Universidade Federal da Bahia
Instituto de Matemática
Programa de Pós-Graduação em Matemática
Dissertação de Mestrado

O Problema do Isomorfismo e a Propriedade do Normalizador para Grupos Adjuntos de um Anel

Ricardo Alcântara Mesquita

Salvador-Bahia
Fevereiro de 2009

O Problema do Isomorfismo e a Propriedade do Normalizador para Grupos Adjuntos de um Anel

Ricardo Alcântara Mesquita

Dissertação de Mestrado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Salvador-Bahia

Fevereiro de 2009

Mesquita, Ricardo Alcântara.

O Problema do Isomorfismo e a Propriedade do Normalizador para Grupos Adjuntos de um Anel / Ricardo Alcântara Mesquita. – Salvador, 2009.

47 f.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Dissertação (mestrado) – Universidade Federal da Bahia, Instituto de Matemática, Programa de Pós-graduação em Matemática, 2009.

Referências bibliográficas.

1. Álgebra. 2. Anéis (Álgebra). 3. Anéis de grupo. I. Lobão, Thierry Corrêa Petit. II. Universidade Federal da Bahia, Instituto de Matemática. III. Título.

CDD - 512.2

- 512.4

O Problema do Isomorfismo e a Propriedade do Normalizador para Grupos Adjuntos de um Anel

Ricardo Alcântara Mesquita

Dissertação de Mestrado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática.

Banca examinadora:

Prof. Dr. Thierry Corrêa Petit Lobão (Orientador)
UFBA

Prof. Dr. Francisco César Polcino Milies
USP

Prof. Dr. Carlos Eduardo Nogueira Bahiano
UFBA

Agradecimentos

Agradeço a Deus por mais uma conquista, a todos os professores que participaram da minha formação, em especial ao professor Thierry, que me orientou e esteve ao meu lado durante esta última fase do curso, aos colegas que trilharam este caminho comigo e que contribuíram bastante para este momento, a minha família e a meus amigos por todo incentivo e motivação.

Resumo

Neste trabalho, trataremos de dois problemas relevantes na teoria de anéis de grupo integrais, que são o Problema do Isomorfismo e a Propriedade do Normalizador. Mostraremos alguns resultados que já foram apresentados na literatura, citando algumas classes de grupos que satisfazem tais problemas e que serão fundamentais para o desenvolvimento do nosso trabalho. Verificaremos a validade de tais propriedades para os grupos círculos; e para os grupos adjuntos obteremos resultados particulares. Apresentaremos resultados parciais necessários para que possamos chegar à validade da propriedade do normalizador considerando o grupo adjunto de um anel com unidade e com característica p, p primo, apresentando a estrutura dos grupos adjuntos nestes casos. Sugeriremos ainda uma possibilidade de extensão para alguns destes resultados, mostrando que estes são válidos para grupos k-adjuntos e k-círculos, de forma que a verificação anterior seja obtida como caso particular, fazendo $k = 1$.

Palavras-chave: Anéis de Grupo Integrais; Problema do Isomorfismo; Propriedade do Normalizador; Grupo Adjunto; Grupo Círculo.

Abstract

In this work, we deal with two relevant problems in the theory of integral group rings, namely, the Isomorphism Problem and the Normalizer Property. We shall show some results already presented in the literature, and deal some classes of groups which meet such problems and will be fundamental to the development of our work. We shall check the validity of these properties for circle groups and, for adjoint groups, we get some particular results as well. We shall present partial results in order to obtain the normalizer property considering the adjoint group of a ring with unity and characteristic p, p prime, and we also obtain the internal structure of this group. We also suggest possible extensions for some of these results, and we prove that these properties are also valid for k-adjoint and k-circle groups, in this way, the previous results are particular cases with $k = 1$.

Keywords: Integral Group Rings; Isomorphism Problem; Normalizer Property; Adjoint Groups; Circle Groups.

Sumário

Introdução

Neste trabalho, trataremos de duas questões relevantes na teoria de anéis de grupo, o Problema do Isomorfismo e a Propriedade do Normalizador.

Utilizaremos aqui principalmente anéis de grupo integrais, denotados por $\mathbb{Z}G$, em que os elementos do grupo G, que é finito, formam uma base para estrutura e os coeficientes são tomados no anel dos inteiros, $\mathbb{Z}$.

O Problema do Isomorfismo consiste em verificar se dois grupos serão isomorfos sempre que seus anéis de grupo o forem. A questão passou a ser estudada considerando-se anéis de grupo integrais a partir dos trabalhos de Higman, 1940, quando então se conjecturou:

$$(Iso) \qquad\qquad \mathbb{Z}G \simeq \mathbb{Z}H \Rightarrow G \simeq H$$

Foi intensa a busca por classes de grupos que satisfazem a tal conjectura. No segundo capítulo, apresentamos este problema e alguns dos principais resultados dando maior atenção àqueles que consideramos mais importantes para nosso trabalho.

A outra questão abordada por nós, ainda com respeito a teoria de anéis de grupo, foi a Propriedade do Normalizador e que também foi apresentada como conjectura: o normalizador de G no grupo das unidades de $\mathbb{Z}G$ é igual ao produto de G pelo centro do grupo das unidades. No terceiro capítulo, trataremos desta questão abordando os resultados que serão mais importantes, principalmente os resultados de Jackowski e Marciniak [7], que terão fundamental utilidade para conclusão dos resultados propostos por nós. Ainda neste capítulo, falaremos da existência de uma relação entre as duas propriedades que foi verificada por M. Mazur em 1995, [10], e dos contra-exemplos apresentados recentemente por M. Hertweck [6], para as duas questões.

Até então buscava-se verificar a validade destas conjecturas, mas, depois dos contra-exemplos citados, mudou-se o caminho da pesquisa, pois agora busca-se determinar as classes de grupos para as quais estas serão satisfeitas.

No capítulo seguinte, estudaremos o grupo adjunto G de um anel R, sendo que G é composto por elementos de R que admitem quase-inverso, ou seja, para $x \in R$, existe $y \in R$, tal que $x \circ y = y \circ x = 0$, com respeito a operação associativa $x \circ y = x + y + xy$, cujo neutro é o zero (pag. 18), de modo que $(G, \circ)$ é um grupo. No caso particular em que todos os elementos do anel R são quase-regulares, chamamos o grupo G de círculo. Considerando R um anel nilpotente, verificamos que o seu grupo adjunto será nilpotente, daí usando o resultado de K. W. Roggenkamp e L. L. Scott [12], podemos concluir que tais grupos adjuntos representam solução para o (Iso), e ainda que tais grupos representam resposta positiva para a propriedade do normalizador já que esta sempre é válida se considerarmos um grupo nilpotente finito. Quando o grupo adjunto é todo o anel, ou seja, trata-se de um grupo círculo, sem a necessidade de supor um anel nilpotente, conseguimos verificar que estes grupos satisfazem o (Iso), o que nos dá um outro caminho para verificarmos um dos resultados de Sandling [13] e ainda conseguimos mostrar que vale a propriedade do normalizador. Estas conclusões para grupos adjunto e círculo, no que diz respeito a propriedade do normalizador, são resultados novos da dissertação.

Ainda no quarto capítulo, tentamos mostrar a validade da propriedade do normalizador para um anel R com unidade e característica prima. Não chegamos a concluir o resultado, mas acreditamos ter dado um grande passo quando conseguimos mostrar que, neste caso, podemos escrever o grupo adjunto de R, G, como um produto semidireto entre o radical de Jacobson J, de R, e um subgrupo B de G, que pode ser escrito como produto direto de grupos gerais lineares, ou seja, o subgrupo B é da forma

$$B \simeq GL(n_1, \mathbb{F}_{q_1}) \times \ldots \times GL(n_k, \mathbb{F}_{q_k}),$$

sendo $G = J \rtimes B$. Mostramos ainda que o conjunto dos automorfismos

$$Aut_{\mathcal{U}}(GL(n, \mathbb{F}_q)) = \{\varphi_u : GL(n, \mathbb{F}_q) \to GL(n, \mathbb{F}_q);\ g \mapsto u^{-1}gu, u \in \mathcal{N}_{\mathcal{U}}(G)\}$$

é subgrupo do grupo de automorfismos internos, $Inn(GL(n, \mathbb{F}_q))$, ou seja, o grupo geral linear $GL(n, \mathbb{F}_q)$ representa uma solução para a propriedade de acordo com a técnica desenvolvida por Jackowski e Marciniak [7]; daí, usando o resultado de Li, Parmenter e Sehgal [8], concluímos que o subgrupo B também será solução para a propriedade do normalizador. E estes são também resultados novos da dissertação.

No quinto e último capítulo, sugeriremos possibilidades de generalizações de alguns dos resultados do capítulo anterior, agora usando grupos k-adjuntos e k-círculos definidos a partir da operação $x \circ_k y = x + y + kxy$ com k inteiro, de forma que se fizermos aqui $k = 1$, teremos exatamente o que foi obtido antes.

Capítulo 1

Definições e resultados preliminares

Neste capítulo, citaremos algumas definições e resultados importantes a respeito das Teorias de Grupos, Anéis e Anéis de Grupo que serão utilizados no decorrer do trabalho. Estes resultados poderão ser verificados pelo leitor nas referências de C. P. Milies e S. K. Sehgal [11], S. K. Sehgal [14] ou em qualquer outro livro introdutório de Teoria de Anéis de Grupo.

1.1 Grupos

Definição 1.1. *Seja H um subgrupo de um grupo G, definimos o normalizador de H em G, $\mathcal{N}_H(G)$, por*

$$\mathcal{N}_H(G) = \{g \in G; g^{-1}Hg = H\}.$$

Definição 1.2. *Um grupo H é chamado nilpotente se contém uma série de subgrupos:*

$$\{1\} = H_0 \subset H_1 \subset \ldots \subset H_n = H$$

tal que cada subgrupo H_{i-1} é normal em H e cada quociente H_i/H_{i-1} está contido no centro de H/H_{i-1}, $1 \leq i \leq n$.

O Teorema seguinte dá uma caracterização usual para grupos nilpotentes finitos.

Teorema 1.3. *Seja G um grupo finito. As seguintes condições são equivalentes:*
i) G é nilpotente.
ii) Todo subgrupo de Sylow de G é normal em G.
iii) G é o produto direto de seus subgrupos de Sylow.

Definição 1.4. *Um grupo G é chamado de grupo metabeliano se contém um subgrupo normal A tal que ambos, A e G/A são abelianos.*

Exemplo 1.5. *Seja S_3 o grupo das permutações em um conjunto de três elementos e A_3 o grupo das permutações pares. Temos que $A_3 \trianglelefteq S_3$, sendo que A_3 e S_3/A_3 são abelianos, mas S_3 não é abeliano, ou seja, S_3 é metabeliano.*

1.2 Anéis

Muitas informações obtemos a respeito de um anel analisando o conjunto dos seus elementos que possuem inverso multiplicativo, chamados unidades e definidos como segue:

Definição 1.6. *Seja $\mathcal{A}$ um anel. O conjunto das unidades de $\mathcal{A}$, denotado por $\mathcal{U}(\mathcal{A})$, é dado por*

$$\mathcal{U}(\mathcal{A}) = \{x \in \mathcal{A} : \exists\ y \in \mathcal{A} \text{ e } xy = yx = 1\}.$$

É fácil observar que tal conjunto é um grupo multiplicativo.

Sejam I e J dois subanéis de um anel R, o produto denotado por $I \cdot J$ ou IJ é o conjunto de todas as somas finitas $\sum i_m j_m$, em que $i_m \in I$ e $j_m \in J$. Em particular podemos pensar em $R^2 = R.R = RR$, ou ainda, generalizando, em R^n para algum inteiro positivo n. Podemos então fazer a seguinte definição:

Definição 1.7. *Dizemos que um anel R é nilpotente, se existe um inteiro positivo n tal que $R^n = 0$.*

Exemplo 1.8. *Seja $T_0(n, K)$ o anel das matrizes triangulares superiores de ordem n, com coeficientes no corpo K e entradas iguais a 0 na diagonal principal. Podemos observar que $T_0^{n-1}(n, K) = 0$, ou seja, $T_0(n, K)$ é um anel nilpotente.*

Definição 1.9. *Uma álgebra A sobre um corpo K é separável se em qualquer extensão $L : K$ a álgebra $A \otimes_K L$ é semi-simples (a Jacobson).*

1.3 Anéis de Grupo

Definição 1.10. *Sejam G um grupo e R um anel com unidade. Um anel de grupo, denotado por RG, é o conjunto de todas as combinações lineares formais da forma*

$$\alpha = \sum_{g \in G} a_g g$$

em que $a_g \in R$, $g \in G$ e $a_g = 0$ para quase todos os g, isto é, apenas um número finito de coeficientes são diferentes de 0 em cada uma dessas somas, com as seguintes operações:

i) A soma de dois elementos em RG:

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

ii) O produto de dois elementos em RG:

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh$$

Observe que gh denota a operação no grupo G. Reordenando os termos em ii), podemos escrever o produto $\alpha\beta$ como

$$\alpha\beta = \sum_{u\in G} c_u u \ \text{ em que } \ c_u = \sum_{gh=u} a_g b_h.$$

iii) Produto de elementos de RG por elementos $\lambda \in R$:

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

ou seja, RG tem uma estrutura de módulo sobre R.

Observe que para $1 \in R$, o elemento neutro do anel R e $g \in G$, temos que $1g = g$, de modo que $G \subseteq RG$ e se $\lambda \in R$, e $e \in G$ é o elemento neutro do grupo G temos que $\lambda e = \lambda$ e então $R \subseteq RG$, ou seja, existem cópias de G e R em RG.

Nesta dissertação, trabalharemos com anéis de grupo integrais, ou seja, tomaremos coeficientes no anel dos inteiros, $\mathbb{Z}$, e os grupos considerados serão sempre finitos.

Definição 1.11. *O homomorfismo de anéis $\varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$, dado por*

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

é chamado aplicação aumento de $\mathbb{Z}G$ e seu núcleo, denotado por $\Delta(G)$, é chamado ideal de aumento de $\mathbb{Z}G$.

Note que, se um elemento $\alpha = \sum_{g\in G} a_g g$ pertence a $\Delta(G)$, então $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$; então podemos escrever α na forma

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Como, claramente, todos os elementos da forma $g-1$, $g \in G$, pertencem a $\Delta(G)$, a observação acima mostra que $\{g - 1 : \ g \in G, \ g \neq 1\}$ é um conjunto de geradores de $\Delta(G)$ sobre $\mathbb{Z}$, e daí obtemos a seguinte caracterização para o ideal aumento:

Proposição 1.12. *O conjunto* $\{g-1: \ g \in G, \ g \neq 1\}$ *é uma base de* $\Delta(G)$ *sobre* $\mathbb{Z}$, *e portanto podemos escrever*

$$\Delta(G) = \left\{ \sum_{g \in G} a_g(g-1) \in \mathbb{Z}G : g \in G, g \neq 1, a_g \in \mathbb{Z} \right\}$$

em que, apenas um número finito de coeficientes a_g *é diferente de 0.*

Definição 1.13. *Seja* H *um subgrupo de* G *e seja* S *um conjunto de geradores de* H, *então,* $\Delta(G,H)$ *é o ideal à esquerda de* $\mathbb{Z}G$ *gerado pelo conjunto* $\{s-1 : s \in S\}$.

