap K\right)}{N\left(K \cap M\right)}.$$

■

1.2 Ações de Grupo

Sejam G um grupo e Ω um conjunto não vazio. Dizemos que G *age* sobre Ω se existir uma aplicação

$$* : G \times \Omega \longrightarrow \Omega,$$

com $*(a, x) = ax$, tal que as seguintes condições são satisfeitas:

1. $a(bx) = (ab)x$, para todo $a, b \in G$, $x \in \Omega$;

2. $1x = x$, para todo $x \in \Omega$.

A aplicação $*$ é chamado a *ação* de G sobre Ω e Ω é chamado um *G-conjunto*. Se $|\Omega| = n$, então n é chamado o *grau* do G-conjunto Ω.

Exemplo 1.1 *Sejam $G = S_n$ e $\Omega = \{1, 2, \ldots, n\}$. Então Ω é um G-conjunto sob a ação*

$$*(\sigma, i) = \sigma(i), \sigma \in S_n, i \in \Omega.$$

Observação 1.2 *Existe uma correspodência biunívoca entre o conjunto de ações de G em Ω e o conjunto de homomorfismos de G em S_Ω. De fato, seja Ω um G-conjunto. Então*

para cada $a \in G$ fixado, a aplicação $\varphi_a(x) = ax$ é uma permutação de Ω, pois

$$\begin{aligned} \varphi_{a^{-1}} \circ \varphi_a(x) &= \varphi_{a^{-1}}(\varphi_a(x)) \\ &= \varphi_{a^{-1}}(ax) \\ &= \left(a^{-1}a\right) x \\ &= 1.x = x \end{aligned}$$

Logo, $\varphi_{a^{-1}} \circ \varphi_a = id$. De modo análogo, mostra-se que $\varphi_a \circ \varphi_{a^{-1}} = id$. Assim, a aplicação

$$\varphi : G \longrightarrow S_\Omega$$

dada por $\varphi(a) = \varphi_a$ é um homomorfismo, pois

$$\varphi_{ab}(x) = (ab)x = a(bx) = \varphi_a(bx) = \varphi_a(\varphi_b(x)) = \varphi_a \circ \varphi_b(x), \forall x \in \Omega.$$

Reciprocamente, suponhamos que $\varphi : G \longrightarrow S_\Omega$ é um homomorfismo. Então é fácil verificar que a aplicação

$$* : G \times \Omega \longrightarrow \Omega,$$

definida por $*(a, x) = \varphi(a)x$ é uma ação de G sobre Ω. Neste caso, dizemos que φ é uma representação por permutação *de G em S_Ω.*

Seja Ω um G-conjunto. Então

$$G_0 = \{a \in G : ax = x, \forall x \in \Omega\}$$

é um subgrupo normal de G. Dizemos que uma ação de G em Ω é *fiel* ou G *age efetivamente* sobre Ω se $\varphi : G \longrightarrow S_\Omega$ é um homomorfismo injetor ou, equivalentemente,

$$\ker \varphi = G_0 = \{1\} \Leftrightarrow ax = x, \forall x \in \Omega \Rightarrow a = 1.$$

1.3 Produtos Semidiretos

Sejam G um grupo e H, N subgrupos de G. Dizemos que G é o *produto semidireto* (*interno*) de N por H se as seguintes condições são satisfeitas:

1. $G = NH$;

2. $N \trianglelefteq G$;

3. $N \cap H = \{1\}$.

Notação: $G = N \rtimes H$.

Exemplo 1.2 *Sejam $G = S_3$, $N = A_3$ e $H = \langle (1,2) \rangle$. Então $G = N \rtimes H$. Como H não é normal em G temos que G não é o produto direto de N e H.*

Observação 1.3 *Seja $G = N \rtimes H$. Então:*

1. *Pelo Teorema* 1.4 *temos que*

$$H = \frac{H}{N \cap H} \simeq \frac{NH}{H} = \frac{G}{N}.$$

e H é chamado um complemento *de N. Consequentemente, se G é finito, obtemos*

$$|G| = |N| \, [G : N] = |N| \, |H| \, ;$$

2. *Como $G = NH$ e $N \trianglelefteq G$ temos que cada $x \in G$ pode ser escrito de modo único na forma $x = nh$, $n \in N$ e $h \in H$.*

3. *Seja $h \in H$ fixado. Então a função $\varphi_h : N \to N$ dada por $\varphi_h(n) = hnh^{-1}$ é um automorfismo de N. Além disso, $\varphi_{hh'} = \varphi_h \circ \varphi_{h'}$, para todo $h, h' \in H$. Portanto, a função $\varphi : H \to \mathrm{Aut}(N)$ dada por $\varphi(h) = \varphi_h$ é um homomorfismo de grupos, chamado* homomorfismo por conjugação *de N. Como*

$$(n_1 h_1)(n_2 h_2) = n_1 \varphi_{h_1}(n_2) \, h_1 h_2 \ \text{ para alguns } n_1, n_2 \in N \ \text{ e } \ h_1, h_2 \in H.$$

temos que a operação do grupo G pode ser expressa em termos das operações de N, H e o homomorfismo φ;

4. *Se $\varphi(h) = \mathrm{I}$, para todo $h \in H$, então $\varphi_h(n) = n$, para todo $n \in N$. Logo,*

$$hnh^{-1} = n \Rightarrow n^{-1}hn = h \in H,$$

isto é, $H \trianglelefteq G$. Portanto,

$$G = N \times H.$$

Reciprocamente, se $G = N \times H$, então os elementos de H comutam com os elementos de N e, assim, o homomorfismo φ é trivial;

5. *Se* $\varphi(h) \neq \mathrm{I}$, *para algum* $h \in H$, *então* $\varphi_h(n) \neq n$, *para algum* $n \in N$. *Logo,*

$$hnh^{-1} \neq n \Rightarrow hn \neq nh.$$

Portanto, G *é não abeliano.*

Sejam N, H grupos e φ um homomorfismo de H em $\mathrm{Aut}\,(N)$. Definimos uma operação binária sobre $N \times H$ do seguinte modo:

$$(n_1, h_1)(n_2, h_2) = \left(n_1 \varphi_{h_1}(n_2), h_1 h_2\right).$$

É fácil verificar que $N \times H$ com esta operação binária é um grupo com elemento identidade $(1,1)$ e que $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$ é o inverso de (n,h). O grupo $N \times H$ é chamado o *produto semidireto* (*externo*) de N por H via φ e será denotado por

$$G = N \rtimes_\varphi H.$$

Note que

$$\mathcal{N} = \{(n,1) : n \in N\} \text{ e } \mathcal{H} = \{(1,h) : h \in H\}$$

são subgrupos de G tais que $N \simeq \mathcal{N}$ e $H \simeq \mathcal{H}$. Dados $(n,h) \in G$ e $(x,1) \in \mathcal{N}$, obtemos

$$\begin{aligned}(n,h)(x,1)(n,h)^{-1} &= (n\varphi_h(x), h)\left(\varphi_{h^{-1}}\left(n^{-1}\right), h^{-1}\right) \\ &= \left(n\varphi_h(x)\,\varphi_h(\varphi_{h^{-1}}\left(n^{-1}\right)), h\right)\left(\varphi_{h^{-1}}\left(n^{-1}\right), hh^{-1}\right) \\ &= \left(n\varphi_h(x)\,n^{-1}), 1\right) \in \mathcal{N}.\end{aligned}$$

Logo, $\mathcal{N} \trianglelefteq G$. Como

$$(n,1)(1,h) = (n\varphi_1(1), h) = (n,h)$$

temos que $G = \mathcal{N}\mathcal{H}$. Além disso, $\mathcal{N} \cap \mathcal{H} = \{(1,1)\}$. Portanto, G é o produto semidireto (interno) de $\mathcal{N}$ por $\mathcal{H}$. Finalmente,

$$(1,h)(n,1)(1,h)^{-1} = (\varphi_h(n), 1)$$

implica que $\psi : \mathcal{H} \to \mathrm{Aut}\,(\mathcal{N})$ definida por $\psi((1,h)) = \psi_{(1,h)}$, onde

$$\psi_{(1,h)}((n,1)) = (\varphi_h(n), 1),$$

é o homomorfismo por conjugação de N. Portanto, identificando $\mathcal{N}$ com N e $\mathcal{H}$ com H, obtemos que φ é o homomorfismo por conjugação de N e G é o produto semidireto (interno) de N por H. Neste caso,

$$N \rtimes_{\varphi} H = \{nh : n \in N, h \in H\},$$

onde

$$(n_1h_1) \cdot (n_2h_2) = n_1\varphi_{h_1}(n_2) \cdot h_1h_2.$$

Proposição 1.3 *Sejam N e H grupos, $\varphi : H \longrightarrow \mathrm{Aut}(N)$ um homomorfismo e $f \in \mathrm{Aut}(N)$. Se $\widehat{f} : \mathrm{Aut}(N) \to \mathrm{Aut}(N)$ é definida por $\widehat{f}(g) = fgf^{-1}$, então*

$$N \rtimes_{\widehat{f}\circ\varphi} H \simeq N \rtimes_{\varphi} H.$$

Prova. Seja $\theta : N \rtimes_{\varphi} H \to N \rtimes_{\widehat{f}\circ\varphi} H$ definida por $\theta(nh) = f(n)h$. Então θ é um homomorfismo de grupos, pois

$$\begin{aligned}
\theta(n_1h_1n_2h_2) &= \theta(n_1\varphi(h_1)(n_2)h_1h_2) \\
&= f(n_1\varphi(h_1)(n_2))h_1h_2 \\
&= f(n_1)f(\varphi(h_1)(n_2))h_1h_2 \\
&= f(n_1)(f\circ\varphi(h_1))(n_2)h_1h_2 \\
&= f(n_1)\left(f\circ\varphi(h_1)\circ f^{-1}\circ f\right)(n_2)h_1h_2 \\
&= f(n_1)\left(f\circ\varphi(h_1)\circ f^{-1}\right)(f(n_2))h_1h_2 \\
&= f(n_1)\left(\widehat{f}\circ\varphi\right)(h_1)(f(n_2))h_1h_2 \\
&= f(n_1)h_1f(n_2)h_2 \\
&= \theta(n_1h_1)\theta(n_2h_2).
\end{aligned}$$

Seja $\alpha : N \rtimes_{\widehat{f}\circ\varphi} H \to N \rtimes_{\varphi} H$ definida por $\alpha(nh) = f^{-1}(n)h$. Então α é um homomorfismo de grupos. Além disso,

$$(\theta\circ\alpha)(nh) = \theta(\alpha(nh)) = \theta\left(f^{-1}(n)h\right) = f\left(f^{-1}(n)\right)h = \left(\left(f\circ f^{-1}\right)(n)\right)h = nh.$$

Analogamente, segue-se que $\alpha\circ\theta = \mathrm{I}$ e, portanto, $N \rtimes_{\widehat{f}\circ\varphi} H \simeq N \rtimes_{\varphi} H$. ■

1.4 Grupos Abelianos Finitamente Gerados

Nesta seção apresentaremos alguns resultados clássicos da teoria dos grupos abelianos finitamente gerados que serão usados nos capítulos posteriores.

Sejam G um grupo abeliano e $a \in G$. Dizemos que a é um *elemento de torção* de G se existir $n \in \mathbb{N}$ tal que

$$a^n = 1.$$

O conjunto

$$T(G) = \{a \in G : o(a) < \infty\}$$

é um subgrupo de G chamado o *subgrupo de torção* de G. Se $T(G) = \{1\}$, dizemos que G é um *grupo livre de torção*. Note que $\frac{G}{T(G)}$ é livre de torção.

Teorema 1.6 *Seja G um grupo abeliano finitamente gerado. Então*:

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s},$$

onde $r, n_1, n_2, \ldots, n_s \in \mathbb{Z}$ com:

1. $r \geq 0$ *e* $n_i \geq 2$;

2. $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$.

Além disso, a expressão acima é única. ■

Corolário 1.1 *Seja G um grupo abeliano finitamente gerado. Então $T(G)$ é finito, $\frac{G}{T(G)}$ é abeliano livre de posto finito e*

$$G \simeq T(G) \times \frac{G}{T(G)}.$$

■

1.5 Séries de Composição

Seja G um grupo. Uma *série subnormal* de G é uma seqüência

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G, \tag{1.1}$$

tal que

$$G_{i-1} \trianglelefteq G_i, 1 \leq i \leq n.$$

Os grupos

$$\frac{G_i}{G_{i-1}}, 1 \leq i \leq n,$$

são chamados de *grupos fatores*. O *comprimento* da série subnormal é o número de grupos fatores não triviais.

Um *refinamento* de uma série subnormal

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

é uma série subnormal obtida a partir desta, pela inserção de alguns (possivelmente nenhum) subgrupos. O refinamento é próprio se algum subgrupo distinto dos já existentes é inserido na série.

A série subnormal (1.1) é uma *série de composição* se ela não admite um refinamento próprio.

Sejam

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G \text{ e } \{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G$$

duas séries subnormais de um grupo G. Dizemos que elas são *equivalentes*, se $n = m$ e existe uma permutação $\sigma \in S_n$, tal que

$$\frac{G_i}{G_{i-1}} \simeq \frac{H_{\sigma(i)}}{H_{\sigma(i)-1}}, 1 \leq i \leq n.$$

Teorema 1.7 (Schreier) *Duas séries subnormais de um grupo G possuem refinamentos que são equivalentes.* ■

Teorema 1.8 *Seja*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

uma série subnormal de um grupo G, onde cada fator é finito ou cíclico. Então o número de fatores cíclicos infinitos nestas séries é um invariante de G, isto é, qualquer outra série subnormal

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G$$

com fatores finito ou cíclicos têm o mesmo número de fatores cíclicos infinito. ■

O número de fatores cíclicos infinitos numa série subnormal de um grupo G, como no Teorema 1.8, é chamado o *número Hirsch* de G e será denotado por $h(G)$.

Seja G um grupo. O *comutador* de dois elementos $h, k \in G$ é definido por

$$[h, k] = h^{-1}k^{-1}hk.$$

O conjunto

$$G' = \langle [h, k] : h, k \in G \rangle$$

é chamado *subgrupo comutador* de G. Mais geralmente, se H e K são subconjuntos de G, então

$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle$$

é um subgrupo de G.

Proposição 1.4 *Seja G um grupo. Então*:

1. *G é abeliano, se e somente se, $G' = \{1\}$;*
2. *G' é um subgrupo caracterísco de G. Em particular, G' é normal em G;*
3. *$\frac{G}{G'}$ é abeliano;*
4. *Se H é um subgrupo de G, então H é normal e $\frac{G}{H}$ é abeliano se, e somente se, $G' \subseteq H$.*
5. *Se $f : G \longrightarrow L$ é um homomorfismo de grupos e H e K são subgrupos de G, então*

$$f([H, K]) = [f(H), f(K)].$$

■

Seja G um grupo. A *série central descendente* (*inferior*)

$$\gamma_1(G) \supseteq \gamma_2(G) \supseteq \cdots \supseteq \gamma_i(G) \supseteq \cdots$$

é definida, indutivamente, por

$$\gamma_1(G) = G, \ldots, \gamma_{i+1}(G) = [\gamma_i(G), G].$$

Proposição 1.5 *Seja G um grupo. Então*:

1. *Cada* $\gamma_i(G)$ *é um subgrupo característico de* G;

2. $\gamma_{i+1}(G) \leq \gamma_i(G)$;

3. $\frac{\gamma_i(G)}{\gamma_{i+1}(G)} \leq \mathcal{Z}\left(\frac{G}{\gamma_{i+1}(G)}\right)$. ■

Seja G um grupo. A *série central ascendente* (*superior*)

$$\mathcal{Z}_0(G) \subseteq \mathcal{Z}_1(G) \subseteq \mathcal{Z}_2(G) \subseteq \cdots \subseteq \mathcal{Z}_n(G)...$$

de G é definida, indutivamente, por

$$\mathcal{Z}_0(G) = \{e\}, \ldots, \mathcal{Z}_{n+1}(G) = \{x \in G : [x, G] \subseteq \mathcal{Z}_n(G)\}.$$

Proposição 1.6 *Seja* G *um grupo. Então*:

1. *Cada* $\mathcal{Z}_n(G)$ *é um subgrupo característico de* G;

2. $\mathcal{Z}_n(G) \subseteq \mathcal{Z}_{n+1}(G)$, *para todo* $n \geq 0$;

3. *Se* $\pi : G \longrightarrow \frac{G}{\mathcal{Z}_n(G)}$ *é a projeção canônica, então*

$$\mathcal{Z}_{n+1}(G) = \pi^{-1}\left(\mathcal{Z}\frac{G}{\mathcal{Z}_n(G)}\right).$$

Consequentemente, $\frac{\mathcal{Z}_{n+1}(G)}{\mathcal{Z}_n(G)}$ *é o centro de* $\frac{G}{\mathcal{Z}_n(G)}$. ■

Teorema 1.9 [16] *Seja* G *um grupo. Então existe* $c \in \mathbb{Z}_+$ *tal que* $\mathcal{Z}_c(G) = G$ *se, e somente se,* $\gamma_{c+1}(G) = \{1\}$. *Além disso,* $\gamma_{i+1}(G) \subseteq \mathcal{Z}_{c-i}(G)$, *para todo* $i \in \mathbb{Z}_+$. ■

Seja G um grupo. Dizemos que G é um grupo *nilpotente*, se existir $c \in \mathbb{Z}_+$ tal que

$$\gamma_{c+1}(G) = \{1\}.$$

Além disso, o menor c tal que $\gamma_{c+1}(G) = \{1\}$ é chamado de *classe de nilpotência* e será denotada por $\gamma(G) = c$.

