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

O Problema do Normalizador em Anéis de Grupos sobre os Inteiros

por

Joelma Ananias de Oliveira

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

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 do Normalizador em Anéis de Grupos sobre os Inteiros

por

Joelma Ananias de Oliveira

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. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. Orlando Stanley Juriaans - USP (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

- Ao meu orientador e amigo, o Professor Dr. *Antônio de Andrade e Silva*, que me conduziu, passo a passo, com seus conhecimentos, experiências, dedicação e reponsável firmeza na orientação desta dissertação.

- Ao meu co-orientador, o Professor Dr. *Orlando Stanley Juriaans* - UME-USP -, pela eficiente e criteriosa orientação.

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

- Em especial ao Aroldo,meu esposo, por estarmos juntos nesta caminhada.

- Aos colegas do curso de mestrado, em especial ao Aroldo e Dércio, pois vencemos muitas barreiras juntos.

- A Sônia, pela competência e presteza no atendimento de secretaria.

- Aos professores do Departamento de Matemática - UFMT - que contribuíram para a minha formação.

- Ao Professor Alberto de Arruda do Departamento de Física - UFMT.

- Aos meus filhos Matheus e Gustavo, a razão do meu viver.

- À minha mãe Vergínia, pela ajuda magnífica que me proporcionou.

Dedicatória

Ao meu pai Valmir (in memoriam)

Resumo

O problema do normalizador de um anel de grupo sobre inteiros de um grupo arbitrário G é investigado.

Mostraremos que qualquer elemento do normalizador $\mathcal{N}_{\mathcal{U}_1}(G)$ de G no grupo das unidades normalizadas $\mathcal{U}_1(\mathbb{Z}G)$ é determinado por um subgrupo normal finito.

Esta redução para subgrupos normais finitos implica que a propriedade do normalizador vale para muitas classes de grupos (infinitos), tal como grupos sem 2-torção, grupos de torção com um 2-subgrupo de Sylow normal, e grupos localmente nilpotentes.

Além disso, mostraremos que o comutador de $\mathcal{N}_{\mathcal{U}_1}(G)$ é igual a G' e $\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{G}$ é finitamente gerado se o subgrupo de torção do grupo de conjugação finita de G for finita.

Abstract

The normalizer problem of an integral group ring of an arbitrary group G is investigated. It is shown that any element of the normalizer $\mathcal{N}_{\mathcal{U}_1}(G)$ of G in the group of normalized units $\mathcal{U}_1(\mathbb{Z}G)$ is determined by a finite normal subgroup. This reduction to finite normal subgroups implies that the normalizer property holds for many classes of (infinite) groups, such as groups without non–trivial 2-torsion, torsion groups with a normal Sylow 2-subgroup, and locally nilpotent groups. Furthermore it is shown that the commutator subgroup of $\mathcal{N}_{\mathcal{U}_1}(G)$ equals G' and $\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{G}$ is finitely generated if the torsion subgroup of the finite conjugacy group of G is finite.

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.

$\mathbb{Z}G$ - Anel de grupo sobre os inteiros

$[L : K]$ - Índice de K em L

$\text{supp}\,(\lambda)$ - 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 produto de Lie

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

$\sim$ - relação de conjugação no 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

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

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

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

$\mathrm{Cl}(g)$ - Classe de conjugação de g em G

G' - Subgrupo derivado

Sumário

Introdução **x**

1 Resultados Básicos **1**

1.1 Grupos 1

1.2 Grupos Abelianos Finitamente Gerados 7

1.3 Ações de Grupo 8

1.4 Grupos Nilpotentes 11

1.5 Grupos FC 15

1.6 Derivações 18

2 Anéis de Grupos **21**

2.1 Anéis 21

2.2 Anéis de Grupos 28

2.3 Unidades Triviais 31

2.4 Normalizador de G em $\mathcal{U}(\mathbb{Z}G)$ 36

3 Problema do Normalizador **43**

3.1 Redução para grupos finitos 43

3.2 Grupos Satisfazendo a Condição do Normalizador 51

Referências Bibliográficas **58**

Introdução

Este trabalho foi baseado no artigo "On The Normalizer Problem," [4] no qual os autores analisam o problema do normalizador.

Sejam G um grupo e $\mathbb{Z}G$ seu anel de grupo sobre os inteiros. Denotamos por $\mathcal{U}_1 = \mathcal{U}_1(\mathbb{Z}G)$ o grupo das unidades normalizadas de $\mathbb{Z}G$. Um problema interessante, o qual é o objetivo deste trabalho, é determinar $\mathcal{N}_{\mathcal{U}_1}(G)$, o normalizador de G em $\mathcal{U}_1$. Tem sido conjecturado que

$$\mathcal{N}_{\mathcal{U}_1}(G) = G\mathcal{Z}(\mathcal{U}_1), \tag{NP}$$

(cf. [8, Problem 43, pg 305]), isto é, o normalizador de G em $\mathcal{U}_1$ é $\langle G, \mathcal{Z}(\mathcal{U}_1)\rangle$, onde $\mathcal{Z}(\mathcal{U}_1)$ é o centro de $\mathcal{U}_1$.

Esta propriedade do normalizador (NP) tem sido provada para muitas classes de grupos finitos. Para grupos infinitos, muito pouco é conhecido. A idéia central desta dissertação é apresentar o teorema da representação para unidades normalizadas que diz que unidades no normalizador estão, até uma unidade trivial, determinada por uma unidade no anel de grupo de um subgrupo normal finito. Tal resultado teve grande importância, pois a partir dele foi possível mostrar que o problema do normalizador vale para várias classes de grupos infinitos.

O trabalho é organizado como segue:

No capítulo 1, apresentamos os conceitos e resultados básicos sobre grupos, os quais são essenciais aos demais capítulos.

No capítulo 2, apresentamos resultados básicos sobre anéis, módulos e anéis de grupos, bem como, as estruturas básicas do grupo normalizador $\mathcal{N}_{\mathcal{U}_1}(G)$.

Finalmente, no capítulo 3, mostramos o resultado principal onde, inicialmente, provamos o teorema de representação para unidades normalizadas e, em seguida, mostramos que o problema do normalizador vale para 3 classes importantes de grupos, a saber, gru-

pos tais que $\Delta^+(G)$ é sem 2-torção trivial, grupos periódicos com um 2-subgrupo de Sylow normal e grupos localmente nilpotentes.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados básicos da teoria dos grupos que serão necessários nos capítulos seguintes.

1.1 Grupos

Um conjunto não vazio G equipado com uma operação binária

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

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

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

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 todos $a, b \in G$.

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 e 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 todos $a, b \in H$.

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 a classe lateral à esquerda aH. O elemento a é chamado um *representante* da classe de equivalência. Um conjunto completo de representantes das classes à esquerda (ou à direita) é chamado uma *transversal* à esquerda (ou à direita) de H em G. É fácil verificar, também, 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 denotamos 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 operação $aHbH = abH$, para todos $a, b \in G$, 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.

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

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

é um grupo. Em particular,

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

Teorema 1.1 *Sejam G um grupo e H, K subgrupos de G tal que $K \leq H$. Então*

$$[G:K] = [G:H][H:K].$$

■

Corolário 1.1 (Teorema de Lagrange) *Sejam G um grupo finito e H um subgrupo de G. Então*

$$|G| = [G:H]\,|H|\,.$$

■

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,o qual será chamado de *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*

$$\langle X\rangle = \left\{\prod_{i=1}^{n} x_i : n\in\mathbb{N} \text{ e } x_i \in X\cup X^{-1}, i=1,\ldots,n\right\},$$

onde $X^{-1} = \{x^{-1} : x \in X\}$. ■

Seja G um grupo. Dizemos que G é *finitamente gerado* se existir um subconjunto X finito 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 um *grupo cíclico*.

Sejam G um grupo e H um subgrupo de G. O conjunto

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

é chamado o *normalizador* de H em G. Dizemos que um subgrupo K normaliza H se $K \leq \mathcal{N}_G(H)$.

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 $\mathcal{N}_G(H)$;*
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 de G se, e somente se, $\mathcal{N}_G(H) = G$.* ■

Sejam G um grupo e H um subgrupo de G. O conjunto

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

é chamado o *centralizador* de H em G. É fácil verificar que $\mathcal{C}_G(H)$ é um subgrupo de G contido no $\mathcal{N}_G(H)$. Em particular,

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

Seja G um grupo. O conjunto

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

é chamado o *centro* de G. É fácil verificar que $\mathcal{Z}(G)$ é um subgrupo normal de G. Além disso,

$$\mathcal{Z}(G) = \bigcap_{x \in G} \mathcal{C}_G(x).$$

Sejam G e H grupos. Uma função φ de G em H é um *homomorfismo de grupos* se

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

para todos $a, b \in G$. Neste caso, a *imagem* de φ é o conjunto

$$\begin{aligned} \operatorname{Im}\varphi &= \{h : h = \varphi(g) \text{ para algum } g \in G\} \\ &= \{\varphi(g) : g \in G\}. \end{aligned}$$

O *núcleo* de φ é o conjunto

$$\ker\varphi = \{g \in G : \varphi(g) = 1\}.$$

É fácil verificar que $\operatorname{Im}\varphi$ é um subgrupo de H e $\ker\varphi$ 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 por $G \simeq H$. Um *endomorfismo* de um grupo G é um homomorfismo $\varphi : G \longrightarrow G$. Denotamos por

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

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

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

É fácil verificar que $\operatorname{Aut}(G)$ é um grupo com a operação composição.

Seja $a \in G$ fixado. A função

$$\begin{aligned} \sigma_a \quad : \quad & G \longrightarrow G \\ & x \mapsto axa^{-1} \end{aligned}$$

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

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

Sejam G grupo e H subgrupo de G. Dizemos que H é um *subgrupo característico* de G se

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

Proposição 1.3 *Sejam G grupo e H, K subgrupos de G. Se K é um subgrupo característico de H e H normal em G. Então K é normal em G.* ■

Teorema 1.2 (1º Teorema de Isomorfismo) *Seja $\varphi : G \longrightarrow G_1$ um homomorfismo de grupos. Então*

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

■

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 do $\mathcal{N}_G(H)$ e $\frac{\mathcal{N}_G(H)}{\mathcal{C}_G(H)}$ é isomorfo a um subgrupo de* $\operatorname{Aut}(H)$.

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

Sejam G um grupo e H um subgrupo normal de G. Consideremos a função $\pi : G \longrightarrow \frac{G}{H}$ dado por $\pi(a) = \overline{a} = aH$, é fácil verificar que, π é um homomorfismo de grupos sobrejetor, o qual é chamado o *homomorfismo canônico*. Note que

$$\pi(1) = 1H = H, \ker(\pi) = H \text{ e } \pi(K) = \frac{K}{H},$$

onde $K \leq G$ e $H \subseteq K$. Em particular, obtemos que todo subgrupo normal H de G é o núcleo de algum homomorfismo.

Sejam G um grupo e $H_i \leq G$, $i = 1, \ldots, n$. Dizemos que G é o *produto direto (interno)* de $H_1, \ldots, H_n$ se as seguintes condições são satisfeitas:

1. $H_i \trianglelefteq G$, $i = 1, \ldots, n$

2. Todo $g \in G$ pode ser escrito de modo único na forma $g = h_1 \cdots h_n, h_i \in H_i$.

Proposição 1.4 *Sejam G um grupo e $H_i \leq G, i = 1, \ldots, n$. Então G é um produto direto (interno) de $H_1, \ldots, H_n$ se, e somente se,*

1. $G = H_1 \cdots H_n$.

2. $H_i \trianglelefteq G$, $i = 1, \ldots, n$.

3. $H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$, $i = 1, \ldots, n$. ■

Sejam G um grupo, H e 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. $N \trianglelefteq G$ e $H \leq G$;
3. $N \cap H = \{1\}$.

Notação: $G = N \rtimes H$.

1.2 Grupos Abelianos Finitamente Gerados

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 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 1.4 *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 $r, n_1, n_2, \ldots, n_s \in \mathbb{N}$ 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 1.2 *Seja G um grupo abeliano finitamente gerado. Então $T(G)$ é finito, $\frac{G}{T(G)}$ é livre de posto finito e*

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

■

1.3 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 todos $a, b \in G$, $x \in \Omega$;

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 1.1 *Existe uma correspodência biunívoca entre o conjunto de ações de G em Ω e o conjunto de homomorfismo 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*

$$\varphi_{a^{-1}} \circ \varphi_a(x) = \varphi_{a^{-1}}(ax) = a^{-1}(ax) = (a^{-1}a)x = x, \forall x \in \Omega.$$

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,

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

Seja G um grupo e Ω um conjunto não vazio. Então $(g, a) \longrightarrow a$ é uma ação de G sobre Ω, chamada *ação trivial.*

O conjunto

$$O(x) = \{ax : a \in G\}$$

é chamado a *órbita* de x. Dados $x, y \in \Omega$, definimos $x \sim y$ se, e somente se, existe $a \in G$ tal que $y = ax$. É fácil verificar que $\sim$ é uma relação de equivalência em Ω e que $O(x)$ são as classes de equivalências de Ω. Logo,

$$\Omega = \dot{\bigcup_{x \in \Omega}} O(x).$$

Seja $x \in \Omega$ fixado, o conjunto

$$G_x = \{a \in G : ax = x\}$$

é um subgrupo de G chamado *estabilizador* de x em G.