O resultado a seguir é uma interpretação para $\Delta(G,H)$ quando H é um subgrupo normal de G. Neste caso o homomorfismo canônico $\omega : G \longrightarrow \frac{G}{H}$ pode ser estendido ao epimorfismo $\overline{\omega} : \mathbb{Z}G \longrightarrow \mathbb{Z}(\frac{G}{H})$ dado por

$$\overline{\omega}\left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \omega(g).$$

Proposição 1.14. *Com a notação anterior,* $Ker(\overline{\omega}) = \Delta(G,H)$.

Corolário 1.15. *Seja* H *um subgrupo normal de um grupo* G, *então,* $\Delta(G,H)$ *é um ideal bilateral de* $\mathbb{Z}G$ *e*

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

A demonstração deste resultado segue dos teoremas de isomorfismo de anéis.

Quando estudamos o anel de grupo integral $\mathbb{Z}G$, a aplicação

$$^* : \mathbb{Z}G \to \mathbb{Z}G$$

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

é uma anti-involução, ou seja, satisfaz as seguintes propriedades:

i) $(\alpha + \beta)^* = \alpha^* + \beta^*$,

ii) $(\alpha\beta)^* = \beta^*\alpha^*$,

iii) $\alpha^{**} = \alpha$.

Assim como definimos o grupo multiplicativo das unidades para um anel $\mathcal{A}$, dados um grupo G e o anel $\mathbb{Z}$, $\mathcal{U}(\mathbb{Z}G)$ denota o grupo das unidades do anel de grupo $\mathbb{Z}G$. Como a aplicação aumento $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$, é um homomorfismo de anéis com unidade e $\varepsilon(1) = 1$, segue que $\varepsilon(u) \in \mathcal{U}(\mathbb{Z}) = \{-1, 1\}$, para todo $u \in \mathcal{U}(\mathbb{Z}G)$.

Denotamos por $\mathcal{U}_1(\mathbb{Z}G)$ o subgrupo das unidades de aumento 1 em $\mathcal{U}(\mathbb{Z}G)$, isto é, $\mathcal{U}_1(\mathbb{Z}G) = \{u \in \mathcal{U}(\mathbb{Z}G) : \varepsilon(u) = 1\}$, chamado também de subgrupo das unidades normalizadas.

Para uma unidade u do anel de grupo integral $\mathbb{Z}G$ temos que $\varepsilon(u) = \pm 1$, então vemos que $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G)$.

Uma unidade trivial de $\mathbb{Z}G$ é um elemento da forma $\pm g, g \in G$.

A seguinte proposição é um resultado acerca da aplicação definida acima e que será utilizada na demonstração de alguns resultados apresentados adiante.

Proposição 1.16. *Seja $u \in \mathcal{U}(\mathbb{Z}G)$ tal que $u^*u = 1$, então, $u = \pm g,\ g \in G$.*

Definição 1.17. *Um isomorfismo $\psi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ é chamado de Isomorfismo Normalizado se, para todo elemento $\alpha \in \mathbb{Z}G$, temos que $\varepsilon(\alpha) = \varepsilon(\psi(\alpha))$ ou, equivalentemente, se, para todo elemento $g \in G$, temos $\varepsilon(\psi(g)) = 1$.*

Observamos que, se existe um isomorfismo $\psi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$, então existe também um isomorfismo normalizado entre estes anéis de grupo. De fato, é suficiente considerar uma nova aplicação $\xi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ dada da seguite forma: para cada elemento $\alpha = \sum_{i=1}^{n} r_i g_i \in \mathbb{Z}G$ definimos $\xi(\alpha) = \sum_{i=1}^{n} \varepsilon(\psi(g_i))^{-1} r_i \psi(g_i)$. (Note que, como $g \in G$ é inversível e ε é um epimorfismo, temos $\varepsilon(\psi(g))$ inversível em $\mathbb{Z}$). Podemos ver que ξ é, de fato, um isomorfismo normalizado.

Seja $\mathcal{C}_g$ a classe de conjugação de g em G, para algum $g \in G$. Seja $\hat{\mathcal{C}}_g = \sum_{x \in \mathcal{C}_g} x = \sum_{x \sim g} x$, denominado a soma de classe da classe $\mathcal{C}_g$, então $y^{-1}\hat{\mathcal{C}}_g y = \hat{\mathcal{C}}_g$ para todo $y \in G$, o que é precisamente dizer que $\hat{\mathcal{C}}_g$ é central em $\mathbb{Z}G$.

Alguns resultados de D. Glauberman e D. Passman nos revelam a existência de uma correspondência bijetora entre as classes de conjugação de G e H que preserva algumas características destas classes, vejamos:

Proposição 1.18. *Se $\psi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ é um isomorfismo e $\hat{\mathcal{C}}_g$ uma soma de classe em G, então $\psi(\hat{\mathcal{C}}_g)$ é uma soma de classes em H, isto é, existe x em H tal que $\psi(\hat{\mathcal{C}}_g) = \hat{\mathcal{C}}_x$; valem ainda:*

i) $\psi(\hat{\mathcal{C}}_g^n) = \hat{\mathcal{C}}_x^n$ para todo inteiro n;

ii) $o(g) = o(x)$ e $|\mathcal{C}_g| = |\mathcal{C}_x|$;

iii) $\psi(\hat{\mathcal{C}}_g) = \hat{\mathcal{C}}_x$ e $\psi(\hat{\mathcal{C}}_h) = \hat{\mathcal{C}}_y$ então existem ν e ω em H tais que $\psi(\hat{\mathcal{C}}_{gh}) = \hat{\mathcal{C}}_{xy^\nu} = \hat{\mathcal{C}}_{x^\omega y}$. (em que $y^\nu = \nu^{-1}y\nu$ e $x^\omega = \omega^{-1}x\omega$).

Observamos que esta correspondência determina uma correspondência entre subgrupos normais de G e H que, entre outras características, preserva a ordem destes subgrupos.

Capítulo 2

O Problema do Isomorfismo

O Problema do Isomorfismo é uma questão muito importante na teoria dos anéis de grupo, uma vez que é um problema de classifição e aparece pela primeira vez em 1940, na tese de doutorado de Higman, em que ele considera anéis de grupo tomando coeficientes no anel $\mathbb{Z}$, ou seja, anéis de grupo integrais.

Em 1947 na Conferência de Álgebra em Michigan, M. Thrall apresentou a seguinte questão:

"Dados um grupo G e um corpo K, determinar todos os grupos H tais que $KG \simeq KH$."

No entanto, as questões sobre quais propriedades de um grupo finito G se refletem sobre o anel de grupo RG já eram estudadas por W. Burnside, G. Frobenius e I. Chur. Com respeito a tais grupos é imediato que se dois grupos são isomorfos, os seus anéis de grupo, determinados a partir de um mesmo anel de coeficientes, também o serão.

A partir de então, muitos resultados a respeito desta questão foram obtidos por diversos matemáticos como: S. Perlis e G. Walker em 1950, W. E. Deskins em 1956 e E. C. Dade em 1972, dentre outros. Após estes resultados a questão passou a ser enunciada da seguite forma:

Se G é um grupo finito, H um outro grupo qualquer e R um anel com unidade tais que $RG \simeq RH$, será então que $G \simeq H$?

Dentre os muitos trabalhos acerca do Problema do Isomorfismo podemos citar alguns resultados: G. Higman em 1940 e S. D. Berman em 1955 mostraram que se G é um grupo abeliano finito e $\mathbb{Z}G \simeq \mathbb{Z}H$, então $G \simeq H$, em 1968, A. Whitcomb mostrou que se G é um grupo metabeliano finito e $\mathbb{Z}G \simeq \mathbb{Z}H$, então $G \simeq H$. Um importante resultado, que vamos utilizar em nosso trabalho, foi demonstrado por, K. Roggenkamp e L. L. Scott, vide [12] e independentemente por A. Weiss [2]; eles mostraram que para os grupos nilpotentes finitos também vale a tese do Problema do Isomorfismo. Além destas, no decorrer do trabalho, apresentaremos outras soluções para o Problema do Isomorfismo obtidas por R. Sandling.

É importante também citar que a existência do isomorfismo $\mathbb{Z}G \simeq \mathbb{Z}H$, mesmo não implicando a princípio numa solução do problema do isomorfismo para grupos finitos, acarreta uma série de semelhanças entre os grupos G e H. Para citar as semelhanças mais interessantes temos, por exemplo, que a ordem é preservada e os centros e os segundos centros dos dois grupos serão isomorfos; características como abelianidade, nilpotência e solubilidade são compartilhadas pelos dois grupos, isto porque a isomorfia dos anéis de grupo integrais determina uma correspondência entre as séries centrais e derivadas dos dois grupos, (também é preservado entre os grupos, o reticulado de subgrupos normais.)

As inúmeras semelhanças entre os dois grupos finitos impostos pelo isomorfismo de seus anéis de grupo integrais sugeriram que o Problema do Isomorfismo para estes anéis de grupo integrais tem resposta positiva para todos os grupos finitos. E esta questão se tornou conhecida como o Problema do Isomorfismo (Iso), ou seja:

$$(Iso) \qquad \mathbb{Z}G \simeq \mathbb{Z}H \Longrightarrow G \simeq H.$$

O seguinte resultado apresenta mais uma razão para nos concentrarmos na questão usando $\mathbb{Z}$ como o anel de coeficientes.

Proposição 2.1. *Sejam G e H dois grupos. Se $\mathbb{Z}G \simeq \mathbb{Z}H$, então $RG \simeq RH$ para qualquer anel comutativo R (como R-álgebra).*

Pela proposição 1.15, demonstra-se a existência de uma correspondência entre os subgrupos normais de G e H, que de fato é um isomorfismo entre estes reticulados, sempre que $\mathbb{Z}G \simeq \mathbb{Z}H$. Além disso, grupos normais correspondentes apresentam uma série de semelhanças. Tais afirmações podem ser verificadas nos livros de Polcino Milies e Sehgal [11] e Sehgal [14].

Na proposição seguinte usaremos que $\hat{N} = \sum_{x \in N} x$ para um subgrupo (ou subconjunto) N de G e denotaremos por N' o subgrupo derivado de N. Este resultado pode ser consultado mais detalhadamente em Polcino Milies e Sehgal [11].

Proposição 2.2. *Sejam G e H grupos finitos tais que $\mathbb{Z}G \simeq \mathbb{Z}H$. Seja N um subgrupo normal de G e seja M o subgrupo de H correspondente, então*

i) $\mathbb{Z}(\frac{G}{N}) \simeq \mathbb{Z}(\frac{H}{M})$;

ii) $\frac{N}{N'} \simeq \frac{M}{M'}$;

iii) Se N é abeliano, então M também é abeliano;

iv) $\psi(\hat{N}) = \hat{M}$;

v) $|N| = |M|$;

vi) $\psi(\Delta(G, N)) = \Delta(H, M)$.

O próximo teorema foi um resultado apresentado por Roggenkamp e Scott, em um artigo de 1987, vide [12]. Este resultado será fundamental para obtenção dos resultados propostos em nosso trabalho.

Teorema 2.3. *Seja G grupo nilpotente finito. Então*

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

Veremos no próximo capítulo alguns resultados de Hertweck, [6], dentre os quais ele apresenta um contra-exemplo para o (Iso), ou seja, ele constrói dois grupos finitos, bem particulares e não isomorfos de forma que seus anéis de grupo integrais sejam isomorfos. Essa descoberta não diminui a importância do (Iso), mas muda-se a linha de pesquisa, pois agora já não buscamos mais mostrar a validade de tal propriedade e sim quais as características que um grupo deve possuir para que seja determinado pelo seu anel de grupo.

Na próxima seção, apresentaremos algumas definições e mostraremos alguns resultados publicados num artigo em 1974, por R. Sandling, vide [13].

2.1 Os resultados de Sandling

Os resultados do artigo de Sandling aos quais daremos mais atenção são as verificações de que os grupos adjunto e círculo de um anel finito são determinados pelos seus anéis de grupo integrais, ou seja, satisfazem ao problema do isomorfismo.

Para chegarmos a tais afirmações, começamos com a definição da operação círculo, que nos permite construir tais classes de grupos. Observamos que esta seção é fundamentada em Polcino Milies e Sehgal, [11].

Definição 2.4. *Seja R um anel, não necessariamente com unidade. Definimos uma nova operação em R, chamada de operação círculo, por:*

$$x \circ y = x + y + xy, \text{ para todo } x, y \in R.$$

Podemos verificar que esta operação é associativa: De fato,

$$x \circ (y \circ z) = x \circ (y + z + yz) = x + y + z + yz + x(y + z + yz) =$$

$$= x + y + z + yz + xy + xz + xyz = x + y + xy + z + (x + y + xy)z =$$

$$= (x + y + xy) \circ z = (x \circ y) \circ z.$$

Observe que,

$$x \circ 0 = x + 0 + x0 = x = 0 + x + 0x = 0 \circ x,$$

ou seja, o elemento $0 \in R$ é o elemento neutro para esta nova operação.

Definição 2.5. *Seja R um anel. Um elemento $x \in R$ é chamado quase-regular à esquerda se existe um elemento $y \in R$ tal que $y \circ x = 0$; esse elemento é chamado um quase-inverso à esquerda de x. Similarmente, x é dito ser quase-regular à direita se existe $y \in R$ tal que $x \circ y = 0$.*

Um elemento $x \in R$ é chamado quase-regular se ele é quase-regular à esquerda e à direita.

Observamos que se um elemento x é quase-regular e y, z são seus quase-inversos à direita e à esquerda respectivamente, então $y = z$. De fato, se $x \circ y = 0 = z \circ x$ então, usando a associatividade da operação círculo, temos que,

$$z = z \circ 0 = z \circ (x \circ y) = (z \circ x) \circ y = 0 \circ y = y.$$

Já verificamos que a operação círculo é associativa e que tem como elemento neutro $0 \in R$, destes fatos não é difícil concluir-se que o conjunto de todos os elementos quase-regulares do anel R, considerando a operação $\circ$, formam um grupo.

Definição 2.6. *Seja R um anel. O grupo de todos os elementos quase-regulares de R, com a operação $\circ$, é chamado o grupo adjunto de R.*

Definição 2.7. *Se todos os elementos de um anel R são quase-regulares, ele é chamado um anel radical. O grupo adjunto de um anel radical é chamado grupo círculo.*

Observamos que, neste caso o grupo círculo é o próprio $(R, \circ)$. Alguns autores chamam o grupo adjunto simplesmente de grupo círculo.