Teorema 1.10 *Todo p-grupo finito é nilpotente.* ■

Proposição 1.7 *Sejam* H *e* K *grupos nilpotentes. Então* $H \times K$ *é nilpotente.* ■

Proposição 1.8 *Sejam G um grupo nilpotente e $H \neq \{1\}$ um subgrupo normal de G. Então*

$$H \cap \mathcal{Z}(G) \neq \{1\}.$$

■

Teorema 1.11 *[16] Sejam G um grupo nilpotente de classe c e H um subgrupo de G. Então*:

1 *H é nilpotente e $\gamma(H) \leq c$.*

2 *Se $H \trianglelefteq G$, então $\frac{G}{H}$ é nilpotente e $\gamma\left(\frac{G}{H}\right) \leq c$.* ■

Teorema 1.12 *Seja G um grupo finito. Então as seguintes condições são equivalentes*:

1. *G é nilpotente.*
2. *Se H é um subgrupo próprio de G, então H é um subgrupo próprio de $\mathcal{N}_G(H)$.*
3. *Todo subgrupo de Sylow de G é normal em G.*
4. *G é o produto direto de seus subgrupos de Sylow.* ■

Proposição 1.9 *[15] Seja G um grupo nilpotente finitamente gerado. Então os grupos fatores são cíclicos infinitos ou de ordem potência de um primo.* ■

Teorema 1.13 *Seja G um grupo nilpotente. Então $T(G)$ é um subgrupo característico e $\frac{G}{T(G)}$ é livre de torção. Além disso, para cada primo p existe um único p-subgrupo maximal T_p de $T(G)$ e $T(G)$ é o produto de todos estes subgrupos.* ■

1.6 Grupos Policíclicos e Seqüências Exatas

Seja G um grupo. Dizemos que G é *policíclico*, se existir uma série subnormal

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

tal que

$$\frac{G_{i+1}}{G_i}, i = 0, \ldots, n-1,$$

é cíclico.

Um grupo G é dito *poli-cíclico-infinito* se G possui uma série subnormal com grupos fatores cíclicos infinito. É claro que todo grupo poli-cíclico-infinito é livre de torção e policíclico mas a recíproca é falsa. Dizemos que G é um grupo *policíclico-por-finito* se os grupos fatores são cíclicos ou finito.

Teorema 1.14 *Sejam G um grupo e H um subgrupo de G. Então*:

1. *Se G é policíclico, então H é policíclico.*

2. *Se H é normal em G, então G é policíclico se, e somente se, H e $\frac{G}{H}$ o são.* ■

Teorema 1.15 [15] *Seja G um grupo policíclico. Então G possui um subgrupo normal poli-cíclico-infinito de índice finito.* ■

Teorema 1.16 [15] *Seja G um grupo poli-cíclico-infinito. Então G possui um subgrupo abeliano normal livre de torção não trivial.* ■

Proposição 1.10 [15] *Seja G um grupo policíclico. Então G é residualmente finito.* ■

Lema 1.2 *Sejam G um grupo policíclico e N um subgrupo normal de G. Então*

$$h(G) = h(N) + h\left(\frac{G}{N}\right).$$

Além disso, $h(G) = h\left(\frac{G}{N}\right)$ se, e somente se, N é finito. ■

Lema 1.3 *Sejam $\{1\} \neq H \trianglelefteq G$ subgrupo livre de torção e*

$$\pi : G \longrightarrow \overline{G} = \frac{G}{H}$$

o homomorfismo canônico. Se $N \leq G$ é um subgrupo de torção, isto é, $N = T(N)$, então $\pi|_N$ é injetora e logo $\pi(N) \simeq N$.

Prova. Seja a função $\varphi = \pi|_N : N \to \overline{G}$ definida por $\varphi(n) = \pi(n)$. Então

$$\begin{aligned} n_0 \quad &\in \quad \ker\varphi \Leftrightarrow n_0 \in N \text{ e } \varphi(n_0) = \pi(n_0) = A \\ &\Rightarrow \quad n_0 \in \ker\pi \cap N = A \cap N \\ &\Rightarrow \quad n_0 \in T(A) = \{1\}. \end{aligned}$$

Portanto, $\varphi = \pi|_N$ é injetora. ■

Lema 1.4 *Seja $G = N \rtimes A$, onde N é finito e A é abeliano livre finitamente gerado. Então o índice de $\mathcal{Z}(G)$ em G é finito.*

Prova. Seja a função $\varphi : A \to \mathrm{Aut}(N)$ o homomorfismo conjugação de G. Então, pelo Teorema 1.2, temos

$$\frac{A}{\ker \varphi} \simeq \mathrm{Im}\, \varphi.$$

Logo,

$$[A : \ker \varphi] = |\mathrm{Im}\, \varphi| < \infty,$$

pois $|\mathrm{Aut}(N)| < \infty$. Por outro lado,

$$[G : \ker \varphi] = [G : A]\,[A : \ker \varphi] = |N|\,[A : \ker \varphi] < \infty,$$

pois $|N| < \infty$. Se $a \in \ker \varphi$ e $n \in N$, então $\varphi(a) = \mathrm{Id}$ e

$$ana^{-1} = \varphi_a(n) = \mathrm{Id}(n) = n \Rightarrow an = na, \forall n \in N.$$

Logo,

$$[N, \ker \varphi] = \{1\} \text{ e } [A, \ker \varphi] = \{1\}$$

e, assim, $\ker \varphi \subseteq \mathcal{Z}(G)$. Logo,

$$[G : \ker \varphi] = [G : \mathcal{Z}(G)]\,[\mathcal{Z}(G) : \ker \varphi] < \infty.$$

Portanto, $[G : \mathcal{Z}(G)] < \infty$. ■

Uma seqüência de homomorfismos de grupos

$$\cdots \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow \cdots$$

é dita *exata* em G se

$$\mathrm{Im}\, \alpha = \ker \beta$$

ou, equivalentemente,

$$\beta\alpha(h) = 1, \forall h \in N$$

e cada $g \in G$ com $\beta(g) = 1$ tem a forma $g = \alpha(h)$, para algum $h \in N$. Uma seqüência é dita *exata* se ela é exata em cada um dos grupos que a constituem. Por exemplo, se N é um subgrupo normal de G, a seqüência

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} \frac{G}{N} \longrightarrow 1,$$

onde i é a inclusão e π a projeção canônica, é exata.

A seqüência

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

é dita *seqüência exata curta*. Neste caso, dizemos que o grupo G é uma *extensão* de N por H. A seqüência cinde se existir um homomorfismo $\gamma : H \to G$ tal que $\beta\gamma = \mathrm{Id}_H$. O homomorfismo γ é chamado de *homomorfismo transversal*. Neste caso, $G = N \rtimes H$.

Duas seqüências exatas curtas

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

e

$$1 \longrightarrow N \xrightarrow{\alpha} L \xrightarrow{\beta} H \longrightarrow 1$$

são *equivalentes* se existir um isomorfismo $\phi : G \to L$ tal que o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & H & \longrightarrow & 1 \\ & & \downarrow & & \downarrow \phi & & \downarrow & & \\ 1 & \longrightarrow & N & \xrightarrow{\alpha} & L & \xrightarrow{\beta} & H & \longrightarrow & 1 \end{array}$$

comuta.

Exemplo 1.3 *Sejam N e H grupos. Então a seqüência exata curta*

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1.$$

onde $G = N \times H$, $\alpha(h) = (h, 0)$ e $\beta(h, q) = q$, cinde, pois $\gamma : H \to G$ dado por $\gamma(q) = (0, q)$ é tal que $\beta\gamma = \mathrm{Id}_H$.

Lema 1.5 *Sejam*

$$1 \longrightarrow N \xrightarrow{\alpha_1} E_1 \xrightarrow{\beta_1} G \longrightarrow 1$$

uma seqüência exata e $\gamma_1 : G \to E_1$ um homomorfismo transversal. Se A é um subgrupo normal de G e $B = \gamma_1(A)$ é normal em E_1, então existe uma seqüência exata

$$1 \longrightarrow N \xrightarrow{\alpha_2} E_2 \xrightarrow{\beta_2} G_1 \longrightarrow 1$$

e um homomorfismo transversal $\gamma_2 : G_1 \to E_2$, onde $E_2 = \frac{E_1}{B}$ e $G_1 = \frac{G}{A}$.

Prova. Consideremos o diagrama abaixo, confira Figura 1.1,

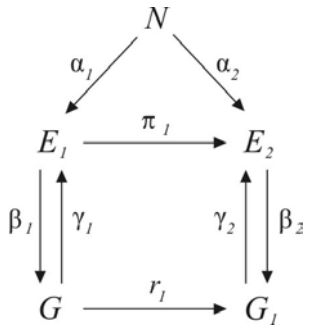

Figura 1.1: Diagrama de seqüências exatas.

onde π_1 e r_1 são as projeções canônicas. Se definirmos α_2 e β_2 por

$$\alpha_2(n) = \alpha_1(n)\,B \;\text{ e }\; \beta_2(eB) = \beta_1(e)\,A,$$

então

$$\beta_2(\alpha_2(n)) = \beta_2(\alpha_1(n)\,B) = \beta_1(\alpha_1(n))\,A = A.$$

Logo,

$$1 \longrightarrow N \xrightarrow{\alpha_2} E_2 \xrightarrow{\beta_2} G_1 \longrightarrow 1$$

é uma seqüência exata. Por outro lado, seja γ_2 definida por

$$\gamma_2(gA) = \gamma_1(g)\,B.$$

Então γ_2 é um homomorfismo. Portanto, γ_2 é um homomorfismo transversal. ■

Lema 1.6 *Sejam*

$$\varphi_1 : G \longrightarrow \mathrm{Aut}(N) \;\; e \;\; \varphi_2 : G_1 \longrightarrow \mathrm{Aut}(N)$$

as aplicações induzidas pelas transversais γ_1 *e* γ_2 *do Lema* 1.5. *Então* $\varphi_1 = \varphi_2 \circ r_1$, *onde* r_1 *é dada no Lema* 1.5.

Prova. Como o diagrama da Figura 1.1 comuta, obtemos

$$\begin{aligned}
\pi_1\left(\gamma_1(g)^{-1}\,\alpha_1(n)\,\gamma_1(g)\right) &= \pi_1\left(\gamma_1(g)^{-1}\right)\pi_1(\alpha_1(n))\,\pi_1(\gamma_1(g)) \\
&= \pi_1 \circ \gamma_1(g)^{-1}\,\pi_1(\alpha_1(n))\,\pi_1 \circ \gamma_1(g) \\
&= \gamma_2(gA)^{-1}\,\alpha_2(n)\,\gamma_2(gA)\,, \forall g \in G.
\end{aligned}$$

Logo,

$$\begin{aligned}
\alpha_2\left(\varphi_2\left(gA\right)\left(n\right)\right) &= \alpha_2\left(\gamma_2\left(gA\right)^{-1} n\gamma_2\left(gA\right)\right) \\
&= \gamma_2\left(gA\right)^{-1}\alpha_2\left(n\right)\gamma_2\left(gA\right) \\
&= \pi_1\left(\gamma_1\left(g\right)^{-1}\alpha_1\left(n\right)\gamma_1\left(g\right)\right) \\
&= \pi_1\left(\alpha_1\left(\gamma_1\left(g\right)^{-1} n\gamma_1\left(g\right)\right)\right) \\
&= \pi_1\circ\alpha_1\left(\gamma_1\left(g\right)^{-1} n\gamma_1\left(g\right)\right) \\
&= \alpha_2\left(\gamma_1\left(g\right)^{-1} n\gamma_1\left(g\right)\right) \\
&= \alpha_2\left(\varphi_1\left(g\right)\left(n\right)\right), \forall g\in G \text{ e } n\in N.
\end{aligned}$$

Como α_2 é injetora temos que

$$\varphi_2\left(gA\right)\left(n\right) = \varphi_1\left(g\right)\left(n\right) \Rightarrow \varphi_2\circ r_1\left(g\right)\left(n\right) = \varphi_1\left(g\right)\left(n\right), \forall g\in G \text{ e } n\in N.$$

Portanto, $\varphi_1 = \varphi_2\circ r_1$. ■

Lema 1.7 *Sejam $\alpha_3 : M \longrightarrow E_3$ um homomorfismo injetor e $\pi_2 : E_3 \longrightarrow E_2$ a projeção canônica tal que $\pi_2\left(\alpha_3\left(M\right)\right) = \alpha_2\left(N\right)$ e $\pi_2|_{\alpha_3(M)}$ é injetora. Então existem uma seqüência exata que cinde*

$$1 \longrightarrow M \xrightarrow{\alpha_3} E_3 \xrightarrow{\beta_3} G_2 \longrightarrow 1,$$

um morfismo (α, π_2, r_2) e um homomorfismo transversal $\gamma_3 : G_3 \longrightarrow E_3$ tal que

$$\pi_2\circ\gamma_3 = \gamma_2\circ r_2.$$

Prova. Consideremos o diagrama abaixo, confira Figura 1.2,

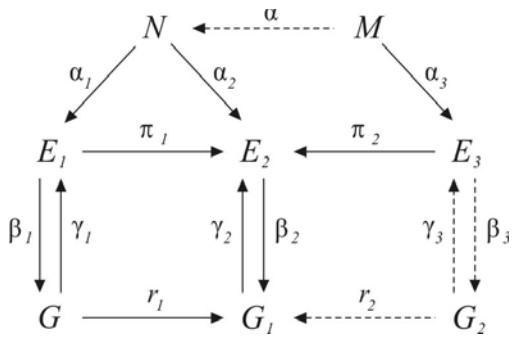

Figura 1.2: Diagrama de seqüências exatas.

Suponhamos que $K = \pi^{-1}(\gamma_2(G_1))$ e $E = \langle \alpha_3(M), K \rangle$. Como

$$\ker(\pi_2) = \pi_2^{-1}(B) \subseteq K \text{ e } (\alpha_2, \beta_2) \text{ cinde}$$

obtemos que

$$\pi_2(\alpha_3(M)) = \alpha_2(N) = B \text{ e } \alpha_3(M) = \ker\left(\pi_2|_{\alpha_3(M)}\right)$$

Assim, $\alpha_3(M) = \{1\}$, pois $\pi_2|_{\alpha_3(M)}$ é injetora. Logo,

$$K \cap \alpha_3(M) = \{1\} \text{ e } E = E_3.$$

Logo, K é um complemento de $\alpha_3(M)$ em E_3. Sejam $G_3 = K$, $r_2 = \beta_2 \circ \pi_2|_K$ e $\alpha : M \longrightarrow N$ um morfismo definido por

$$\alpha_2(\alpha(m)) = \pi_2(\alpha_3(M)).$$

Note que,

$$\alpha_2(\alpha(M)) = \pi_2(\alpha_3(M)) = \alpha_2(N) \Longrightarrow \alpha(M) = N.$$

Logo, $\alpha_2 \circ \alpha = \pi_2 \circ \alpha_3$. Temos assim, que existe uma seqüência exata

$$1 \longrightarrow M \xrightarrow{\alpha_3} E_3 \xrightarrow{\beta_3} G_2 \longrightarrow 1,$$

e um homomorfismo (α, π_2, r_2). Seja

$$\gamma_3(k) = k, \forall k \in K.$$

Então γ_3 é um homomorfismo transversal tal que

$$\pi_2 \circ \gamma_3 = \gamma_2 \circ r_2.$$

■

Lema 1.8 *Com as notações do Lema* 1.6 *e da prova do Lema* 1.7*, seja f_3 a aplicação induzida por γ_3 de G_3 em* $\mathrm{Aut}(M)$*. Então*

$$f_2 \circ r_2(k) = \alpha \circ f_3(k) \circ \alpha^{-1}, \text{ para algum } k \in K.$$

Prova. Como $N \simeq M$ e

$$\begin{aligned} \pi_2^{-1}\left(\gamma_2(gA)^{-1}\alpha_2(\alpha(m))\gamma_2(gA)\right) &= \pi_2^{-1}\gamma_2(gA)^{-1}\pi_2^{-1}(\alpha_2(\alpha(m)))\pi_2^{-1}\gamma_2(gA) \\ &= \gamma_3(k)^{-1}\alpha_3\left(\alpha^{-1}(n)\right)\gamma_3(k) \end{aligned}$$

temos que

$$\begin{aligned}
\alpha_3\left(f_3\left(\gamma_3\left(k\right)\right)\left(\alpha^{-1}\left(n\right)\right)\right) &= \alpha_3\left(\gamma_3\left(k\right)^{-1}\left(\alpha^{-1}\left(n\right)\right)\gamma_3\left(k\right)\right) \\
&= \gamma_3\left(k\right)^{-1}\alpha_3\left(\alpha^{-1}\left(n\right)\right)\gamma_3\left(k\right) \\
&= \pi_2^{-1}\left(\gamma_2\left(gA\right)^{-1}\alpha_2\left(\alpha\left(m\right)\right)\gamma_2\left(gA\right)\right) \\
&= \pi_2^{-1}\left(\alpha_2\left(\gamma_2\left(gA\right)^{-1}\alpha\left(m\right)\gamma_2\left(gA\right)\right)\right) \\
&= \pi_2^{-1}\circ\alpha_2\left(\gamma_2\left(gA\right)^{-1}\alpha\left(m\right)\gamma_2\left(gA\right)\right) \\
&= \alpha_3\left(\gamma_2\left(r_2\left(k\right)\right)^{-1}\alpha^{-1}\left(n\right)\gamma_2\left(r_2\left(k\right)\right)\right) \\
&= \alpha_3\left(f_2\left(r_2\left(k\right)\right)\left(\alpha^{-1}\left(n\right)\right)\right) \\
&= \alpha_3\left(\left(f_2\left(r_2\left(k\right)\right)\circ\alpha^{-1}\right)\left(n\right)\right) \\
&= \alpha_3\left(\left(\alpha^{-1}\circ f_2\left(r_2\left(k\right)\right)\right)\left(n\right)\right).
\end{aligned}$$