Dizemos que G *age transitivamente* sobre Ω ou Ω *é um G-conjunto transitivo*, se para quaisquer $x, y \in \Omega$, existir $a \in G$ com $ax = y$ ou, equivalentemente, $\Omega = O(x)$, $\forall x \in \Omega$.

Proposição 1.5 *Seja G um grupo agindo em um conjunto não vazio Ω. Então*

$$[G : G_x] = |O(x)|,$$

para todo $x \in \Omega$. Em particular, se G é finito, então $|O(x)|$ divide $|G|$, para todo $x \in \Omega$. ■

Sejam G um grupo e $\Omega = G$. A função $* : G \times \Omega \longrightarrow \Omega$ dada por $*(g, a) = gag^{-1}$ é uma ação de G em Ω. Dado $a \in \Omega$, a órbita de Ω

$$O(a) = \{gag^{-1} : g \in G\}$$

é chamada a *classe de conjugação* de Ω e será denotada por $\mathrm{Cl}(a)$. O estabilizador de a

$$G_a = \{g \in G : gag^{-1} = a\} = \mathcal{C}_G(a)$$

é o centralizador de a em G. Assim, pela Proposiçao acima,

$$|Cl(a)| = [G : \mathcal{C}_G(a)].$$

Sejam G um grupo finito e p um número primo. Dizemos que G é um *p-grupo* se sua ordem é uma potência de p, isto é,

$$|G| = p^n$$

para algum $n \in \mathbb{N}$. Pelo Teorema de Lagrange, todo subgrupo de G é um *p-grupo*.

Seja G um grupo abeliano, dizemos que G é *abeliano elementar* se existe um inteiro primo p tal que todos elementos diferente da identidade de G são de ordem p. Definimos o *expoente* de um grupo G como sendo o menor inteiro positivo m tal que $g^m = 1$, para todo $g \in G$ e o denotaremos por $exp(G)$.

Seja G um grupo de ordem $p^n m$, onde $\mathrm{mdc}(p, m) = 1$. Um subgrupo H de G é um *p-subgrupo de Sylow* de G se a ordem de H é p^n.

Teorema 1.5 (Teoremas de Sylow) *Seja G um grupo de ordem $p^n m$, com $\mathrm{mdc}(p, m) = 1$. Então*:

1. *G contém um p-subgrupo de Sylow.*

2. *Se H é um p-subgrupo de Sylow de G e K qualquer p-subgrupo de G, então existe $a \in G$ tal que $aKa^{-1} \subseteq H$. Em particular, quaisquer dois p-subgrupos de Sylow de G são conjugados.*

3. *O número n_p de p-subgrupos de Sylow de G é da forma $1 + kp, k \in \mathbb{Z}_+$. Além disso,*

$$n_p = [G : \mathcal{N}_G(H)],$$

para todo p-subgrupo de Sylow H de G e $n_p \mid m$.

Proposição 1.6 *Sejam G um grupo, P um p-subgrupo de sylow de G e H um subgrupo de G. Se $\mathcal{N}_G(P) \subseteq H$, então*

$$H = \mathcal{N}_G(H).$$

■

1.4 Grupos Nilpotentes

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* ou *subgrupo derivado* 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.

Lema 1.1 *Sejam x, y, e z elementos de um grupo G. Então*:

1. $(x, y) = 1$ *se, e somente se,* $xy = yx$;
2. $(x, y)^{-1} = (y, x)$;
3. $(xy, z) = (x, z)^y(y, z) = (x, z)((x, z), y)(y, z)$;
4. $(x, yz) = (x, z)(x, y)^z = (x, z)(x, y)((x, y), z)$. ■

Proposição 1.7 *Sejam G um grupo , $x, y \in G$ e H um subgrupo de G. Então*:

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

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

Em particular, $f(G') = (\operatorname{Im} f)'$. ■

Proposição 1.8 *Se K é um subgrupo normal em G e $K \leq H \leq G$, então $(H, G) \leq K$ se, e somente se,*

$$\frac{H}{K} \leq \mathcal{Z}\left(\frac{G}{K}\right)$$

■

Uma *série subnormal* de um grupo G é uma sequência de subgrupos

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

tal que

$$G_{i+1} \trianglelefteq G_i, 0 \leq i \leq n.$$

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

Seja G um grupo. A *série central descendente*

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

é definida, indutivamente, por

$$\gamma_1(G) = G; \cdots \gamma_{i+1}(G) = (\gamma_i(G), G).$$

Proposição 1.9 *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*

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

de G é definida, indutivamente, por

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

Proposição 1.10 *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* $\frac{G}{\mathcal{Z}_n(G)}$. ■

Dizemos que um grupo G é *nilpotente* se $\mathcal{Z}_m(G) = G$ para algum m. O menor m tal que $\mathcal{Z}_m(G) = G$ é chamado a *classe de nilpotência* de G. Claramente temos que um grupo abeliano é nilpotente, pois $\mathcal{Z}_1(G) = \mathcal{Z}(G) = G$.

Lema 1.2 *Subgrupos e grupos quocientes de grupos nilpotentes são nilpotentes.* ■

Proposição 1.11 *Se* H *e* K *são nilpotentes então seu produto direto*

$$H \times K$$

é nilpotente. ■

Proposição 1.12 *Se* G *é nilpotente e* $H \lneq G$, *então* $H \lneq \mathcal{N}_G(H)$. ■

Teorema 1.6 *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.* ■

Teorema 1.7 [7]*Seja* G *um grupo nilpotente. Então, o conjunto* $T(G)$ *é um subgrupo característico e* $\frac{G}{T(G)}$ *é livre de torção.* ■

Seja $\mathcal{X}$ uma *classe de grupos*. Um grupo G é chamado *poly-*$\mathcal{X}$ se G tem uma série

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

tal que cada fator

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

pertence à *classe* $\mathcal{X}$.

O Teorema 1.7 mostra que se G é um grupo nilpotente finitamente gerado então $\frac{G}{T(G)}$ é *policíclico infinito* e G é um *policíclico-por- finito*.

Lema 1.3 [7]*Seja $\mathcal{X}$ uma classe de grupos. Se $\mathcal{X}$ é fechado sobre subgrupos. Então a classe de grupos poly-$\mathcal{X}$ também o é.* ■

Lema 1.4 (Poincaré) *A interseção de um número finito de subgrupos de índice finito em um grupo G é também de índice finito em G.* ■

Teorema 1.8 *Seja G um grupo policíclico-por-finito. Então, G contém um subgrupo característico H o qual é um policíclico-infinito e tal que $\frac{G}{H}$ é finito.* ■

Corolário 1.3 *Sejam G um grupo nilpotente finitamente gerado. Então G contém um subgrupo característico H livre de torção tal que $\frac{G}{H}$ seja finito.* ■

Seja G um grupo finito. Então G possui um único subgrupo nilpotente normal maximal que é chamado de *subgrupo Fitting* e que será denotado por $Fit(G)$.

Sejam G um grupo e Π um conjunto de números primos. Dizemos que o elemento $x \in G$ é um Π-elemento se $o(x)$ é divisível somente pelos primos em Π. Em particular, temos a noção de um p-elemento. Similarmente, um grupo é chamado um Π-*grupo* se $|G|$ é divisível somente pelos primos em Π. Vamos denotar por $\Pi(G)$ o conjunto do divisores primos de $|G|$. O conjunto complementar dos primos em Π será denotado por Π'. Portanto, temos também a noção de Π' e p' elementos, bem como Π' e p' grupos. Por exemplo, um $2'$-elemento é simplesmente um elemento de ordem ímpar.

Se G é um grupo que contém um série de composição, então os grupos fatores desta série são chamados de fatores de composição de G. Dizemos que G é Π-*separável* se toda fator de composição de G é Π-grupo ou Π'-grupo.

Sejam G um grupo e H e K Π-subgrupos normais de G. Então HK também o é. Assim, G possui um único Π-subgrupo normal maximal, o qual denotamos por $O_\Pi(G)$. Claramente, $O_\Pi(G)$ é característico. Além disso, por definição de $O_\Pi(G)$, obtemos $O_\Pi(\overline{G}) = \{\overline{1}\}$, onde

$$\overline{G} = \frac{G}{O_\Pi(G)}.$$

Em $\overline{G}$, consideremos o único Π'-subgrupo normal maximal $O_{\Pi'}(\overline{G})$ e denotemos sua imagem inversa em G por

$$O_{\Pi,\Pi'}(G).$$

Teorema 1.9 [3, $Theorem 3.2, pg.228$]*Se G é Π-separável e $\overline{G} = \frac{G}{O_{\Pi'}(G)}$, então*

$$\mathcal{C}_{\overline{G}}(O_\Pi(\overline{G})) \subseteq O_\Pi(\overline{G}).$$

Em particular, se $O_{\Pi'}(G) = \{1\}$*, então* $\mathcal{C}_G(O_\Pi(G)) \subseteq \mathcal{Z}(O_\Pi(G))$. ■

1.5 Grupos FC

Lema 1.5 *Seja* G *um grupo. Então o conjunto*

$$\Phi(G) = \{x \in G : [G : \mathcal{C}_G(x)] < \infty\}$$

é um subgrupo característico de G

Prova. Dados $g, h \in \Phi(G)$

$$\mathcal{C}_G(gh^{-1}) \supseteq \mathcal{C}_G(g) \cap \mathcal{C}_G(h^{-1}) = \mathcal{C}_G(g) \cap \mathcal{C}_G(h)$$

Logo, pelo Lema 1.4,

$$[G : \mathcal{C}_G(gh^{-1})] \leq [G : \mathcal{C}_G(g) \cap \mathcal{C}_G(h)] < \infty.$$

Portanto, $gh^{-1} \in \Phi(G)$. Finalmente, se $\varphi \in \mathrm{Aut}(G)$ temos

$$[G : \mathcal{C}_G(\varphi(g))] = [G : \mathcal{C}_G(g)] < \infty$$

Portanto, $\varphi(g) \in \Phi(G)$. ■

O subgrupo característico $\Phi(G)$ é chamado de *subgrupo FC de* G. Em particular, quando $\Phi(G) = G$, dizemos que G é um *grupo FC*. Note que todos os grupos abelianos e todos os grupos finitos são grupos FC.

Lema 1.6 *Seja* G *um grupo* FC*. Então subgrupos e grupos quocientes de* G *são grupos* FC*.* ■

Lema 1.7 *Seja* G *um grupo* FC *finitamente gerado. Então* $[G : \mathcal{Z}(G)]$ *é finito.*

Prova. Sejam $x_1, \ldots, x_n \in G$ tais que

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

Como

$$[G : \mathcal{C}_G(x_i)] < \infty, 1 \leq i \leq n$$

e

$$\mathcal{Z}(G) = \bigcap_{i=1}^{n} \mathcal{C}_G(x_i)$$

temos, pelo Lema 1.4, que $[G : \mathcal{Z}(G)] < \infty$. ■

Lema 1.8 (Schur) *Seja G um grupo tal que $[G : \mathcal{Z}(G)] = n$. Então G' é finito e*

$$|G'| \leq (n^2)^{n^3}.$$

■

Seja G um grupo. Dizemos que G é localmente finito se todo subgrupo finitamente gerado de G é finito.

Teorema 1.10 *Seja G um grupo FC. Então G' é um subgrupo de torção e $T(G)$ é um subgrupo característico localmente finito. Além disso, se G é finitamente gerado, então G' é finito.* ■

Lema 1.9 *Seja G um grupo FC finitamente gerado. Então existe um subgrupo H de G tal que*

1. $[G : H] < \infty$.
2. $T(H) = \{1\}$.
3. *H é um subgrupo característico.*

Prova.Como G é FC finitamente gerado, temos, pelo Lema 1.7, que $[G : \mathcal{Z}(G)] < \infty$ e, $\mathcal{Z}(G)$ é finitamente gerado e abeliano. Portanto,

$$\mathcal{Z}(G) = T(\mathcal{Z}(G)) \times H,$$

$H \simeq \mathbb{Z}^m$, para algum $m \in \mathbb{N}$, tal que $T(H) = \{1\}$. $H \trianglelefteq G$, pois $H \subseteq \mathcal{Z}(G)$.

$$[\mathcal{Z}(G) : H] = |T(\mathcal{Z}(G))| < \infty.$$

Como

$$[G : H] = [G : \mathcal{Z}(G)][\mathcal{Z}(G) : H],$$

temos que $[G : H] < \infty$ e $T(H) = \{1\}$. ■

Lema 1.10 *Seja G um grupo FC. Então existe um subgrupo normal H de G tal que*

1. $T(H) = \{1\}$;
2. *$\frac{G}{H}$ é um grupo de torção.*

Prova.1. Se $T(G) = G$, nada há para ser provado. Caso contrário, existe $g_0 \in G$ tal que $o(g_0) = \infty$. Seja

$$N = \left\langle x^{-1} g_0 x : x \in G \right\rangle .$$

Então N é normal em G e finitamente gerado, pois $g_0 \in \Phi(G) = G$. Pelo Lema 1.9, existe um subgrupo H de N tal que H é um subgrupo característico, $T(H) = \{1\}$ e $[N : H] < \infty$. Logo, pela Proposição 1.3, H é um subgrupo normal de G.