Claramente, se 1 é o elemento identidade do anel R, então o elemento -1 não é quase-regular. De fato, $-1 \circ x = -1 + x + (-1)x = -1 \neq 0$. Assim, um anel com unidade não é um anel radical. Observamos também que se um elemento x do anel R é nilpotente, então x é quase-regular. De fato, se n é o menor inteiro positivo tal que $x^n = 0$ o quase-inverso de x é o elemento

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

Exemplo 2.8. *Seja $T(4,K)$ o conjunto das matrizes triangulares superiores com coeficientes no corpo K. Isto é, T é o conjunto das matrizes da forma*

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{bmatrix}.$$

Denotaremos por $T_0(4,K)$ o conjunto das matrizes em $T(4,K)$ que tem entradas iguais a 0 na diagonal principal. Facilmente verificamos que $T_0(4,K)$ é fechado para somas e produtos e ainda que seus elementos são nilpotentes; assim, fazendo uso da observação citada acima, concluímos que $T_0(4,K)$ é um anel radical. Então este conjunto com a operação $\circ$ é um grupo círculo.

Proposição 2.9. *Seja R um anel com unidade e seja $\mathcal{U}(\mathcal{R})$ o grupo das unidades de R. Seja G o grupo adjunto de R. Então $\mathcal{U}(\mathcal{R}) = 1 + G$ e $\mathcal{U}(\mathcal{R}) \simeq G$.*

Demonstração. Vamos tomar $g \in G$ arbitrário e considerar que $h \in G$ é o quase-inverso de g, ou seja, $g \circ h = h \circ g = 0$. Teremos que,

$$(1+g)(1+h) = 1 + g + h + gh = 1 + (g + h + gh) = 1 + (g \circ h) = 1$$

e analogamente verificamos que $(1+h)(1+g) = 1$, mostrando que $1 + g \in \mathcal{U}(\mathcal{R})$. Por outro lado, se $u \in \mathcal{U}(\mathcal{R})$ e considerando que v é o inverso de u $(uv = vu = 1)$ temos que

$$(u-1) \circ (v-1) = (u-1) + (v-1) + (u-1)(v-1) =$$

$$= u - 1 + v - 1 + uv - u - v + 1 = 0$$

e analogamente verificamos que $(v-1) \circ (u-1) = 0$, o que mostra que $u - 1 \in G$, ou seja, $\mathcal{U}(\mathcal{R}) = 1 + G$. Com estas informações concluímos que a aplicação

$$\varphi : G \longrightarrow \mathcal{U}(\mathcal{R})$$

$$g \longmapsto 1 + g$$

é uma bijeção. Para chegarmos ao resultado final temos que mostrar que φ é um homomorfismo de grupos. Tomemos então $g, h \in G$, assim

$$\varphi(g \circ h) = 1 + (g \circ h) = 1 + (g + h + gh) = 1 + g + h + gh =$$

$$= (1+g)(1+h) = \varphi(g)\varphi(h).$$

Concluímos assim que $\mathcal{U}(\mathcal{R}) \simeq G$. $\square$

Observamos que este resultado, para matrizes de ordem 4, pode ser generalizado para matrizes triangulares superiores de ordem n.

Dentre os resultados de Sandling [13], estamos interessados em verificar que os grupos adjuntos finitos e os grupos círculos finitos são determinados por seus anéis de grupo integrais, ou seja, se G é um grupo adjunto finito e H é um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$, então $G \simeq H$, e o mesmo ocorre se G for um grupo círculo finito.

Apresentamos adiante alguns teoremas principais e também alguns resultados técnicos que serão de fundamental importância para obtermos os resultados desejados.

Sendo G o grupo adjunto do anel R definimos o seguinte homomorfismo de grupos aditivos

$$\theta : \mathbb{Z}G \longrightarrow R \tag{2.1}$$

$$\sum_{g \in G} a(g)g \longmapsto \sum_{g \in G} a(g)g.$$

Agora, para mostrar que θ restrito ao ideal de aumento $\Delta(G)$ é um homomorfismo de anéis, vamos mostrar que essa restrição é um homomorfismo multiplicativo. De fato, sejam $g, h \in G$ assim,

$$\theta((g-1) \circ (h-1)) = \theta(g \circ h - g - h + 1) = g \circ h - g - h = gh + g + h - g - h = gh,$$

em que 1, representa o elemento identidade de G, que no entanto é o elemento 0 de R, de modo que um elemento da forma $g - 1 \in \mathbb{Z}G$ é levado em $g \in R$, pela aplicação θ. E concluímos que θ restrito $\Delta(G)$ é um homomorfismo de anéis e $\theta(\Delta(G))$ é um subanel de R.

Teorema 2.10. *Um grupo G é o grupo adjunto de um anel se, e somente se, ele é o grupo adjunto de um anel quociente de $\Delta(G)$.*

Demonstração. Para mostrarmos a condição necessária do teorema, vamos assumir que G é o grupo adjunto de um certo anel R. Considerando $\theta : \Delta(G) \longrightarrow R$, o homomorfismo de anéis construído acima temos, pelo teorema do isomorfismo, que

$$\frac{\Delta(G)}{Ker(\theta)} \simeq \theta(\Delta(G)).$$

Daí, como $\theta(\Delta(G))$ é um subanel de R contendo G, temos que G é o grupo adjunto de $\theta(\Delta(G))$ e pelo isomorfismo acima temos que G é também o grupo adjunto de $\frac{\Delta(G)}{Ker(\theta)}$. A condição suficiente do teorema segue imediatamente. □

Teorema 2.11. *Seja G um grupo finito, então G é um grupo círculo se, e somente se, existe um ideal J de $\mathbb{Z}G$, contido em $\Delta(G)$, tal que:*

i) O índice do subgrupo aditivo de J em $\Delta(G)$ é igual a $|G|$, e,
ii) $(1+J)\cap G=\{1\}$

Neste caso, tem-se que

$$G \simeq 1+\frac{\Delta(G)}{J}.$$

Demonstração. Vamos primeiro considerar G um grupo círculo de um anel R e mostrar que as condições $i)$ e $ii)$ são satisfeitas: Seja $\theta : \Delta(G) \longrightarrow R$ o homomorfismo de anéis visto acima e tomemos $J = Ker(\theta)$. Note que para todo $g \in G$, $g-1 \in \Delta(G)$ e sabemos que $\theta(g-1) = g$, portanto $G \subseteq \theta(\Delta(G))$. Mas G é grupo círculo e então $G = R$, daí $R \subseteq \theta(\Delta(G)) \subseteq R$, ou seja, $\theta(\Delta(G)) = R$. Assim

$$\frac{\Delta(G)}{J} \simeq R = G.$$

Como $\Delta(G)$ e J são ideais, também são grupos com a operação de soma. Isto é, J é subgrupo de $\Delta(G)$ (normal pois são abelianos), logo o índice aditivo de J em $\Delta(G)$ é igual a $|G|$ ($[\Delta(G):J]=|G|$), concluindo $i)$.

Para provar $ii)$, vamos tomar $x \in (1+J)\cap G$. Então $x-1 \in J$ assim $\theta(x-1) = 0$. Como $x \in G$ temos que $\theta(x-1) = x$, portanto segue que $x = 0$ em R, mas este é o elemento identidade do grupo círculo G, ou seja, $x = 1$ em G, concluindo $ii)$.

Para verificar que as condições são também suficientes vamos tomar a seguinte aplicação

$$\begin{aligned} \phi : G &\longrightarrow 1+\frac{\Delta(G)}{J} \\ x &\longmapsto 1+(x-1)+J \end{aligned}$$

e mostrar que esta é um isomorfismo de grupos. De fato, para $g,\ h \in G$ temos

$$\phi(g)\phi(h) = (1+(g-1)+J)(1+(h-1)+J) = 1+(gh-1)+J = \phi(gh)$$

e assim mostramos que ϕ é um homomorfismo.

Note que se $g \in G$ é tal que $\phi(g) = 1+J$ (isto é g pertence ao núcleo de ϕ) temos que $g-1 \in J$ pela definição da ϕ, ou seja, $g \in 1+J$ e então $g \in (1+J)\cap G$, concluindo assim, por $ii)$, que $g = 1$. Com isso mostramos que o núcleo é trivial e portanto ϕ é injetiva. Este resultado, junto com o fato de ϕ estar definida para grupos finitos de mesma ordem garante a sobrejetividade e então ϕ é bijetiva.

Temos então que $|G| = |\Delta(G)/J|$, mas na demontração do teorema anterior, considerando $\theta : \Delta(G) \longrightarrow R$, concluímos que $\Delta(G)/J \simeq \theta(\Delta(G))$ e ainda que G é o grupo adjunto de $\theta(\Delta(G))$, portanto

$$|G| = |\Delta(G)/J| = |\theta(\Delta(G))|,$$

ou seja, G é o grupo círculo de $\theta(\Delta(G))$. $\square$

Lema 2.12. *Sejam G e H grupos finitos e seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Seja J um ideal de $\mathbb{Z}G$ tal que $(1+J)\cap G = \{1\}$. Então temos $(1+\phi(J))\cap H = \{1\}$.*

Demonstração. Note que, pelas hipóteses do lema, $\phi(J)$ é um ideal de $\mathbb{Z}H$.

Suponhamos, por contradição, que $M = (1 + \phi(J)) \cap H$ seja não trivial. Mostraremos inicialmente que M é um subgrupo de H.

De fato, dados $a, b \in M$ temos que $a - 1$ e $b - 1 \in \phi(J)$. Vamos mostrar que $ab \in 1 + \phi(J)$, ou seja, $ab - 1 \in \phi(J)$, mas

$$(a-1)(b-1) = ab - a - b + 1 = (ab-1) - (a-1) - (b-1)$$

e como $\phi(J)$ é um ideal temos que $ab - 1 \in \phi(J)$ e então $ab \in M$.

Por outro lado, observe que $-a^{-1}(a - 1) \in \phi(J)$, ainda pelo fato de $\phi(J)$ ser um ideal, logo $(a^{-1} - 1) \in \phi(J)$, ou seja, $a^{-1} \in 1 + \phi(J)$ e assim $a^{-1} \in M$. Concluindo que M é subgrupo de H.

Agora para mostrar que M é normal em H, tome $a \in M$ e $b \in H$, note que $a \in H$ e $a \in (1 + \phi(J))$, assim $b^{-1}ab \in H$ e ainda $a - 1 \in \phi(J)$ e então, como $\phi(J)$ é ideal $b^{-1}(a - 1)b \in \phi(J)$, ou seja, $b^{-1}ab - 1 \in \phi(J)$ e $b^{-1}ab \in 1 + \phi(J)$. Concluímos então que $b^{-1}ab \in M$ e M é subgrupo normal de H.

Note que $M = \{h \in H; h - 1 \in \phi(J)\}$, ou seja, $\Delta(M) \subset \phi(J)$. Considere N o subgrupo normal de G correspondente a M como na proposição 2.2. Então $|N| = |M|$, ou seja N não é trivial e $\Delta(N) = \phi^{-1}(\Delta(M)) \subseteq J$, logo como $g - 1 \in \Delta(N)$ para todo $g \in N$ temos que $g \in 1 + J$ e daí $N \subset (1 + J) \cap G$, o que nos leva a $(1 + J) \cap G \neq \{1\}$, o que contradiz a hipótese. $\square$

Teorema 2.13. *Um grupo círculo finito é determinado por seu anel de grupo integral.*

Demonstração. Seja G um grupo círculo finito. Pelo teorema 2.11 sabemos que existe um ideal $J \subset \Delta(G)$ tal que $(1 + J) \cap G = \{1\}$ e $G \simeq 1 + \frac{\Delta(G)}{J}$. Seja H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$ e seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Então $\phi(J)$ é um ideal de $\mathbb{Z}H$, contido em $\Delta(H)$ e pelo lema anterior temos que $(1 + \phi(J)) \cap H = \{1\}$.

Já que $\phi(\Delta(G)) = \Delta(H)$, segue que $[\Delta(H) : \phi(J)] = [\Delta(G) : J] = |G| = |H|$ e então, pelo teorema 2.11, temos que H é um grupo círculo isomorfo a $1 + \frac{\Delta(H)}{\phi(J)}$. Consequentemente, temos que

$$G \simeq 1 + \frac{\Delta(G)}{J} \simeq 1 + \frac{\Delta(H)}{\phi(J)} \simeq H.$$

$\square$

Lema 2.14. *Seja J um ideal de um anel de grupo integral $\mathbb{Z}G$ tal que $(1 + J) \cap G = \{1\}$. Então G é isomorfo a um subgrupo do grupo das unidades do anel quociente $\mathbb{Z}G/J$.*

Demonstração. Como no teorema 2.11 consideremos a aplicação

$$\phi : G \longrightarrow 1 + \frac{\Delta(G)}{J}$$
$$x \longmapsto 1 + (x - 1) + J.$$

No teorema citado acima nós verificamos que tal aplicação é um monomorfismo de grupos, ou seja, ϕ é um homomorfismo injetivo e portanto, sendo G finito, é isomorfo a $\phi(G)$, que é um subgrupo do grupo das unidades de $\mathbb{Z}G/J$, donde segue o resultado. □

Teorema 2.15. *O grupo das unidades de um anel finito é determinado por seu anel de grupo integral.*

Demonstração. Seja G o grupo das unidades de um anel finito A. Tomemos o subanel R, de A, gerado por G. Consideremos a aplicação

$$\theta : \mathbb{Z}G \to R$$

$$\theta(\sum_{g \in G} a(g)g) = \sum_{g \in G} a(g)g.$$

Como as multiplicações de G e R são as mesmas, segue que θ é um homomorfismo de anéis e então vale que $\theta(\mathbb{Z}G) = R$. Se denotarmos $J = Ker(\theta)$; temos que $R = \theta(\mathbb{Z}G) \simeq \mathbb{Z}G/J$.

Vamos agora considerar, um outro grupo H tal que $\mathbb{Z}G \simeq \mathbb{Z}H$ e $\phi : \mathbb{Z}G \to \mathbb{Z}H$ seja um isomorfismo normalizado. Então $\mathbb{Z}G/J \simeq \mathbb{Z}H/\phi(J)$. Sabendo que $(1 + J) \cap G = \{1\}$, usando o lema 2.12, concluímos que $(1 + \phi(J)) \cap H = \{1\}$. Segue então do lema anterior que H é um subgrupo do grupo das unidades de $\mathbb{Z}H/\phi(J) \simeq \mathbb{Z}G/J \simeq R$. Já que o grupo das unidades de R é o próprio G, segue que H é isomorfo a um subgrupo de G e uma vez que estes grupos tem a mesma ordem e são finitos, concluímos que $H \simeq G$. □

Faremos aqui uma observação que será utilizada na demonstração do teorema 2.16. Note que, se estamos trabalhando com um anel sem unidade R, podemos definir o conjunto $R_1 = \mathbb{Z} \times R$, formado por todos os pares do tipo (a, x), com $a \in \mathbb{Z}$ e $x \in R$ e considerar as seguintes operações em R_1

$$(a, x) + (b, y) = (a + b, x + y) \ \text{ e } \ (a, x).(b, y) = (ab, ay + bx + xy)$$

para todo $a, b \in \mathbb{Z}$ e todo $x, y \in R$. Podemos mostrar que R_1 é um anel e que a aplicação $\varphi : R \hookrightarrow \mathbb{Z} \times R = R_1$ que leva $x \in R$ em $(0, x) \in R_1$ é um mergulho de R em R_1. Desta forma a partir de um anel sem unidade R, construímos um anel R_1, que possui como elemento unidade o par $(1, 0)$.