Logo,

$$\alpha_3\left(f_3\left(\gamma_3\left(k\right)\right)\left(\alpha^{-1}\left(n\right)\right)\right) = \alpha_3\left(\left(\alpha^{-1}\circ f_2\left(r_2\left(k\right)\right)\right)\left(n\right)\right).$$

Sendo α_3 injetora, obtemos

$$\begin{aligned}
f_3\left(\gamma_3\left(k\right)\right)\circ\alpha^{-1} &= \alpha^{-1}\circ f_2\left(r_2\left(k\right)\right) \\
&\Rightarrow \quad f_3\left(k\right)\circ\alpha^{-1} = \alpha^{-1}\circ f_2\left(r_2\left(k\right)\right), \text{ para algum } k\in K.
\end{aligned}$$

Portanto,

$$f_2\left(r_2\left(k\right)\right) = \alpha\circ f_3\left(k\right)\circ\alpha^{-1}, \text{ para algum } k\in K.$$

■

Lema 1.9 *Seja $\rho : G \longrightarrow G_3$ um homomorfismo injetor tal que $r_2\circ\rho = r_1$. Então E_1 é isomorfo a um subgrupo de E_3.*

Prova. Seja $\varphi : E_1 \to E_3$ definida por

$$\varphi\left(\alpha_1\left(n\right)\gamma_1\left(g\right)\right) = \left(\alpha_3\cdot\alpha^{-1}\left(n\right)\right)\gamma_3\left(\rho\left(g\right)\right).$$

Então é fácil verificar que φ está bem definida, é injetora e

$$\operatorname{Im}\varphi = \alpha_3\left(M\right)\rtimes\gamma_3\rho\left(G\right).$$

Vamos mostrar que φ é um homomorfismo de grupos. É claro que $\varphi\left(1\right) = 1$. Dados

$$a = \alpha_1\left(n\right)\gamma_1\left(g\right), b = \alpha_1\left(m\right)\gamma_1\left(h\right)\in E_1, \text{ com } n,m\in N \text{ e } g,h\in G,$$

obtemos

$$\begin{aligned}
\varphi(ab) &= \varphi(\alpha_1(n)\gamma_1(g)\alpha_1(m)\gamma_1(h)) \\
&= \varphi\left(\alpha_1(n)\gamma_1(g)\alpha_1(m)\gamma_1(g)^{-1}\gamma_1(g)\gamma_1(h)\right) \\
&= \varphi\left(\alpha_1(n)\left(\alpha_1 f_1\left(g^{-1}(m)\right)\right)\gamma_1(gh)\right) \\
&= \varphi\left(\alpha_1\left(nf_1\left(g^{-1}\right)(m)\right)\gamma_1(gh)\right) \\
&= \alpha_3\alpha^{-1}\left(nf_1\left(g^{-1}\right)(m)\right)\gamma_3(\rho(gh)) \\
&= \alpha_3\left(\alpha^{-1}(n)\right)\left(\alpha_3\alpha^{-1}f_1\left(g^{-1}\right)(m)\gamma_3(\rho(gh))\right).
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
\varphi(a)\varphi(b) &= \left(\alpha_3\alpha^{-1}(n)\gamma_3(\rho(g))\right)\left(\alpha_3\alpha^{-1}(m)\gamma_3(\rho(h))\right) \\
&= \alpha_3\alpha^{-1}(n)\gamma_3(\rho(g))\alpha_3\alpha^{-1}(m)\gamma_3(\rho(g))^{-1}\times\gamma_3(\rho(g))\gamma_3(\rho(gh)) \\
&= \left(\alpha_3\alpha^{-1}(n)\right)\left(\alpha_3\left(\left(f_3\left(\rho\left(g^{-1}\right)\right)\right)\left(\alpha^{-1}(m)\right)\right)\right)\gamma_3(\rho(gh)).
\end{aligned}$$

Assim, para provar que

$$\varphi(ab) = \varphi(a)\varphi(b),$$

é suficiente mostrar que

$$f_1\left(g^{-1}\right)(m) = \alpha\left(f_3\left(\rho\left(g^{-1}\right)\right)\right)\left(\alpha^{-1}(m)\right),$$

pois α_3 é injetora. Pelo Lema 1.8, obtemos

$$\alpha\left(f_3\left(\rho\left(g^{-1}\right)\right)\right)\left(\alpha^{-1}(m)\right) = f_2\left(r_2\left(\rho\left(g^{-1}\right)\right)\right).$$

Como, por hipótese $r_2\circ\rho = r_1$, temos que

$$\alpha f_3\left(\rho\left(g^{-1}\right)\right)\alpha^{-1} = f_2\left(r_2\left(\rho\left(g^{-1}\right)\right)\right) = f_2\left(r_1\left(g^{-1}\right)\right).$$

Finalmente, pelo 1.6

$$\alpha f_3\left(\rho\left(g^{-1}\right)\right)\alpha^{-1} = f_1\left(g^{-1}\right).$$

Portanto, φ é um homomorfismo de grupos e E_1 é isomorfo a um subgrupo de E_3. ■

Teorema 1.17 *[16] Sejam A um grupo abeliano livre com base X, G um grupo abeliano e $f: X \longrightarrow G$ uma função. Então existe um único homomorfismo $\varphi: A \longrightarrow G$ estentendo f tal que*

$$\varphi(x) = f(x), \forall x \in X.$$

■

Teorema 1.18 (Propriedade Projetiva) *[16] Sejam $\beta : B \longrightarrow C$ um homomorfismo de grupos sobrejetor, A um grupo abeliano livre e $\alpha : A \longrightarrow C$ um homomorfismo de grupos. Então existe um homomorfismo $\gamma : A \longrightarrow B$ com diagrama comutando, isto é, $\beta\gamma = \alpha$. Além disso, se α é sobrejetora, então γ também o é.* ■

Teorema 1.19 *Sejam*

$$1 \longrightarrow N \xrightarrow{\alpha_1} E_1 \xrightarrow{\beta_1} G \longrightarrow 1$$

uma seqüência exata de um grupo finito N, G um grupo abeliano livre de torção e γ_1 um homomorfismo transversal. Sejam A um subgrupo normal de G,

$$E_2 = \frac{E_1}{B} \ \ e \ \ B = \gamma_1(A) \trianglelefteq E_1.$$

Suponhamos que existem uma seqüência exata

$$1 \longrightarrow M \xrightarrow{\alpha_3} E_3 \xrightarrow{\pi_2} E_2 \longrightarrow 1$$

e

$$\pi_2 \circ \alpha_2 : M \longrightarrow \pi_1\alpha_1(N)$$

um isomorfismo, onde $\pi_1 : E_1 \longrightarrow E_2$ é a projeção canônica. Se $h(E_1) = h(E_3)$ e $\frac{E_3}{\alpha_2(M)}$ é abeliano, então E_1 é isomorfo a um subgrupo de E_3.

Prova. Pelo o diagrama da Figura 1.2 e pelo Lema 1.9, basta verificar que existe um homomorfismo de grupos injetor

$$\rho : G \longrightarrow G_2, \ \text{tal que} \ r_2 \circ \rho = r_1.$$

Sejam

$$r_1 : G \longrightarrow G_1 \ \text{e} \ r_2 : G_2 \longrightarrow G_1$$

os homomorfismos sobrejetor. Como G é abeliano livre temos, pelo Teorema 1.18, que existe um homomorfismo sobrejetor

$$\rho : G \longrightarrow G_2, \ \text{tal que} \ r_2 \circ \rho = r_1.$$

Como a seqüência

$$1 \longrightarrow N \xrightarrow{\alpha_1} E_1 \xrightarrow{\beta_1} G \longrightarrow 1$$

cinde temos que

$$\frac{E_3}{\alpha_3(M)} \simeq G_2.$$

Logo, G_2 é abeliano. Sendo N finito, obtemos, pelo Lema 1.2, que $h(G) = h(E_1)$. Por outro lado, obtemos $\pi_1 \circ \alpha_1(N)$ é finito e, assim, M é finito. Logo, $h(G_3) = h(E_3)$. Por hipótese, obtemos $h(G) = h(G_3)$. Como

$$\frac{G}{\ker \rho} \simeq G_2$$

temos que $h(\ker \rho) = 0$. Assim, $\ker \rho$ é um subgrupo periódico de G. Logo, $\ker \rho = \{1\}$, pois G é abeliano livre. Portanto, ρ é um homomorfismo injetor. ■

Capítulo 2

Anéis de Grupos

Neste capítulo apresentaremos alguns resultados básicos sobre anéis, anéis de grupos e subgrupo de dimensão que serão nescessários para o desenvolvimento do próximo capítulo.

2.1 Anéis

Um *anel* é um conjunto não vazio R equipado com duas operações binárias, adição $(x, y) \to x + y$ e multiplicação $(x,y) \to xy$, tal que as seguintes propriedades valem:

1. R é um grupo comutativo com a adição.
2. $x(yz) = (xy)z$, para todo x, y, $z \in R$.
3. $x(y + z) = xy + xz$, $(x + y)z = xz + yz$, para todo x, y, $z \in R$.

   Se um anel R satisfaz a propriedade:

4. Existe $1 \in R$ tal que $x1 = 1x = x$, para todo $x \in R$, dizemos que R é um *anel com identidade.*
5. Se $xy = yx$, para quaisquer x, $y \in R$, dizemos que R é um *anel comutativo*

   Se um anel R satisfaz a propriedade:

6. Para todo $x, y \in R$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que R é um *anel sem divisores de zero.* Caso contrário, dizemos que R é um *anel com divisores de zero.*

Dizemos que um elemento $x \in R$, $x \neq 0$, é *regular* se x não é divisor de zero. Se R é um anel comutativo, com identidade e sem divisores de zero, dizemos que R é um *domínio.*

Um elemento $x \in R$ é dito uma *unidade* de R se existir $y \in R$, tal que $xy = yx = 1$. Denotaremos por $\mathcal{U}(R)$ o conjunto de todas as unidades de R. Se

$$\mathcal{U}(R) = R^* = R - \{0\},$$

dizemos que R é um *corpo*.

Sejam R um anel com identidade e $x \in R$. Se $n \in \mathbb{Z}$, definimos $nx \in R$ por

$$nx = \begin{cases} (n-1)x + x, & \text{se } n > 0 \\ 0, & \text{se } n = 0 \\ (-n)(-x), & \text{se } n < 0 \end{cases}$$

Sejam R um anel com identidade e $S = \{n \in \mathbb{N} : na = 0, \forall a \in R\}$. Se S é não vazio, então pelo princípio da boa ordenação, S contém um menor elemento, digamos $k \in S$. O elemento k é chamado de *característica* do anel R. Caso contrário, dizemos que R tem característica zero.

Um subconjunto não vazio S de um anel R com unidade é um *subanel* de R se as seguintes condições são satisfeitas:

1. para todo $x, y \in S$, tem-se $x - y \in S$;
2. para todo $x, y \in S$, tem-se $xy \in S$;
3. $1 \in S$.

Um subconjunto não vazio I de um anel R é um *ideal* de R se as seguintes condições são satisfeitas:

1. para todo $x, y \in I$, tem-se $x - y \in I$;
2. Para todo $x \in I$ e $r \in R$, tem-se rx e $xr \in I$.

Um ideal I do anel R tal que $I \neq 0$ e $I \neq R$ é chamado *ideal próprio*.

Sejam R e S dois anéis. Uma função $\phi : R \longrightarrow S$ é um *homomorfismo de anéis* se as seguintes condições são satisfeitas:

1. $\phi(x + y) = \phi(x) + \phi(y)$, para todo x, $y \in R$;
2. $\phi(xy) = \phi(x)\phi(y)$, para todo $x, y \in R$.

Um homomorfismo de anéis $\phi : R \longrightarrow S$ é um *isomorfismo* se ϕ for bijetora. Quando existir um isomorfismo entre R e S dizemos que R e S são *isomorfos* e denotaremos por $R \simeq S$.

Teorema 2.1 *Sejam R e S anéis e $\phi : R \longrightarrow S$ um homomorfismo de anéis. Então*

$$\frac{G}{\ker \phi} \simeq \operatorname{Im} \phi.$$

■

Seja R um anel comutativo com unidade. Um *módulo* V sobre R é um grupo comutativo aditivo, junto com uma função

$$R \times V \longrightarrow V, (r, \mathbf{v}) \longmapsto r\mathbf{v},$$

tal que as seguintes condições são satisfeitas:

1. $r(s\mathbf{v}) = (rs)\mathbf{v}$, para todo $r, s \in R$ e $\mathbf{v} \in V$.
2. $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$, para todo $r \in R$ e $\mathbf{u}, \mathbf{v} \in V$.
3. $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$, para todo $r, s \in R$ e $\mathbf{v} \in V$.
4. $1\mathbf{v} = \mathbf{v}$, para todo $\mathbf{v} \in V$.

Note que, se R é um corpo, então um módulo V sobre R é um *espaço vetorial* sobre R.

Um subconjunto W de um módulo V sobre R é um *submódulo* de V se:

1. Para todo $\mathbf{w}_1, \mathbf{w}_2 \in W$, tem-se $\mathbf{w}_1 - \mathbf{w}_2 \in W$,
2. Para todo $r \in R$ e $\mathbf{w} \in W$, tem-se $r\mathbf{w} \in W$.

Sejam S um subconjunto de um módulo V sobre R e

$$\mathcal{A} = \{W : W \text{ é submódulo de } V \text{ e } S \subset W\}.$$

Então

$$\langle S \rangle = \bigcap_{W \in \mathcal{A}} W$$

é o menor submódulo de V contendo S e será chamado de *submódulo gerado por* S sobre R.

Seja V um módulo sobre R. Se $\mathbf{v} \in V$ pode ser escrito como

$$\mathbf{v} = \sum\nolimits_{i=1}^{n} r_i \mathbf{v}_i : r_i \in R \text{ e } \mathbf{v}_i \in V,$$

então dizemos que $\mathbf{v}$ é uma *combinação linear* dos elementos $\mathbf{v}_1, \ldots, \mathbf{v}_n$ sobre R. Neste caso, o conjunto de todas as combinações lineares de $\mathbf{v}_1, \ldots, \mathbf{v}_n$ é o submódulo

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle = \left\{ \sum_{i=1}^{n} r_i \mathbf{v}_i : r_i \in R \right\},$$

gerado por $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Quando existe um subconjunto finito S de um módulo V sobre R tal que $V = \langle S \rangle$, dizemos que V é um *módulo finitamente gerado* sobre R. Se $S = \{\mathbf{v}\}$, isto é, S consiste de um único elemento, temos

$$\langle \mathbf{v} \rangle = \{ r\mathbf{v} : r \in R \}$$

e $\langle \mathbf{v} \rangle$ será chamado de *submódulo cíclico gerado por* $\mathbf{v}$ sobre R.

Uma seqüência finita $\mathbf{v}_1, \ldots, \mathbf{v}_n$ de elementos de um módulo V sobre R é chamada *linearmente independente* se

$$\sum_{i=1}^{n} r_i \mathbf{v}_i = 0 \Rightarrow r_1 = r_2 = \cdots = r_n = 0.$$

Caso contrário, dizemos que a seqüência é *linearmente dependente*. Um subconjunto S de um módulo V sobre R é dito *linearmente independente* se qualquer seqüência finita de elementos distintos de S é linearmente independente. Caso contrário, S é dito *linearmente dependente*.

Um subconjunto S de um módulo V sobre R é dito uma *base* sobre R se as seguintes propriedades valem:

1. $V = \langle S \rangle$.

2. S é linearmente independente.

Um módulo V sobre R é chamado de *módulo livre* sobre R se possui uma base. A cardinalidade da base sobre R é chamada de *posto* de V sobre R.

Seja V um espaço vetorial sobre um corpo F. Então o conjunto de todos os operadores lineares invertíveis sobre V será denotado por

$$\mathrm{GL}(V).$$

Seja G um grupo finito agindo sobre V. Dizemos que a ação de G sobre V é *linear* se

1. $a(\mathbf{v}+\mathbf{w}) = a\mathbf{v} + a\mathbf{w}$, para todo $a \in G$ e $\mathbf{v}, \mathbf{w} \in V$;

2. $a(x\mathbf{v}) = x(a\mathbf{v})$, para todo $a \in G$, $x \in R$ e $\mathbf{v} \in V$.