2. A família

$$\mathcal{F} = \{K : \{1\} \neq K \trianglelefteq G \text{ e } T(K) = \{1\}\}.$$

é não vazia, pelo item 1 e parcialmente ordenada por inclusão. Seja $\mathcal{F}'$ qualquer subfamília totalmente ordenada de $\mathcal{F}$. Então

$$H = \bigcup_{K \in \mathcal{F}'} K$$

é um subgrupo normal de G. De fato, $H \neq \emptyset$, pois $1 \in K$, para todo $K \in \mathcal{F}'$. Dados $x, y \in H$, existem $K_1, K_2 \in \mathcal{F}'$ tais que $x \in K_1$ e $y \in K_2$. Assim, $xy^{-1} \in K_1$ ou $xy^{-1} \in K_2$, pois $K_1 \subseteq K_2$ ou $K_2 \subseteq K_1$. Logo $xy^{-1} \in H$, isto é, H é um subgrupo de G. Agora, dados $g \in G$ e $h \in H$, existe $K \in \mathcal{F}'$ tal que $h \in K$. Logo,

$$g^{-1} h g \in K$$

e, assim, $g^{-1} h g \in H$, isto é, H é normal em G. Além disso, se $h \in T(H)$, então existe $K \in \mathcal{F}'$ tal que $h \in K$. Assim, $h \in T(K) = \{1\}$, isto é, $h = 1$ e, portanto, $T(H) = \{1\}$. Portanto, $H \in \mathcal{F}$. Isto prova que cada subfamília totalmente ordenada de $\mathcal{F}$ tem uma cota superior em G. Assim, pelo Lema de Zorn, existe $M \in \mathcal{F}$ maximal.

Seja $\pi : G \to \overline{G}$ a projeção canônica, onde $\overline{G} = \frac{G}{M}$. Então, pelo Lema 1.6, $\overline{G}$ é um grupo FC. Suponhamos que $T(\overline{G}) \neq \overline{G}$, isto é, existe $\overline{g}_0 \in \overline{G}$ tal que $o(\overline{g}_0) = \infty$ e

$$\langle \overline{g}_0 \rangle \trianglelefteq \overline{G}.$$

Então, pelo item 1., existe $\{\overline{1}\} \neq \overline{K} \trianglelefteq \overline{G}$ tal que $T(\overline{K}) = \{\overline{1}\}$. Seja $M_0 = \pi^{-1}(\overline{K})$. Então, pelo Teorema da Correspondência, M_0 é um subgrupo normal de G, com $M \subseteq M_0$, pois

$$M = \pi^{-1}(\langle \overline{1} \rangle) \subseteq \pi^{-1}(\overline{K}) = M_0.$$

Sejam $h \in T(M_0) \subset M_0$ e $\overline{h} = \pi(h)$. Então

$$\pi|_{\langle h\rangle} : \langle h\rangle \to \pi(\langle h\rangle)$$

é injetora, pois $T(M) = \{1\}$. Logo, $\langle h\rangle \simeq \pi(\langle h\rangle)$. Assim, $o(\pi(h)) = o(h) < \infty$. Mas $\pi(h) \in \pi(M_0) = \overline{K}$ e $\pi(h) \in T(\overline{K}) = \{\overline{1}\}$. Portanto,

$$1 = o(\pi(h)) = o(h).$$

Logo, $h = 1$ e $T(M_0) = \{1\}$. Assim, $M_0 \in \mathcal{F}$, com $M \subsetneq M_0$, o que contradiz a maximalidade de M. Portanto, $\overline{G} = T(\overline{G})$. ■

1.6 Derivações

Sejam K e Q grupos. Dizemos que um grupo G é uma *extensão* de K por Q se G contém um subgrupo normal H tal que

$$H \simeq K \text{ com } \frac{G}{H} \simeq Q.$$

Sejam G um grupo,K e Q subgrupos de G. Dizemos que Q é um *complemento* de K em G se

$$K \cap Q = \{1\} \text{ e } KQ = G.$$

Uma tripla ordenada (Q, K, θ) é chamada uma *data* se K é um grupo abeliano, Q um grupo e $\theta : Q \to \mathrm{Aut}(K)$ é um homomorfismo de grupos. Dizemos que um grupo G *realiza* esta data se G é uma extensão de K por Q e para qualquer transversal $T : Q \to G$,

$$a^x = \theta(a) = T(x)^{-1}aT(x), \forall x \in Q \text{ e } a \in K.$$

Seja (Q, K, θ) uma data , onde θ é um homomorfismo, não necessariamente trivial, que induz uma ação de Q em K. Uma *derivação* ou *homomorfismo cruzado* é uma função

$$d : Q \to K$$

tal que $d(xy) = d(x)^y d(y)$, para todos $x, y \in Q$, onde $d(x)^y = y^{-1}d(x)y$. Note que $d(1) = 1$ e $d(x^{-1}) = (xd(x)x^{-1})^{-1}$.

O conjunto de todas as derivações de Q em K será denotado por

$$\mathrm{Der}(Q, K).$$

Em particular, se θ é trivial, então

$$\mathrm{Der}(Q,K) = \mathrm{Hom}(Q,K).$$

O conjunto $\mathrm{Der}(Q,K)$ pode ser equipado com uma estrutura de grupo abeliano do seguinte modo:

$$(d+d')(x) = d(x)d'(x), \forall d, d' \in \mathrm{Der}(Q,K) \text{ e } x \in Q,$$

com elemento identidade é 0 e $-d$ é a inversa de d.

Para cada $a \in K$, a função $d_a : Q \to K$ definida por $d_a(x) = (x,a)$ é uma derivação. De fato, dados $x, y \in Q$,

$$\begin{aligned} d_a(xy) &= (xy,a) \\ &= (x,a)^y(y,a) \\ &= d_a(x)^y d(y). \end{aligned}$$

Neste caso, dizemos que d_a é uma *derivação interna*. O subconjunto de todas as derivações internas será denotado por

$$\mathrm{Inn}(K,Q).$$

Dados $a, b \in K$, obtemos

$$\begin{aligned} d_{ab^{-1}}(x) &= (x, ab^{-1}) \\ &= (x,b)^{-1}(x,a) \\ &= (x,a)(x,b)^{-1}, \end{aligned}$$

pois K é abeliano. Assim,

$$\begin{aligned} d_{ab^{-1}}(x) &= d_a(x)d_b(x)^{-1} \\ &= d_a(x) - d_b(x) \\ &= (d_a - d_b)(x), \forall x \in Q. \end{aligned}$$

Portanto, $\mathrm{Inn}(Q,K)$ é um subgrupo normal de $\mathrm{Der}(Q,K)$.

Seja (Q,K,θ) uma data. O grupo quociente

$$H^1(Q,K) = \frac{\mathrm{Der}(Q,K)}{\mathrm{Inn}(Q,K)}$$

é chamado de *primeiro grupo de cohomologia*.

Observação 1.2 *Se* $H^1(Q,K) = \{0\}$*, então toda derivação é interna.*

Lema 1.11 (Schur-Zassenhauss) *[5]Sejam* G *um grupo finito e* N *um subgrupo normal em* G *tal que* $\mathrm{mdc}(|N|, [G:N]) = 1$*. Então existe um subgrupo* H *de* G *tal que*

$$G = N \rtimes H.$$

Além disso, se K *for outro subgrupo de* G *tal que*

$$G = N \rtimes K$$

então $K = g^{-1}Hg$*, para algum* $g \in G$*.* ■

Corolário 1.4 *Se* $\mathrm{mdc}(|Q|, |K|) = 1$*, então* $H^1(Q,K) = \{0\}$*.* ■

Capítulo 2

Anéis de Grupos

Neste capítulo apresentaremos alguns resultados básicos sobre anéis e anéis de grupos necessários 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 sob a adição.
2. $x(yz) = (xy)z$, para todos x, y, $z \in R$.
3. $x(y + z) = xy + xz$, $(x + y)z = xz + yz$, para todos x, y, $z \in R$.

   Se um anel R satisfaz as propriedades:

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

   Se um anel R satisfaz a propriedade:

6. Para todos $x, y \in R$, $xy = 0 \Rightarrow x = 0$ 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 todos $x, y \in S$, tem-se $x - y \in S$;
2. para todos $x, y \in S$, tem-se $xy \in S$;
3. $1 \in S$.

Um subconjunto não vazio I de um anel R é um *ideal à esquerda* (*à direita*) de R se as seguintes condições são satisfeitas:

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

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

1. para todos $x, y \in I$, tem-se $x - y \in I$;
2. Para todo $x \in I$ e $r \in R$, tem-se $rx \in I$ 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 um anel e I um ideal à esquerda de R. Dizemos que I é *minimal* se as seguintes condições são satisfeitas:

1. $I \neq \{0\}$;

2. Se J um ideal à esquerda de R tal que $J \neq \{0\}$ e $J \subseteq I$, então $J = I$.

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 todos x, $y \in R$;

2. $\phi(xy) = \phi(x)\phi(y)$, para todos $x, y \in R$.

Um homomorfismo de anéis $\phi : R \longrightarrow S$ é um *isomorfismo* se ϕ é 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 todos $r, s \in R$ 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 todos $r, s \in R$ 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.

Um R-módulo M é chamado *semisimples* (completamente redutível) se todo submódulo de M é um somando direto. Um anel R é chamado *semisimples* se R visto como R-módulo é semisimples.

Teorema 2.2 *Seja R um anel. As seguintes afirmações são equivalentes*:

1. *Todo R-módulo é semisimples.*

2. *R é um anel semisimples.*

3. *R é soma direta de um número finito de ideais a esquerda minimais.* ■

Proposição 2.1 *Seja*

$$R = L_1 \oplus \cdots \oplus L_t,$$

onde L_i são ideais à esquerda minimais de R. Então existe uma família

$$\{e_1, \ldots, e_t\}$$

de elementos de R tais que:

1. *$e_i \neq 0$ é um idempotente, $1 \leq i \leq t$.*

2. *Se $i \neq j$, então $e_i e_j = 0$.*

3. *$1 = e_i + \cdots + e_t$.*

4. *Cada e_i não pode ser escrito como $e_i = e_i' + e_i^{\text{J}}$, onde e_i', e_i^{J} são idempotentes tais que*

$$e_i', e_i^{\text{J}} \neq 0 \ \ e \ \ e_i' \cdot e_i^{\text{J}} = 0, 1 \leq i \leq t.$$

5. $L_i = Re_i = \langle e_i \rangle$, $1 \leq i \leq t$.

Reciprocamente, se existir uma família de idempotentes satisfazendo as condições 1 *a* 4 *acima, então os ideais* $L_i = Re_i$ *são ideais à esquerda minimais de* R *tais que*

$$R = L_1 \oplus \cdots \oplus L_t.$$

■

Uma família de idempotentes $\{e_1, \cdots, e_t\}$ de um anel R satisfazendo as condições 1., 2. e 3. do Teorema acima é chamada uma *família completa de idempotentes ortogonais*. Um idempotente satisfazendo a condição 4. acima é chamado *primitivo*.

Um anel R é chamado *simples* se, e somente se, os únicos ideais são $\{0\}$ e R.

Teorema 2.3 *Seja* R *um anel semisimples tal que*

$$R = L_1 \oplus \cdots \oplus L_t,$$

onde L_i *são ideais minimais de* R. *Então existe uma família*

$$\{e_1, \ldots, e_t\}$$

de elementos de R *tais que*:

1. $e_i \neq 0$ *é um idempotente central,* $1 \leq i \leq t$.
2. *Se* $i \neq j$, *então* $e_i \cdot e_j = 0$.
3. $1 = e_i + \cdots + e_t$.
4. e_i *não pode ser escrito como* $e_i = e_i' + e_i^{\text{J}}$, *onde* e_i', e_i^{J} *são idempotentes centrais tais que*

$$e_i', e_i^{\text{J}} \neq 0 \ \ e \ \ e_i' \cdot e_i^{\text{J}} = 0, 1 \leq i \leq t.$$

■

Os elementos $\{e_1, \ldots, e_t\}$ no teorema acima são chamados *idempotentes centrais primitivos* de 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 em 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 $a \in G$, $x \in F$ 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 de representação* e a *dimensão* da representação φ é a dimensão de V. Se ρ e φ são representações do grupo G com espaços de representações 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

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

Sejam $\dim V = n$,

$$M_n(F) = \{\mathbf{A} : \mathbf{A} \text{ é uma matriz de ordem } n \text{ sobre } F\}$$

e

$$\mathrm{GL}_{\ n}(F) = \{\mathbf{A} \in M_n(F) : \det(\mathbf{A}) \neq 0\}.$$

Então fixada uma base para V sobre F podemos definir um isomorfismo entre $\mathrm{GL}(V)$ e $\mathrm{GL}_n(F)$ associando cada elemento de $\mathrm{GL}(V)$ a sua matriz na base fixada em $\mathrm{GL}_n(F)$.