Facilmente podemos verificar que o grupo das unidades deste novo anel R_1 é isomorfo ao produto de um grupo isomorfo a G, o adjunto de R, por um grupo cíclico de ordem 2, ou seja, $\mathcal{U}(R_1) \simeq C_2 \times G$, em que G é o grupo adjunto do nosso anel de partida R. De fato, se

$$(a, r)(b, s) = (1, 0), \text{ teremos } (ab, as + br + rs) = (1, 0)$$

o que implica que $ab = 1$ e portanto $a = b = \pm 1$. Teremos assim que $s + r + rs = 0$ ou $-s - r + (-r)(-s) = 0$, ou seja, $r \in G$.

Usaremos este fato para estender o nosso resultado para o grupo adjunto de um anel finito, quando considerarmos um anel sem unidade. Segue então o teorema.

Teorema 2.16. *O grupo adjunto de um anel finito é determinado por seu anel de grupo integral.*

Demonstração. Seja G o grupo adjunto de um anel finito R. Se considerarmos em primeiro lugar que R é uma anel com unidade, concluímos pela proposição 2.8, que G é isomorfo ao grupo das unidades de R e então pelo teorema anterior obtemos que G é determinado pelo seu anel de grupo integral.

Para verificar a validade do teorema para um anel R sem unidade usaremos a observação feita acima e podemos mergulhar o nosso anel R em um anel com unidade R_1, de modo que $G_1 \simeq \mathcal{U}(R_1) = C_2 \times G$, em que C_2 é um grupo cíclico de ordem 2.

Seja H outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então

$$\mathbb{Z}G_1 \simeq \mathbb{Z}[C_2 \times G] \simeq \mathbb{Z}C_2 \otimes_{\mathbb{Z}} \mathbb{Z}G \simeq \mathbb{Z}C_2 \otimes_{\mathbb{Z}} \mathbb{Z}H \simeq \mathbb{Z}[C_2 \times H].$$

Como G_1 é o grupo das unidades de R_1, pelo teorema 2.15, concluímos que $G_1 \simeq C_2 \times H$. Sendo estes grupos finitos, temos que

$$G \simeq G_1/C_2 \simeq H.$$

$\square$

Capítulo 3

A Propriedade do Normalizador

Neste capítulo, apresentaremos uma outra questão de grande importância na teoria de anéis de grupo, que é a Propriedade do Normalizador.

A propriedade em pauta tem sido tema de estudo nesta área e muitas descobertas têm sido obtidas a respeito desta. Neste capítulo, falaremos a respeito do seu surgimento e daremos destaque a alguns resultados que consideramos fundamentais para o desenvolvimento dos nossos objetivos.

Considerando um anel de grupo $\mathbb{Z}G$, sabemos que o grupo G é subgrupo do grupo das unidades de $\mathbb{Z}G$, o que nos leva implicitamente a pensar quem seria o normalizador, $\mathcal{N}_{\mathcal{U}}(G)$, de G em $\mathcal{U}(\mathbb{Z}G)$.

A propriedade do normalizador surge então como uma resposta para esta questão. Na referência [14], S. K. Seghal apresenta tal propriedade da seguinte forma:

Sejam G um grupo finito, $\mathbb{Z}G$ o seu anel de grupo integral, $\mathcal{U} = \mathcal{U}(\mathbb{Z}G)$ o grupo das unidades de $\mathbb{Z}G$ e $\mathcal{N}_{\mathcal{U}}(G)$ o normalizador de G em $\mathcal{U}$. Sendo G um subgrupo de $\mathcal{U}$ vale

$$(Nor) \qquad \mathcal{N}_{\mathcal{U}}(G) = G.\zeta \ ?$$

Em que ζ é o centro de $\mathcal{U}$.

Esta questão foi inicialmente apresentada como uma conjectura devido a alguns resultados que até então tinham sido obtidos, como por exemplo os resultados de Coleman que apresentaremos mais adiante. A partir daí foram várias as tentativas de se verificar a validade de tal conjectura, mas assim como aconteceu com o (Iso), Hertweck apresentou em [6], contra-exemplo para o (Nor). No fim deste capítulo, voltaremos a falar a respeito dos contra-exemplos citados.

Essa mesma questão foi também proposta por S. Jackowski e Z. Marciniak [7], de forma distinta porém equivalente. Vejamos:

Dado um elemento u de $\mathcal{N}_{\mathcal{U}}(G)$, temos a aplicação φ_u em G definida por $\varphi_u(g) = u^{-1}gu$ para todo $g \in G$.

Se denotarmos por $Aut_{\mathcal{U}}(G)$ o conjunto dos automorfismos definidos deste modo, é imediato que $Aut_{\mathcal{U}}(G)$ é um grupo que contém como subgrupo o grupo dos automorfismos internos de G, $Inn(G)$. Temos a propriedade do normalizador verdadeira se, e somente se, para todo u em $\mathcal{N}_{\mathcal{U}}(G)$, $u = g_o c_o$, com g_o em G e c_o em ζ; sendo assim, segue que $\varphi_u(g) = u^{-1}gu = g_o^{-1}gg_o$, pois c_o é central; o que equivale a afirmar que φ_u é um automorfismo interno de G. E então, os autores citados acima apresentam a questão do normalizador da seguinte forma:

Se G é um grupo finito, vale $Aut_{\mathcal{U}}(G) = Inn(G)$?

A partir daí, muitos estudiosos procuraram verificar a validade desta questão para diversas classes de grupos. Aqui vamos apresentar os resutados obtidos desde o início das pesquisas no que diz respeito a este assunto, dando sempre prioridade àqueles que consideramos mais importantes e que terão participação fundamental no decorrer do nosso trabalho.

3.1 Os resultados de Coleman

A primeira resposta afirmativa à questão do normalizador foi apresentada num artigo em 1964, por D. B. Coleman, em que ele prova o seguinte resultado:

Teorema 3.1. *(Coleman, 1964). Seja G um p-grupo finito e K um corpo de característica p, então vale $\mathcal{N}_{\mathcal{U}}(G) = G.\zeta$ na álgebra de grupo KG.*

Adaptando a demonstração de Coleman, os autores Jackowski e Marciniak obtiveram uma extensão do resultado anterior para anéis de grupo integrais, o que representa um grande desenvolvimento para pesquisa pois, revela que a propriedade é verdadeira, em uma versão local, para todos os p-subgrupos de um grupo finito. Este resultado foi desenvolvido em Sehgal [14], como segue:

Teorema 3.2. *Sejam P um p-subgrupo do grupo finito G e $u \in \mathcal{N}_{\mathcal{U}}(G)$, existe então y em G tal que $\varphi_u(g) = y^{-1}gy$, para todo g em P.*

Demonstração. Para todo elemento $g \in G$, $\varphi_u(g) = u^{-1}gu$ é um elemeneto de G pois u está em $\mathcal{N}_{\mathcal{U}}(G)$. Temos ainda que

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

Escrevendo $u = \sum_{x \in G} u(x)x$, temos $\sum_{x \in G} u(x)x = \sum_{x \in G} g^{-1}x\varphi_u(g)$.

Define-se então uma ação σ do subgrupo P sobre o conjunto G do seguinte modo: se $g \in P$ e $x \in G$, tem-se

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

então a função $u : G \to \mathbb{Z}$ dada por $x \mapsto u(x)$ é constante nas órbitas da ação σ; uma vez que o comprimento destas órbitas é um divisor da ordem do p-subgrupo P, segue que este comprimento é uma potência de p. Sendo u uma unidade em $\mathbb{Z}G$, seu aumento, ε, obedece a:

$$\pm 1 = \varepsilon(u) = \sum_i c_i p^{t_i},$$

em que $c_i = u(x_i)$ e p^{t_i} é o comprimento da órbita de x_i, sendo x_i um elemento em G. Segue então que existe uma órbita de comprimento um, pois do contrário o número primo p seria um divisor de ± 1 e isto é o mesmo que dizer que existe um elemento $x_o \in G$ tal que $\sigma_g(x_o) = x_o$, para todo g em P.

Isto implica que

$$\sigma_g(x_o) = x_o = g^{-1}x_o\varphi_u(g) = x_o,$$

para todo g em P, ou ainda

$$\varphi_u(g) = x_o^{-1}gx_o,$$

para todo g em P. □

Vale notar que o resultado, de fato, afirma que $\mathcal{N}_{\mathcal{U}}(G) \leq G.\zeta$, uma vez que $u^{-1}gu = x_o^{-1}gx_o$, com $x_o \in G$. Lembrando agora que o centralizador de G em $\mathcal{U}$ é precisamente o centro de $\mathcal{U}$, segue a nossa afirmação de que o mesmo aponta para uma solução local da propriedade para os p-subgrupos de G.

Aplicando o teorema anterior, é possível obter a validade da propriedade para a importante classe dos grupos nilpotentes finitos, como segue:

Corolário 3.3. *Seja G um grupo nilpotente finito, então $\mathcal{N}_{\mathcal{U}}(G) = G.\zeta$.*

Demonstração. Sendo G um grupo nilpotente finito, podemos escrevê-lo como um produto de seus p-subgrupos de Sylow. Aplicando então o teorema anterior a cada um destes subgrupos de Sylow, P_i. Segue que $u^{-1}gu = x^{-1}gx$, para todo $g \in G$ com $x = \prod x_i$, $x_i \in P_i$ e $u \in \mathcal{N}_{\mathcal{U}}(G)$. □

3.2 Os resultados de Jackowski e Marciniak

Nesta seção, daremos atenção a alguns resultados publicados num artigo de 1987, de Jackowski e Marciniak [7], em que os autores apresentam interesse em encontrar uma solução geral para a propriedade do normalizador para grupos finitos.

Os resultados obtidos no artigo citado acima serão fundamentais para a obtenção dos resultados propostos em nosso trabalho, por isso, faremos uma análise detalhada dos que consideramos mais relevantes. As demontrações destes resultados podem ser verificadas em Sehgal [14].

Seja u uma unidade do normalizador de G em $\mathcal{U}$ e seja $\varphi_u : G \to G$ o automorfismo dado por $\varphi_u(g) = u^{-1}gu$.

Lema 3.4. *A ordem de φ_u é divisível apenas pelos primos que dividem a ordem de G.*

Demonstração. Suponhamos por absurdo que a ordem de φ_u seja divisível por um primo p tal que $p \nmid |G|$. Tomando, se necessário uma potência de φ_u, podemos assumir que $\varphi_u^p = id$. Consideremos o subgrupo dos elementos de G fixados por φ_u, $H = \{g \in G; \varphi_u(g) = g\}$.

Seja $\mathcal{C}$ uma classe de conjugação em G, como as somas de classes são elementos centrais dos anéis de grupo, temos $u^{-1}(\sum\limits_{g\in\mathcal{C}} g)u = \sum\limits_{g\in\mathcal{C}} g$. Portanto, φ_u age em $\mathcal{C}$. Como a ordem de $\mathcal{C}$ divide a ordem de G que é relativamente prima à ordem de φ_u, segue que existe em $\mathcal{C}$ um ponto fixado por φ_u, isto diz que $H \cap \mathcal{C}$ é não vazia, então, $G = \bigcup\limits_y y^{-1}Hy$, o que é uma contradição pois H tem $[G : \mathcal{N}_G(H)]$ conjugados e como $H \subseteq \mathcal{N}_G(H)$, $[G : \mathcal{N}_G(H)] \leq [G : H]$ e assim $G = \bigcup\limits_y y^{-1}Hy$, possui no máximo $1 + (|H| - 1)[G : H]$ elementos. Isto induz $G = H$, ou seja, $\varphi_u = id$. □

No próximo lema, * denota a involução em $\mathbb{Z}G$, mencionada no primeiro capítulo e que opera como $^*(\sum\limits_g a_g g) = \sum\limits_g a_g g^{-1}$.

Lema 3.5. *Se u é uma unidade de $\mathbb{Z}G$, então u pertencerá ao normalizador $\mathcal{N}_{\mathcal{U}}(G)$ se e somente se, u^*u for central em $\mathbb{Z}G$.*

Demonstração. Seja $u \in \mathcal{N}_{\mathcal{U}}(G)$, para $g \in G$ temos $\varphi_u(g) = u^{-1}gu$, aplicando * em ambos os membros da igualdade, obtemos $[\varphi_u(g)]^* = u^*g^{-1}(u^{-1})^*$ e substituindo g por g^{-1} obtemos $\varphi_u(g) = (u^*)g(u^*)^{-1}$ ou $g = (u^*)^{-1}\varphi_u(g)u^*$; consequentemente

$$(uu^*)^{-1}g(uu^*) = (u^*)^{-1}u^{-1}guu^* = (u^*)^{-1}\varphi_u(g)u^* = g,$$

ou seja, uu^* é central. Mas,

$$u^*u = u^{-1}uu^*u = uu^*.$$

Reciprocamente, suponha uu^* central. Para todo $g \in G$ devemos verificar que $u^{-1}gu \in G$. Como $u^*u = uu^*$, obtemos, para todo $g \in G$,

$$(u^{-1}gu)(u^{-1}gu)^* = u^{-1}guu^*g^{-1}(u^{-1})^* = u^{-1}uu^*(u^{-1})^* = u^*(u^*)^{-1} = 1;$$

Usando a proposição 1.13 das preliminares, temos que $u^{-1}gu = \pm g_o$, e então aplicando ε em ambos os membros da igualdade acima, obtemos

$$1 = \varepsilon(u^{-1})\varepsilon(g)\varepsilon(u) = \varepsilon(g) = \varepsilon(\pm g_o)$$

e segue que $u^{-1}gu$ está em G; isto é, u pertence a $\mathcal{N}_{\mathcal{U}}(G)$. □

O lema anterior nos permite verificar a seguinte proposição. Ver Sehgal [14, Proposição 9.5]

Proposição 3.6. *(Krempa). Se u pertence a $\mathcal{N}_{\mathcal{U}}(G)$, então u^2 estará em $G.\zeta$.*

Demonstração. Consideremos a unidade $v = u^*u^{-1}$. Temos pelo último lema,

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

Usando a proposição 1.13, temos que v é uma unidade trivial; e como $\varepsilon(v) = 1$, concluímos que $v = g_o$ para g_o em G. Consequentemente,

$$u^* = g_o u \qquad \text{e} \qquad g_o u^2 = u^*u \in \zeta.$$

Portanto, u^2 pertence a $G.\zeta$, pois u^*u é central. □

Sehgal [14, Teorema 9.6] também lembra que:

Teorema 3.7. *Se G é grupo de ordem ímpar, vale a propriedade do normalizador para G.*

Demonstração. Se u está em $\mathcal{N}_{\mathcal{U}}(G)$, pela proposição anterior, φ_u^2 é um automorfismo interno de G. Sendo a ordem de G ímpar, a ordem, t, de φ_u também o será pelo lema 3.4. Deste modo, t e 2 serão primos relativos; então existem r e s, números inteiros, tais que $2.r + t.s = 1$, e portanto

$$\varphi_u = \varphi_u^{2r+ts} = \varphi_u^{2r}.\varphi_u^{ts} = \varphi_u^{2r};$$

já que φ_u^2 é um automorfismo interno, φ_u será também um automorfismo interno de G. Segue então o resultado, pela reformulação equivalente da propriedade. □

O último teorema nos dá a garantia da validade do (Nor) para os grupos finitos de ordem ímpar, assim quando investigamos a validade da propriedade do normalizador basta analisar os grupos finitos de ordem par. Os autores Jackowski e Marciniak obtiveram um resultado para tal classe de grupos, mas para isto, fizeram uma restrição. Antes de citar tal resultado, apresentaremos o teorema que serviu de ferramenta principal para sua demonstração.