Observação 2.1 *Existe uma correspodência biunívoca entre o conjunto de ações lineares de G em V e o conjunto de homomorfismos de G em* $\mathrm{GL}(V)$.

Um homomorfismo $\varphi : G \longrightarrow \mathrm{GL}(V)$ é chamado de *representação linear* de G em V. Neste caso, dizemos que V é o *espaço representação* e a *dimensão* da representação é a dimensão de V. Se ρ e φ são representações do grupo G com espaços representação V_1 e V_2, respectivamente, então dizemos que ρ e φ são representações *equivalentes* ou *isomorfas* se existir um isomorfismo T de V_1 sobre V_2 tal que

$$T\rho(a) = \varphi(a)T, \forall a \in G.$$

Exemplo 2.1 (A representação natural) *Se $G = S_n$, então existe uma* representação natural *em termos de matrizes de permutação. Denotaremos esta representação por ρ_N. Seja*

$$\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$$

uma base para V. Definimos a transformação linear de V em V por

$$\rho_N(\sigma)(\mathbf{v}_i) = \mathbf{v}_{\sigma(i)}, \sigma \in G.$$

Exemplo 2.2 (A representação regular) *Sejam G um grupo de ordem n e V um espaço vetorial de dimensão n com uma base*

$$\{\mathbf{v}_a : a \in G\}.$$

Definimos uma transformação linear de V em V por

$$\rho_R(a)\mathbf{v}_h = \mathbf{v}_{ah}, a, h \in G.$$

Isto é a representação regular *de G. Em termos de matrizes, é conveniente ordenar os elementos $a_i \in G, i = 1, 2, \ldots, n$. Então*

$$\boldsymbol{\rho}_R(a_k) = \begin{cases} 1 & , se\ a_i = a_k a_j \\ 0 & , se\ a_i \neq a_k a_j \end{cases}$$

e isto produz uma representação matricial de G por matrizes de permutação.

2.2 Anéis de Grupos

Nesta seção apresentaremos algumas definições da teoria de anéis de grupos necessárias para o desenvolvimento do nosso trabalho. Para maiores detalhes consulte [17, 19].

Sejam R um anel e G um grupo. O *suporte* de uma função $\alpha : G \to R$ é o conjunto de todos os $g \in G$, tais que $\alpha(g) \neq 0$, isto é,

$$\text{supp}(\alpha) = \{g \in G : \alpha_g \neq 0\}$$

Seja

$$RG = \{\alpha = \sum_{g \in G} \alpha_g g : \alpha_g \in R \text{ e } |\text{supp}(\alpha)| < \infty\}$$

o conjunto das *somas formais* sobre R tais que $\text{supp}(\alpha)$ seja finito. Dados

$$\alpha = \sum_{g \in G} \alpha_g g, \mu = \sum_{g \in G} \mu_g g \in RG,$$

dizemos que

$$\alpha = \mu \Leftrightarrow \alpha_g = \mu_g, \forall g \in G.$$

Definimos em RG duas operações binárias, adição e multiplicação, por

$$\alpha + \mu = \sum_{g \in G} \left(\alpha_g + \mu_g\right) g \text{ e } \alpha\mu = \sum_{k \in G} \nu_k k,$$

onde

$$\nu_k = \sum_{gh=k} \alpha_g \mu_h = \sum_{g \in G} \alpha_g \mu_{g^{-1}k}.$$

Note que, estas operações são bem definidas, pois

$$\text{supp}(\lambda + \mu) \subseteq \text{supp}(\lambda) \cup \text{supp}(\mu) \text{ e } \text{supp}(\lambda\mu) \subseteq \text{supp}(\lambda) \cdot \text{supp}(\mu).$$

Com estas operações RG é um anel, o qual será chamado de *anel de grupo*. Apagando as componentes zero da soma formal α podemos escrever

$$\alpha = \sum_{i=1}^{n} \alpha_i g_i,$$

onde $n = |\text{supp}(\alpha)|$. Note que $rg = gr$, para todo $r \in R$ e $g \in G$ e, assim,

$$(\alpha_g g)(\mu_h h) = \alpha_g \mu_g gh, \forall g, h \in G.$$

Seja

$$S = \{r \cdot e_G : r \in R\} = Re_G,$$

onde e_G é o elemento identidade de G. Então S é um subanel de RG isomorfo a R. Assim, podemos identificar

$$R \text{ com } Re_G.$$

Portanto, 1 é o elemento identidade de RG. De modo análogo, identificamos

$$G \text{ com } 1G.$$

Com estas identificações

$$r\alpha = \sum_{i=1}^{n} (r\alpha_i) g_i, \forall r \in R.$$

Deste modo RG é um *módulo livre* sobre R com os elementos de G como uma base.

Observação 2.2 *RG é um anel comutativo se, e somente se, G e R são comutativos.*

A função $\varepsilon : RG \to R$ definida por

$$\varepsilon(\alpha) = \varepsilon\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g$$

é um homomorfismo de anéis sobrejetor, chamada de *função de aumento* de RG. O

$$\Delta_R(G) = \ker \varepsilon = \{\alpha = \sum_{g \in G} \alpha_g g \in RG : \sum_{g \in G} \alpha_g = 0\}$$

é chamado o *ideal de aumento* de RG.

Seja N um subgrupo normal de G. Então a função $\varphi : RG \to R\left(\frac{G}{N}\right)$ definida por

$$\varphi(\alpha) = \varphi\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g gN$$

é um homomorfismo de anéis, com

$$\Delta_R(G,N) = \ker\varphi = \left\{ \sum_{g\in G} \alpha_g g \in RG : \sum_{g\in G} \alpha_g gN = 0 \right\}.$$

Como

$$G = \bigcup_{i=1}^{k} g_i N, \text{ onde } k = [G:N]$$

temos que

$$\alpha = \sum_{g\in G} \alpha_g g = \sum_{i=1}^{k} \sum_{n\in N} \alpha_{g_i n} g_i n = \sum_{i=1}^{k} g_i \left(\sum_{n\in N} \alpha_{g_i n} n \right).$$

Note que

$$\begin{aligned} \alpha \quad &\in \quad \Delta_R(G,N) \Leftrightarrow \varphi(\alpha) = 0 \Leftrightarrow \sum_{i=1}^{k} \sum_{n\in N} \alpha_{g_i n} \varphi(g_i)\varphi(n) = 0 \\ &\Leftrightarrow \quad \sum_{i=1}^{k} \left(\sum_{n\in N} \alpha_{g_i n} \right) \varphi(g_i) = 0 \Leftrightarrow \sum_{n\in N} \alpha_{g_i n} = 0, \forall i. \end{aligned}$$

Portanto,

$$\begin{aligned} \alpha &= \sum_{i=1}^{k} g_i \left(\sum_{n\in N} \alpha_{g_i n} n \right) \\ &= \sum_{i=1}^{k} g_i \left(\sum_{n\in N} \alpha_{g_i n} n - \sum_{n\in N} \alpha_{g_i n} \right) \\ &= \sum_{i=1}^{k} g_i \sum_{n\in N} \alpha_{g_i n} (n-1) \in \langle x-1 : x \in N \rangle_{RG}. \end{aligned}$$

Em particular, $\Delta_R(G) = \Delta_R(G,G)$.

Observação 2.3 *Se G é finito e R é comutativo, então $\Delta_R(G)$ é um R-módulo livre de posto $|G|-1$.*

Seja G um grupo. Denotamos por

$$\mathcal{U}(\mathbb{Z}G) = \{\alpha \in \mathbb{Z}G : \alpha \text{ é inversível}\},$$

o *grupo das unidades* de $\mathbb{Z}G$ e

$$\mathcal{U}_1(\mathbb{Z}G) = \{\alpha \in \mathcal{U}(\mathbb{Z}G) : \varepsilon(\alpha) = 1\},$$

o grupo das *unidades normalizadas* de $\mathbb{Z}G$.

Se $u \in \mathcal{U}(\mathbb{Z}G)$, então $\varepsilon(u) = \pm 1$. Como

$$\mathcal{U}_1(\mathbb{Z}G) \leq \mathcal{U}(\mathbb{Z}G) \text{ temos que } \mathcal{U}(\mathbb{Z}G) = \{\pm 1\} \times \mathcal{U}_1(\mathbb{Z}G).$$

Os elementos $\pm g$ são *unidades* em $\mathbb{Z}G$ com o inverso $\pm g^{-1}$. Estas unidades são chamadas *unidades triviais*.

Observação 2.4 *Seja G um grupo. Dizemos que G satisfaz a* condição do normalizador *se*

$$\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G) = \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))\, G.$$

A álgebra do grupo complexo $\mathbb{C}G$ tem uma involução: para $\gamma = \sum_{g \in G} \gamma(g) g$, seja $\gamma^* = \sum_{g \in G} \overline{\gamma}(g) g^{-1}$, onde $-$ denota o conjugado complexo. Então para todo $\gamma, \beta \in \mathbb{Z}G$ e $c \in \mathbb{Z}$ temos que:

1. $(\gamma + \beta)^* = \gamma^* + \beta^*$
2. $(\gamma\beta)^* = \beta^*\gamma^*$
3. $(\gamma^*)^* = \gamma$
4. $(c\gamma^*) = c\gamma^*$

Além disso,

$$\gamma\gamma^*(1) = \sum (\gamma(g))^2,$$

o que implica que $\gamma\gamma^* = 0$ se, e somente se, $\gamma = 0$.

Proposição 2.1 *Para $\gamma \in \mathbb{Z}G$, $\gamma\gamma^* = 1$ se, e somente se, $\gamma = \pm g$, $g \in G$.* ■

Seja R um anel e $x, y \in R$. O *comutador de Lie* de x e y é o elemento

$$(x, y) = xy - yx$$

e $[R, R]$ é o subgrupo aditivo de R gerado por todos os comutadores de Lie $(x, y), x, y \in R$.

Sejam G um grupo e R um anel comutativo. Então (RG, RG) é um R-módulo com a ação

$$r(x, y) = (rx, y), \forall x, y \in RG \text{ e } r \in R.$$

Para cada

$$\alpha = \sum_{g \in G} \alpha_g g \in RG,$$

definimos

$$\widetilde{\alpha}_g = \sum_{h \sim g} \alpha_h,$$

onde $\sim$ denota a conjugação em G, isto é, $h = aga^{-1}$, para algum $a \in G$.

Lema 2.1 *Sejam G um grupo e R um anel comutativo. Então*:

1 *(RG, RG) é gerado por todas as combinações lineares de (g, h), $g, h \in G$;*

2 *Seja $\alpha \in (RG, RG)$. Então $\widetilde{\alpha}_g = 0$, para todo $g \in G$. Em particular, $\alpha_z = 0$, para todo $z \in \mathcal{Z}(G)$.*

Prova. 1) Sejam

$$\beta = \sum_{g \in G} \beta_g g, \gamma = \sum_{g \in G} \gamma_g g \in RG.$$

Então

$$\begin{aligned} (\beta, \gamma) &= \left(\sum_{g \in G} \beta_g g, \sum_{h \in G} \gamma_h h \right) \\ &= \sum_{g,h \in G} \beta_g \gamma_h (g, h) \\ &= \sum_{g,h \in G} \beta_g \gamma_h (gh - hg). \end{aligned}$$

2) Seja $\alpha \in (RG, RG)$. Então

$$\alpha = \sum_{g,h \in G} \alpha_{gh} (gh - hg).$$

Como

$$g(hg) = (gh) g \Rightarrow hg = g^{-1} (gh) g,$$

temos que

$$\widetilde{\alpha}_g = 0, \forall g \in G.$$

■

Seja $\varphi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ um isomorfismo de anéis de grupos. Dizemos que φ é um *isomorfismo normalizado* se

$$\varepsilon_H \circ \varphi = \varepsilon_G,$$

isto é, se o seguinte diagrama comuta

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{\varphi} & \mathbb{Z}H \\ \varepsilon_G \searrow & & \swarrow \varepsilon_H \\ & \mathbb{Z} & \end{array}$$

A aplicação

$$\varphi^*\left(\sum_{g\in G}\alpha_g g\right) = \sum_{g\in G}\alpha_g \varepsilon\left(\varphi\left(g\right)\right)^{-1}\varphi\left(g\right)$$

é um isomorfismo normalizado. De fato,

$$\begin{aligned} \varepsilon \circ \varphi^*(\alpha) &= \varepsilon\left(\varphi^*\left(\sum_{g\in G}\alpha_g g\right)\right) \\ &= \varepsilon\left(\sum_{g\in G}\alpha_g \varepsilon\left(\varphi\left(g\right)\right)^{-1}\varphi\left(g\right)\right) \\ &= \sum_{g\in G}\alpha_g \varepsilon\left(\varphi\left(g\right)\right)^{-1}\varepsilon\left(\varphi\left(g\right)\right) \\ &= \sum_{g\in G}\alpha_g \\ &= \varepsilon(\alpha), \forall \alpha \in \mathbb{Z}G. \end{aligned}$$

Note que, como $g \in G$ é uma unidade de $\mathbb{Z}G$ e ε é um homomorfismo sobrejetor temos que $\varepsilon\left(g\right)$ é uma unidade em $\mathbb{Z}$. Nesta dissertação, salvo menção explícita em contrário, todos os isomorfismo considerados são os normalizados.

Proposição 2.2 *[17] Seja G um grupo finito e H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então, $\mathcal{Z}\left(G\right) \simeq \mathcal{Z}\left(H\right)$.* ■

Sejam G um grupo, R um anel comutativo e

$$\{C_i\}_{i\in I}$$

o *conjunto das classes de conjugação* de G, o qual contém somente um número finito de elementos. Para cada $i \in I$, o conjunto

$$\gamma_i = \widehat{C}_i = \sum_{x\in C_i} x$$

é chamado *soma de classe* de G sobre R.

Teorema 2.2 *[17] Sejam G, H grupos finitos e $\varphi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ um isomorfismo. Sejam $\{\gamma_i\}_{i\in I}$ e $\{\delta_j\}_{j\in J}$ as somas das classes de G e H, respectivamente. Então para cada γ_i, existe um único δ_j tal que $\varphi(\gamma_i) = \delta_j$.* ■

Teorema 2.3 *Sejam G um grupo e*

$$\mathfrak{L}(G) = \{N : N \trianglelefteq G \ \ e \ \ |N| < \infty\}$$

o reticulado de subgrupos normais finitos de G. Se $\mathbb{Z}G = \mathbb{Z}H$, então existe uma função

$$\begin{array}{rccc} \varphi: & \mathfrak{L}(G) & \rightarrow & \mathfrak{L}(H) \\ & N & \mapsto & \varphi(N) \end{array}$$

tal que:

1. *Se $N_1 \leq N_2$, então $\varphi(N_1) \leq \varphi(N_2)$;*
2. *$|N| = |\varphi(N)|$;*
3. *$\Delta(G, N) = \Delta(H, \varphi(N))$;*
4. *$\mathbb{Z}\left(\frac{G}{N}\right) \simeq \mathbb{Z}\left(\frac{H}{\varphi(N)}\right)$.* ■

2.3 Resultados sobre Anéis de Grupos

Proposição 2.3 (Berman-Higman) *Sejam G um grupo de ordem n e $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{Z}G$, tal que $\alpha^m = 1$. Se $\alpha_1 \neq 0$, então $\alpha = \pm 1$.*

Prova. Sejam $\rho_R : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ a representacão regular e $\rho_R^* : \mathbb{C}G \longrightarrow M_n(\mathbb{C})$. A extensão de ρ_R a $\mathbb{C}G$,

$$\rho_R^*(\beta) = \rho_R^*\left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G} \beta_g \rho_R(g).$$

Em particular,

$$\rho_R^*(\alpha) = \sum_{g\in G} \alpha_g \rho_R(g).$$

Sendo $\rho_R(g)$ uma matriz de permutação temos que

$$\mathrm{tr}(\rho_R(g)) = \begin{cases} 0 & \text{se } g \neq 1 \\ |G| & \text{se } g = 1. \end{cases}$$

Assim, se $g = 1$, então $\mathrm{tr}\left(\rho_R^*(\alpha)\right) = \alpha(1)\, n$. Como $\alpha^m = 1$ temos que $\rho_R^*(\alpha)$ é raiz do polinômio $x^m - 1$. Logo, o polinômio minimal é divisor de $x^m - 1$. Como $x^m - 1$ se decompõe em $\mathbb{C}[x]$ em fatores lineares distintos temos que $\rho_R^*(\alpha)$ é diagonalizável e sua matriz é semelhante a

$$A = \begin{pmatrix} \epsilon_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \epsilon_n \end{pmatrix}.$$

Logo,

$$\mathrm{I} = A^m = \begin{pmatrix} \epsilon_1^m & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \epsilon_n^m \end{pmatrix},$$

onde ϵ_i, $1 \leq i \leq n$, são raízes m-ésimas da unidade. Assim,

$$n\alpha(1) = \mathrm{tr}\left(\rho_R^*(\alpha)\right) = \epsilon_1 + \cdots + \epsilon_n$$

$$\Rightarrow |\alpha(1)| = \frac{\left|\sum_{i=1}^{n} \epsilon_i\right|}{n} \leq \frac{\sum_{i=1}^{n} |\epsilon_i|}{n} \leq 1.$$

Sendo $0 \neq \alpha(1) \in \mathbb{Z}$, obtemos a igualdade e, assim,

$$\epsilon_1 = \epsilon_2 = \cdots = \epsilon_n.$$

Logo, $\epsilon_1 = \alpha(1) = \pm 1$ e o polinômio característico de $\rho_R^*(x)$ é

$$(x - \epsilon_1)(x - \epsilon_1)\cdots(x - \epsilon_1) = (x - \epsilon_1)^n$$

e o polinômio minimal é um divisor comum entre

$$x^m - 1 \text{ e } (x - \epsilon_1)^n,$$

isto é, $m(x) = x - \epsilon_1$. Logo,

$$0 = m\left(\rho_R^*(\alpha)\right) = \rho_R^*(\alpha) - \epsilon_1 \mathrm{I} \Rightarrow \rho_R^*(\alpha) = \pm 1\, \mathrm{I}.$$

Como ρ_R^* é injetora temos que $\alpha = \pm 1$. ■

Teorema 2.4 [19]*Sejam G um grupo abeliano finito e H um grupo tal que*

$$\mathbb{Z}G \simeq \mathbb{Z}H.$$

Então $G \simeq H$. ■

Corolário 2.1 *Sejam* $\alpha \in \mathbb{Z}G, \alpha^m = 1$ *e* $\alpha \neq \pm 1$. *Então* $\alpha_1 = 0$. ■

Corolário 2.2 *Seja* A *um grupo abeliano finito. Então* $\mathcal{U}(T(\mathbb{Z}A)) = \pm A$.