Uma representação matricial de G sobre F de grau n é um homomorfismo $\phi : G \longrightarrow \mathrm{GL}_n(F)$. Assim, se

$$T : \mathrm{GL}_{\ n}(F) \longrightarrow \mathrm{GL}(V)$$

é um isomorfismo, então

$$T\phi : G \longrightarrow \mathrm{GL}(V)$$

é uma representação de G. De modo análogo, a cada representação de G,

$$\phi : G \longrightarrow \mathrm{GL}(V),$$

podemos associar uma representação matricial

$$T^{-1}\phi : G \longrightarrow \mathrm{GL}_{\ n}(F).$$

Por causa disto, não faremos distinção explícita entre representação e representação matricial. Seja

$$\phi : G \longrightarrow \mathrm{GL}_n(F)$$

definida por $\phi(a) = \mathbf{I}$, para todo $a \in G$. Então ϕ é claramente uma representação de G, e é chamada de *representação trivial* quando $n = 1$.

Observação 2.2 *Uma representação de dimensão* 1 *de um grupo* G *é um homomorfismo* $\psi : G \longrightarrow F^*$.

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

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

$$\mathrm{supp}(\lambda) = \{g \in G : \lambda(g) \neq 0\}.$$

Seja

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

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

$$\lambda = \sum_{g \in G} \lambda(g)g, \mu = \sum_{g \in G} \mu(g)g \in RG,$$

dizemos que

$$\lambda = \mu \Leftrightarrow \lambda(g) = \mu(g), \forall g \in G.$$

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

$$\lambda + \mu = \sum_{g \in G} (\lambda(g) + \mu(g))g \text{ e } \lambda\mu = \sum_{k \in G} \nu(k)k,$$

onde

$$\nu(k) = \sum_{gh=k} \lambda(g)\mu(h) = \sum_{g \in G} \lambda(g)\mu(g^{-1}k).$$

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 λ podemos escrever

$$\lambda = \sum_{i=1}^{n} \lambda_i g_i,$$

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

$$(\lambda(g)g)(\mu(h)h) = \lambda(g)\mu(g)gh, \forall g, h \in G.$$

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

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

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

Observação 2.3 *RG é um anel comutativo se, e somente se, G e R são comutativos.*

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

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

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

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

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

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

é um homomorfismo de anéis, com

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

Como

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

temos que

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

Note que

$$\alpha \in \Delta_R(G,N) \Leftrightarrow \varphi(\alpha) = 0 \Leftrightarrow \sum_{i=1}^{k}\sum_{n\in N}\alpha(g_in)\varphi(g_i)\varphi(n) = 0$$

$$\Leftrightarrow \sum_{i=1}^{k}\left(\sum_{n\in N}\alpha(g_in)\right)\varphi(g_i) = 0 \Leftrightarrow \sum_{n\in N}\alpha(g_in) = 0, \forall i.$$

Portanto,

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

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

Observação 2.4 *Se G é finito e R é comutativo, então $\Delta_R(G)$ é um R-módulo livre de posto $|G|-1$.*

2.3 Unidades Triviais

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

Observação 2.5 *Seja $u \in \mathcal{U}(\mathbb{Z}G)$. Então $\varepsilon(u) = \pm 1$. Portanto, podemos escrever*

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

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 todos $\gamma, \beta \in \mathbb{Z}G$ 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 2.2 *Para $\gamma \in \mathbb{Z}G$, $\gamma\gamma^* = 1$ se, e somente se, $\gamma = \pm g$, $g \in G$.*

Prova. Claramente se $\gamma = \pm g$, $\gamma^* = \pm g^{-1}$ e $\gamma\gamma^* = 1$. Reciprocamente, suponhamos que

$$\gamma = \sum_{g\in G} \gamma(g)g, \gamma^* = \sum_{g\in G} \gamma(g)g^{-1}, \text{ com } \gamma\gamma^* = 1.$$

Então

$$1 = \gamma\gamma^* = \sum_{g\in G} \gamma^2(g)\cdot 1 + \sum_{g\neq 1} \gamma(g)g.$$

Logo,

$$\sum_{g\in G} \gamma^2(g) = 1$$

e, portanto, $\gamma(g_0) = \pm 1$ para um único g_0, pois $\gamma(g) \in \mathbb{Z}, \forall g \in G$. Assim,

$$\gamma = \sum_{g\in G} \gamma(g)g = \sum \gamma(g_0)g_0 + \sum_{g\neq g_0} \gamma(g)g = \pm g_0.$$

■

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

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

Mas então

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

onde ϵ_i, $1 \leq i \leq n$, são as raízes m-ésima 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

$$\rho_R^*(\alpha) = \epsilon_1 I = \pm I = \rho_R^*(\pm 1)$$

sendo ρ_R^* injetora segue que $\alpha = \pm 1$. ■

Corolário 2.1 *Sejam $\gamma \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$, de ordem finita, e G um grupo finito. Então γ é da forma $\pm g$, com $g \in \mathcal{Z}(G)$.*

Prova. Seja

$$\gamma = \sum_{g \in G} \gamma(g)\, g$$

um elemento central de ordem finita m. Suponhamos que

$$\gamma(g_0) \neq 0$$

para algum $g_0 \in G$. Então γg_0^{-1} é também uma unidade de ordem finita em $\mathbb{Z}G$. Além disso, temos que o coeficiente de 1 na expressão de γg_0^{-1} é $\gamma(g_0) \neq 0$. Pela Proposição 2.3 obtemos que,

$$\gamma g_0^{-1} = \pm 1.$$

Portanto,

$$\gamma = \pm g_0.$$

■

Teorema 2.4 *Seja G um grupo finito. Então $T(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))) = \mathcal{Z}(G)$.* ■

Lema 2.1 *Seja G é 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, $\mathcal{U}_1(\mathbb{Z}G) = \pm G$. ■

Teorema 2.5 (Kaplansky) [7]*Sejam G um grupo finito e K um corpo de característica 0. Suponha que $e = e^2 = \sum e(g)g \in KG$. Então*

1. $0 \leq e(1) \leq 1$,
2. $e(1) = 0 \Leftrightarrow e = 0$, *e* $e(1) = 1 \Leftrightarrow e = 1$. ■

Teorema 2.6 (Passman-Bass) [7]*Sejam $\gamma \in \mathbb{Z}G, \gamma^m = 1$ e $\gamma \neq \pm 1$. Então $\gamma(1) = 0$.* ■

Corolário 2.2 *Suponhamos que $\gamma \in \mathbb{Z}G$ tem a propriedade de comutar com γ^*. Se γ é uma unidade de ordem finita, então $\gamma = \pm g_0$ para algum $g_0 \in G$.*

Prova. Seja n a ordem de γ , como $\gamma\gamma^* = \gamma^*\gamma$, temos que $(\gamma\gamma^*)^n = 1$. Além disso,

$$(\gamma\gamma^*)(1) = \sum \gamma(g)^2 \neq 0.$$

Pelo Teorema 2.6, temos que $\gamma\gamma^* = 1$. Consequentemente $\sum \gamma(g)^2 = 1$. Portanto, existe um único coeficiente $\gamma(g_0)$ o qual é diferente de zero. Assim, concluímos que $\gamma = \pm g_0$. ■

Sejam 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 um 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 $\alpha = \sum_{g \in G} \alpha(g)g \in RG$, definimos

$$\widetilde{\alpha}(g) = \sum_{h \sim g} \alpha(h),$$

onde $\sim$ denota a conjugação em G, isto é, $h = aga^{-1}$, para algum $a \in G$. Isto é a soma dos coeficicientes de α na classe de conjugação de g.

Lema 2.2 *Sejam G um grupo e R um anel comutativo. Então*:

1 $[RG, RG] = \{\sum_{1}^{n} r_i[g_i, h_i] : n \in \mathbb{N}, g_i, h_i \in G\}$

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

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

temos que

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

■

2.4 Normalizador de G em $\mathcal{U}(\mathbb{Z}G)$

Seja G um grupo arbitrário, denotamos por $\mathcal{N}_{\mathcal{U}}(G)$ o normalizador de G em $\mathcal{U} = \mathcal{U}(\mathbb{Z}G)$. Os elementos centrais de $\mathcal{U}$, claramente normalizam G, bem como todos os elementos de G. Até recentemente um problema em aberto foi, (cf. [8, problem 43, pg 305]),

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

isto é, o normalizador de G em $\mathcal{U}$ é $\langle G, \mathcal{Z}(\mathcal{U})\rangle$. Como $\mathcal{U} = \pm\mathcal{U}_1(\mathbb{Z}G)$, muitas vezes trabalharemos com $\mathcal{N}_{\mathcal{U}_1}(G)$, $\mathcal{U}_1 = \mathcal{U}_1(\mathbb{Z}G)$. Assim, temos a condição do normalizador

$$\mathcal{N}_{\mathcal{U}_1}(G) = G\mathcal{Z}(\mathcal{U}_1) \qquad \text{(NP)}$$

O grupo $\mathcal{N}_{\mathcal{U}_1}(G)$ age por conjugação em G, e o grupo dos automorfismo de G obtido desta maneira é denotado por $\mathrm{Aut}_{\mathbb{Z}}(G)$, ou seja,

$$\underset{\mathbb{Z}}{\mathrm{Aut}}(G) = \{\varphi \in \mathrm{Aut}(G) : \exists u \in \mathcal{U}(\mathbb{Z}G) \text{ tal que } \varphi(g) = u^{-1}gu\}.$$

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, $u^*u \in \mathcal{Z}(\mathbb{Z}G)$.*

Prova. Sejam $u \in \mathcal{N}_{\mathcal{U}_1}(G)$ e $\varphi \in \mathrm{Aut}_{\mathbb{Z}}(G)$ tal que $\varphi(x) = u^{-1}xu$. Aplicando $(*)$, em ambos os lados de $\varphi(x) = u^{-1}xu$, obtemos

$$(\varphi(x))^* = \left(u^{-1}xu\right)^* = u^*x^{-1}(u^{-1})^*.$$

Assim, substituindo x por x^{-1}, obtemos

$$\begin{aligned} \left(\varphi(x^{-1})\right)^* &= u^*x(u^*)^{-1} \\ \left(\varphi(x)^{-1}\right)^* &= u^*x(u^*)^{-1} \\ \varphi(x) &= u^*x(u^*)^{-1}. \end{aligned}$$

Logo,

$$x = (u^*)^{-1}\varphi(x)u^*.$$

Assim,

$$(uu^*)^{-1}x\,(uu^*) = (u^*)^{-1}\left(u^{-1}xu\right)u^* = (u^*)^{-1}\varphi(x)u^* = x.$$

Portanto, $uu^* \in \mathcal{Z}(\mathbb{Z}G)$. Além disso, como $uuu^* = uu^*u$ temos que $uu^* = u^*u \in \mathcal{Z}(\mathbb{Z}G)$.

Reciprocamente, seja $u^*u \in \mathcal{Z}(\mathbb{Z}G)$. Então $u^*u = uu^*$, queremos mostrar que $u^{-1}xu \in G$, para todo $x \in G$. Temos

$$(u^{-1}xu)(u^{-1}xu)^* = u^{-1}xuu^*x^{-1}(u^*)^{-1} = u^{-1}uu^*(u^*)^{-1} = u^*(u^*)^{-1} = 1$$

segue da Proposição 2.2 que $(u^{-1}xu) \in G$. ■

Lema 2.3 *Seja $u \in \mathcal{N}_{\mathcal{U}}(G)$. Então $u \in G\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ se, e somente se, $\varphi_u \in \mathrm{Inn}(G)$.*

Prova. Suponhamos que $u = g_0z$, $g_0 \in G$, $z \in \mathcal{Z}(\mathbb{Z}G)$. Assim, para todo $g \in G$

$$\varphi_u(g) = u^{-1}gu = (g_0z)^{-1}gg_0z = z^{-1}(g_0^{-1}gg_0)z = \varphi_{g_0}(g).$$

Portanto $\varphi_u = \varphi_{g_0}$. Reciprocamente, suponha que $\varphi_u \in \mathrm{Inn}(G)$, isto é, $\varphi_u = \varphi_{g_0}$, para algum $g_0 \in G$. Assim, para todo $g \in G$

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

ou

$$g = ug_0^{-1}gg_0u^{-1} = (ug_0^{-1})g(ug_0^{-1})^{-1}$$

e $ug_0^{-1} = z \in \mathcal{U}(\mathbb{Z}G)$, logo para todo $g \in G$

$$g = z^{-1}gz \Rightarrow z \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G)).$$

Portanto,

$$ug_0^{-1} = z \in \mathcal{Z}(\mathcal{U}) \Rightarrow u = g_0 z \in G\mathcal{Z}(\mathcal{U})$$

■

Proposição 2.5 (Krempa) *Seja $u \in \mathcal{U}_1(\mathbb{Z}G)$. 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 em G determinado por conjugação de u^2 é interno em G.