Para um 2-subgrupo de Sylow, S, arbitrário porém fixado em G, define-se o subconjunto I_S de $Aut_{\mathcal{U}}(G)$:

$$I_S = \{\varphi_u \in Aut_{\mathcal{U}}(G); \varphi_u^2 = i,\ \varphi_u|_S = i\}.$$

Segue então o teorema que pode ser verificado no artigo de Jackowski e Marciniak [7]:

Teorema 3.8. *Se I_S está contido em $Inn(G)$ - o subgrupo dos automorfismos internos de G - para um 2-subgrupo de Sylow S de G, então vale a propriedade do normalizador para o grupo G.*

Apresentamos agora um grande resultado de Jackowski e Marciniak que será muito utilizado em nosso trabalho.

Teorema 3.9. *(Jackowski e Marciniak, 1987). Se o grupo finito G possui um 2-subgrupo de Sylow normal, então vale a propriedade do normalizador para G.*

Na demonstração deste teorema os autores aplicaram a teoria de cohomologia de grupos, que não foi abordada por nós; portanto, apesar da sua importância para nosso trabalho, não desenvolveremos esta demonstração, que pode ser verificada no artigo de Jackowski e Marciniak [7].

Na próxima seção, apresentamos os contra-exemplos de Hertweck, que foram citados anteriormente.

3.3 O resultado de Mazur e os contra-exemplos de Hertweck

Além do fato do Problema do Isomorfismo e da Propriedade do Normalizador serem duas questões importantes na teoria de anéis de grupo, uma outra característica que favoreceu para que nós estudássemos estas duas questões, foi o fato de existir uma certa relação entre elas, no que diz respeito a algumas extensões infinitas de grupos finitos. Este resultado foi verificado em 1995, por Mazur, ver [10], e segue no teorema abaixo.

Teorema 3.10. *Se G é um grupo finito e C_∞ representa um grupo cíclico infinito, então o problema do isomorfismo para $\mathbb{Z}(G \times C_\infty)$ tem resposta afirmativa se, e somente se, tem resposta afirmativa para G e vale a conjectura do normalizador em G.*

Hertweck conseguiu uma generalização para tal resultado, para extensões finitas de G. E então, em 2001, fazendo uso de tal resultado, apresentou contra-exemplos para as duas questões centrais do nosso trabalho.

Teorema 3.11. *([6, Teorema B]). Existe um grupo solúvel X, que é o produto semi-direto de um subgrupo normal G e um subgrupo cíclico $\langle c \rangle$, tal que*

i) Existe um automorfismo não interno τ em G e uma unidade $t \in \mathcal{U}_1(\mathbb{Z}G)$ tal que $\tau(g) = g^t$ para todo $g \in G$;

ii) Em $\mathbb{Z}X$, o elemento c inverte o elemento t;

iii) O subgrupo $Y = \langle G, tc \rangle$ *de* $\mathcal{U}_1(\mathbb{Z}G)$ *tem a mesma ordem de* X *mas não é isomorfo a* X;

iv) A ordem de X *é* $2^{21}.97^{28}$. *O grupo* X *tem um 97-subgrupo de Sylow normal e o comprimento da série derivada de* X *é 4.*

E $\mathbb{Z}X \simeq \mathbb{Z}Y$ mas X não é isomorfo a Y.

Teorema 3.12. *([6, Teorema A]). Existe um grupo finito* G *com um automorfismo de grupo não-interno* τ, *tal que* $\tau(g) = u^{-1}gu$ *com* $u \in \mathcal{U}_1(\mathbb{Z}G)$, *para todo* $g \in G$. *O grupo* G *tem ordem* $2^{25}.97^2$, *um 97-subgrupo de Sylow normal, e é metabeliano.*

Dessa forma obtemos um grupo G tal que $Aut_{\mathcal{U}}(G) \subsetneq Inn(G)$

Uma abordagem mais detalhada sobre tais contra-exemplos pode ser obtida em Hertweck [6].

Capítulo 4

Resultados Obtidos

Dividiremos este capítulo em três seções: na primeira, considerando R um anel nilpotente finito, mostraremos que seu grupo adjunto G é solução para o Problema do Isomorfismo e para a Propriedade do Normalizador. Na seção seguinte, considerando R agora um anel radical, ou seja, todos os seus elementos são quase-regulares, verificaremos que seu grupo adjunto, que é chamado de grupo círculo, satisfaz o (Iso) e o (Nor), neste caso sem considerar a hipótese de que R é nilpotente. Destacamos que, este resultado, se trata de uma nova demonstração do resultado de Sandling num caso particular e ainda , que satisfaz a Propriedade do Normalizador, o que é um resultado novo da dissertação. Na última seção apresentaremos a estrutura do grupo adjunto de um anel particular.

Para mostrar os resultados citados acima faremos uso dos teoremas apresentados no decorrer do trabalho.

4.1 O grupo adjunto como solução para o (Iso) e o (Nor)

Vamos então considerar um anel R nilpotente finito, não necessariamente com unidade, e vamos mostrar que seu grupo adjunto G, é um grupo nilpotente. Daí, usando resultados apresentados nos capítulos anteriores, concluímos que G é determinado pelo seu anel de grupo integral e ainda satisfaz a Propriedade do Normalizador.

Sendo R nilpotente temos que existe um número inteiro positivo n, tal que $R^n = 0$ e então podemos considerar a seguite cadeia de ideais

$$R \supset R^2 \supset R^3 \supset \ldots \supset R^n = 0.$$

Fazendo a intersecção de G em cada uma das parcelas acima obtemos:

$$G = G \cap R \supset G \cap R^2 \supset G \cap R^3 \supset \ldots \supset G \cap R^n = 0.$$

Para simplificar a nossa notação iremos considerar $G \cap R^i = H_i$, para $2 \leq i \leq n$, obtendo

$$G \supset H_2 \supset H_3 \supset \ldots \supset H_n = 0.$$

Vamos agora verificar que G é um grupo nilpotente, para isto, devemos provar os seguintes fatos:

1. $H_i \lhd G$;

2. $H_{i+1}/H_i \subset \zeta(G/H_i)$.

Para verificar a condição 1, vamos primeiro mostrar que H_i é subgrupo de G.

$i)$ $H_i \neq \emptyset$. De fato,

$$0 \in G,\ 0 \in R^i \Longrightarrow 0 \in H_i.$$

$ii)$ Sendo $g, h \in H_i$ e h' o quase-inverso de h, temos que $g \circ h' \in H_i$. De fato, como $g, h \in G$, logo $h' \in G$ e ainda, sendo G um grupo com a operação $\circ$ temos que $g \circ h' \in G$.

Por outro lado, $g, h \in R^i$ e sabemos que $h \circ h' = 0$, ou seja, $h + h' + hh' = 0$. Mas como R^i é um ideal bilateral temos que $hh' \in R^i$, daí $h' = -h - hh'$ pertence a R^i.

Deste modo temos que $g \circ h' = g + h' + gh'$ pertence a R^i.

Concluímos então, de $i)$ e $ii)$, que H_i é subgrupo de G.

Vamos agora mostrar que H_i é normal em G. Para isto, dado $h \in H_i$ queremos verificar que $g' \circ h \circ g \in H_i$, em que $g \in G$ e g' é o seu quase-inverso. Sabemos que

$$g' \circ h \circ g = g' \circ (h + g + hg) = g' + h + g + hg + g'h + g'g + g'hg =$$

$$= h + hg + g'h + g'hg,$$

pois $g' + g + g'g = 0$.

E então, como $h \in R^i$ e R^i é um ideal bilateral, concluímos que

$$g' \circ h \circ g \in R^i.$$

Como $h, g \in G$ temos também que $g' \circ h \circ g \in G$, concluindo que $g' \circ h \circ g \in H_i$ e então H_i é normal em G.

Para mostrar a condição 2, devemos mostrar que os elementos de H_{i+1}/H_i comutam com os elementos de G/H_i. Tomemos então

$$h \circ H_i \in H_{i+1}/H_i \;\; \text{com} \;\; h \in H_{i+1} \qquad \text{e}$$

$$g \circ H_i \in G/H_i \;\; \text{com} \;\; g \in G$$

e vamos mostrar que

$$(h \circ H_i) \circ (g \circ H_i) = (g \circ H_i) \circ (h \circ H_i)$$

ou equivalentemente, mostrar que

$$h' \circ g' \circ h \circ g \in H_i.$$

De fato, como $h, g \in G$, já temos que $h' \circ g' \circ h \circ g \in G$. Mas $h \in H_{i+1}$, ou seja $h \in R^{i+1}$ e como $R^{i+1} \subseteq R^i$, temos que $h, h' \in R^i$.

Daí,

$$h' \circ g' \circ h \circ g = h' \circ g' \circ (h + g + hg) =$$
$$= h' \circ (g' + h + g + hg + g'h + g'g + g'hg) =$$
$$= h' + h + hg + g'h + g'hg + h'(h + hg + g'h + g'hg) \in R^i,$$

já que R^i é ideal.

Mostramos assim que

$$h' \circ g' \circ h \circ g \in H_i.$$

e então segue-se o resultado da condição 2.

Finalmente, concluímos que G é um grupo nilpotente e então pelo teorema 2.3,

$$\mathbb{Z}G \simeq \mathbb{Z}H \Longrightarrow G \simeq H,$$

ou seja, G é determinado pelo seu anel de grupo integral. Podemos ainda concluir, usando o corolário 3.3, que vale o (Nor) para o grupo G.

4.2 O grupo círculo como solução para o (Iso) e o (Nor)

Agora, considerando R um anel finito e G o seu grupo círculo mostraremos que G possui um 2-subgrupo de Sylow normal e lembrando da apresentação feita no terceiro capítulo concluiremos que G satisfaz a propriedade do normalizador. Na verdade, verificamos que todos os p-subgrupos de Sylow de G são normais em G, assim, usando resultados anteriores concluímos que G também satisfaz o (Iso).

De fato, temos por definição que se G é o grupo círculo de R então G e R são iguais como conjuntos, além disso, sendo R um anel, temos que R munido com a operação de soma, (R,+), é um grupo abeliano finito e então podemos escrever,

$$(R,+) = A_{p_1} \oplus A_{p_2} \oplus \ldots \oplus A_{p_s}$$

em que $A_{p_1}, A_{p_2}, \ldots, A_{p_s}$ são p_i-subgrupos de Sylow de (R,+).

Vamos mostrar que cada um destes p_i-subgrupos é um ideal de R.

De fato, se $x \in A_p$ e $y \in A_q$ com $p \neq q$, então $xy = 0$, pois $o(x) = p^n$ e $o(y) = q^m$. Logo,

$$\underbrace{xy + xy + \ldots + xy}_{p^n} = \underbrace{(x + \ldots + x)}_{p^n} y = 0$$

$$\underbrace{xy + xy + \ldots + xy}_{q^m} = x \underbrace{(y + \ldots + y)}_{q^m} = 0$$

e então $o(xy)|p^n$ e $o(xy)|q^m$ sendo $o(xy) = 1$ e portanto $xy = 0$.

Por outro lado se $x, y \in A_p$ então, tomando no desenvolvimento acima $p = q$, temos que $o(xy)|p^n$ e portanto $o(xy) = p^m$ logo $xy \in A_p$.

Considerando $a \in R$ e $b \in A_{p_i}$ temos que $a = a_{p_1} + a_{p_2} + \ldots + a_{p_s}$ e logo $ab = a_{p_i}b \in A_{p_i}$ e $ba = ba_{p_i} \in A_{p_i}$. Com estas observações concluímos que $A_{p_1}, A_{p_2}, \ldots, A_{p_s}$ são ideais de R.

Uma vez que $G = R$, $G \cap A_{p_i} = A_{p_i}$; e A_{p_i} é um ideal, mostraremos que A_{p_i} é também um subgrupo normal de G. De fato,

1. $0 \in A_{p_i}$, logo $A_{p_i} \neq \emptyset$;

2. Tome $a, b \in A_{p_i}$ e $b' \in G$ o quase-inverso de b, ou seja, $b' = -b - bb'$ e então $b' \in A_{p_i}$ e $a \circ b' = a + b' + ab' \in A_{p_i}$;

3. Tome $h \in A_{p_i}$ e $g \in G$, teremos que

$$g' \circ h \circ g = g' + h + g + hg + g'(h + g + hg) =$$

$$= h + hg + g'h + g'hg \in A_{p_i}.$$

Então usando as verificações 1, 2 e 3 concluímos que $A_{p_i} = G \cap A_{p_i}$ é um subgrupo normal de G e em particular A_{p_1} é o 2-subgrupo de Sylow normal em G.

Concluímos, usando o teorema 3.9, que G satisfaz a propriedade do normalizador.

Obtemos o mesmo resultado para um p-subgrupo de Sylow, sendo p um primo qualquer, ou seja, verificamos que todos os p-subgrupos de sylow de G são normais em G, daí usando o teorema 1.3 concluímos que G é nilpotente e portanto satisfaz o problema do isomorfismo.

Note que esta é uma demonstração alternativa à de Sandling, fazendo uso do resultado de Roggenkamp e Scott, [12].

4.3 A estrutura do grupo adjunto

Na seção anterior um dos nossos resultados foi mostrar que, quando o grupo adjunto G é todo o anel R, ou seja, G é um grupo círculo, vale a propriedade do normalizador, mas imediatamente pensamos, se seria possível verificar tal resultado para um caso mais geral, considerando agora G um grupo adjunto qualquer.

Tentamos então conhecer melhor como seria a estrutura do grupo adjunto G. Conseguimos verificar que, no caso em que um anel finito com unidade R tem característica p, p primo, G pode ser escrito como um produto semidireto entre o radical de Jacobson $J = J(R)$, de R e um subgrupo B, de G, que pode ser escrito como produto direto de grupos gerais lineares. Antes, citaremos algumas definições e resultados que utilizaremos:

Definição 4.1. *Seja R um anel. O Radical de Jacobson de R, denotado por $J(R)$, é o ideal maximal que é composto por elementos quase-regulares.*

Observamos então, que J pode ser visto como um anel radical, tendo como grupo círculo ele próprio e pelo que verificamos na seção anterior, J será nilpotente, representando uma resposta positiva para o (Nor).

Definição 4.2. *Um anel R que não possui ideais próprios, formados por elementos quase-regulares, é chamado semi-simples, ou seja, se R é semi-simples seu único ideal formado por elementos quase-regulares é o* (0).