Prova. Suponhamos que $\alpha \in \mathbb{Z}A, \alpha^n = 1$ e $\alpha(g_0) \neq 0$, para algum $g_0 \in A$. Como A é abeliano temos que $\left(\alpha g_0^{-1}\right)^{nk} = 1$, com $g_0^k = 1$. Além disso, $\left(\alpha g_0^{-1}\right)(1) = \alpha(g_o) \neq 0$. Assim, pela Proposição 2.3 temos que $\alpha g_0^{-1} = \pm 1$. Portanto, $\alpha = \pm g_0$. ■

Corolário 2.3 *Seja* G *um grupo finito. Então* $\mathcal{U}(T(\mathcal{Z}(\mathbb{Z}G))) = \pm \mathcal{Z}(G)$. ■

Lema 2.2 *Seja* H *subgrupo finito de* $\mathcal{U}_1(\mathbb{Z}G)$. *Então* H *é um conjunto linearmente independente.*

Prova. Suponhamos que

$$H = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{U}_1(\mathbb{Z}G) \text{ e } c_1\alpha_1 + \cdots + c_n\alpha_n = 0, \text{ com } c_i \in \mathbb{Z}.$$

Multiplicando esta última expressão por α_1^{-1}, obtemos

$$c_1 + c_2\left(\alpha_2^{-1}\alpha_1\right) + \cdots + c_n\left(\alpha_n^{-1}\alpha_1\right) = 0.$$

Como H é um grupo finito temos que $\alpha_i^{-1}\alpha_1 = \mu_i \in H$ é de ordem finita e

$$c_1 + c_2\mu_2 + \cdots + c_n\mu_n = 0.$$

Seja

$$\mu_i = \sum_{g \in G} \mu_{ig} g.$$

Então $\mu_i \neq 1$. Pelo Corolário 2.1, obtemos $\mu_{i1} = 0$ e, assim, $c_i = 0, \forall i$. Portanto H é um conjunto linearmente independente. ■

Lema 2.3 *Seja* H *um subgrupo de* $\mathcal{U}_1(\mathbb{Z}G)$ *tal que* $|H| = |G|$. *Então* $\mathbb{Z}G = \mathbb{Z}H$.

Prova. Claramente $\mathbb{Z}H \subseteq \mathbb{Z}G$. Pelo Lema 2.2, H é linearmente independente e, assim, $\mathbb{Q}G = \mathbb{Q}H$. Logo,

$$n\mathbb{Z}G \subseteq \mathbb{Z}H, \text{ para algum } n \in \mathbb{N}.$$

Seja $g \in G$. Então

$$ng = \sum z_i h_i, z_i \in \mathbb{Z} \text{ e } h_i \in H.$$

Afirmação. Cada z_i é um múltiplo de n.

De fato, como

$$ngh_i^{-1} = \sum z\left(h_j h_i^{-1}\right) = z_i + \sum_{i \neq j} z_i\left(h_j h_i^{-1}\right) \text{ e } h_j h_i^{-1} \neq \pm 1$$

temos, pelo Corolário 2.1, que $\left(h_j h_i^{-1}\right)(1) = 0$. Assim,

$$ngh^{-1}(1) = z_i.$$

Logo, z_i é um múltiplo de n. Portanto, $\mathbb{Z}G = \mathbb{Z}H$. ■

Lema 2.4 *Seja G um grupo ordenado. Então $\mathcal{U}_1(\mathbb{Z}G) = \pm G$.*

Prova. Suponhamos que

$$u = \sum_{i=1}^{t} u_i g_i, u^{-1} = \sum_{i=1}^{l} v_i h_i \in \mathcal{U}_1(\mathbb{Z}G),$$

com

$$g_1 < g_2 < \cdots < g_t \text{ e } h_1 < h_2 < \cdots < h_l.$$

Multiplicando u por u^{-1}, obtemos

$$\begin{aligned} 1 &= uu^{-1} \\ &= \left(\sum_{i=1}^{t} u_i g_i\right)\left(\sum_{i=1}^{l} v_i h_i\right) \\ &= \sum_{i=1}^{t}\sum_{j=1}^{l} u_i v_j g_i h_j \\ &= u_1 v_1 g_1 h_1 + \cdots + u_t v_l g_t h_l, \end{aligned}$$

com $g_1 h_1$ o menor e $g_t h_l$ o maior dos produtos $\{g_i h_j\}$. Assim,

$$g_1 h_1 = 1 = g_t h_l \Rightarrow h_1 = g_1^{-1} \text{ e } h_l = g_t^{-1}.$$

Por outro lado,

$$g_1 < g_t \Rightarrow g_1^{-1} > g_t^{-1}.$$

Logo,

$$h_1 = g_1^{-1} \text{ e } h_l = g_t^{-1} \Rightarrow h_1 > h_l,$$

o que é uma contradição. Portanto, $\mathcal{U}_1(\mathbb{Z}G) = \pm G$. ■

Lema 2.5 *Seja G um grupo nilpotente livre de torção. Então $\mathcal{U}(\mathbb{Z}G) = G$.*

Prova. Suponhamos que

$$u \in \mathcal{U}(\mathbb{Z}G) \text{ e } G_0 = \langle \operatorname{supp}(u) \rangle .$$

Logo, $u \in \mathbb{Z}G_0$. Como G_0 é finitamente gerado, nilpotente e $T(G_0) = \{1\}$ temos que G_0 é um grupo ordenado. Portanto, pelo Lema 2.4 obtemos $u \in G_0$. ■

Lema 2.6 *Sejam R um domínio de característica 0, G e H grupos abelianos livres de torção de posto n e m, respectivamente, e $\rho : RG \to RH$ um homomorfismo de anéis sobrejetor. Então $n \geq m$.* ■

Teorema 2.5 [11] *Seja G um grupo nilpotente finitamente gerado. Suponhamos que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então H é nilpotente finitamente gerado e $T(G) \simeq T(H)$.* ■

Teorema 2.6 [7] *Sejam G um grupo tal que $T(G)$ seja um subgrupo finito e $\frac{G}{T(G)}$ um grupo ordenado. Então dado $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, existem $v \in \mathbb{Z}T(G)$ e $g \in G$ tais que $u = vg$. Além disso, existe um inteiro positivo n tal que $g^n, v^n \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$.* ■

Corolário 2.4 *Seja G como no Teorema 2.6. Então $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \pm\mathcal{Z}(G)$ se, e somente se, $\mathcal{U}_1(\mathbb{Z}T(G)) \cap \mathcal{Z}(\mathbb{Z}G) \subseteq T(G)$.*

Prova. Suponhamos que

$$\mathcal{U}_1(\mathbb{Z}T(G)) \cap \mathcal{Z}(\mathbb{Z}G) \subseteq T(G).$$

Dado

$$u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)),$$

queremos provar que $u \in \mathcal{Z}(G)$. Se $o(u) < \infty$, então pelo Corolário 2.3 $u \in \pm\mathcal{Z}(G)$. Caso contrário, pelo Teorema 2.6, podemos escrever

$$u = vg \text{ com } v \in \mathbb{Z}T(G) \text{ e } g \in G,$$

e, ainda, pelo Teorema 2.6, existe $n \in \mathbb{Z}$ tal que $v^n \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$. Assim,

$$v^n \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) \cap \mathbb{Z}T(G) = \mathcal{U}_1(\mathbb{Z}T(G)) \cap \mathcal{Z}(\mathbb{Z}G).$$

Por hipótese, $v^n \in T(G)$. Como $T(G)$ é um subgrupo finito temos que existe $r \in \mathbb{N}$ tal que $(v^n)^r = (v)^{nr} = 1$. Seja $m = o(v)$. Então

$$u^m = (vg)^m = v^m g^m = g^m.$$

Como $o(u) = \infty$ temos que $A = \langle u^m \rangle$ é cíclico infinito. Seja

$$\pi : \mathbb{Z}G \longrightarrow \mathbb{Z}\left(\frac{G}{A}\right).$$

Então $\pi(u) \in \mathcal{U}(T(\mathbb{Z}\left(\frac{G}{A}\right)))$. Como u é central temos que $\pi(u)$ é central e de torção. Pelo Corolário 2.3, temos que $\pi(u), \pi(v) \in T\left(\mathcal{Z}\left(\frac{G}{A}\right)\right)$. Logo,

$$|\mathrm{supp}(\overline{v})| = 1.$$

Sendo A livre de torção obtemos, pelo Lema 1.3, que $\pi|_{T(G)}$ é injetora. Assim,

$$|\mathrm{supp}(v)| = |\mathrm{supp}(\overline{v})| = 1.$$

Portanto, v é uma unidade trivial, isto é, $u \in \pm\mathcal{Z}(G)$.

A recíproca é imediata. ■

Corolário 2.5 *Sejam G e $u = vg$ como no Teorema 2.6. Então*

$$v \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}T(G))}(T(G)).$$

Se

$$\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}T(G))}(T(G)) = \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G)))\,T(G),$$

então podemos tomar

$$v \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G))) \quad \textit{e neste caso } g \in \mathcal{Z}(\mathcal{C}_G(T(G))).$$

Prova. Como $u = vg \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$ temos que

$$\begin{aligned} uT(G) &= T(G)u \\ &\Rightarrow u^{-1}T(G)u = T(G) \\ &\Rightarrow (vg)^{-1}T(G)(vg) = T(G) \\ &\Rightarrow g^{-1}v^{-1}T(G)vg = T(G) \\ &\Rightarrow v^{-1}T(G)v = gT(G)g^{-1} = T(G), \end{aligned}$$

pois $T(G) \trianglelefteq G$. Portanto, $v \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}T(G))}(T(G))$. Finalmente, se

$$\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}T(G))}(T(G)) = \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G)))\,T(G),$$

então podemos escrever

$$v = v_1 t, \text{ com } t \in T(G) \text{ e } v_1 \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G))).$$

Isto prova que neste caso podemos tomar $v \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G)))$. Como

$$u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) \text{ e } v \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G)))$$

temos que $g = uv^{-1}$ centraliza $T(G)$. Além disso, se

$$g_1 \in \mathcal{C}_G(T(G)),$$

então

$$vg_1g = (vg_1)g = (g_1v)g = g_1(vg) = g_1u = ug_1 = vgg_1.$$

Assim,

$$g_1g = gg_1.$$

Portanto, $g \in \mathcal{Z}(\mathcal{C}_G(T(G)))$. ■

Lema 2.7 *A condição* $\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G) = \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))G$ *é equivalente a* $\mathrm{Aut}_{\mathbb{Z}}(G) = \mathrm{Inn}(G)$, *onde* $\mathrm{Aut}_{\mathbb{Z}}(G)$ *é o grupo dos automorfismo de* G, *que são induzidos por conjugação com unidades normalizadas.*

Prova. Queremos provar que

$$u \in G\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) \Leftrightarrow \varphi_u \in \mathrm{Inn}\,G, \text{ onde } \varphi_u(\alpha) = u^{-1}\alpha u.$$

Dado $u \in G\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, existem $g_0 \in G$ e $z \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$ tais que $u = g_0z$. Logo,

$$\begin{aligned}
\varphi_u(g) &= u^{-1}gu \\
&= (g_0z)^{-1}g(g_0z) \\
&= z^{-1}\left(g_0^{-1}gg_0\right)z \\
&= \left(g_0^{-1}gg_0\right)z^{-1}z \\
&= g_0^{-1}gg_0 \\
&= \varphi_{g_0}(g), \forall g \in G.
\end{aligned}$$

Portanto, $\varphi_u(g) = \varphi_{g_0}(g)$, isto é, $\varphi_u \in \mathrm{Inn}\,G$. Reciprocamente, suponhamos que $\varphi_u \in \mathrm{Inn}\,G$, isto é, existe um $g_0 \in G$ tal que

$$\varphi_u(g) = \varphi_{g_0}(g), \forall g \in G.$$

Então,

$$u^{-1}gu = \varphi_u(g) = \varphi_{g_0}(g) = g_0^{-1}gg_0$$

$$\Rightarrow \quad g = g_0 u^{-1} g u g_0^{-1}$$
$$\Rightarrow \quad g = \left(u g_0^{-1}\right)^{-1} g \left(u g_0^{-1}\right), \forall g \in G.$$

Fazendo $ug_0^{-1} = z \in \mathcal{U}_1(\mathbb{Z}G)$, segue que

$$g = z^{-1} g z, \forall g \in G \Rightarrow zg = gz, \forall g \in G \Rightarrow z \in \mathcal{Z}\left(\mathcal{U}_1(\mathbb{Z}G)\right).$$

Portanto,

$$u = g_0 z \in G\mathcal{Z}\left(\mathcal{U}_1(\mathbb{Z}G)\right).$$

■

Teorema 2.7 *Sejam p um número primo e P um p-subgrupo finito de um grupo G. Então para qualquer $u \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G)$, existe $x \in \mathrm{supp}(u)$ tal que $u^{-1}gu = x^{-1}gx$, para todo $g \in P$.*

Prova. Sejam $u \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G)$ e $X = \mathrm{supp}(u)$. Então $\varphi(g) = u^{-1}gu \in G$ e $gu = u\varphi(g)$, para todo $g \in G$. Fazendo

$$u = \sum_{h \in G} u(h)h,$$

obtemos

$$gu = \sum_{h \in G} u(h)gh = \sum_{h \in G} u(h)h\varphi(g).$$

Logo, para todo $x \in X$, existe um único $\psi_g(x) \in X$ tal que

$$\psi_g(x) = g^{-1}x\varphi(g)$$

e a função $u : X \to \mathbb{Z}$ dada por $x \to u(x)$ é constante nas órbitas desta ação. Restringindo esta ação a P, obtemos que $|O(x)|$ divide $|P|$, para todo $x \in X$. Portanto, $|O(x)|$ é uma potência de p ou 1. Assim, se $z \in O(x)$ então $u(z) = u(x)$. Como

$$X = \dot{\bigcup_{x_i \in X}} O(x_i)$$

temos que

$$\begin{aligned} u &= \sum u(x)x \\ &= \sum \sum_{z \in O(x_i)} u(z)z. \end{aligned}$$

Logo,

$$\pm 1 = \varepsilon(u) = \sum \sum_{z \in O(x_i)} u(z) = \sum u(x_i)\left|O(x_i)\right| = \sum u(x_i)p^{r_i},$$

onde $p^{r_i} = |O(x_i)|$, $r_i \geq 0$. Portanto,

$$1 = \sum u(x_i)p^{r_i}.$$

Assim, existe $r_{i_0} = 0$, caso contrário $p \mid \pm 1$, isto é, $|O(x_i)| = p^{r_{i_0}} = 1$. Logo,

$$O(x_{i_0}) = \{\psi_g(x_{i_0}) : g \in P\} = \{x_{i_0}\}, \forall g \in P.$$

Assim, $gx_{i_0} = \psi_g(x_{i_0})\varphi_u(g)$ e

$$\varphi_u(g) = x_{i_0}^{-1} g x_{i_0}, \forall g \in P.$$

Portanto, tomando $x = x_{i_0}$, obtemos $u^{-1}gu = x^{-1}gx$, *para todo* $g \in P$. ■

Corolário 2.6 *Seja G um grupo finito nilpotente. Então*

$$\mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))\, G.$$

Prova. Pelo Teorema 1.12 temos que $G = \Pi P_i$, onde P_i, é o p_i-subgrupos de Sylow. Seja

$$u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G).$$

Então pelo Teorema 2.7, existe $x_i \in G$ tal que

$$u^{-1}gu = x_i^{-1} g x_i \ , \forall g \in P_i.$$

Sendo G nilpotente e $g \in P_i$ pode-se tomar x_i em P_i. Então

$$u^{-1}gu = x^{-1}gx, \forall g \in G \text{ com } x = \Pi x_i,$$

pois x_i comuta com x_j. Assim,

$$\begin{aligned} gu &= ux^{-1}gx, \forall g \in G \\ &\Rightarrow gux^{-1} = ux^{-1}g, \forall g \in G \\ &\Rightarrow g\left(ux^{-1}\right) = \left(ux^{-1}\right) g, \forall g \in G \\ &\Rightarrow ux^{-1} \in \mathcal{Z}(G) \\ &\Rightarrow ux^{-1} \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G)). \end{aligned}$$