Prova. Suponhamos que $u \in \mathcal{N}_{\mathcal{U}_1}(G)$ e seja $\varphi \in \mathrm{Aut}_{\mathbb{Z}}(G)$, tal que $\varphi(x) = u^{-1}xu$. Consideremos $v = u^*u^{-1} \in \mathcal{U}_1$. 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, $\varphi^2 \in \mathrm{Inn}(G)$. ■

Observação 2.6 *Seja $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Então*

1. *$\varphi_{u^2} \in \mathrm{Inn}(G)$, onde $\varphi_{u^2} = \varphi_u^2 = \varphi_u \circ \varphi_u$.*
2. *Se $|G| < \infty \Rightarrow o(\varphi_u) < \infty$*
3. *Se um primo $p \mid o(\varphi_u)$ então $p \mid |G|$*
4. *Se $o(\varphi_u)$ é impar, então $\langle \varphi_u \rangle = \langle \varphi_u^2 \rangle \Rightarrow \varphi_u \in \mathrm{Inn}(G)$*
5. *Se $|G|$ é ímpar então $\mathrm{Aut}_{\mathbb{Z}}(G) = \mathrm{Inn}(G)$*

6. *Suponha* $o(\varphi_u) = 2^n.m$, $2 \nmid m$, *sejam* $\varphi_1 = \varphi_{u^m}$ *e* $\varphi_2 = \varphi_{u^{2^n}}$. *Então* $o(\varphi_1) = 2^n$, $o(\varphi_2) = m$ *e*

$$\langle \varphi_u \rangle = \langle \varphi_1, \varphi_2 \rangle$$

Portanto, $\varphi_u = \varphi_1^i \varphi_2^j$, *para algum* $i, j \in \mathbb{N}$. *Como* $2 \nmid o(\varphi_2)$ *temos que* $\varphi_2 \in \mathrm{Inn}(G)$. *Logo*

$$\varphi_u \in \mathrm{Inn}(G) \Leftrightarrow \varphi_1 \in \mathrm{Inn}(G).$$

Assim, sempre podemos supor que $o(\varphi_u)$ *é uma potência de* 2.

Proposição 2.6 (Coleman) *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 $u : G \to \mathbb{Z}$ 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,

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

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,

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

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* $g \in P$. ■

Proposição 2.7 *A condição* (NP) *vale para qualquer grupo de ordem ímpar.*

Prova. Sejam G um grupo tal que $|G| = s$, com 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,

$$\varphi = \varphi^1 = \varphi^{2l+st} = (\varphi^2)^l(\varphi^s)^t = \varphi^{2l} = (\varphi^l)^2$$

Portanto, φ é interno e, portanto, $u \in G\mathcal{Z}(\mathbb{Z}G)$. ■

Proposição 2.8 (Jackowski e Marciniak) *Condição* (NP) *vale para qualquer grupo de ordem finita com um* 2*-subgrupo de Sylow normal.*

Prova. Sejam G um grupo qualquer, P um 2-subgrupo de Sylow normal e $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Pela Proposição 2.6 existe $z \in G$ tal que $\varphi_u|_P = \varphi_z|_P$, ou seja, $\varphi_{z^{-1}} \circ \varphi_u = \varphi_{z^{-1}u}|_P = Id$. Podemos supor $\varphi_u|_P = Id$.

Afirmação: Existe $g_0 \in G$ tal que $g_0^{-1}u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, ou seja, $u = g_0 z$, com z elemento central de $\mathcal{U}_1(\mathbb{Z}G)$.

De fato, podemos supor que $o(\varphi_u)$ é uma potência de 2 com $\varphi_u : G \longrightarrow G$, como $P \trianglelefteq G$ temos $\overline{G} = \frac{G}{P}$. Defindo $\overline{\varphi}_u : \overline{G} \longrightarrow \overline{G}$ por

$$\overline{\varphi}_u(\overline{g}) = \overline{\varphi_u(g)}.$$

$\overline{\varphi}_u$ está bem definida pois $\varphi_u(P) \subseteq P$. De fato, seja $g \in P$,

$$\varphi_u(g) = u^{-1}gu \in G$$

e é conjugado a g em $\mathcal{U}_1(\mathbb{Z}G)$.

$$u^{-1}gu - g = u^{-1}(gu) - (gu)u^{-1} = [u^{-1}, gu] = \alpha$$

logo,

$$0 = \widetilde{\alpha}(g) = 1 - 1$$

assim,

$$\varphi_u(g) = g^x = x^{-1}gx$$

para algum $x \in G$, portanto,

$$\varphi_u(g) \in P^x = x^{-1}Px = P.$$

Temos que

$$\overline{\varphi_u(g)} = \overline{u^{-1}}\overline{gu} = \varphi_{\overline{u}}(\overline{g}).$$

Como $2 \nmid \left|\overline{G}\right|$, existe $g_0 \in G$ tal que $\overline{\varphi_u(g)} = \overline{\varphi_{g_0}(g)}$ logo, $\overline{\varphi_{g_0^{-1}u}(g)} = \overline{g}$. Escreva $w = g_0^{-1}u$

$$\overline{\varphi_w(g)} = \overline{g} \Rightarrow \overline{\varphi_w(g)g^{-1}} = \overline{1} \Rightarrow \varphi_w(g)g^{-1} \in P.$$

Defina $\rho(g) = \varphi_w(g)g^{-1}$, assim,

$$\varphi_w(g) = \rho(g)g, \rho(g) \in P, \forall g \in G,$$

e $o(\varphi_u) = 2^n$. $\overline{\varphi}_u$ é um automorfismo interno, assim existe $\overline{g}_0 \in \overline{G}$ tal que $\overline{\varphi}_u = \varphi_{\overline{g}_0}$

$$o(\varphi_u) = 2^n \Rightarrow o(\overline{\varphi}_u)|_{2^n}$$

Assim, $x = \varphi_{\overline{g}_0}^{2^n}(x) = \overline{g}_0^{-2^n} x \overline{g}_0^{2^n}$, isto implica que $o(\overline{g}_0)$ $|_{2^n}$. Mas $o(\overline{g}_0)$ também divide a ordem de $\overline{G}$, $\left|\overline{G}\right|$ é ímpar. Portanto,

$$o(\overline{g}_0) = 1 \Rightarrow \overline{g}_0 = 1.$$

$$\overline{\varphi_u(g)} = \varphi_{\overline{1}}(\overline{g}) = \overline{g} \Rightarrow \varphi_u(g) = \rho(g)g, \rho(g) \in P.$$

$$\varphi_u^2(g) = \varphi_u(\varphi_u(g)) = \varphi_u(\rho(g)g) = \varphi_u(\rho(g))\varphi_u(g) = \rho(g)\rho(g)g = \rho^2(g)g.$$

Seja $x \in P$ e $g \in G$. Então $g^{-1}xg \in P$. Logo

$$\begin{aligned} g^{-1}xg &= \varphi_u(g^{-1}xg) \\ &= \varphi_u(g)^{-1}x\varphi_u(g) \\ &= (\rho(g)g)^{-1}x(\rho(g)g) \\ &= g^{-1}(\rho(g)^{-1}x\rho(g))g. \end{aligned}$$

Assim,

$$x = \rho(g)^{-1}x\rho(g), \ \ \forall g \in G.$$

Portanto, $\rho(g) \in \mathcal{Z}(P)$.

$$\rho(g) = \varphi_u(g)g^{-1} = u^{-1}gug^{-1} = (u, g^{-1}).$$

Logo, obtemos uma derivação

$$\rho : G \longrightarrow A = \mathcal{Z}(P).$$

Se $g \in P$, temos que $\rho(g) = \varphi_u(g)g^{-1} = gg^{-1} = 1$. Assim , obtemos uma derivação

$$\overline{\rho} : \frac{G}{P} \longrightarrow A$$

tal que $\overline{\rho}(\overline{g}) := \rho(g)$. Logo, $\overline{\rho}$ está bem definida. Como $(\left|\frac{G}{P}\right|, |A|) = 1$, pelo Lema 1.4 $H^1(\frac{G}{P}, A) = 0$. Portanto $\overline{\rho}$ é interno, logo ρ é interno e, portanto, φ_u é interno. ■

Proposição 2.9 *Se $u \in N_{\mathcal{U}_1}(G)$ e $u^n \in G$ para qualquer inteiro positivo n, então $u \in G$.*

Prova. Seja $u \in \mathcal{N}_{\mathcal{U}_1}(G)$ e $u^n = g \in G$ para algum inteiro positivo n. Como $u \in \mathcal{N}_{\mathcal{U}_1}(G)$ sabemos que $u^*u = uu^* \in \mathcal{Z}(\mathbb{Z}G)$. Devido $u^n \in G$ obtemos que

$$(u^*u)^n = (u^n)^*u^n = g^{-1}g = 1.$$

Assim, u^*u é uma unidade central periódica e, portanto, $u^*u \in \mathcal{Z}(\mathbb{Z}G)$. Escreva

$$u = \sum_{g \in G} u_g g, u_g \in \mathbb{Z}$$

como

$$(u^*u)(1) = \sum (u(g))^2 \neq 0$$

pela Proposição 2.3 temos que $u^*u = 1$ e, portanto, $u \in G$. ■

Capítulo 3

Problema do Normalizador

Neste capítulo apresentaremos o Teorema da Representação para unidades normalizadas e, em seguida aplicaremos o teorema para mostrar que o problema do normalizador vale para três classes de grupos. Terminamos mostrando que o problema vale para qualquer grupo FC com subgrupo comutador um p-grupo.

O centro de conjugação finita de um grupo G é denotado por $\Delta(G)$ e seu subgrupo de torção por $\Delta^+(G)$. Se $\Delta(G)$ é finitamente gerado, então seu centro é de índice finito e, $\Delta^+(G)$ é um grupo finito, com $\frac{\Delta(G)}{\Delta^+(G)}$ abeliano livre finitamente gerado.

3.1 Redução para grupos finitos

Iniciamos analisando o suporte de elementos do $\mathcal{N}_{\mathcal{U}(RG)}(G)$.

Lema 3.1 *Sejam G um grupo e R um anel com unidade. Se $u \in \mathcal{N}_{\mathcal{U}(RG)}(G)$, então*

$$\begin{aligned} \sigma \ &: \ G \longrightarrow S_{\mathrm{supp}(u)} \\ &\quad g \longmapsto \sigma_g \end{aligned}$$

é um homomorfismo, onde

$$\sigma_g(h) = ghu^{-1}g^{-1}u.$$

Além disso, se $1 \in \mathrm{supp}(u)$ então $\ker\sigma = \mathcal{C}_G(\mathrm{supp}(u))$. Assim, $\frac{G}{\mathcal{C}_G(\mathrm{supp}(u))}$ é isomorfo a um subgrupo de $S_{\mathrm{supp}(u)}$ e, portanto, $u \in R\Delta(G)$.

Prova. Suponha $u \in \mathcal{N}_{\mathcal{U}(RG)}(G)$ e seja $X = \mathrm{supp}(u)$. Escreva

$$u = \sum_{x \in X} u(x)x, \quad u(x) \in R.$$

Para cada $g \in G$ existe $g^u = u^{-1}gu \in G$ tal que $gu = ug^u$, isto é,

$$g\left(\sum_{x\in X} u(x)x\right) = \sum_{x\in X} u(x)gx = \left(\sum_{x\in X} u(x)x\right) g^u.$$

Assim, para todo $x \in X$ existe um único $\sigma_g(x) \in X$ tal que $gx = \sigma_g(x)g^u$. Portanto, $\sigma_g : X \longrightarrow X$ definida por

$$\sigma_g(x) = gxg^{-1} = gx(u^{-1}g^{-1}u)$$

é uma permutação de X. Note que

$$\begin{aligned}
\sigma_{g_1g_2}(x) &= g_1g_2xu^{-1}(g_1g_2)^{-1}u \\
&= g_1(g_2x(u^{-1}g_2^{-1}u)u^{-1}g_1^{-1} \\
&= g_1\sigma_{g_2}(x)u^{-1}g_1^{-1}u \\
&= \sigma_{g_1}\sigma_{g_2}(x).
\end{aligned}$$

Assim, $\sigma_{g_1g_2} = \sigma_{g_1} \circ \sigma_{g_2}$. Logo a função

$$\begin{aligned}
\sigma &: G \longrightarrow S_X \\
&\quad g \longmapsto \sigma_g
\end{aligned}$$

é um homomorfismo de grupos.

Mostraremos agora que, $\ker\sigma = \mathcal{C}_G(X)$ se $1 \in X$. Note que,

$$\begin{aligned}
\ker\sigma &= \{g \in G : \sigma_g = Id\} \\
&= \{g \in G : \sigma_g(x) = x, \quad \forall x \in X\} \\
&= \{g \in G : gxu^{-1}g^{-1}u = x, \quad \forall x \in X\} \\
&= \{g \in G : x^{-1}gx = u^{-1}gu, \quad \forall x \in X\}.
\end{aligned}$$

Como $1 \in X$, obtemos $g = u^{-1}gu$ e, portanto,

$$\begin{aligned}
\ker\sigma &= \{g \in G : x^{-1}gx = g, \quad \forall x \in X\} \\
&= \{g \in G : xg = gx, \quad \forall x \in X\} \\
&= \mathcal{C}_G(X).
\end{aligned}$$

Pelo primeiro Teorema de Isomorfismo temos,

$$\frac{G}{\mathcal{C}_G(X)} \simeq \mathrm{Im}(\sigma) \leq S_{\mathrm{supp}(u)} \Rightarrow X \subset \Delta(G).$$

Assim, $u \in R\Delta(G)$. ■

Para mostrarmos que em um grupo G qualquer os elementos do normalizador $\mathcal{N}_{\mathcal{U}_1}(G)$ têm uma presentação da forma gv com $g \in G$ e $v \in \mathcal{U}(\mathbb{Z}N)$ com N um subgrupo normal finito de G, precisamos provar o lema seguinte.