Este conceito de "semi-simples"é devido a N. J. Divinsky, o conceito clássico é: *R é semi-simples se é artiniano e se não tem ideais nilpotentes não triviais!* É neste sentido que vale o teorema seguinte. Mas note que, se W for o radical clássico ou o de Wedderburn (que é a soma de todos os ideais nilpotentes em R) então R/W é semi-simples se R é artiniano e ainda teremos $J = W$. Mas o anel R é artiniano já que é finito e logo, no nosso caso, as definições são equivalentes.

Teorema 4.3. *(Wedderburn-Artin). Um anel R é semi-simples se, e somente se, ele é soma direta de anéis de matrizes sobre anéis de divisão:*

$$R \simeq Mat_{n_1}(D_1) \oplus \ldots \oplus Mat_{n_k}(D_k).$$

Nesta parte do trabalho escreveremos o nosso grupo adjunto G como produto direto de seus subgrupos normais, então a seguinte proposição, ver [8], nos possibilita trabalhar com estes subgrupos, pois se verificarmos a validade da propriedade para estes, podemos estender para todo G.

Proposição 4.4. *Seja G o produto direto dos grupos G_1 e G_2, $G = G_1 \times G_2$. Então a propriedade do normalizador vale para G se, e somente se, ela vale para G_1 e G_2.*

Demonstração. Denote por $\varphi_i : G \to G_i$ a projeção natural de G em G_i. Sua extensão aos anéis de grupo também será indicada por φ_i. Observe que $G_i = Ker(\varphi_j)$, se $i \neq j$. Suponha que a propriedade do normalizador vale para G e seja $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G_i)}(G_i)$ uma unidade no normalizador de G_i. Então u está também no normalizador de G e consequentemente $u = wg$, com $g \in G$ e $w \in \zeta(\mathcal{U}(\mathbb{Z}G))$. Logo, temos que $u = \varphi_i(u) = \varphi_i(w)\varphi_i(g)$ e então vale a propriedade do normalizador para G_i.

Para verificar que a condição é também suficiente, suponha que a propriedade do normalizador vale para os grupos G_1 e G_2, e seja $u \in \mathcal{N}_{\mathcal{U}}(G)$ uma unidade no normalizador de G. Sendo $u_i = \varphi_i(u)$, temos que u_i está no normalizador de G_i e assim $u_i = w_i g_i$, com w_i uma unidade central em $\mathbb{Z}G_i$ e $g_i \in G_i$. Como G é o produto direto de G_1 e G_2, temos que w_i é também uma unidade central em $\mathbb{Z}G$. Definindo $w = uu_1^{-1}u_2^{-1}$, claramente w é uma unidade central de $\mathbb{Z}G$. Temos então que $u = u_2u_1w = g_2g_1w_1w_2w \in G\cdot\zeta$, e portanto vale a propriedade do normalizador para G.

Para verificar que w é central, observe que $w = uw_1^{-1}w_2^{-1}g_1^{-1}g_2^{-1}$ está no normalizador de G, e $\varphi_i(w) = \pm 1$. Logo segue que para todo $g \in G$, $[w, g] = g_o$ para algum $g_o \in G$. Aplicando φ_i em ambos os lados da expressão acima, obtemos $\varphi_i(g_o) = \varphi_i(w^{-1})\varphi_i(g^{-1})\varphi_i(w)\varphi_i(g) = 1$. Assim $g_o = 1$ e portanto w é uma unidade central de $\mathbb{Z}G$. $\square$

O próximo teorema, vide [5], nos possibilita decompor R em subanéis como uma soma direta de espaços vetoriais.

Teorema 4.5. *(Wedderburn-Malcev). Seja R uma álgebra de dimensão finita sobre um corpo $\mathbb{F}$, com radical de Jacobson J, tal que R/J seja separável, então existe uma subálgebra R_0, tal que $R = R_0 \oplus J$ (como espaços vetoriais), em que $R_0 \simeq R/J$.*

Para concluirmos que R/J é uma álgebra separável usamos o seguinte resultado. Vide [5].

Teorema 4.6. *Se um corpo $\mathbb{F}$ é perfeito (por exemplo, com característica p ou finito), então toda $\mathbb{F}$-álgebra semi-simples é separável.*

No nosso caso, vamos considerar o corpo finito $\mathbb{Z}_p$, e então sendo R/J uma $\mathbb{Z}_p$-álgebra semi-simples, usando este teorema, teremos que R/J é separável e estaremos dentro das hipóteses do teorema de Wedderburn-Malcev.

Observamos que o próximo teorema é um resultado novo da dissertação e enunciaremos este nosso resultado como segue:

Teorema 4.7. *Seja R um anel finito com unidade e R_{p_i} os seus p_i-subgrupos de Sylow, todos com característica p_i. Sendo G o grupo adjunto de R, então podemos escrever $G = J \rtimes B$, em que J é o radical de Jacobson de R e B é um subgrupo de G que pode ser escrito como produto direto de grupos gerais lineares.*

Demonstração. Sendo R um anel finito com unidade, temos que $(R, +)$ é um grupo abeliano e podemos escrevê-lo como soma direta de seus p_i-subgrupos de Sylow, ou seja,

$$R = R_{p_1} \oplus \ldots \oplus R_{p_n},$$

lembrando que cada R_{p_i} é um ideal, sendo esta uma decomposição de R em p-anéis.

Seja G o grupo adjunto de R e consideremos $G_{p_i} = G \cap R_{p_i}$. Já mostramos, na seção 4.2, p.28, que G_{p_i} é subgrupo normal de G, temos ainda que se $a \in R_{p_i}$, e a é quase-regular, ou seja, $a \in G$, então existe $b \in G$ tal que $a + b + ab = 0$ e logo $b = -a - ab$ é um elemento de R_{p_i}, já que este é ideal e logo $b \in G_{p_i}$. Portanto concluímos que $G_{p_i} = G \cap R_{p_i}$ é o grupo adjunto de R_{p_i}. Deste modo, usando a proposição 2.8, teremos $G_{p_i} \simeq \mathcal{U}(R_{p_i})$, e como é fácil verificar que

$$\mathcal{U}(R) = \mathcal{U}(R_{p_1}) \times \ldots \times \mathcal{U}(R_{p_n}),$$

poderemos escrever G, como o seguinte produto direto,

$$G = G_{p_1} \circ \ldots \circ G_{p_n}.$$

Assim, para conseguir o resultado desejado, basta verificar o problema do normalizador para cada G_{p_i}. Desta forma, reduzimos o nosso trabalho a um anel R do tipo p-anel, ou seja, se $r \in R$ temos $r + \ldots + r = 0$, se somarmos r um número de vezes igual a uma potência de p.

Seja $J = J(R)$ o radical de Jacobson de R, sabemos que o quociente R/J, é um anel semi-simples; já que R é finito é artiniano, logo podemos escrever como uma soma direta de anéis de matrizes definidas sobre anéis de divisão, ou seja,

$$R/J \simeq Mat_{n_1}(D_1) \oplus \ldots \oplus Mat_{n_k}(D_k),$$

em que os D_i são anéis de divisão.

Vamos agora supor que o nosso anel R possui característica p, sendo p primo, ou seja, existe uma cópia do $\mathbb{Z}_p$ dentro de R e podemos considerar o nosso anel como sendo uma álgebra sobre $\mathbb{Z}_p$.

Já que $char(R) = p$, cada um dos anéis de matrizes têm também característica p, assim como os anéis de divisão D_i. Portanto os anéis de divisão, por serem finitos, são na verdade corpos finitos de modo que $D_i = \mathbb{F}_{q_i}$, em que $q_i = p^{k_i}$.

Ainda pela $char(R) = p$, temos que $char(R/J) = p$, ou seja, R/J também é uma $\mathbb{Z}_p$-álgebra que é semi-simples, portanto, pelo teorema 4.6, temos que R/J é separável. Podemos então aplicar o teorema 4.5 e concluir que existe uma subálgebra A, com $A \simeq R/J$, sendo

$$R = A \oplus J, \quad \text{como espaços vetoriais.}$$

Queremos mostrar que $G = J \rtimes B$, em que $B = G \cap A$. Lembramos que $J \trianglelefteq G$ como subgrupo em relação à operação $\circ$. De fato, uma vez que J é ideal de R,

$$a, b \in J, \text{ temos que } a \circ b = a + b + ab \in J$$

e sendo a' tal que $a \circ a' = 0$, temos

$$a + a' + aa' = 0 \text{ e portanto } a' = -a - aa' \in J,$$

concluindo assim que $J \leqslant G$.

Agora se $a \in J$ e $g \in G$, temos

$$g' \circ a \circ g = a + g'a + ag + g'ag \in J$$

e então $J \trianglelefteq G$.

Mostraremos agora que $B \leqslant G$. De fato:

1. Note que $0 \in B$, portanto $B \neq \emptyset$;

2. Sejam $a, b \in B$, logo $a \circ b = a + b + ab \in A$, pois A é subanel de R, como $a, b \in G$, $a \circ b \in G$, logo $a \circ b \in G \cap A = B$;

3. Sendo $b \in B$, mostraremos que $b' \in B$. Como $b' \in G$ e $G \subseteq R$ temos que, $b' = a + h$, com $a \in A$ e $h \in J$. Mas $b \circ b' = 0$, logo

$$b + a + h + ba + bh = 0, \text{ isto é, } b + a + ba = -h - bh,$$

mas $b + a + ba \in A$ e $-h - bh \in J$ então $b + a + ba = 0$ e portanto $a = b'$ e $b' \in A$, mas sendo b' o quase-inverso de b, temos $b' \in G$, donde $b' \in B$. Concluindo assim que $B \leqslant G$.

Mostraremos agora que $B \circ J = G$. Note que, para todo $g \in G,\ g = a + h$, com $a \in A,\ h \in J$ e $g' = b + f$, com $b \in A,\ f \in J$. Mas,

$$g \circ g' = 0 = a + b + ab + h + f + af + hb + hf,\ \text{logo } a + b + ab = 0,$$

isto é, a é quase-regular e portanto $a \in G$, ou seja, $a \in B = G \cap A$.

Mostramos assim que $G = B + J$; vamos mostrar que $B + J = B \circ J$. De fato,

1. Sendo $b \in B$ e $h \in J$, temos $b \circ h = b + (h + bh) \in B + J$. Donde,

$$B \circ J \subseteq B + J.$$

2. Observe que $b + h = b \circ (h + b'h) \in B \circ J$. De fato,

$$b \circ (h + b'h) = b + h + b'h + bh + bb'h = b + h + (b' + b + bb')h = b + h.$$

Logo $B + J \subseteq B \circ J$. E de 1 e 2 concluímos que $B + J = B \circ J$.

Chegamos então ao fato de que $G = J \rtimes B$.

Por fim, sendo $B = G \cap A$, consideraremos em $Mat_n(\mathbb{F}_q)$ as matrizes quase-regulares, mas como $Mat_n(\mathbb{F}_q)$ é um anel com unidade, usando a proposição 2.8, concluímos que tais matrizes são da forma $u - 1$, em que u é uma matriz inversível, ou seja, $u \in \mathcal{U}(Mat_n(\mathbb{F}_q))$.

Podemos usar a seguinte notação: $\mathcal{U}(Mat_n(\mathbb{F}_q)) = GL(n, \mathbb{F}_q)$ e escrever B como produto direto de tais grupos gerais lineares:

$$B \simeq GL(n_1, \mathbb{F}_{q_1}) \times \ldots \times GL(n_k, \mathbb{F}_{q_k}).$$

$\square$

Chegamos assim que o grupo adjunto G, de um anel finito com unidade R, sendo $char(R) = p$, pode ser escrito como um produto semidireto do radical de Jacobson $J = J(R)$ por um produto direto de grupos gerais lineares.

Para o caso em que o anel R não possui unidade, vamos considerar G o seu grupo adjunto e usar a observação feita no capítulo 2 para definir um anel R_1, tal que $R_1 = \mathbb{Z} \times R$, sendo G_1 o seu grupo adjunto, ainda pela observação, concluímos que $G_1 \simeq C_2 \times G$, em que C_2 é um grupo cíclico de ordem 2, e daí se conseguirmos obter o (Nor) para um anel com unidade ficamos com $J \rtimes B \simeq C_2 \times G$, e teremos mostrado também para o grupo adjunto de um anel sem unidade, fazendo uso da proposição 4.4.

Já observamos anteriormente que J é solução para a Propriedade do Normalizador, mostraremos ainda que tal propriedade é também satisfeita pelo grupo B apresentado acima e para esta conclusão mostraremos que o grupo geral linear é solução para o (Nor). Antes citaremos os quatro tipos de geradores do grupo de automorfismos de $GL(n, \mathbb{F}_q)$, $Aut(GL)$, ver [3].

1. Automorfismos internos: $\varphi_1(M) = N^{-1}MN$, para alguma matriz invertível N.

2. Automorfismos induzidos por automorfismos do corpo $\mathbb{F}_q$. Se $\lambda : \mathbb{F}_q \to \mathbb{F}_q$, então sendo $M = [m_{ij}]$, teremos $\varphi_2(M) = [\lambda(m_{ij})] = \lambda(M)$.

3. Homotetias: $\varphi_3(M) = \mathcal{X}(M).M$, sendo $\mathcal{X}$ um morfismo dos grupos multiplicativos $\mathcal{X} : GL(n, \mathbb{F}_q) \to \mathbb{F}_q^*$, tal que $\mathcal{X}(\alpha I) = \alpha^{-1} \Leftrightarrow \alpha = 1$.

4. A transformação contragradiente: $\varphi_4(M) = (M^t)^{-1}$.

Observamos que os automorfismos de cada um dos tipos citados gera um subgrupo de $Aut(GL)$, em particular os do 1 geram o subgrupo normal $Inn(GL)$, dos automorfismos internos.

Agora apresentamos dois resultados que serão fundamentais para mostrar que o grupo geral linear é solução para o (Nor). Primeiro citamos um teorema de Thierry Petit e Sehgal,[9].

Teorema 4.8. *Se $u \in \mathcal{N}_{\mathcal{U}}(G)$, então $\varphi_u(g) = u^{-1}gu$ é um conjugado a g, para qualquer $g \in G$, isto é, existe $h \in G$ tal que $u^{-1}gu = h^{-1}gh$, com h fixado, mas dependendo do g.*

Antes de citar o próximo resultado, definimos transvecções como sendo os conjugados de $X_{ij}(\alpha)$, ou seja, $N^{-1}X_{ij}(\alpha)N,\ N \in GL(n, \mathbb{F}_q)$. Sendo $X_{ij}(\alpha) = I + \alpha E_{ij},\ \alpha \in \mathbb{F}_q^*$, em que E_{ij} é a matriz, com $i \neq j$, da base canônica do espaço de matrizes.

Segue então o teorema que pode ser encontrado em [1].

Teorema 4.9. *$GL(n, \mathbb{F}_q)$ é gerado pelo conjunto de todas as transvecções e todas as matrizes diagonais invertíveis.*

Segue finalmente o importante resultado para o grupo geral linear:

Teorema 4.10. *Vale a Propriedade do Normalizador para o grupo geral linear, $GL(n, \mathbb{F}_q)$.*

Demonstração. Observamos que a ordem do nosso grupo, ver [11], é dada por $|GL(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-1})$, $(n \geq 2)$, de modo que é um valor par, ou seja, não estamos com um caso trivial do teorema 3.7.