Logo,

$$u = u\left(x^{-1}x\right) = \left(ux^{-1}\right) x \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))\, G$$

e, assim,

$$\mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G) \subseteq \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))\, G.$$

A outra inclusão é imediata. Portanto,

$$\mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))\, G.$$

■

Proposição 2.4 *Sejam G um grupo arbitrário e $u \in \mathcal{U}_1$. Então $u \in \mathcal{N}_{\mathcal{U}_1}(G)$ se, e somente se, $uu^* \in \mathcal{Z}(\mathbb{Z}G)$.* ■

Proposição 2.5 (Krempa) *Seja G um grupo. Se $u \in \mathcal{N}_{\mathcal{U}_1}(G)$, então $u^2 = g_0(u^*u) \in G\mathcal{Z}(\mathbb{Z}G)$, para algum $g_0 \in G$, isto é, o automorfismo de G determinado pela conjugação com u^2 é interno.*

Prova. Suponhamos $u \in \mathcal{N}_{\mathcal{U}_1}(G)$ e $\varphi \in \mathrm{Aut}_{\mathcal{U}_1}(G)$, tal que $\varphi(x) = u^{-1}xu$. Considere $v = u^*u^{-1} \in \mathcal{U}_1(\mathbb{Z}G)$. Assim,

$$vv^* = u^*u^{-1}(u^{-1})^*u = u^*(u^*u)^{-1}u = u^*u(u^*u)^{-1} = 1$$

e temos $\varepsilon(v) = 1$. Assim, $v = g_0$, para algum $g_0 \in G$. Consequentemente, $g_0 = u^*u^{-1}$. Logo, $u^* = g_0u$ e $g_0u^2 = u^*u = c \in \mathcal{Z}(\mathbb{Z}G)$. Mas,

$$\varphi^2(x) = \varphi(\varphi(x)) = \varphi(u^{-1}xu) = u^{-2}xu^2 = c^{-1}g_0xg_0^{-1}c = g_0xg_0^{-1}, \forall x \in G$$

isto é, $\varphi^2 \in \mathrm{Inn}(G)$. ■

Teorema 2.8 (Krempa) *Seja G um grupo de ordem ímpar. Então*

$$\mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))\, G.$$

Prova. Sejam $|G| = s$ ímpar e $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G)$. Seja $\varphi \in \mathrm{Aut}(G)$ dado por

$$\varphi(g) = u^{-1}gu, \forall g \in G.$$

Pela Proposição 2.5, obtemos que φ^2 é um automorfismo interno e $\varphi^s = \mathrm{Id}$. Como $\mathrm{mdc}(s, 2) = 1$ temos que existem $l, t \in \mathbb{Z}$ tais que $2l + st = 1$. Logo,

$$\varphi = \varphi^1 = \varphi^{2l+st} = (\varphi^2)^l(\varphi^s)^t = \varphi^{2l} = (\varphi^l)^2 \Rightarrow \varphi \in \mathrm{Inn}(G).$$

Assim,

$$\mathrm{Aut}_{\mathbb{Z}}(G) = \mathrm{Inn}(G).$$

Pelo Lema 2.7,

$$\mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))\,G.$$

■

Corolário 2.7 *Sejam G um grupo como no Teorema 2.6 e*

$$\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G).$$

Se $H \subseteq \mathcal{U}_1(\mathbb{Z}G)$ é outra base para $\mathbb{Z}G$, então $\mathcal{Z}(H) = \mathcal{Z}(G)$.

Prova. Seja

$$\varphi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$$

um isomorfismo. Então, pelo Teorema 2.3, obtemos

$$\Delta(G, T(G)) = \Delta(H, T),$$

para algum subgrupo normal $T = \varphi(T(G))$ de H com $|T| = |T(G)|$ e, portanto, T é finito. Assim, pelo Teorema 2.1, obtemos

$$\mathbb{Z}\left(\frac{G}{T(G)}\right) \simeq \frac{\mathbb{Z}G}{\Delta(G, T(G))} = \frac{\mathbb{Z}H}{\Delta(H, T)} \simeq \mathbb{Z}\left(\frac{H}{T}\right)$$

e, assim, $\mathbb{Z}\left(\frac{H}{T}\right)$ é um domínio, pois $\frac{H}{T}$ é nilpotente livre de torção. Logo, $T = T(H)$. Pelo Lema 2.4, temos que as unidades de

$$\mathbb{Z}\left(\frac{G}{T(G)}\right)$$

são triviais. Assim,

$$\frac{G}{T(G)} \simeq \frac{H}{T(H)}.$$

Em particular, $\frac{H}{T(H)}$ é ordenado. Se $u \in \mathcal{Z}(G)$, então $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}H))$, pois H é outro grupo base. Se $o(u) < \infty$, então pelo Corolário 2.3 temos que $u \in \mathcal{Z}(H)$. Caso contrário, pelo Teorema 2.6, podemos escrever

$$u = vh \text{ com } v \in \mathbb{Z}T(H) \text{ e } h \in H$$

e existe um inteiro n tal que

$$v^n \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}H)) \subseteq \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G).$$

Logo,

$$v^n \in \mathcal{Z}(G) \cap \mathbb{Z}T(H) = \mathcal{Z}(T(H)).$$

Como $s = |T(H)|$ temos que $v^{ns} = 1$. Seja $o(v) = m$. Então

$$u^m = (vh)^m = v^m h^m = h^m \Rightarrow h^m \in \mathcal{Z}(G).$$

Sejam

$$A = \langle h^m \rangle \text{ e } \pi : \mathbb{Z}G \longrightarrow \mathbb{Z}\left(\frac{G}{A}\right).$$

Note que

$$\Delta(G, A) = \Delta(H, A) \text{ e } \overline{H} = \pi(H) \subseteq \mathbb{Z}\left(\frac{G}{A}\right) \text{ é uma base para } \mathbb{Z}G.$$

Sendo $u \in \mathcal{Z}(G)$ obtemos que $\pi(u)$ é central e de torção. Pelo Corolário 2.3, temos que $\pi(u) \in \overline{H}$. Logo, $\overline{v} \in \overline{H}$ e, portanto,

$$|\text{supp}(\overline{v})| = 1.$$

Sendo A livre de torção e $T(H)$ um subgrupo de H pelo Lema 1.3, obtemos que $\pi|_{T(H)}$ é injetora. Logo

$$|\text{supp}(v)| = |\text{supp}(\overline{v})| = 1.$$

Logo, v é uma unidade trivial e, portanto, $u \in \mathcal{Z}(H)$. Assim,

$$\mathcal{Z}(G) \subseteq \mathcal{Z}(H).$$

Por outro lado,

$$u \in \mathcal{Z}(H) \Rightarrow uh = hu, \forall h \in H.$$

Em particular,

$$u\alpha = \alpha u, \forall \alpha \in \mathcal{U}_1(\mathbb{Z}G) \Rightarrow u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G).$$

Logo, $\mathcal{Z}(H) \subseteq \mathcal{Z}(G)$. Portanto, $\mathcal{Z}(G) = \mathcal{Z}(H)$. ■

2.4 Subgrupo de Dimensão

Veremos agora a definição de Subgrupo de Dimensão que será necessária para o desenvolvimento do próximo capítulo.

Sejam G um grupo e

$$\gamma_1(G) \supseteq \gamma_2(G) \supseteq \cdots \supseteq \gamma_i(G) \supseteq \cdots$$

a sua série central descendente (inferior). Como

$$\begin{aligned} x^{-1}y^{-1}xy - 1 &= x^{-1}y^{-1}(xy - yx) \\ &= x^{-1}y^{-1}[(x-1)(y-1) - (y-1)(x-1)] \end{aligned}$$

temos que

$$\gamma_2(G) - 1 \subseteq \Delta^2(G).$$

De modo indutivo, obtemos que

$$\gamma_n(G) - 1 \subseteq (\Delta^n(G)).$$

Logo,

$$\gamma_n(G) \subseteq (1 + \Delta^n(G)), \forall n \in \mathbb{N}.$$

O subgrupo

$$D_n(G) = G \cap (1 + \Delta^n(G)), \forall n \in \mathbb{N}$$

é chamado *n-ésimo subgrupo de dimensão*. É fácil ver que $D_n(G)$ é normal em G. Portanto, obtemos a série normal

$$G = D_1(G) \supseteq D_2(G) \supseteq \cdots \supseteq D_n(G) \supseteq \cdots$$

Além disso,

$$\gamma_n(G) \subseteq D_n(G), \forall n \in \mathbb{N}.$$

É verificado que

$$D_n(G) = \gamma_n(G),$$

para $n = 1, 2, 3$ e para $n = 4$ se $|G|$ é ímpar. Porém em geral $D_n(G) \supsetneq \gamma_n(G)$.

Capítulo 3

O Problema do Isomorfismo

Este capítulo trata do problema de isomorfismo para anéis de grupos sobre os inteiros de grupos infinitos, e é dividido em três seções. Na primeira seção respondemos a questão do Mazur, dando condições para que o problema do isomorfismo seja válido para anéis de grupos sobre os inteiros, onde os grupos são da forma $G = N \times A$, com N um grupo finito e A um grupo abeliano livre finitamente gerado. Nessa seção também mostramos que o problema do isomorfismo para anéis de grupos sobre os inteiros de grupos infinitos é bastante relacionado com a conjectura do normalizador. Na segunda seção informamos sobre a conjectura do automorfismo com o propósito de construir diferentes bases de grupo para o anel de grupo sobre os inteiros de grupos infinitos. Finalmente, na terceira seção, respondemos parcialmente o problema de Sehgal, isto é, mostramos que as classes de nilpotência de um grupo G finitamente gerado é determinada por seu anel de grupo sobre os inteiros, contanto que G tenha somente torção ímpar. Quando G tem classe de nilpotência 2, então não é nescessária nenhuma restrição. Portanto, junto com um resultado de Ritter e Sehgal, estabelecemos o problema do isomorfismo para grupos nilpotentes finitamente gerados de classe 2. Além disso, ressaltamos uma ligação entre este problema e o do subgrupo de dimensão.

3.1 Isomorfismo de Produto Direto

Nesta seção provamos o problema de isomorfismo para algumas classes de grupos policíclicos-por-finito e damos uma condição nescessária e suficiente para que este problema seja válido. Além disso, mostraremos como constuir contra-exemplos para o pro-

blema de isomorfismo de grupos infinitos.

Lema 3.1 *Seja $G = N_1 \times N_2$. Então G satisfaz à condição do normalizador se, e somente se, N_1 e N_2 satisfazem à condição do normalizador.*

Prova. Seja

$$\varphi_i : G \longrightarrow N_i, \varphi_i (n_1, n_2) = n_i, i = 1, 2.$$

É claro que

$$N_i \simeq \frac{G}{N_j}, N_i = \ker \varphi_j, i \neq j, \text{ e } \widehat{\varphi}_i : \mathbb{Z}G \longrightarrow \mathbb{Z}N_i$$

é um homomorfismo sobrejetor de $\mathbb{Z}G$ em $\mathbb{Z}N_i$. Suponhamos que G satisfaz à condição do normalizador e $u \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}N_1)}(N_1)$. Então u normaliza G, pois $G = N_1 \times N_2$ e, assim,

$$u = wg, \text{ para algum } g \in G \text{ e } w \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)).$$

Logo,

$$u = \varphi_1(u) = \varphi_1(wg) = \varphi_1(w)\varphi_1(g).$$

Portanto, N_1 satisfaz à condição do normalizador. De modo análogo, obtemos que N_2 também satisfaz à condição do normalizador.

Reciprocamente, suponhamos que N_1 e N_2 satisfazem à condição do normalizador e

$$u \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}G)}(G).$$

Seja $u_i = \varphi_i(u)$. Então

$$u_i \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}N_i)}(N_i),$$

pois φ_i é sobrejetora. Por hipótese, obtemos

$$u_i = w_i n_i, \text{ com } w_i \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}N_i)) \text{ e } n_i \in N_i.$$

Como $w_i \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}N_i))$ temos que

$$w_i \in \mathcal{Z}(\mathbb{Z}G),$$

pois $[N_1, N_2] = \{1\}$. Seja

$$w = uu_1^{-1}u_2^{-1}.$$

Afirmação: w é uma unidade central.

De fato, sejam

$$n \in N_i \text{ e } g = w^{-1}nw. \tag{3.1}$$

Como w normaliza G temos que $g \in G$. Por outro lado,

$$g - n = w^{-1}nw - n = \left(w^{-1}n, w\right).$$

Pela demonstração do Lema 2.1, obtemos que g e n são conjugados em G, isto é, existe $k \in G$ tal que

$$knk^{-1} = g \Longrightarrow g = n_i, \text{ pois } N_i \trianglelefteq G.$$

Logo, pela expressão 3.1, obtemos

$$w^{-1}N_iw = N_i.$$

Assim,

$$\begin{aligned} w^{-1}n_iw &= \varphi_i\left(w^{-1}n_iw\right) = n_i, \forall n_i \in N_i \\ &\Longrightarrow w^{-1}n_iw = n_i, \forall n_i \in N_i \\ &\Longrightarrow wn_i = n_iw, \forall n_i \in N_i. \end{aligned}$$

Portanto, w é uma unidade central.

Logo,

$$\begin{aligned} u &= u\left(u_1^{-1}u_1\right)\left(u_2^{-1}u_2\right) = uu_1^{-1}\left(u_1^{-1}u_2\right)u_2 = uu_1^{-1}\left(u_2^{-1}u_1\right)u_2 \\ &\Longrightarrow u = \left(uu_1^{-1}u_2^{-1}\right)u_1u_2 = wu_1u_2. \end{aligned}$$

Por hipótese, obtemos:

$$\begin{aligned} u &= w\left(w_1n_1\right)\left(w_2n_2\right) = w\left(w_1n_1\right)\left(n_2w_2\right) \\ &= ww_1\left[\left(n_1n_2\right)w_2\right] = ww_1\left[w_2\left(n_1n_2\right)\right] \\ &= \left(ww_1w_2\right)\left(n_1n_2\right), \end{aligned}$$

onde

$$ww_1w_2 \in \mathcal{Z}\left(\mathcal{U}_1\left(\mathbb{Z}G\right)\right) \text{ e } n_1n_2 \in G.$$

Portanto, G satisfaz a condição do normalizador. ■

Teorema 3.1 *Seja $G = N \times A$, onde N é finito e A é abeliano finitamente gerado não periódico. Suponhamos que o problema do isomorfismo vale para N. Então a condição do normalizador vale para N se, e somente se, o problema do isomorfismo vale para G.*

Prova. Sem perda de generalidade podemos supor que A é livre de torção. De fato, seja

$$A = B \times A_1,$$

com $B = T(A)$ e A_1 livre de torção. Assim,

$$G = N \times (B \times A_1) = (N \times B) \times A_1.$$

Logo,

$$G = N_1 \times A_1, \text{ onde } N_1 = N \times B.$$

Agora mostraremos que o problema do isomorfismo vale para N_1. Suponhamos

$$\phi : \mathbb{Z}N_1 \to \mathbb{Z}K$$

um isomorfismo. Pelo Teorema 2.3, existe $\phi(B) \subseteq K$ tal que

$$|\phi(B)| = |B|, \Delta(N_1, B) = \Delta(K, \phi(B)) \text{ e } \mathbb{Z}\left(\frac{N_1}{B}\right) \simeq \mathbb{Z}\left(\frac{K}{\phi(B)}\right).$$

Como $\mathbb{Z}\left(\frac{N_1}{B}\right) \simeq \mathbb{Z}N$ temos por hipótese que $N \simeq \frac{K}{\phi(B)}$. De maneira análoga, obtemos

$$\mathbb{Z}\left(\frac{N_1}{B}\right) \simeq \mathbb{Z}\left(\frac{K}{\phi(N)}\right).$$

Como $\mathbb{Z}B \simeq \mathbb{Z}\left(\frac{N_1}{B}\right)$ temos pelo Teorema 2.4 que $B \simeq \frac{K}{\phi(N)}$. Pelo Teorema 2.3 temos que

$$\{1\} = N \cap B \longrightarrow \phi(N) \cap \phi(B).$$

Logo, $\phi(N) \cap \phi(B) = \{1\}$. Como $\phi(N) \trianglelefteq K$ e $\phi(B) \trianglelefteq K$ temos que $K = \phi(N) \times \phi(B)$. Assim,

$$N \simeq \frac{K}{\phi(B)} \simeq \phi(N) \text{ e } B \simeq \frac{K}{\phi(N)} \simeq \phi(B).$$

Portanto, $K = \phi(N) \times \phi(B) \simeq N \times B = N_1$, isto é, o problema do isomorfismo vale para N_1. Como N e B satisfazem a condição do normalizador, pelo Lema 3.1 obtemos que

$$N_1 = N \times B$$

satisfaz a condição do normalizador. Por outro lado A_1 é livre de torção. Portanto, o problema do isomorfismo vale para G.

Suponhamos

$$\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}N)}(N) = \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}N))N$$

e $H \subseteq \mathcal{U}_1(\mathbb{Z}G)$ um grupo base para $\mathbb{Z}G$.