Lema 3.2 *Seja G um grupo FC finitamente gerado. Se $u \in \mathcal{N}_{\mathcal{U}_1}(G)$, então*:

1. *$u^m \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$ para algum inteiro m positivo.*

2. *$u = gw$ para algum $g \in G$ e $w \in \mathcal{U}_1(\mathbb{Z}\Delta^+(G))$.*

Prova. Seja $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Pela Proposição (2.4), $u^2 = gv$ para algum $g \in G$ e $v \in \mathcal{Z}(\mathbb{Z}G) \subseteq \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$. Como G é um grupo FC finitamente gerado, temos pelo Lema 1.7 que, $[G : \mathcal{Z}(G)] = m' < \infty$.

Assim,

$$u^{2m'} = (gv)^{m'} = (g)^{m'}(v)^{m'} \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)).$$

Portanto, $u^m \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$, com $m = 2m'$.

Tome $T = \Delta^+(G)$. Como $\frac{G}{T}$ é um grupo abeliano livre finitamente gerado, podemos escolher um transversal S de T em G tal que $g \in S$ implica $g^{-1} \in S$.

Como $\frac{G}{T}$ é um grupo ordenado, S herda a ordem da identificação natural de S em $\frac{G}{T}$. Escreva

$$u = \sum_{f \in S} u_f f \quad \text{e} \quad u^{-1} = \sum_{f \in S} w_f f^{-1} \tag{3.1}$$

com $u_f, w_f \in \mathbb{Z}T$. Claramente u normaliza T, assim $u\mathbb{Q}T = \mathbb{Q}Tu$, consequentemente $u_f\mathbb{Q}T = \mathbb{Q}Tu_f$ para todo $f \in S$.

Seja E o conjunto de idempotentes centrais primitivos de $\mathbb{Q}T$. Para $e \in E$, seja o conjunto

$$I(e) = \{f \in S : eu_f \neq 0\}.$$

Se $f \in I(e)$ então $u_f e\mathbb{Q}T = e\mathbb{Q}Tu_f = e\mathbb{Q}T$. Assim, $u_f e\mathbb{Q}T$ é um ideal não-nulo da álgebra simples $e\mathbb{Q}T$, consequentemente, eu_f é um unidade de $e\mathbb{Q}T$.

Note que G age em E por conjugação. Afirmamos que $I(e) = I(geg^{-1})$ para todo $e \in E$ e $g \in G$.

De fato, note que $(g^{-1}, u^{-1}) \in G'$ pois g e ugu^{-1} são conjugados e, portanto,

$$(g^{-1}, u^{-1}) = t \in G' \subseteq T(G).$$

Assim, $gug^{-1} = ut^{-1}$ para algum $t \in T$. Portanto,

$$\begin{aligned}\sum_{f\in S}(geg^{-1})u_f f &= geg^{-1}u = geg^{-1}ut^{-1}t = geug^{-1}t = ge\sum_{f\in S}u_f fg^{-1}t = \sum_{f\in S}geu_f fg^{-1}t \\ &= \sum_{f\in S}g(eu_f)g^{-1}(gfg^{-1})t\end{aligned}$$

e, portanto,

$$\begin{aligned}\sum_{f\in S}(geg^{-1})u_f f &= \sum_{f\in S}g(eu_f)g^{-1}(t_f f)t, t_f \in T \\ &= \sum_{f\in S}g(eu_f)g^{-1}(t_f(ftf^{-1})f\end{aligned}$$

onde $t_f \in T$ para cada $f \in S$. Segue que, para cada $f \in S$,

$$geg^{-1}uf = g(eu_f)g^{-1}t_f(ftf^{-1}).$$

Em particular, para cada $f \in S$, $geg^{-1}u_f = 0$ se, e somente se, $eu_f = 0$. Como u é uma unidade é claro que para cada $e \in E$ o conjunto $I(e)$ é não vazio. Agora, mostraremos que cada $I(e)$ consiste de exatamente um elemento o qual será denotado por $f(e)$. Sejam k e l o menor e o maior elemento de $I(e)$, respectivamente. Seja r o maior elemento tal que $ew_r \neq 0$ e seja s o menor elemento tal que $ew_s \neq 0$. Como $I(e) = I(geg^{-1})$, para cada $g \in G$, os valores de r, s não mudam se substituírmos e com qualquer G-conjugado de e. Escreva $kr^{-1} = t_1$ e $ls^{-1} = t_2 n$ para algum $t_1, t_2 \in T$ e $m, n \in S$. Por (3.1), na soma

$$\begin{aligned}e &= e(uu^{-1}) \\ &= e(\sum_{f\in S}u_f f\sum_{h\in S}w_h h^{-1}) \\ &= \sum_{f,h\in S}eu_f(fw_h f^{-1})fh^{-1} \\ &= \sum_{f,h\in S}eu_f[f(f^{-1}efw_h)f^{-1}]fh^{-1}\end{aligned}$$

m é o menor elemento o qual aparece com um coeficiente não nulo $eu_k(ekw_r k^{-1})t_1$ (é não nulo desde que eu_k e $ekw_r k^{-1} = k(k^{-1}ekw_r)k^{-1}$ sejam unidades em $e\mathbb{Q}T$) e n é o maior elemento com coeficiente não nulo $eu_l(elw_s l^{-1})t_2$. Portanto $m = n = 1$ e consequentemente $k = l = r = s = f(e)$. Consequentemente

$$eu = eu_{f(e)}f(e) \quad \text{e} \quad eu^{-1} = ew_{f(e)}f(e)^{-1},$$

como $u = \sum_{e \in E} eu$, temos

$$u_f = \sum_{f(e)=f} eu_f \quad \text{e} \quad w_f = \sum_{f(e)=f} ew_f,$$

como os idempotentes primitivos são ortogonais e o conjunto $\{e \in E : f(e) = f\}$ é G-estável, temos $u_f u_h = 0$ e $u_f g w_h g^{-1} = 0 = g w_h g^{-1} u_f$ para todo $f \neq h \in S$ e para todo $g \in G$. Portanto,

$$1 = uu^{-1} = \sum_{f \in S} u_f f w_f f^{-1}. \tag{3.2}$$

Portanto, para qualquer $f \in S$ temos $u_f = u_f f w_f f^{-1} u_f$, o qual implica que $u_f f w_f f^{-1}$ é um idempotente de $\mathbb{Z}T$. Como a identidade é o único idempotente não nulo de $\mathbb{Z}T$, segue que para cada f o idempotente $u_f f w_f f^{-1}$ é 0 ou 1. Por (3.2), existe exatamente um $f \in S$ tal que este idempotente é 1, isto é, existe exatamente um f tal que $u_f \neq 0$. ■

Teorema 3.1 (Teorema da Representação) *Seja G um grupo e $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Então, existe $g \in G$ tal que $g^{-1}u \in \mathbb{Z}\Delta^+(G)$, isto é, $u = gw$ para algum $g \in G$ e $w \in ZN$, com N um subgrupo normal finito de G. Além disso, w induz um automorfismo φ de ordem um divisor de $2|N|$. No caso em que $|N|$ é ímpar, então φ é interno em G.*

Prova. Seja $X = \text{supp}(u)$. Para provar o resultado considere que $1 \in X$. Segue do Lema 3.1 que $X \subseteq \Delta(G)$. Assim, X tem somente um número finito de conjugados em G e, portanto, $X \subseteq H$, com H um subgrupo normal finitamente gerado de G contido em $\Delta(G)$. Em particular, H é FC finitamente gerado. Assim, $N = T(H)$ é um subgrupo invariante finito de H e $\frac{H}{N}$ é abeliano livre e, portanto, ordenado.

Como $u \in \mathcal{U}_1(\mathbb{Z}H)$, o Lema 3.2 implica que $u = hw$ para algum $h \in H$ e $w \in \mathbb{Z}N$. Como N é normal em G, temos a presentação desejada para u. Claramente $w \in \mathcal{N}_{\mathcal{U}_1}(G)$, assim, pela Proposição 2.5 existe $g_0 \in G$ tal que $g_0^{-1} w^2 = w^* w$.

É Claro que $g_0 \in N$ e induz o mesmo automorfismo em w^2, ou seja, $\varphi_{g_0} = \varphi_{w^2}$. Note que, $\varphi_w^2 = \varphi_{w^2}$.

Seja $k = |N|$. Então

$$\varphi_w^{2k} = \varphi_{w^2}^k = \varphi_{g_0}^k = \varphi_{g_0^k} = \varphi_1 = Id, \quad \text{pois} \quad g_0 \in N.$$

Logo, o automorfismo φ induzido por w tem ordem um divisor de $2|N|$. Para a última parte, assumimos que $|N|$ é ímpar. Pela Proposição 2.7, obtemos que $w = g_1 v$ com $g_1 \in G$

e $v \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}N))$. Agora é suficiente mostrar que o automorfismo φ induzido por v é um automorfismo interno em g.

De fato, para cada $g \in G$

$$\varphi(g) = v^{-1}gv \Rightarrow (v, g^{-1}) = \varphi(g)g^{-1} =: \phi(g).$$

Assim,

$$\varphi(g) = \phi(g)g$$

com $\phi(g) \in N$, pois $(v, g^{-1}) \in G \cap \mathbb{Z}N = N$. φ é a identidade quando restrita a N, pois $v \in \mathcal{Z}(\mathbb{Z}N)$.

Note que $\varphi^2(g) = \varphi \circ \varphi(g) = \varphi(v^{-1}gv)$ e

$$\begin{aligned} \varphi(v^{-1}gv) &= \varphi(\phi(g)g) \\ v^{-1}v^{-1}gvv &= \varphi(\phi(g))\varphi(g) \\ v^{-2}gv^2 &= \phi(g)\phi(g)g \\ v^{-2}gv^2 &= \phi(g)^2 g. \end{aligned}$$

Logo $\varphi^2(g) = v^{-2}gv^2 = \phi(g)^2 g$. Indutivamente, temos

$$\varphi^n(g) = v^{-n}gv^n = \phi(g)^n g, \forall n \in \mathbb{N}.$$

Portanto,

$$\varphi_v^{|N|}(g) = v^{-|N|}gv^{|N|} = \phi(g)^{|N|}g.$$

Como $\phi(g) \in N$, temos

$$\varphi^{|N|}(g) = g, \forall g \in G.$$

Como $|N|$ é ímpar, temos que φ tem ordem ímpar, logo, pela Proposição 2.5, φ^2 é interno. Assim, φ é interno. ■

Corolário 3.1 *Para um grupo qualquer G, os grupos $\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{G}$ e $\frac{\mathcal{Z}(\mathcal{U}_1)}{\mathcal{Z}(G)}$ são isomorfos a um subgrupo do grupo abeliano livre*

$$\frac{\mathcal{Z}(\mathcal{U}_1) \cap \mathcal{U}_1(\mathbb{Z}\Delta^+(G))}{\mathcal{Z}(G) \cap \Delta^+(G)}$$

e, eles todos tem o mesmo posto livre de torção. Além disso, $\mathcal{N}_{\mathcal{U}_1}(G)' = G'$ e, se $\Delta^+(G)$ é finito, todos esses grupos são finitamente gerados .

Prova. Seja

$$\begin{array}{rcl} f & : & \mathcal{N}_{\mathcal{U}_1}(G) \longrightarrow \frac{\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))}{\mathcal{Z}(G)} \\ & & uG \mapsto uu^*\mathcal{Z}(G) \end{array}.$$

Então f é um homomorfismo de grupos injetor e a sua imagem está contida em

$$\frac{\mathcal{Z}(\mathcal{U}_1) \cap \mathcal{U}_1(\mathbb{Z}\Delta^+(G))}{\mathcal{Z}(G) \cap \Delta^+(G)}.$$

De fato,

$$f(uGvG) = f(uvG) = uv(uv)^*\mathcal{Z}(G),$$

pela Proposição 2.4 temos que $vv^* \in \mathcal{Z}(\mathbb{Z}G)$, assim,

$$f(uGvG) = uu^*vv^*\mathcal{Z}(G) = uu^*\mathcal{Z}(G)vv^*\mathcal{Z}(G) = f(uG)f(vG),$$

portanto, f é um homomorfismo.

Seja $uG \in \ker f$, então $f(uG) = \mathcal{Z}(G)$. Logo,

$$uu^*\mathcal{Z}(G) = \mathcal{Z}(G) \Longrightarrow uu^* \in \mathcal{Z}(G).$$

Por outro lado, temos pela Proposição 2.5 que, $u^2 = g(u^*u)$, ou seja, $u^2 \in G$. Assim, pela Proposiçao 2.9, $u \in G$. Portanto, $\ker f = G$ e, assim, f é injetiva.