Se $n = 1$, então $GL(n, \mathbb{F}_q) = \mathbb{F}_q^*$, mas sabemos que o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico, logo abeliano e então todo p-subgrupo é normal, portanto, pelo teorema 3.9, vale o (Nor) em $GL(1, \mathbb{F}_q)$.

No caso em que $n \neq 1$, teremos como elementos de $GL(n, \mathbb{F}_q)$, matrizes invertíveis de ordem maior ou igual a dois. Neste caso, analisaremos cada um dos quatro automorfismos separadamente e também suas possíveis combinações. No final, concluiremos que a única possibilidade para automosfismos de $GL(n, \mathbb{F}_q)$, são os internos e daí teremos o resultado. Aqui vamos desenvolver a mesma técnica utilizada por Jackowski e Marciniak na demonstração do teorema 3.8.

Observe que automorfismos dos tipos 2 e 4 comutam. De fato, sendo $MM^{-1} = I$, temos $\lambda(MM^{-1}) = \lambda(I) = I$, já que λ é automorfismo de $\mathbb{F}_q$, e logo $\lambda(M^{-1}) = (\lambda(M))^{-1}$. Teremos que $\varphi_4(\varphi_2(M)) = [(\lambda(M))^t]^{-1} = [\lambda(M^t)]^{-1} = \lambda[(M^t)^{-1}] = \varphi_2(\varphi_4(M))$.

Assim como os automorfismos do tipo 1, os do tipo 3 também geram um subgrupo normal. De fato, $\varphi_3(M) = \mathcal{X}(M)M$, com $\mathcal{X}(M) \in \mathbb{F}_q^*$, logo $\varphi_3(M)M^{-1} = \mathcal{X}(M)I$, ou seja, $\varphi_3(M)M^{-1}$ é uma matriz escalar, portanto central. Considere ψ um automorfismo qualquer de $GL(n, \mathbb{F}_q)$, defina $\varphi' = \psi \circ \varphi_3 \circ \psi^{-1}$. Temos que

$$\varphi'(N) = \psi(\varphi_3(\psi^{-1}(N))) = \psi(\varphi_3(\psi^{-1}(N)))N^{-1}N = \psi(\varphi_3(\psi^{-1}(N)))\psi(\psi^{-1}(N^{-1}))N =$$

$$= \psi(\varphi_3(\psi^{-1}(N))(\psi^{-1}(N))^{-1})N,$$

mas já vimos que $\varphi_3(\psi^{-1}(N))(\psi^{-1}(N))^{-1}$ é central, logo $\mathcal{X}'(N) = \psi(\varphi_3(\psi^{-1}(N))(\psi^{-1}(N))^{-1})$ também será. Podemos mostrar facilmente que $\mathcal{X}'$ é um morfismo de grupos: de fato,

$$\mathcal{X}'(N_1N_2) = \psi(\varphi_3(\psi^{-1}(N_1N_2))(\psi^{-1}(N_1N_2))^{-1}) =$$

$$= \psi(\varphi_3(\psi^{-1}(N_1))\underbrace{\varphi_3(\psi^{-1}(N_2))(\psi^{-1}(N_2))^{-1}}_{central}(\psi^{-1}(N_1))^{-1}) =$$

$$= \psi(\varphi_3(\psi^{-1}(N_1))(\psi^{-1}(N_1))^{-1})\psi(\varphi_3(\psi^{-1}(N_2))(\psi^{-1}(N_2))^{-1}) = \mathcal{X}'(N_1)\mathcal{X}'(N_2).$$

E concluímos então que $\varphi'(N) = \mathcal{X}'(N)N$ é de fato uma homotetia.

Estes resultados nos permite fazer com que qualquer combinação envolvendo todos os quatro tipos de automorfismos possíveis, seja escrita na seguinte ordem: $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4$. Agora vamos considerar matrizes da forma:

$$M = \begin{bmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & -1 \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & -1 \\ 0 & 0 & \dots & 0 & -1 \end{bmatrix}.$$

É fácil ver que $M^2 = I$. Seja S o 2-subgrupo de Sylow mencionado no teorema 3.8 tal que $M \in S$. Os automorfismos tipo 4 obviamente não fixam esta matriz, porém os do tipo 2 fixam tal matriz, portanto automorfismos do tipo 4 não ocorrem sós nem em composição com os do tipo 2, já que estes comutam, exceto possivelmente os casos triviais.

Tomemos agora matrizes do tipo

$$D = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & \alpha \end{bmatrix},$$

com α arbitrário em $\mathbb{F}_q^*$. Considerando um automorfismo tipo 2 e usando o teorema 4.8, temos que $\varphi_2(D) = N^{-1}DN$, em que D é da forma acima. Se $\mathbb{F}_q = \mathbb{Z}_2$, claramente φ_2 será a identidade, caso contrário se aplicarmos o determinante teremos, do mesmo modo, que $\lambda(\alpha) = \alpha$, portanto não há automorfismos do tipo 2, não triviais, atuando isoladamente, ou seja, se φ é um automorfismo tipo 2, $\varphi \notin I_S$.

Para analisarmos automorfismos do tipo 3, vamos considerar a matriz $X_{ij}(\alpha) = I + \alpha E_{ij}$, apresentada anteriormente, por exemplo, $X_{ij}(\alpha)$ pode ser a matriz

$$X_{ij}(\alpha) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{bmatrix}.$$

Considerando o automorfismo $\varphi_3(X_{ij}(\alpha)) = \mathcal{X}(X_{ij}(\alpha))X_{ij}(\alpha)$, ou seja, $\mathcal{X}(X_{ij}(\alpha))X_{ij}(\alpha) = N^{-1}X_{ij}(\alpha)N$ pelo teorema 4.8 ou $\mathcal{X}(X_{ij}(\alpha))NX_{ij}(\alpha) = X_{ij}(\alpha)N$, sendo a matriz $X_{ij}(\alpha)$ do tipo citado acima e $N = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ uma matriz invertível, dependendo de $X_{ij}(\alpha)$. Daí, supondo que $\mathcal{X}(X_{ij}(\alpha)) = k$, a igualdade acima ficaria $kNX_{ij}(\alpha) = X_{ij}(\alpha)N$, ou seja,

$$\begin{bmatrix} ka_{11} & ka_{12} & k(\alpha a_{12} + a_{13}) \\ ka_{21} & ka_{22} & k(\alpha a_{22} + a_{23}) \\ ka_{31} & ka_{32} & k(\alpha a_{32} + a_{33}) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} + \alpha a_{31} & a_{22} + \alpha a_{32} & a_{23} + \alpha a_{33} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

e como não podemos ter na matriz N uma coluna nula, já que esta é invertível, obtemos que $\mathcal{X}(X_{ij}(\alpha)) = 1$ e portanto φ_3 é a identidade para tais matrizes. Tal resultado, feito para uma matriz de ordem 3, pode ser estendido para matrizes de ordem n, já que matrizes do tipo $X_{ij}(\alpha)$, quando multiplicadas pela direita de uma matriz N, substituem nesta última matriz uma coluna por uma combinação de duas de suas colunas e o análogo ocorre com relação à esquerda para uma das linhas.

Se considerarmos conjugados de $X_{ij}(\alpha)$, teremos:

$$\varphi_3(N^{-1}X_{ij}(\alpha)N) = \varphi_3(N^{-1})X_{ij}(\alpha)\varphi_3(N) = (\mathcal{X}(N)N)^{-1}X_{ij}(\alpha)\mathcal{X}(N)N =$$

$$= (\mathcal{X}(N))^{-1}N^{-1}X_{ij}(\alpha)\mathcal{X}(N)N = N^{-1}X_{ij}(\alpha)N.$$

Portanto automorfimos do tipo 3 também fixam os conjugados de $X_{ij}(\alpha)$, fixando as transvecções. Devemos ainda verificar que estes automorfismos, quando aplicados à matrizes diagonais invertíveis, se comportam como a identidade, para chegarmos a este resultado basta verificar que matrizes do tipo: $D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{bmatrix}$, são fixadas por φ_3, visto que matrizes diagonais invertíveis podem ser escritas como produto destas, fazendo apenas α mudar de posição na diagonal principal. Usando a matriz D acima e aplicando o teorema 4.8 temos que $kND = DN$, sendo $k = \mathcal{X}(D)$, ou seja,

$$\begin{bmatrix} ka_{11} & ka_{12} & k(\alpha a_{13}) \\ ka_{21} & ka_{22} & k(\alpha a_{23}) \\ ka_{31} & ka_{32} & k(\alpha a_{33}) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \alpha a_{31} & \alpha a_{32} & \alpha a_{33} \end{bmatrix}.$$

Analisando a igualdade acima concluímos que $k = 1$ ou ($k\alpha = 1$ e $k = \alpha$). No primeiro caso temos que φ_3 fixa a matriz D, no segundo temos que D possui ordem 2, ou seja, D pertence a algum 2-subgrupo de Sylow de $GL(n, \mathbb{F}_q)$ (talvez não o nosso S fixado inicialmente), se D pertencer ao 2-subgrupo de Sylow S, teremos $D = \varphi_3(D) = kD$, sendo $k = 1$. Caso contrário um conjugado de D está em S, ou seja, $L^{-1}DL \in S,\ L \in GL(n, \mathbb{F}_q)$. Logo $\varphi_3(L^{-1}DL) = L^{-1}DL$, já que φ_3 fixa os elementos de S, porém

$$L^{-1}DL = \varphi_3(L^{-1}DL) = \varphi_3(L^{-1})\varphi_3(D)\varphi_3(L) =$$

$$l^{-1}L^{-1}kDlL = L^{-1}kDL, \text{ com } k, l \in \mathbb{F}_q^*,$$

donde $D = kD$, mas sendo D invertível temos $k = 1$. Observamos que o mesmo resultado pode ser obtido facilmente para uma matriz de ordem n, já que, quando uma matriz do tipo D é multiplicada à direita de uma matriz N, uma coluna desta última é substituída por um múltiplo e o análogo ocorre com relação à esquerda para uma das linhas.

Concluímos assim que automorfismos do tipo 3, não triviais, não ocorrem em I_S.

Aplicando automorfismos compostos dos tipos 3 e 2, ($\varphi_3 \circ \varphi_2$) nas matrizes $X_{ij}(\alpha)$, usando o teorema 4.8 e aplicando o mesmo raciocínio anterior, obtemos que $\mathcal{X}(X_{ij}(\lambda(\alpha))) = 1$ e portanto ficaríamos apenas com o automorfismo do tipo 2, que já verificamos que não ocorre só em I_S. Do mesmo modo, aplicando tal composição em matrizes do tipo D, citada acima, obtemos que $\mathcal{X}(X_{ij}(\lambda(\alpha))) = 1$, ficando só com o tipo 2, ou ainda que $\lambda(\alpha) = \alpha^{-1}$, o que é um absudo pois não existe este tipo de isomorfismo de corpo finito. Considerando conjugados de $X_{ij}(\alpha)$ $(C^{-1}X_{ij}(\alpha)C)$ e denotando $\varphi_3 \circ \varphi_2$ por ψ, temos, usando 4.8, que

$$\varphi_3 \circ \varphi_2(X_{ij}(\alpha)) = \psi(X_{ij}(\alpha)) = N^{-1}X_{ij}(\alpha)N$$

$$\psi(C^{-1}X_{ij}(\alpha)C) = \psi(C^{-1})\psi(X_{ij}(\alpha))\psi(C) = N^{-1}C^{-1}X_{ij}(\alpha)CN$$
$$\psi(X_{ij}(\alpha)) = \psi^{-1}(C^{-1})N^{-1}C^{-1}X_{ij}(\alpha)CN\psi^{-1}(C)$$
$$\psi(X_{ij}(\alpha)) = L^{-1}X_{ij}(\alpha)L,$$

que já analisamos. Portanto automorfismo do tipo 3 e 2, não triviais, não ocorrem em I_S.

Para as composições $\varphi_3 \circ \varphi_4$ e $\varphi_2 \circ \varphi_3 \circ \varphi_4$, usando a matriz que está no 2-subgrupo de Sylow S, $M = \begin{bmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & -1 \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & -1 \\ 0 & 0 & \dots & 0 & -1 \end{bmatrix}$, abordada anteriormente e supondo que estes automorfismos estão em I_S, ou seja, deveriam fixar esta matriz, obtemos contradições.

Para o caso de composições envolvendo os quatro tipos teríamos, para uma matriz invertível A e usando 4.8, que $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4(A) = N^{-1}AN$, ou seja, $\varphi_2 \circ \varphi_3 \circ \varphi_4(A) = \varphi_1^{-1}(N^{-1}AN) = P^{-1}N^{-1}ANP = L^{-1}AL$, mas acabamos de concluir que composições não triviais dos tipos 2,3 e 4 não ocorrem.

Para os casos de composições dos tipos 1 com qualquer um dos outros três tipos chegamos em situações já analisadas. De fato, sendo φ um automorfismo do tipo 2, 3 ou 4 e B uma matriz invertível, temos: $\varphi_1(\varphi(B)) = N^{-1}BN$, logo $\varphi(B) = \varphi_1^{-1}(N^{-1}BN)$, e portanto $\varphi(B) = L^{-1}BL$.

Com isso investigamos todas as possibilidades e então podemos concluir que os únicos automosfismos de $GL(n, \mathbb{F}_q)$, em I_S, são os internos. Portanto o grupo geral linear é solução para a propriedade do normalizador. $\square$

Então, como se trata de um grupo G, tal que $G = J \rtimes B$, sendo J e B grupos que representam soluções para o (Nor), acreditamos ter dado um grande passo para verificar a validade da propriedade do normalizador para mais esta classe de grupos.

Capítulo 5

Possíveis Generalizações

Nesta parte do trabalho, iremos generalizar algumas definições que aparecem na seção 2.1, como a da operação círculo, a de grupos adjuntos dentre outras e daremos, fazendo uso destas definições, possíveis generalizações de alguns dos resultados obtidos no capítulo anterior, pensando em extensões dos grupos adjunto e círculo.

Para generalizar as definições vamos sempre considerar um elemento $k \in \mathbb{Z}$, de modo que k funcione simplesmente como um "*contador*" no decorrer das contas, ou seja,

$$kxy = \begin{cases} \underbrace{xy + xy + \ldots + xy}_{k-vezes}, & \text{se } k > 0 \\ -\underbrace{(xy + xy + \ldots + xy)}_{k-vezes}, & \text{se } k < 0 \end{cases}.$$

Para $k = 0$ a próxima definição seria a conhecida operação de soma. Seguimos fazendo as definições como segue:

Definição 5.1. *Seja R um anel, não necessariamente com unidade. Definimos a nova operação em R por:*

$$x \circ_k y = x + y + kxy \quad \textit{para todo } x, y \in R.$$

Podemos verificar que esta operação continua sendo associativa: De fato,

$$x \circ_k (y \circ_k z) = x \circ_k (y + z + kyz) = x + y + z + kyz + kx(y + z + kyz) =$$

$$= x + y + z + kyz + kxy + kxz + kxkyz = x + y + kxy + z + k(x + y + kxy)z =$$

$$= (x + y + kxy) \circ_k z = (x \circ_k y) \circ_k z.$$

Veja que durante as contas usamos o fato de k ser um "*contador*" pertencente a $\mathbb{Z}$.