Seja

$$\theta : \mathbb{Z}G \longrightarrow \mathbb{Z}H$$

um isomorfismo. Como $N \trianglelefteq G$, pelo Teorema 2.3, temos que, existe

$$M \trianglelefteq H, \text{ com } |M| = |N|$$

tal que

$$\theta(N) = M \text{ e } \Delta(G, N) = \Delta(H, M).$$

Seja

$$\varphi : \mathbb{Z}G \longrightarrow \mathbb{Z}A,$$

um homomorfismo sobrejetor. Pelo Teorema 2.1, obtemos que

$$\mathbb{Z}A \simeq \frac{\mathbb{Z}G}{\Delta(G, N)}$$

é um domínio. Logo, $M = T(H)$. Seja

$$A = \langle x_1, x_2, \ldots, x_n \rangle,$$

com n o posto de A. Então, existem

$$y_1, y_2, \ldots, y_n \in H,$$

tais que

$$\frac{\mathbb{Z}G}{\Delta(G, N)} \simeq \mathbb{Z}\langle x_1, x_2, \ldots, x_n \rangle \simeq \mathbb{Z}\langle \overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n \rangle.$$

Pelo Corolário 2.5, podemos encontrar

$$v_i \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}M)) \text{ e } h_i \in \mathcal{Z}(\mathcal{C}_H(M)), 1 \leq i \leq n \text{ tal que } x_i = v_i h_i.$$

Como

$$\langle x_1, x_2, \ldots, x_n \rangle = \langle \overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n \rangle$$

são as unidades triviais de aumento em $\mathbb{Z}A \simeq \mathbb{Z}\left(\frac{H}{M}\right)$, podemos supor que cada $y_i = h_i$. Logo,

$$\langle y_1, y_2, \ldots, y_n \rangle$$

é um grupo abeliano finitamente gerado. Seja

$$\langle y_1, y_2, \ldots, y_n \rangle = T(\langle y_1, y_2, \ldots, y_n \rangle) \times B,$$

onde B é um grupo abeliano livre de posto n. Como

$$\frac{H}{M} = \overline{B} \text{ e } B \subseteq \mathcal{C}_H(M),$$

temos que $H = M \times B$. Para provar que $H \simeq G$, basta mostrar que $N \simeq M$. Seja

$$\varphi : \mathbb{Z}G \longrightarrow \mathbb{Z}N$$

um homomorfismo sobrejetor. Então pelos Lemas 1.3 e 2.3 temos que

$$\mathbb{Z}N = \mathbb{Z}\varphi(M).$$

Por hipótese, obtemos

$$N \simeq \varphi(M) \simeq M \text{ e, portanto, } G \simeq H.$$

Portanto, o problema do isomorfismo vale para G.

Para provar a recíproca exibiremos no Teorema 3.3 um contra-exemplo no caso onde G não satisfaz a condição do normalizador. ■

Corolário 3.1 *Seja $G = N \times A$, onde N é finito e A é abeliano livre finitamente gerado não trivial. Então o problema do isomorfismo vale para G se, e somente se, tanto a condição do normalizador quanto o problema do isomorfismo valem para N.*

Prova. Seja

$$\varphi : \mathbb{Z}N \longrightarrow \mathbb{Z}M$$

um isomorfismo de $\mathbb{Z}N$ em $\mathbb{Z}M$. Como

$$G = N \times A \text{ com } T(A) = \{1\}$$

temos que

$$\mathbb{Z}G = (\mathbb{Z}A)[N].$$

Além disso, φ induz um isomorfismo

$$\widehat{\varphi} : \mathbb{Z}G \longrightarrow (\mathbb{Z}A)[M] = \mathbb{Z}(A \times M),$$

tal que

$$\widehat{\varphi}|_{\mathbb{Z}A} = \mathrm{Id},$$

onde

$$\widehat{\varphi}(n) = \varphi(n), \forall n \in N.$$

Por hipótese, existe um isomorfismo de G em H, isto é,

$$\tau = \widehat{\varphi}|_G : G = N \times A \longrightarrow H = M \times A.$$

Pelo Lema 1.3, obtemos

$$\tau(N) \subseteq T(M \times A) = M \text{ e } \tau^{-1}(M) \subseteq T(N \times A) = N.$$

Assim,

$$\tau\left(\tau^{-1}(M)\right) \subseteq \tau(N) \Longrightarrow M \subseteq \tau(N).$$

Logo, $\tau(N) = M$ e, portanto,

$$N \simeq \tau(N) = M.$$

A recíproca é imediata, pelo Teorema 3.1. ■

Note que a prova do Teorema 3.1 dá muito pouca informação até mesmo sem a suposição da condição do normalizador. No contexto mais geral, obtemos somente que os elementos

$$v_i \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}M)}(M).$$

Teorema 3.2 *Sejam H um grupo e $G = N \times A$, onde N é um grupo finito e*

$$A = \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$$

é um grupo abeliano livre finitamente gerado. Então $\mathbb{Z}G \simeq \mathbb{Z}H$ se, e somente se, as seguintes condições são satisfeitas:

1. *$M = T(H)$ é um subgrupo e $\mathbb{Z}N \simeq \mathbb{Z}M$;*
2. *Existem $y_1, y_2, \ldots, y_n \in H$ tal que $\frac{H}{M} = \langle y_1 M \rangle \times \cdots \times \langle y_n M \rangle$ é abeliano livre de posto n;*
3. *Para cada i, existe $v_i \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}M)}(M)$ tal que $v_i y_i$ é um elemento central. Além disso, $\langle v_1 y_1, \ldots, v_n y_n \rangle \simeq A$.*

Prova. (Ver [7, Theorem 3.4].) ■

Agora mostraremos como construir contra-exemplos para o problema do isomorfismo para grupos infinitos.

Lema 3.2 *Sejam*

$$G = N \rtimes_{\sigma} \mathbb{Z} \ \ e \ \ H = N \rtimes_{\tau} \mathbb{Z},$$

onde N *é um grupo qualquer. Então* $G \simeq H$ *se, e somente se, existe* $\varphi \in \mathrm{Aut}\,(N)$ *tal que*

$$\varphi^{-1}\sigma\varphi \ \ e \ \ \tau$$

sejam iguais módulo $\mathrm{Inn}\,(N)$.

Prova. Segue pela demostração da Proposição 1.3. ■

Seja

$$G = N \times \langle z \rangle,$$

onde N é um grupo finito e $\langle z \rangle$ é um grupo cíclico infinito. Sejam $u \in \mathcal{N}_{\mathcal{U}_1(\mathbb{Z}N)}(N)$ e $\tau_u : N \to N$ um automorfismo dado por

$$\tau_u(n) = u^{-1}nu.$$

Dado $v = zu$. Se $n \in N$, então

$$\begin{aligned} v^{-1}nv &= (zu)^{-1} n (zu) \\ &= u^{-1}z^{-1}nzu \\ &= u^{-1}nz^{-1}zu \\ &= u^{-1}nu, \ \text{pois} \ z \in \mathcal{Z}(G). \end{aligned}$$

Logo,

$$v^{-1}nv = u^{-1}nu = \tau(n),$$

e, portanto,

$$H = N \rtimes_{\tau} \langle v \rangle \subseteq \mathcal{U}_1(\mathbb{Z}G), \langle N, v \rangle \simeq H.$$

■

Lema 3.3 *Seja* $H = N \rtimes_{\tau} \langle v \rangle$. *Então o grupo* H *é uma base para* $\mathbb{Z}G$.

Prova. Queremos provar que $H = N \rtimes_\tau \langle v \rangle = \langle N, v \rangle$ e $\mathbb{Z}H = \mathbb{Z}G$. De fato, suponhamos que

$$\begin{aligned} 0 &= \sum_{\substack{n\in N \\ k\in\mathbb{Z}}} c_{n,k} n v^k = \sum_{\substack{n\in N \\ k\in\mathbb{Z}}} c_{n,k} n (zu)^k = \sum_{\substack{n\in N \\ k\in\mathbb{Z}}} c_{n,k} n \left(z^k u^k\right) \\ &= \sum_{\substack{n\in N \\ k\in\mathbb{Z}}} c_{n,k} n u^k z^k, \text{ pois } z \in \mathcal{Z}(G) \\ \Longrightarrow\ 0 &= \sum_{\substack{n\in N \\ k\in\mathbb{Z}}} c_{n,k} n v^k = \sum_{\substack{n\in N \\ k\in\mathbb{Z}}} c_{n,k} n u^k z^k \in \mathbb{Z}N < z > . \end{aligned}$$

Como os elementos do $< z >$ são linearmente independentes sobre $\mathbb{Z}N$, obtemos

$$\sum_{n\in N} c_{n,k} n u^k = 0, \forall k \Rightarrow \left(\sum_{n\in N} c_{n,k} n\right) u^k = 0 \Rightarrow \sum_{n\in N} c_{n,k} n = 0, \forall k,$$

pois u^k é uma unidade. Como os elementos de N são linearmente independentes temos que

$$\sum c_{n,k} = 0, \forall n \in N \text{ e } k \in \mathbb{Z}.$$

Portanto, $\langle N, v \rangle$ é linearmente independente. Sejam

$$R = \mathbb{Z}\langle N, v \rangle, u \in \mathbb{Z}N \text{ e } z \in \mathcal{Z}(G).$$

Então $u \in R$. Logo,

$$u^{-1}v = u^{-1}(zu) = u^{-1}zu = zu^{-1}u = z \in \mathbb{Z}G.$$

Assim, $R \subseteq \mathbb{Z}G$. Por outro lado,

$$\mathbb{Z}G = \mathbb{Z}\langle N, z \rangle \subseteq R.$$

Portanto, $\mathbb{Z}H = \mathbb{Z}G$. ■

Observação 3.1 : *Sejam $G = N \times \langle z \rangle$ e $H = N \rtimes_\tau \langle v \rangle$. Então G é isomorfo a H se, e somente se, τ é interno.*

A prova desta, segue pela demonstração do Lema 2.7. ■

Teorema 3.3 *Seja N um grupo finito. Se*

$$\mathcal{N}_{\mathcal{U}_1(\mathbb{Z}N)}(N) \neq \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}N))N,$$

então o problema do isomorfismo não vale para $G = N \times \langle z \rangle$, com z de ordem infinita. Além disso, isto não vale para $G = N \times A$, onde A é um grupo abeliano fintamente gerado não periódico.

Prova. Um exemplo é o grupo de ordem $2^{21}97^{28}$ dado recentemente por Hertweck. O leitor interessado em maiores detalhes consulte [6, Pag. 115]. ■

3.2 Automorfismo de Produto Direto

Agora mostraremos como os resultados das seções anteriores dão informações sobre o automorfismo de certos anéis de grupo sobre os inteiros. O objetivo principal é a construção de diferentes grupos que são bases.

Lema 3.4 *Seja G um grupo e suponhamos que a conjectura do automorfismo vale para G. Se $H \subseteq \mathcal{U}_1(\mathbb{Z}G)$ é um grupo base que é isomorfo a G, então $\mathcal{Z}(G) = \mathcal{Z}(H)$.*

Prova. É imediato. ■

O próximo resultado dá um critério para um subgrupo ser linearmente independente sobre $\mathbb{Z}$.

Lema 3.5 *Sejam G um grupo residualmente finito, $N \subseteq \mathcal{U}_1(\mathbb{Z}G)$ um subgrupo e $H = \langle N, A\rangle$. Se $S = G \cap H$ tem índice finito em H, então H é linearmente independente sobre $\mathbb{Z}$.*

Prova. Suponhamos

$$\sum c_h h = 0,$$

com $c_h \in \mathbb{Z}$ e $c_h \neq 0$. Seja X a união do suporte (com respeito a G) de $h \in H$ aparecendo nesta soma. Como G e residualmente finito, existe um subgrupo normal M de índice finito em G tal que

$$\pi : \mathbb{Z}G \longrightarrow \mathbb{Z}\left(\frac{G}{M}\right)$$

é injetiva sobre X. Por outro lado,

$$M \trianglelefteq G \text{ e } S \leq G \Longrightarrow MS \leq G,$$

pelo Teorema 1.4, obtemos

$$\frac{MS}{M} \simeq \frac{S}{M \cap S}.$$

Como $M \leq MS \leq G$ temos que

$$[G : M] = [G : MS]\,[MS : M].$$

Assim, $[MS : M] < \infty$, pois $[G : M] < \infty$. Logo,

$$[S : M \cap S] < \infty.$$

Por hipótese,

$$[H : S \cap M] = [H : S]\,[S : S \cap M] < \infty,$$

Logo, $\pi(H)$ é finito. Pelo Lema 2.2, temos que $\pi(H)$ é linearmente independente e, assim, todo $c_h = 0$, o que é uma contradição. Portanto, H é linearmente independente. ■

Teorema 3.4 *Seja $G = N \times A$, onde N é finito e A é um grupo abeliano livre finitamente gerado não trivial. A conjectura do automorfismo vale para G se, e somente se, as seguintes condições são satisfeitas*:

1. $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G)$, *isto é,* $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}T(G)))$ *é trivial*;
2. *Subgrupos de* $\mathcal{U}_1(\mathbb{Z}G)$, *os quais são isomorfos a* N, *são racionalmente conjugados a* N.

Prova. Suponhamos que a conjectura do automorfismo vale para G. Pelo Corolário 2.4 para provar a propriedade 1 é suficiente mostrar que, dado

$$u \in \mathcal{U}_1(\mathbb{Z}N) \cap \mathcal{Z}(\mathbb{Z}G)$$

temos que $u \in N$. Suponhamos o contrário, isto é,

$$u \in \mathcal{U}_1(\mathbb{Z}N) \cap \mathcal{Z}(\mathbb{Z}G) \text{ tal que } u \notin N.$$

Pelo Corolário 2.3, as unidades centrais de torção são triviais. Logo, u é uma unidade não periódica. Sejam

$$A = A_1 \times < z > \text{ e } B = A_1 \times < uz >,$$

onde $A_1 \trianglelefteq A$ e $< z >$ é cíclico infinito. Pelo Lema 3.3, obtemos que $N \times B$ é um grupo base para $\mathbb{Z}G$. É claro que

$$N \times A \simeq N \times B.$$

Como a conjectura do automorfismo é válida para G por hipótese, pelo Lema 3.4 temos que

$$\mathcal{Z}(G) = \mathcal{Z}(N \times B).$$

Note que

$$(uz) \in \mathcal{Z}(N \times B),$$

e, assim, $uz \in \mathcal{Z}(G)$. Logo,

$$u \in (\mathcal{Z}(G) \cap \mathbb{Z}N) = \mathcal{Z}(N),$$

o que é uma contradição. Portanto,

$$\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G).$$

Para provar a propriedade 2, suponhamos $M \subseteq \mathcal{U}_1(\mathbb{Z}G)$ e $M \simeq N$. Seja $H = M \times A$. Note que G é policíclico-por-finito e, assim, residualmente finito. Pelo Lema 3.5, os elementos de H são linearmente independentes sobre $\mathbb{Z}$. Seja

$$\varphi : \mathbb{Z}H \longrightarrow \mathbb{Z}A$$

um homomorfismo sobrejetor de $\mathbb{Z}H$ em $\mathbb{Z}A$. Pelo Lema 2.6, φ preserva as unidades normalizadas de $\mathbb{Z}A$. Logo,

$$H \subseteq \mathcal{U}_1(\mathbb{Z}G)$$

e, assim, o grupo H é base para $\mathbb{Z}G$. Como

$$G \simeq H,$$

existe

$$\phi : \mathbb{Z}G \longrightarrow \mathbb{Z}G$$

um automorfismo, o qual aplica

$$\phi : G \longrightarrow H.$$

Como vale a conjectura do automorfismo para G e ambos N e M são subgrupos característicos e, respectivamente, subgrupos de torção, temos que existe uma unidade

$$u \in \mathbb{Q}G, \text{ tal que } M = uNu^{-1}.$$

Reciprocamente, sejam ϕ

$$\phi : \mathbb{Z}G \longrightarrow \mathbb{Z}G$$

um automorfismo e $M = \phi(N)$. Pela condição 1), obtemos que

$$\begin{aligned} \phi(G) &= \phi(N \times A) \\ &= \phi(N) \times \phi(A) \\ &= M \times A. \end{aligned}$$

Pela condição 2, existe uma unidade

$$u \in \mathbb{Q}G \text{ tal que } M = uNu^{-1}.$$

Logo,

$$\begin{aligned} u^{-1}\phi(G)\,u &= u^{-1}(M \times A)\,u \\ &= u^{-1}Mu \times u^{-1}Au \\ &= u^{-1}Mu \times \left(u^{-1}A\right)u \\ &= N \times \left(Au^{-1}\right)u \\ &= N \times A \\ &= G. \end{aligned}$$

Portanto, a conjectura do automorfismo é válida para G. ■

Como as unidades de torção são triviais nos anéis de grupo sobre os inteiros de um grupo N abeliano finito, é claro que a conjectura do automorfismo é válida para $\mathbb{Z}N$. Também, para um grupo A abeliano livre finitamente gerado, as unidades de

$$\mathbb{Z}(N \times A)$$

são triviais se, e somente se, as unidades de $\mathbb{Z}N$ são triviais conforme Corolário 2.4. Logo, como uma consequência imediata dos Teoremas anteriores obtemos uma caracterização de quando a conjectura do automorfismo é válida para grupos abelianos finitamente gerados.