Pelo primeiro teorema do isomorfismo, temos que

$$\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{G} \simeq \operatorname{Im} f \subseteq \frac{\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))}{\mathcal{Z}(G)}.$$

Além disso, pelo Teorema 3.1, temos que existe $u = vg_0$ tal que $v \in \mathbb{Z}\Delta^+(G)$. Assim,

$$uu^* = vg_0g_0^{-1}v^* = vv^* \in \mathcal{Z}(\mathcal{U}_1) \cap \mathbb{Z}\Delta^+(G).$$

Portanto,

$$\operatorname{Im} f \subset \frac{\mathcal{Z}(\mathcal{U}_1) \cap \mathcal{U}_1(\mathbb{Z}\Delta^+(G))}{\mathcal{Z}(G) \cap \Delta^+(G)}.$$

Temos também que, se $u \in \mathcal{Z}(\mathcal{U}_1)$ então $f(uG) = u^2\mathcal{Z}(G)$. De fato, pelo Proposição 2.5

$$u^2 = g_0(uu^*) \in G\mathcal{Z}(\mathbb{Z}G) \subseteq G\mathcal{Z}(\mathcal{U}_1).$$

Como

$$uu^* = g_0^{-1}u^2 \in \mathcal{Z}(\mathcal{U}_1)$$

temos que $g_0 \in \mathcal{Z}(\mathcal{U}_1)$, logo $g_0 \in \mathcal{Z}(G)$. Assim,

$$f(uG) = uu^*\mathcal{Z}(G) = g_0^{-1}u^2\mathcal{Z}(G) = u^2\mathcal{Z}(G).$$

Portanto, $\frac{\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))}{\mathcal{Z}(G)}$ é periódico (de expoente 2) módulo a imagem de f e, portanto, os grupos abelianos livres de torção $\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{G}$ e $\frac{\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))}{\mathcal{Z}(G)}$ têm o mesmo posto livre. Como $\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{G}$ é abeliano temos que $(\mathcal{N}_{\mathcal{U}_1}(G))' \subseteq G$. Agora considere o homomorfismo canônico

$$\begin{aligned} \varphi \ &: \ \mathbb{Z}G \longrightarrow \mathbb{Z}\left(\tfrac{G}{G'}\right) \\ &\gamma \longrightarrow \overline{\gamma} \end{aligned}$$

Sejam $x, y \in \mathcal{N}_{\mathcal{U}_1}(G)$, então temos que $(x, y) \in (\mathcal{N}_{\mathcal{U}_1}(G))'$, segue que $\pi((x, y)) = 1$. Assim,

$$(x, y) \in 1 + \ker \pi,$$

portanto,

$$(x, y) \in (\mathcal{N}_{\mathcal{U}_1}(G))' \cap (1 + \ker \pi) \subseteq G \cap (1 + \ker \pi).$$

Mas,

$$G \cap (1 + \ker \pi) = G \cap (1 + \Delta(G, G') = G',$$

portanto, $(\mathcal{N}_{\mathcal{U}_1}(G))' \subseteq G'$.

Além disso, se $\Delta^+(G)$ é finito, então é bem conhecido que $\mathcal{Z}(\mathcal{U}_1(\Delta^+)$ é finitamente gerado. Assim, o último resultado segue. ■

Corolário 3.2 *Seja G um grupo tal que $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$ e $\mathcal{N}_{\mathcal{U}_1}(G)$ são grupos finitamente gerados (por exemplo, se G é um grupo finito). Então*

$$\frac{\mathcal{N}_{\mathcal{U}_1}(G)}{\langle G, \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))\rangle}$$

é um 2-grupo abeliano elementar de posto no máximo o posto livre de torção de $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$.

Prova. [cf. [4, corollary 1.6]]. ■

Corolário 3.3 *Seja G um grupo arbitrário. Então, as seguintes condições são equivalentes*

1. $\mathcal{N}_{\mathcal{U}_1}(G) = G$
2. $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G)$, *isto é, todas unidades centrais são triviais*
3. *Todas unidades em $\mathbb{Z}\Delta^+(G)$ que são centrais são triviais*

Prova. (1. $\Rightarrow$ 2.) Seja $u \in \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$. Então $u \in \mathcal{N}_{\mathcal{U}_1}(G) = G$, assim $u \in G$ e, portanto $u \in \mathcal{Z}(G)$. Logo $\mathcal{Z}(\mathcal{U}_1) \subseteq \mathcal{Z}(G)$. Claramente $\mathcal{Z}(G) \subseteq \mathcal{Z}(\mathcal{U}_1)$. Portanto, $\mathcal{Z}(\mathcal{U}_1) = \mathcal{Z}(G)$.

(2. $\Rightarrow$ 3.) Seja $u \in \mathbb{Z}\Delta^+(G)$ central. Então $u \in \mathcal{Z}(\mathcal{U}_1)$. Logo, $u \in \mathcal{Z}(G)$ e, portanto u é trivial.

(3. $\Rightarrow$ 1.) Podemos supor que $G = \langle \mathrm{supp}(u) \rangle$. Dado $u \in \mathcal{N}_{\mathcal{U}_1}(G)$, pelo Lema 3.2, existe m tal que $u^{2m} \in \mathcal{Z}(\mathcal{U}_1) = \mathcal{Z}(G) \subseteq G$. Logo, pela Proposição 2.9, $u \in G$ ■

Terminamos esta seção com uma consequência a respeito de unidades hipercentrais de $\mathcal{U}_1(\mathbb{Z}G)$. Por $\mathcal{Z}_n(H)$ denotamos o n-ésimo centro de um grupo H e por $\widetilde{Z}(H)$ denotamos as unidades hipercentrais, isto é, $\widetilde{Z}(H) = \cup_n \mathcal{Z}_n(H)$.

Proposição 3.1 *Seja G um grupo. Se $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G)$, então $\widetilde{Z}(\mathcal{U}_1(\mathbb{Z}G)) \subseteq G$.*

Prova. Pelo Corolário 3.3, a hipótese $\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}(G)$ é equivalente com $\mathcal{N}_{\mathcal{U}_1}(G) = G$. A hipótese também implica que $\mathcal{Z}_2(\mathcal{U}_1(\mathbb{Z}G)) \subseteq \mathcal{N}_{\mathcal{U}_1}(G)$. De fato, sabemos que

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

seja $u \in \mathcal{Z}_2(\mathcal{U}_1(\mathbb{Z}G))$., Então

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

Assim, para algum $g \in G$,

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

Logo $u^{-1}gu \in G$ para algum $g \in G$. Portanto, $u \in \mathcal{N}_{\mathcal{U}_1}(G) = G$. Assim, $\mathcal{Z}_2(\mathcal{U}_1(\mathbb{Z}G)) \subseteq G$.

Suponhamos agora que $\mathcal{Z}_n(\mathcal{U}_1(\mathbb{Z}G)) \subseteq G$, para algum inteiro positivo n. Seja $\alpha \in \mathcal{Z}_{n+1}(\mathcal{U}_1(\mathbb{Z}G))$. Então para algum $g \in G$, $(\alpha, g) \in \mathcal{Z}_n(\mathcal{U}_1(\mathbb{Z}G)) \subseteq G$. Assim, $\alpha g \alpha^{-1} \in G$ para algum $g \in G$. Portanto, $\alpha \in \mathcal{N}_{\mathcal{U}_1}(G) = G$. Logo, $\mathcal{Z}_n(\mathcal{U}_1(\mathbb{Z}G)) \subseteq G$, para todo $n \in \mathbb{N}$. Assim, $\cup_n \mathcal{Z}_n(\mathcal{U}_1(\mathbb{Z}H)) \subseteq G$ e consequentemente $\widetilde{Z}(\mathcal{U}_1(\mathbb{Z}G)) \subseteq G$, pois $\widetilde{Z}(\mathcal{U}_1(\mathbb{Z}G)) \leq \cup_n \mathcal{Z}_n(\mathcal{U}_1(\mathbb{Z}H))$. ■

3.2 Grupos Satisfazendo a Condição do Normalizador

Nesta seção provaremos que o problema do normalizador vale para várias classes de grupos.

Teorema 3.2 *Seja G um grupo qualquer. Se $\Delta^+(G)$ não tem elementos de ordem 2 então (NP) vale para G.*

Prova. Seja $u \in \mathcal{N}_{\mathcal{U}_1}(G)$, pelo Teorema 3.1, existe um subgrupo normal finito N tal que $w = g_0^{-1}u$, com $w \in \mathbb{Z}N$. $\varphi_u \in \mathrm{Inn}(G)$ se, e somente se, $\varphi_w \in \mathrm{Inn}(G)$. Vamos provar que φ_w é interno.

Sejam $n \in N$ e $g \in G$, $g^{-1}ng \in N$, logo $Cl(n) \subset N$, assim, $|Cl(n)| \leq |N| < \infty$. Logo, $n \in \Delta(G)$. O que implica $N \subset \Delta^+(G)$. Assim, $2 \nmid |N|$ e pelo Teorema 3.1, $\varphi_w \in \mathrm{Inn}(G)$. portanto φ_u é interno.

Teorema 3.3 *Seja G um grupo de torção. Se os 2-elementos de G formam um subgrupo normal de G então (NP) vale para G.*

Prova. Pelo Teorema 3.1 é suficiente mostrar que, se $w \in \mathcal{N}_{\mathcal{U}_1}(G) \cap \mathbb{Z}N$, com N um subgrupo normal finito de G, então $w \in G\mathcal{Z}(\mathbb{Z}G)$. Por hipótese os 2-elementos formam um subgrupo normal S de G. Como $w \in \mathbb{Z}N$, temos que $\mathrm{supp}(w) \subseteq N$. Assim, pela Proposição 2.6 temos que existe $g_0 \in N$ tal que $v = g_0 w$ age trivialmente em S. Como $v \in \mathcal{N}_{\mathcal{U}_1}(G) \cap \mathcal{U}_1(\mathbb{Z}N)$, segue que $(v, G) = \{v^{-1}g^{-1}vg : g \in G\} \subseteq N$. De fato,

$$\begin{aligned}(v,g) &= (g_0^{-1}w, g)\\ &= (g_0^{-1}, g)^w(w,g)\\ &= (g_0 g^{-1} g_0 g)^w(w^{-1}g^{-1}wg) \in \mathbb{Z}N.\end{aligned}$$

Assim, $(v, g) \in G \cap \mathbb{Z}N = N$.

Seja $\varphi = \varphi_v$

$$\begin{aligned}\varphi &: G \longrightarrow G\\ &\quad g \longmapsto v^{-1}gv\end{aligned}$$

Como $S \trianglelefteq G$, para todo $g \in G$ e $x \in S$, temos $g^{-1}xg \in S$, assim,

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

Logo, para todo $g \in G$, $x \in S$

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

isto é,

$$\rho(g) = \varphi(g)g^{-1} \in \mathcal{C}_G(S). \tag{3.3}$$

Pela Proposição 2.5 sabemos que $\varphi^2 = \varphi_{g_1}$ para algum $g_1 \in G$. Como G é de torção segue que φ^2 e, portanto, φ é de ordem finita. Novamente pela Proposição 2.5, podemos assumir que $o(\varphi) = 2^n$ (note que ainda assim φ restrita a S é a identidade)

Seja $\overline{G} = \frac{G}{S}$, $\overline{\varphi} : \overline{G} \longrightarrow \overline{G}$ a função natural induzida por φ. Como $\overline{G}$ não tem elementos de ordem 2, pelo Teorema 3.2, $\overline{\varphi}$ é um automorfismo interno. Assim, $\overline{\varphi} = \varphi_{\overline{g}_0}$, para algum $\overline{g}_0 \in \overline{G}$.

$$(\overline{\varphi})^{2^n} = (\varphi_{\overline{g}_0})^{2^n} = \varphi_{\overline{g}_0^{2^n}} = id \Rightarrow \overline{g}_0^{2^n} \in \mathcal{Z}(\overline{G})$$

Note que, $2 \nmid o(\overline{g}_0)$, pois $\overline{G}$ não tem 2-torsão. Logo,

$$\langle \overline{g}_0 \rangle = \langle \overline{g}_0^{2^n} \rangle \subseteq \mathcal{Z}(\overline{G})$$

Portanto,$g_0 \in \mathcal{Z}(\overline{G})$. Assim, $\overline{\varphi} = 1$, segue que $\rho(g) \in S$, para todo $g \in G$. Assim, por (3.3) $\rho(g) \in \mathcal{Z}(S)$, para todo $g \in G$. Mas

$$\rho(g) = \varphi(g)g^{-1} = v^{-1}gvg^{-1} = [v, g^{-1}] \in N$$

Assim, obtemos uma derivação

$$\rho : G \longrightarrow A = \mathcal{Z}(S) \cap N$$

com A um grupo abeliano finito e $\rho|_S = 1$. De fato,

$$\begin{aligned} \rho(gh) &= [v, gh] \\ &= [v, h][v, g]^h \\ &= \rho(h)\rho(g)^h \\ &= \rho(g)^h\rho(h) \end{aligned}$$

e para todo $g \in S$, temos

$$\rho(g) = \varphi(g)g^{-1} = gg^{-1} = 1.$$

Seja $M = \mathcal{C}_G(N)$. Então M é um subgrupo normal de G e $[G : M] < \infty$. De fato, como N é finito, $N \subset \Delta(G)$, assim, temos $[G : \mathcal{C}_G(n)], \forall n \in N$. Logo, pelo 1.4, $M = \bigcap_{n \in N} \mathcal{C}_G(n)$ tem índice finito em G. Para todo $g \in M$, temos que

$$\rho(g) = [v, g^{-1}] = 1$$

pois, g comuta com todo elemento de $\mathbb{Z}N$.