Observe que,

$$x \circ_k 0 = x + 0 + kx0 = x = 0 + x + k0x = 0 \circ_k x,$$

ou seja, o elemento $0 \in R$ continua sendo o neutro para a generalização.

Definição 5.2. *Seja R um anel. Um elemento $x \in R$ é chamado k-quase-regular à esquerda se existe um elemento $y \in R$ tal que $y \circ_k x = 0$; esse elemento é chamado um k-quase-inverso à esquerda de x. Similarmente, x é dito ser k-quase-regular à direita se existe $y \in R$ tal que $x \circ_k y = 0$.*

Um elemento $x \in R$ é chamado k-quase-regular se ele é k-quase-regular à esquerda e à direita.

Note que, se $x \circ_k y = 0 = z \circ_k x$, então $z = z \circ_k 0 = z \circ_k (x \circ_k y) = (z \circ_k x) \circ_k y = 0 \circ_k y = y$, ou seja, os k-quase-inversos à esquerda e à direita de um elemento k-quase-regular coincidem.

Já verificamos que a operação k-círculo é associativa e que tem o $0 \in R$, como elemento neutro, então podemos facilmente concluir que o conjunto de todos os elementos k-quase-regulares do anel R, considerando a operação $\circ_k$, formam um grupo.

Definição 5.3. *Seja R um anel. O grupo de todos os elementos k-quase-regulares de R, com a operação $\circ_k$, é chamado o grupo k-adjunto de R.*

Definição 5.4. *Se todos os elementos de um anel R são k-quase-regulares, ele é chamado um anel k-radical. O grupo k-adjunto de anel k-radical é chamado um grupo k-círculo.*

Observamos que se um elemento $x \in R$ é nilpotente, então x é k-quase-regular. De fato, se n é o menor inteiro tal que $x^n = 0$, o seu k-quase-inverso será o elemento

$$y = -x + kx^2 - k^2x^3 + k^3x^4 - k^4x^5 + \ldots + (-1)^{n-1}k^{n-2}x^{n-1}.$$

Nas próximas seções apresentaremos possíveis generalizações para alguns dos resultados do capítulo anterior.

5.1 O grupo k-adjunto como solução para o (Iso) e o (Nor)

Nesta seção, consideremos um anel nilpotente finito R, não necessariamente com unidade, e vamos mostrar que seu grupo k-adjunto, G_k, em que este $k \in \mathbb{Z}$, é um grupo nilpotente. Daí, concluímos que G_k é solução para as duas propriedades centrais.

Sendo R nilpotente temos que existe um número inteiro positivo n, tal que $R^n = 0$ e então podemos considerar a seguite cadeia de ideais

$$R \supset R^2 \supset R^3 \supset \ldots \supset R^n = 0.$$

Fazendo a intersecção de G_k em cada uma das parcelas acima obtemos:

$$G_k = G_k \cap R \supset G_k \cap R^2 \supset G_k \cap R^3 \supset \ldots \supset G_k \cap R^n = 0.$$

Para simplificar a nossa notação iremos considerar $G_k \cap R^i = H_i$, para $2 \leq i \leq n$, obtendo

$$G_k \supset H_2 \supset H_3 \supset \ldots \supset H_n = 0.$$

Vamos agora verificar que G_k é um grupo nilpotente, observamos que esta demonstração é análoga a que foi desenvolvida no capítulo anterior para o grupo adjunto G, diferenciando apenas pela presença do fator k.

Devemos então provar os seguintes fatos:

1. $H_i \lhd G_k$;

2. $H_{i+1}/H_i \subset \zeta(G_k/H_i)$.

Para mostrar a condição 1, vamos primeiro mostrar que H_i é subgrupo de G_k.

i) $H_i \neq \emptyset$. De fato,

$$0 \in G_k,\ 0 \in R^i \Longrightarrow 0 \in H_i.$$

ii) Sendo $g, h \in H_i$ e h' o k-quase-inverso de h temos que $g \circ_k h' \in H_i$. De fato, como temos que $g, h \in G_k$, logo $h' \in G_k$ e ainda, sendo G_k um grupo com a operação $\circ_k$ temos que $g \circ_k h' \in G_k$.

Por outro lado, $g, h \in R^i$ e sabemos que $h \circ_k h' = 0$, ou seja, $h + h' + khh' = 0$. Mas como R^i é um ideal bilateral temos que $khh' \in R^i$, daí $h' = -h - khh'$ pertence a R^i.

Deste modo temos que $g \circ_k h' = g + h' + kgh'$ pertence a R^i.

Concluímos então, de *i)* e *ii)*, que H_i é subgrupo de G_k.

Vamos agora mostrar que H_i é normal em G_k. Para isto, dado $h \in H_i$ queremos verificar que $g' \circ_k h \circ_k g \in H_i$, em que $g \in G_k$ e g' é o seu k-quase-inverso. Sabemos que

$$g' \circ_k h \circ_k g = g' \circ_k (h + g + khg) = g' + h + g + khg + kg'h + kg'g + k^2 g'hg =$$

$$= h + k(hg + g'h + kg'hg),$$

pois $g' + g + kg'g = 0$.

E então como $h \in R^i$ e R^i é um ideal bilateral, concluímos que

$$g' \circ_k h \circ_k g \in R^i.$$

Como $h, g \in G_k$ temos também que $g' \circ_k h \circ_k g \in G_k$, concluindo que $g' \circ_k h \circ_k g \in H_i$ e então H_i é normal em G_k.

Para mostrar a condição 2, devemos mostrar que os elementos de H_{i+1}/H_i comutam com os elementos de G_k/H_i. Tomemos então

$$h \circ H_i \in H_{i+1}/H_i \quad \text{com} \quad h \in H_{i+1} \qquad \text{e}$$

$$g \circ H_i \in G_k/H_i \quad \text{com} \quad g \in G_k$$

e vamos mostrar que

$$(h \circ_k H_i) \circ_k (g \circ_k H_i) = (g \circ_k H_i) \circ_k (h \circ_k H_i)$$

ou equivalentemente, mostrar que

$$h' \circ_k g' \circ_k h \circ_k g \in H_i.$$

De fato, como $h, g \in G_k$, já temos que $h' \circ_k g' \circ_k h \circ_k g \in G_k$. Mas $h \in H_{i+1}$, ou seja, $h \in R^{i+1}$ e como $R^{i+1} \subseteq R^i$, temos que $h, h' \in R^i$.

Daí,

$$h' \circ_k g' \circ_k h \circ_k g = h' \circ_k g' \circ_k (h + g + khg) =$$

$$= h' \circ_k (g' + h + g + khg + k(g'h + g'g + kg'hg)) =$$

$$= h' + h + khg + k(g'h + kg'hg) + kh'(h + khg + k(g'h + kg'hg)) \in R^i,$$

já que R^i é ideal.

Mostramos assim que

$$h' \circ_k g' \circ_k h \circ_k g \in H_i.$$

e então segue-se o resultado da condição 2.

Finalmente, concluímos que G_k é um grupo nilpotente e então pelo teorema 2.3,

$$\mathbb{Z}G_k \simeq \mathbb{Z}H \Longrightarrow G_k \simeq H$$

ou seja, G_k é determinado pelo seu anel de grupo integral como queríamos demonstrar. E ainda podemos concluir que G_k, satisfaz o (Nor).

5.2 O grupo k-círculo como solução para o (Iso) e o (Nor)

Lembrando da apresentação feita no terceiro capítulo a respeito do problema do normalizador vamos considerar R um anel finito e G_k o seu grupo k-círculo. Mostraremos que os p-subgrupos de Sylow de G_k são normais em G_k e então G_k satisfaz as propriedades centrais do nosso trabalho.

Para obtermos tal resultado, faremos uma demonstração análoga à que foi desenvolvida no capítulo anterior.

De fato, temos por definição que se G_k é o grupo k-círculo de R então G_k e R são iguais como conjuntos, além disso, sendo R um anel, temos que R munido com a operação de soma, (R,+), é um grupo abeliano finito e então podemos escrever,

$$(R, +) = A_{p_1} \oplus A_{p_2} \oplus \ldots \oplus A_{p_s}$$

em que $A_{p_1}, A_{p_2}, \ldots, A_{p_s}$ são p_i-subgrupos de Sylow de (R,+).

Vamos mostrar que cada um destes p_i-subgrupos é um ideal de R.

De fato, se $x \in A_p$ e $y \in A_q$ com $p \neq q$, então $xy = 0$ pois, $o(x) = p^n$ e $o(y) = q^m$. Logo,

$$\underbrace{xy + xy + \ldots + xy}_{p^n} = \underbrace{(x + \ldots + x)}_{p^n} y = 0$$

$$\underbrace{xy + xy + \ldots + xy}_{q^m} = x \underbrace{(y + \ldots + y)}_{q^m} = 0$$

e então $o(xy)|p^n$ e $o(xy)|q^m$ sendo $o(xy) = 1$ e portanto $xy = 0$.

Por outro lado se $x, y \in A_p$ então, tomando no desenvolvimento acima $p = q$, temos que $o(xy)|p^n$ e portanto $o(xy) = p^m$ logo $xy \in A_p$.

Considerando $a \in R$ e $b \in A_{p_i}$ temos que $a = a_{p_1} + a_{p_2} + \ldots + a_{p_s}$ e logo $ab = a_{p_i}b \in A_{p_i}$ e $ba = ba_{p_i} \in A_{p_i}$. Com estas observações concluímos que $A_{p_1}, A_{p_2}, \ldots, A_{p_s}$ são ideais de R.

Temos ainda que $A_{p_i} = G_k \cap A_{p_i}$ é um subgrupo normal de G_k. De fato,

1. $0 \in A_{p_i}$, logo $A_{p_i} \neq \emptyset$;

2. Tome $a, b \in A_{p_i}$ e $b' \in G_k$ o k-quase-inverso de b, ou seja, $b' = -b - kbb'$ e então $b' \in A_{p_i}$ e $a \circ_k b' = a + b' + kab' \in A_{p_i}$;

3. Tome $h \in A_{p_i}$ e $g \in G_k$, teremos que

$$g' \circ_k h \circ_k g = g' + h + g + khg + kg'(h + g + khg) =$$

$$= h + khg + kg'h + k^2 g'hg \in A_{p_i}.$$

Então usando as verificações 1, 2 e 3 concluímos que $A_{p_i} = G_k \cap A_{p_i}$ é um subgrupo normal de G_k e em particular A_{p_1} é um 2-subgrupo de Sylow normal em G_k.

Concluímos então que G_k é uma solução para a propriedade do normalizador.

De modo análogo, verificamos que todos os p-subgrupos de sylow de G_k são normais em G_k e portando este é um grupo nilpotente, satisfazendo ao problema do isomorfismo.

Os resultados obtidos neste capítulo nos dão uma generalização dos resultados apresentados no capítulo anterior de forma que se fizermos aqui $k = 1$, obteremos os resultados anteriores.

Conclusão

No nosso trabalho, abordamos duas questões relevantes na teoria de anéis de grupo integrais, o Problema do Isomorfismo e a Propriedade do Normalizador. A importância de tais propriedades junto ao fato da existência de uma relação entre elas foram decisivas para que tratássemos das duas questões paralelamente.

Após a apresentação das questões centrais e de alguns resultados que foram fundamentais para o decorrer do trabalho, conseguimos mostrar a validade das duas propriedades para os grupos adjuntos, tendo para isto que considerar um anel nilpotente, por outro lado mostramos que no caso em que o anel é radical, seu grupo círculo representa solução para o (Iso) e para o (Nor) e neste caso não foi necessária a hipótese do anel ser nilpotente.

Conseguimos ainda extensões para estes fatos, mostrando que os grupos k-adjuntos (admitindo um anel nilpotente) e os grupos k-círculo são soluções para o (Iso) e para o (Nor).

No caso do grupo círculo acabamos conseguindo uma demonstração alternativa para um dos resultados de Sandling, e com relação aos grupos adjuntos de um anel com unidade e de característica p conseguimos muitas informações a seu respeito na tentativa de mostrar que vale a propriedade do normalizador para tais grupos. Não chegamos a concluir a demonstração, mas acreditamos ter dado um passo importante e continuaremos buscando a conclusão deste resultado.

Durante a pesquisa não obtivemos, nas publicações, demonstrações a respeito do (Nor), considerando grupos adjuntos, círculos ou grupos gerais lineares e também não vimos nada a respeito dos k-adjuntos e dos k-círculo, portanto acreditamos ter apresentado novas classes de grupos que representam soluções positivas para o Problema do Isomorfismo e a Propriedade do Normalizador.

Referências

[1] ALPERIN, J. P.; ROWEN, B. Bell. *Groups and Representations.* New York: Springer-Verlag, 1995.

[2] WEISS, A. Rigidity of p-adic torsion, *Ann. Math.*, v. **127**, p. 317-332, 1988.

[3] COHN, P. M. Automorphisms of two-dimensional linear groups over Euclidean Domains, *J. London. Math. Soc.*, v. **1**, n. **2**, p. 279-292, 1969.

[4] DIVINSKY, N. J. *Rings and Radicals.* Toronto: University of Toronto Press, 1965.

[5] DROZD, Y. A.; KIRICHENKO, V. V. *Finite Dimensional Algebras.* Berlin: Springer-Verlag, 1994.

[6] HERTWECK, M. A counterexample to the isomorphism problem for integral group rings, *Ann. Math.*, v. **154**, n. **1**, p. 115-138, 2001.

[7] JACKOWSKI, S.; MARCINIAK, Z. Group automorphisms inducing the identity map on cohomology, *J. Pure Appl. Alg.*, v. **44**, p. 241-250, 1987.

[8] LI, Y.; SEHGAL, S. K.; PARMENTER, M. M. On the normalizer property for integral group rings, *Comm. Alg.*, v. **27**, p. 4217-4223, 1999.

[9] LOBÃO, T. C. Petit; SEHGAL, S. K. The normalizer property for integral group rings of complete monomial groups, *Comm. Alg.*, v. **31**, p. 2971-2983, 2003.

[10] MAZUR, M. On the isomorphism problem for infinite group rings, *Expo. Math.*, v. **13**, p. 433-445, 1995.

[11] MILIES, C. P.; SEHGAL, S. K. *An Introduction to Group Rings.* Dordrecht: Kluwer Academic Publishers, 2002.

[12] ROGGENKAMP, K. W.; SCOTT, L. L. Isomorphisms of p-adic group rings, *Ann. Math.*, v. **126**, p. 593-647, 1987.

[13] SANDLING, R. Group rings of circle and unit groups, *Math. Z.*, v. **140**, p. 195-202, 1974.

[14] SEHGAL, S. K. *Units in Integral Group Rings*. Harlow: Longman Scientific and Technical, 1993. (Pitman Monographs and Surveys in Pure and Applied Mathematics, **69**)