Corolário 3.2 *Seja G um grupo abeliano finitamente gerado. A conjectura do automorfismo vale para G se, e somente se, as seguintes condições são satisfeitas*:

1. *G é finito*;

2. *$\mathbb{Z}T(G)$ tem somente unidades triviais.*

No caso onde G é infinito a conjectura do automorfismo vale se, e somente se, $\mathbb{Z}G$ tem somente unidades triviais. ■

3.3 Isomorfismo Para Grupos Nilpotentes

Nesta seção estamos preocupados com a seguinte questão de Sehgal. Seja G um grupo infinito nilpotente. Então

$$\mathbb{Z}G \simeq \mathbb{Z}H \Rightarrow G \simeq H \ ?$$

Não conhecemos nem mesmo se G e H têm a mesma classe de nilpotência, sabemos apenas que qualquer grupo que é base para $\mathbb{Z}G$ é também nilpotente. A resposta para este problema não é conhecida nem mesmo para grupos nilpotentes de classe 2, que não são finitamente gerados. Ritter e Sehgal mostraram que, se G e H são grupos nilpotentes finitamente gerados de classe 2 tal que

$$\mathbb{Z}G \simeq \mathbb{Z}H,$$

então

$$G \simeq H.$$

Mostraremos também que a propriedade nilpotente de classe 2 é determinada pelo anel de grupos sobre os inteiros. Note que não assumimos que os grupos envolvidos são finitamente gerados.

Teorema 3.5 *Sejam G um grupo nilpotente de classe 2 e H um grupo que é base para $\mathbb{Z}G$. Então H é um grupo nilpotente de classe 2.*

Em particular, o problema do isomorfismo vale para qualquer grupo finitamente gerado nilpotente de classe 2.

Prova. Como $H \subseteq \mathcal{U}_1(\mathbb{Z}G)$ temos que

$$\Delta(G, T(G)) = \Delta(H, T(H)).$$

Pelo Teorema 2.1, obtemos que

$$\mathbb{Z}\left(\frac{G}{T(G)}\right) \simeq \frac{\mathbb{Z}G}{\Delta(G, T(G))} = \frac{\mathbb{Z}H}{\Delta(H, T(H))} \simeq \mathbb{Z}\left(\frac{H}{T(H)}\right).$$

Assim, pelo Lema 2.5, temos que

$$\frac{G}{T(G)} \simeq \frac{H}{T(H)}.$$

Seja de

$$H = \gamma_1(H) \supseteq \gamma_2(H) \supseteq \cdots \supseteq \gamma_n(H) \supseteq \gamma_{n+1}(H) = \{1\} \text{ e } L = \gamma_n(H),$$

respectivamente, a série central inferior e o último termo não trivial desta série. Se L é não periódico, então

$$L \nsubseteq T(H).$$

Logo,

$$H \text{ e } \frac{H}{T(H)} \text{ têm a mesma classe de nilpotência.}$$

Daí

$$2 \leq \gamma(H) = \gamma\left(\frac{H}{T(H)}\right) = \gamma\left(\frac{G}{T(G)}\right) \leq \gamma(G) = 2.$$

Logo, $\gamma(H) = 2$.

Suponhamos que L seja de torção. Como L é de torção e central, pelo Corolário 2.3 temos que $L \subseteq G$. Para provar o resultado é suficiente mostrar que $n \leq 2$. Suponhamos o contrário, isto é, $n > 2$. Como

$$\gamma_3(H) = H \cap \left(1 + \Delta^3(H)\right) \text{ e } \Delta(G) = \Delta(H),$$

(veja [5, Corollary IV]) temos que

$$L \subseteq G \cap \left(1 + \Delta^3(G)\right) = D_3(G) = \gamma_3(G).$$

Sendo $\gamma(G) = 2$ temos que L é trivial, o que é uma contradição. Portanto, $n = 2$. ■

A seguir mostraremos que a classe de nilpotência de qualquer grupo nilpotente finitamente gerado é determinada pelo anel de grupo sobre os inteiros.

Seja $\mathcal{F}$ um conjunto de grupos nilpotente finitamente gerados tal que as seguintes condições são satisfeitas:

1. $\mathcal{F}$ é homomorficamente fechado;

2. Se H é algum grupo nilpotente finitamente gerado com $T(H) \simeq T(G)$, então $H \in \mathcal{F}$.

Note que pelas observações feitas no começo desta seção, qualquer grupo H que é base de $\mathbb{Z}G$ com $G \in \mathcal{F}$ é também um grupo nilpotente finitamente gerado e, assim, pelo Teorema 2.5, obtemos que:

$$T(H) \simeq T(G).$$

Logo, pela condição 2, $H \in \mathcal{F}$. Seja $\mathcal{F}_c$ o subconjunto daqueles grupos $G \in \mathcal{F}$ cujos anéis de grupos sobre os inteiros contêm um grupo base H, tal que

$$\gamma(G) \neq \gamma(H).$$

Como os grupos nilpotentes finitamente gerados livres de torção são ordenados, pelo Lema 2.4, obtemos que o problema do isomorfismo é válido e, assim, os elementos de $\mathcal{F}_c$ não são livres de torção. Sejam

$$\delta(G) = h(G) + \gamma(G) + |T(G)|$$

e $\mathcal{F}_{mc}$ o conjunto daqueles grupos G em $\mathcal{F}_c$, que têm $\delta(G)$ o menor possível. Como $\frac{G}{T(G)}$ é um grupo ordenado, temos pelo Lema 2.4 que $h(G) = h(H)$. Como $T(G)$ e $T(H)$ também têm a mesma ordem temos que

$$\begin{aligned} \delta(G) - \delta(H) &= h(G) - h(H) + \gamma(G) - \gamma(H) + |T(G)| - |T(G)| \\ &= \gamma(G) - \gamma(H). \end{aligned}$$

Lema 3.6 *Seja $G \in \mathcal{F}_{mc}$. Então $T(G)$ é um p-grupo. Se o grupo H é uma base para $\mathbb{Z}G$, então*

$$\gamma(G) \leq \gamma(H) \leq \gamma(G) + 1.$$

Além disso, se $\gamma(H) = \gamma(G)+1$, então o último termo não trivial da série central inferior de G não é de torção enquanto o de H é de torção de ordem prima e é o único subgrupo normal de ordem prima. Em particular, $\mathcal{Z}(G)$ tem torção cíclica.

Prova. Sejam as séries centrais inferiores

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq \cdots \supseteq \gamma_n(G) \supseteq \gamma_{n+1}(G) = \{1\}$$

e

$$H = \gamma_1(H) \supseteq \gamma_2(H) \supseteq \cdots \supseteq \gamma_{m-1}(H) \supseteq \gamma_m(H) \supseteq \gamma_{m+1}(H) = \{1\}$$

de G e H, respectivamente e $n = \gamma(G)$ e $m = \gamma(H)$. Como G e $H \in \mathcal{F}_c$ temos que $n \leq m$. Para provar o resultado assumimos que $n < m$. Suponhamos que

$$A = \gamma_n(G) \text{ e } B = \gamma_m(H)$$

são ambos de torção. Logo, A e B são centrais e de torção, pelo Corolário 2.3, obtemos que

$$A \subset (G \cap H) \text{ e } B \subset (G \cap H).$$

Suponhamos $B \nsubseteq A$. Como $\mathcal{F}$ é fechado por imagem homomórfica temos que

$$n - 1 = \gamma\left(\frac{G}{A}\right) = \gamma\left(\frac{H}{A}\right) = m,$$

o que é uma contradição, pois $n < m$. Se $B \subset A$, então

$$n \geq \gamma\left(\frac{G}{B}\right) = \gamma\left(\frac{H}{B}\right) = m - 1.$$

Como $n < m$ temos que $n = m - 1$. Por outro lado,

$$n - 1 = \gamma\left(\frac{G}{A}\right) = \gamma\left(\frac{H}{A}\right),$$

e, assim,

$$\gamma_n(H) \subseteq A \text{ é central.}$$

Portanto, $m = \gamma(H) = n$, novamente uma contradição.

Se ambos A e B não são de torção, então pela prova do Teorema 3.5, obtemos que

$$n = \gamma\left(\frac{G}{T(G)}\right) = \gamma\left(\frac{H}{T(H)}\right) = m,$$

o que é uma contradição, pois $n < m$. Agora provemos que $A = \gamma_n(G)$ não é de torção. Suponhamos o contrário. Então pelas considerações anteriores B não é de torção. Pelo Corolário 2.3, obtemos que

$$A \subset (G \cap H).$$

Logo,

$$\Delta(G, A) = \Delta(H, A) \text{ e } \mathbb{Z}\left(\frac{G}{A}\right) \simeq \frac{\mathbb{Z}G}{\Delta(G, A)} = \frac{\mathbb{Z}H}{\Delta(H, A)} \simeq \mathbb{Z}\left(\frac{H}{A}\right).$$

Como $G \in \mathcal{F}_{mc}$ obtemos

$$m = \gamma\left(\frac{H}{A}\right) = \gamma\left(\frac{G}{A}\right) = n - 1,$$

o que é uma contradição. Portanto, concluímos que A não é de torção e B é de torção.

Como G contém torção, pela Proposição 1.8 temos que

$$T(\mathcal{Z}(G)) \neq \{1\}.$$

Seja C um subgrupo não trivial finito e central de G. Então pelo Corolário 2.3, obtemos que

$$C \subset (G \cap H).$$

Logo,

$$\Delta(G, C) = \Delta(H, C), \mathbb{Z}\left(\frac{G}{C}\right) \simeq \frac{\mathbb{Z}G}{\Delta(G, C)} = \frac{\mathbb{Z}H}{\Delta(H, C)} \simeq \mathbb{Z}\left(\frac{H}{C}\right)$$

e

$$\left|T\left(\frac{G}{C}\right)\right| < |T(G)|$$

Como $G \in \mathcal{F}_{mc}$ temos que

$$\gamma\left(\frac{G}{C}\right) = \gamma\left(\frac{H}{C}\right).$$

Por outro lado,

$$\gamma\left(\frac{G}{C}\right) = n,$$

pois A não é de torção. Se $B \nsubseteq C$, então

$$\gamma\left(\frac{H}{C}\right) = m.$$

Logo, $m = n$, o que é uma contradição. Portanto, $B \subset C$. Pelo Teorema 1.13, $T(G)$ é um subgrupo normal e finito de G. Além disso, para cada divisor primo p da ordem de $T(G)$, existe um elemento central $g_0 \in G$ de ordem p. Logo, podemos tomar C como sendo o grupo gerado por g_0, isto é, $C =< g_0 >$. Assim, se existissem diferentes primos dividindo a ordem de $T(G)$, teríamos que B estaria contido em todos eles e, portanto, B seria trivial, o que é uma contradição. Dessa forma, $T(G)$ deve ser um p-grupo.

Se a torção do centro de G não fosse cíclica chegaríamos à mesma contradição: De fato, a torção do centro de G é um grupo abeliano finito e, assim, é um produto direto de grupos finitos e, portanto, um produto direto de grupos cíclicos. Tomando C como um fator deste produto direto teríamos que B estaria contido em cada fator direto. Porém a intersecção dos fatores diretos da torção do centro de G é trivial e, portanto, B seria trivial. Assim, a torção do centro de G deve ser cíclica de ordem prima. Pelo fato citado acima sobre grupos nilpotentes finitamente gerados, devemos ter que $T(G)$ é um p-grupo. Como

$$n = \gamma\left(\frac{G}{B}\right) = \gamma\left(\frac{H}{B}\right) = m - 1$$

temos que $m = n + 1$. Portanto,

$$\gamma(G) \leq \gamma(H) \leq \gamma(G) + 1.$$

■

Proposição 3.1 *Seja $G \in \mathcal{F}_{mc}$. Suponhamos que existe um grupo H base de $\mathbb{Z}G$ com*

$$n = \gamma(G) \neq \gamma(H) = m.$$

Então $\gamma_m(H) \subseteq D_{m+1}(G)$ e, assim, G é um contra-exemplo para o problema do subgrupo de dimensão. Além disso, existe um p-grupo finito que é uma imagem homomórfica de G e também um contra-exemplo para o subgrupo de dimensão.

Prova. (Ver [7, Proposition 5.3].) ■

A Proposição 3.1 aponta uma ligação entre o problema do subgrupo de dimensão e o segundo problema considerado nesta seção, isto é, a classe de nilpotência é determinada pelo anel de grupo sobre os inteiros. O Teorema seguinte mostra que, se o problema do subgrupo de dimensão vale para um grupo G nilpotente finitamente gerado, então obtemos uma solução positiva para nosso problema. Recordamos que o problema do subgrupo dimensão não vale em geral, nem mesmo para grupos nilpotentes de classe de nilpotência três, já que existem contra-exemplos. Este exemplo tem as mesmas propriedades que aquelas listadas na Proposição 3.1. Embora que, se G tem classe de nilpotência três e $T(G)$ não tem 2-torção, então podemos dar uma prova elementar para a solução de nosso problema.

Para isto utilizamos que

$$D_4^2(G) \subseteq \gamma_4(G),$$

para qualquer grupo G, (veja [5]). Logo, se G é um grupo nilpotente de classe três e $T(G)$ não contém 2-torção, então $D_4(G)$ é trivial. Também, se H é como na proposição 3.1 com $\gamma(H) \neq 3$, então pelo Lema 3.6

$$4 = \gamma(H).$$

Assim, pela Proposição 3.1, obtemos que

$$\{1\} \neq \gamma_4(H) \subseteq D_5(G) = \{1\},$$

o que é uma contradição.

Teorema 3.6 *Seja G um grupo nilpotente finitamente gerado tal que uma das seguintes condições é satisfeita*:

1. *Todo elemento de $\mathcal{F}$ satisfaz a conjectura do subgrupo de dimensão*;

2. *As unidades centrais de $\mathbb{Z}G$ são triviais e $\gamma(G) \leq 3$*;

3. $\mathcal{Z}(\mathbb{Z}T(G)) \cap \mathcal{Z}(\mathbb{Z}G) = \mathcal{Z}(T(G))$ *e* $\gamma(G) \leq 3$.

Então todos os grupos que são bases de $\mathbb{Z}G$ *têm a mesma classe de nilpotência.*

Prova. (Ver [7, Theorem 5.4].) ■

Corolário 3.3 *Seja* G *um grupo nilpotente finitamente gerado. Se* G *é sem* 2*-torsão, então todo grupo que é base de* $\mathbb{Z}G$ *tem a mesma classe de nilpotência.*

Prova. Por um resultado de N. Gupta [4] temos que $D_n(G) = \gamma_n(G)$. Portanto, pelo Teorema 3.6, todos os grupos que são base de $\mathbb{Z}G$ têm a mesma classe de nilpotência. ■

Referências Bibliográficas

[1] Alperin, J. L. and Bell, Rowen B., *Groups and Representations. Springer-Verlag New York,* 1995.

[2] Bhattacharya, P. B., Jain, S. K. end Nagpaul, S. R., *Basic Abstract Algebra.* Cambridge, New York, 1995.

[3] Dummit, D. S. and Foote, R. M., *Abstract Algebra. Prentice-Hall,* 1991.

[4] Gupta, N., "The dimension subgroup conjecture holds for odd order groups," Journal of Group Theory, Vol 5, pp. 481 – 491, 2002.

[5] Gupta, N., "Free group rings," Contemp. Math, 1987.

[6] Hertweck, M., "A counterexample to the isomorphism problem for integral group rings," Annals of Mathematics, vol. 154, pp. 115 – 138, 2001.

[7] Juriaans, S. O. and Jespers, E., "Isomorphisms of Integral Group Rings of Infinite Groups," Journal of Algebra, Vol 223, pp. 171 – 189, 2000.

[8] Juriaans, S. O., "Trace properties of torsion units in group rings II," IME, São Paulo, 1996.

[9] Klinger, L., "Construction of a counterexample to a conjecture of Zassenhaus," Comm. Algebra, pp. 2303 – 2330, 1991.

[10] Lidl, R. and Pilz, G., *Applied Abstract Algebra.* Springer. New York, 1998.

[11] Marciniak, Z. S. and Sehgal, S. K., "Finite Matrix Groups over Nilpotent Group Rings," Journal of Algebra, vol. 181, pp. 565 – 583, 1996.

[12] Milies, F. C. Polcino, *Anéis de Grupos.* Sociedade Brasileira de Matemática, São Paulo, 1976.

[13] Milies, F. C. Polcino, *Anéis e Módulos.* IME, São Paulo, 1972.

[14] Ritter, J. and Sehgal, S., " Isomorphism of group rings," Arch. Math., Vol. 40, pp. $32 - 39$, 1993.

[15] Robinson, D. J. S. , *A Course in the Theory of Groups.* Springer-Verlag, New York, Heidelberg, Berlin, 1980.

[16] Rotman, J. J., *Galois Theory.* Springer, New York, 1998.

[17] Sehgal, S. K. and Milies, F.C. Polcino , *An Introduction to Group Rings.* Kluwer, Boston, 2002.

[18] Sehgal, S. K., *Units in Integral Group Rings.* Longman Scientific & Technical, New York 1993.

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

[20] Spindler, K., *Abstract Algebra With Applications.* Marcel Dekker, vol. 1, New York, 1994.