Assim, $\varphi|_{\langle S,M\rangle}$ é a identidade. Pondo, $H = \frac{G}{\langle S,M\rangle}$ temos que H é um $2'$-grupo finito e obtemos uma derivação induzida natural

$$\overline{\rho} : H \longrightarrow A$$

dada por $\overline{\rho}(h) = \rho(h)$. Como $|H|$ e $|A|$ são relativamente primos, segue-se, pelo Corolário 1.4, que $H^1(H, A) = 0$, ou seja, $\overline{\rho}$ é interno, assim ρ é interno e, portanto, φ é interno. ■

Proposição 3.2 *Seja G um grupo nilpotente finitamente gerado com subgrupo normal finito N. Se $u \in \mathbb{Z}G$ é uma unidade normalizando G e* $\mathrm{supp}(u) \subseteq N$, *então existe $g_0 \in N$ tal que ug_0^{-1} é central em $\mathbb{Z}G$.*

Prova. Sejam $N := T(G)$, $u \in \mathcal{N}_{\mathcal{U}_1}(G)$, $u \in \mathbb{Z}T(G)$. Como G é um grupo policíclico por finito, temos pelo Teorema 1.8 existe um subgrupo normal H de G livre de torção e de índice finito em G. Definindo $\overline{G} := \frac{G}{H}$ temos $\left|\overline{G}\right| = [G : H] < \infty$. Considere a projeção canônica

$$\begin{aligned} \pi \quad : \quad & \mathbb{Z}G \longrightarrow \mathbb{Z}\overline{G} \\ & u \longrightarrow \overline{u}. \end{aligned}$$

Como $\overline{G}$ é um grupo nilpotente finito, segue que $\overline{G}$ é o produto direto de seus subgrupos de Sylow

$$\overline{G} = P_1 \times P_2 \times ... \times P_m.$$

Pela Proposição 2.6 temos que para todo i obtemos $y_i \in \mathrm{supp}(u)$ tal que $\varphi_u|P_i = \varphi_{y_i}|P_i$. Assim, podemos pegar $y_i \in P_i \cap \mathrm{supp}(u)$.

Assim,

$$\begin{aligned} y_i &= t_i r_i \in P_i, \qquad r_i \in P_1 \times ...P_{i-1} \times P_{i+1}... \times P_m, t_i \in P_i \\ \varphi_u(g) &= y_i^{-1} g y_i = t_i^{-1} g t_i, \ \text{ pois } \ (r_i, g) = 1, \forall g \in P_i \end{aligned}$$

Seja $y := t_1...t_m \in \langle \mathrm{supp}(u)\rangle$. Para todo $g \in G$, $g = \prod g_i$, $g_i \in P_i$, assim,

$$\varphi_y(g) = g^y = \prod g_i^{y_i} = \prod g_i^u = \prod \varphi_u(g_i) = \varphi_u(g),$$

logo, $\varphi_u = \varphi_y$. Portanto, existe $\overline{g}_0 \in \langle \mathrm{supp}(u)\rangle \subseteq \overline{T(G)}$, com $g_0 \in N$ tal que $\overline{ug_0^{-1}} = \overline{u}\,\overline{g_0^{-1}} \in \mathcal{Z}(\mathbb{Z}\overline{G})$. De fato, $\overline{v} = \overline{u}\,\overline{g_0^{-1}} \in \mathbb{Z}\overline{T(G)}$, logo $\overline{u} = \overline{v}\overline{g}_0$.

Afirmação: $v \in \mathcal{Z}(\mathbb{Z}G)$.

De fato, observe que $\overline{v} \in \mathcal{Z}(\mathbb{Z}\overline{G})$. Seja $g \in G$, assim, $(v,g) \in (\mathcal{N}_{\mathcal{U}_1}(G))' \subset G$ e

$$\overline{(v,g)} = (\overline{v}, \overline{g}) = \overline{1},$$

pois $\overline{v}$ é central em $\mathbb{Z}\overline{G}$. Portanto,

$$(v,g) \in G \cap (1 + \Delta(G, \ker \pi)) = H$$

e, por outro lado, $(v,g) \in \mathbb{Z}T(G)$. Assim,

$$(v,g) \in T(G) \cap H = T(H) = 1,$$

logo $(v,g) = 1$, para todo $g \in G$. Portanto v é central em $\mathbb{Z}G$. ■

Teorema 3.4 *Seja G um grupo localmente nilpotente . Então (NP) vale para G.*

Prova. Seja $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Usando o Teorema da Representação, escreva $u = gw$ com $g \in G$ e $w \in \mathbb{Z}N$, $\text{supp}(w) \subseteq N$, onde $N \lhd G$ é finito.

Seja $H_0 = \mathcal{C}_G(N)$. Então como $|N| < \infty$ e $N \subset \Delta(G)$ segue que

$$[G : H_0] < \infty.$$

Logo $H = \bigcap_{g \in G} H_0^g$ é um subgrupo normal de G e de índice finito em G. Escolha um transversal $g_1, ..., g_n$ de H em G e seja $G_0 = \langle N, g_1, ..., g_n \rangle$., Note que, $\text{supp}(w) \subseteq N$, portanto, $[x,h] = 1$ para todo $x \in \text{supp}(w)$ e para todo $h \in H$, assim, $[w,h] = 1$, $\forall h \in H$. Como G é localmente nilpotente , temos que, G_0 é um grupo nilpotente finitamente gerado e $w \in \mathbb{Z}N \subseteq \mathcal{Z}T(G_0)$, pois $N \subset T(G_0)$ e $|T(G_0)|$ é finito. Assim, pela Proposição 3.2, existe $n_0 \in N$ tal que $v := n_0^{-1}w \in \mathcal{Z}(\mathbb{Z}G_0)$. Em particular para todo $i = 1, ..., n$ temos $(v, g_i) = 1$, mas $v = n_0^{-1}w \in \mathbb{Z}N$, então

$$(v,h) = (n_0^{-1}w, h) = (n_0^{-1}w, h)^w (w,h) = 1,$$

para todo $h \in H$, portanto, $(v,h) = 1$, $\forall h \in H$. Mas

$G = \bigcup_{i=1}^{n} g_i H$ e para todo i, $(v, g_i H) = 1$. Assim, $(v, G) = 1$, logo $v \in \mathcal{Z}(\mathbb{Z}G)$ e $w = n_0 v$. Portanto,

$$\varphi_w \in \text{Inn}(G) \Rightarrow \varphi_u \in \text{Inn}(G).$$

■

Terminamos com 2 resultados que em algum sentido da um argumento de indução provando (NP).

Teorema 3.5 *Seja G um grupo finito e suponha que o subgrupo de Fitting, F, de G tenha ordem ímpar e contém seu centralizador em G. Então qualquer automorfismo ϕ de G que induzir a identidade em F tem ordem ímpar. Em particular, se ϕ é induzido por uma unidade em $\mathcal{N}_{\mathcal{U}_1}(G)$ então ϕ é interno. Seja π o conjunto de divisores primos de $|F|$ e suponha que G é π-separável. Então as conclusões do teorema valem.*

Prova. Seja $g \in G$, $x \in F \trianglelefteq G$. Então

$$g^{-1}xg = \phi(g^{-1}xg) = \phi(g^{-1})x\phi(g)$$

Assim, $\phi(g)g^{-1}$ centraliza F. Por hipótese $\phi(g)g^{-1} \in F$. Logo, para todo $g \in G$, $\psi(g) = \phi(g)g^{-1} \in \mathcal{C}_G(F)$. Como $\mathcal{C}_G(F) \subseteq F$, temos que, $\psi(g) \in \mathcal{Z}(F)$. Escreva $\phi(g) = \psi(g)g$ e seja $n = \exp(F)$. Então

$$\phi^n(g) = \psi(g)^n g = g.$$

Assim, a ordem de ϕ divide n e, portanto, é ímpar. Além disso, se ϕ é induzido por $u \in \mathcal{N}_{\mathcal{U}_1}(G)$, então pela Proposição 2.5, ϕ é interno em G.

Se G é π-separável então, pelo Teorema 1.9 , F contém seu centralizador em G e assim a última parte do teorema segue. ■

Proposição 3.3 *Seja G um grupo. Suponhamos que N seja um subgrupo normal tal que $G' \cap N = \{1\}$. Se $\frac{G}{N}$ satisfaz (NP) então G satisfaz (NP).*

Prova. Seja $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Então pelo Teorema 3.1, existe um subgrupo normal finito N_0 de G tal que $u = wg$ para algum $g \in G$ e $w \in \mathbb{Z}N_0$. Considere o homomorfismo natural

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

Sabemos que $w \in \mathcal{N}_{\mathcal{U}_1}(G)$. Como por hipótese $\frac{G}{N}$ satisfaz o problema do normalizador e por $\beta = \pi(w)$ normaliza $\frac{G}{N}$, obtemos que $\beta = \pi(x)v$ para algum v em $\mathcal{Z}(\mathbb{Z}\left(\frac{G}{N}\right))$ e $x \in G$.

Afirmação: $z = wx^{-1}$ é central em $\mathbb{Z}G$.

De fato, para qualquer $g \in G$,

$$\pi[z,g] = [\pi(z), \pi(g)] = [\pi(w)\pi^{-1}(x), \pi(g)] = [\pi(x)v\pi^{-1}(x), \pi(g)] = [v, \pi(g)] = 1$$

Assim, $[z,g] \in N$. Por outro lado, como $\mathbb{Z}\left(\frac{G}{G'}\right)$ é comutativo e $[z,g] \in G$ temos que $[z,g] \in G'$. Como por hipótese $G' \cap N = \{1\}$, obtemos que $[z,g] = 1$ para qualquer $g \in G$. Portanto

$$u = wg = zxg = hz \in G\mathcal{Z}(\mathcal{U}_1(\mathbb{Z}G))$$

como queríamos. ■

Corolário 3.4 *A condição* (NP) *vale para qualquer grupo* FC G *com* G' *um* p*-grupo.*

Prova. Como G é um grupo FC existe, pelo Lema 1.10, um subgrupo livre de torção N tal que $\frac{G}{N}$ é periódico. Como G' é um p-grupo, G contém um p-subgrupo de Sylow normal P, tal que $G' \subseteq P$. Seja φ o automorfismo induzido por uma unidade $u \in \mathcal{N}_{\mathcal{U}_1}(G)$. Veremos que φ é um automorfismos interno em G. Pelo Teorema 3.1 e as Proposições 2.4 e 2.5, podemos assumir que φ tem ordem uma potência de 2 e $\varphi|_P = 1_P$. Como $\frac{G}{P}$ é abeliano, φ induz a identidade em $\frac{G}{P}$. Portanto, para qualquer $g \in G$, $\varphi(g) = \phi(g)g$ com $\phi(g) \in P$. Como φ é um 2-elemento, cada $\phi(g)$ é também um 2-elemento e, portanto, $p = 2$. Considere a projeção canônica $\pi : G \longrightarrow \frac{G}{N}$, assim $\pi(P) = \frac{PN}{N} \subseteq \frac{G}{N}$, ou seja , $\frac{G}{N}$ contém um 2-subgrupo de Sylow normal. Assim, pelo Teorema 3.3, (NP) vale para $\frac{G}{N}$. Como $T(N) = 1$, temos que $G' \cap N = \{1\}$, logo, pela Proposição 3.3, temos que G satisfaz (NP). ■

Referências Bibliográficas

[1] Bhattacharya, P. B., Jain, S. K. e Nagpaul, S. R., *Basic Abstract Algebra*. Cambridge, New York, 1995.

[2] Dummit, D. S. and Foote, M., *Abstract Algebra*, Prentice-Hall International, Inc.

[3] D. Gorentein, *Finite Groups*, Harper & Row, New York,1968.

[4] Jespers, E., Juriaans, S.O., Miranda, J. M. de, Rogério, J. R., "On the Normalizer Problem," *Journal of Algebra*, 247(2002), 24-36.

[5] Robinson, D. J. S, *A course in the Theory of Groups*, Springer-Verlag, New York/Heidbg, 1980.

[6] Rotman, J. J., *Galois Theory*. Springer, New York, 1998.

[7] Sehgal S. K., César, P. M., *An Introduction to Group Rings,* Kluwer Academic Publishers, London, 2002.

[8] Sehgal S. K., *Units in Integral Group Rings*, Longman, Essex, 1993

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